Proofs, Arguments, and Zero-Knowledge

Other titles in Foundations and Trends® in Privacy and Security

Assured Autonomy Survey
Christopher Rouff and Lanier Watkins
ISBN: 978-1-63828-038-5

Hardware Platform Security for Mobile Devices
Lachlan J. Gunn, N. Asokan, Jan-Erik Ekberg, Hans Liljestrand, Vijayanand Nayani and Thomas Nyman
ISBN: 978-1-68083-976-0

Cloud Computing Security: Foundations and Research Directions
Anrin Chakraborti, Reza Curtmola, Jonathan Katz, Jason Nieh, Ahmad-Reza Sadeghi, Radu Sion and Yinqian Zhang
ISBN: 978-1-68083-958-6

Expressing Information Flow Properties
Elisavet Kozyri, Stephen Chong and Andrew C. Myers
ISBN: 978-1-68083-936-4

Accountability in Computing: Concepts and Mechanisms
Joan Feigenbaum, Aaron D. Jaggard and Rebecca N. Wright
ISBN: 978-1-68083-784-1

Proofs, Arguments, and Zero-Knowledge

Justin Thaler
Georgetown University
jt1157@georgetown.edu

the essence of knowledge
Boston — Delft

Foundations and Trends® in Privacy and Security

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

J. Thaler. *Proofs, Arguments, and Zero-Knowledge*. Foundations and Trends® in Privacy and Security, vol. 4, no. 2–4, pp. 117–660, 2022.

ISBN: 978-1-63828-125-2

Foundations and Trends® in Privacy and Security
Volume 4, Issue 2–4, 2022

Editorial Board

Editorial Scope

Topics

Foundations and Trends® in Privacy and Security publishes survey and tutorial articles in the following topics:

- Access control
- Accountability
- Anonymity
- Application security
- Artifical intelligence methods in security and privacy
- Authentication
- Big data analytics and privacy
- Cloud security
- Cyber-physical systems security and privacy
- Distributed systems security and privacy
- Embedded systems security and privacy
- Forensics
- Hardware security
- Human factors in security and privacy
- Information flow
- Intrusion detection
- Malware
- Metrics
- Mobile security and privacy
- Language-based security and privacy
- Network security
- Privacy-preserving systems
- Protocol security
- Security and privacy policies
- Security architectures
- System security
- Web security and privacy

Information for Librarians

Foundations and Trends® in Privacy and Security, 2022, Volume 4, 4 issues. ISSN paper version 2474-1558. ISSN online version 2474-1566. Also available as a combined paper and online subscription.

Contents

Proofs, Arguments, and Zero-Knowledge

Justin Thaler

Georgetown University, USA; jt1157@georgetown.edu

ABSTRACT

Interactive proofs (IPs) and arguments are cryptographic protocols that enable an untrusted prover to provide a guarantee that it performed a requested computation correctly. Introduced in the 1980s, IPs and arguments represented a major conceptual expansion of what constitutes a "proof" that a statement is true.

Traditionally, a proof is a static object that can be easily checked step-by-step for correctness. In contrast, IPs allow for interaction between prover and verifier, as well as a tiny but nonzero probability that an invalid proof passes verification. Arguments (but not IPs) even permit there to be "proofs" of false statements, so long as those "proofs" require exorbitant computational power to find. To an extent, these notions mimic in-person interactions that mathematicians use to convince each other that a claim is true, without going through the painstaking process of writing out and checking a traditional static proof.

This work is supported by NSF CAREER award CCF-1845125 and by DARPA under Agreement No. HR00112020022. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the United States Government or DARPA.

Justin Thaler (2022), "Proofs, Arguments, and Zero-Knowledge", Foundations and Trends® in Privacy and Security: Vol. 4, No. 2–4, pp 117–660. DOI: 10.1561/3300000030.

Celebrated theoretical results from the 1980s and 1990s such as **IP** = **PSPACE** and **MIP** = **NEXP** showed that, in principle, surprisingly complicated statements can be verified efficiently. What is more, any argument can in principle be transformed into one that is *zero-knowledge*, which means that proofs reveal no information other than their own validity. Zero-knowledge arguments have a myriad of applications in cryptography.

Within the last decade, general-purpose zero-knowledge arguments have made the jump from theory to practice. This has opened new doors in the design of cryptographic systems, and generated additional insights into the power of IPs and arguments (zero-knowledge or otherwise). There are now no fewer than five promising approaches to designing efficient, general-purpose zero-knowledge arguments. This survey covers these approaches in a unified manner, emphasizing commonalities between them.

1

Introduction

This monograph is about verifiable computing (VC). VC refers to cryptographic protocols called interactive proofs (IPs) and arguments that enable a prover to provide a guarantee to a verifier that the prover performed a requested computation correctly. Introduced in the 1980s, IPs and arguments represented a major conceptual expansion of what constitutes a "proof" that a statement is true. Traditionally, a proof is a static object that can be easily checked step-by-step for correctness, because each individual step of the proof should be trivial to verify. In contrast, IPs allow for interaction between prover and verifier, as well as a tiny but nonzero probability that an invalid proof passes verification. The difference between IPs and arguments is that arguments (but not IPs) permit the existence of "proofs" of incorrect statements, so long as those "proofs" require exorbitant computational power to find.[1]

Celebrated theoretical results from the mid-1980s and early 1990s indicated that VC protocols can, at least in principle, accomplish amazing feats. These include enabling a cell phone to monitor the execution of a powerful but untrusted (even malicious) supercomputer, enabling

[1] For example, an argument, but not an IP, might make use of a cryptosystem, such that it is possible for a cheating prover to find a convincing "proof" of a false statement if (and only if) the prover can break the cryptosystem.

computationally weak peripheral devices (e.g., security card readers) to offload security-critical work to powerful remote servers, or letting a mathematician obtain a high degree of confidence that a theorem is true by looking at only a few symbols of a purported proof.[2]

VC protocols can be especially useful in cryptographic contexts when they possess a property called *zero-knowledge*. This means that the proof or argument reveals nothing but its own validity.

To give a concrete sense of why zero-knowledge protocols are useful, consider the following quintessential example from authentication. Suppose that Alice chooses a random password x and publishes a hash $z = h(x)$, where h is a one-way function. This means that given $z = h(x)$ for a randomly chosen x, enormous computational power should be required to find a preimage of z under h, i.e., an x' such that $h(x') = z$. Later, suppose that Alice wants to convince Bob that she is the same person who published z. She can do this by proving to Bob that she knows an x' such that $h(x') = z$. This will convince Bob that Alice is the same person who published z, since it means that either Alice knew x to begin with, or she inverted h (which is assumed to be beyond the computational capabilities of Alice).

How can Alice convince Bob that she knows a preimage of z under h? A trivial proof is for Alice to send x to Bob, and Bob can easily check that $h(x) = z$. But this reveals much more information than that Alice knows a preimage of z. In particular it reveals the preimage itself. Bob can use this knowledge to impersonate Alice forevermore, since now he too knows the preimage of z.

In order to prevent Bob from learning information that can compromise the password x, it is important that the proof reveals nothing beyond its own validity. This is exactly what the zero-knowledge property guarantees.

A particular goal of this survey is to describe a variety of approaches to constructing so-called zero-knowledge Succinct Non-interactive Arguments of Knowledge, or zk-SNARKs for short. "Succinct" means that the proofs are short. "Non-interactive" means that the proof is

[2] So long as the proof is written in a specific, mildly redundant format. See our treatment of *probabilistically checkable proofs* (PCPs) in Section 9.

static, consisting of a single message from the prover. "Of Knowledge" roughly means that the protocol establishes not only that a statement is true, but also that the prover *knows* a "witness" to the veracity of the statement.[3] Argument systems satisfying all of these properties have a myriad of applications throughout cryptography.

Practical zero-knowledge protocols for highly specialized statements of cryptographic relevance (such as proving knowledge of a discrete logarithm [223]) have been known for decades. However, general-purpose zero-knowledge protocols have only recently become plausibly efficient enough for cryptographic deployment. By general-purpose, we mean protocol design techniques that apply to arbitrary computations. This exciting progress has involved the introduction of beautiful new protocols, and brought a surge of interest in zero-knowledge proofs and arguments. This survey seeks to make accessible, in a unified manner, the main ideas and approaches to the design of these protocols.

