

Dissertation for Doctor of Philosophy

Researches on Wideband Sensing and
Security of Blockchains

Jehyuk Jang

School of Electrical Engineering and Computer Science

Gwangju Institute of Science and Technology

2021

박 사 학 위 논 문

광대역 신호 획득 및
블록체인의 보안성에 관한 연구

장 재 혁

전 기 전 자 컴 퓨 터 공 학 부

광 주 과 학 기 술 원

2021

Researches on Wideband Sensing and Security of Blockchains

Advisor: Professor Heung-No Lee

by

Jehyuk Jang

School of Electrical Engineering and Computer Science

Gwangju Institute of Science and Technology

A dissertation submitted to the faculty of the Gwangju Institute of Science and Technology in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Electrical Engineering and Computer Science

Gwangju, Republic of Korea

May 17, 2021

Approved by



Professor Heung-No Lee

Committee Chair

Researches on Wideband Sensing and Security of Blockchains

Jehyuk Jang

Accepted in partial fulfillment of the requirements for
the degree of Doctor of Philosophy

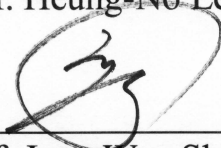
May 17, 2021

Committee Chair



Prof. Heung-No Lee

Committee Member



Prof. Jong Won Shin

Committee Member



Prof. Euseok Hwang

Committee Member



Prof. Jong-Hyok Lee

Committee Member



Prof. Pierre-Olivier Goffard

Dedicated to my family

Ph.D./EC Jehyuk Jang. Researches on Wideband Sensing and Security of
20162010 Blockchains. Electrical Engineering and Computer Science, 2021.
122p. Advisor: Prof. Heung-No Lee.

Abstract

In this dissertation, we discuss two research fields. One is wideband signal sensing via sub-Nyquist sampling of ultra-wideband multiband signals, and the other is the security analysis of blockchains via the profitability analysis of double-spending attacks. In each of the two fields, we provide new results by the virtue of approaching research problems in novel perspectives.

In the field of sub-Nyquist sampling of ultra-wideband multiband signals, we propose a novel idea, intentional aliasing method to improve the sampling performance of a sub-Nyquist sampling system, called modulated wideband converter (MWC). MWCs have been designed to exploit a set of fast alternating pseudo random (PR) signals. Through parallel analog channels, an MWC compresses a multiband spectrum by mixing it with PR signals in the time domain, and acquires its sub-Nyquist samples. Previously, the ratio of compression was fully dependent on the specifications of PR signals. That is, to further reduce the sampling rate without information loss, faster and longer-period PR signals were needed. The implementation of such PR signal generators however results in high power consumption and large fabrication area. With practical PR signals with low complexity, the proposed intentional aliasing method is adopted to improve the

ratio of compression, which results in aliased modulated wideband converter (AMWC). AMWC can further reduce the sampling rate of MWC with fixed PR signals. The main idea is to induce intentional signal aliasing at the analog-to-digital converter (ADC). In addition to the first spectral compression by the signal mixer, the intentional aliasing compresses the mixed spectrum once again. We demonstrate that AMWC reduces the number of analog channels and the rate of ADC for lossless sub-Nyquist sampling without needing to upgrade the speed or the period of PR signals. Conversely, for a given fixed number of analog channels and sampling rate, AMWC significantly improves the performance of signal reconstruction.

In the field of profitability analysis of double-spending attacks on blockchains, we provide new mathematical tools for a precise profitability analysis, which enables us to propose an algorithm for optimization of user parameters utilized to prevent double-spending (DS) attacks. It was well understood that a successful DS attack is established when the proportion of computing power an attacker possesses is higher than that of the honest network. What is not yet well understood is how threatening a DS attack with less than 50% computing power used can be. Namely, DS attacks at any proportion can be a threat as long as the chance to make a good profit exists. Profit is obtained when the revenue from making a successful DS attack is greater than the cost of carrying out one. We have developed a novel probability theory for calculating a finite time attack probability. This can be used to size up attack resources needed to obtain the profit. The results enable us to derive a sufficient and necessary condition on the value of a transaction targeted by a DS attack. Our result is quite surprising: we theoretically show how a DS attack at any proportion of computing power can be made profitable. Given

one's transaction value, the results can also be used to assess the risk of a DS attack. An example of profitable DS attack against BitcoinCash is provided.

The results in the two fields can be integrated and utilized in a field of the Internet of things (IoT). To deal with huge amounts of data, IoT applications need energy-efficient sensors and secure data management system. The intentional aliasing method contributes to improve the efficiency of sensors, and the profitability analysis of double-spending attacks contributes to improve the security of data management by blockchains.

©2021

Jehyuk Jang

ALL RIGHTS RESERVED

Ph.D./EC 장재혁. 광대역 신호 획득 및 블록체인의 보안성에 관한 연구.
20162010 전기전자컴퓨터공학, 2021. 122p. 지도교수: 이홍노.

국 문 요 약

이 논문에서, 우리는 두 연구 분야에 관해 논의한다. 하나는 초 광대역 다중대역 신호의 부분 나이퀴스트 표본화를 통한 광대역 신호 획득이며, 다른 하나는 이중 지불 공격의 수익성 분석을 통한 블록체인의 보안성 분석이다. 각각의 두 분야에서, 우리는 새로운 관점으로 연구 문제에 접근하고 이에 따른 새로운 결과를 제공한다.

초 광대역 다중대역 신호의 부분 나이퀴스트 표본화에 관하여, 우리는 modulated wideband converter (MWC)라 불리는 부분 표본화 시스템의 표본화 성능을 개선하기 위해 고의적 에일리어싱 방법이라는 새로운 아이디어를 제안한다. MWC 는 빠르게 진동하는 유사랜덤 (PR) 신호들을 활용하는 부분 표본화 시스템이다. MWC 는 여러 개의 병렬구조의 아날로그 수신 채널을 통하여 PR 신호들과의 혼합을 통해 다중대역 신호를 압축시킨 후 부분 나이퀴스트 표본들을 획득한다. 이전까지는 신호의 압축 비율이 PR 신호들의 성능에 온전히 의존적이었다. 즉, 신호 손실 없이 표본화 속도를 더 낮추기 위해서는, 더 빠르게 진동하고 더 긴 패턴을 주기로 갖는 PR 신호들이 요구되었다. 그러나 이러한 PR 신호들의 생성기를 구현하기 위해서는 큰 전력 소모를 감수해야 하고 넓은 공정 (fabrication) 면적의 사용이 불가피하다. 실용적이며 구조가 단순한 PR 신호들이 사용되는 MWC 의 압축 비율 개선을 위해 제안된 고의적 에일리어싱 방법을

채택하였으며, 이에 따라 에일리어싱 MWC (AMWC)라는 새로운 표본화 시스템을 제안한다. AMWC 는 PR 신호의 성능을 개선하지 않아도 표본화 속도를 더욱 줄일 수 있다. AMWC 의 핵심 아이디어는 아날로그 디지털 변환기 (ADC)에서 고의적인 신호 에일리어싱을 유도하는 것이다. 결과적으로, PR 신호와의 혼합과정이며 신호 압축이 발생 한 이후에 고의적인 신호 에일리어싱을 통해 한번 더 압축하는 효과이다. 우리는 시뮬레이션을 통해, AMWC 가 PR 신호의 성능 개선 없이 무손실로 신호를 압축표본화 하기 위해 필요한 아날로그 채널의 수와 ADC 의 속도를 크게 감소시킴을 실증하였다. 또한 역으로, 아날로그 채널의 수와 ADC 의 속도가 고정되어 있을 때, AMWC 가 더 복잡한 다중대역 신호의 복원 성능을 크게 개선함을 보였다.

블록체인에 대한 이중 지불 공격의 수익성 분석과 공격 방지법에 관하여, 우리는 수익성 분석을 위한 새로운 수학적 도구를 제공하며, 이를 통해 이중 지불 (DS) 공격 방지에 활용되는 사용자 파라미터들을 최적화 하는 알고리즘을 제안한다. 이전까지 DS 공격의 성공의 충분 조건이 공격자가 점유한 계산 자원이 블록체인 네트워크의 계산 자원보다 큰 것임은 잘 알려져 있었다. 반면 잘 알려지지 않은 것은 공격자가 50% 미만의 자원을 점유하였을 때, 즉 블록체인 네트워크보다 적은 자원을 점유하였을 때 DS 공격이 위협적일 수 있는지에 관한 연구 결과이다. 공격자가 얼마만큼의 계산 자원을 점유하고 있던, 이중지불 공격이 공격자에게 이윤을 가져다 줄 가능성이 있다면, DS 공격은 위협적일 것이다. 이윤이란 DS 공격 수행의 소요 비용보다 수익이 더 큰 경우 발생한다. 우리는 유한한 시간과 DS 공격의 성공에 관한 확률 모델을 개발하였다. 그 결과를 활용하면 DS 공격에 소요되는 비용과 시간의 규모를 예측 할 수 있다. 구체적으로,

우리는 DS 공격이 이윤을 창출 할 수 있도록 하는 거래의 금액에 대한 필요충분 조건을 얻었다. 우리의 결과는 공격자가 어떤 비율의 계산자원을 점유하고 있더라도 DS 공격이 이윤을 창출할 수 있음을 보였다. 이는 곧, 거래할 금액이 주어지면, 사용자는 자신의 거래가 DS 공격으로부터 안전한지 평가 할 수 있음을 의미한다. 우리는 결과를 실용적으로 활용하는 예로써, BitcoinCash 를 상대로 DS 공격이 이윤을 발생시키기 위한 조건을 계산하였다.

서로 다른 두 분야에서 도출된 결과들은 Internet-of-things (IoT) 분야에서 통합 및 활용 될 수 있다. IoT 어플리케이션들은 방대한 양의 빅데이터를 다루기 위하여 에너지 효율이 우수한 센서와 안전한 데이터 관리 시스템을 필요로 한다. 우리가 제안한 고의적 에일리어싱은 센서의 효율 개선에 기여하며, 이중지불 공격의 수익성 분석은 블록체인에 의한 데이터 관리의 보안성 개선에 기여한다.

©2021

장 재 혁

ALL RIGHTS RESERVED

List of Contents

Abstract	i
List of Contents	vii
List of Tables	x
List of Figures	xii
Chapter 1 Introduction	1
1.1. Motivation.....	1
1.2. Preliminaries	2
1.2.1. Compressed Sensing	2
1.2.2. Blockchain and Double-Spending Attacks	5
1.3. Dissertation Outline and Summaries	8
1.3.1. Dissertation Outline	8
1.3.2. Summary of Chapter 2.....	8
1.3.3. Summary of Chapter 3.....	9
Chapter 2 Intentional Aliasing Method to Improve Sub-Nyquist Sampling System	11
2.1. Introduction.....	11
2.1.1. Related Works.....	12
2.1.2. Contributions.....	13
2.1.3. Contents of Chapter	14
2.2. Modulated Wideband Converters (MWC).....	14
2.2.1. Conventional MWC.....	18
2.2.2. Choosing PR Signals for Conventional MWC.....	20
2.2.3. Sampling Efficiency.....	23
2.2.4. Limitation of Conventional MWC.....	26
2.3. Aliased Modulated Wideband Converters (AMWC)	27
2.3.1. Problem Formulation	27
2.3.2. Intentional Aliasing Method	29
2.3.3. Input-Output Relationship of AMWC.....	36

2.3.4. Choosing the Aliasing Parameter	41
2.3.5. Improvement of Sampling Efficiency	42
2.4. Non-Ideal Low-Pass Filters	43
2.5. Simulation	48
2.5.1. Spark of Sensing Matrix	48
2.5.2. Reduction of Total Sampling Rate	52
2.6. Conclusion	57
Appendices.....	57
Appendix 2.A Proof of Lemma 2.2	57
Appendix 2.B Proofs of Proposition 2.4 and Lemma 2.7.....	59
Appendix 2.C Proof of Proposition 2.5.....	63
Chapter 3 Profitable Double-Spending Attacks	66
3.1. Introduction.....	66
3.1.1. Contributions.....	69
3.1.2. Contents of Chapter	70
3.2. The Attack Model	70
3.2.1. Attack Scenario.....	71
3.2.2. Stochastic Model	72
3.2.3. DS Attack Achieving Time.....	74
3.3. The Attack Probabilities	76
3.4. Profitable DS Attacks	80
3.5. Practical Example of Profitable DS Attacks against BitcoinCash.....	87
3.6. Related Works.....	88
3.7. Checking Formulas by Monte Carlo Experiments	92
3.8. Conclusions.....	97
Appendices.....	98
Appendix 3.A Proof of Lemma 3.5	98
Appendix 3.B Proofs of Corollary 3.6 and Proposition 3.8	100
Appendix 3.C Proof of Proposition 3.7.....	105
Appendix 3.D Comparison of Attack Success Probability with [65]	108

Appendix 3.E Generalized Hypergeometric Function [81].....	109
Chapter 4 Summary of Contributions and Future Research Direction.....	111
4.1. Summary of Contributions.....	111
4.1.1. Contributions to Ultra-Wideband Sub-Nyquist Sampling of Multiband Signals	111
4.1.2. Contributions to Profitability Analysis of Double-Spending Attacks on Blockchains	112
4.2. Future Research Direction	113
Bibliography.....	115

List of Tables

Table 2.1	Sampling system of AMWC. The system is equivalent to cMWC when $p = 1$ and $q' = q$. In AMWC, the sampling rate is p -times lower than the filter bandwidth with $p > 1$ to intentionally induce aliasing.....	28
Table 2.2	Summary of AMWC Parameters (cMWC when $p = 1$ and $q' = q$).....	40
Table 2.3	The Total Sampling Rate Required for 90% Support Recovery Rate with Various SNR and Values of p . The floating numbers in cells indicate the minimal total sampling rate in GHz which achieves the support rate recovery of 90%. The number of analog channels and multibands were set to $M = 3$ and $K_B = 10$, respectively.....	56
Table 3.1	Numerical computations of required resources for profitable DS attacks with $p_A = 0.35$ when $t_{cut} = cN_{BC}\lambda_H^{-1}$ with $c = 4$	85
Table 3.2	Numerical computations of required resources for profitable DS attacks with $p_A = 0.4$ when $t_{cut} = cN_{BC}\lambda_H^{-1}$ with $c = 4$	86
Table 3.3	A pseudo-code to simulate the stochastic behavior of double-spending attacks modeled in sub-section 3.2.2.	95
Table 3.4	Comparisons of the probabilities of successful double-spending attacks for given block confirmation number N_{BC} and attacker's computational proportion p_A when cut-time is set to $4N_{BC}\lambda_H^{-1}$ for $\lambda_H^{-1} = 600$ seconds. The values on the columns labeled "Calculation" are obtained from the calculation of equation (3.19). The values on the	

columns labeled “Experiment” are obtained from Monte Carlo tests
using Table 3.3.....95

List of Figures

- Figure 2.1 Sampling system of AMWC. The system is equivalent to cMWC when $p = 1$ and $q' = q$. In AMWC, the sampling rate is p -times lower than the filter bandwidth with $p > 1$ to intentionally induce aliasing.17
- Figure 2.2 Successful recovery rates of all nonzero subbands of $X(f)$ from RPFMWC for various lengths M of the base sequence and numbers m of channels. The number of mutlibands is $K_b = 4$.The sparsity of sensing model is $K \leq 2K_b$22
- Figure 2.3 Sampling system of AMWC. The system is equivalent to cMWC when $p = 1$ and $q' = q$. In AMWC, the sampling rate is p -times lower than the filter bandwidth with $p > 1$ to intentionally induce aliasing.....25
- Figure 2.4 Principle of improving the sampling efficiency by AMWC at a single analog channel is illustrated, with setting $q = 3$, $q' = q$, $p = 2$, and $m = 3$. At the first stage, the input spectrum $X(f)$ is aliased by mixing it with the PR signal and low-pass filtering it. This aliased-version of $X(f)$ is depicted as $Y_i(f)$. In (a), the main difference between cMWC and AMWC is how to take time-samples of $Y_i(f)$. cMWC prevents the spectrum from being aliased in taking time-samples. AMWC, on the contrary, aims to make the spectrum $Y_i(f)$ intentionally aliased once again, as depicted as $\tilde{Y}_i(f)$ in (b). In (c), as a result, the splitting-interval of cMWC is f_p , whereas in (d), that

of AMWC is halved to f_p' . Thus, the sampling efficiency of AMWC becomes doubled (as $p = 2$).	35
Figure 2.5. Independency rates under various p and q' for which randomly selected Mq' columns of the sensing matrix $\mathbf{D} \in \mathbb{C}^{Mq' \times N}$ of AMWC are independent. When p and q' are coprime and $q' > p$, every selection of Mq' columns is linearly independent.	47
Figure 2.6. Rate of successful support recovery of cMWC and AMWC as a function of total sampling rate for various aliasing parameters p and multibands K_B . The number of channels was fixed to $M = 3$. Ideal ((a)-(b)) and random ((c)-(d)) low-pass filters were used.	49
Figure 2.7. Rate of successful support recovery of cMWC and AMWC as a function of total sampling rate when SNR=3 [dB]. The number of channels was fixed to $M = 3$, and the number of multibands in $X(f)$ is fixed to $K_B = 10$. Ideal (a) and random (b) low-pass filters were used.	50
Figure 2.8. Rate of successful support recovery of cMWC and AMWC as a function of sampling rate of each channel for various aliasing parameters p and the number of channels M . The number of multibands was fixed to $K_B = 10$. Ideal (a) and random (b) low-pass filters were used	51
Figure 3.1. Computation power distribution among the largest mining pools provided by <i>BTC.com</i> (date accessed: Nov. 24, 2020).	68
Figure 3.2. Comparisons of the probability distributions of the time spent for a success of double-spending attack when attacker's computational proportion is (a) $p_A = 0.25$ and (b) $p_A = 0.45$. Block confirmation number and cut-time are set to $N_{BC} = 5$ and $t_{cut} = 4N_{BC}\lambda_H^{-1}$ for	

$\lambda_H^{-1} = 600$ seconds, respectively. The bars on both subplots are histograms of $\hat{\mathbf{f}}_{T_{AS}}$ obtained from Monte Carlo tests in Table 3.3. The red curves on both subplots are the calculation of equation (3.21).....96

Chapter 1

Introduction

1.1. Motivation

The advances of electronic devices and wireless communication technologies have facilitated small devices to communicate with each other. The Internet of things (IoT) depends on the reliability of data, i.e., it needs to collect and manage huge amounts of data from all things connected to internet in order to optimize numerous problems arising in various applications from industry to daily life [1]. This data reliability still has challenges to be addressed such as the energy efficiency of sensors to obtain more high-quality data, the capacity of data storage, the reliability and credibility of data, and secure management of data for immutability [2], [3].

In this dissertation, we focus on two key technologies to solve the challenges of data reliability, which are compressed sensing and blockchain.

Compressed sensing provides energy-efficient analog-to-digital sensors. Literature [3] have reported real-world applications of the integration between IoT applications and compressed sensing. Specifically, a compressed sensing system makes a compression of analog signal which can be sparse in a certain domain of linear basis, and then digitizes it. The compression should be lossless, which are supported by signal recovery algorithms based on compressed sensing theory. This reduces the number of sensors required to obtain a larger amount of data while keeping the original quality of data. A challenge on sensors equipped with the compressed sensing is, however, an increased complexity of hardware implementation due to additional functionality for the analog signal compression. In Chapter 2 of this dissertation, we will propose an idea for a sensor in order to reduce the hardware complexity and improve the performance of analog signal compression.

Blockchain provides immutable peer-to-peer distributed database. Blockchain is a chain of data blocks, i.e., the previous block affects the contents of the next block. This structure technically keeps data immutable. Specifically, in order to publish a block, a sufficient number of peers must make a consensus for the process after checking the validity of block contents. Thus, it is impossible for a peer to manipulate the contents of block published in the past, and any change of block requires a consensus of a large number of distributed peers. This distributed property not only improves the reliability and credibility of data but also enables the secure management of data for immutability.

Examples of the integration between IoT applications and blockchain have been surveyed in [2]. In the literature, the authors reported that blockchain has increased the autonomy of IoT devices by virtue of easy interaction with reliable information in transparent distributed database. But they also pointed that challenges still remain. First, storage capacity and scalability problem arise from the huge volume of blockchain database. It requires newly participating peers to have large storage capacity, and therefore it demotivates them. Second, anonymity and data privacy problem arise from the transparency of blockchain, as many IoT applications deal with confidential data obtained from person such as e-health records. Last, security problem by network attacks is critical as many real-world instances have been reported. Fortunately, a cryptographic technology, zero-knowledge proofs would be helpful to solve the first and second problems. Combining with the recent advances in zero-knowledge proofs [4], the capacity of data storage can be dramatically reduced [5], and the privacy of data can also be kept. In addition, in Chapter 3 of this dissertation, we will provide a security analysis for a type of network attack called double-spending attack that will be helpful to improve the security of blockchain.

1.2. Preliminaries

1.2.1. Compressed Sensing

A compressed sensing (CS) [6]–[10] is a signal processing framework that includes from signal acquisition to post-processing. The signals of interest are sparse signals, which can

be sparsely represented in a particular domain. In other words, a signal is sparse if there exists a domain on which the isomorphic projection has a small proportion of non-zero values. In a sparse signals, only a few non-zero elements can have uncertainty, which implies that they can be compressed into shorter-length measurements without any perceptual loss [7].

A CS aims to convert a sparse analog-signal into a digital compression. A digital compression is a result of analog encoding and has a shorter length than a directly-digitized version. If an original signal is sparse enough and an encoding is well-designed, a short digital compression can be decoded for a recovery of a directly-digitized version. As a result, compared to direct conversion of an analog signal to digital, obtaining a digital compression from a CS reduces the number of sensors required for lossless digitalization. Examples of applications include analog-to-digital conversion (ADC) of wideband radio frequency signals at a sub-Nyquist sampling rate [11], [12], hyperspectral imaging [13], holography [14], magnetic resonance imaging [15], and ultrasound imaging [16].

Formally, we express a *signal* by $\mathbf{x} \in \mathbb{C}^n$, a linear encoding by $\mathbf{A} \in \mathbb{C}^{m \times n}$ called a *sensing matrix*, and a digital compression by $\mathbf{y} \in \mathbb{C}^m$ called a *measurement*. We consider \mathbf{x} is *k-sparse*, which means there exists a unitary linear basis $\mathbf{F} \in \mathbb{C}^{n \times n}$ for $\mathbf{s} = \mathbf{F}^{-1}\mathbf{x}$ such that \mathbf{s} has at most k nonzero entries supported by a set \mathcal{S} of indices for the nonzeros. For given \mathbf{y} and \mathbf{A} with $m < n$, a CS problem is to find an inverse solution \mathbf{x} such that

$$\mathbf{y} = \mathbf{A}\mathbf{x}. \quad (1.1)$$

In general, there can exist infinitely many solutions of \mathbf{x} , since the linear system of (1.1) is underdetermined as the number of indeterminate variables in \mathbf{x} is greater than the number of observations in \mathbf{y} . Thus, we need to relax the problem (1.1) to

$$\mathbf{y} = \mathbf{\Phi}\mathbf{s}, \quad (1.2)$$

where $\mathbf{\Phi} = \mathbf{A}\mathbf{F}$. The inverse problem now turns to finding the support set \mathcal{S} . Once the supports are given, the linear system (1.2) is equivalent to a overdetermined linear system

$\mathbf{y} = \Phi_{\mathcal{S}} \mathbf{s}_{\mathcal{S}}$, where $\mathbf{s}_{\mathcal{S}} \in \mathbb{C}^k$, i.e., the unique solution to minimize the L^2 norm $\|\mathbf{s}_{\mathcal{S}}\|_2$ such that the linear equations hold can be found.

To define the problem to find the supports \mathcal{S} from the equations (1.2), Donoho has defined a special function called L^0 “norm”, which counts the number of nonzero elements. Formally, for a vector \mathbf{s} of length n , the L^0 “norm” $\|\mathbf{s}\|_0 := \sum_{i=1}^n s_i^0$ [6]. For (1.2), the problem to find the supports \mathcal{S} can be solved by

$$\arg \min_{\mathbf{s}} \|\mathbf{s}\|_0 \text{ s.t. } \mathbf{y} = \Phi \mathbf{s}. \quad (1.3)$$

A well-known result on the existence of the unique solution of (1.3) uses the spark of a matrix. The spark of a matrix Φ is the smallest number l such that there exists a set of l columns in Φ which are linearly dependent. In other words, $\text{spark}(\Phi) := \min_{\mathbf{s} \neq 0} \|\mathbf{s}\|_0$ s.t. $\Phi \mathbf{s} = 0$. The spark of a m -by- n matrix Φ for $m \leq n$ cannot be not greater than $m+1$. A sufficient and necessary condition for the problem (1.3) to have the unique solution is given by

$$k < \frac{\text{spark}(\Phi)}{2}. \quad (1.4)$$

If Φ has the maximum spark, i.e., $\text{spark}(\Phi) = m+1$, the condition (1.4) turns to $m \geq 2k$. In short, if $m \geq 2k$ and Φ has the full maximum, the underdetermined inverse problem for (1.1) is well-defined.

Satisfying condition (1.4) the existence of unique solution, but does not provide a practical algorithm to find it. The problem (1.3) is an NP problem. Candes *et al.* have relaxed problem (1.3) to a sub-optimal L^1 norm minimization such that

$$\arg \min_{\mathbf{s}} \|\mathbf{s}\|_1 \text{ s.t. } \mathbf{y} = \Phi \mathbf{s} \quad (1.5)$$

for a small ε and have shown that the relaxation (1.5) has a unique and sparse solution if Φ has a special property, restricted isometry property (RIP) [17]. Including the solver of (1.5), many practical algorithms such as greedy algorithms have been proposed [18].

In some applications, it is possible to acquire multiple snapshots of measurements. Multiple measurements can be more helpful to find supports \mathcal{S} , if they are independent. We denote a bunch of l sparse signals $\mathbf{S} \in \Phi^{n \times l}$ and the corresponding measurements by $\mathbf{Y} \in \mathbb{C}^{m \times l}$ in a relationship

$$\mathbf{Y} = \Phi \mathbf{S}. \quad (1.6)$$

We assume all l columns of \mathbf{S} share a supports set \mathcal{S} . For a fixed k , recovery of \mathbf{S} from the multiple measurement vectors (MMV) \mathbf{Y} requires a smaller number m of sensors than the single measurement vector (SMV) problem in (1.2). By Chen and Huo [19] and Davies [10], a sufficient and necessary condition for the problem (1.6) to have the unique solution is given by

$$k < \frac{\text{spark}(\Phi) - 1 + \text{rank}(\mathbf{Y})}{2}. \quad (1.7)$$

In short, for a MMV model, if Φ and \mathbf{Y} with $m \leq k$ respectively has the maximum spark $m+1$ and the maximum rank m , the condition (1.7) turns to $m \geq k+1$, which is more relaxed than the condition $m \geq 2k$ for a SMV model. The multiple snapshots can replace some of sensors. Many practical algorithms to solve MMV recovery models have been proposed [18].

1.2.2. Blockchain and Double-Spending Attacks

Blockchain is distributed data maintenance protocol working on a peer-to-peer network. Early design of blockchain given in Bitcoin [20] by Satoshi Nakamoto mainly has focused on secure storage of cryptocurrency transactions. But recent applications for example IoT have demanded blockchain as a data storage [2]. Publishing and distributing a new data block or a modification of a previous data block requires a consensus of a large number of

unspecified peers. This distributed structure of blockchain with cryptographies makes data transparent and immutable.

The data structure of blockchain is called *chain*. A chain consists of *blocks*, and a block is composed of its block header and *transactions*. A transaction is a digital file which records a data including an exchange of cryptocurrency. As a transaction is digital, the data in it can be encrypted for privacy, e.g., ZCash (formerly Zerocash) [21]. Every block is chained in series with previous blocks by a cryptographic hash function [22], i.e., in every block header, the hash of the previous block is written. To chain a new block, a peer must make a proof of examination of the validity of block and append the result into the block header.

The procedure of publishing a block follows a communication protocol called *consensus*. There are many sorts of consensus depending on the type of the block validity proofs, e.g., Proof-of-Work (PoW), Proof-of-Stake (PoS), practical Byzantium fault tolerance algorithm (PBFT) [23]. PoW picks a block validator through competition of computation resources. PoW allows anyone having a computer to contribute to the consensus, but it also comes with disadvantages. When the competition is overheated due to the increase of the number of participants, excessive amount of computations are used, which in turn accelerates the destruction of the natural environment by huge energy consumption. In addition, for a newly launched blockchain, its small scale network can be centralized by the other large blockchain networks that already have huge computational resources. Moreover, to prevent a chain from being forked, blockchains equipped with PoW would set the period of block generation to be long. These disadvantages are the reason why a blockchain equipped with PoW cannot be easily commercialized. To overcome the disadvantages of PoW, PoS would pick a block validator through competition of stakes. This mechanism may imply PoS networks centralized by the rich. PBFT usually validates a block through communications of permissioned committee members. Blockchains equipped with PBFT would limit the number of committee members due to the delay by the communication of a lot of messages. These pros and cons of the consensus methods are often called blockchain trilemma to categorize them in three-folds such as decentralization, scalability, and security [24]. As no consensus that solves the trilemma at once has been proposed up to the date, recent blockchains often combines the existing consensus methods depending on applications [25].

Throughout this dissertation, we focus on blockchains equipped with PoW. PoW requires a peer to generate a proof of solving a cryptographic puzzle using a cryptographic hash function. Specifically, a peer uses a hash function, where the input is a block data combined with a changeable nonce value. The peer repeats making the hash until the output is less than a given threshold while changing the nonce. Once the peer finds the solution nonce, it appends it into the block header as a proof. Since cryptographic hash functions are irreversible and behaves like a random function, PoW takes intractable amount of computations. Blockchain system allows the first solver of cryptographic puzzle to issue cryptocurrency, which incentivizes the participation of new peers into the competition of PoW. After molding a block with the nonce and attaching it to the chain, the updated chain is spread to a peer-to-peer network. Meanwhile, all peers who download a new chain from the network need to make a decision whether to accept it or not. Only one chain survives in their local storage. To resolve the conflict of existing two or more different chains called *forks*, for example, a node is programmed to choose the longest chain and discard the rests. This rule for PoW used in Bitcoin is called *longest chain consensus*. There is also the other consensus for PoW called GHOST used in Ethereum [26]. A consensus resolves the conflict when two or more groups of peers temporarily hold different forks due to network problems such as propagation delays.

The design goal of blockchain is to keep immutability of block contents. For example, in blockchain with the longest chain consensus, a group of peers who try to modify a block previously published needs to resolve the cryptographic puzzles for all the next blocks chained after it, as the contents of the blocks have been changed. However, this modification can be realizable, if a peer group invests a huge amount of computation resources for running a cryptographic hash function which is comparable to the sum of computation resources used by all the other peers in the network. If so, there is a possibility to make the modified fork longer than the current longest chain called the *status-quo chain* in order to convince the other peers. Attacks exploiting this weak point are called *double-spending attacks* [20].

Double-spending (DS) attacks aim to double-spend cryptocurrency for the price of a goods or services that has been already delivered. To double spend, attackers need to replace the status-quo chain in the network with their new one, after taking the goods or services.

Nakamoto [20] and Rosenfeld [27] have shown that the higher computing power is employed, the higher probability to make a DS attack successful is. In addition, if an attacker invests more computing power than that invested by the honest network, a success of DS attack is guaranteed. Such attacks are called the 51% attack. Unfortunately, for small scale blockchains, double-spending attacks have been realized many times. For example, in 2018 and 2019 *Verge*, *BitcoinGold*, *Ethereum Classic*, *Feathercoin*, and *Vertcoin* suffered from DS attacks and millions of US dollars were lost [28].

1.3. Dissertation Outline and Summaries

1.3.1. Dissertation Outline

In Chapter 2, we will discuss ultra-wideband sub-Nyquist sampling of multiband signals. We will propose a compressed sensing-based analog-to-digital sensing system to improve the energy efficiency of sensors. By the results of Chapter 2, we expect that our system can contribute to solve the sensor efficiency problem by data reliability in IoT applications. In Chapter 3, we will study the profitability of double-spending attacks on blockchains equipped by PoW and applying the longest chain rule. One of our results gives a necessary and also sufficient condition to economically motivate double-spending attackers. This can be used to come up with a strategy, conversely, to demotivate the attackers [29]. The results of Chapter 3 can contribute to solve the data immutability and credibility problems by data reliability in IoT applications. Finally, Chapter 4 summarizes the contributions of this dissertation and suggests future research directions.

1.3.2. Summary of Chapter 2

Prior works have given a practical solution for efficient sub-Nyquist sampling of multiband signals spread over a wideband up to few gigahertz. Increasing their receiving bandwidth to an ultra-wideband of tens of gigahertz, however, requires impractical hardware implementation. In Chapter 2, we will propose a new idea to solve the problem, which is intentional aliasing method. Specifically, to cover an ultra-wideband bandwidth, our approach intentionally allows a well-controlled aliasing at the sampling device. This

intentional aliasing has the effect of replacing the requirement of impractical hardware, at the cost of increased computational complexity in post-digital signal processing. Ideally, with the proposed method, the sampling efficiency of a sub-Nyquist sampling system can reach a theoretical limit without the aid of impractical hardware.