Background and Context. In the mid-1980s and 1990s, theoretical computer scientists showed that IPs and arguments can be vastly more efficient (at least, in an asymptotic sense) than traditional **NP** proofs,[4] which are static and information-theoretically secure.[5] The foundational results characterizing the power of these protocols (such as **IP** = **PSPACE** [186], [231], **MIP** = **NEXP** [17], and the PCP theorem [10], [11]) are some of the most influential and celebrated in computational complexity theory.[6]

Despite their remarkable asymptotic efficiency, general-purpose VC protocols were long considered wildly impractical, and with good reason: naive implementations of the theory would have had comically high

[3]For example, the authentication scenario above really requires a zero-knowledge proof *of knowledge* for the statement "there exists a password x such that $h(x) = z$". This is because the application requires that Bob be convinced not just of the fact that there *exists* a preimage x of z under h (which will always be true if h is a surjective function), but also that Alice knows x.

[4]We formally define notions such as **NP** and **IP** in Section 3.3.

[5]The term information-theoretically secure here refers to the fact that **NP** proofs (like IPs, but unlike arguments) are secure against computationally unbounded provers.

[6]The results **IP** = **PSPACE** and **MIP** = **NEXP** are both covered in this survey (see Sections 4.5.5 and 8.5 respectively).

concrete costs (trillions of years for the prover, even for very short computations). But the last decade has seen major improvements in the costs of VC protocols, with a corresponding jump from theory to practice. Even though implementations of general-purpose VC protocols remain somewhat costly (especially for the prover), paying this cost can often be justified if the VC protocol is zero-knowledge, since zero-knowledge protocols enable applications that may be totally impossible without them. Moreover, emerging applications to public blockchains have elevated the importance of proving relatively simple statements, on which it is feasible to run modern VC protocols despite their costs.

Approaches to Zero-Knowledge Protocol Design, and Philosophy of This Survey. Argument systems are typically developed in a two-step process. First, an information-theoretically secure protocol, such as an IP, *multi-prover interactive proof* (MIP), or *probabilistically checkable proof* (PCP), is developed for a model involving one or more provers that are assumed to behave in some restricted manner (e.g., in an MIP, the provers are assumed not to send information to each other about the challenges they receive from the verifier). Second, the information-theoretically secure protocol is combined with cryptography to "force" a (single) prover to behave in the restricted manner, thereby yielding an argument system. This second step also often endows the resulting argument system with important properties, such as zero-knowledge, succinctness, and non-interactivity. If the resulting argument satisfies all of these properties, then it is in fact a zk-SNARK.

By now, there are a variety promising approaches to developing efficient zk-SNARKs, which can be categorized by the type of information-theoretically secure protocol upon which they are based. These include (1) IPs, (2) MIPs, (3) PCPs, or more precisely a related notion called *interactive oracle proofs* (IOPs), which is a hybrid between an IP and a PCP, and (4) *linear PCPs*. Sections 1.2.1–1.2.3 below give a more detailed overview of these models. This survey explains in a unified manner how to design efficient protocols in all four information-theoretically secure models, emphasizing commonalities between them.

IPs, MIPs, and PCPs/IOPs can all be transformed into succinct interactive arguments by combining them with a cryptographic primitive called a *polynomial commitment scheme*; the interactive arguments can then be rendered non-interactive and publicly verifiable by applying a cryptographic technique called the *Fiat-Shamir transformation* (Section 5.2), yielding a SNARK. Transformations from linear PCPs to arguments are somewhat different, though closely related to certain polynomial commitment schemes. As with the information-theoretically secure protocols themselves, this survey covers these cryptographic transformations in a unified manner.

Because of the two-step nature of zk-SNARK constructions, it is often helpful to first understand proofs and arguments *without* worrying about zero-knowledge, and then at the very end understand how to achieve zero-knowledge as an "add on" property. Accordingly, we do not discuss zero-knowledge until relatively late in this survey (Section 11). Earlier sections are devoted to describing efficient protocols in each of the information-theoretically secure models, and explaining how to transform them into succinct arguments.

By now, zk-SNARKs have been deployed in a number of real-world systems, and there is a large and diverse community of researchers, industry professionals, and open source software developers working to improve and deploy the technology. This survey assumes very little formal mathematical background—mainly comfort with modular arithmetic, some notions from the theory of finite fields and groups, and basic probability theory—and is intended as a resource for anyone interested in verifiable computing and zero-knowledge. However, it does require significant mathematical maturity and considerable comfort with theorems and proofs. Also helpful (but not strictly necessary) is knowledge of standard complexity classes like **P** and **NP**, and complexity-theoretic notions such as **NP**-completeness.

Ordering of Information-Theoretically Secure Models in This Survey. We first cover IPs, then MIPs, then PCPs and IOPs, then linear PCPs. This ordering roughly follows the chronology of the models' introduction to the research literature. Perhaps ironically, the models have been applied to practical SNARK design in something resembling *reverse*

chronological order. For example, the first practical SNARKs were based on linear PCPs. In fact, this is not a coincidence: a primary motivation for introducing linear PCPs in the first place was the goal of obtaining simpler and more practical succinct arguments, and specifically the *impracticality* of arguments derived from PCPs.

Section-by-section Outline. Section 2 familiarizes the reader with randomness and the power of probabilistic proof systems, through two easy but important case studies. Section 3 introduces technical notions that will be useful throughout the survey. Sections 4 describes state-of-the-art interactive proofs. Section 5 describes the Fiat-Shamir transformation, a key technique that is used to remove interaction from cryptographic protocols. Section 7 introduces the notion of a polynomial commitment scheme, and combines it with the IPs of Section 4 and the Fiat-Shamir transformation of Section 5 to obtain the first SNARK covered in the survey. Section 8 describes state-of-the-art MIPs and SNARKs derived thereof. Sections 9–10 describe PCPs and IOPs, and SNARKs derived thereof.

Section 6 is a standalone section describing techniques for representing computer programs in formats amenable to application of such SNARKs.

Section 11 introduces the notion of zero-knowledge. Section 12 describes a particularly simple type of zero-knowledge argument called Σ-protocols, and uses them to derive commitment schemes. These commitment schemes serve as important building blocks for more complicated protocols covered in subsequent sections. Section 13 describes efficient techniques for transforming non-zero-knowledge protocols into zero-knowledge ones. Sections 14–16 cover practical polynomial commitment schemes, which can be used to turn any IP, MIP, or IOP into a succinct zero-knowledge argument of knowledge (zkSNARK). Section 17 covers our final approach to designing zkSNARKs, namely through linear PCPs. Section 18 describes how to recursively compose SNARKs to improve their costs and achieve important primitives such as so-called *incrementally verifiable computation*. Finally, Section 19 provides a taxonomy of design paradigms for practical zkSNARKs, and delineates the pros and cons of each approach.

Suggestions for Reading the Monograph. The monograph may happily be read from start to finish, but non-linear paths may offer a faster route to a big-picture understanding of SNARK design techniques. Suggestions to this effect are as follows.

Sections 2 and 3 introduce basic technical notions used throughout all subsequent sections (finite fields, IPs, arguments, low-degree extensions, the Schwartz-Zippel lemma, etc.), and should not be skipped by readers unfamiliar with these concepts.

Readers may next wish to read the *final* section, Section 19, which provides a birds-eye view of all SNARK design approaches and how they relate to each other. Section 19 uses some terminology that may be unfamiliar to the reader at this point, but it should nonetheless be understandable and it provides context that is helpful to have in mind when working through more technical sections.

After that, there are many possible paths through the monograph. Readers specifically interested in the SNARKs that were the first to be deployed in commercial settings can turn to Section 17 on linear PCPs. This section is essentially self-contained but for its use of pairing-based cryptography that is introduced in Section 15.1 (and, at the very end, its treatment of zero-knowledge, a concept introduced formally in Section 11).

Otherwise, readers should turn to understanding the alternative approach to SNARK design, namely to combine a *polynomial IOP* (of which IPs, MIPs, and PCPs are special cases) with a *polynomial commitment scheme*.

To quickly understand polynomial IOPs, we suggest a careful reading of Section 4.1 on the sum-check protocol, followed by Section 4.6 on the GKR interactive proof protocol for circuit evaluation, or Section 8.2 giving a 2-prover MIP for circuit satisfiability. Next, the reader can turn to Section 7, which explains how to combine such protocols with polynomial commitments to obtain succinct arguments.

To understand polynomial commitment schemes, the reader can either tackle Sections 10.4 and 10.5 to understand IOP-based polynomial commitments, or instead turn to Sections 12 and 14–16 (in that order) to understand polynomial commitments based on the discrete logarithm problem and pairings.

A compressed overview of polynomial IOPs and polynomial commitments is provided in a sequence of three talk videos posted on this monograph's webpage.[7] Readers may find it useful to watch these videos prior to a detailed reading of Sections 4–10.

Material That can be Skipped on a First Reading. Sections 4.2–4.5 are devoted to detailed example applications of the sum-check protocol and explaining how to efficiently implement the prover within it. While these sections contain interesting results and are useful for familiarizing oneself with the sum-check protocol, subsequent sections do not depend on them. Similarly, Section 5 on the Fiat-Shamir transformation and Section 6 on front-ends are optional on a first reading. Sections 9.3 and 9.4 provide PCPs that are mainly of historical interest and can be skipped.

Sections 11 and 13 offer treatments of zero-knowledge that largely stand on their own. Similarly, Section 18 discusses SNARK composition and stands on its own.

1.1 Mathematical Proofs

This survey covers different notions of *mathematical proofs* and their applications in computer science and cryptography. Informally, what we mean by a proof is anything that convinces someone that a statement is true, and a "proof system" is any procedure that decides what is and is not a convincing proof. That is, a proof system is specified by a verification procedure that takes as input any statement and a claimed "proof" that the statement is true, and decides whether or not the proof is valid.

What properties do we want in a proof system? Here are four obvious ones.

- Any true statement should have a convincing proof of its validity. This property is typically referred to as *completeness*.
- No false statement should have a convincing proof. This property is referred to as *soundness*.

[7] https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.html.

- Ideally, the verification procedure will be "efficient". Roughly, this means that simple statements should have short (convincing) proofs that can be *checked* quickly.
- Ideally, proving should be efficient too. Roughly, this means that simple statements should have short (convincing) proofs that can be *found* quickly.

Traditionally, a mathematical proof is something that can be written and checked line-by-line for correctness. This traditional notion of proof is precisely the one captured by the complexity class **NP**.[8] However, over the last 30+ years, computer scientists have studied much more general and exotic notions of proofs. This has transformed computer scientists' notions of what it means to prove something, and has led to major advances in complexity theory and cryptography.

1.2 What Kinds of Non-Traditional Proofs Will We Study?

All of the notions of proofs that we study in this survey will be probabilistic in nature. This means that the verification procedure will make random choices, and the soundness guarantee will hold with (very) high probability over those random choices. That is, there will be a (very) small probability that the verification procedure will declare a false statement to be true.

1.2.1 Interactive Proofs (IPs)

To understand what an interactive proof is, it is helpful to think of the following application. Imagine a business (verifier) that is using a commercial cloud computing provider to store and process its data. The business sends all of its data up to the cloud (prover), which stores it, while the business stores only a very small "secret" summary of the data (meaning that the cloud does not know the user's secret summary). Later, the business asks the cloud a question about its data, typically

[8] Roughly speaking, the complexity class **NP** contains all problems for which the correct answer on any input is either YES or NO, and for all YES instances, there is an efficiently-checkable (traditional) proof that the correct answer is YES. See Section 3.3 for details.

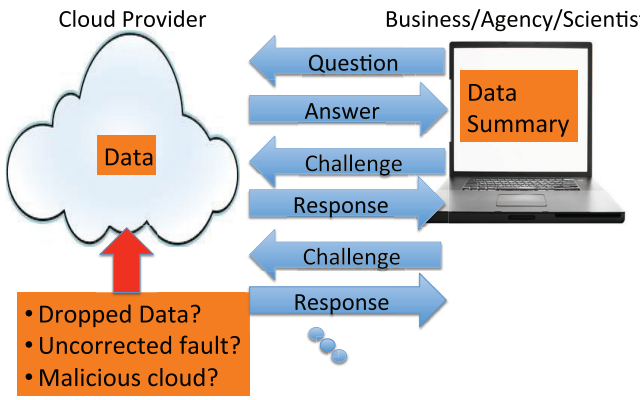

Figure 1.1: Depiction of an interactive proof or argument used to check that a cloud computing provider is storing and processing a user's data correctly.

in the form of a computer program f that the business wants the cloud to run on its data using the cloud's vast computing infrastructure. The cloud does so, and sends the user the claimed output of the program, $f(\mathsf{data})$. Rather than blindly trust that the cloud executed the program on the data correctly, the business can use an interactive proof system (IP) to obtain a formal *guarantee* that the claimed output is correct.

In the IP, the business interrogates the cloud, sending a sequence of challenges and receiving a sequence of responses. At the end of the interrogation, the business must decide whether to accept the answer as valid or reject it as invalid. See Figure 1.1 for a diagram of this interaction.

Completeness of the IP means that if the cloud correctly runs the program on the data and follows the prescribed protocol, then the user will be convinced to accept the answer as valid. Soundness of the IP means that if the cloud returns the wrong output, then the user will reject the answer as invalid with high probability *no matter how hard the cloud works to trick the user* into accepting the answer as valid. Intuitively, the interactive nature of the IP lets the business exploit the element of surprise (i.e., the fact that the cloud cannot predict the business's next challenge) to catch a lying cloud in a lie.

It is worth remarking on an interesting difference between IPs and traditional static proofs. Static proofs are *transferrable*, meaning that if

Peggy (prover) hands Victor (verifier) a proof that a statement is true, Victor can turn around and convince Tammy (a third party) that the same statement is true, simply by copying the proof. In contrast, an interactive proof may not be transferrable. Victor can try to convince Tammy that the statement is true by sending Tammy a transcript of his interaction with Peggy, but Tammy will not be convinced unless Tammy trusts that Victor correctly represented the interaction. This is because soundness of the IP only holds if, every time Peggy sends a response to Victor, Peggy does not know what challenge Victor will respond with next. The transcript alone does not give Tammy a guarantee that this holds.

1.2.2 Argument Systems

Argument systems are IPs, but where the soundness guarantee need only hold against cheating provers that run in polynomial time.[9] Argument systems make use of cryptography. Roughly speaking, in an argument system a cheating prover cannot trick the verifier into accepting a false statement unless it breaks some cryptosystem, and breaking the cryptosystem is assumed to require superpolynomial time.

1.2.3 Multi-Prover Interactive Proofs, Probabilistically Checkable Proofs, etc.

An MIP is like an IP, except that there are multiple provers, and these provers are assumed not to share information with each other regarding what challenges they receive from the verifier. A common analogy for MIPs is placing two or more criminal suspects in separate rooms before interrogating them, to see if they can keep their story straight. Law enforcement officers may be unsurprised to learn that the study of MIPs has lent theoretical justification to this practice. Specifically, the study of MIPs has revealed that if one locks the provers in separate rooms and then interrogates them separately, they can convince their

[9] Roughly speaking, this means that if the input has size n, then the prover's runtime (for sufficiently large values of n) should be bounded above by some constant power of n, e.g., n^{10}.

interrogators of much more complicated statements than if they are questioned together.

In a PCP, the proof is static as in a traditional mathematical proof, but the verifier is only allowed to read a small number of (possibly randomly chosen) characters from the proof.[10] This is in analogy to a lazy referee for a mathematical journal, who does not feel like painstakingly checking the proofs in a submitted paper for correctness. The PCP theorem [10], [11] essentially states that *any* traditional mathematical proof can be written in a format that enables this lazy reviewer to obtain a high degree of confidence in the validity of the proof by inspecting just a few words of it.

Philosophically, MIPs and PCPs are extremely interesting objects to study, but they are not directly applicable in most cryptographic settings, because they make unrealistic or onerous assumptions about the prover(s). For example, soundness of any MIP only holds if the provers do not share information with each other regarding what challenges they receive from the verifier. This is not directly useful in most cryptographic settings, because typically in these settings there is only a single prover, and even if there is more than one, there is no way to force the provers not to communicate. Similarly, although the verifier only reads a few characters of a PCP, a direct implementation of a PCP would require the prover to transmit the whole proof to the verifier, and this would be the dominant cost in most real-world scenarios (the example of a lazy journal referee notwithstanding). That is, once the prover transmits the whole proof to the verifier, there is little real-world benefit to having the verifier avoid reading the whole proof.

However, by combining MIPs and PCPs with cryptography, we will see how to turn them into argument systems, and these *are* directly applicable in cryptographic settings. For example, we will see in Section 9.2 how to turn a PCP into an argument system in which the prover does *not* have to send the whole PCP to the verifier.