The contents of Chapter 2 have been partially published in [11], [30]:

[11] Jehyuk Jang, Sanghun Im, and Heung-No Lee, “Intentional aliasing method to improve sub-Nyquist sampling system,” *IEEE Trans. Signal Process.*, vol. 66, no. 12, pp. 3311-3326, Apr. 2018.

[30] Jehyuk Jang, Nam Yul Yu, and Heung-No Lee, “A study on mixing sequences in modulated wideband converters,” in *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Washington DC, DC, USA, Dec. 2016.

1.3.3. Summary of Chapter 3

By Satoshi Nakamoto, it has been well known that running a majority portion of computing resources, i.e., occupation of more computing resources by a party of attacker nodes than honest full-nodes, always leads to the success of a double-spending attack [20]. What is less well-known, on the other hand, is the risk of double-spending attacks that use a minority of computing resources, minority double-spending attacks. The success of minority double-spending attacks is not guaranteed, but still it can be expected to bring significant returns. In Chapter 3, we will provide mathematical tools to calculate the expected profit of all double-spending attacks including ones running a minority of computing resources. Our tools will enable us to derive sufficient and necessary conditions for profitable double-spending attacks.

The contents of Chapter 3 have been partially published in [29], [31]:

[31] J. Jang and H.-N. Lee, “Profitable Double-Spending Attacks,” *Applied Sciences*, vol. 10, no. 23, p. 8477, Nov. 2020.

[29] J. H. Jang and H. N. Lee, "Transaction Verification System for Blockchain, and Transaction Verification Method for Blockchain," patent, PCT/KR2019/017571, Nov. 12, 2019.

Chapter 2

Intentional Aliasing Method to Improve Sub-Nyquist Sampling System

2.1. Introduction

Applications of electronic warfare (EW) systems, electronic intelligence (ELINT) systems, or cognitive radios are demanding the observation of a multiband signal, i.e., a collection of multiple narrow-band signals, each with different center frequencies, scattered across a wide frequency range up to tens of gigahertz (GHz). The Nyquist sampling rate is twice the maximum frequency of the wide range. When a multiband signal is *sparse*, i.e. consists of a few narrow bands, the signal can be sampled without information loss at a sub-Nyquist rate far less than the Nyquist rate. The theoretical lower limit of the rate required for lossless sub-Nyquist sampling is the sum of the bandwidths, known as the Landau rate, when the spectral locations of all the narrow-band signals are known [32]. When spectral locations are unknown, the lower limit is doubled [33].

The modulated wideband converter (MWC) proposed by Mishali *et al.* [12] is a lossless sub-Nyquist sampler that aims at achieving the theoretical lower limit of sampling rate. Similar to other sub-Nyquist samplers proposed in [34]–[36], MWC exploits pseudo-random (PR) signals, which periodically output pulsed patterns. MWC has multiple analog channels, each of which consists of a PR signal generator, signal mixer, low-pass filter (LPF) for anti-aliasing, and low-rate analog-to-digital converter (ADC) in sequence. The system compresses a multiband spectrum through the mixing and LPF procedures, following which it samples at a sub-Nyquist rate. The reconstruction of the input multiband spectrum is guaranteed under some conditions of the compressed sensing (CS) theory [6]–[10]. With the help of CS reconstruction algorithms in [33], [37] developed for the MWCs,

it has been proved that an MWC can achieve the theoretical lower limit of the lossless sub-Nyquist sampling rate.

However, to achieve the lower limit of the lossless sub-Nyquist sampling rate, the previously proposed MWC by Mishali *et al.* relied on a high-end PR signal generator, since it was the only spectral compressor. The ratio of spectral compression was fully dependent on the *oscillation speed* and *length of the pulsed patterns* within a single period of the PR signals. Specifically, to improve the compression ratio for a sparser multiband signal, PR signals with a greater pattern length were required. In addition, the oscillation speed should be faster than the Nyquist rate for a lossless compression. Unfortunately, increasing the pattern length of a PR signal generator with tens of GHz-range switching speed leads to difficult research problems in the field of chip engineering, such as high power consumption and large fabrication area due to the high chip speed [38], [39], which hinder the commercial availability of such a PR signal generator chip.

In this Chapter, we aim to reduce the lossless sub-Nyquist sampling rate for given practical PR signals. To this end, we propose an aliased MWC (AMWC). The main idea of AMWC is to break the anti-aliasing rule and induce *intentional aliasing* at the ADC of each spatial channel by setting the bandwidth of the prior LPF to be greater than the ADC sampling rate. In addition to the first spectral compression by the mixing and LPF procedures, this intentional aliasing leads to another spectral compression under a certain relation between the ADC sampling rate and bandwidth of the prior LPF. Through the two spectral compression procedures, the compression ratio is improved without faster or longer PR signals. Consequently, for a given and fixed PR signal generator, the lossless sub-Nyquist sampling rate of AMWC is closer to the lower limit than that of MWC.

2.1.1. Related Works

Efforts to reduce the rate for lossless sub-Nyquist sampling with MWC closer to the theoretical lower limit without upgrading the PR signal generators have been made in [40], [41]. In [40], the authors proposed a method that channelizes the multiband spectrum into few orthogonal subbands before mixing with the PR signals. Since the channelized signals have a lower Nyquist rate than the original input, for a given oscillation speed and pattern

length of PR signals, the method achieves a higher ratio of spectral compression. Although the method led to a further reduction of the lossless sub-Nyquist sampling rate, it requires additional hardware resources for the channelization, such as band-pass filters, local oscillators, and a greater number of independent PR signal generators proportional to the number of subbands. In [41], a method similar to that proposed in [40] was presented, in which the input signal was divided into in-phase (I) and quadrature (Q) channels before mixing it with PR signals. The lossless sub-Nyquist sampling rate can be reduced by the same principle as in [40], although the authors did not mention this point. However, the system also required additional hardware resources for the I-Q division.

The proposed AMWC achieves the same effect as in previous works [40], [41], i.e., reduction in the lossless sub-Nyquist sampling rate without upgrading the PR signal generators, but unlike [15] and [16], it does not require additional hardware components. To our knowledge, AMWC is *novel* in that no study has thus far improved the sub-Nyquist sampling capability of MWC by improving the utilization efficiency of given hardware resources.

In [42], [43], variations of MWC similar to AMWC that include aliasing at the ADC have been investigated for analyzing channel capacity. Their main results indicate that suppressing non-active subbands before spectral compression minimizes the loss of information rate incurred by aliasing the noise spectrum. Interestingly, the authors of [43] introduced a rule for determining the sampling rate of each spatial channel similar to that of AMWC (see Section 2.3.2 for details). However, the rule was designed to make a fair comparison with other filterbank-based systems by flexibly controlling the bandwidth of subbands, rather than to exploit the aliasing at the ADC to reduce the lossless sub-Nyquist sampling rate. Additionally, according to our results, the rule in [43] is insufficient and aliasing at the ADC may lead to information loss.

2.1.2. Contributions

Our main contribution is that the anti-aliasing rule of MWC is shown to be unnecessary for lossless sub-Nyquist sampling. We reveal a certain relationship between the ADC sampling rate and bandwidth of the prior LPF so that AMWC can avoid the loss of signal information

during the additional spectral compression. We demonstrate that, for given oscillation speed and pattern length of PR signals, the sampling rate and analog channels of AMWC required for the reconstruction of a multiband signal are further reduced. For given sampling rate and number of analog channels, we show that the reconstruction performance of AMWC for a multiband signal with a given sparsity is improved.

Additionally, we show that the benefits from intentional aliasing can be further strengthened using a non-flat LPF. The non-flat frequency response of LPF results in a different input-output relationship for each frequency component of the sub-Nyquist samples of AMWC. Simulation results show that the reduction of lossless sub-Nyquist sampling rate is boosted when the filter response is samples of a random distribution as the input-output relationships of different frequency components become independent.

2.1.3. Contents of Chapter

The remainder of this chapter is organized as follows. In Section 2.2, we briefly introduce MWC with the anti-aliasing rule and then discuss the performance limitation. In Section 2.3, we propose AMWC and derive its input-output relationship. The relationship between the sampling rate of ADC and bandwidth of LPF to avoid information loss is also provided. In Section 2.4, a revised input-output relationship of AMWC corresponding to the use of a non-ideal LPF is provided. Simulation results are provided in Section 2.5. Section 2.6 concludes this chapter with summarizing contributions.

2.2. Modulated Wideband Converters (MWC)

Throughout this chapter, signals to be digitalized are multiband radio frequency (RF) signals. An RF signal $x(t)$ is a multiband signal if its spectrum $X(f)$ on positive frequency $f > 0$ is composed of K_B disjoint continuous bands of maximum bandwidth B , for any $K_B \in \mathbb{N}$ and $B \in \mathbb{R}^+$ [12], [33]. We assume the center frequencies of K_B bands in $X(f)$ are unknown. We assume that the maximum frequency of a target

multiband signal does not exceed f_{\max} , i.e., $X(f)=0$ for $f \in \mathcal{F}_{\text{NYQ}}^c$, where $\mathcal{F}_{\text{NYQ}} \triangleq [-f_{\max}, f_{\max})$, and $\mathcal{F}_{\text{NYQ}}^c$ is the complementary set of \mathcal{F}_{NYQ} . We denote the Nyquist rate by $f_{\text{NYQ}} \triangleq 2f_{\max}$. We assume spectrally sparse $x(t)$ such that actual spectral occupancy BK_B is far smaller than the maximum frequency f_{\max} , i.e., $BK_B \ll f_{\max}$.

To take samples $x[N]$ of $x(t)$ without loss, Nyquist sampling theorem provides a sufficient condition for the sampling rate, which is the Nyquist sampling rate f_{NYQ} . Taking samples of a signal at the Nyquist sampling rate prevent the spectrum from being aliased.

Another optimal sampling rate is Landau rate [32], which gives the minimum sampling rate BK_B required for lossless sampling of multiband signals. When the center frequencies of multi-bands are known, it is easy to realize a sampling system working at the Landau rate: for each of K_B bands in a signal $x(t)$, we can modulate the signal in order to shift the center of band to zero, take a low-pass filter of bandwidth B , and finally take samples at rate B . Since multi-bands are fragmented and then respectively sampled at a sufficiently high sampling rate, they are not aliased among themselves. Therefore, the original signal $x(t)$ can be reconstructed.

When the center frequencies of multi-bands are unknown, the minimum sampling rate required for lossless sampling of a multiband signal $x(t)$ is doubled from Landau rate, i.e., the minimum sampling rate is $2BK_B$ [33]. In this case, the realization of a sampling system working at the minimum rate is quite challenging. When $BK_B \ll f_{\text{NYQ}}$, i.e., $x(t)$ is spectrally sparse, then compressed sensing theory [7] can be applied to realize a practical sampling system for unknown center frequencies of multi-bands working near the minimum rate.

MWC is a sub-Nyquist sampling system exploiting PR signals for spectral compression. MWC consists of M analog channels in parallel (see Figure 2.1-(a)). Each channel consists of a PR signal generator, a mixer, an LPF, and an ADC in sequence. Each PR signal $p_i(t)$ for channel index i is T_p -periodic and outputs chips of an odd length L within a single

period T_p . Each chip lasts for a chip duration $T_c = T_p L^{-1}$. We denote the chip speed by $f_c \triangleq T_c^{-1}$ and the repetition rate of the PR signal by $f_p \triangleq T_p^{-1}$. The LPF has a cut-off frequency $W_{LPF}/2$, where W_{LPF} denotes the bandwidth of the filter including negative frequency. The LPF bandwidth is set to $W_{LPF} = qf_p$, where q is the channel-trading parameter, an odd positive integer. Finally, we denote the sampling rate, which is equal at every channel, by f_s . The total sampling rate is the sum of sampling rates of all channels, defined by $f_{s,total} \triangleq Mf_s$.

MWC first compresses the input multiband spectrum using PR signals. After that, nonzero subbands of the multiband spectrum are recovered by CS recovery algorithms. For the successful CS recovery, all spectral components within the Nyquist range \mathcal{F}_{NYQ} of each PR signal are needed to be independent, which requires a fast chip speed $f_c \geq f_{NYQ}$ [12]. Throughout this chapter, we set $f_c = f_{NYQ}$.

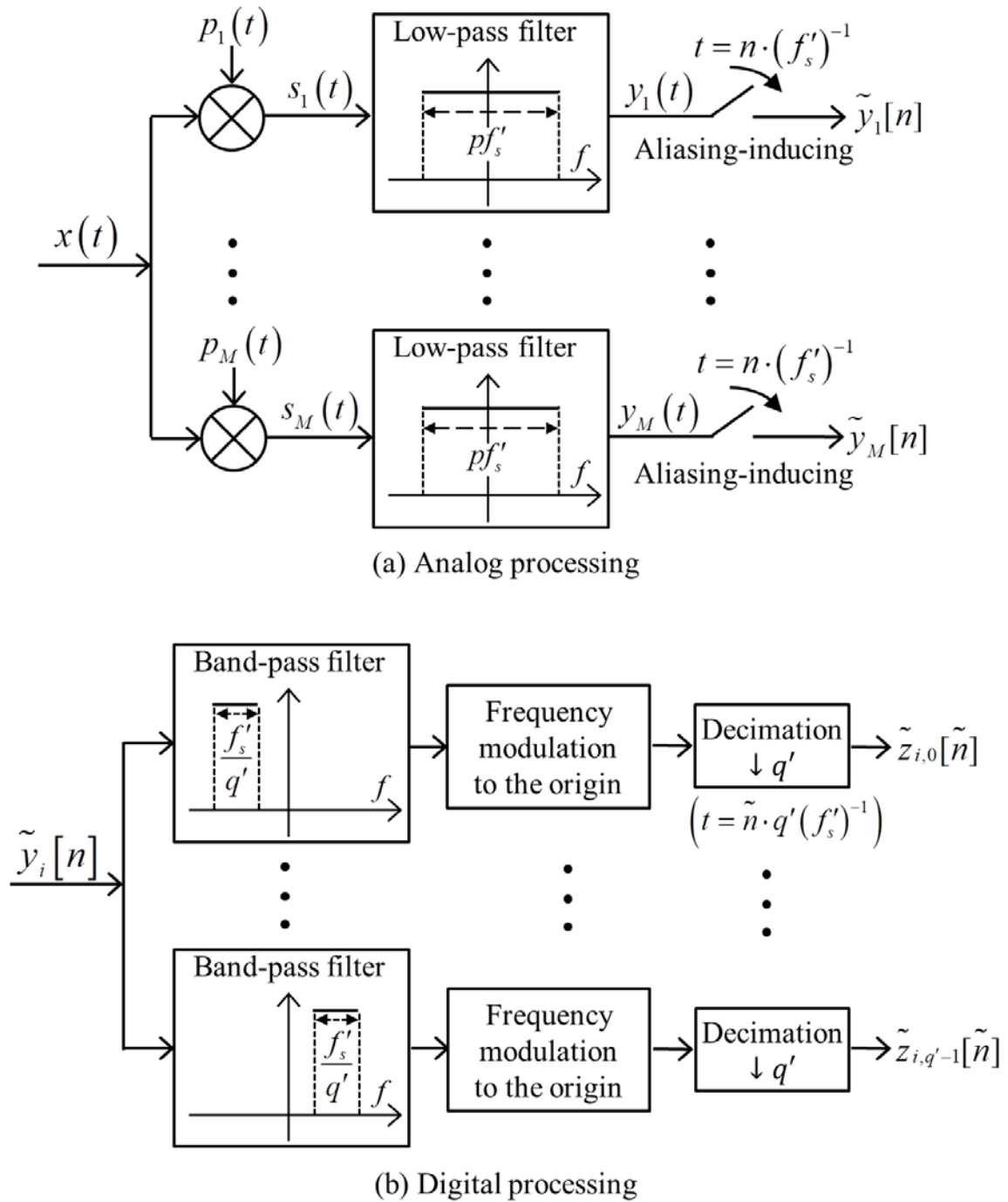


Figure 2.1 Sampling system of AMWC. The system is equivalent to cMWC when $p = 1$ and $q' = q$. In AMWC, the sampling rate is p -times lower than the filter bandwidth with $p > 1$ to intentionally induce aliasing.

2.2.1. Conventional MWC

In the original paper [12] by Mishali et al., for lossless sub-Nyquist sampling, the ADC followed the anti-aliasing rule, i.e., $f_s \geq W_{LPF}$. This conventional rule has sufficed for lossless sub-Nyquist sampling. We refer to MWC that follows the anti-aliasing rule as conventional MWC (cMWC).

The input-output relationship of cMWC is given in [12]. The input $x(t)$ at the i -th channel is first mixed with the T_p -periodic PR signal $p_i(t)$ that periodically outputs a sequence of L mixing chips. By the periodicity, the Fourier transform (FT) of $p_i(t)$ is an impulse train. The FT of the mixed signal $s_i(t) = x(t)p_i(t)$ is the convolution $*$ of the two spectra:

$$\begin{aligned} S_i(f) &\triangleq \int_{-\infty}^{\infty} s(t) e^{-j2\pi ft} dt \\ &= P_i(f) * X(f) \\ &= \sum_{l=-\infty}^{\infty} c_{i,l} X(f - lf_p), \end{aligned} \tag{2.1}$$

where $c_{i,l}$ for $l = -\infty, \dots, \infty$ are the Fourier series coefficients of $p_i(t)$. The mixed signal $s_i(t)$ and $X(f - lf_p)$ in (2.1) are filtered by the LPF $H(f)$. We let $H(f) = 1$ for $f \in \mathcal{F}_{LPF}$, and otherwise, $H(f) = 0$, where $\mathcal{F}_{LPF} \triangleq [-W_{LPF}/2, W_{LPF}/2]$. Since $X(f)$ is band-limited by \mathcal{F}_{NYQ} , the infinite-order summation in (2.1) is reduced to a finite order as follows:

$$\begin{aligned} Y_i(f) &= S_i(f) H(f) \\ &= \sum_{l=-(L_0+q_0)}^{L_0+q_0} c_{i,l} X(f - lf_p), \text{ for } f \in \mathcal{F}_{LPF}, \end{aligned} \tag{2.2}$$

where L_0 is computed by $L_0 = (L-1)/2$ [12], and $q_0 \triangleq (q-1)/2$. Next, the ADC of rate $f_s = T_s^{-1}$ takes samples of $y_i(t)$, i.e., $y_i[n] = y_i(t)|_{t=nT_s}$. By the conventional anti-

aliasing rule, we set $f_s = W_{LPP}$. Then, the discrete-time FT (DTFT) of $y_i[n]$ preserves the spectrum of (2.2).

In (2.2), every subband $X(f - lf_p)$ is spectrally correlated with nearby $q - 1$ subbands, since the bandwidth W_{LPP} is wider than the shifting interval f_p . To make them spectrally orthogonal, the samples $y_i[n]$ are modulated and low-pass filtered in parallel through q digital channels by

$$z_{i,s}[\tilde{n}] = \left[\left(y_i[n] e^{-j2\pi s f_p T_s n} \right) * h_{f_p}[n] \right] \Big|_{n=\tilde{n}q} \quad (2.3)$$

for $s = -q_0, \dots, q_0$, where $h_{f_p}[n]$ is a digital LPF with the cut-off frequency of $f_p/2$ and a flat passband response. The DTFT of (2.3) is

$$Z_{i,s}(e^{j2\pi f q T_s}) = \sum_{l=-L_0}^{L_0} c_{i,l+s} X(f - lf_p) \text{ for } f \in \mathcal{F}_p, \quad (2.4)$$

where $\mathcal{F}_p \triangleq [-f_p/2, f_p/2]$. The subbands $X(f - lf_p)$ in (2.4) are spectrally orthogonal to each other, since the bandwidth equals the shifting interval. As $X(f)$ is a multiband signal, only a few subbands in (2.4) have nonzero values. If $f_p \geq B$, the upper bound on the sparsity K of the subbands is $K \leq 2K_B$, since the uniform grid of interval f_p splits each band into two pieces at most.

Consequently, each analog channel outputs q different sequences, and therefore, cMWC obtains totally Mq equations for input reconstruction. Depending on the number of equations, it was shown in [12] that the input spectrum can be perfectly reconstructed. Previously, to obtain more equations for a fixed number of channels M and for a given specification f_p for PR signal generation, cMWC has to rely on the increased sampling rate $f_s = qf_p$ by controlling the *channel-trading* parameter q . In this chapter, we aim to show there is another way to obtain more equations and improve the input reconstruction

performance, without the cost intensive ways of increasing the total sampling rate $f_{s,total} = Mf_s$ or reducing f_p , or both.

2.2.2. Choosing PR Signals for Conventional MWC

In this subsection, we present a study on the hardware-friendly selection of PR signals, which was published in [30].

Motivation In the MWC, the input signal is mixed with a multiple number of periodic PR signals in parallel. PR signals play a significant role in recovering the input from the sub-Nyquist samples by CS theory. In the original paper [12], instead of pseudo-random signals, signals generated from independently drawn random Bernoulli sequences were used to exploit a theoretical result of CS. However, in the perspective of implementation, such true-random signal generators are inefficient, since it requires memory banks as many as the chips of random sequences. In addition, even if one considers signal generators based on pseudo-random sequences, it is still burdening to implement m independent generators due to synchronization issues among them and large fabrication area.

Related Work For efficient generation of mixing signals, single well-designed base sequence has been employed to generate all m mixing sequences by its random cyclic shifts [44]–[46]. In the literatures, the CS recovery was guaranteed if the discrete Fourier transform (DFT) elements of a base sequence have flat magnitudes. In [45] and [46], real- and complex-valued sequences with flat spectra have been respectively chosen as the base sequence. For enhanced noise robustness and memory efficiency, exclusive-OR operations of the random cyclic shifts were exploited [44]. In the literature, the spectrum of a base sequence was not restricted to be flat with the absence of theoretical performance analysis.

The prior works restricted their focuses on base sequences having flat spectra. Although it is well known to construct non-bipolar sequences with flat spectra (e.g., ternary sequences [47]), using arbitrary-valued sequences requires high complexity in implementation. Meanwhile, it is conjectured that a bipolar sequence with flat spectrum exists only for length 4. Instead, M-sequences and Legendre sequences with the nearly-flat spectra can be considered [44], but their lengths are still inflexible. For example, m -sequences exist in

lengths $M = 2^n - 1$ for a positive integer n , and Legendre sequences exist in prime lengths M such that $M \equiv 3 \pmod{4}$.

Goal We scope the conventional MWC using random cyclic shifts of a base mixing sequence, which is referred to as random partial Fourier structured MWC (RPFMWC). Since the length of mixing sequence is a major parameter in deciding a sampling rate for the lossless sampling, inflexible length of mixing sequences can increase the sampling rate unnecessarily. Therefore, the flexibility in choosing the lengths of mixing sequences is important for performance optimization.

We investigate the use of pseudo-random sequences supporting flexible choice of lengths as the base sequence. In the perspective of flexible sequence length, using a bipolar sequence having non-flat spectrum as the base sequence, e.g., a sequence randomly generated and then fixed, would be a reasonable choice. Therefore, it is needed to investigate the CS recovery performance of the RPFMWC with the bipolar base sequence having non-flat spectrum.

Results We show that the CS recovery of the RPFMWC is guaranteed if and only if all spectral elements of a base sequence are nonzero.

Theorem 2.1 (Theorem 1 in [30]) Consider sensing model (2.4). When $m \geq O(K \ln^4 M)$, where M is the length of base sequence, the reconstruction of at most K nonzero subbands of $X(f)$ by L^1 norm minimization given in (1.5) is successful, if and only if σ has nonzero elements, i.e., Σ is invertible.

Theorem 2.1 is demonstrated by Monte Carlo experiments in Figure 2.2.

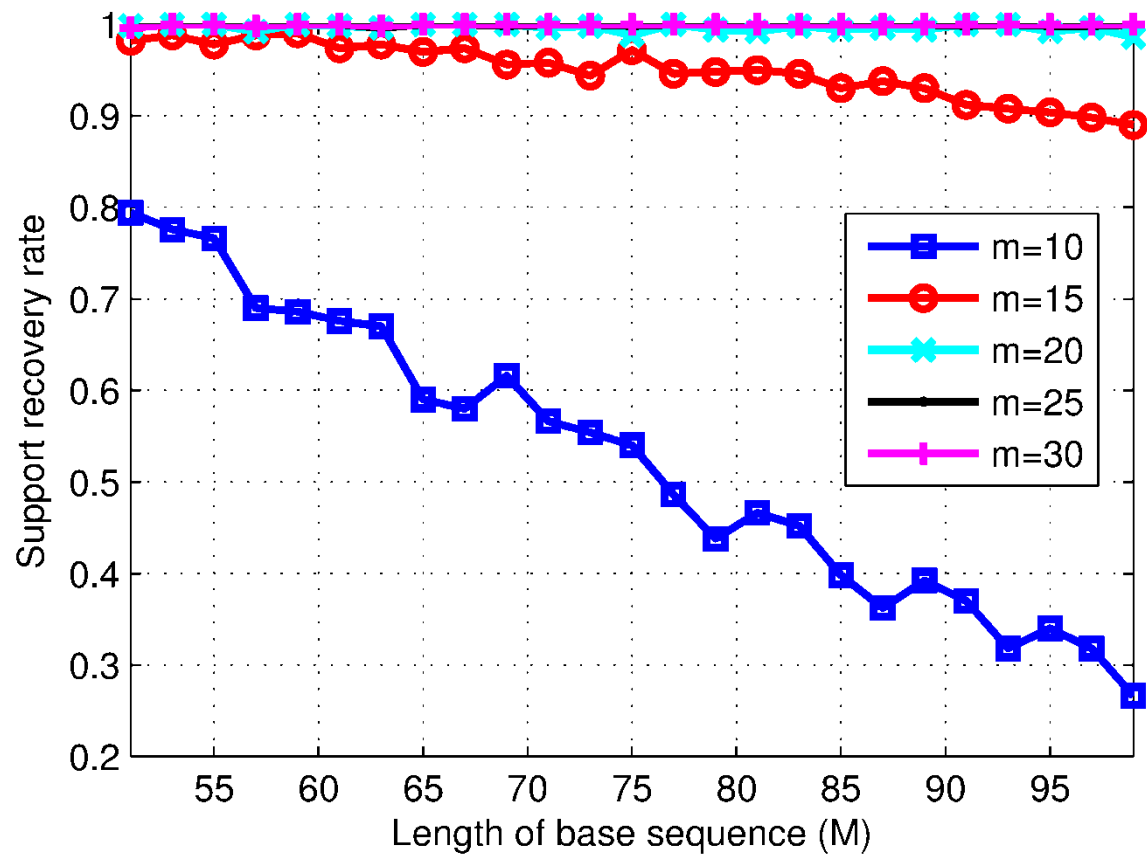


Figure 2.2 Successful recovery rates of all nonzero subbands of $X(f)$ from RPFMWC for various lengths M of the base sequence and numbers m of channels. The number of multibands is $K_B = 4$. The sparsity of sensing model is $K \leq 2K_B$.

2.2.3. Sampling Efficiency

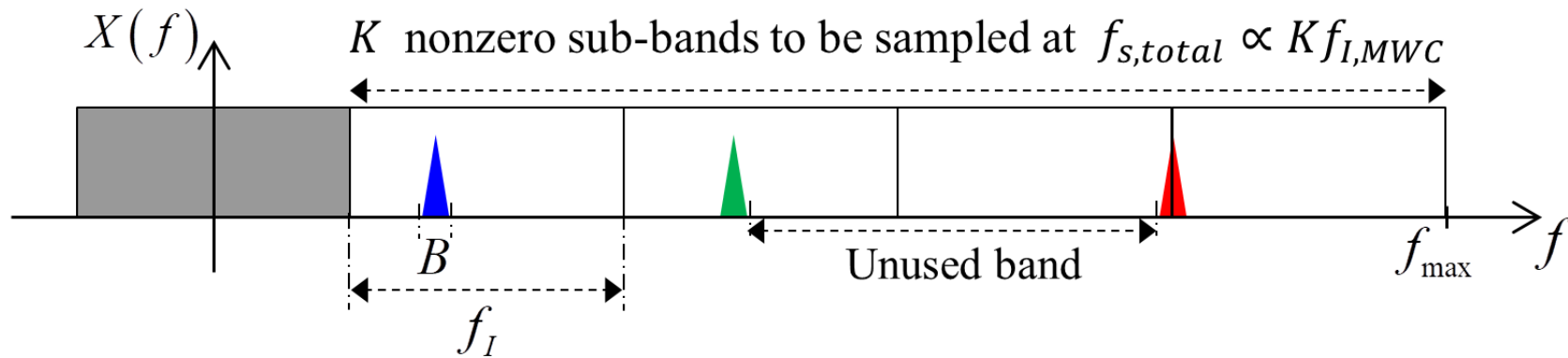
In (2.4), MWC splits the input spectrum into many subbands along a uniform grid of a *splitting interval*, and it then takes samples of the weighted sum of subbands. We denote the splitting interval by f_I . Note that the splitting interval of cMWC $f_{I,cMWC}$ equals f_p . From the samples, a CS recovery algorithm (e.g., [10], [19], [37], [48]) finally recovers the K nonzero subbands containing the split pieces of the K_B multibands. Consequently, the total sampling rate is consumed to take samples of K nonzero subbands of bandwidth f_I . This indicates that the total sampling rate required for lossless sampling by an MWC would be at least $f_{s,total} \geq 2Kf_I$, where the factor of 2 arises from the unknown supports of the nonzero subbands. In contrast, a result in [33] states that, for a general sub-Nyquist sampling system, the minimum requirement for lossless sampling of a multiband signal is $f_{s,total} \geq 2K_B B$, where $K_B B$ is the upper bound of the *actual spectral occupancy* of a multiband signal. That is, when f_I is far greater than B , MWC consumes a portion of the total sampling rate inefficiently. Specifically, f_I greater than B yields a higher probability for the K nonzero subbands to be comprised of unused bands, i.e., zeros. The inefficient use of total sampling rate is illustrated in Figure 2.3.

Ideally, when the splitting interval f_I becomes finer and closer to B while satisfying $f_I \geq B$, the sampling efficiency is improved, as shown in Figure 2.3. The efficiency is maximized when $Kf_I = K_B B$. Based on this observation, we define the *sampling efficiency* α of MWC as the ratio between the actual spectral occupancy of the multiband signal and the total bandwidth of the recovered subbands, i.e.,

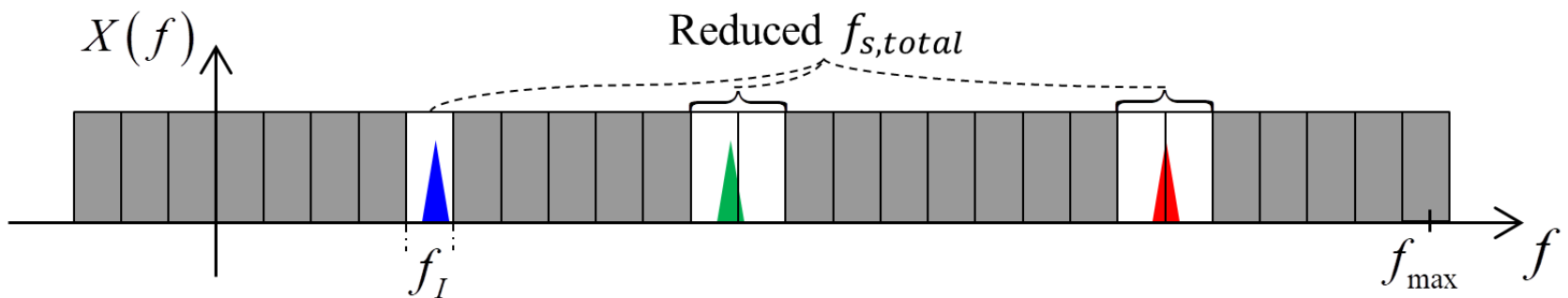
$$\alpha \triangleq \frac{K_B B}{Kf_I}. \quad (2.5)$$

Note that, by the definition of K , $\alpha \leq 1$ always holds.

In summary, improving α has two advantages. First, for the lossless sampling of a given multiband signal, it would reduce the required total sampling rate $f_{s,total}$ closer to the theoretical minimum requirement $f_{s,total} \geq 2K_B B$. By the definition, the higher α closer to 1 indicates that a portion of $f_{s,total}$ inefficiently consumed for taking samples of the unused bands in Figure 2.3 is reduced. By the reduced $f_{s,total}$, the number of channels M or the sampling rate f_s of ADC at each channel is reduced. Secondly, for given and fixed $f_{s,total}$, we will show throughout the rest of chapter that improving α yields more independent equations for signal reconstruction, and thus, more complex multiband signals with higher K_B can be recovered perfectly.



(a) Inefficient sampling



(b) Improved sampling efficiency

Figure 2.3 Sampling system of AMWC. The system is equivalent to cMWC when $p=1$ and $q'=q$. In AMWC, the sampling rate is p -times lower than the filter bandwidth with $p > 1$ to intentionally induce aliasing.