[10] More precisely, a PCP verifier is allowed to read as much of the proof as it wants. However, for the PCP to be considered efficient, it must be the case that the verifier only needs to read a tiny fraction of the proof to ascertain with high confidence whether or not the proof is valid.

Section 10.2 of this survey in fact provides a unifying abstraction, called *polynomial IOPs*, of which all of the IPs, MIPs, and PCPs that we cover are a special case. It turns out that any polynomial IOP can be transformed into an argument system with short proofs, via a cryptographic primitive called a polynomial commitment scheme.

References

[1] B. Abdolmaleki, K. Baghery, H. Lipmaa, and M. Zajac, "A subversion-resistant SNARK," in *Advances in Cryptology – ASIACRYPT 2017 – 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3–7, 2017, Proceedings, Part III*, T. Takagi and T. Peyrin, Eds., ser. Lecture Notes in Computer Science, vol. 10626, pp. 3–33, Springer, 2017.

[2] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo, "Structure-preserving signatures and commitments to group elements," in *Annual Cryptology Conference*, Springer, pp. 209–236, 2010.

[3] W. Aiello and J. Hastad, "Statistical zero-knowledge languages can be recognized in two rounds," *Journal of Computer and System Sciences*, vol. 42, no. 3, pp. 327–345, 1991.

[4] M. Albrecht, L. Grassi, C. Rechberger, A. Roy, and T. Tiessen, "MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 191–219, 2016.

[5] J. Alman and V. V. Williams, "A refined laser method and faster matrix multiplication," in *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, SIAM, pp. 522–539, 2021.

[6] A. Aly, T. Ashur, E. Ben-Sasson, S. Dhooghe, and A. Szepieniec, "Efficient symmetric primitives for advanced cryptographic protocols (A Marvellous contribution)," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 426, 2019.

[7] S. Ames, C. Hazay, Y. Ishai, and M. Venkitasubramaniam, "Ligero: Lightweight sublinear arguments without a trusted setup," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2087–2104, 2017.

[8] B. Applebaum, I. Damgård, Y. Ishai, M. Nielsen, and L. Zichron, "Secure arithmetic computation with constant computational overhead," in *Annual International Cryptology Conference*, Springer, pp. 223–254, 2017.

[9] S. Arora and B. Barak, *Computational Complexity: A Modern Approach*, 1st edn. New York, NY, USA: Cambridge University Press, 2009.

[10] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, "Proof verification and the hardness of approximation problems," *Journal of the ACM (JACM)*, vol. 45, no. 3, pp. 501–555, 1998.

[11] S. Arora and S. Safra, "Probabilistic checking of proofs: A new characterization of NP," *J. ACM*, vol. 45, no. 1, pp. 70–122, 1998.

[12] S. Arora and M. Sudan, "Improved low-degree testing and its applications," *Combinatorica*, vol. 23, no. 3, pp. 365–426, 2003.

[13] A. Arun, C. Ganesh, S. Lokam, T. Mopuri, and S. Sridhar, Dew: Transparent constant-sized zksnarks, Cryptology ePrint Archive, Report 2022/419, 2022. URL: https://ia.cr/2022/419.

[14] T. Attema, S. Fehr, and M. Klooß, fiat-shamir transformation of multi-round interactive proofs, Cryptology ePrint Archive, Report 2021/1377, 2021. URL: https://ia.cr/2021/1377.

[15] L. Babai, "Trading group theory for randomness," in *STOC*, R. Sedgewick, Ed., pp. 421–429, ACM, 1985.

[16] L. Babai, "Graph isomorphism in quasipolynomial time," in *Proceedings of the Forty-Eighth Annual Acm Symposium on Theory of Computing*, pp. 684–697, 2016.

[17] L. Babai, L. Fortnow, and C. Lund, "Non-deterministic exponential time has two-prover interactive protocols," *Computational Complexity*, vol. 1, pp. 3–40, 1991.

[18] E. Bangerter, J. Camenisch, and S. Krenn, "Efficiency limitations for Σ-protocols for group homomorphisms," in *Theory of Cryptography Conference*, Springer, pp. 553–571, 2010.

[19] B. Barak and O. Goldreich, "Universal arguments and their applications.," in *IEEE Conference on Computational Complexity*, pp. 194–203, IEEE Computer Society, 2002.

[20] N. Barić and B. Pfitzmann, "Collision-free accumulators and fail-stop signature schemes without trees," in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 480–494, 1997.

[21] J. Bartusek, L. Bronfman, J. Holmgren, F. Ma, and R. D. Rothblum, "On the (in) security of Kilian-based SNARGs," in *Theory of Cryptography Conference*, Springer, pp. 522–551, 2019.

[22] C. Baum, J. Bootle, A. Cerulli, R. del Pino, J. Groth, and V. Lyubashevsky, "Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits," in *Advances in Cryptology – CRYPTO 2018 – 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part II*, H. Shacham and A. Boldyreva, Eds., Lecture Notes in Computer Science, vol. 10992, pp. 669–699, Springer, 2018.

[23] C. Baum, A. J. Malozemoff, M. B. Rosen, and P. Scholl, "Mac'n' Cheese: Zero-knowledge proofs for boolean and arithmetic circuits with nested disjunctions," in *Annual International Cryptology Conference*, Springer, pp. 92–122, 2021.

[24] S. Bayer and J. Groth, "Efficient zero-knowledge argument for correctness of a shuffle," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 263–280, 2012.

[25] J. Baylina, "Verifying STARKs with SNARKs," zk7 Zero Knowledge Summit 7 on April 21, 2022. URL: https://youtu.be/j7An-33Zs0.

[26] M. Bellare, A. Boldyreva, and A. Palacio, "An uninstantiable random-oracle-model scheme for a hybrid-encryption problem," in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 171–188, 2004.

[27] M. Bellare, D. Coppersmith, J. Håstad, M. A. Kiwi, and M. Sudan, "Linearity testing in characteristic two," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1781–1795, 1996.

[28] M. Bellare, G. Fuchsbauer, and A. Scafuro, "NIZKs with an untrusted CRS: security in the face of parameter subversion," in *Advances in Cryptology – ASIACRYPT 2016 – 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4–8, 2016, Proceedings, Part II*, J. H. Cheon and T. Takagi, Eds., ser. Lecture Notes in Computer Science, vol. 10032, pp. 777–804, 2016.

[29] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proceedings of the 1st ACM conference on Computer and communications security*, pp. 62–73, 1993.

[30] A. Belling and O. Bgassat, *Using GKR inside a SNARK to reduce the cost of hash verification down to 3 constraints*, 2020. URL: https://ethresear.ch/t/using-gkr-inside-a-snark-to-reduce-the-cost-of-hash-verification-down-to-3-constraints/7550.

[31] V. E. Beneš, "Mathematical theory of connecting networks and telephone traffic," *Academic Press*, 1965.

[32] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson, "Multi-prover interactive proofs: How to remove intractability assumptions," in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2–4, 1988,* Chicago, Illinois, USA, ACM, pp. 113–131, 1988.

[33] E. Ben-Sasson, I. Bentov, A. Chiesa, A. Gabizon, D. Genkin, M. Hamilis, E. Pergament, M. Riabzev, M. Silberstein, E. Tromer, *et al.*, "Computational integrity with a public random string from quasi-linear PCPs," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 551–579, 2017.

[34] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Fast reed-solomon interactive oracle proofs of proximity," in *45th International Colloquium on Automata, Languages, and Programming (ICALP 2018)*, Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[35] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable zero knowledge with no trusted setup," in *Advances in Cryptology – CRYPTO 2019 – 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part III*, A. Boldyreva and D. Micciancio, Eds., ser. Lecture Notes in Computer Science, vol. 11694, pp. 701–732, Springer, 2019.

[36] E. Ben-Sasson, D. Carmon, Y. Ishai, S. Kopparty, and S. Saraf, "Proximity gaps for Reed–Solomon codes," in *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE, pp. 900–909, 2020.

[37] E. Ben-Sasson, D. Carmon, S. Kopparty, and D. Levit, "Elliptic curve fast fourier transform (ECFFT) part I: Fast polynomial algorithms over all finite fields," *CoRR*, vol. abs/2107.08473, 2021.

[38] E. Ben-Sasson, D. Carmon, S. Kopparty, and D. Levit, "Scalable and transparent proofs over all large fields, via elliptic curves," *Electron. Colloquium Comput. Complex.*, vol. TR22-110, 2022.

[39] E. Ben-Sasson, A. Chiesa, M. A. Forbes, A. Gabizon, M. Riabzev, and N. Spooner, "Zero knowledge protocols from succinct constraint detection," in *Theory of Cryptography Conference*, Springer, pp. 172–206, 2017.

[40] E. Ben-Sasson, A. Chiesa, D. Genkin, and E. Tromer, "Fast reductions from rams to delegatable succinct constraint satisfaction problems: Extended abstract," in *ITCS*, R. D. Kleinberg, Ed., pp. 401–414, ACM, 2013.

[41] E. Ben-Sasson, A. Chiesa, D. Genkin, and E. Tromer, "On the concrete efficiency of probabilistically-checkable proofs," in *STOC*, pp. 585–594, 2013.

[42] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, "SNARKs for C: Verifying program executions succinctly and in zero knowledge," in *Advances in Cryptology – CRYPTO 2013 – 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2013. Proceedings, Part II*, R. Canetti and J. A. Garay, Eds., ser. Lecture Notes in Computer Science, vol. 8043, pp. 90–108, Springer, 2013.

[43] E. Ben-Sasson, A. Chiesa, M. Riabzev, N. Spooner, M. Virza, and N. P. Ward, "Aurora: Transparent succinct arguments for R1CS," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 103–128, 2019.

[44] E. Ben-Sasson, A. Chiesa, and N. Spooner, "Interactive oracle proofs," in *Theory of Cryptography – 14th International Conference, TCC 2016-B, Beijing, China, October 31 – November 3, 2016, Proceedings, Part II*, M. Hirt and A. D. Smith, Eds., ser. Lecture Notes in Computer Science, vol. 9986, pp. 31–60, 2016.

[45] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Scalable zero knowledge via cycles of elliptic curves," in *Advances in Cryptology – CRYPTO 2014 – 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17–21, 2014, Proceedings, Part II*, J. A. Garay and R. Gennaro, Eds., ser. Lecture Notes in Computer Science, vol. 8617, pp. 276–294, Springer, 2014.

[46] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von Neumann architecture," in *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20–22, 2014*, pp. 781–796, 2014.

[47] E. Ben-Sasson, L. Goldberg, and D. Levit, *Stark friendly hash – survey and recommendation*, Cryptology ePrint Archive, Report 2020/948, 2020. URL: https://eprint.iacr.org/2020/948.

[48] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, and S. P. Vadhan, "Short PCPs verifiable in polylogarithmic time," in *20th Annual IEEE Conference on Computational Complexity (CCC 2005), 11–15 June 2005, San Jose, CA, USA*, pp. 120–134, 2005.

[49] E. Ben-Sasson, S. Kopparty, and S. Saraf, "Worst-case to average case reductions for the distance to a code," in *33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA*, R. A. Servedio, Ed., ser. LIPIcs, vol. 102, 24:1–24:23, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2018.

[50] E. Ben-Sasson and M. Sudan, "Short PCPs with polylog query complexity," *SIAM J. Comput.*, vol. 38, no. 2, pp. 551–607, 2008.

[51] D. Bernhard, O. Pereira, and B. Warinschi, "How not to prove yourself: Pitfalls of the Fiat-Shamir heuristic and applications to Helios," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 626–643, 2012.

[52] D. J. Bernstein, "Curve25519: New Diffie-Hellman speed records," in *International Workshop on Public Key Cryptography*, Springer, pp. 207–228, 2006.

[53] R. Bhadauria, Z. Fang, C. Hazay, M. Venkitasubramaniam, T. Xie, and Y. Zhang, "Ligero++: A new optimized sublinear IOP," in *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*, J. Ligatti, X. Ou, J. Katz, and G. Vigna, Eds., pp. 2025–2038, ACM, 2020.

[54] E. Birrell and S. Vadhan, "Composition of zero-knowledge proofs with efficient provers," in *Theory of Cryptography Conference*, Springer, pp. 572–587, 2010.

[55] N. Bitansky and A. Chiesa, "Succinct arguments from multi-prover interactive proofs and their efficiency benefits," in *CRYPTO*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, pp. 255–272, Springer, 2012.

[56] N. Bitansky, A. Chiesa, Y. Ishai, R. Ostrovsky, and O. Paneth, "Succinct non-interactive arguments via linear interactive proofs," in *TCC*, pp. 315–333, 2013.

[57] A. R. Block, J. Holmgren, A. Rosen, R. D. Rothblum, and P. Soni, "Time-and space-efficient arguments from groups of unknown order," in *Annual International Cryptology Conference*, Springer, pp. 123–152, 2021.

[58] M. Blum, "How to prove a theorem so no one else can claim it," in *Proceedings of the International Congress of Mathematicians*, Citeseer, vol. 1, p. 2, 1986.

[59] M. Blum, W. Evans, P. Gemmell, S. Kannan, and M. Naor, "Checking the correctness of memories," *Algorithmica*, pp. 90–99, 1995.

[60] M. Blum, M. Luby, and R. Rubinfeld, "Self-testing/correcting with applications to numerical problems," *J. Comput. Syst. Sci.*, vol. 47, no. 3, pp. 549–595, 1993.

[61] A. J. Blumberg, J. Thaler, V. Vu, and M. Walfish, "Verifiable computation using multiple provers," *IACR Cryptology ePrint Archive*, vol. 2014, p. 846, 2014.

[62] D. Boneh and X. Boyen, "Short signatures without random oracles," in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 56–73, 2004.

[63] D. Boneh, B. Bünz, and B. Fisch, "Batching techniques for accumulators with applications to IOPs and stateless blockchains," in *Annual International Cryptology Conference*, Springer, pp. 561–586, 2019.

[64] D. Boneh, J. Drake, B. Fisch, and A. Gabizon, "Halo infinite: Proof-carrying data from additive polynomial commitments," in *Annual International Cryptology Conference*, Springer, pp. 649–680, 2021.

[65] J. Bonneau, I. Meckler, V. Rao, and E. Shapiro, "Coda: Decentralized cryptocurrency at scale.," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 352, 2020.

[66] J. Bootle, A. Cerulli, P. Chaidos, J. Groth, and C. Petit, "Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 327–357, 2016.

[67] J. Bootle, A. Cerulli, E. Ghadafi, J. Groth, M. Hajiabadi, and S. K. Jakobsen, "Linear-time zero-knowledge proofs for arithmetic circuit satisfiability," in *Advances in Cryptology – ASIACRYPT 2017 – 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3–7, 2017, Proceedings, Part III*, T. Takagi and T. Peyrin, Eds., ser. Lecture Notes in Computer Science, vol. 10626, pp. 336–365, Springer, 2017.

[68] J. Bootle, A. Cerulli, J. Groth, S. Jakobsen, and M. Maller, "Arya: Nearly linear-time zero-knowledge proofs for correct program execution," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 595–626, 2018.

[69] J. Bootle, A. Chiesa, and J. Groth, "Linear-time arguments with sublinear verification from tensor codes," in *Theory of Cryptography – 18th International Conference, TCC 2020, Durham, NC, USA, November 16–19, 2020, Proceedings, Part II*, R. Pass and K. Pietrzak, Eds., ser. Lecture Notes in Computer Science, vol. 12551, pp. 19–46, Springer, 2020.

[70] J. Bootle, A. Chiesa, and K. Sotiraki, "Sumcheck arguments and their applications," in *Annual International Cryptology Conference*, Springer, pp. 742–773, 2021.

[71] J. Bootle, V. Lyubashevsky, N. K. Nguyen, and G. Seiler, *A non-PCP approach to succinct quantum-safe zero-knowledge*, Cryptology ePrint Archive, Report 2020/737, To appear in CRYPTO, 2020. URL: https://eprint.iacr.org/2020/737.

[72] R. B. Boppana, J. Hastad, and S. Zachos, "Does co-NP have short interactive proofs?" *Inf. Process. Lett.*, vol. 25, no. 2, pp. 127–132, 1987.

[73] P. Bottinelli, An illustrated guide to elliptic curve cryptography validation, 2021.

[74] S. Bowe, A. Chiesa, M. Green, I. Miers, P. Mishra, and H. Wu, "Zexe: Enabling decentralized private computation," in *2020 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 947–964, 2020.

[75] S. Bowe, J. Grigg, and D. Hopwood, "Recursive proof composition without a trusted setup," *Cryptol. ePrint Arch., Tech. Rep*, vol. 1021, p. 2019, 2019.