2.2.4. Limitation of Conventional MWC

For cMWC, the sampling efficiency depends entirely on the hardware capabilities of PR signal generators, which may result in severe implementation problems. The sampling efficiency of cMWC depends on the specifications of PR signal generators since $f_{I,cMWC}$ is fixed to f_p . By the definition, the only way to improve the sampling efficiency α_{cMWC} of cMWC has been to make the repetition rate f_p of the PR signals closer to B . As discussed, the chip speed f_c of PR signals should not be less than the Nyquist rate, i.e., $f_c \geq f_{NYQ}$. Thus, from the relation $f_p = f_c L^{-1}$, the chip length L is the only free parameter to control f_p . Since B is usually far smaller than f_{NYQ} , to fit f_p closer to B , a very long L is needed. However, in applications where f_{NYQ} reaches tens of gigahertz, due to the extremely high chip speed f_c , implementing PR signal generators having a high chip length L poses problems in terms of power consumption and fabrication area [38], [39]. Hence, other means to improve α without relying on the chip length L of the PR signals are very important.

For example, suppose one is observing on-air radar signals of bandwidth up to $B = 30$ [MHz] over an extremely wide observation frequency scope $f_{\max} = 40$ [GHz]. This setting is reasonable in radar systems [49], [50]. We discussed that the chip speed should not be less than the Nyquist rate, i.e., $f_c \geq f_{NYQ}$, where $f_{NYQ} = 80$ [GHz]. In this example, to achieve $f_p \approx B$, the chip length needs to be $L = 2^{11} - 1$. Although hardware implementations of such PR signal generators having $f_c = 80$ [GHz] and chip length greater than $L = 2^{11} - 1$ were proposed in the literature [51], [52], they require very large fabrication areas and high power consumption, which has hindered practical uses thus far.

2.3. Aliased Modulated Wideband Converters (AMWC)

2.3.1. Problem Formulation

The goal of this section is to introduce the proposed sampling system which aims to improve the sampling efficiency α with given and fixed specifications f_p , f_c , and L for PR signal generation. Throughout this section, we assume small L and B and a large $f_{NYQ} = f_c$, which implies f_p large enough compared to B and makes room for improving α . That is, $f_p \geq pB$ for a natural number $p > 1$. Then, improving α can be made without upgrading the PR signal generators and causing the said implementation issues such as higher power consumption and larger fabrication area discussed in the previous subsection. Thus, very wideband signals can be losslessly sampled using commercially available PR signal generators and ADCs, while this was not possible in the past with the conventional cMWC system.

Multiband model		
$f_{NYQ} = 18$ [GHz]	$B = 30$ [MHz]	$K_B = 10$
System specification		
$L = 2^7 - 1$	$f_p \approx 142$ [MHz]	$M = 3$
Parameters	cMWC	AMWC (with $p = 4$)
Channel-trading parameter	$q = 5$	$q' = 19$
Sampling rate [MHz]	$f_s = f_p q \approx 710$	$f'_s = f_p q' p^{-1} \approx 674.5$
Splitting interval [MHz]	$f_l = f_p = 142$	$f_l = f_p p^{-1} = 35.5$
Sparsity	$K \leq 2K_B = 20$	$K \leq 2K_B = 20$
Number of rows of \mathbf{X}	$N = L = 127$	$N = Lp = 508$
Total number of equations	$Mq = 15$	$Mq' = 57$

Table 2.1 Sampling system of AMWC. The system is equivalent to cMWC when $p = 1$ and $q' = q$. In AMWC, the sampling rate is p -times lower than the filter bandwidth with $p > 1$ to intentionally induce aliasing.

2.3.2. Intentional Aliasing Method

The AMWC system is depicted in Figure 2.1. As mentioned already, compared to cMWC, AMWC is designed to not satisfy the anti-aliasing rule at the ADC; rather, it is designed to induce *intentional* aliasing by setting the bandwidth of LPF greater than the sampling rate. In fact, in both cMWC and AMWC, an aliasing is introduced first by the mixer. The effect of this first aliasing is shown in (2.2), where the mixer shifts, gives weights, and has the signal spectrum $X(f)$ overlapped with shifted versions of itself at intervals of f_p . By the second aliasing at the ADC, the overlapped spectrum is aliased again at intervals of new sampling rate of AMWC f'_s , which is smaller than the filter bandwidth. By adjusting the relationship between f_p and f'_s , the splitting interval f_l , which is the interval at which $X(f)$ is split in the outputs of AMWC, is regulated.

Specifically, we set the new sampling rate f'_s of AMWC:

$$f'_s = \frac{q'}{p} f_p, \quad (2.6)$$

where q' is the new channel trading parameter for AMWC and an odd number. The bandwidth of LPF is $W_{LPF} = q'f_p$, and therefore, $W_{LPF} = pf'_s$ for the integer *aliasing parameter* $p > 1$. We will show that coprime p and q' with $q' > p$ is necessary for no information loss of $X(f)$. The new sampling rate induces additional aliasing and regulates the splitting interval f_l to improve the sampling efficiency. We let

$$f'_p \triangleq \frac{f_p}{p} \quad (2.7)$$

denote *the least common shifting interval* (LCS), which will become the splitting interval of AMWC, i.e., $f_{l,AMWC} = f'_p$.

With the introduction of new sampling rate f'_s in (2.6), it becomes easier to compare AMWC with cMWC. Specifically, with the sampling rate fixed, the number of equations for the input reconstruction obtained by cMWC and that by AMWC can be compared; with the number of equations fixed, the sampling rates for the two can be compared. For a given sampling rate $f'_s = q' f_p / p$, we will show in this section, the number of equations obtained by AMWC is Mq' . For a given sampling rate $f_s = qf_p$, from Section 2.2.1, the number of equations obtained by cMWC is Mq . With the sampling rate fixed the same, i.e., $f_s = f'_s$, we note that $q' = qp$. This implies that AMWC has p -times more equations than that of cMWC. Table 2.1 presents an example of the increase in the number of equations of AMWC. With the number of equations fixed, i.e., $Mq = Mq'$, on the other hand, AMWC requires p -times smaller sampling rate than cMWC does.

In [43], a variation of MWC using a sampling rate similar to (2.6) was considered, to analyze the noise factor incurred by the aliasing of subbands. There appear coprime relations between p and q' similar to that in this chapter. However, the purpose of using coprime p and q' in [18] was completely different from that of this chapter, i.e., they regulated the splitting interval of the subbands to make a fair comparison with other filterbank-based sampling systems with regard to the effect of noise. No relation between p and q' for lossless sampling and improving sampling efficiency was studied in [18].

To support intentional aliasing, AMWC requires an ADC with an operating bandwidth wider than its sampling rate. Such an ADC can be implemented by using a wideband track-and-hold amplifier (THA) developed by Hittite Corp. for the applications of EW and ELLINT in [53]. This THA has an 18 GHz bandwidth and can be integrated at the front end of commercially available ADCs of sampling rate up to 4 giga-samples per second.

To show that the AMWC obtains Mq' equations, we observe the input-output relationships of the aliased samples $\tilde{y}_i[n]$ in Figure 2.1. Without loss of generality, we assume $q' = q$ and $f_s = pf'_s$. By the sampling theorem, the DTFT of $\tilde{y}_i[n]$ is the sum of shifts of $Y_i(f)$:

$$\begin{aligned}
\tilde{Y}_i(e^{j2\pi f T'_s}) &= \sum_{r=-\infty}^{\infty} Y_i(f - rf'_s) \\
&= \sum_{r=-\infty}^{\infty} \sum_{l=-\infty}^{\infty} c_{i,l} X(f - rf'_s - lf_p) H(f - rf'_s),
\end{aligned} \tag{2.8}$$

where $T'_s \triangleq (f'_s)^{-1}$ and $Y_i(f)$ given in (2.2) is the spectrum of the output of the LPF $H(f)$. Within only a single period of $\tilde{Y}_i(e^{j2\pi f T'_s})$ in (2.8), i.e., $\mathcal{F}'_s(f_0) \triangleq [f_0, f_0 + f'_s)$ for any $f_0 \in \mathbb{R}$, because the bandwidth of $Y_i(f)$ is limited by the LPF $H(f)$, most of the shifts $Y_i(f - rf'_s)$ for sufficiently large $|r|$ are zeros. In other words, there exist (f_0, R_1, R_2) such that the infinite order of the outer summation in (2.8) is reduced to a finite order, i.e.,

$$\tilde{Y}_i(e^{j2\pi f T'_s}) = \sum_{r=R_1}^{R_2} \sum_{l=-\infty}^{\infty} c_{i,l} X(f - rf'_s - lf_p) H(f - rf'_s) \tag{2.9}$$

for $f \in \mathcal{F}'_s(f_0)$. Assuming $H(f) = 1$ for $f \in \mathcal{F}_{LPF}$, if f_0 , R_1 , and R_2 satisfy the conditions of Lemma 2.2, the LPF responses in (2.9) are replaced with $H(f - rf'_s) = 1$ for $f \in \mathcal{F}'_s(f_0)$. Note that, when $p = 1$, i.e., no aliasing exists at the ADC, $R_1 = R_2$, which is equivalent to cMWC.

Lemma 2.2. Equation (2.9) is equivalent to (2.8) if f_0 , R_1 , and R_2 with $R_1 < R_2 \in \mathbb{Z}$ satisfy

$$R_2 - R_1 = p - 1, \tag{2.10}$$

and

$$f_0 = \left(R_2 - \frac{p}{2} \right) f'_s. \tag{2.11}$$

Proof: See Appendix 2.A.

We represent the shifting indices $rf'_s + lf'_p$ in (2.9) in terms of the LCS f'_p . Then,

$$\tilde{Y}_i(e^{j2\pi fT'_s}) = \sum_{r=R_1}^{R_1+p-1} \sum_{l=-\infty}^{\infty} c_{i,l} X(f - (rq' + lp) f'_p) \quad (2.12)$$

for $f \in \mathcal{F}'_s(f_0)$. To merge the inner and outer summations in (2.12), we use Lemma 2.3.

Lemma 2.3. If p and q' are coprime, the linear combination $rq' + lp$ for $r \in \mathcal{P} \triangleq \{R_1, \dots, R_1 + p - 1\}$ and $l \in \mathbb{Z}$ spans every integer.

Proof: We consider the following congruent relationship

$$k \equiv rq' \pmod{p}. \quad (2.13)$$

By modular arithmetic, if p and q' are coprime, there always exists one-to-one correspondence between r and k in the least residue system modulo p . Since $|\mathcal{P}| = p$, $rq' \pmod{p}$ for $r \in \mathcal{P}$ in (2.13) spans every number in the least residue system of modulo p . Hence, for $r \in \mathcal{P}$ and $l \in \mathbb{Z}$, $rq' + lp = k \pmod{p} + lp$ spans every integer. ■

By denoting $k = rq' + lp$ in (2.12), we have the equivalent relationship

$$\tilde{Y}_i(e^{j2\pi fT'_s}) = \sum_{k=-\infty}^{\infty} d_{i,k}(R_1, p, q') X(f - kf'_p) \quad (2.14)$$

for $f \in \mathcal{F}'_s(f_0)$, where $d_{i,k}(R_1, p, q')$ are the new sensing coefficients of AMWC. Proposition 2.4 provides the rule to obtain the coefficients $d_{i,k}$ from the Fourier coefficients $c_{i,l}$ of PR signals.

Proposition 2.4. For coprime p and q' , let us define

$$I(k; R_1, p, q') \triangleq \frac{1}{p} \left\{ k - q' \left[\left((q')^{-1} k - R_1 \right) \pmod{p} + R_1 \right] \right\}, \quad (2.15)$$

where $(q')^{-1} \pmod{p}$ is the multiplicative inverse of q' modulo p . Equation (2.14) is equivalent to (2.12) if

$$d_{i,k}(R_1, p, q') = c_{i, I(k; R_1, p, q')}. \quad (2.16)$$

Proof: See Appendix 2.B.

In (2.14), the bandwidth of the subbands $X(f - kf'_p)$ for $f \in \mathcal{F}'_s(f_0)$ equals f'_p and is q' times wider than their shifting interval f'_p . Therefore, every subband is correlated with the closest $q'-1$ subbands. By making these subbands spectrally orthogonal, the M relationships for $i=1, \dots, M$ are expanded to Mq' equations to enhance the input reconstruction performance. A similar work was done for cMWC through (2.3) to (2.4), which further divides the observing frequency domain $\mathcal{F}'_s(f_0)$ (2.14) into q' tiny domains. Specifically, for $u=0, \dots, q'-1$, the u -th tiny frequency domain is defined by $\mathcal{F}'_p(f_0 + uf'_p)$, where

$$\mathcal{F}'_p(f_0) \triangleq [f_0, f_0 + f'_p). \quad (2.17)$$

Then, the corresponding divided outputs have relationships

$$\begin{aligned} & \tilde{Y}_i^{(u)}(e^{j2\pi f T'_p}) \\ &= \sum_{k=-\infty}^{\infty} d_{i,k}(R_1, p, q') X(f - kf'_p) \text{ for } f \in \mathcal{F}'_p(f_0 + uf'_p), \end{aligned} \quad (2.18)$$

for $u=0, \dots, q'-1$. Finally, we define the output $\tilde{Z}_{i,u}(e^{j2\pi f T'_p})$ of AMWC as follows:

$$\begin{aligned} \tilde{Z}_{i,u}(e^{j2\pi f T'_p}) &\triangleq \tilde{Y}_i^{(u)}(e^{j2\pi f T'_p}) \Big|_{f=f+uf'_p} \\ &= \sum_{k=-\infty}^{\infty} d_{i,k+u}(R_1, p, q') X(f - kf'_p) \end{aligned} \quad (2.19)$$

for $f \in \mathcal{F}'_p(f_0)$. The final output $\tilde{z}_{i,u}[\tilde{n}]$ in the discrete-time domain can be obtained by performing digital frequency modulation and low-pass filtering on $\tilde{y}_i[n]$, as similarly done for cMWC in (2.3). The specific design of the digital processing system is shown in Figure 2.1-(b).

Consequently, in (2.19), the input $X(f)$ is split into spectrally orthogonal subbands at intervals of f'_p . Therefore, the splitting interval of AMWC equals the LCS f'_p :

$$f_{L,AMWC} = f'_p \triangleq \frac{f_p}{p}, \quad (2.20)$$

which is p times lower than $f_{L,cMWC}$. By reducing the splitting interval by controlling the aliasing parameter p , the sampling efficiency of AMWC in (2.5) is improved. Figure 2.4 illustrates how AMWC regulates the splitting interval and improves the sampling efficiency. In contrast, as discussed in Section 2.2.4, regulating the splitting interval of cMWC requires a very costly solution of advanced PR signal generators with a larger chip length. Consequently, both cMWC and AMWC obtain $Mq = Mq'$ equations for input reconstruction, although AMWC consumes a p -times lower total sampling rate (2.6). In Section 2.3.4, we will show that the Mq' equations of AMWC are independent.

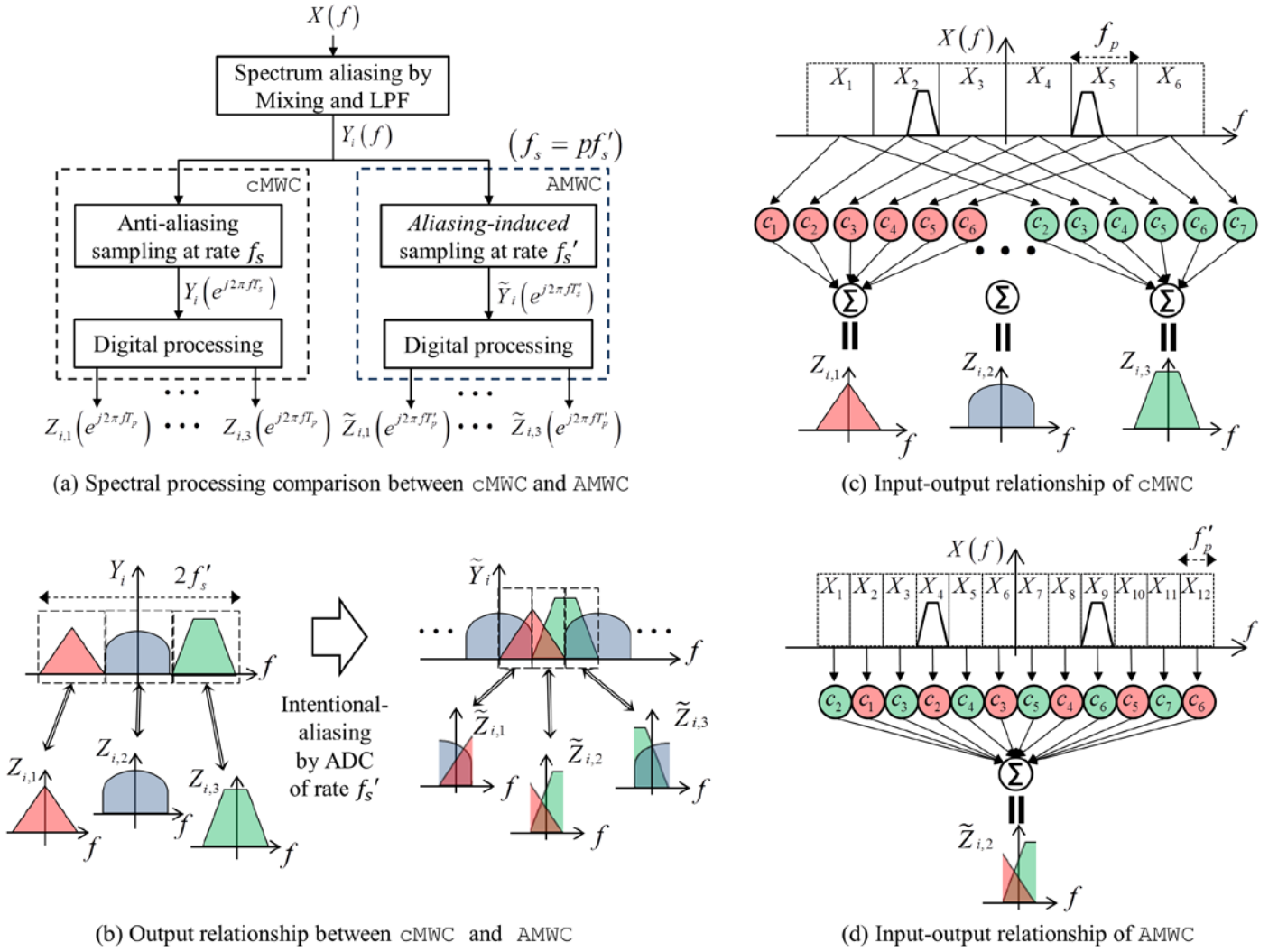


Figure 2.4 Principle of improving the sampling efficiency by AMWC at a single analog channel is illustrated, with setting $q = 3$, $q' = q$, $p = 2$, and $m = 3$. At the first stage, the input spectrum $X(f)$ is aliased by mixing it with the PR signal and low-pass filtering it. This aliased-version of $X(f)$ is depicted as $Y_i(f)$. In (a), the main difference between cMWC and AMWC is how to take time-samples of $Y_i(f)$. cMWC prevents the spectrum from being aliased in taking time-samples. AMWC, on the contrary, aims to make the spectrum $Y_i(f)$ intentionally aliased once again, as depicted as $\tilde{Y}_i(f)$ in (b). In (c), as a result, the splitting-interval of cMWC is f_p , whereas in (d), that of AMWC is halved to f'_p . Thus, the sampling efficiency of AMWC becomes doubled (as $p = 2$).

2.3.3. Input-Output Relationship of AMWC

For convenience of analyzing and solving linear simultaneous Mq' equations (2.19), we cast them as a matrix equation. To this end, we first reduce the infinite summation in (2.19) to be finite. We then discretize the continuous spectra to form a matrix with a finite number of columns.

Since $X(f)$ is band-limited to $f \in \mathcal{F}_{NYQ}$, within the limited frequency range $f \in \mathcal{F}'_p(f_0)$, the infinite summation order in (2.19) is reduced to a finite order as follow:

$$\begin{aligned} & \tilde{Z}_{i,u} \left(e^{j2\pi f T'_p} \right) \\ &= \sum_{k=N_1}^{N_2} d_{i,k+u} (R_1, p, q') X(f - kf_{I,AMWC}) \text{ for } f \in \mathcal{F}'_p(f_0), \end{aligned} \quad (2.21)$$

where N_1 and N_2 are, respectively, the smallest and largest index k of the subbands $X(f - kf_{I,AMWC})$ that contain some active value of $X(f)$ within $f \in \mathcal{F}_{NYQ}$. Namely, these indices N_1 and N_2 indicate $X(f - kf_{I,AMWC}) = 0$ for $k < N_1$ and $k > N_2$, and thus help us obtain a matrix equation of (2.21) with finite dimensions. To mathematically define N_1 and N_2 , note that the k -th subband $X(f - kf_{I,AMWC})$ in (2.21) observes the frequency range

$$\mathcal{F}_k \triangleq [f_0 - kf_{I,AMWC}, f_0 - kf_{I,AMWC} + f'_p] \quad (2.22)$$

of $X(f)$. Then, the indices N_1 and N_2 are defined by

$$\begin{aligned} N_1 &\triangleq \min \{k \in \mathbb{Z} : \mathcal{F}_k \cap \mathcal{F}_{NYQ} \neq \emptyset\} \\ &= \min \{k \in \mathbb{Z} : f_0 - kf_{I,AMWC} < f_{\max}\} \end{aligned} \quad (2.23)$$

and

$$\begin{aligned}
N_2 &\triangleq \max \left\{ k \in \mathbb{Z} : \mathcal{F}_k \cap \mathcal{F}_{\text{NYQ}} \neq \emptyset \right\} \\
&= \max \left\{ k \in \mathbb{Z} : f_0 - kf_{I,AMWC} + f'_p > -f_{\max} \right\},
\end{aligned} \tag{2.24}$$

respectively. Using the parameters and relations given in Table 2.2 and Lemma 2.2, the two problems (2.23) and (2.24) turn into

$$N_1 = \min \left\{ k \in \mathbb{Z} : R_2 q' - \frac{(q'+L)p}{2} < k \right\} \tag{2.25}$$

and

$$N_2 = \max \left\{ k \in \mathbb{Z} : R_2 q' - \frac{(q'-L)p}{2} + 1 > k \right\} \tag{2.26}$$

respectively. As both q' and L are odd positive integers, the solutions of two problems (2.25) and (2.26) are determined as follow:

$$N_1 = R_2 q' - \frac{(q'+L)p}{2} + 1, \tag{2.27}$$

and

$$N_2 = R_2 q' - \frac{(q'-L)p}{2}. \tag{2.28}$$

Finally, the output spectrum $\tilde{Z}_{i,u} \left(e^{j2\pi f T'_p} \right)$ in (2.21) turns into a linear combination of unknown subbands $X(f - kf_{I,AMWC})$ for $f \in \mathcal{F}'_p(f_0)$. The matrix-multiplication form $\mathbf{Z} = \mathbf{D}\mathbf{X}$ of (2.21) is provided by

$$\begin{aligned}
& \underbrace{\begin{pmatrix} \tilde{\mathbf{Z}}_{1,0} \left(e^{j2\pi f T'_p} \right) \\ \vdots \\ \tilde{\mathbf{Z}}_{1,q'-1} \left(e^{j2\pi f T'_p} \right) \\ \tilde{\mathbf{Z}}_{2,0} \left(e^{j2\pi f T'_p} \right) \\ \vdots \\ \tilde{\mathbf{Z}}_{M,q'-1} \left(e^{j2\pi f T'_p} \right) \end{pmatrix}}_{\triangleq \mathbf{Z} \in \mathbb{C}^{Mq' \times \infty}} = \underbrace{\begin{pmatrix} d_{1,N_1} & d_{1,N_1+1} & \cdots & d_{1,N_2} \\ \vdots & \vdots & & \vdots \\ d_{1,N_1+(q'-1)} & d_{1,N_1+(q'-1)+1} & \cdots & d_{1,N_2+(q'-1)} \\ d_{2,N_1} & d_{2,N_1+1} & \cdots & d_{2,N_2} \\ \vdots & \vdots & & \vdots \\ d_{M,N_1+(q'-1)} & d_{M,N_1+(q'-1)+1} & \cdots & d_{M,N_2+(q'-1)} \end{pmatrix}}_{\triangleq \mathbf{D} \in \mathbb{C}^{Mq' \times N}} \underbrace{\begin{pmatrix} X(f - N_1 f'_p) \\ X(f - (N_1 + 1) f'_p) \\ \vdots \\ X(f - N_2 f'_p) \end{pmatrix}}_{\triangleq \mathbf{X} \in \mathbb{C}^{N \times \infty}}. \\
& \tag{2.29}
\end{aligned}$$

We denote the number of subbands, i.e., the dimension of matrix \mathbf{X} , by N , which equals

$$\begin{aligned}
N &= N_2 - N_1 + 1 \\
&= Lp.
\end{aligned} \tag{2.30}$$

Since $X(f)$ consists of K_B narrow bands over the wide Nyquist range, only a few of its subbands $X(f - kf_{I,AMWC})$ for $f \in \mathcal{F}'_p(f_0)$ have nonzero values. Therefore, the matrix \mathbf{X} in (2.29) is row-wise sparse with a sparsity K related to K_B .

To draw a relationship between the analytic result (2.29) and actually acquired samples $\tilde{z}_{i,u}[\tilde{n}]$, we convert the DTFT (2.29) to the DFT of $\tilde{z}_{i,u}[\tilde{n}]$ by taking the frequency samples of the infinite columns of \mathbf{Z} and \mathbf{X} . When the input is observed for a finite duration T_o , taking samples of the spectrum (2.21) at frequency intervals of $\Delta f = T_o^{-1}$ does not cause any information loss. The samples of spectrum $\tilde{\mathbf{Z}}_{i,u}(e^{j2\pi f T'_p})$ is obtained by taking the DFT of the actually acquired time-samples $z_{i,u}[\tilde{n}]$. Consequently, for a finite observation time $T_o = 2WT'_p$ for a sample length $2W$, we rewrite the matrix-multiplication form (2.29) as

$$\mathbf{Z}_{2W} = \mathbf{D}\mathbf{X}_{2W}, \tag{2.31}$$

where columns of $\mathbf{Z}_{2W} \in \mathbb{C}^{Mq' \times 2W}$ and $\mathbf{X}_{2W} \in \mathbb{C}^{N \times 2W}$ are sub-columns of \mathbf{Z} and \mathbf{X} , respectively, at frequency intervals of Δf . This concept will be exploited in Section 2.4 to derive a revised input-output relationship of AMWC for using LPF with a non-flat frequency response.

Symbol	Description and Relationship
f_{\max}	maximum frequency of multiband signal
f_{NYQ}	Nyquist rate of multiband signal, $f_{NYQ} \triangleq 2f_{\max}$
B, K_B	maximum bandwidth and number of the narrow bands in a multi-band signal
K	number of nonzero subbands (sparsity), $K \leq 2K_B$ if $f'_p \geq B$.
M	number of analog channels
L	length of PR chips within a single period
f_c	chip speed of PR signals, $f_c = f_{NYQ}$
f_p	repetition rate of PR signals, $f_p = f_c L^{-1}$
q', p	channel-trading parameter, aliasing parameter
W_{LPF}	bandwidth of LPF, $W_{LPF} = q'f_p$
f'_p	least common shifting interval, $f'_p \triangleq f_p p^{-1} \geq B$
f'_s	sampling rate of an ADC, $f'_s = W_{LPF} p^{-1}$
$f_{s,total}$	total sampling rate, $f_{s,total} \triangleq Mf'_s$
$f_{I,AMWC}$	splitting interval, $f_{I,AMWC} = f'_p$
α_{AMWC}	sampling efficiency, $\alpha_{AMWC} \triangleq \frac{K_B B}{K f_{I,AMWC}}$

Table 2.2 Summary of AMWC Parameters (CMWC when $p=1$ and $q'=q$)

2.3.4. Choosing the Aliasing Parameter

For a given total sampling rate, AMWC obtains more equations used for input reconstruction than cMWC does. What remains is to check if the extended equations provide independent information. We reveal a condition on the aliasing parameter p that necessitates the linear system (2.29) to be well-posed for every K -sparse signal matrix \mathbf{X} .

Proposition 2.5. There exists the unique solution of (2.29) for every K -sparse signal \mathbf{X} only if p and q' are coprime and $q' > p$.

Proof. See Appendix 2.C.

Proposition 2.5 gives a condition $q' < p$ for coprime p and q' that makes AMWC an ill-posed system. This indicates that, within the set of coprime $q' > p$, there may be a subset that makes AMWC guarantees the existence of unique solution of (2.29) for every K -sparse signal matrix \mathbf{X} .

In [10], a CS result states there exist the unique solution of a multiple measurement vector (MMV) CS equation $\mathbf{Z} = \mathbf{D}\mathbf{X}$ for every K -sparse signal \mathbf{X} if

$$2K < \text{spark}(\mathbf{D}) - 1 + \text{rank}(\mathbf{X}), \quad (2.32)$$

where *spark* is the minimum number of linearly dependent columns in \mathbf{D} . Meanwhile, the spark of an Mq' -by- N matrix is upper bounded to $Mq' + 1$ by the Singleton bound [54]. Based on these results, we find a sufficient condition on p and q' from Monte Carlo experiments in Section 2.5.1 (Figure 2.5) that maximizes the spark of \mathbf{D} .

Main Result 2.6. Let $Mq' \geq 2K$. For every K -sparse signal \mathbf{X} , there exists the unique solution of (2.29), and therefore, AMWC does not lose any information of K -sparse signal \mathbf{X} , if p and q' are coprime and $q' > p$.

Meanwhile, we choose p to minimize the maximum of the sparsity K , which is the number of nonzero subbands of $X(f)$ at splitting intervals $f_{I,AMWC} = f'_p$. The sparsity

K is dependent on the center frequencies of K_B multibands and their maximum bandwidth B . When $f_{I,AMWC} \geq B$, every multiband occupies at most two subbands, which implies $K \leq 2K_B$. On the other hand, when $f_{I,AMWC} < B$, some multibands may occupy more than two subbands, which provides an opportunity to increase K beyond $2K_B$. Hence, we recommend choosing the aliasing parameter p as

$$p \leq \left\lfloor \frac{f_p}{B} \right\rfloor. \quad (2.33)$$

2.3.5. Improvement of Sampling Efficiency

We compare the sampling efficiencies of AMWC, α_{AMWC} , and cMWC, α_{cMWC} , defined in (2.5). The sampling efficiencies are functions of the sparsity K , which is a random variable in general. We denote the sparsity of cMWC and AMWC by K_{cMWC} and K_{AMWC} , respectively. To make them deterministic, we put assumptions on K_{cMWC} and K_{AMWC} that in both cMWC and AMWC, the K_B bands in $X(f)$ respectively occupies exactly one subband, i.e., $K_{cMWC} = K_{AMWC} = K_B$. This occurs with high probability when $f_p p^{-1} \gg B$ and the center frequencies of multibands are far enough apart from each other with a small K_B .

Under the assumption above, the sampling efficiencies of cMWC and AMWC are obtained by

$$\alpha_{cMWC} = \frac{K_B B}{K_{cMWC} f_{I,cMWC}} = \frac{B}{f_p}, \quad (2.34)$$

and

$$\alpha_{AMWC} = \frac{K_B B}{K_{AMWC} f_{I,AMWC}} = \frac{pB}{f_p}, \quad (2.35)$$

respectively. Note that if $p=1$, AMWC and cMWC are completely identical, and therefore $\alpha_{AMWC} = \alpha_{cMWC}$. When $p > 1$, the intentional aliasing of AMWC takes effect and improves the sampling efficiency proportionally to p .

2.4. Non-Ideal Low-Pass Filters

The input-output relationship in the previous section is based on the ideal LPF $H(f)$ having a flat pass-band response. However, in real applications, the pass-band response of an LPF significantly fluctuates. In the case of cMWC, a post digital-processing technique to equalize the effects of non-flat filter responses was proposed in [55]. Unfortunately, owing to the aliasing at ADC, the equalizations cannot be applied to AMWC. In this section, we instead provide a revised input-output relationship of AMWC based on the fluctuated LPF $G(f)$. Without loss of generality, we assume all analog channels use the same LPF. We assume that the response $G(f)$ is nonzero and known within the pass-band $f \in \mathcal{F}_{LPF}$ and is zero for $f \in \mathcal{F}_{LPF}^c$. We derive a revised input-output relationship reflecting the effect of $G(f)$. Paradoxically, our empirical results in Section 2.5 conclude that, for a given sampling efficiency, an irregularly fluctuated filter response is helpful to further decrease the total sampling rate required for lossless sub-Nyquist sampling.