[76] Z. Brakerski, V. Koppula, and T. Mour, "NIZK from LPN and trapdoor hash via correlation intractability for approximable relations," in *Annual International Cryptology Conference*, Springer, pp. 738–767, 2020.

[77] G. Brassard, D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge," *Journal of Computer and System Sciences*, vol. 37, no. 2, pp. 156–189, 1988.

[78] G. Brassard, P. Høyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions," in *Latin American Symposium on Theoretical Informatics*, Springer, pp. 163–169, 1998.

[79] B. Braun, A. J. Feldman, Z. Ren, S. Setty, A. J. Blumberg, and M. Walfish, "Verifying computations with state," in *Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles*, ACM, pp. 341–357, 2013.

[80] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *2018 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 315–334, 2018.

[81] B. Bünz, A. Chiesa, W. Lin, P. Mishra, and N. Spooner, "Proof-carrying data without succinct arguments," in *Annual International Cryptology Conference*, Springer, pp. 681–710, 2021.

[82] B. Bünz, A. Chiesa, P. Mishra, and N. Spooner, "Proof-carrying data from accumulation schemes.," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 499, 2020.

[83] B. Bünz, B. Fisch, and A. Szepieniec, "Transparent snarks from DARK compilers," in *Advances in Cryptology – EUROCRYPT 2020 – 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part I*, A. Canteaut and Y. Ishai, Eds., ser. Lecture Notes in Computer Science, vol. 12105, pp. 677–706, Springer, 2020.

[84] B. Bünz, M. Maller, P. Mishra, N. Tyagi, and P. Vesely, "Proofs for inner pairing products and applications," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 65–97, 2021.

[85] D. Butler, A. Lochbihler, D. Aspinall, and A. Gascón, "Formalising Σ-Protocols and Commitment Schemes Using CryptHOL," *Journal of Automated Reasoning*, vol. 65, no. 4, pp. 521–567, 2021.

[86] M. Campanelli, A. Faonio, D. Fiore, A. Querol, and H. Rodríguez, "Lunar: A toolbox for more efficient universal and updatable zksnarks and commit-and-prove extensions," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 3–33, 2021.

[87] M. Campanelli, D. Fiore, and A. Querol, "Legosnark: Modular design and composition of succinct zero-knowledge proofs," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2075–2092, 2019.

[88] R. Canetti, Y. Chen, J. Holmgren, A. Lombardi, G. N. Rothblum, R. D. Rothblum, and D. Wichs, "Fiat-Shamir: From practice to theory," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pp. 1082–1090, 2019.

[89] R. Canetti, Y. Chen, and L. Reyzin, "On the correlation intractability of obfuscated pseudorandom functions," in *Theory of cryptography conference*, Springer, pp. 389–415, 2016.

[90] R. Canetti, Y. Chen, L. Reyzin, and R. D. Rothblum, "Fiat-shamir and correlation intractability from strong kdm-secure encryption," in *Advances in Cryptology – EUROCRYPT 2018 – 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29–May 3, 2018 Proceedings, Part I*, J. B. Nielsen and V. Rijmen, Eds., ser. Lecture Notes in Computer Science, vol. 10820, pp. 91–122, Springer, 2018.

[91] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *Journal of the ACM (JACM)*, vol. 51, no. 4, pp. 557–594, 2004.

[92] A. Chakrabarti, G. Cormode, A. McGregor, and J. Thaler, "Annotations in data streams," *ACM Transactions on Algorithms*, vol. 11, no. 1, p. 7, 2014, Preliminary version by the first three authors in *ICALP*, 2009.

[93] M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, and G. Zaverucha, "Post-quantum zero-knowledge and signatures from symmetric-key primitives," in *Proceedings of the 2017 Acm Sigsac Conference on Computer and Communications Security*, pp. 1825–1842, 2017.

[94] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[95] B. Chen, B. Bünz, D. Boneh, and Z. Zhang, "HyperPlonk: Plonk with linear-time prover and high-degree custom gates," *Cryptology ePrint Archive*, 2022.

[96] W. Chen, A. Chiesa, E. Dauterman, and N. P. Ward, "Reducing participation costs via incremental verification for ledger systems.," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 1522, 2020.

[97] A. Chiesa, M. A. Forbes, T. Gur, and N. Spooner, "Spatial isolation implies zero knowledge even in a quantum world," in *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7–9, 2018*, M. Thorup, Ed., pp. 755–765, IEEE Computer Society, 2018.

[98] A. Chiesa, Y. Hu, M. Maller, P. Mishra, N. Vesely, and N. Ward, "Marlin: Preprocessing zkSNARKs with universal and updatable SRS," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 738–768, 2020.

[99] A. Chiesa, P. Manohar, and N. Spooner, "Succinct arguments in the quantum random oracle model," in *Theory of Cryptography Conference*, Springer, pp. 1–29, 2019.

[100] A. Chiesa, D. Ojha, and N. Spooner, "Fractal: Post-quantum and transparent recursive proofs from holography," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 769–793, 2020.

[101] D. Clarke, S. Devadas, M. Van Dijk, B. Gassend, and G. E. Suh, "Incremental multiset hash functions and their application to memory integrity checking," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 188–207, 2003.

[102] G. Cormode, M. Mitzenmacher, and J. Thaler, "Practical verified computation with streaming interactive proofs," in *ITCS*, S. Goldwasser, Ed., pp. 90–112, ACM, 2012.

[103] G. Cormode, J. Thaler, and K. Yi, "Verifying computations with streaming interactive proofs," *Proc. VLDB Endow.*, vol. 5, no. 1, pp. 25–36, 2011.

[104] R. Cramer and I. Damgård, "Zero-knowledge proofs for finite field arithmetic, or: Can zero-knowledge be for free?" In *Annual International Cryptology Conference*, Springer, pp. 424–441, 1998.

[105] I. B. Damgård, "On the existence of bit commitment schemes and zero-knowledge proofs," in *Conference on the Theory and Application of Cryptology*, Springer, pp. 17–27, 1989.

[106] I. Dinur, D. Kales, A. Promitzer, S. Ramacher, and C. Rechberger, "Linear equivalence of block ciphers with partial nonlinear layers: Application to lowmc," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 343–372, 2019.

[107] S. Dittmer, Y. Ishai, and R. Ostrovsky, Line-point zero knowledge and its applications, Cryptology ePrint Archive, Report 2020/1446, 2020. URL: https://eprint.iacr.org/2020/1446.

[108] S. Dobson, S. D. Galbraith, and B. Smith, *Trustless unknown-order groups*, Cryptology ePrint Archive, Report 2020/196, 2020, URL: https://ia.cr/2020/196.

[109] M. Driscoll, *The animated elliptic curve*, Github source code, 2022, URL: https://github.com/syncsynchalt/animated-curves.

[110] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[111] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Conference on the Theory and Application of Cryptographic Techniques*, Springer, pp. 186–194, 1986.

[112] L. Fortnow, "The complexity of perfect zero-knowledge," in *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, pp. 204–209, 1987.

[113] L. Fortnow, J. Rompel, and M. Sipser, "On the power of multi-power interactive protocols," in *Structure in Complexity Theory Conference, 1988. Proceedings., Third Annual*, IEEE, pp. 156–161, 1988.

[114] T. K. Frederiksen, J. B. Nielsen, and C. Orlandi, "Privacy-free garbled circuits with applications to efficient zero-knowledge," in *Advances in Cryptology – EUROCRYPT 2015 – 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*, E. Oswald and M. Fischlin, Eds., ser. Lecture Notes in Computer Science, vol. 9057, pp. 191–219, Springer, 2015.

[115] R. Freivalds, "Probabilistic machines can use less running time," in *IFIP congress*, vol. 839, p. 842, 1977.

[116] G. Fuchsbauer, "Subversion-zero-knowledge SNARKs," in *Public-Key Cryptography – PKC 2018 – 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25–29, 2018, Proceedings, Part I*, M. Abdalla and R. Dahab, Eds., ser. Lecture Notes in Computer Science, vol. 10769, pp. 315–347, Springer, 2018.

[117] G. Fuchsbauer, E. Kiltz, and J. Loss, "The algebraic group model and its applications," in *Annual International Cryptology Conference*, Springer, pp. 33–62, 2018.

[118] E. Fujisaki and T. Okamoto, "Statistical zero knowledge protocols to prove modular polynomial relations," in *Annual International Cryptology Conference*, Springer, pp. 16–30, 1997.