The derivation starts from substituting $H(f)$ in the input-output relations of (2.8)-(2.12) with $G(f)$. Without loss of generality, we assume $q' = q$ and $f_s = pf'_s$. Equation (2.9) then turns into

$$\tilde{Y}_i \left(e^{j2\pi f'_s T'_s} \right) = \sum_{r=R_1}^{R_2} \sum_{l=-\infty}^{\infty} c_{i,l} X \left(f - (rq' + lp) f'_p \right) G \left(f - rq' f'_p \right) \quad (2.36)$$

for $f \in \mathcal{F}'_s(f_0)$, where R_1 and R_2 are chosen from Lemma 2.2. By Lemma 2.3, we substitute $rq' + lp = k$ and merge the outer and inner summations:

$$\tilde{Y}_i(e^{j2\pi f T_s'}) = \sum_{k=N_1}^{N_2} d_{i,k}(R_1, p, q') X(f - kf'_p) G(f - \gamma_p(k) f'_p) \quad (2.37)$$

for $f \in \mathcal{F}'_s(f_0)$, where the sensing coefficients $d_{i,k}(R_1, p, q')$, N_1 , and N_2 are, respectively, computed from Proposition 2.4, (2.27), and (2.28). We define the function γ_p of k that maps k in (2.37) to the corresponding rq' in (2.36) so that the two equations are equivalent. Lemma 2.7 reveals the mapping rule for $\gamma_p(k)$.

Lemma 2.7. Under the conditions of Lemma 2.2 and Lemma 2.3, (2.36) and (2.37) are equivalent if the mapping rule of γ_p is assigned by

$$\gamma_p(k) = k - pI(k; R_1, p, q'), \quad (2.38)$$

where the picking regularity $I(k; R_1, p, q')$ is defined in (2.15).

Proof: See Appendix 2.B.

As done in (2.14) to (2.19), the final outputs $\tilde{z}_{i,u}[\tilde{n}]$ for $u=0, \dots, q'-1$ are obtained by processing the time-samples $\tilde{y}_i[n]$ of the spectrum (2.37) using the digital system given in Figure 2.1-(b). Then, those spectra $\tilde{Z}_{i,u}(e^{j2\pi f T_p'})$ have the following input-output relationships:

$$\begin{aligned} & \tilde{Z}_{i,u}(e^{j2\pi f T_p'}) \\ &= \sum_{k=N_1}^{N_2} d_{i,k+u}(R_1, p, q') X(f - kf'_p) G(f + uf'_p - \gamma_p(k+u) f'_p) \\ &= \sum_{k=N_1}^{N_2} d_{i,k+u}(R_1, p, q') G(f - \gamma'_p(k, u) f'_p) X(f - kf'_p) \end{aligned} \quad (2.39)$$

for $f \in \mathcal{F}'_p(f_0)$, where $\gamma'_p(k, u) \triangleq \gamma_p(k+u) - u$.

Consequently, the linear coefficients on the subbands $X(f - kf'_p)$ in (2.39) become frequency-selective. To numerically solve (2.39), we discretize the continuous frequency, as discussed in Section 2.3.3. We assume that the signal is observed for the finite duration $T_o = 2WT'_p$, where $2W$ is the length of the discretized signal. Then, the samples of spectrum are defined by

$$\begin{aligned}\tilde{\mathbf{Z}}_{i,u}[w] &\triangleq \tilde{\mathbf{Z}}_{i,u}\left(e^{j2\pi f T'_p}\right)\Big|_{f=wT_o^{-1}} \\ &= \sum_{k=N_1}^{N_2} d_{i,k+u} \left[G\left(f - \gamma'(k,u) f'_p\right) X\left(f - kf'_p\right) \right]_{f=wT_o^{-1}} \\ &= \sum_{k=N_1}^{N_2} b_{(i,u),k}[w] X\left(f - kf'_p\right)\Big|_{f=wT_o^{-1}}\end{aligned}\quad (2.40)$$

for $w \in \mathcal{W} \triangleq \{f_0 T_o, \dots, (f_0 + f'_p) T_o - 1\}$, where the frequency-selective sensing coefficients $b_{(i,u),k}[w]$ are defined as

$$b_{(i,u),k}[w] \triangleq d_{i,k+u} G\left(f - \gamma'(k,u) f'_p\right)\Big|_{f=wT_o^{-1}} \quad (2.41)$$

for $w \in \mathcal{W}$. Note that, by the relation between DFT and DTFT, the spectrum samples (2.40) are obtained by taking the DFT as follows:

$$\tilde{\mathbf{Z}}_{i,u}[w] = \sum_{n=0}^{2W-1} \tilde{z}_{i,u}[\tilde{n}] e^{j2\pi \frac{\tilde{n}}{2W} (w \bmod 2W)} \quad \text{for } w \in \mathcal{W}, \quad (2.42)$$

where $\tilde{z}_{i,u}[\tilde{n}]$ are the output sequences of AMWC.

For convenience, we represent the input-output relation of (2.40) for $w \in \mathcal{W}$ in a vector form as

$$\tilde{\mathbf{Z}}[w] = \mathbf{B}[w] \mathbf{X}[w], \quad (2.43)$$

where the elements of the output column vector $\tilde{\mathbf{Z}}[w] \in \mathbb{C}^{Mq'}$ are $\tilde{Z}_{i,u}[w]$ for row indices $i = 1, \dots, M$ and $u = 0, \dots, q' - 1$. The unknown column vector $\mathbf{X}[w] \in \mathbb{C}^N$ consists of $X(f - kf'_p) \Big|_{f=WT_o^{-1}}$ for row indices $k = N_1, \dots, N_2$. The frequency-selective sensing matrix $\mathbf{B}[w] \in \mathbb{C}^{Mq' \times N}$ consists of $b_{(i,u),k}[w]$ with row indices i and u and column index k . The CS model (2.43) is called MMV with different sensing matrices, for which many numerical solvers have been developed [8], [56].

The existence of unique solution of (2.43) depends on the spark of sensing matrix $\mathbf{B}[w]$. Note that from (2.41), the elements of $\mathbf{B}[w]$ are multiplications of the elements of \mathbf{D} and the samples of the low pass filter $G(f)$. In [57], Davies *et al.* proved that the spark of a matrix from an independent continuous distribution achieves the Singleton bound with probability one. When the filter response $G(f)$ is designed to be irregular, i.e., its samples are drawn from an independent random distribution, the spark of $\mathbf{B}[w]$ after multiplication with the samples of $G(f)$ should grow closer to achieving the Singleton bound. When the spark of $\mathbf{B}[w]$ indeed achieves the Singleton bound and the condition (2.32) holds, for every K -sparse signal \mathbf{X} the unique solution to (2.43) always exists.

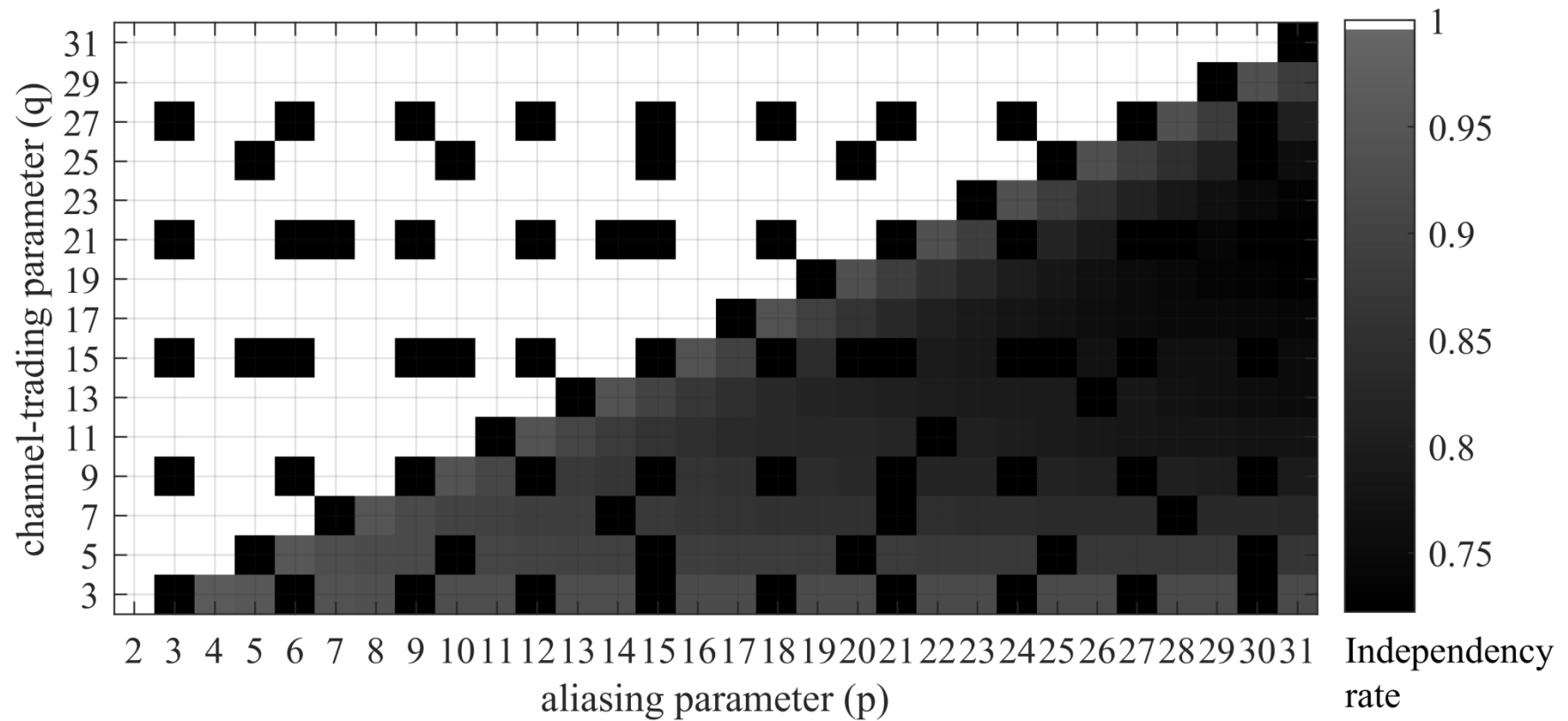


Figure 2.5. Independency rates under various p and q' for which randomly selected Mq' columns of the sensing matrix $\mathbf{D} \in \mathbb{C}^{Mq' \times N}$ of AMWC are independent. When p and q' are coprime and $q' > p$, every selection of Mq' columns is linearly independent.

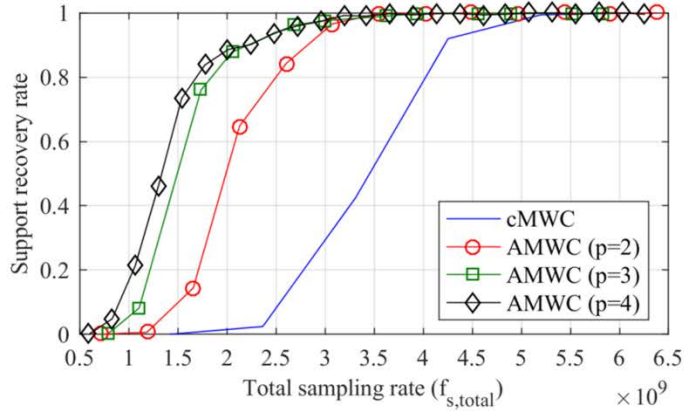
2.5. Simulation

2.5.1. Spark of Sensing Matrix

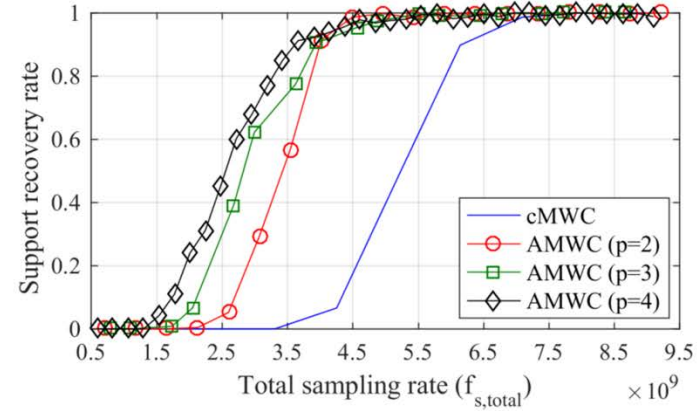
To support Main Result 2.6, the sufficiency of lossless sub-Nyquist sampling by AMWC, we demonstrate that the sensing matrix \mathbf{D} with coprime parameters $q' > p$ achieves the Singleton bound.

Monte Carlo experiments were performed under various settings of p and q' . With $L = 127$, we used the maximum length sequences of length L as the chip values of PR signal for each channel $i = 1, \dots, M$. We set the number of analog channels to $M = 3$. For 5×10^5 independent trials, we randomly selected Mq' columns of \mathbf{D} and counted the rate for which the selected columns are linearly independent.

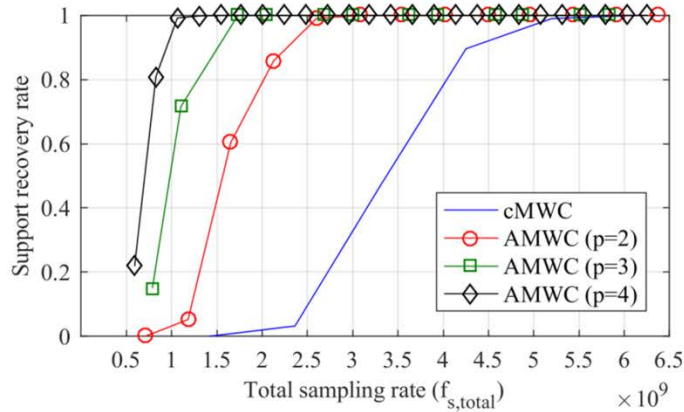
Figure 2.5 shows how the linear independency of columns in \mathbf{D} varies as p and q' change. The white points in the plot indicate the pairs of p and q' where every selection of Mq' columns of \mathbf{D} is linearly independent. The dark points indicate that at least one selection of Mq' columns has linear dependency. The upper triangular area indicates the region of (p, q') with $q' > p$ where all points except for the points that p and q' are not coprime belong to the white set. That is, for coprime $q' > p$, all the selections of Mq' columns are linearly independent, and thus the spark of \mathbf{D} achieves the Singleton bound. This result is consistent with Proposition 2.5 and supports Main Result 2.6.



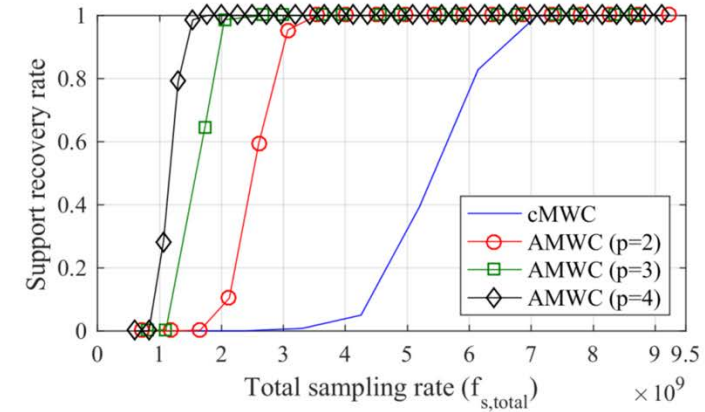
(a) $K_B = 10$, ideal low-pass filters



(b) $K_B = 20$, ideal low-pass filters

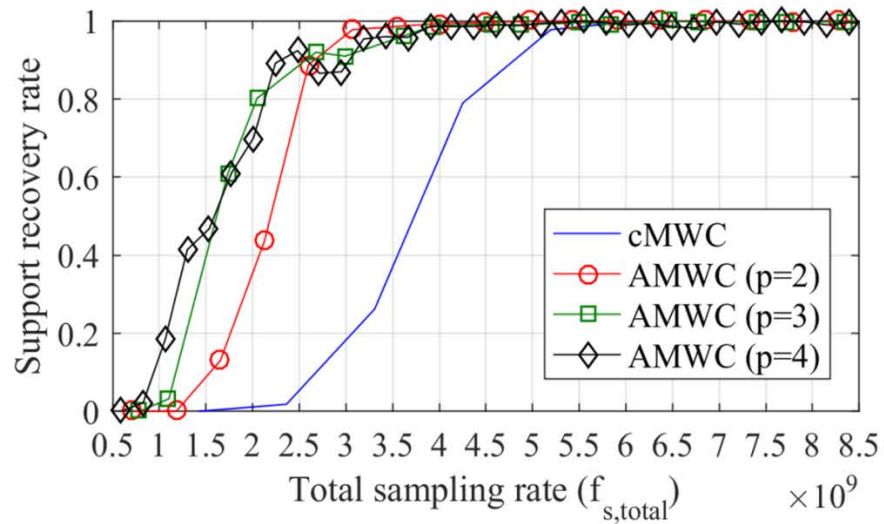


(c) $K_B = 10$, random low-pass filters

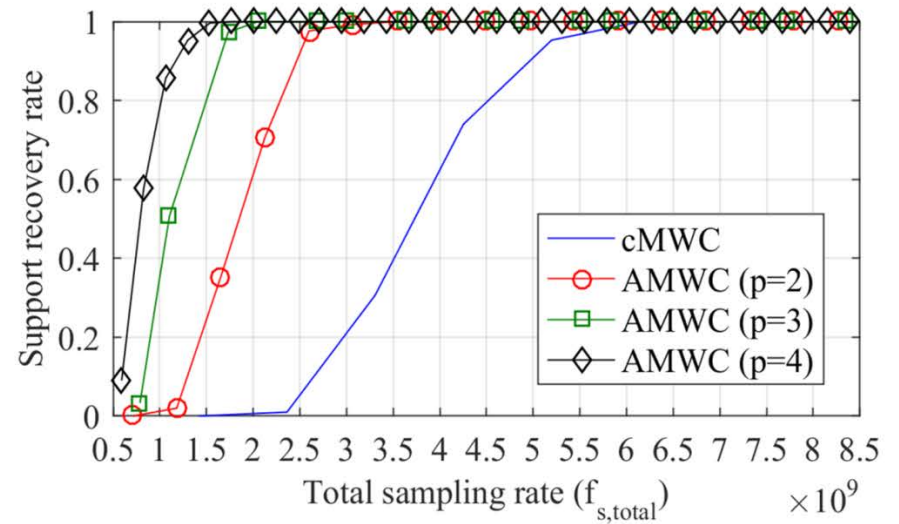


(d) $K_B = 20$, random low-pass filters

Figure 2.6. Rate of successful support recovery of cMWC and AMWC as a function of total sampling rate for various aliasing parameters p and multibands K_B . The number of channels was fixed to $M = 3$. Ideal ((a)-(b)) and random ((c)-(d)) low-pass filters were used.

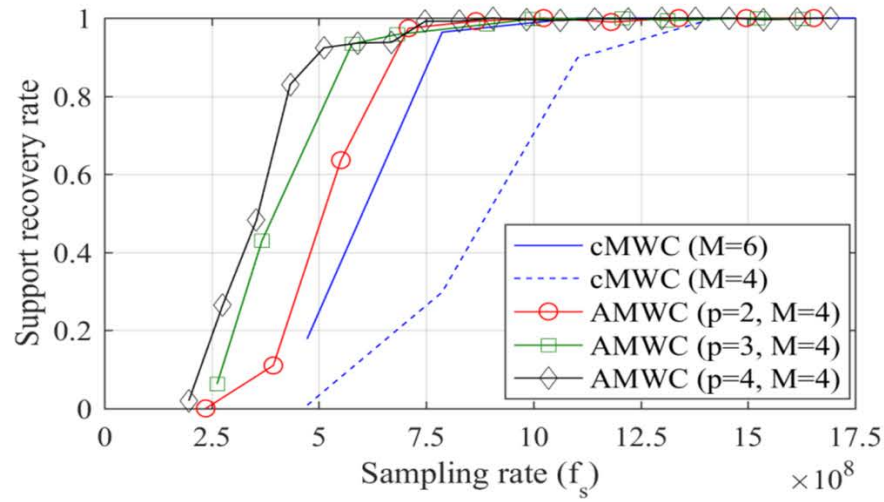


(a) Ideal low-pass filters

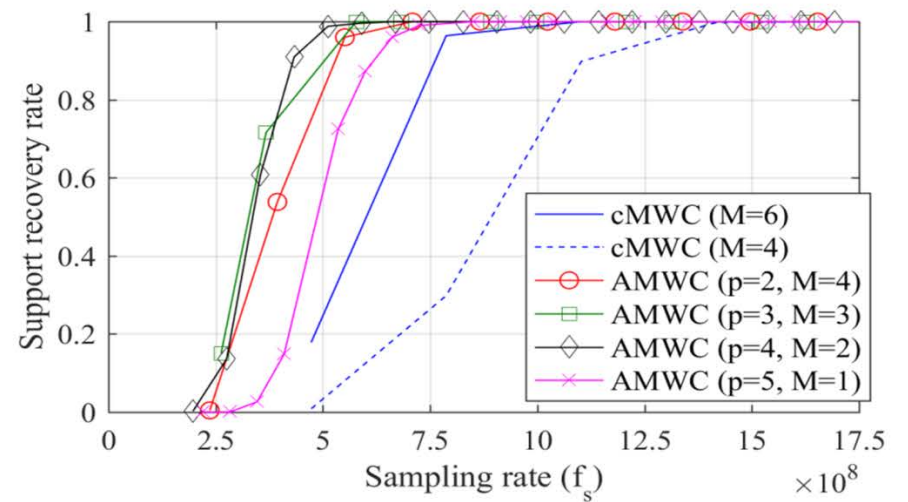


(b) Random low-pass filters

Figure 2.7. Rate of successful support recovery of cMWC and AMWC as a function of total sampling rate when SNR=3 [dB]. The number of channels was fixed to $M = 3$, and the number of multibands in $X(f)$ is fixed to $K_b = 10$. Ideal (a) and random (b) low-pass filters were used.



(a) Ideal low-pass filters



(b) Random low-pass filters

Figure 2.8. Rate of successful support recovery of cMWC and AMWC as a function of sampling rate of each channel for various aliasing parameters p and the number of channels M . The number of multibands was fixed to $K_B = 10$. Ideal (a) and random (b) low-pass filters were used

2.5.2. Reduction of Total Sampling Rate

We demonstrate that, with the improved sampling efficiency, AMWC indeed reduces the total sampling rate required for lossless sub-Nyquist sampling for given specifications of PR signals. Additionally, when the frequency response of low-pass filters is drawn at random, the reduction of total sampling rate is boosted. The reduction of total sampling rate reduces the number of channels as well as the sampling rate of each channel.

For simulation, we generated real-valued multiband inputs $x(t)$ as the sum of K_B narrow band signals of bandwidth $B = 5$ [MHz]. The energies of narrow bands are equal. The center frequencies of narrow band signals were drawn at random, while those spectra were not overlapped with each other. The maximum frequency of $x(t)$ does not exceed $f_{\max} = 10$ [GHz]. The signals last for the duration $T_o = 2WT'_p$ seconds with $W = 15$. The parameters of PR signals were $L = 127$, $f_p = 2f_{\max}L^{-1} \approx 157.48$ [MHz]. We used maximum length sequences with different initial seeds as the chip values of PR signals for channel indices $i = 1, \dots, M$. We expressed the continuous signals in simulation on a dense discrete-time grid with intervals of $(2q'f_{NYQ})^{-1}$ seconds. The bandwidth of low-pass filters and the sampling rate followed the parameter relations of AMWC, i.e., $W_{LPF} = q'f_p$ and $f'_s = p^{-1}W_{LPF}$. We considered the ideal LPF $H(f)$ with a flat passband response and the non-ideal LPF $G(f)$ with an irregular passband response. In simulation, the impulse response of $G(f)$ was drawn initially from the normal distribution, windowed to limit the filter bandwidth, and then held fixed throughout the whole simulation. We call $G(f)$ the random LPF with this irregular passband response. Under various settings of p , q' , and K_B with coprime $q' > p$, we measured the rate of successful recovery of the supports of \mathbf{X} by the distributed CS orthogonal matching pursuit (DCS-SOMP) algorithm [56]. For single supports estimation, DCS-SOMP was run for $2K_B$ iterations. It aimed to find one distinct support per each iteration out of K supports, given $K \leq 2K_B$. Once the supports are found, x can be reconstructed by the least squares. The successful

support recovery was declared if $\mathcal{S} \subseteq \hat{\mathcal{S}}$, where \mathcal{S} and $\hat{\mathcal{S}}$ are, respectively, the true and found supports. The support recovery rate in simulations was defined as the number of successful support recovery divided by total 500 trials with randomly regenerated $x(t)$.

Figure 2.6 shows the support recovery rate of AMWC as a function of total sampling rate when $M = 3$. We set $K_B = \{10, 20\}$. Plots (a) and (b) are results of using the ideal LPF $H(f)$. It is demonstrate that compared to cMWC, AMWC reduces the total sampling rate required for reconstruction of given multiband signals. Inversely, for a given total sampling rate, AMWC takes sub-Nyquist samples of more multibands than cMWC does, without information loss.

However, when p increases, although the sampling efficiency is improved proportionally to p from (2.35), the total sampling rate does not decrease anymore. This is caused by the lack of degrees of freedom in the sensing matrix \mathbf{D} . The elements of \mathbf{D} are made of the Fourier coefficients $c_{i,l}$ of the PR signals, and most elements are repeatedly reused. Although it was demonstrated in the previous sub-section that \mathbf{D} has the maximum spark and well preserves the sparse signal \mathbf{X} , recovering \mathbf{X} by non-optimal CS algorithms requires \mathbf{D} to have a large degrees of freedom [9]. This limitation is overcome by using the random LPF $G(f)$.

Plots (c) and (d) are the results of using the random LPF $G(f)$. It is shown that AMWC further reduces the total sampling rate required for successful support recovery as the sampling efficiency improves. Consequently, the random response of $G(f)$ enhances the degrees of freedom of sensing matrices $\mathbf{B}[w]$ for different frequency indices w and improves the recovery performance by the non-optimal algorithm DCS-SOMP. This enhancement cannot be applied for cMWC, since the effect of random response becomes removable by equalization [55].

In Figure 2.7, additive white Gaussian noise $n(t)$ of SNR=3 [dB] was considered, where the signal-to-ratio noise (SNR) in decibel is defined as $\text{SNR} \triangleq 10 \log_{10} \left(\frac{\|x\|^2}{\|n\|^2} \right)$. We

fixed $K_B = 10$. Plots (a) and (b) are the results for using the ideal LPF and the random LPF, respectively. Despite the additive noise, the results show that AMWC still reduces the total sampling rate or improves the recovery performance. Including the results in Figure 2.8, we conducted more simulations under various $\text{SNR} = \{-6, -3, 0, 3, 12\}$ [dB] but omitted to repeat the plots as the graphs exhibit the similar pattern. Instead, we summarized the minimal sampling point results in Table 2.3, where the minimal sampling point is defined as the minimal total sampling rate which achieves the support recovery rate of 90%. In the results, as p and/or SNR increase, the minimal sampling point gets smaller, which is expected.

Figure 2.8 demonstrates that AMWC reduces the number of channels required for the support recovery. We set $K_B = 10$ and compared the support recovery rates of cMWC and AMWC for various M and given sampling rate of each channel. In plot (a), the support recovery rate of AMWC slightly outperforms cMWC, although AMWC uses fewer channels with a lower sampling rate of each channel than cMWC. Additionally, in plot (b), when the random low-pass filter is used, AMWC using a single channel outperforms cMWC using six channels.

As the increase in the number of rows in \mathbf{Z} in (2.29) or in (2.43) by p -times, the performance of AMWC is improved but the computational complexity (CC) for the support recovery with AMWC inevitably increases as well. The CC of a compressed sensing algorithm depends on the sizes of matrices in the linear inverse problem $\mathbf{Z} = \mathbf{D}\mathbf{X}$. Let $Q_{equation}$, Q_{sample} , and $Q_{subband}$ denote the number of rows and columns of \mathbf{Z} and the number of rows of \mathbf{X} for cMWC problem, respectively. We make note of the report that the CC of DCS-SOMP with cMWC is $O(Q_{equation}^2 Q_{subband} Q_{sample})$ [56]. When the two total sampling rates $f_{s,total}$ of cMWC and $f'_{s,total}$ of AMWC are equal to each other, the number of rows of \mathbf{Z} of AMWC becomes $pQ_{equation}$ and that of \mathbf{X} becomes $pQ_{subband}$, respectively, as discussed in Section 2.3.2. In addition, since the bandwidth of the subbands of AMWC is

p -times narrower than that of cMWC, the number of columns of \mathbf{Z} becomes $p^{-1}Q_{sample}$.
Thus, the CC of DCS-SOMP with AMWC is $O(p^2 Q_{equation}^2 Q_{subband} Q_{sample})$.

SNR [dB]	LPF	$p=1$ (cMWC)	$p=2$ (AMWC)	$p=3$ (AMWC)	$p=4$ (AMWC)
-6	Ideal	6.142	4.016	3.622	3.898
	Random	6.142	3.543	2.677	2.244
-3	Ideal	6.142	3.543	3.622	3.425
	Random	6.142	3.071	2.047	1.535
0	Ideal	5.197	3.071	2.677	2.953
	Random	5.197	2.598	1.732	1.535
3	Ideal	5.197	3.071	2.677	2.480
	Random	5.197	2.598	1.732	1.299
12	Ideal	5.197	3.071	2.677	2.244
	Random	5.197	2.126	1.732	1.063

Table 2.3 The Total Sampling Rate Required for 90% Support Recovery Rate with Various SNR and Values of p . The floating numbers in cells indicate the minimal total sampling rate in GHz which achieves the support rate recovery of 90%. The number of analog channels and multibands were set to $M = 3$ and $K_B = 10$, respectively.

2.6. Conclusion

We proposed a new MWC system called AMWC which improves the sampling efficiency by intentionally inducing an aliasing at the ADC. We showed that the improved sampling efficiency leads to reduction on the sampling rate and number of channels required for obtaining a certain number of equations for signal reconstruction. We provided conditions that the sensing matrix of the equations obtained by AMWC achieves the Singleton bound, and thus no loss from sampling is guaranteed. In summary, the improved sampling efficiency of AMWC reduces the total sampling rate required for lossless sampling. In other words, with fewer channels and less sampling rate of each channel than those of the conventional MWCs, a multiband signal can be captured without information loss by AMWC. Conversely, for given hardware resources, the input reconstruction with AMWC outperforms the conventional MWCs. Extensive simulation demonstrated that AMWC indeed reduces the total sampling rate or improves the reconstruction performance significantly. Additionally, it was demonstrated that the benefits of AMWC are maintained in various SNRs. Moreover, use of LPF with random passband response, it was shown, further improves the sampling efficiency.

Appendices

Appendix 2.A Proof of Lemma 2.2

With the relationship $f_{LPF} = pf'_s$, the pass-band frequency of $H(f - rf'_s)$ in (2.8) is given by $f \in \left[rf'_s - \frac{pf'_s}{2}, rf'_s + \frac{pf'_s}{2} \right)$. When we observe (2.8) only for a single period $\mathcal{F}'_s(f_0)$, since $W_{LPF} > f'_s$, some of $H(f - rf'_s)$, the pass bands of which include the frequency domain $\mathcal{F}'_s(f_0)$, can be replaced by the constant frequency response. Without loss of generality, we set the pass-band response to one, i.e., $H(f) = 1$ for $f \in \mathcal{F}_{LPF}$. Then, for $r \in \mathbb{Z}$ satisfying

$$rf'_s - \frac{pf'_s}{2} \leq f_0 \quad (2.44)$$

and

$$rf'_s + \frac{pf'_s}{2} \geq f_0 + f'_s, \quad (2.45)$$

the shifts of filter responses in (2.8) are replaced with $H(f - rf'_s) = 1$ within $f \in \mathcal{F}'_s(f_0)$. Let R_1 and R_2 be the minimum and maximum integers r satisfying (2.44) and (2.45), respectively. Additionally, for (2.8) and (2.9) to be equivalent, we add some conditions on R_1 and R_2 such that the pass bands of $H(f - rf'_s)$ for r smaller than R_1 and greater than R_2 have no intersection with $f \in \mathcal{F}'_s(f_0)^c$. In other words, we have following conditions on R_1 and R_2 :

$$(R_2 + 1)f'_s - \frac{pf'_s}{2} \geq f_0 + f'_s \quad (2.46)$$

and

$$(R_1 - 1)f'_s + \frac{pf'_s}{2} \leq f_0 \quad (2.47)$$

so that $H(f - rf'_s) = 0$ within $f \in \mathcal{F}'_s(f_0)$ for $r < R_1$ or $r > R_2$. By combining (2.44) and (2.46), we have a condition on R_2 that

$$R_2 f'_s - \frac{pf'_s}{2} = f_0, \quad (2.48)$$

and from (2.45) and (2.47), we have a condition on R_1 that

$$R_1 f'_s + \frac{pf'_s}{2} = f_0 + f'_s. \quad (2.49)$$

Finally, combining (2.48) and (2.49) provides the conditions of Lemma 2.2. ■

Appendix 2.B Proofs of Proposition 2.4 and Lemma 2.7

Proof of Proposition 2.4

We track the input-output relation starting from (2.12):

$$\tilde{Y}_i(e^{j2\pi fT_s'}) = \sum_{r=R_1}^{R_2} \sum_{l=-\infty}^{\infty} c_{i,l} X(f - (lp + rq') f_p')$$

for $f \in \mathcal{F}'_s(f_0)$, where R_1 , R_2 , and f_0 satisfy Lemma 2.2. Alternatively, by using $r' = r - R_1$, we have

$$\begin{aligned} \tilde{Y}_i(e^{j2\pi fT_s'}) &= \sum_{r'=0}^{R_2-R_1} \sum_{l=-\infty}^{\infty} c_{i,l} X(f - (lp + (r' + R_1)q') f_p') \\ &= \sum_{r'=0}^{p-1} \sum_{l=-\infty}^{\infty} c_{i,l} X(f - (lp + (r' + R_1)q') f_p') \end{aligned} \quad (2.50)$$

for $f \in \mathcal{F}'_s(f_0)$, where $R_2 - R_1 = p - 1$ by Lemma 2.2. We replace the term $(r' + R_1)q'$ in (2.50) by a combination of its quotient $\mu_p(r'; q', R_1)$ and remainder $\rho_p(r'; q', R_1)$ by divisor p , which are, respectively, defined by

$$\mu_p(r'; q', R_1) \triangleq \left\lfloor \frac{(r' + R_1)q'}{p} \right\rfloor \quad (2.51)$$

and

$$\rho_p(r'; q', R_1) \triangleq ((r' + R_1)q') \bmod p. \quad (2.52)$$

By substituting $(r' + R_1)q' = p \cdot \mu_p(r'; q', R_1) + \rho_p(r'; q', R_1)$ into (2.50), we have

$$\begin{aligned}
& \tilde{Y}_i(e^{j2\pi f T'_s}) \\
&= \sum_{l=-\infty}^{\infty} \sum_{r'=0}^{p-1} c_{i,l} X(f - (lp + p \cdot \mu(r') + \rho(r')) f'_p) \\
&= \sum_{l=-\infty}^{\infty} \sum_{r'=0}^{p-1} c_{i,l-\mu(r')} X(f - (lp + \rho(r')) f'_p)
\end{aligned} \tag{2.53}$$

for $f \in \mathcal{F}'_s(f_0)$, where the notations $\mu_p(r'; q', R_1)$ and $\rho_p(r'; q', R_1)$ are simplified to $\mu(r')$ and $\rho(r')$, respectively. When p and q' are coprime, by modular arithmetic, there exists one-to-one correspondence between $\rho(r')$ and r' modulo p . We arrange the order of inner summation of (2.53) by introducing a utility variable $v \triangleq \rho(r') \in \{0, \dots, p-1\}$:

$$\begin{aligned}
& \tilde{Y}_i(e^{j2\pi f T'_s}) \\
&= \sum_{l=-\infty}^{\infty} \sum_{v=0}^{p-1} c_{i,l-\mu(\rho_p^{-1}(v; q', R_1))} X(f - (lp + v) f'_p)
\end{aligned} \tag{2.54}$$

for $f \in \mathcal{F}'_s(f_0)$, where the inverse $\rho_p^{-1}(v; q', R_1)$ of the remainder $\rho_p(r; q', R_1)$ modulo p is computed by

$$\rho_p^{-1}(v; q', R_1) \triangleq (v(q')^{-1} - R_1) \bmod p, \tag{2.55}$$

where $(q')^{-1} \bmod p$ is the multiplicative inverse of q' modulo p . We simplify the expression $\rho_p^{-1}(v; q', R_1)$ to $\rho^{-1}(v)$. From Lemma 2.3, we can merge the inner and outer summations of (2.54) as follows:

$$\tilde{Y}_i(e^{j2\pi f T'_s}) = \sum_{k=-\infty}^{\infty} c_{i, \lfloor \frac{k}{p} \rfloor - \mu(\rho^{-1}(k \bmod p))} X(f - kf'_p) \tag{2.56}$$

for $f \in \mathcal{F}'_s(f_0)$.

We now simplify the picking regularity of the coefficients $c_{i,J(\cdot)}$ in (2.56), which is defined by

$$\begin{aligned} J(k; R_1, p, q') &\triangleq \left\lfloor \frac{k}{p} \right\rfloor - \mu(\rho^{-1}(k \bmod p)) \\ &= \left\lfloor \frac{k}{p} \right\rfloor - \mu(\rho^{-1}(k)). \end{aligned} \quad (2.57)$$

Meanwhile, by the definitions of the quotient $\mu(\cdot)$ and remainder $\rho(\cdot)$, we have

$$\begin{aligned} \mu(\rho^{-1}(k)) &= \left\lfloor \frac{(\rho^{-1}(k) + R_1)q'}{p} \right\rfloor \\ &= \frac{1}{p} \left((\rho^{-1}(k) + R_1)q' - ((\rho^{-1}(k) + R_1)q' \bmod p) \right) \\ &= \frac{1}{p} \left((\rho^{-1}(k) + R_1)q' - \rho(\rho^{-1}(k)) \right) \\ &= \frac{1}{p} \left((\rho^{-1}(k) + R_1)q' - k \bmod p \right). \end{aligned} \quad (2.58)$$

By substituting (2.58) into (2.57),

$$\begin{aligned} J(k; R_1, p, q') &= \left\lfloor \frac{k}{p} \right\rfloor + \frac{k \bmod p}{p} - \frac{(\rho^{-1}(k) + R_1)q'}{p} \\ &= \frac{k}{p} - \frac{(\rho^{-1}(k) + R_1)q'}{p} \\ &= \frac{1}{p} \left\{ k - q' \cdot \left[(k(q')^{-1} - R_1) \bmod p + R_1 \right] \right\} \\ &= I(k; R_1, p, q'). \end{aligned} \quad (2.59)$$

Thus, the proof is completed. ■

Proof of Lemma 2.7

We track the input-output relation starting from (2.36):

$$\tilde{Y}_i(e^{j2\pi fT'_s}) = \sum_{r=R_1}^{R_2} \sum_{l=-\infty}^{\infty} c_{i,l} X(f - (rq' + lp) f'_p) G(f - rq' f'_p)$$

for $f \in \mathcal{F}'_s(f_0)$. Under the conditions of Lemma 2.2 and Lemma 2.3, by using $r' \triangleq r - R_1$, we have

$$\begin{aligned} & \tilde{Y}_i(e^{j2\pi fT'_s}) \\ &= \sum_{r'=0}^{R_2-R_1} \sum_{l=-\infty}^{\infty} c_{i,l} X(f - (lp + (r' + R_1)q') f'_p) G(f - (r' + R_1)q' f'_p) \quad (2.60) \\ &= \sum_{r'=0}^{p-1} \sum_{l=-\infty}^{\infty} c_{i,l} X(f - (lp + (r' + R_1)q') f'_p) G(f - (r' + R_1)q' f'_p) \end{aligned}$$

for $f \in \mathcal{F}'_s(f_0)$. As done in (2.50) to (2.54), we introduce a utility variable $v \triangleq \rho(r')$ and substitute $(r' + R_1)q' = p \cdot \mu(\rho^{-1}(v)) + v$ into the inputs of X and G in (2.60). It then follows

$$\tilde{Y}_i(e^{j2\pi fT'_s}) = \sum_{l=-\infty}^{\infty} \sum_{v=0}^{p-1} \left(c_{i,J(k;R_1,p,q')} X(f - (lp + v) f'_p) \cdot G(f - (p\mu(\rho^{-1}(v)) + v) f'_p) \right) \quad (2.61)$$

for $f \in \mathcal{F}'_s(f_0)$. After merging the inner and outer summations based on Lemma 2.3, we obtain (2.37)

$$\tilde{Y}_i(e^{j2\pi fT'_s}) = \sum_{k=-\infty}^{\infty} d_{i,k}(R_1, p, q') X(f - kf'_p) G(f - \gamma_p(k) f'_p)$$

for $f \in \mathcal{F}'_s(f_0)$, where $\gamma_p(k)$ is defined by

$$\begin{aligned} \gamma_p(k) &\triangleq p\mu(\rho^{-1}(k \bmod p)) + k \bmod p \\ &= p\mu(\rho^{-1}(k)) + k \bmod p. \end{aligned} \quad (2.62)$$

By (2.58) and the definition of $\rho^{-1}(k)$ in (2.55), (2.62) turns into

$$\begin{aligned}
\gamma_p(k) &= (\rho^{-1}(k) + R_1)q' \\
&= q' \left[(kq^{-1} - R_1) \bmod p + R_1 \right].
\end{aligned} \tag{2.63}$$

By the definition of $I(k; R_1, p, q')$ in (2.15), we finally have

$$\gamma_p(k) = k - pI(k; R_1, p, q'). \tag{2.64}$$

Thus, the proof is completed. ■

Appendix 2.C Proof of Proposition 2.5

We first show that if $p > q'$ for coprime p and q' , at least two columns of \mathbf{D} are identical. Then, from a result in [10], this violates a necessary condition for the unique existence of a K -sparse solution.

We first mathematically formulate the meaning of two columns of \mathbf{D} being identical. From Proposition 2.4 and (2.29), the entries $d_{i,k+u}(R_1, p, q')$ of \mathbf{D} are picked from $c_{i,I(k; R_1, p, q')}$, where k and u in $d_{i,k+u}$ represent the column and row position, respectively. To search for identical columns in \mathbf{D} , we investigate the existence of pairs (k^*, ω^*) of a column index k^* and shift index ω^* such that $d_{i,k^*+u} = d_{i,k^*+u+\omega^*}$ for every row index $u \in \mathcal{Q} \triangleq \{0, \dots, q'-1\}$. In other words, we find pairs (k^*, ω^*) satisfying

$$I(k^* + \omega^* + u; R_1, p, q') = I(k^* + u; R_1, p, q'). \tag{2.65}$$

for every $u \in \mathcal{Q}$, where the function I is defined in (2.15). We use a computation result of $I(k) \triangleq I(k; R_1, p, q')$ in the second line of (2.59):

$$I(k) = \frac{k}{p} - \frac{(\rho^{-1}(k) + R_1)q'}{p}, \tag{2.66}$$

where $\rho^{-1}(k) \triangleq \rho_p^{-1}(k; q', R_1)$ is a function modulo p defined in (2.55) by $\rho_p^{-1}(k; q', R_1) \triangleq (k(q')^{-1} - R_1) \bmod p$. By substituting (2.66) into (2.65), we rewrite (2.65) as

$$\begin{aligned} I(k^* + \omega^* + u) &= I(k^* + u) \\ \Leftrightarrow \rho^{-1}(k^* + \omega^* + u) &= \rho^{-1}(k^* + u) + \frac{\omega^*}{q'}. \end{aligned} \quad (2.67)$$

We show that, if $p > q'$ and coprime, there exists at least one pair (k^*, ω^*) of the column index k^* and shifting index ω^* that satisfy (2.67) for every row index $u \in \mathcal{Q}$. Before proceeding, we check a computation of $\rho^{-1}(k + q' + u)$ for every $u \in \mathcal{Q}$. By the definition, it follows

$$\begin{aligned} \rho^{-1}(k + q' + u) &= ((k + q' + u)(q')^{-1} - R_1) \bmod p \\ &= (((k + u)(q')^{-1} - R_1) \bmod p + 1) \bmod p \\ &= (\rho^{-1}(k + u) + 1) \bmod p. \end{aligned} \quad (2.68)$$

Note that (2.68) indicates when ω^* is chosen to q' , it satisfies (2.67), for $k^* \in \mathbb{Z}$ such that $\rho^{-1}(k^* + u) < p - 1$.

What task remains is to show the existence k^* satisfies $\rho^{-1}(k^* + u) < p - 1$ for every row index $u \in \mathcal{Q}$, which implies the existence of identical columns in \mathbf{D} and completes the proof. To this end, we find a set of $\bar{k} \pmod{p}$ such that $\rho^{-1}(\bar{k} + u) = p - 1$. From the definition, we have

$$\begin{aligned} \rho^{-1}(\bar{k} + u) &\equiv p - 1 \pmod{p} \\ (\bar{k} + u)(q')^{-1} - R_1 &\equiv p - 1 \pmod{p} \\ \bar{k} &\equiv (p - 1 + R_1)q' - u \pmod{p} \\ \bar{k} &\equiv (R_1 - 1)q' - u \pmod{p}. \end{aligned} \quad (2.69)$$

Note that $(R_1 - 1)q'$ is a constant. Since the right-hand side of (2.69) varies by $u \in \mathcal{Q}$, the cardinality of set of $\bar{k} \pmod{p}$ such that $\rho^{-1}(\bar{k} + u) = p - 1$ is $|\mathcal{Q}| = q'$. Since $p > q'$, this implies there exists $k^* \pmod{p} \in \{0, 1, \dots, p - 1\}$ such that $\rho^{-1}(k^* + u) < p - 1$, and $k^* \in \mathbb{Z}$ such that $\rho^{-1}(k^* + u) < p - 1$ exists as well.

Consequently, if coprime $p > q'$, there must exist at least one pair of identical columns in \mathbf{D} . The existence of identical columns in \mathbf{D} implies $\text{spark}(\mathbf{D}) = 2$. Theorem 2 in [10] states that there exist the unique solution of a linear equation $\mathbf{Z} = \mathbf{D}\mathbf{X}$ for every K -sparse solution \mathbf{X} only if

$$K < \frac{\text{spark}(\mathbf{D}) - 1 + \text{rank}(\mathbf{X})}{2}, \quad (2.70)$$

where *spark* is the minimum number of linearly dependent columns in \mathbf{D} . If $\text{spark}(\mathbf{D}) = 2$, for signals \mathbf{X} with $\text{rank}(\mathbf{X}) \leq 2K - 1$, the condition $p > q'$ violates (2.70). ■

Chapter 3

Profitable Double-Spending Attacks

3.1. Introduction

A blockchain is a distributed ledger which has originated from the desire to find a novel alternative to centralized ledgers such as transactions through third parties [20]. Besides the role as a ledger, blockchains have been applied to many areas, e.g., managing the access authority to shared data in the cloud network [58] and averting collusion in e-Auction [59]. In a blockchain network based on the proof-of-work (PoW) mechanism, each miner verifies transactions and tries to put them into a block and mold the block to an existing chain by solving a cryptographic puzzle. This series of processes is called *mining*. But the success of *mining* a block is given to only a single *miner* who solves the cryptographic puzzle for the first time. The reward of minting a certain amount of coins to the winner motivates more miners to join and remain in the network. As a result, blockchains have been designed so that the validity of transactions is confirmed by a lot of decentralized miners in the network.

A consensus mechanism is programmed for decentralized peers in a network to share a common chain. If a full-node succeeds in generating a new block, it has the latest version of the chain. All of the nodes in the network continuously communicate with each other to share the latest chain. A node may run into a situation in which it encounters mutually different chains more than one. In such a case, it utilizes a consensus rule with which it selects a single chain. Satoshi Nakamoto suggested the *longest chain consensus* for *Bitcoin* protocol in which the node selects the longest chain among all competing chains [20]. There are also other consensus rules [23],[60], but a common goal of consensus rules is to select the single chain by which the most computation resources have been consumed based on the belief that it may have been verified by the largest number of miners.

A double-spending (DS) attack aims to double-spend a cryptocurrency for the worth of which a corresponding delivery of goods or services has already been completed. The records of payment are written in transactions and shared in a network via the status-quo chain. Thus, to double spend, attackers need to replace the status-quo chain in the network with their new one, after taking the goods or services. For example, under the longest chain consensus, this attack will be possible if an attacker builds a longer chain than the status-quo. Nakamoto [20] and Rosenfeld [27] have shown that the higher computing power is employed, the higher probability to make a DS attack successful is. In addition, if an attacker invests more computing power than that invested by a network, a success of DS attack is guaranteed. Such attacks are called the 51% attack.

In the last few years, unfortunately, blockchain networks have been recentralized [61],[62], which make them vulnerable to DS attacks. To increase the chance of mining blocks, some nodes may form a pool of computing chips. The problem arises when a limited number of pools occupy a major proportion of the computing power in the network. For example, the pie chart shown in Figure 3.1 illustrates the proportion of computing power in the Bitcoin network as of January 2020. In the chart, five pools such as F2Pool, BTC.com, Poolin, and Huobi.pool, occupy more than 50% of the total computing power of Bitcoin. In a recentralized network, since most computing resources are concentrated on a small number of pools, it could be not difficult for them to conspire to alter the block content for their own benefits, if not aiming to double spend, more probable. Indeed, there have been a number of reports in 2018 and 2019 in which cryptocurrencies such as *Verge*, *BitcoinGold*, *Ethereum Classic*, *Feathercoin*, and *Vertcoin* suffered from DS attacks and millions of US dollars have been lost [28].

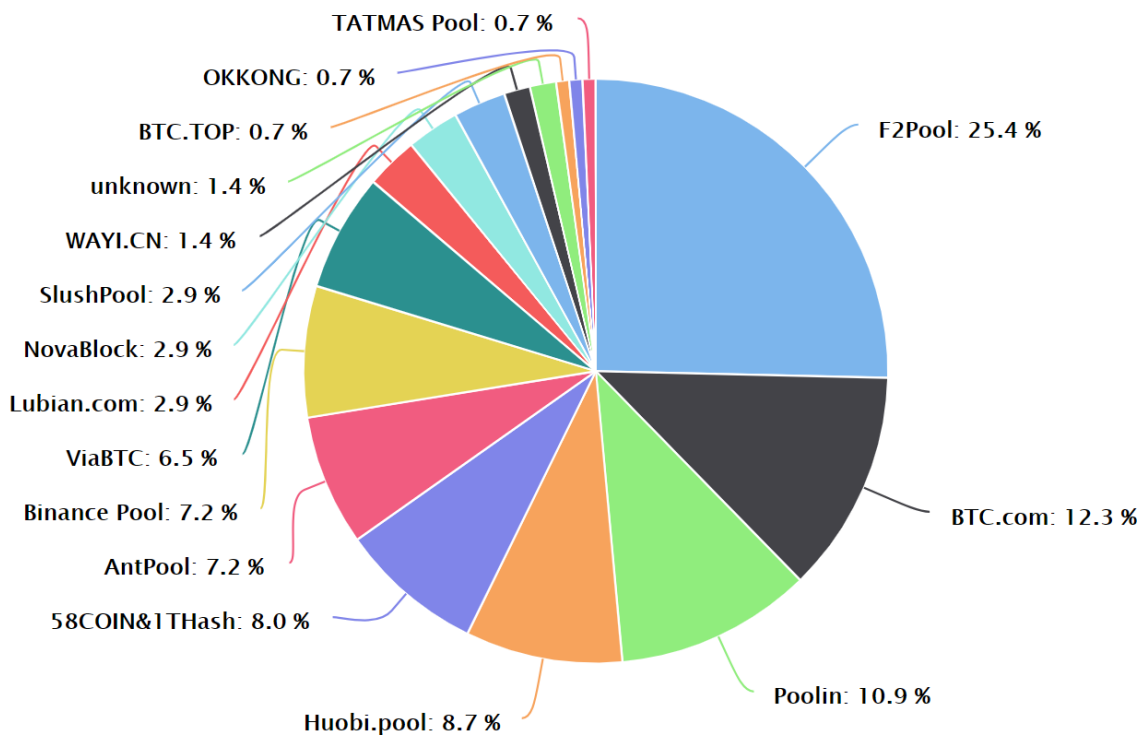


Figure 3.1. Computation power distribution among the largest mining pools provided by *BTC.com* (date accessed: Nov. 24, 2020).

In addition to the recentralization, the advent of rental services which lend the computing resources can be a concern as well [63]. Rental services such as *nicehash.com* which provide a brokerage service between the suppliers and the consumers have indeed become available. The rental service can be misused for making DS attacks easier. The presence of such computing resource rental services make the cost, to make a profit from double spending, significantly reduced. It is because renting a required computing power for a few hours is much cheaper than building such a computing network. Indeed, *nicehash.com* attracts DS attackers to use their service by posting one-hour fees for renting 51% of the total computing power against dozens of blockchain networks on their website *crypto51.app*.

Success by making DS attacks is possible but is believed to be difficult for a public blockchain with a large pool of mining network support. By the results in [20] and [27], 51% attack has been considered as the requirement for a successful DS attack [64]. This

conclusion however shall be reconsidered given our result in the sequel that there are significant chances of making a good profit from DS attacks regardless of the proportion of computing power. The problem to consider, therefore, is to analyze the profitability of such attacks.

The analysis of attack profitability requires the ability to predict the time an attack will consume for a success, since the profit would be a function of time. Studies in [65]–[73] provided DS attack profitability analyses, but their time predictions were not accurate. Specifically, to make the time prediction easier, they either added impractical assumptions to the DS attack model defined by Nakamoto [20] and Rosenfeld [27] or oversimplified the time prediction formula (see Section 3.6 for details). Whereas, we follow the definition of DS attack in [20],[27], and therefore we need to develop a new set of mathematical tools for precise analysis of attack profitability that we aim to report in this chapter.

3.1.1. Contributions

We study the profitability of DS attacks. The concept of *cut-time* is introduced. *Cut-time* is defined to be the duration of an attack attempt, from the start time to the end time of an attack. For each DS attempt, the attacker needs to pay for the cost to run his mining rig. A rational attacker would not, therefore, continue an attack indefinitely especially when operating within the regime of less than 50% computing power. To reduce the cost, the attacker needs to figure out how his attack success probability rolls out to be as the time progresses. We define that a DS attack is profitable if and only if the expected profit, the difference between revenue and cost (see equation (3.29)), is positive. Our contributions are summarized into two-folds:

First, we theoretically show that DS attacks can be profitable not only in the regime of 51% attack but also in the sub-50% regime where the computing power invested by the attacker is smaller than that invested by the target network. Specifically, a sufficient and necessary condition is derived for profitable DS attacks on the minimum value of target transaction. In the sub-50% regime, we also show that profitable DS attacks necessitate setting a finite cut-time.

Second, we derive novel mathematical results that are useful for an analysis of the attack success time. Specifically, the probability distribution function and the first moment expectation of the attack success time have been derived. They enable us to estimate the expected profit of a DS attack for a given cut-time. All mathematical results are numerically-calculable. All the examples to find the theoretical results in this chapter are provided in our web-site¹.

3.1.2. Contents of Chapter

The remainder of this chapter is organized as follows. In Section 3.2, we define DS attack scenario and sufficient and necessary conditions required for successful DS attacks. Also, we define random variables that are useful in analyzing the attack profits. Section 3.3 comprises the analytic results of stochastics of the time-finite attack success. In Section 3.4, we define the profit function of DS attacks, followed by new theoretical results about the conditions for making them profitable. In Section 3.5, an example analysis of DS attack profitability in sub-50% regime against BitcoinCash network is given. Section 3.6 compares our results with related works. In Section 3.7, by using Monte Carlo experiments, we check the correctness of our mathematical results given in 3.3. Finally, Section 3.8 concludes the paper with a summary.

3.2. The Attack Model

We define DS attack that we consider throughout this chapter. We also define DS attack achieving (DSA) time, which is the least time spent for an occurrence of double-spending. The DSA time is a random variable derived from a random walk of Poisson counting processes (PCP).

¹ <https://codeocean.com/capsule/2308305/tree>

3.2.1. Attack Scenario

We extend a DS attack scenario which has been considered by Nakamoto [20] and Rosenfeld [27]. Specifically, we additionally investigate a time-finite attack scenario: an ongoing attack can be stopped at a predetermined time for some profit. There are two groups of miners, the normal group of honest miners and a single attacker. The normal group works for the honest chain.

When the attacker decides to launch a DS attack, he/she makes a target transaction for the payment of goods or services. In the target transaction, the transfer of cryptocurrency ownership from the attacker to a victim is written. We denote $t=0$ as the time at which the last block of the honest chain has been generated. At time $t=0$, the attacker announces the target transaction to normal group so that normal group starts to put it into the honest chain. At the same time $t=0$, the attacker makes a fork of the honest chain which stems from the last block and builds it in secret. We refer to this secret fork as fraudulent chain. In the fraudulent chain, a fraudulent transaction is contained which alters the target transaction in a way that deceives the victim and benefits the attacker.

Before shipping goods or providing services to the attacker, the victim will obviously choose to wait for a few more blocks on the honest chain in addition to the block on which the his/her transaction has been entered, i.e., so-called block confirmation. Karame et al. in [74] showed the importance of block confirmation: attackers are able to double-spend against zero block-confirmation even without mining a single block on the fraudulent chain at all. The number of blocks the victim chooses to wait for is referred to as the block confirmation number $N_{BC} \in \mathbb{N}$, which includes the block on which the target transaction is entered.

The attacker chooses to make the fraudulent chain public if his/her attack was successful. An attack is successful if the fraudulent chain is longer than the honest chain after the moment the block confirmation is satisfied. We define two necessary conditions $\mathcal{G}^{(1)}$, $\mathcal{G}^{(2)}$ for a success of DS attack:

Definition 3.1. A DS attack succeeds only if there exists a DS attack achieving (DSA) time $T_{DSA} \in (0, \infty)$ such that

1. $\mathcal{G}^{(1)}$: (block confirmation) the length of the honest chain for the duration of time T_{DSA} has grown greater than or equal to N_{BC} , and
2. $\mathcal{G}^{(2)}$: (success in PoW competition) the length of the fraudulent chain for the duration of time T_{DSA} has grown longer than that of the honest chain.

Rational attackers will not wait for his success indefinitely since growing the attacker's chain incurs the expense per time spent for operating the computing power. The attack thus shall put a limit to the end time to cut the increase of loss. We refer to this end time as the cut-time $t_{cut} \in \mathbb{R}^+$. A sufficient condition for the success of DS attack can be defined with applying the cut-time t_{cut} :

Definition 3.2. For a given cut-time $t_{cut} \in \mathbb{R}^+$, the success of DS attack is declared if and only if there exists a DSA time $T_{DSA} \in (0, t_{cut})$ at which $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ in Definition 3.1 has been achieved.

3.2.2. Stochastic Model

We model the conditions in Definition 3.2 with a stochastic model. We fit the block generation process using the PCP [75] with a given block generation rate λ (blocks per second). Including Nakamoto [20] and Rosenfeld [27], it has been most conventional to analyze the block generation process of a blockchain using PCP. A rationale why the block generation process is modeled as PCP is given in Bowden *et al.* [76], where experiments show the fitness of PCP model to real data samples from a live network.

We denote the lengths of the honest chain and the fraudulent chain over time $t \in (0, \infty]$ by two independent PCPs, $H(t) \in \mathbb{N}_0$ with the block generation rate λ_H (blocks per second) and $A(t) \in \mathbb{N}_0$ with the block generation rate λ_A , respectively. Both processes

start at the time origin $t = 0$ (at which the DS attack is launched) at which the both chains are at the zero states, i.e., $H(0) = A(0) = 0$. Each chain independently increases at most by 1 at a time point. An increment of 1 in the counting process occurs when the pertinent network adds a new block to its chain.

We represent the difference between $A(t)$ and $H(t)$ in a discrete-time domain as a random walk $S_i \in \mathbb{Z}$ for $i \in \mathbb{N}$. For this purpose, we first define two continuous stochastic processes $M(t)$ and $S(t)$, which are respectively defined as

$$M(t) := H(t) + A(t), \quad (3.1)$$

and

$$S(t) := H(t) - A(t). \quad (3.2)$$

The first process $M(t)$ is also a PCP [75] with the rate

$$\lambda_T := \lambda_A + \lambda_H. \quad (3.3)$$

The second process $S(t)$ is the continuous-time analog of the random walk $S_i \in \mathbb{Z}$ for $i \in \mathbb{N}$ such that

$$S_i := S(T_i), \quad (3.4)$$

where T_i is the state progression time defined by

$$T_i := \inf \{ t \in \mathbb{R}^+ : M(t) = i \}, \quad (3.5)$$

which increases as i increases. Random walk S_i is a stationary Markov chain starting from $S_0 = 0$. The state transition probabilities [75] are given by

$$p_A := \Pr(S_i = n-1 | S_{i-1} = n) = \frac{\lambda_A}{\lambda_T}, \quad (3.6)$$

and

$$p_H := \Pr(S_i = n+1 | S_{i-1} = n) = \frac{\lambda_H}{\lambda_T}, \quad (3.7)$$

for all $i \in \mathbb{N}$ and $n \in \mathbb{Z}$. The state transition probabilities p_H and p_A are the proportions of computing power occupied by the normal miners and that by the attacker, respectively.

We define independent and identically distributed (i.i.d.) state transition random variables $\Delta_i \in \{\pm 1\} \sim \text{Bernoulli}(p_H)$ as

$$\Delta_i := S_i - S_{i-1}, \quad (3.8)$$

for $i \in \mathbb{N}$. Note that $S_i = \sum_{k=0}^i \Delta_k$.

The stochastic process S_i is measurable with respect to a filtration $\mathcal{F}_i = \sigma(\Delta_1, \Delta_2, \dots, \Delta_i)$, i.e., the σ -algebra generated by Δ_k for all $1 \leq k \leq i$. Also, Given events $\{M(t) = i\}$ for $i \in \mathbb{N}$, we define a sequence of probability space $(\Omega_i, \mathcal{F}_i, \mathbb{P}_i)$, where $\Omega_i = \{\pm 1\}^i$ and \mathbb{P}_i is the probability measuer.

Definition 3.3. A DS attack $\text{DS}(p_A, t_{cut}; N_{BC})$ is a random experiment that picks a sample $\omega \in \Omega_\infty$.

3.2.3. DS Attack Achieving Time

Definition 3.4. For a given DS sample ω of $\text{DS}(p_A, t_{cut}; N_{BC})$ which achieves the necessary conditions $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ in Definition 3.1 at a state index i , we define the DSA time T_{DSA} by the state progression time T_i defined in (3.5).

To express T_{DSA} as a random variable, we construct two events $\mathcal{D}_j^{(1)} \subset \Omega_\infty$ and $\mathcal{D}_{i,j}^{(2)} \subset \Omega_\infty$. One event set $\mathcal{D}_j^{(1)}$ for $j \in \{N_{BC}, N_{BC} + 1, \dots, \infty\}$ consist of DS samples ω which achieves the block confirmation $\mathcal{G}^{(1)}$ at state j for the first time. The other event set $\mathcal{D}_{i,j}^{(2)}$ for $i \in \{j, j+1, \dots, \infty\}$ and $j \in \{N_{BC}, N_{BC} + 1, \dots, \infty\}$ consists of ω which achieves the success in the PoW competition $\mathcal{G}^{(2)}$ at state i for the first time with assuming that $\mathcal{G}^{(1)}$ has been already achieved at state j . Subsequently, we aim for the samples $\omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}$ to achieve the two conditions in Definition 3.1 at a state pair (i, j) for the first time.

Formally, we first construct the set $\mathcal{D}_j^{(1)}$ focusing only on the first j transitions Δ_k for $k = 1, \dots, j$ of DS samples ω with two requirements; one is that they must have N_{BC} number of $+1$'s and $j - N_{BC}$ number of -1 's; and the other is that the j -th transition Δ_j must be $+1$ to guarantee that they have never been achieved in any states prior to the state j . The former requirement implies that all $\omega \in \mathcal{D}_j^{(1)}$ hold $S_j = \sum_{k=1}^j \pi_{\Delta_k}(\omega) = 2N_{BC} - j$. For example, when $N_{BC} = 2$ and $j = 5$, a sequence $(+1, -1, -1, -1, +1, \dots)$ of state transitions satisfies the first requirement, and also satisfies $S_j = 2N_{BC} - j$.

We next construct the set $\mathcal{D}_{i,j}^{(2)}$ which does not care about the first j transitions Δ_k for $k = 1, \dots, j$, but only focuses on the interim transitions Δ_m for $m = j+1, \dots, i$. By the definition, all sequences $\omega \in \mathcal{D}_{i,j}^{(2)}$ must achieve $\mathcal{G}^{(1)}$ before the j -th state, which implies that they must hold $S_j = 2N_{BC} - j$. The rest requirement for each $\omega \in \mathcal{D}_{i,j}^{(2)}$ is that the state changes from the starting state $S_j = 2N_{BC} - j$ to the goal state $S_i = -1$, while any interim states S_k remain non-negative; i.e., $S_k \geq 0$ for each $k = j+1, \dots, i-1$.

The sets $\mathcal{D}_j^{(1)}$ for each j are mutually exclusive as each of which represents the first satisfaction of the block confirmation condition exactly at the j -th state. For example, if $\omega \in \mathcal{D}_5^{(1)}$ then $\omega \notin \mathcal{D}_6^{(1)}$ since ω already has achieved the block confirmation at the 5-th state for the first time before reaching the 6-th state. The sets $\mathcal{D}_{i,j}^{(2)}$ for all (i, j) are also mutually exclusive for the same reason. Thus, their intersections $\mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}$ for all (i, j) are also mutually exclusive.

By Definition 3.4, the attack achieving time T_{DSA} can be measured if there exist index pairs (i, j) such that $\omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}$. By the mutual exclusivity of $\mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}$ for indices i and j , if there exists such a pair (i, j) , it must be unique. That is, if $\omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}$, T_{DSA} equals T_i . As the result, T_{DSA} can be rewritten as follow,

$$T_{DSA} = \begin{cases} T_i, & \text{if } \exists (i, j) \in \mathbb{N}^2: \omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}, \\ \infty, & \text{otherwise.} \end{cases} \quad (3.9)$$

3.3. The Attack Probabilities

We aim to calculate the probability distribution function (PDF) of the DSA time T_{DSA} . Using this, the success probability of DS attack with a given cut-time t_{cut} can be figured out as the probability that $T_{DSA} < t_{cut}$. Also, the expectation of attack success time can be calculated. The expected attack success time will be used in Section 3.4 to estimate the attack profits.