[119] M. Furer, O. Goldreich, Y. Mansour, M. Sipser, and S. Zachos, "On completeness and soundness in interactive proof systems," *Randomness and Computation (Volume 5 of Advances in Computing Research)*, pp. 429–442, 1989.

[120] A. Gabizon, Auroralight: Improved prover efficiency and srs size in a soniclike system, IACR Cryptology ePrint Archive, 2019: 601, 2019.

[121] A. Gabizon, "On the security of the BCTV Pinocchio zk-SNARK variant.," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 119, 2019.

[122] A. Gabizon and Z. J. Williamson, *Plookup: A simplified polynomial protocol for lookup tables*, Cryptology ePrint Archive, Report 2020/315, 2020. URL: https://ia.cr/2020/315.

[123] A. Gabizon, Z. J. Williamson, and O. Ciobotaru, "PlonK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge.," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 953, 2019.

[124] N. Gailly, M. Maller, and A. Nitulescu, "SnarkPack: Practical snark aggregation," *Cryptology ePrint Archive*, 2021.

[125] R. Gennaro, C. Gentry, B. Parno, and M. Raykova, "Quadratic span programs and succinct NIZKs without PCPs," in *EUROCRYPT*, pp. 626–645, 2013.

[126] C. Gentry and D. Wichs, "Separating succinct non-interactive arguments from all falsifiable assumptions," in *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6–8 June 2011*, L. Fortnow and S. P. Vadhan, Eds., pp. 99–108, ACM, 2011.

[127] I. Giacomelli, J. Madsen, and C. Orlandi, "ZKBoo: Faster zero-knowledge for boolean circuits," in *25th USENIX Security Symposium*, pp. 1069–1083, 2016.

[128] L. Goldberg, S. Papini, and M. Riabzev, *Cairo? A Turing-complete STARK-friendly CPU architecture*, Cryptology ePrint Archive, Paper 2021/1063, URL: https://eprint.iacr.org/2021/1063, 2021.

[129] O. Goldreich, *On post-modern cryptography*, Cryptology ePrint Archive, Report 2006/461, URL: https://eprint.iacr.org/2006/461, 2006.

[130] O. Goldreich, *Foundations of cryptography: Volume 1, Basic tools*. Cambridge university press, 2007.

[131] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems," *Journal of the ACM (JACM)*, vol. 38, no. 3, pp. 690–728, 1991.

[132] O. Goldreich, S. P. Vadhan, and A. Wigderson, "On interactive proofs with a laconic prover," *Computational Complexity*, vol. 11, no. 1–2, pp. 1–53, 2002.

[133] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM J. Comput.*, vol. 18, pp. 186–208, 1989, Preliminary version in STOC 1985. Earlier versions date to 1982.

[134] S. Goldwasser and Y. T. Kalai, "On the (in) security of the Fiat-Shamir paradigm," in *44th Annual IEEE Symposium on Foundations of Computer Science, 2003. Proceedings.*, IEEE, pp. 102–113, 2003.

[135] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, "Delegating computation: Interactive proofs for muggles," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, ser. STOC '08, pp. 113–122, New York, NY, USA: ACM, 2008.

[136] S. Goldwasser and M. Sipser, "Private coins versus public coins in interactive proof systems," in *STOC*, J. Hartmanis, Ed., pp. 59–68, ACM, 1986.

[137] A. Golovnev, J. Lee, S. T. V. Setty, J. Thaler, and R. S. Wahby, "Brakedown: Linear-time and post-quantum snarks for R1CS," *IACR Cryptol. ePrint Arch.*, p. 1043, 2021.

[138] L. Grassi, D. Kales, D. Khovratovich, A. Roy, C. Rechberger, and M. Schofnegger, "Starkad and poseidon: New hash functions for zero knowledge proof systems.," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 458, 2019.

[139] M. D. Green, J. Katz, A. J. Malozemoff, and H.-S. Zhou, "A unified approach to idealized model separations via indistinguishability obfuscation," in *International Conference on Security and Cryptography for Networks*, Springer, pp. 587–603, 2016.

[140] J. Groth, "A verifiable secret shuffle of homomorphic encryptions," *Journal of Cryptology*, vol. 23, no. 4, pp. 546–579, 2010.

[141] J. Groth, "Short pairing-based non-interactive zero-knowledge arguments," in *ASIACRYPT*, M. Abe, Ed., ser. Lecture Notes in Computer Science, vol. 6477, pp. 321–340, Springer, 2010.

[142] J. Groth, "On the size of pairing-based non-interactive arguments," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 305–326, 2016.

[143] J. Groth, *Homomorphic trapdoor commitments to group elements*, Cryptology ePrint Archive, Report 2009/007, 2009, URL: https://ia.cr/2009/007.

[144] J. Groth and Y. Ishai, "Sub-linear zero-knowledge argument for correctness of a shuffle," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 379–396, 2008.

[145] U. Haböck, A summary on the FRI low degree test. Cryptology ePrint Archive, Paper 2022/1216, URL: https://eprint.iacr.org/2022/1216, 2022.

[146] T. Haines, S. J. Lewis, O. Pereira, and V. Teague, "How not to prove your election outcome," in *2020 IEEE Symposium on Security and Privacy*, pp. 644–660, 2020. DOI: 10.1109/SP40000.2020.00048.

[147] M. Hamburg, "Decaf: Eliminating cofactors through point compression," in *Annual Cryptology Conference*, Springer, pp. 705–723, 2015.

[148] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper, I–III.," *Journal für die reine und angewandte Mathematik*, vol. 175, 1936.

[149] D. Heath and V. Kolesnikov, "Stacked garbling for disjunctive zero-knowledge proofs," in *Advances in Cryptology – EUROCRYPT 2020 – 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part III*, A. Canteaut and Y. Ishai, Eds., ser. Lecture Notes in Computer Science, vol. 12107, pp. 569–598, Springer, 2020.

[150] J. Holmgren and A. Lombardi, "Cryptographic hashing from strong one-way functions (or: One-way product functions and their applications)," in *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, M. Thorup, Ed., pp. 850–858, IEEE Computer Society, 2018.

[151] J. Holmgren, A. Lombardi, and R. D. Rothblum, "Fiat-shamir via list-recoverable codes (or: Parallel repetition of GMW is not zero-knowledge)," in *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, S. Khuller and V. V. Williams, Eds., pp. 750–760, ACM, 2021.

[152] J. Holmgren and R. Rothblum, "Delegating computations with (almost) minimal time and space overhead," in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE, pp. 124–135, 2018.

[153] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, "Zcash protocol specification," *GitHub: San Francisco, CA, USA*, 2016.

[154] Y. E. Housni and A. Guillevic, "Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition," in *International Conference on Cryptology and Network Security*, Springer, pp. 259–279, 2020.

[155] R. Impagliazzo and A. Wigderson, "P= bpp if e requires exponential circuits: Derandomizing the xor lemma," in *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pp. 220–229, 1997.

[156] Y. Ishai, E. Kushilevitz, and R. Ostrovsky, "Efficient arguments without short PCPs," in *22nd Annual IEEE Conference on Computational Complexity (CCC 2007), 13–16 June 2007, San Diego, California, USA*, pp. 278–291, IEEE Computer Society, 2007.

[157] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Zero-knowledge proofs from secure multiparty computation," *SIAM Journal on Computing*, vol. 39, no. 3, pp. 1121–1152, 2009.

[158] R. Jawale, Y. T. Kalai, D. Khurana, and R. Zhang, "SNARGs for bounded depth computations and PPAD hardness from sub-exponential LWE," in *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pp. 708–721, 2021.

[159] M. Jawurek, F. Kerschbaum, and C. Orlandi, "Zero-knowledge using garbled circuits: How to prove non-algebraic statements efficiently," in *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*, A.-R. Sadeghi, V. D. Gligor, and M. Yung, Eds., pp. 955–966, ACM, 2013.

[160] Y. Kalai, "A new perspective on delegating computation," Talk at Workshop on Probabilistically Checkable and Interactive Proofs @ STOC 2017 Theory Fest, 2017.

[161] Y. T. Kalai, G. N. Rothblum, and R. D. Rothblum, "From obfuscation to the security of Fiat-Shamir for proofs," in *Advances in Cryptology – CRYPTO 2017 – 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part II*, J. Katz and H. Shacham, Eds., ser. Lecture Notes in Computer Science, vol. 10402, pp. 224–251, Springer, 2017.