From (3.9), the PDF of T_{DSA} requires the probabilities of two random events; one is the state progression time T_i in (3.5); and the other is the event that a given state index i satisfies $\omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}$. It has been well known that T_i follows Erlang distribution [75] given as

$$f_{T_i}(t) = \frac{\lambda_T (\lambda_T t)^{i-1} e^{-\lambda_T t}}{(i-1)!} \quad (3.10)$$

for $t > 0$. We provide the probability for the latter event, i.e., $p_{DSA,i} = \Pr(\omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)})$ in the following Lemma 3.5:

Lemma 3.5. For a sample ω of random experiment $DS(p_A, t_{cut}; N_{BC})$, the probability $p_{DSA,i} = \Pr(\omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)})$ can be computed as

$$p_{DSA,i} = \sum_{j=N_{BC}}^{j=2N_{BC}} \binom{j-1}{N_{BC}-1} C_{\frac{i-1}{2}-N_{BC}, 2N_{BC}-j} p_A^{\frac{i+1}{2}} p_H^{\frac{i-1}{2}} + \binom{i-1}{N_{BC}-1} p_H^{N_{BC}} p_A^{i-N_{BC}} \quad (3.11)$$

for odd $i > 2N_{BC}$, where $C_{n,m}$ is the ballot number [77] given by

$$C_{n,m} := \begin{cases} \frac{m+1}{n+m+1} \binom{2n+m}{n}, & n, m \in \mathbb{Z}^+ \cup \{0\}, \\ 0, & \text{otherwise,} \end{cases} \quad (3.12)$$

and for $i \leq 2N_{BC}$ and for all even-numbered i , $p_{DSA,i} = 0$.

Proof: See Appendix 3.A.

By taking infinite summations of $p_{DSA,i}$ in Lemma 3.5 for all indices $i \in \mathbb{N}$, we can compute the probability \mathbb{P}_{DSA} that a DS attack will ever achieve the necessary conditions in Definition 3.1.

Corollary 3.6. For a sample ω of random experiment $DS(p_A, t_{cut}; N_{BC})$ with $t_{cut} = \infty$, the probability \mathbb{P}_{DSA} has an algebraic expression

$$\mathbb{P}_{DSA} = \begin{cases} 1, & p_H \leq p_A, \\ 1 - p_A^{N_{BC}+1} p_H^{N_{BC}} \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} A_j, & p_H > p_A, \end{cases} \quad (3.13)$$

where

$$A_j := p_A^{j-2N_{BC}-1} - p_H^{j-2N_{BC}-1}. \quad (3.14)$$

Proof. See Appendix 3.B.

From (3.9), the PDF of T_{DSA} follows the PDF of T_i at a given state index i , if at which it holds that $\omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}$, with the probability of $p_{DSA,i}$. If there does not exist such an index i , with the probability of $1 - \mathbb{P}_{DSA}$, then $T_{DSA} = \infty$. Thus, we can write a (generalized) PDF $f_{T_{DSA}}$ of T_{DSA} as follow,

$$f_{T_{DSA}}(t) = \sum_{i=2N_{BC}+1}^{\infty} p_{DSA,i} f_{T_i}(t) + (1 - \mathbb{P}_{DSA}) \delta(t - \infty), \quad (3.15)$$

where $\delta(t)$ is the Dirac delta function.

Proposition 3.7. The PDF $f_{T_{DSA}}$ has an analytic expression:

$$f_{T_{DSA}}(t) = \frac{p_A \lambda_T e^{-\lambda_T t} (p_A p_H (\lambda_T t)^2)^{N_{BC}}}{(2N_{BC})!} \cdot \sum_{j=N_{BC}}^{j=2N_{BC}} \binom{j-1}{N_{BC}-1} {}_2F_3(\mathbf{a}; \mathbf{b}; p_A p_H (\lambda_T t)^2) + \frac{e^{-\lambda_T t} (p_H \lambda_T t)^{N_{BC}}}{t (N_{BC}-1)!} \left(e^{p_A \lambda_T t} - \sum_{i=0}^{N_{BC}} \frac{(p_A \lambda_T t)^i}{i!} \right) + (1 - \mathbb{P}_{DSA}) \delta(t - \infty), \quad (3.16)$$

where ${}_pF_q(\mathbf{a}; \mathbf{b}; x)$ is the generalized hypergeometric function (See Appendix 3.E for definition) with the parameter vectors

$$\mathbf{a} = \begin{bmatrix} N_{BC} + 1 - j/2 \\ N_{BC} + 1/2 - j/2 \end{bmatrix} \quad (3.17)$$

and

$$\mathbf{b} = \begin{bmatrix} 2N_{BC} + 2 - j \\ N_{BC} + 1 \\ N_{BC} + 1/2 \end{bmatrix}. \quad (3.18)$$

Proof. See Appendix 3.C.

By Definition 3.2, the probability \mathbb{P}_{AS} that a DS attack $DS(p_A, t_{cut}; N_{BC})$ succeeds equals

$$\mathbb{P}_{AS}(t_{cut}) = \Pr(T_{DSA} < t_{cut}). \quad (3.19)$$

Note that for a special case of $t_{cut} = \infty$, $\mathbb{P}_{AS}(t_{cut}) = \mathbb{P}_{DSA}$, which coincides with the result in Rosenfeld [27].

It will be shown to be convenient to define the attack success time T_{AS} of a DS attack as

$$T_{AS} := \begin{cases} T_{DSA}, & \text{if } T_{DSA} < t_{cut}, \\ \text{not defined}, & \text{otherwise.} \end{cases} \quad (3.20)$$

A random variable for $T_{DSA} > t_{cut}$ does not need to be defined since it is not useful. The PDF $f_{T_{AS}}$ of T_{AS} is just a truncated version of $f_{T_{DSA}}(t)$ in (3.16) for $0 < t < t_{cut}$ with a scaling factor of \mathbb{P}_{AS}^{-1} . Formally, the PDF $f_{T_{AS}}(t)$ equals

$$f_{T_{AS}}(t) = \begin{cases} \frac{f_{T_{DSA}}(t)}{\mathbb{P}_{AS}}, & \text{for } 0 \leq t < t_{cut}, \\ 0, & \text{for } t \geq t_{cut}. \end{cases} \quad (3.21)$$

The expectation of attack success time is computed as

$$\mathbb{E}_{T_{AS}}(t_{cut}) = \frac{\int_0^{t_{cut}} t f_{T_{DSA}}(t) dt}{\mathbb{P}_{AS}(t_{cut})}. \quad (3.22)$$

The following Proposition 3.8 gives an explicit formula of $\mathbb{E}_{T_{AS}}$ for the special case when $t_{cut} = \infty$.

Proposition 3.8. Let $p_M := \max(p_A, p_H)$, $p_m := \min(p_A, p_H)$. If $t_{cut} = \infty$, the expectation $\mathbb{E}_{T_{AS}}(t_{cut})$ has a closed-form expression:

$$\lim_{t_{cut} \rightarrow \infty} \mathbb{E}_{T_{AS}}(t_{cut}) = \frac{\lambda_T^{-1} \left(\sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} Z_j + \frac{N_{BC}}{p_H} \right)}{\mathbb{P}_{DSA}}, \quad (3.23)$$

where

$$Z_j := p_A p_m^{N_{BC}} p_M^{-(N_{BC}-j+1)} \left(\frac{2N_{BC} - 2jp_m + 1}{p_M - p_m} \right) - jp_A^{-(N_{BC}-j)} p_H^{N_{BC}}. \quad (3.24)$$

Proof: See Appendix 3.B.

3.4. Profitable DS Attacks

The previous probabilistic analyses in [20] and [27] show that the success of DS attacks is not guaranteed when $p_A < 0.5$. However, DS attacks with $p_A < 0.5$ can be vigorously pursued as long as they bring profit.

We analyze the profitability of DS attacks and to this end, we define a profit function P of a DS attack $DS(C, p_A, t_{cut}; N_{BC})$, where C is the value of a fraudulent transaction, in terms of revenue and operating expense (OPEX) of the computing power.

The OPEX X (e.g. the rental fee for the computing power) and the block mining reward R tend to increase with respect to λ_A and the time t consumed during the attack. Thus, X and R are expressed as functions of λ_A and t , and they can be any increasing

function; e.g., linear, exponential, or logarithm. We define X and R , respectively, as follows:

$$X(\lambda_A, t) := \gamma \lambda_A t (\log_{x_1} x_2)^{\lambda_A} (\log_{x_3} x_4)^t \quad (3.25)$$

for real constants $\gamma > 0$, $x_1, x_2 > 1$, and $x_3, x_4 > 1$, and

$$R(\lambda_A, t) := \beta \lambda_A t (\log_{r_1} r_2)^{\lambda_A} (\log_{r_3} r_4)^t \quad (3.26)$$

for real constants $\beta > 0$, $r_1, r_2 > 1$, and $r_3, r_4 > 1$. By setting the constants, one can transform the the cost and reward functions in (3.25) and (3.26) into a form of linear, exponential, or logarithm function depending on the real-world environment. We denote the ratio of γ and β by

$$\mu := \beta \gamma^{-1}. \quad (3.27)$$

With regards to P , if an attack succeeds, the revenue comes from C , as it is double-spent, and R for the number of blocks mined during the time duration T_{AS} , i.e., $R(\lambda_A, T_{AS})$. In this case, the cost is the OPEX for the time duration T_{AS} , i.e., $X(\lambda_A, T_{AS})$. If the attack fails, the cost is the OPEX $X(\lambda_A, t_{cut})$ for the time duration t_{cut} , and there is no revenue. Hence, for a DS attack $DS(C, p_A, t_{cut}; N_{BC})$, we define P as follow,

$$P := \begin{cases} C + R(\lambda_A, T_{AS}) - X(\lambda_A, T_{AS}), & \text{if } T_{DSA} < t_{cut}, \\ -X(\lambda_A, t_{cut}), & \text{otherwise.} \end{cases} \quad (3.28)$$

Subsequently, the expected profit function is

$$\begin{aligned} \mathbb{E}_P &= \mathbb{P}_{AS}(t_{cut}) \cdot (C + \mathbb{E}[R(\lambda_A, T_{AS})] - \mathbb{E}[X(\lambda_A, T_{AS})]) - (1 - \mathbb{P}_{AS}(t_{cut})) X(\lambda_A, t_{cut}) \\ &= \mathbb{P}_{AS}(t_{cut}) \cdot (C + \mathbb{E}[R(\lambda_A, T_{AS})]) - \mathbb{E}_X, \end{aligned} \quad (3.29)$$

where \mathbb{E}_X is the expected OPEX defined as

$$\mathbb{E}_X := \mathbb{P}_{AS}(t_{cut}) \mathbb{E}[X(\lambda_A, T_{AS})] + (1 - \mathbb{P}_{AS}(t_{cut})) X(\lambda_A, t_{cut}). \quad (3.30)$$

Definition 3.9. A DS attack $DS(C, p_A, t_{cut}; N_{BC})$ is said to be profitable if and only if the expected profit $\mathbb{E}_p > 0$, where \mathbb{E}_p is defined in (3.29).

The key factor in determining the profitability of DS attacks is the value C of the fraudulent transaction. Thus, attackers would be interested in the minimum value required for profitable DS attacks [78]. Definition 3.9 implies that a DS attack $DS(C, p_A, t_{cut}; N_{BC})$ is profitable if and only if $C > C_{Req.}$, where the required value of target transaction $C_{Req.}$ is

$$C_{Req.} = \frac{\mathbb{E}_X}{\mathbb{P}_{AS}} - \mathbb{E}[R(\lambda_A, T_{AS})]. \quad (3.31)$$

The following results in Theorem 3.10 and Theorem 3.11 focus on the case where both $X(\lambda_A, t)$ and $R(\lambda_A, t)$ are linearly increasing functions of λ_A and t .

Theorem 3.10. Suppose $x_1 = x_2$ and $x_3 = x_4$ in (3.25), and $r_1 = r_2$ and $r_3 = r_4$ in (3.26). Then, a DS attack $DS(C, p_A, t_{cut}; N_{BC})$ for any $p_A \in (0, 1)$ and for any $t_{cut} \in (0, \infty]$ is profitable if and only if $C > C_{Req.}$, where

$$C_{Req.} = \frac{(1 - \mathbb{P}_{AS}(t_{cut}))}{\mathbb{P}_{AS}(t_{cut})} \gamma \lambda_A t_{cut} - (\mu - 1) \gamma \lambda_A \mathbb{E}_{T_{AS}}(t_{cut}). \quad (3.32)$$

Proof. Substituting $x_1 = x_2$, $x_3 = x_4$, $r_1 = r_2$, and $r_3 = r_4$ into (3.31) results in (3.32). ■

Theorem 3.10 shows that not only superior attackers with $p_A \in (0.5, 1)$ but also inferior attackers with $p_A \in (0, 0.5)$ are able to expect profitable DS attacks once a high enough value C greater than $C_{Req.}$ of the target transaction is designed. The condition $C_{Req.}$ in (3.32) can be pre-computed before carrying out an attack, as it stochastically estimates the

future expected cost, for a given position $p_A \in (0,1)$ and a cut-time t_{cut} of an attacker, and a given set of network environment parameters γ and β .

Table 3.1 and Table 3.2 list the resources including C_{Req} , \mathbb{E}_X , and $\mathbb{E}_{T_{AS}}$ required for profitable DS attacks respectively using $p_A = 0.35$ and $p_A = 0.4$, when $t_{cut} = cN_{BC}\lambda_H^{-1}$ with $c = 4$. Note that the expectation of the time spent for the block confirmation equals $N_{BC}\lambda_H^{-1}$, and we let t_{cut} linear to it. In other words, as normal traders wait for $N_{BC}\lambda_H^{-1}$ seconds on the average, attackers shall be tolerable as well and wait for the same scale of time duration. Note that the \mathbb{P}_{AS} for $N_{BC} = 1$ is smaller than that for $N_{BC} = 3$ due to not long enough t_{cut} . We scaled the results by parameters λ_H and γ , which we will explain how to obtain from internet in the next subsection.

The following Theorem 3.11 is for the inferior attackers with $p_A \in (0,0.5)$ and shows the importance of setting a finite t_{cut} .

Theorem 3.11. Suppose $x_1 = x_2$ and $x_3 = x_4$ in (3.25), and $r_1 = r_2$ and $r_3 = r_4$ in (3.26). Then, a DS attack $DS(C, p_A, t_{cut}; N_{BC})$ with $p_A \in (0,0.5)$ is profitable only if $t_{cut} < \infty$.

Proof: For any $p_A \in (0,0.5)$, it always holds that $\mathbb{P}_{AS} < 1$. In this case, if $t_{cut} \rightarrow \infty$ then $C_{Req} \rightarrow \infty$ from (3.32); i.e., infinite value C of fraudulent transaction is required for a DS attack $DS(C, p_A, t_{cut}; N_{BC})$ to be profitable. Thus, for a DS attack with $p_A \in (0,0.5)$ to be profitable, a finite cut-time $t_{cut} < \infty$ must be set. ■

Theorem 3.11 shows that for $p_A \in (0,0.5)$, setting $t_{cut} = \infty$ is expected to incur infinite deficit. On the contrary, for $p_A \in (0.5,1)$, what we have numerically checked out but omitted due to space limitation is the result that \mathbb{E}_p is an increasing function of t_{cut} ; i.e.,

setting $t_{cut} = \infty$ is the optimal choice in the superior attack regime. Applying $p_A \in (0.5, 1)$ and $t_{cut} = \infty$ into (3.32) leads to $\mathbb{P}_{AS} = 1$, and thus $C_{\text{Req.}}$ turns into

$$C_{\text{Req.}} = -(\mu - 1)\gamma\lambda_A \mathbb{E}_{T_{AS}}, \quad (3.33)$$

where a closed-form expression of $\mathbb{E}_{T_{AS}}$ is given in Proposition 3.8. In this case, if $\beta > \gamma$; i.e., $\mu > 1$, DS attacks are always profitable regardless of C . According to nicehash.com, most networks maintain $\beta > \gamma$ by the economic equilibrium. As the result, in addition to the results in [20] and [27] that DS attacks with $p_A \in (0.5, 1)$ guarantee probabilistic success, we show that such attacks guarantee economic gain as well.

Block confirmation number (N_{BC})		1	3	5	7	9
Attack success probability (\mathbb{P}_{AS})		0.315	0.279	0.218	0.170	0.132
Expected attack success time ($\mathbb{E}_{T_{AS}}$)	Scaled by λ_H^{-1}	2.004	5.518	8.681	11.694	14.607
Expected OPEX (\mathbb{E}_X)	Scaled by γ	1.815	5.487	9.440	13.588	17.859
Required value of target transaction ($C_{Suf.}$)		$1.079 \cdot (1 - \mu) + 4.680$	$2.971 \cdot (1 - \mu) + 16.68$	$4.675 \cdot (1 - \mu) + 38.62$	$6.297 \cdot (1 - \mu) + 73.84$	$7.866 \cdot (1 - \mu) + 127.00$

Table 3.1. Numerical computations of required resources for profitable DS attacks with $p_A = 0.35$ when $t_{cut} = cN_{BC}\lambda_H^{-1}$ with $c = 4$.

Block confirmation number (N_{BC})		1	3	5	7	9
Attack success probability (\mathbb{P}_{AS})		0.411	0.419	0.376	0.334	0.297
Expected attack success time ($\mathbb{E}_{T_{AS}}$)	Scaled by λ_H^{-1}	1.953	5.338	8.434	11.418	14.325
Expected OPEX (\mathbb{E}_X)	Scaled by γ	2.106	6.139	10.436	14.977	19.716
Required value of target transaction ($C_{Suf.}$)		$1.302 \cdot (1 - \mu) + 3.819$	$3.559 \cdot (1 - \mu) + 11.10$	$5.622 \cdot (1 - \mu) + 22.15$	$7.612 \cdot (1 - \mu) + 37.25$	$9.550 \cdot (1 - \mu) + 56.96$

Table 3.2. Numerical computations of required resources for profitable DS attacks with $p_A = 0.4$ when $t_{cut} = cN_{BC}\lambda_H^{-1}$ with $c = 4$.

3.5. Practical Example of Profitable DS Attacks against BitcoinCash

We analyze resources required for profitable DS attacks against BitcoinCash network. The resources include the computing power proportion p_A , expected OPEX \mathbb{E}_X , expected attack success time $\mathbb{E}_{T_{AS}}$, and the required value of fraudulent transaction C_{Req} .

To this end, we first recall the parameters involved in block mining reward R and the OPEX X . The parameters used in (3.25) and (3.26) are assumed to $x_1 = x_2$, $x_3 = x_4$, $r_1 = r_2$, and $r_3 = r_4$ which lead to linear functions $X(\lambda_A, t)$ and $R(\lambda_A, t)$ with respect to λ_A and t . There are three more parameters: γ , β , and λ_H^{-1} . From (3.25) and (3.26), the parameter γ is the expected cost for generating one block; and the parameter β is the reward per generating a block. Parameter λ_H^{-1} is the average block generation time of the honest chain. All the parameters are different for each blockchain network.

In BitcoinCash, the reward β per block mining was 12.5 BCH (without transaction fees), which is around $\beta = 0.44$ BTC per block mining (as of 26th Feb. 2020). The average block generation time was fixed at $\lambda_H^{-1} = 600$ seconds.

The parameter γ is obtainable from nicehash.com. BitcoinCash uses the SHA-256 cryptographic puzzle for which the unit of computation is hash. As of 26th Feb. 2020, the rental fee for 1-peta (P) hashes per second for a day was around 0.017 BTC, which was around $1.97 \cdot 10^{-7}$ BTC per second. In other words, the rental fee was approximately $1.97 \cdot 10^{-22}$ BTC per the computing of a hash. Referring to BTC.com, the network's computing speed is 3.57-exa (E) hashes per second; i.e., $3.57E \cdot 600 = 2142E$ hashes are needed to generate one block on the average. As the result, the parameter γ is obtained as

$$\begin{aligned} \gamma &= 1.97 \cdot 10^{-22} \text{ [BTC/hash]} \times 2142E \text{ [hashes/block mining]} \\ &\approx 0.422 \text{ [BTC/block mining]}. \end{aligned} \tag{3.34}$$

Note that it holds $\beta > \gamma$. From (3.33), this relationship makes DS attack $\text{DS}(C, p_A, t_{cut}; N_{BC})$ with $p_A > 0.5$ and $t_{cut} = \infty$ always profitable regardless of the value C of target transaction.

In case of DS attacks with $p_A < 0.5$, the cut-time t_{cut} must be determined as a finite value for profitable DS attacks by Theorem 3.11. We set $t_{cut} = cN_{BC}\lambda_H^{-1} = 12000$ seconds with $c = 4$ and $p_A = 0.35$. We compute the resources required for profitable DS attacks against BitcoinCash when $N_{BC} = 5$. Results are obtainable from the values in Table 3.1 and Table 3.2 by multiplying the scaling parameters $\gamma = 0.422$ and $\lambda_H^{-1} = 600$ and by substituting $\mu = \beta\gamma^{-1} = 1.04$ and $c = 4$.

As the results, we obtain $\mathbb{P}_{AS} \approx 0.218$, $\mathbb{E}_{T_{AS}} \approx 5200$ seconds, $\mathbb{E}_X \approx 3.98$ BTC, and $C_{Req.} \approx 16.22$ BTC. One can compute expected running time; i.e., the expected time spent for a single DS attack attempt as $\mathbb{P}_{AS}\mathbb{E}_{T_{AS}} + (1 - \mathbb{P}_{AS})t_{cut}$, which is around 2 hours and 55 minutes. That is to say, attackers can repeatedly perform n number of attacks every 2 hours and 55 minutes on the average. With the value C of target transaction, by the strong law of large numbers, the multiple attack attempts will return net profit $n\mathbb{P}_{AS}(t_{cut}) \cdot (C - C_{Req.})$ as $n \rightarrow \infty$ with probability 1.

3.6. Related Works

By Nakamoto [20] and Rosenfeld [27], the probabilities have been studied that a DS attack will ever succeed when there is no time limit, i.e., the cut-time is set to $t_{cut} = \infty$. Both of them applied PCPs to model the growth of chains $H(t)$ and $A(t)$. On one hand, the main difference between them was in probability calculations of the block confirmation process $\mathcal{G}^{(1)}$ in Definition 3.1. Rosenfeld applied the PCPs to both $H(t)$ and $A(t)$, whereas Nakamoto assumed the time spent for $H(t) \geq N_{BC}$ deterministic to simplify the calculation. On the other hand, they both used the gambler's ruin approach to obtain the

asymptotical behavior of S_i as $i \rightarrow \infty$ by manipulating the recurrence relationship between two adjacent states. Namely, their results are based on an assumption that an indefinite number of attack chances are given [65].

On the contrary, we introduce the cut-time t_{cut} which generalizes analytical framework to the more interesting finite attack time and inferior attacker regime. By setting t_{cut} infinite, the same result \mathbb{P}_{DSA} was obtained in [27] as well. By setting a finite t_{cut} , our results shall be useful when attack chances are limited due to limited amount of resources such as time and cost. In addition, we show in Theorem 3.11 that DS attacks with $p_A < 0.5$ must set a finite t_{cut} in order to expect a non-negative profit. It shall be noted that there has been no intermediate result like $p_{DSA,i}$ in Lemma 3.5. We use Lemma 3.5 to derive the novel results.

Rosenfeld [27] and Bissias et al. [66] have analyzed the profitability of DS attacks. But they put additional assumptions on the attack scenario to simplify the calculation of the attack time. Specifically, Rosenfeld assumed the attack time to be a constant. Bissias et al. assumed that the attack stops if either the normal peers or the attacker achieves the block confirmation first. On the contrary, in our model, an attack can be continued for a random attack time as long as it brings profit, even if the normal peers achieve the block confirmation before the attacker does.

In Zaghloul et al. [67], the profit of DS attack has been analyzed. Interestingly, they have discussed the need of cut-time for DS attacks with $p_A < 0.5$, which is theoretically proven in this chapter in Theorem 3.11. They also calculated the profit of DS attacks with a finite time-limit (see Section IV-C in [67]), but their calculation was not as precise as ours in three points:

First, the probability of attack success within a finite time-limit, i.e., $\mathbb{P}_{AS}(t_{cut})$ in (3.19) was never considered, which requires the distribution of the DS achieving time, i.e., T_{DSA} given in Proposition 3.7. Instead, their calculation used \mathbb{P}_{DSA} referring to the result in

Rosenfeld [66]. This contradicts their time-limited attack scenario, since \mathbb{P}_{DSA} was resulted from the assumption of infinite time-limit.

Second, they approximated costs and revenues of DS attack spent within a time-limit. Estimation of the costs and revenues requires estimations of the numbers of blocks respectively mined by honest nodes and attackers within a time-limit, but those were assumed to be constant. This was due to the absence of the time analysis we provide in Proposition 3.7.

Third, they assumed the average block generation rates λ_H , λ_A respectively by honest miners and by attackers are always the same. Since, the proportions p_H , p_A of computing power occupied by the two groups can be quite different in general, such a result is not very useful. We agree to their assumption that most blockchains control the difficulty of block mining puzzle to keep the average speed of block generation constant, and thus λ_H can be considered as a constant. But λ_A should be left as a varying quantity by p_A . The fact is that the computing power invested by attacker cannot be monitored by the honest network and thus it cannot be reflected in the difficulty control routine.

Budish [68] conducted simulations on the profitability of DS attacks only in the cases of $p_A > 0.5$. Under the cases, a condition on the value of the target transaction that makes DS attacks not profitable has been given based on the simulations. We give theoretical and numerically-calculable results for any $p_A \in (0,1)$, which do not require massive simulations.

Gervais et al. [69] and Sompolinsky et al. [65] have used a Markov decision process (MDP) to analyze profits from DS attacks. These works differ from our contributions in the following regards:

First, they did not follow the DS attacks scenario considered by Nakamoto [20] and Rosenfeld [27]. Instead, the scenario in [65] was a special case of the pre-mining strategy which was introduced in [70] and [71]. We show that the success of DS attack under this scenario is even more difficult to occur than the success of the DS attack under the

scenario of Nakamoto and Rosenfeld (see Appendix 3.D for details). Also, the attack scenario in [69] went even further by modifying the condition $\mathcal{G}^{(1)}$ for block confirmation in Definition 3.1. Specifically, under $\mathcal{G}^{(1)}$, it is required for the honest chain to have added N_{BC} blocks, while under their condition, it was the fraudulent chain to do so (see Section 3 of [69]). Thus, it was not ensured that the potential victim has shipped the goods or service, and an attack success did not guarantee for the attacker to obtain the benefit of attacking.

Second, one important new advance in this chapter is the derivation of the time analysis $f_{T_{AS}}$ given in Proposition 3.7. When one uses the MDP framework, one can obtain similar information such as the estimations for the attack success time $\mathbb{E}_{T_{AS}}$, the future profit P that an attacker will earn in the end, and the minimum value of target transaction C_{Req} . But using MDP, to make such estimations, would have required extensive Monte Carlo simulations. Using our mathematical results, such estimations can be obtained without Monte Carlo simulations.

In addition, we believe that our mathematical results can be utilized in the MDP frameworks to improve the reliability of analyses. Conventionally, a rational user of an MDP will make a decision at every state whether to stop or to continue the process by comparing the rewards that will be incurred in the future by his/her decision. The rewards for stop actions are clear because such actions are either an attack success or a give-up. The reward for the continue action is complex because it needs to consider all the actions in all future possible states as well. In [65] and [69], the rewards for the continue action were over-simplified as they were evaluated only for the very next state and did not include the estimation of the profits in further future actions. To improve the reliability, the PDF $f_{T_{AS}}$ in Proposition 3.7 can be used at any intermediate Markov state to estimate the future profits. Specifically, the conditional expectation of the time left for an attack success T_{AS} given $T_{AS} > \tau$ can be calculated using $f_{T_{AS}}$, where τ is the observable time elapsed for reaching the current state. Once the time left is estimated, the estimation of future profits can be updated by substituting it into (3.29). That is to say, at each state, the estimation of profits can be updated and used as the rewards resulting from the continue action.

Goffard [72] and Karame et al. [73] have derived the PDFs of attack success time, but none of their DS attack scenarios matched with ours in Definition 3.1. In [72], Goffard derived the PDF of catch-up time spent for the fraudulent chain to catch up with the honest chain given that the length of honest chain is initially ahead by several blocks. The author used counting processes such as order statistic point process and renewal process which are more general than PCP, but there was no analytic result similar to what is given in Proposition 3.7. In [73], Karame et al. derived the PDF of the first attack success time under a fast-payment model which fixed $N_{BC} = 0$. To sum up, the attack success time in neither analysis included the time spent for achieving the first condition $\mathcal{G}^{(1)}$: the block confirmation should be realized.

3.7. Checking Formulas by Monte Carlo Experiments

To check the correctness of our mathematical result in Proposition 3.7, we conduct Monte Carlo experiments with a simulation of DS attack. Proposition 3.7 gives a probability distribution of the time spent for a success of DS attack. We compare the experimental results with two formulas (3.19) and (3.21). Formula (3.19) gives the probability that a DS attack succeeds within a cut-time. Formula (3.21) is a truncated version of Proposition 3.7, where the time domain is truncated by a cut-time.

A pseudo code of simulation is summarized in Table 3.3. This code aims to simulate the stochastic behavior of DS attacks modeled in sub-section 3.2.2. We uploaded a MATLAB implementation of this simulation on web-site². The simulation takes inputs such as block generation rates λ_A and λ_H of a fraudulent chain and a honest chain respectively, a block confirmation number N_{BC} , and a cut-time t_{cut} . The input λ_A can be replaced by the computational proportion p_A of attacker. The simulation results in two outputs: One is an estimation $\hat{\mathbb{P}}_{AS}$ of the DS attack success probability within t_{cut} , and the other is a

² <https://codeocean.com/capsule/2308305/tree>

sample vector $\hat{\mathbf{f}}_{T_{AS}}$ of the time spent for a DS attack success within t_{cut} . For each combination of input parameters, we conducted the experiments for $N=100000$ times. We fixed $\lambda_H=1/600$ blocks per second. For given N_{BC} , we set $t_{cut}=4N_{BC}\lambda_H^{-1}$, which is a multiple of the expected time spent for the completion of a block confirmation, i.e., $N_{BC}\lambda_H^{-1}$.

Table 3.4 compares the probabilities of successful DS attacks. We varied block confirmation number $N_{BC} \in \{3, 5, 7\}$ and attacker's computational proportion $p_A \in \{0.25, 0.3, 0.35, 0.4, 0.45\}$. The values on the columns labeled "Calculation" were obtained from calculations of \mathbb{P}_{AS} in (3.19). The values on the columns labeled "Experiment" were the estimations $\hat{\mathbb{P}}_{AS}$ obtained from Monte Carlo tests using Table 3.3. The results show $\hat{\mathbb{P}}_{AS}$ well estimate \mathbb{P}_{AS} with negligible errors. That is, the probability calculation in (3.19) has been verified by the Monte Carlo experiments.

Figure 3.2 compares of the probability distributions of the time spent for a success of DS attack. In subplot (a), we set attacker's computational proportion $p_A=0.25$, and in subplot (b), we set $p_A=0.45$. The bars on both subplots are the histograms of $\hat{\mathbf{f}}_{T_{AS}}$ obtained from the Monte Carlo experiments in Table 3.3. Out of $N=100000$ trials, we obtained 4584 samples for subplot (a) and 56951 samples for subplot (b). The differences in the numbers of samples came from the differences of p_A and the differences of the success probability of DS attacks. We can obtain a sample of time spent for an attack success only if an attack succeeds. The histograms were compared with the red curves on both subplots, which are scaled versions of the calculation of equation (3.21). The results show the red curves from the calculations well fit to the shapes of histograms. As the results, the probability distribution in (3.21) has been verified by the Monte Carlo experiments.

Algorithm: Pseudocode of Monte Carlo experiments for double-spending attacks

Input: Double-spending attack parameters λ_A , λ_H , N_{BC} , and t_{cut} and the number of experiments N .

Output: An estimation $\hat{\mathbb{P}}_{AS}$ of (3.19) and a histogram $\hat{\mathbf{f}}_{T_{AS}}$ for $f_{T_{AS}}(t)$ in (3.21).

- 1: Define a function $\text{exp}(\lambda)$ that returns a sample in \mathbb{R}^+ from an exponential distribution with the rate parameter $\lambda \in \mathbb{R}^+$
- 2: Define a function $\text{last}(\mathbf{t}, n)$ for an array \mathbf{t} of entries in \mathbb{R}^+ that returns the n -th entry from the last of \mathbf{t} (if \mathbf{t} is empty, it returns 0, and if n is omitted, $n=1$)
- 3: Define a function $\text{hist}(\mathbf{t})$ for an array \mathbf{t} of entries in \mathbb{R}^+ that returns a histogram of \mathbf{t}
- 4: Allocate an empty array \mathbf{t}_{DS} of entries in \mathbb{R}^+
- 5: **for** $n \leftarrow 1$ **to** N
- 6: Allocate empty arrays \mathbf{t}_A and \mathbf{t}_H of entries in \mathbb{R}^+
- 7: **while** 1
- 8: Concatenate $\mathbf{t}_A \leftarrow [\mathbf{t}_A \quad \text{last}(\mathbf{t}_A) + \text{exp}(\lambda_A)]$
- 9: Concatenate $\mathbf{t}_H \leftarrow [\mathbf{t}_H \quad \text{last}(\mathbf{t}_H) + \text{exp}(\lambda_H)]$
- 10: **if** $\text{last}(\mathbf{t}_A) \geq t_{cut}$ **then**
- 11: **break**
- 12: **end if**
- 13: **if** $|\mathbf{t}_H| > N_{BC}$ **and** $\text{last}(\mathbf{t}_H) > \text{last}(\mathbf{t}_A)$ **then**
- 14: **if** $|\mathbf{t}_H| = N_{BC} + 1$ **then**
- 15: $t_{DS} \leftarrow \text{last}(\mathbf{t}_H, 2)$
- 16: **else**
- 17: $t_{DS} \leftarrow \text{last}(\mathbf{t}_A)$
- 18: **end if**
- 19: **if** $t_{DS} < t_{cut}$ **then**
- 20: Concatenate $\mathbf{t}_{DS} \leftarrow [\mathbf{t}_{DS} \quad t_{DS}]$
- 21: **break**
- 22: **end if**
- 23: **end if**
- 24: **end while**

```

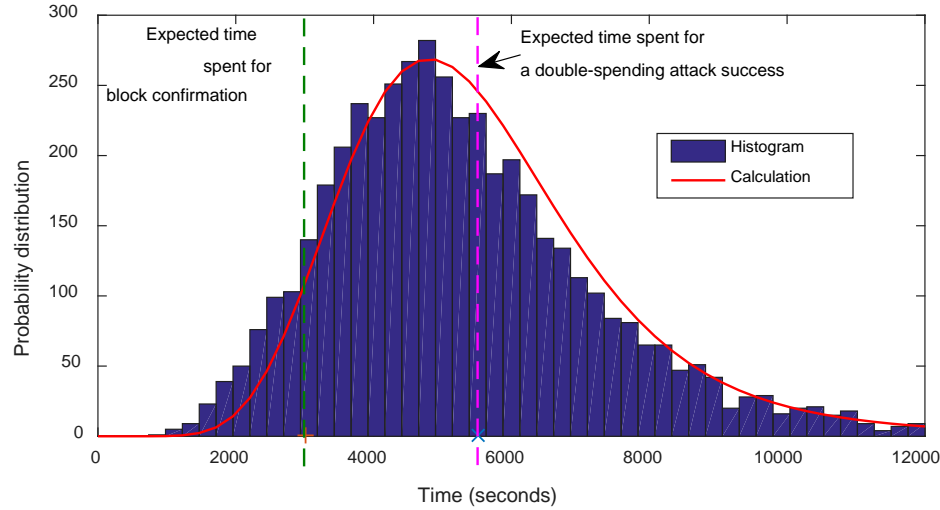
25: end for
26:  $\hat{\mathbb{P}}_{AS} \leftarrow \frac{|\mathbf{t}_{DS}|}{N}$ 
27:  $\hat{\mathbf{f}}_{T_{AS}} \leftarrow hist(\mathbf{t}_{DS})$ 
28: return  $\hat{\mathbb{P}}_{AS}$  and  $\hat{\mathbf{f}}_{T_{AS}}$ 

```

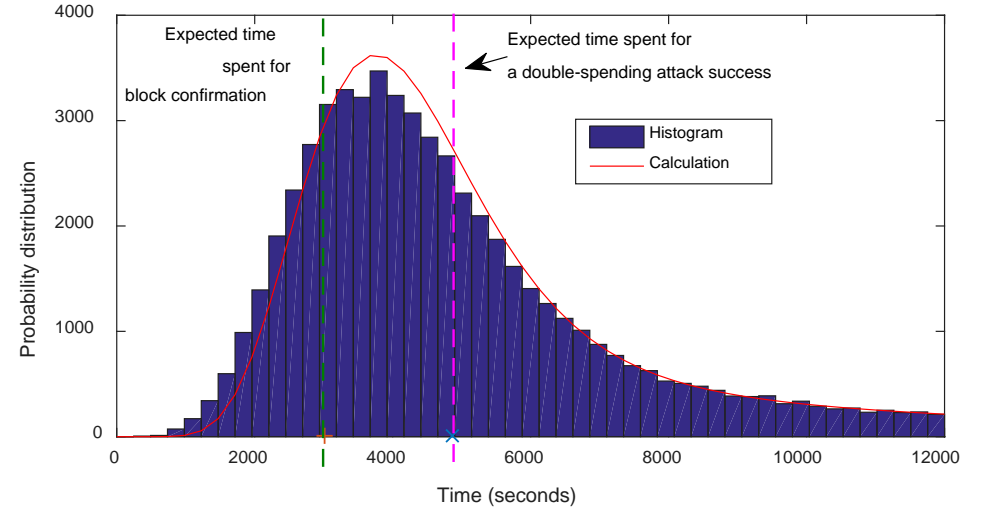
Table 3.3 A pseudo-code to simulate the stochastic behavior of double-spending attacks modeled in sub-section 3.2.2.

Probabilities	$N_{BC} = 3$		$N_{BC} = 5$		$N_{BC} = 7$	
	Calcula- tion	Experi- ment	Calcula- tion	Experi- ment	Calcula- tion	Experi- ment
$p_A = 0.25$	0.0896	0.0895	0.0451	0.0458	0.0230	0.0230
$p_A = 0.3$	0.1684	0.1681	0.1089	0.1107	0.0706	0.0713
$p_A = 0.35$	0.2793	0.2788	0.2180	0.2189	0.1696	0.1690
$p_A = 0.4$	0.4189	0.4208	0.3758	0.3775	0.3338	0.3313
$p_A = 0.45$	0.5765	0.5768	0.5679	0.5695	0.5516	0.5513

Table 3.4 Comparisons of the probabilities of successful double-spending attacks for given block confirmation number N_{BC} and attacker’s computational proportion p_A when cut-time is set to $4N_{BC}\lambda_H^{-1}$ for $\lambda_H^{-1} = 600$ seconds. The values on the columns labeled “Calculation” are obtained from the calculation of equation (3.19). The values on the columns labeled “Experiment” are obtained from Monte Carlo tests using Table 3.3.



(a) $p_A = 0.25$



(b) $p_A = 0.45$

Figure 3.2. Comparisons of the probability distributions of the time spent for a success of double-spending attack when attacker's computational proportion is (a) $p_A = 0.25$ and (b) $p_A = 0.45$. Block confirmation number and cut-time are set to $N_{BC} = 5$ and $t_{cut} = 4N_{BC}\lambda_H^{-1}$ for $\lambda_H^{-1} = 600$ seconds, respectively. The bars on both subplots are histograms of $\hat{\mathbf{f}}_{T_{AS}}$ obtained from Monte Carlo tests in Table 3.3. The red curves on both subplots are the calculation of equation (3.21).

3.8. Conclusions

We showed that DS attacks using 50% or a less proportion of computing power can be profitable and thus quite threatening. We provided how much quantitative resources are required to make a profitable DS attack. We derive the PDF of attack success time which enables us to figure out the operating time and the expense of mining rigs. We verified our mathematical results using Monte Carlo experiments. We provided MATLAB codes on the website³ for the numerical evaluation of expected profit function in (3.29) and for the Monte Carlo experiments. We also listed an example of the minimum resources required for a profitable DS attack, which is applicable to any blockchain networks by substituting the network parameters γ , β , and λ_H . We also showed a more specific example of the required resources against BitcoinCash network.

Our results quantitatively guide how to set a block confirmation number for a safe transaction. The less the block confirmation number is, the less the minimum resource is required for a profitable attack. A solution can be utilized by the network developers to discourage such an attack. On the one hand, given a block confirmation number, we can have the value of any transaction to be set below the required value of making a profitable attack in a given network. On the other hand, given the value of transaction, the network can provide a service to inform the payee with the least block confirmation number that leads to negative DS attack profit.

³ <https://codeocean.com/capsule/2308305/tree>

Appendices

Appendix 3.A Proof of Lemma 3.5

For a given sample ω and a given index i , we seek an intermediate index j and the corresponding set $\mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}$ to which ω belongs, i.e., $\omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}$. If such a set exists, by the mutual exclusiveness of $\mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}$ for integers j , it is unique. Thus, we can write the probability $p_{DSA,i}$ as follow,

$$\begin{aligned} p_{DSA,i} &= \Pr\left(\exists j \in \mathbb{N}: \omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}\right) \\ &= \sum_{j=N_{BC}}^{\infty} \Pr\left(\omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}\right). \end{aligned} \quad (3.35)$$

Note that $\mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)} = \emptyset$ for $i \leq 2N_{BC}$, since the minimum number of states for an successful attack is $2N_{BC} + 1$; N_{BC} number of $+1$'s state transitions for the block confirmation; and $N_{BC} + 1$ number of -1 's state transitions for the success of PoW competition. Thus, $p_{DSA,i} = 0$ for $i \leq 2N_{BC}$.

We further explore $\mathcal{D}_j^{(1)}$ and $\mathcal{D}_{i,j}^{(2)}$. We divide the domain of state index j in (3.35) into two exclusive domains; one is $j \leq 2N_{BC}$; and the other is $j > 2N_{BC}$. First, for $j \leq 2N_{BC}$, two sets $\mathcal{D}_j^{(1)}$ and $\mathcal{D}_{i,j}^{(2)}$ are independent, since their requirements on the state transitions are focusing on disjoint indices of state by their definitions. Formally, $\Pr\left(\omega \in \mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)}\right) = \Pr\left(\omega \in \mathcal{D}_j^{(1)}\right)\Pr\left(\omega \in \mathcal{D}_{i,j}^{(2)}\right)$. Second, we explore the domain $j > 2N_{BC}$. By the definition of $\mathcal{D}_j^{(1)}$, all $\omega \in \mathcal{D}_j^{(1)}$ satisfy $S_j = \sum_{k=1}^j \Delta_k = 2N_{BC} - j$. Thus, for every $j > 2N_{BC}$, S_j is already negative, which implies all $\omega \in \mathcal{D}_j^{(1)}$ satisfy both $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ at state j . The set $\mathcal{D}_{i,j}^{(2)} = \emptyset$ for $j > 2N_{BC}$ and $j < i$, since the state $S_j = 2N_{BC} - j$ contradicts one requirement of $\mathcal{D}_{i,j}^{(2)}$: the interim transitions between the

states j and i should be non-negative. For $j > 2N_{BC}$ and $j = i$, let us set $\mathcal{D}_{i,j}^{(2)} = \Omega_\infty$, since there is no interim state to apply the requirement to. To sum up, $\mathcal{D}_j^{(1)} \cap \mathcal{D}_{i,j}^{(2)} = \mathcal{D}_i^{(1)}$ for $j > 2N_{BC}$ and $i = j$, and $\mathcal{D}_j^{(1)} \cap (\mathcal{D}_{i,j}^{(2)}) = \emptyset$ for $j > 2N_{BC}$ and $i > j$. Subsequently, (3.35) is computed as

$$p_{DSA,i} = \sum_{j=N_{BC}}^{2N_{BC}} \Pr(\omega \in \mathcal{D}_j^{(1)}) \Pr(\omega \in \mathcal{D}_{i,j}^{(2)}) + \Pr(\omega \in \mathcal{D}_i^{(1)}). \quad (3.36)$$

We now compute the ingredient probabilities $\Pr(\omega \in \mathcal{D}_j^{(1)})$ and $\Pr(\omega \in \mathcal{D}_{i,j}^{(2)})$ in (3.36). First, by the definition, all samples in $\mathcal{D}_j^{(1)}$ must have $N_{BC} - 1$ number of $+1$'s state transitions among the first $j - 1$ transitions. And the rest of the $j - 1$ transitions must be valued by -1 . In addition, the j -th transition must be valued by $+1$ so that the block confirmation is achieved exactly at the j -th state index. As the result, the probability $\Pr(\omega \in \mathcal{D}_j^{(1)})$ equals the point mass function of a negative binomial distribution:

$$\Pr(\omega \in \mathcal{D}_j^{(1)}) = \binom{j-1}{N_{BC}-1} p_H^{N_{BC}} p_A^{j-N_{BC}}. \quad (3.37)$$

Second, computing the probability $\Pr(\omega \in \mathcal{D}_{i,j}^{(2)})$ starts from counting the number of combinations of state transitions satisfying the requirements of set $\mathcal{D}_{i,j}^{(2)}$. Recall the requirements on every element of $\mathcal{D}_{i,j}^{(2)}$, for $j = N_{BC}, \dots, 2N_{BC}$, are that the state starts from the state $S_j = 2N_{BC} - j$ and ends at the state $S_i = -1$ while all the $i - j - 1$ interim states remain nonnegative. The i -th transition should be $\Delta_i = -1$ so that the success of PoW competition is achieved exactly at the state index i . The number of combinations of such state transitions can be counted using the ballot number $C_{n,m}$ [77], which is the number of random walks that consist of $2n + m$ steps and never become negative, starting from the origin and ending at the point m . In our problem, the number of random walk

steps is $2n + m = i - j - 1$ with $m = 2N_{BC} - j$. As a result, by multiplying the probabilities p_A and p_H for state transitions, the probability $\Pr(\omega \in \mathcal{D}_{i,j}^{(2)})$ is computed as

$$\Pr(\omega \in \mathcal{D}_{i,j}^{(2)}) = C_{n,m} p_A^{(n+m+1)} p_H^n, \quad (3.38)$$

where $2n + m = i - j - 1$ and $m = 2N_{BC} - j$.

Finally, substituting (3.37) and (3.38) into (3.36) results in (3.11). ■

Appendix 3.B Proofs of Corollary 3.6 and Proposition 3.8

Proofs of Corollary 3.6

Taking infinite summations of $p_{DSA,i}$ for all indices i results in \mathbb{P}_{DSA} :

$$\mathbb{P}_{DSA} = \sum_{i=2N_{BC}+1}^{\infty} p_{DSA,i} \quad (3.39)$$

By substituting $p_{DSA,i}$ in Lemma 3.5 into (3.39), the probability \mathbb{P}_{DSA} becomes

$$\mathbb{P}_{DSA} = \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} p_A \sum_{i=2N_{BC}+1}^{\infty} C_{\frac{i-1}{2}-N_{BC}, 2N_{BC}-j} (p_A p_H)^{\frac{i-1}{2}} + \left(\frac{p_H}{p_A}\right)^{N_{BC}} \sum_{i=2N_{BC}+1}^{\infty} \binom{i-1}{N_{BC}-1} p_A^i. \quad (3.40)$$

By rearranging the indices i in the summations, we can obtain

$$\begin{aligned} \mathbb{P}_{DSA} = & \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} p_A \sum_{i=0}^{\infty} C_{i, 2N_{BC}-j} (p_A p_H)^{i+N_{BC}} \\ & + \left(\frac{p_H}{p_A}\right)^{N_{BC}} \left(\sum_{i=N_{BC}}^{\infty} \binom{i-1}{N_{BC}-1} p_A^i - \sum_{i=N_{BC}}^{2N_{BC}} \binom{i-1}{N_{BC}-1} p_A^i \right). \end{aligned} \quad (3.41)$$

We define two generating functions as

$$M_k(x) := \sum_{i=0}^{\infty} C_{i,k} x^i, \quad (3.42)$$

and

$$G_k(x) := \sum_{i=k}^{\infty} \binom{i}{k} x^i. \quad (3.43)$$

By substituting M_k and G_k into (3.41), we can write

$$\begin{aligned} \mathbb{P}_{DSA} = & \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} p_A (p_A p_H)^{N_{BC}} M_{2N_{BC}-j}(p_A p_H) \\ & + \left(\frac{p_H}{p_A} \right)^{N_{BC}} \left(p_A G_{N_{BC}-1}(p_A) - \sum_{i=N_{BC}}^{2N_{BC}} \binom{i-1}{N_{BC}-1} p_A^i \right). \end{aligned} \quad (3.44)$$

The function $M_k(x)$ is a generating function of the ballot numbers $C_{i,k}$, for which the algebraic expression given in [79] is

$$M_k(x) = \left(\frac{2}{1 + \sqrt{1-4x}} \right)^{k+1}. \quad (3.45)$$

Putting $x = p_A p_H$ into $M_k(x)$ results in

$$\begin{aligned} M_k(p_A p_H) &= \left(\frac{2}{1 + \sqrt{1-4p_A p_H}} \right)^{k+1} \\ &= \begin{cases} \left(\frac{2}{1 + \sqrt{1-4p_A(1-p_A)}} \right)^{k+1}, & \text{if } p_A < p_H, \\ \left(\frac{2}{1 + \sqrt{1-4(1-p_H)p_H}} \right)^{k+1}, & \text{if } p_A \geq p_H \end{cases} \\ &= \left(\frac{1}{p_M} \right)^{k+1}, \end{aligned} \quad (3.46)$$

where $p_M := \max(p_H, p_A)$. The function $G_k(x)$ is a generating function of binomial coefficients, and the algebraic expression for it is given in [80]:

$$G_k(x) = \frac{x^k}{(1-x)^{k+1}}. \quad (3.47)$$

Putting $x = p_A$ into $G_k(x)$ results in

$$G_k(p_A) = p_H^{-1} \left(\frac{p_A}{p_H} \right)^k. \quad (3.48)$$

Substituting (3.46) and (3.48) into (3.44) provides

$$\mathbb{P}_{DSA} = \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} p_A (p_A p_H)^{N_{BC}} p_M^{-(2N_{BC}-j+1)} + 1 - \left(\frac{p_H}{p_A} \right)^{N_{BC}} \sum_{i=N_{BC}}^{2N_{BC}} \binom{i-1}{N_{BC}-1} p_A^i. \quad (3.49)$$

We define $p_m := \min(p_A, p_H)$, then the relationship $p_A p_H = p_m p_M$ holds. By rearranging the order of operands, we can obtain

$$\mathbb{P}_{DSA} = 1 - \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} \left(\left(\frac{p_H}{p_A} \right)^{N_{BC}} p_A^j - \frac{p_A}{p_M} \left(\frac{p_m}{p_M} \right)^{N_{BC}} p_M^j \right), \quad (3.50)$$

which is equal to (3.13). ■

Proof of Proposition 3.8

From (3.15) and (3.22), when $t_{cut} = \infty$, we obtain

$$\begin{aligned}
\mathbb{E}_{T_{AS}} &= \frac{\lim_{t_{cut} \rightarrow \infty} \int_0^{t_{cut}} t f_{T_{DSA}}(t) dt}{\mathbb{P}_{AS}(t_{cut})} = \frac{\sum_{i=2N_{BC}+1}^{\infty} \mathbb{E}[T_i] p_{DSA,i}}{\mathbb{P}_{DSA}} \\
&= \frac{\sum_{i=2N_{BC}+1}^{\infty} \frac{i}{\lambda_T} p_{DSA,i}}{\mathbb{P}_{DSA}}, \tag{3.51}
\end{aligned}$$

where $E[T_i] = i\lambda_T^{-1}$ [75]. By substituting $p_{DSA,i}$ in (3.11) into (3.51) and rearranging the order of operands, we obtain

$$\begin{aligned}
\lambda_T \mathbb{P}_{DSA} \mathbb{E}_{T_{AS}} &= \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} \sum_{i=2N_{BC}}^{\infty} (i+1) C_{i, 2N_{BC}-j} p_A^{\frac{i+2}{2}} p_H^{\frac{i}{2}} \\
&+ \sum_{i=N_{BC}-1}^{\infty} (i+1) \binom{i}{N_{BC}-1} p_A^{i+1-N_{BC}} p_H^{N_{BC}} - \sum_{i=N_{BC}-1}^{2N_{BC}-1} (i+1) \binom{i}{N_{BC}-1} p_A^{i+1-N_{BC}} p_H^{N_{BC}}. \tag{3.52}
\end{aligned}$$

By rearranging the indices of summations, we arrive at

$$\begin{aligned}
\lambda_T \mathbb{P}_{DSA} \mathbb{E}_{T_{AS}} &= \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} p_A^{N_{BC}+1} p_H^{N_{BC}} \cdot \sum_{i=0}^{\infty} (2i+2N_{BC}+1) C_{i, 2N_{BC}-j} (p_A p_H)^i \\
&+ p_A \left(\frac{p_H}{p_A} \right)^{N_{BC}} \sum_{i=N_{BC}-1}^{\infty} (i+1) \binom{i}{N_{BC}-1} p_A^i - \sum_{i=N_{BC}}^{2N_{BC}} i \binom{i-1}{N_{BC}-1} p_A^{i-N_{BC}} p_H^{N_{BC}}. \tag{3.53}
\end{aligned}$$

By substituting the generating functions $M_k(x)$ and $G_k(x)$ defined respectively in (3.42) and (3.43), (3.53) becomes

$$\begin{aligned}
\lambda_T \mathbb{P}_{DSA} \mathbb{E}_{T_{AS}} &= \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} p_A^{N_{BC}+1} p_H^{N_{BC}} \\
&\cdot \left(2 \sum_{i=0}^{\infty} i C_{i, 2N_{BC}-j} (p_A p_H)^i + (2N_{BC}+1) M_{2N_{BC}-j}(p_A p_H) \right) \\
&+ p_A \left(\frac{p_H}{p_A} \right)^{N_{BC}} \left(\sum_{i=N_{BC}-1}^{\infty} i \binom{i}{N_{BC}-1} p_A^i + G_{N_{BC}-1}(p_A) \right) \\
&- \sum_{i=N_{BC}}^{2N_{BC}} i \binom{i-1}{N_{BC}-1} p_A^{i-N_{BC}} p_H^{N_{BC}}. \tag{3.54}
\end{aligned}$$

We use the following relationships,

$$\sum_{i=0}^{\infty} i C_{i,k} x^i = x M'_k(x) \quad (3.55)$$

and

$$\sum_{i=k}^{\infty} i \binom{i}{k} x^i = x G'_k(x), \quad (3.56)$$

and their derivatives are given by

$$\begin{aligned} M'_k(x) &:= \frac{d}{dx} M_k(x) = \sum_{i=0}^{\infty} i C_{i,k} x^{i-1} \\ &= \frac{(k+1)}{\sqrt{1-4x}} \left(\frac{2}{1+\sqrt{1-4x}} \right)^{k+2} \end{aligned} \quad (3.57)$$

and

$$\begin{aligned} G'_k(x) &:= \frac{d}{dx} G_k(x) \\ &= \sum_{i=k}^{\infty} i \binom{i}{k} x^{i-1} \\ &= \frac{(kx^{k-1} + x^k)}{(1-x)^{k+2}}. \end{aligned} \quad (3.58)$$

By substituting (3.55) and (3.56) into (3.54), we obtain

$$\begin{aligned} \lambda_T \mathbb{P}_{DSA} \mathbb{E}_{T_{AS}} &= \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} p_A^{N_{BC}+1} p_H^{N_{BC}} \\ &\quad \cdot \left(2p_A p_H M'_{2N_{BC}-j}(p_A p_H) + (2N_{BC}+1) M_{2N_{BC}-j}(p_A p_H) \right) \\ &\quad + p_A \left(\frac{p_H}{p_A} \right)^{N_{BC}} \left(p_A G'_{N_{BC}-1}(p_A) + G_{N_{BC}-1}(p_A) \right) \\ &\quad - \sum_{i=N_{BC}}^{2N_{BC}} i \binom{i-1}{N_{BC}-1} p_A^{i-N_{BC}} p_H^{N_{BC}} \end{aligned} \quad (3.59)$$

Putting $x = p_A p_H$ into $M'_k(x)$ in (3.57) results in

$$M'_k(p_A p_H) = M'_k(p_m p_M) = \frac{(k+1)}{1-2p_m} \left(\frac{1}{p_M} \right)^{k+2}. \quad (3.60)$$

Putting $x = p_A$ into $G'_k(x)$ in (3.58) gives

$$G'_k(p_A) = \frac{(k p_A^{k-1} + p_A^k)}{p_H^{k+2}}. \quad (3.61)$$

By substituting (3.46), (3.48), (3.60), and (3.61) into (3.59), we finally obtain (3.23). ■

Appendix 3.C Proof of Proposition 3.7

We use a generating function and generalized hypergeometric functions to compute the infinite summations in (3.15).

By substituting $p_{DSA,i}$ in (3.11) and $f_{T_i}(t)$ in (3.10) into (3.15), we arrive at

$$\begin{aligned} f_{T_{DSA}}(t) - (1 - \mathbb{P}_{DSA}) \delta(t - \infty) &= \sum_{j=N_{BC}}^{j=2N_{BC}} \binom{j-1}{N_{BC}-1} \\ &\cdot \sum_{i=2N_{BC}+1}^{\infty} C_{\frac{i-1}{2}, N_{BC}, 2N_{BC}-j} p_A^{\frac{i+1}{2}} p_H^{\frac{i-1}{2}} \frac{\lambda_T^i t^{i-1} e^{-\lambda_T t}}{(i-1)!} \\ &+ \sum_{i=2N_{BC}+1}^{\infty} \binom{i-1}{N_{BC}-1} p_H^{N_{BC}} p_A^{i-N_{BC}} \frac{\lambda_T^i t^{i-1} e^{-\lambda_T t}}{(i-1)!}. \end{aligned} \quad (3.62)$$

By rearranging the indices of summations and the order of operands, we obtain

$$\begin{aligned} f_{T_{DSA}}(t) - (1 - \mathbb{P}_{DSA}) \delta(t - \infty) &= \sum_{j=N_{BC}}^{j=2N_{BC}} \binom{j-1}{N_{BC}-1} \\ &\sum_{i=0}^{\infty} \left(C_{i, 2N_{BC}-j} p_A^{N_{BC}+i+1} p_H^{N_{BC}+i} \cdot \frac{\lambda_T^{2N_{BC}+2i+1} t^{2N_{BC}+2i} e^{-\lambda_T t}}{(2N_{BC}+2i)!} \right) \\ &+ \left(\frac{p_H}{p_A} \right)^{N_{BC}} e^{-\lambda_T t} \left(\sum_{i=N_{BC}}^{\infty} \binom{i-1}{N_{BC}-1} p_A^i \frac{\lambda_T^i t^{i-1}}{(i-1)!} - \sum_{i=N_{BC}}^{2N_{BC}} \binom{i-1}{N_{BC}-1} p_A^i \frac{\lambda_T^i t^{i-1}}{(i-1)!} \right). \end{aligned} \quad (3.63)$$

We can define two generating functions as

$$\begin{aligned}
B(x) &:= \sum_{i=0}^{\infty} C_{i, 2N_{BC}-j} \frac{x^i}{(2N_{BC} + 2i)!} \\
&= (2N_{BC} - j + 1) \sum_{i=0}^{\infty} \frac{(2i + 2N_{BC} - j)!}{i!(i + 2N_{BC} - j + 1)!(2N_{BC} + 2i)!} x^i,
\end{aligned} \tag{3.64}$$

and

$$H(x) := \sum_{i=N_{BC}}^{\infty} \binom{i-1}{N_{BC}-1} \frac{x^{i-1}}{(i-1)!} = \sum_{i=N_{BC}-1}^{\infty} \binom{i}{N_{BC}-1} \frac{x^i}{i!}. \tag{3.65}$$

By substituting $B(x)$ and $H(x)$ into (3.63), we obtain

$$\begin{aligned}
f_{T_{DSA}}(t) - (1 - \mathbb{P}_{DSA}) \delta(t - \infty) &= \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} p_A \lambda_T \\
&\cdot e^{-\lambda_T t} \left(p_A p_H (\lambda_T t)^2 \right)^{N_{BC}} B \left(p_A p_H (\lambda_T t)^2 \right) \\
&+ \left(\frac{p_H}{p_A} \right)^{N_{BC}} e^{-\lambda_T t} \left(p_A \lambda_T H(p_A \lambda_T t) - \sum_{i=N_{BC}}^{2N_{BC}} \binom{i-1}{N_{BC}-1} p_A^i \frac{\lambda_T^i t^{i-1}}{(i-1)!} \right).
\end{aligned} \tag{3.66}$$

We replace function $B(x)$ in (3.64) with the generalized hypergeometric functions (See Appendix 3.E for definition). For this purpose, we first denote the sequences in $B(x)$ by

$$\beta_i := \frac{(2i + 2N_{BC} - j)!}{i!(i + 2N_{BC} - j + 1)!(2N_{BC} + 2i)!}, \tag{3.67}$$

and

$$\beta_0 := \frac{1}{(2N_{BC} - j + 1)(2N_{BC})!}. \tag{3.68}$$

Next, the function $B(x)$ can be rewritten as

$$B(x) = (2N_{BC} - j + 1) \sum_{i=0}^{\infty} \beta_i x^i = (2N_{BC} - j + 1) \beta_0 \left(x^0 + \frac{\beta_1}{\beta_0} x^1 + \frac{\beta_2 \beta_1}{\beta_1 \beta_0} x^2 + \dots \right). \quad (3.69)$$

The reformulated sequence in (3.69) is computed by

$$\frac{\beta_{i+1}}{\beta_i} = \frac{(i+1+N_{BC}-j/2)(i+1/2+N_{BC}-j/2)}{(i+2+2N_{BC}-j)(i+1+N_{BC})(i+1/2+N_{BC})(i+1)}, \quad (3.70)$$

which has 2 polynomials in i on the numerator and 3 polynomials in i except for $(i+1)$ on the denominator. $B(x)$ can be expressed in terms of a generalized hypergeometric function ${}_2F_3$ [81] as follow,

$$\begin{aligned} B(x) &= (2N_{BC} - j + 1) \beta_0 {}_2F_3(\mathbf{a}_j; \mathbf{b}_j; x) \\ &= \frac{1}{(2N_{BC})!} {}_2F_3(\mathbf{a}_j; \mathbf{b}_j; x), \end{aligned} \quad (3.71)$$

where vectors \mathbf{a}_j and \mathbf{b}_j respectively defined in (3.17) and (3.18) are the constants in the polynomials in i of the numerator and denominator in (3.70), respectively.

We use a closed-form expression of generating function $H(x)$ in (3.65) given by

$$\begin{aligned} H(x) &= \sum_{i=N_{BC}-1}^{\infty} \binom{i}{N_{BC}-1} \frac{x^i}{i!} = \frac{1}{(N_{BC}-1)!} \sum_{i=N_{BC}-1}^{\infty} \frac{x^i}{(i-N_{BC}+1)!} \\ &= \frac{x^{N_{BC}-1}}{(N_{BC}-1)!} e^x, \end{aligned} \quad (3.72)$$

where the following relationship is used [82]:

$$\sum_{i=0}^{\infty} \frac{x^i}{i!} = e^x. \quad (3.73)$$

By substituting (3.71) and (3.72) into (3.66), we arrive at

$$\begin{aligned}
& f_{T_{DSA}}(t) - (1 - \mathbb{P}_{DSA}) \delta(t - \infty) \\
&= \frac{p_A \lambda_T e^{-\lambda_T t} (p_A p_H (\lambda_T t)^2)^{N_{BC}}}{(2N_{BC})!} \cdot \sum_{j=N_{BC}}^{j=2N_{BC}} \binom{j-1}{N_{BC}-1} {}_2F_3(\mathbf{a}_j; \mathbf{b}_j; p_A p_H (\lambda_T t)^2) \\
&+ \left(\frac{p_H}{p_A} \right)^{N_{BC}} e^{-\lambda_T t} \left(p_A \lambda_T \frac{(p_A \lambda_T t)^{N_{BC}-1}}{(N_{BC}-1)!} e^{p_A \lambda_T t} - \sum_{i=N_{BC}}^{2N_{BC}} \binom{i-1}{N_{BC}-1} p_A^i \frac{\lambda_T^{i-1}}{(i-1)!} \right) \quad (3.74) \\
&= \frac{p_A \lambda_T e^{-\lambda_T t} (p_A p_H (\lambda_T t)^2)^{N_{BC}}}{(2N_{BC})!} \cdot \sum_{j=N_{BC}}^{j=2N_{BC}} \binom{j-1}{N_{BC}-1} {}_2F_3(\mathbf{a}_j; \mathbf{b}_j; p_A p_H (\lambda_T t)^2) \\
&+ \left(\frac{p_H}{p_A} \right)^{N_{BC}} e^{-\lambda_T t} \left(p_A \lambda_T \frac{(p_A \lambda_T t)^{N_{BC}-1}}{(N_{BC}-1)!} e^{p_A \lambda_T t} - \frac{1}{(N_{BC}-1)!} \sum_{i=N_{BC}}^{2N_{BC}} p_A^i \frac{\lambda_T^{i-1}}{(i-N_{BC})!} \right).
\end{aligned}$$

We obtain (3.16) by rearranging the indices of the summations and the order of operands. ■

Appendix 3.D Comparison of Attack Success Probability with [65]

In [65], a different DS success condition other than the conditions in Definition 3.1 has been used. Specifically, the only condition was to have the fraudulent chain to grow longer than the honest chain by N_{BC} , i.e., $A(t) > H(t) + N_{BC}$ (see Section 7 of [65]). We refer to $\mathbb{P}_{\text{pre-mine}}$ as the probability of satisfying this condition. The literature has shown that satisfying this condition suffices a success of DS attack [65]. What they have not shown, however, is that this condition is not a necessary one. Thus, we here aim to show that their condition is indeed not a necessary condition, by showing that $\mathbb{P}_{DSA} > \mathbb{P}_{\text{pre-mine}}$ for all $p_A \in (0, 0.5)$. First, it has been given that $\mathbb{P}_{\text{pre-mine}} = (p_A/p_H)^{N_{BC}+1}$. Under the condition of [65], it is required that the fraudulent chain catches up with the honest chain with additional N_{BC} blocks. The catch-up probability has been derived by Nakamoto in [20] using the gambler's ruin approach as $(p_A/p_H)^k$, where k is the number of blocks that the honest chain leads by at the initial status. Next, we refer to an intermediate step in the derivation of \mathbb{P}_{DSA} by Rosenfeld [27]:

$$\mathbb{P}_{DSA} = \sum_{k=0}^{N_{BC}+1} \binom{N_{BC}+k-1}{k} p_H^{N_{BC}} p_A^k \left(\frac{p_A}{p_H} \right)^{N_{BC}-k+1} + \sum_{k=N_{BC}+2}^{\infty} \binom{N_{BC}+k-1}{k} p_H^{N_{BC}} p_A^k. \quad (3.75)$$

Finally, clear inequalities can be used to show $\mathbb{P}_{DSA} > \mathbb{P}_{\text{pre-mine}}$:

$$\begin{aligned}
\mathbb{P}_{DSA} &> \sum_{k=0}^{N_{BC}+1} \binom{N_{BC}+k-1}{k} p_H^{N_{BC}} p_A^k \left(\frac{p_A}{p_H}\right)^{N_{BC}-k+1} \\
&+ \sum_{k=N_{BC}+2}^{\infty} \binom{N_{BC}+k-1}{k} p_H^{N_{BC}} p_A^k \left(\frac{p_A}{p_H}\right)^{N_{BC}+1} \\
&> \left(\frac{p_A}{p_H}\right)^{N_{BC}+1} \sum_{k=0}^{\infty} \binom{N_{BC}+k-1}{k} p_H^{N_{BC}} p_A^k \\
&= \left(\frac{p_A}{p_H}\right)^{N_{BC}+1} = \mathbb{P}_{\text{pre-mine}}.
\end{aligned} \tag{3.76}$$

For numerical example, when $p_A = 0.35$ and $N_{BC} = 5$ the probabilities can be computed as $\mathbb{P}_{DSA} = 0.2287$ and $\mathbb{P}_{\text{pre-mine}} = 0.0244$. As the gap is significant, it is shown that the DS attack success condition defined in [65] was indeed only a sufficient condition, set to be too strict.

Appendix 3.E Generalized Hypergeometric Function [81]

For a variable z and a given set of coefficients $\beta_0, \dots, \beta_\infty$, if the ratio of coefficients b_n can be expressed in terms of two polynomials $A(n)$ and $B(n)$ in n as follow,

$$\frac{\beta_{n+1}}{\beta_n} = \frac{A(n)}{B(n)(n+1)} \tag{3.77}$$

for all integer $n \geq 0$, a power series $\sum_{n \geq 0} \beta_n z^n$ is a generalized hypergeometric series, where the polynomials are in the forms of

$$A(n) = c(a_1 + n) \cdots (a_p + n) \tag{3.78}$$

and

$$B(n) = d(b_1 + n) \cdots (b_q + n), \tag{3.79}$$

for real numbers c and d and complex numbers a_1, \dots, a_p and b_1, \dots, b_q . The generalized hypergeometric series is denoted by

$${}_pF_q(\mathbf{a}; \mathbf{b}; z) := \sum_{n \geq 0} \beta_n z^n, \quad (3.80)$$

where \mathbf{a} and \mathbf{b} are the vectors of a_1, \dots, a_p and b_1, \dots, b_q , respectively.

A generalized hypergeometric series can be a generalized hypergeometric function, if it converges. If $p < q + 1$, the ratio (3.77) goes to zero as $n \rightarrow \infty$. This implies the series (3.80) converges for any finite value z and thus can be defined as a function.

Chapter 4

Summary of Contributions and Future Research

Direction

4.1. Summary of Contributions

4.1.1. Contributions to Ultra-Wideband Sub-Nyquist Sampling of Multiband Signals

MWC has been a practical system of sub-Nyquist sampling of multiband signals spread over a wideband up to one gigahertz. The sampling efficiency of conventional MWC is limited by the speed and period of PR signals. Up to date, there has been no practical implementation of a PR signal generator running at scores of gigahertz with a sufficiently long period of chips. This impracticality hinders the input bandwidth of MWC.

We propose AMWC equipped with a new idea, intentional aliasing method. This idea improves the sampling efficiency while using PR signals with a short period. AMWC allows aliasing at ADC of MWC controlled by a parameter p . As the result, for a given specification of PR signals, at the cost of increased computational complexity of OMP by p^2 -times, AMWC improves the sampling efficiency by p -times. This also enables to widen the input bandwidth of MWC for given practical hardware of PR signal generators.

Our new idea contributes to improve the efficiency of sensors (ADC). By simulations, we showed that the improvement of sampling efficiency indeed leads to reduction on the sampling rate and number of channels required for obtaining a certain number of equations for signal reconstruction. We provided a condition on the control parameter p such that the sensing matrix of the equations obtained by AMWC achieves the Singleton bound, and thus no loss from sampling is guaranteed. In summary, the improved sampling efficiency

of AMWC reduces the total sampling rate required for lossless sampling: with fewer channels and less sampling rate of each channel than those of the conventional MWCs, a multiband signal of the wider bandwidth can be captured without information loss by AMWC. In other words, for given hardware resources, the input reconstruction with AMWC outperforms the conventional MWCs. Also, it was demonstrated that the benefits of AMWC are maintained in various SNRs. Moreover, use of LPF with random passband response, it was shown, further improves the sampling efficiency.

4.1.2. Contributions to Profitability Analysis of Double-Spending Attacks on Blockchains

Against blockchains based on PoW and the longest chain consensus, the success of a DS attack depends on the amount of computing resources run by an attacker. It has been well known that sub-50% DS attacks which use less computing resources than those used by honest miners do not guarantee the success. Nevertheless, if a success of sub-50% DS attack returns a high income compared to an expected cost, the attacker would repeat the attack until an attack succeeds. Previous works have tried to calculate the expectation of profit from sub-50% DS attacks based on stochastic models, but none of the works gave a precisely calculable tool; all of them added some assumptions to the original DS attack defined by Satoshi Nakamoto. To figure out how sub-50% DS attacks are threatening, we studied mathematical tools for symbolic computation of the profitability of DS attacks.

As the results, first, we theoretically showed that DS attacks can be profitable if and only if the value of transactions targeted by attacks are greater than the expected cost given in the right-hand side of equation (3.32). For given amount of computing resources run by attacker, this condition depends on the status of a blockchain network such as the block rewards, the amount of computing resources run by honest miners, the cost-per-time of mining rigs. In the sub-50% regime, we also showed that profitable DS attacks necessitate setting a finite cut-time. Without stopping a sub-50% DS attack at an appropriate time, it is never expected to return a profit. Second, we derived novel mathematical results that are useful for an analysis of the attack success time. They enabled us to estimate the expected profit of a DS attack for a given cut-time. All mathematical results are numerically-calculable. We provided a software for the symbolic computation of (3.32).

Our results contribute to improve the security of blockchains equipped with PoW. Our results quantitatively guide how to set a block confirmation number for transaction to be safe from a minority DS attack. The less the block confirmation number is, the less the computing resources are required for a profitable DS attack. A solution can be utilized by the network developers to discourage such an attack. On the one hand, given a block confirmation number, we can have the value of any transaction to be set below the required value of making a profitable attack in a given network. On the other hand, given the value of transaction, a network can provide a service to inform the user of the least block confirmation number that leads to make a DS attack return a negative profit.

4.2. Future Research Direction

In blockchain, a recent issue which hinders real-world applications from being practically used is scalability problem. Scalability problem is a limitation in increasing the population of users of a blockchain. There are many reasons for the problem, and one we aim to discuss is the huge memory size of blockchain. As the more transactions are recorded in a blockchain, the size accumulates. As of Apr. 2021, the size of Bitcoin blockchain exceeds 300G Bytes. Every full-node of Bitcoin needs to download the entire blockchain and store it in local storage. This requires to newly joining full-nodes to have a large storage capacity and thus demotivates them. In the perspective of the cloud of storages of all full-nodes, it is not efficient to download the same data repeatedly.

In [83], Zhou et al. have summarized the problem of huge scales of blockchains. They categorized solutions for this problem as *storage scheme optimization*. This category includes inter-node cooperative schemes such as *CUB* [84] and *Jidar* [85]. Their main idea is to separate the parts of blocks in a chain and to assign them to different groups of full-nodes. When each of the full-nodes is needed to check the validity of a chain, one node asks to the other node to check the validity of missing data (blocks or transactions). That is, they cooperate with each other. As the result, the CUB and Jidar release the burden of storage capacity to a full-node and improve the efficiency of the storage cloud.

When it comes to the compression of the whole chain, zero-knowledge proof also has been used as a solution. In zero-knowledge proving protocols, to a verifier, a prover aims to prove an NP statement composed of secret and open information without delivering the secrets. Recent advances in zero-knowledge proofs have provided succinct protocols [86], which have short length of proofs and low computational complexities for verification. As the result, the length of proofs is far shorter than original NP statements, and the verifications of proofs are done faster than verifying the NP statements themselves [87]. In addition, recursive proof verification techniques enable [88], [89] to verify a collection of many proofs at a single verification, which further reduce the net computational complexity for the verifications of multiple proofs.

Mina protocol [5] is one of the blockchains exploiting the benefits of zero-knowledge proof with the recursive proof verification proposed in [88]. They have claimed that the size of the entire chain of Mina protocol is 22k Bytes, which is about ten millionths of the size of Bitcoin. Mina protocol replaces all original data in a chain with proofs. This may work well if all of data are just records of the ownership transfers of cryptocurrency. This is because if the proof for the previous transfer is verifiable, it is not necessary to refer to the original record of the previous transfer at the time of the next transfer. However, recent and future blockchains are called for playing a role of distributed database for general data. Therefore, in addition to zero-knowledge proof, compressed sensing combined with CUB or Jida is still needed to improve the scalability of blockchains.

In this dissertation, we have discussed compressed sensing and blockchain. The goal of compressed sensing has been to remove redundancies in original data and to compress the length of it. When a blockchain is used as data storage, storing the same chain to respective storages of all full-nodes is redundant. To resolve this redundancy, we may be able to use compressed sensing in CUB or Jidar to improve the assignment cooperative querying schedules. In addition, compressed sensing may be applied to zero-knowledge proof, since the two technologies has the similar goal of compressing data. The next research direction can be to find the connection among the compressed sensing and the storage scheme optimizations, and the zero-knowledge proof for efficient and secure data storage.

Bibliography

- [1] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1–25, 2017, doi: 10.1155/2017/9324035.
- [2] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities,” *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.
- [3] H. Djelouat, A. Amira, and F. Bensaali, “Compressive Sensing-Based IoT Applications: A Review,” *JSAN*, vol. 7, no. 4, p. 45, Oct. 2018, doi: 10.3390/jsan7040045.
- [4] J. Partala, T. H. Nguyen, and S. Pirttikangas, “Non-Interactive Zero-Knowledge for Blockchain: A Survey,” *IEEE Access*, vol. 8, pp. 227945–227961, 2020, doi: 10.1109/ACCESS.2020.3046025.
- [5] J. Bonneau, I. Meckler, and V. Rao, “Mina: Decentralized Cryptocurrency at Scale,” *Available online: <https://minaprotocol.com/wp-content/uploads/technicalWhitepaper.pdf>*, p. 47.
- [6] D. L. Donoho, “Compressed sensing,” *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006, doi: 10.1109/TIT.2006.871582.
- [7] E. J. Candès, J. Romberg, and T. Tao, “Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information,” *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006, doi: 10.1109/TIT.2005.862083.
- [8] S. Park, N. Y. Yu, and H.-N. Lee, “An Information-Theoretic Study for Joint Sparsity Pattern Recovery with Different Sensing Matrices,” *IEEE Transactions on Information Theory*, vol. 63, no. 9, pp. 5559–5571, 2017, doi: 10.1109/TIT.2017.2704111.
- [9] M. F. Duarte and Y. C. Eldar, “Structured Compressed Sensing: From Theory to Applications,” *IEEE Transactions on Signal Processing*, vol. 59, no. 9, pp. 4053–4085, Sep. 2011, doi: 10.1109/TSP.2011.2161982.
- [10] M. E. Davies and Y. C. Eldar, “Rank Awareness in Joint Sparse Recovery,” *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 1135–1146, Feb. 2012, doi: 10.1109/TIT.2011.2173722.

- [11] J. Jang, S. Im, and H.-N. Lee, "Intentional Aliasing Method to Improve Sub-Nyquist Sampling System," *IEEE Trans. Signal Process.*, vol. 66, no. 12, pp. 3311–3326, Jun. 2018, doi: 10.1109/TSP.2018.2824257.
- [12] M. Mishali and Y. C. Eldar, "From Theory to Practice: Sub-Nyquist Sampling of Sparse Wideband Analog Signals," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no. 2, pp. 375–391, Apr. 2010, doi: 10.1109/JSTSP.2010.2042414.
- [13] C. Kim, W.-B. Lee, S. K. Lee, Y. T. Lee, and H.-N. Lee, "Fabrication of 2D thin-film filter-array for compressive sensing spectroscopy," *Optics and Lasers in Engineering*, vol. 115, pp. 53–58, Apr. 2019, doi: 10.1016/j.optlaseng.2018.10.018.
- [14] D. J. Brady, K. Choi, D. L. Marks, R. Horisaki, and S. Lim, "Compressive Holography," *Opt. Express*, vol. 17, no. 15, p. 13040, Jul. 2009, doi: 10.1364/OE.17.013040.
- [15] Y. Zhang, Z. Dong, P. Phillips, S. Wang, G. Ji, and J. Yang, "Exponential Wavelet Iterative Shrinkage Thresholding Algorithm for compressed sensing magnetic resonance imaging," *Information Sciences*, vol. 322, pp. 115–132, Nov. 2015, doi: 10.1016/j.ins.2015.06.017.
- [16] P. Ni and H.-N. Lee, "High-Resolution Ultrasound Imaging Using Random Interference," *IEEE Trans. Ultrason., Ferroelect., Freq. Contr.*, vol. 67, no. 9, pp. 1785–1799, Sep. 2020, doi: 10.1109/TUFFC.2020.2986588.
- [17] E. J. Candes and T. Tao, "Decoding by Linear Programming," *IEEE Trans. Inform. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005, doi: 10.1109/TIT.2005.858979.
- [18] E. Crespo Marques, N. Maciel, L. Naviner, H. Cai, and J. Yang, "A Review of Sparse Recovery Algorithms," *IEEE Access*, vol. 7, pp. 1300–1322, 2019, doi: 10.1109/ACCESS.2018.2886471.
- [19] J. Chen and X. Huo, "Theoretical Results on Sparse Representations of Multiple-Measurement Vectors," *IEEE Transactions on Signal Processing*, vol. 54, no. 12, pp. 4634–4643, Dec. 2006, doi: 10.1109/TSP.2006.881263.
- [20] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Available online: <https://bitcoin.org/bitcoin.pdf>*, 2008, [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [21] E. Ben Sasson *et al.*, "Zerocash: Decentralized Anonymous Payments from Bitcoin," in *2014 IEEE Symposium on Security and Privacy*, San Jose, CA, May 2014, pp. 459–474. doi: 10.1109/SP.2014.36.
- [22] S. Al-Kuwari, J. H. Davenport, and R. J. Bradford, "Cryptographic Hash Functions: Recent Design Trends and Security Notions," 565, 2011. Accessed: Apr. 29, 2021. [Online]. Available: <https://eprint.iacr.org/2011/565>

- [23] G.-T. Nguyen and K. Kim, “A Survey about Consensus Algorithms Used in Blockchain,” *Journal of Information Processing Systems*, vol. 14, no. 1, pp. 101–128, 2018, doi: 10.3745/JIPS.01.0024.
- [24] C. Lepore, M. Ceria, A. Visconti, U. P. Rao, K. A. Shah, and L. Zanolini, “A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS,” *Mathematics*, vol. 8, no. 10, p. 1782, Oct. 2020, doi: 10.3390/math8101782.
- [25] X. Fu, H. Wang, and P. Shi, “A survey of Blockchain consensus algorithms: mechanism, design and applications,” *Sci. China Inf. Sci.*, vol. 64, no. 2, p. 121101, Feb. 2021, doi: 10.1007/s11432-019-2790-1.
- [26] D. G. Wood, “ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER,” *Available online: <https://ethereum.github.io/yellowpaper/paper.pdf>*, p. 39, 2013.
- [27] M. Rosenfeld, “Analysis of Hashrate-Based Double Spending,” *arXiv:1402.2009 [cs]*, Feb. 2014, Accessed: Oct. 11, 2018. [Online]. Available: <http://arxiv.org/abs/1402.2009>
- [28] E. Attah, “Five most prolific 51% attacks in crypto: Verge, Ethereum Classic, Bitcoin Gold, Feathercoin, Vertcoin,” *CryptoSlate*, Apr. 24, 2019. <https://cryptoslate.com/prolific-51-attacks-crypto-verge-ethereum-classic-bitcoin-gold-feathercoin-vertcoin/> (accessed Feb. 27, 2020).
- [29] J. H. Jang and H. N. Lee, “Transaction Verification System for Blockchain, and Transaction Verification Method for Blockchain,” patent, PCT/KR2019/017571, Nov. 12, 2019 Accessed: Apr. 29, 2021. [Online]. Available: <https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2020241995>
- [30] J. Jang, N. Y. Yu, and H.-N. Lee, “A study on mixing sequences in modulated wide-band converters,” in *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Washington DC, DC, USA, Dec. 2016, pp. 1408–1412. doi: 10.1109/GlobalSIP.2016.7906073.
- [31] J. Jang and H.-N. Lee, “Profitable Double-Spending Attacks,” *Applied Sciences*, vol. 10, no. 23, p. 8477, Nov. 2020, doi: 10.3390/app10238477.
- [32] H. J. Landau, “Necessary density conditions for sampling and interpolation of certain entire functions,” *Acta Mathematica*, vol. 117, no. 1, pp. 37–52, 1967.
- [33] M. Mishali and Y. C. Eldar, “Blind Multiband Signal Reconstruction: Compressed Sensing for Analog Signals,” *IEEE Transactions on Signal Processing*, vol. 57, no. 3, pp. 993–1009, Mar. 2009, doi: 10.1109/TSP.2009.2012791.
- [34] Y. Chen, H. Chi, T. Jin, S. Zheng, X. Jin, and X. Zhang, “Sub-Nyquist Sampled Analog-to-Digital Conversion Based on Photonic Time Stretch and Compressive Sensing

With Optical Random Mixing,” *Journal of Lightwave Technology*, vol. 31, no. 21, pp. 3395–3401, Nov. 2013, doi: 10.1109/JLT.2013.2282088.

- [35] Y. Zhao, Y. H. Hu, and J. Liu, “Random Triggering-Based Sub-Nyquist Sampling System for Sparse Multiband Signal,” *IEEE Transactions on Instrumentation and Measurement*, vol. 66, no. 7, pp. 1789–1797, Jul. 2017, doi: 10.1109/TIM.2017.2665983.
- [36] J. A. Tropp, J. N. Laska, M. F. Duarte, J. K. Romberg, and R. G. Baraniuk, “Beyond Nyquist: Efficient Sampling of Sparse Bandlimited Signals,” *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 520–544, Jan. 2010, doi: 10.1109/TIT.2009.2034811.
- [37] S. A. Varma and K. M. M. Prabhu, “A new approach to near-theoretical sampling rate for modulated wideband converter,” *Signal Processing and Communications (SPCOM), 2014 International Conference on*, pp. 1–5, 2014.
- [38] M. Sakare, “A Power and Area Efficient Architecture of a PRBS Generator With Multiple Outputs,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 64, no. 8, pp. 927–931, Aug. 2017, doi: 10.1109/TCSII.2016.2641582.
- [39] L. Vera and J. R. Long, “A 40-Gb/s $2^{11} - 1$ PRBS With Distributed Clocking and a Trigger Countdown Output,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 63, no. 8, pp. 758–762, Aug. 2016, doi: 10.1109/TCSII.2016.2531091.
- [40] T. Chen, M. Guo, Z. Yang, and W. Zhang, “A novel and efficient compressive multiplexer for multi-channel compressive sensing based on modulated wideband converter,” *2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference*, pp. 347–351, May 2016, doi: 10.1109/ITNEC.2016.7560379.
- [41] T. Haque, R. T. Yazicigil, K. J.-L. Pan, J. Wright, and P. R. Kinget, “Theory and Design of a Quadrature Analog-to-Information Converter for Energy-Efficient Wideband Spectrum Sensing,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 2, pp. 527–535, Feb. 2015, doi: 10.1109/TCSI.2014.2360756.
- [42] Y. Chen, A. J. Goldsmith, and Y. C. Eldar, “On the Minimax Capacity Loss Under Sub-Nyquist Universal Sampling,” *IEEE Transactions on Information Theory*, vol. 63, no. 6, pp. 3348–3367, Jun. 2017, doi: 10.1109/TIT.2017.2695541.
- [43] Y. Chen, Y. C. Eldar, and A. J. Goldsmith, “Shannon Meets Nyquist: Capacity of Sampled Gaussian Channels,” *IEEE Transactions on Information Theory*, vol. 59, no. 8, pp. 4889–4914, Aug. 2013, doi: 10.1109/TIT.2013.2254171.
- [44] L. Gan and W. Huali, “Deterministic Binary Sequences For Modulated Wideband Converter,” Sep. 2013, doi: 10.5281/ZENODO.54396.

- [45] J. Zhang, N. Fu, and X. Peng, “Compressive Circulant Matrix Based Analog to Information Conversion,” *IEEE Signal Process. Lett.*, vol. 21, no. 4, pp. 428–431, Apr. 2014, doi: 10.1109/LSP.2013.2285444.
- [46] X. Yang, X. Tao, Y. J. Guo, X. Huang, and Q. Cui, “Subsampled circulant matrix based analogue compressed sensing,” *Electron. Lett.*, vol. 48, no. 13, p. 767, 2012, doi: 10.1049/el.2012.0366.
- [47] T. Hoholdt and J. Justesen, “Ternary sequences with perfect periodic autocorrelation (Corresp.),” *IEEE Trans. Inform. Theory*, vol. 29, no. 4, pp. 597–600, Jul. 1983, doi: 10.1109/TIT.1983.1056707.
- [48] Y. Jin and B. D. Rao, “Support Recovery of Sparse Signals in the Presence of Multiple Measurement Vectors,” *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 3139–3157, May 2013, doi: 10.1109/TIT.2013.2238605.
- [49] IEEE Aerospace and Electronic Systems Society, Radar Systems Panel, Institute of Electrical and Electronics Engineers, and IEEE-SA Standards Board, “IEEE standard for letter designations for radar-frequency bands.” 2003.
- [50] F. E. Nathanson, P. J. O’Reilly, and M. N. Cohen, *Radar design principles: signal processing and the environment*. Raleigh, NC: Scitech Publ., 2004.
- [51] T. O. Dickson *et al.*, “An 80-Gb/s $2^{31}-1$ pseudorandom binary sequence generator in SiGe BiCMOS technology,” *IEEE Journal of Solid-State Circuits*, vol. 40, no. 12, pp. 2735–2745, Dec. 2005, doi: 10.1109/JSSC.2005.856578.
- [52] A. Gharib, A. Talai, R. Weigel, and D. Kissinger, “A 1.16 pJ/bit 80 Gb/s $2^{11}-1$ PRBS generator in SiGe bipolar technology,” *European Microwave Integrated Circuit Conference (EuMIC), 2014 9th*, pp. 277–280, 2014.
- [53] “Hittite’s 18 GHz Ultra Wideband Track-and-Hold Amplifier Enhances High Speed ADC Performance,” *Hittite Microwave*, Available: http://www.analog.com/media/en/technical-documentation/technical-articles/track-n-hold_0411.pdf.
- [54] R. Singleton, “Maximum distance q-nary codes,” *IEEE Transactions on Information Theory*, vol. 10, no. 2, pp. 116–118, 1964.
- [55] Y. Chen, M. Mishali, Y. C. Eldar, and A. O. Hero III, “Modulated Wideband Converter with Non-ideal Lowpass Filters,” *2010 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*, pp. 3630–3633, Jun. 2010, doi: 10.1109/ICASSP.2010.5495912.
- [56] D. Baron, M. F. Duarte, M. B. Wakin, S. Sarvotham, and R. G. Baraniuk, “Distributed compressive sensing,” *arXiv preprint arXiv:0901.3403*, 2009, Accessed: Aug. 07, 2017. [Online]. Available: <https://arxiv.org/abs/0901.3403>

- [57] T. Blumensath and M. E. Davies, "Sampling Theorems for Signals From the Union of Finite-Dimensional Linear Subspaces," *IEEE Transactions on Information Theory*, vol. 55, no. 4, pp. 1872–1882, Apr. 2009, doi: 10.1109/TIT.2009.2013003.
- [58] H. Ritzdorf, C. Soriente, G. O. Karame, S. Marinovic, D. Gruber, and S. Capkun, "Toward Shared Ownership in the Cloud," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 3019–3034, Dec. 2018, doi: 10.1109/TIFS.2018.2837648.
- [59] S. Wu, Y. Chen, Q. Wang, M. Li, C. Wang, and X. Luo, "CREAM: A Smart Contract Enabled Collusion-Resistant e-Auction," *IEEE Transactions on Information Forensics and Security*, 2018, doi: 10.1109/TIFS.2018.2883275.
- [60] Y. Sompolinsky and A. Zohar, "Secure High-Rate Transaction Processing in Bitcoin," Puerto Rico, Jan. 2015, pp. 507–527.
- [61] A. Beikverdi and JooSeok Song, "Trend of centralization in Bitcoin's distributed network," in *2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, Takamatsu, Jun. 2015, pp. 1–6. doi: 10.1109/SNPD.2015.7176229.
- [62] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is Bitcoin a Decentralized Currency?," *IEEE Secur. Privacy*, vol. 12, no. 3, pp. 54–60, May 2014, doi: 10.1109/MSP.2014.49.
- [63] J. Bonneau, "Why buy when you can rent? Bribery attacks on Bitcoin consensus," presented at the The 3rd Workshop on Bitcoin and Blockchain Research (BITCOIN '16), Barbados, Feb. 2016. doi: http://dx.doi.org/10.1007/978-3-662-53357-4_2.
- [64] S. Sayeed and H. Marco-Gisbert, "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack," *Applied Sciences*, vol. 9, no. 9, p. 1788, Apr. 2019, doi: 10.3390/app9091788.
- [65] Y. Sompolinsky and A. Zohar, "Bitcoin's Security Model Revisited," *arXiv:1605.09193 [cs]*, May 2016, Accessed: Oct. 14, 2018. [Online]. Available: <http://arxiv.org/abs/1605.09193>
- [66] G. Bissias, B. N. Levine, A. P. Ozisik, and G. Andresen, "An Analysis of Attacks on Blockchain Consensus," *arXiv:1610.07985 [cs]*, Oct. 2016, Accessed: Oct. 14, 2018. [Online]. Available: <http://arxiv.org/abs/1610.07985>
- [67] E. Zaghoul, T. Li, M. W. Mutka, and J. Ren, "Bitcoin and Blockchain: Security and Privacy," *IEEE Internet Things J.*, pp. 1–1, 2020, doi: 10.1109/JIOT.2020.3004273.
- [68] E. B. Budish, "The Economic Limits of Bitcoin and the Blockchain," *SSRN Journal*, 2018, doi: 10.2139/ssrn.3197300.

- [69] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the Security and Performance of Proof of Work Blockchains,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS’16*, Vienna, Austria, 2016, pp. 3–16. doi: 10.1145/2976749.2978341.
- [70] G. Ramezan, C. Leung, and Z. Jane Wang, “A Strong Adaptive, Strategic Double-Spending Attack on Blockchains,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCoM) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, Jul. 2018, pp. 1219–1227. doi: 10.1109/Cybermatics_2018.2018.00216.
- [71] C. Pinzón and C. Rocha, “Double-spend Attack Models with Time Advantage for Bitcoin,” *Electronic Notes in Theoretical Computer Science*, vol. 329, pp. 79–103, Dec. 2016, doi: 10.1016/j.entcs.2016.12.006.
- [72] P.-O. Goffard, “Fraud risk assessment within blockchain transactions,” *Adv. Appl. Probab.*, vol. 51, no. 2, pp. 443–467, Jun. 2019, doi: 10.1017/apr.2019.18.
- [73] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, “Misbehavior in Bitcoin: A Study of Double-Spending and Accountability,” *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, p. 2:1-2:32, May 2015, doi: 10.1145/2732196.
- [74] G. O. Karame, E. Androulaki, and S. Capkun, “Double-spending fast payments in bitcoin,” in *Proceedings of the 2012 ACM conference on Computer and communications security - CCS ’12*, Raleigh, North Carolina, USA, 2012, p. 906. doi: 10.1145/2382196.2382292.
- [75] A. Papoulis and S. U. Pillai, “Random walks and other applications,” in *Probability, Random Variables and Stochastic Processes*, 4th edition., Boston, Mass.: McGraw-Hill Europe, 2002.
- [76] R. Bowden, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, “Block arrivals in the Bitcoin blockchain,” *arXiv:1801.07447 [cs]*, Jan. 2018, Accessed: Dec. 11, 2019. [Online]. Available: <http://arxiv.org/abs/1801.07447>
- [77] P. Flajolet and R. Sedgewick, “Combinatorial structures and ordinary generating functions,” in *Analytic Combinatorics*, Cambridge University Press, 2009.
- [78] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, “A Survey on Security and Privacy Issues of Bitcoin,” *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018, doi: 10.1109/COMST.2018.2842460.
- [79] H. S. Wilf, “Analytic and asymptotic methods,” in *generatingfunctionology: Third Edition*, 3 edition., Wellesley, Mass: A K Peters/CRC Press, 2005.

- [80] H. S. Wilf, “Introductory ideas and examples,” in *generatingfunctionology: Third Edition*, 3 edition., Wellesley, Mass: A K Peters/CRC Press, 2005.
- [81] G. Gasper and M. Rahman, “Basic Hypergeometric series,” in *Basic hypergeometric series*, Second., vol. 96, Cambridge University Press, Cambridge, 2004. doi: 10.1017/CBO9780511526251.
- [82] P. Flajolet and R. Sedgewick, “Labelled structures and exponential generating functions,” in *Analytic Combinatorics*, Cambridge University Press, 2009.
- [83] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, “Solutions to Scalability of Blockchain: A Survey,” *IEEE Access*, vol. 8, pp. 16440–16455, 2020, doi: 10.1109/ACCESS.2020.2967218.
- [84] Z. Xu, S. Han, and L. Chen, “CUB, a Consensus Unit-Based Storage Scheme for Blockchain System,” in *2018 IEEE 34th International Conference on Data Engineering (ICDE)*, Paris, Apr. 2018, pp. 173–184. doi: 10.1109/ICDE.2018.00025.
- [85] X. Dai, J. Xiao, W. Yang, C. Wang, and H. Jin, “Jidar: A Jigsaw-like Data Reduction Approach Without Trust Assumptions for Bitcoin System,” in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, Dallas, TX, USA, Jul. 2019, pp. 1317–1326. doi: 10.1109/ICDCS.2019.00132.
- [86] J. Groth, “On the Size of Pairing-Based Non-interactive Arguments,” in *Advances in Cryptology – EUROCRYPT 2016*, vol. 9666, M. Fischlin and J.-S. Coron, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 305–326. doi: 10.1007/978-3-662-49896-5_11.
- [87] B. Parno, J. Howell, C. Gentry, and M. Raykova, “Pinocchio: Nearly Practical Verifiable Computation,” in *2013 IEEE Symposium on Security and Privacy*, Berkeley, CA, May 2013, pp. 238–252. doi: 10.1109/SP.2013.47.
- [88] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, “Scalable Zero Knowledge via Cycles of Elliptic Curves,” in *Advances in Cryptology – CRYPTO 2014*, vol. 8617, J. A. Garay and R. Gennaro, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 276–294. doi: 10.1007/978-3-662-44381-1_16.
- [89] A. Chiesa, D. Ojha, and N. Spooner, “Fractal: Post-quantum and Transparent Recursive Proofs from Holography,” in *Advances in Cryptology – EUROCRYPT 2020*, vol. 12105, A. Canteaut and Y. Ishai, Eds. Cham: Springer International Publishing, 2020, pp. 769–793. doi: 10.1007/978-3-030-45721-1_27.