[162] D. Kales, S. Ramacher, C. Rechberger, R. Walch, and M. Werner, "Efficient FPGA implementations of LowMC and picnic," in *Cryptographers' Track at the RSA Conference*, Springer, pp. 417–441, 2020.

[163] D. Kales and G. Zaverucha, "Improving the performance of the picnic signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 154–188, 2020.

[164] A. Kate, G. M. Zaverucha, and I. Goldberg, "Constant-size commitments to polynomials and their applications," in *Advances in Cryptology – ASIACRYPT 2010 – 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5–9, 2010. Proceedings*, M. Abe, Ed., ser. Lecture Notes in Computer Science, vol. 6477, pp. 177–194, Springer, 2010.

[165] A. Kattis, K. Panarin, and A. Vlasov, "Redshift: Transparent snarks from list polynomial commitment iops," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 1400, 2019.

[166] J. Katz, V. Kolesnikov, and X. Wang, "Improved non-interactive zero knowledge with applications to post-quantum signatures," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 525–537, 2018.

[167] J. Katz, C. Zhang, and H.-S. Zhou, *An analysis of the algebraic group model*, Cryptology ePrint Archive, Report 2022/210, URL: https://ia.cr/2022/210, 2022.

[168] J. Kilian, "A note on efficient zero-knowledge proofs and arguments (extended abstract)," in *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, ser. STOC '92, pp. 723–732, New York, NY, USA: ACM, 1992.

[169] A. R. Klivans and D. Van Melkebeek, "Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses," *SIAM Journal on Computing*, vol. 31, no. 5, pp. 1501–1526, 2002.

[170] N. Koblitz and A. J. Menezes, "The random oracle model: A twenty-year retrospective," *Designs, Codes and Cryptography*, vol. 77, no. 2–3, pp. 587–610, 2015.

[171] A. E. Kosba, Z. Zhao, A. Miller, Y. Qian, T.-H. H. Chan, C. Papamanthou, R. Pass, A. Shelat, and E. Shi, "How to use SNARKs in universally composable protocols.," *IACR Cryptol. ePrint Arch.*, vol. 2015, p. 1093, 2015.

[172] A. Kosba, D. Papadopoulos, C. Papamanthou, and D. Song, "MIRAGE: Succinct arguments for randomized algorithms with applications to universal zk-SNARKs," in *USENIX Security Symposium*, 2020.

[173] A. Kosba, Z. Zhao, A. Miller, Y. Qian, H. Chan, C. Papamanthou, R. Pass, A. Shelat, and E. Shi, *C∅C∅: A framework for building composable zero-knowledge proofs*, Cryptology ePrint Archive, Report 2015/1093, 2015.

[174] A. Kothapalli and B. Parno, "Algebraic reductions of knowledge," *Cryptology ePrint Archive*, 2022.

[175] A. Kothapalli, S. Setty, and I. Tzialla, "Nova: Recursive zero-knowledge arguments from folding schemes," in *Annual International Cryptology Conference*, Springer, pp. 359–388, 2022.

[176] D. Kozen, *Theory of Computation*, ser. Texts in Computer Science. Springer, 2006.

[177] E. Kushilevitz and N. Nisan, *Communication Complexity*. New York, NY, USA: Cambridge University Press, 1997.

[178] F. Le Gall, "Powers of tensors and fast matrix multiplication," in *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ACM, pp. 296–303, 2014.

[179] J. Lee, "Dory: Efficient, transparent arguments for generalised inner products and polynomial commitments," in *Theory of Cryptography Conference*, Springer, pp. 1–34, 2021.

[180] F. T. Leighton, *Introduction to Parallel Algorithms and Architectures: Array, Trees, Hypercubes*. Morgan Kaufmann Publishers Inc., 1992.

[181] G. Leurent and T. Peyrin, "SHA-1 is a shambles: First chosen-prefix collision on SHA-1 and application to the PGP web of trust," in *29th USENIX Security Symposium (USENIX Security 20)*, pp. 1839–1856, 2020.

[182] S.-J. Lin, T. Y. Al-Naffouri, Y. S. Han, and W.-H. Chung, "Novel polynomial basis with fast fourier transform and its application to reed-solomon erasure codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6284–6299, 2016, Preliminary version in FOCS 2014.

[183] R. J. Lipton, *Fingerprinting sets*. Princeton University, Department of Computer Science, 1989.

[184] R. J. Lipton, "Efficient checking of computations," in *STACS*, pp. 207–215, 1990.

[185] A. Lombardi and V. Vaikuntanathan, "Correlation-intractable hash functions via shift-hiding," in *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 – February 3, 2022, Berkeley, CA, USA*, M. Braverman, Ed., ser. LIPIcs, vol. 215, 102:1–102:16, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.

[186] C. Lund, L. Fortnow, H. Karloff, and N. Nisan, "Algebraic methods for interactive proof systems," *J. ACM*, vol. 39, pp. 859–868, 1992.

[187] M. Maller, S. Bowe, M. Kohlweiss, and S. Meiklejohn, "Sonic: Zero-knowledge SNARKs from linear-size universal and updatable structured reference strings," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2111–2128, 2019.

[188] U. Maurer, "Abstract models of computation in cryptography," in *IMA International Conference on Cryptography and Coding*, Springer, pp. 1–12, 2005.

[189] U. Maurer, "Unifying zero-knowledge proofs of knowledge," in *International Conference on Cryptology in Africa*, Springer, pp. 272–286, 2009.

[190] O. Meir, "IP = PSPACE using error-correcting codes," *SIAM J. Comput.*, vol. 42, no. 1, pp. 380–403, 2013.

[191] R. Merkle, "Secrecy, authentication, and public key systems," Ph.D. dissertation, Electrical Engineering, Stanford, 1979.

[192] S. Micali, "Computationally sound proofs," *SIAM J. Comput.*, vol. 30, no. 4, pp. 1253–1298, 2000.

[193] P. B. Miltersen and N. V. Vinodchandran, "Derandomizing Arthur–Merlin games using hitting sets," *Computational Complexity*, vol. 14, no. 3, pp. 256–279, 2005.

[194] D. Moshkovitz, "An alternative proof of the Schwartz-Zippel lemma.," in *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 17, p. 96, 2010.

[195] D. Moshkovitz and R. Raz, "Sub-constant error low degree test of almost-linear size," *SIAM J. Comput.*, vol. 38, no. 1, pp. 140–180, 2008.

[196] M. Naehrig, P. S. L. M. Barreto, and P. Schwabe, "On compressible pairings and their computation," in *Progress in Cryptology – AFRICACRYPT 2008*, ser. Lecture Notes in Computer Science, vol. 5023, pp. 371–388, Springer, 2008.

[197] M. Naor, "On cryptographic assumptions and challenges," in *Annual International Cryptology Conference*, Springer, pp. 96–109, 2003.

[198] C. A. Neff, "A verifiable secret shuffle and its application to e-voting," in *Proceedings of the 8th ACM conference on Computer and Communications Security*, pp. 116–125, 2001.

[199] J. B. Nielsen, "Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case," in *Annual International Cryptology Conference*, Springer, pp. 111–126, 2002.

[200] A. Ozdemir, R. Wahby, B. Whitehat, and D. Boneh, "Scaling verifiable computation using efficient set accumulators," in *29th USENIX Security Symposium*, pp. 2075–2092, 2020.

[201] P. Paillier and D. Vergnaud, "Discrete-log-based signatures may not be equivalent to discrete log," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 1–20, 2005.

[202] C. Papamanthou, E. Shi, and R. Tamassia, "Signatures of correct computation," in *Theory of Cryptography Conference*, Springer, pp. 222–242, 2013.

[203] B. Parno, J. Howell, C. Gentry, and M. Raykova, "Pinocchio: Nearly practical verifiable computation," in *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, ser. SP '13, pp. 238–252, Washington, DC, USA: IEEE Computer Society, 2013.

[204] R. Pass, "On deniability in the common reference string and random oracle model," in *Annual International Cryptology Conference*, Springer, pp. 316–337, 2003.

[205] A. Pavan, A. L. Selman, S. Sengupta, and N. V. Vinodchandran, "Polylogarithmic-round interactive proofs for coNP collapse the exponential hierarchy," *Theor. Comput. Sci.*, vol. 385, no. 1-3, pp. 167–178, 2007.

[206] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Annual International Cryptology Conference*, Springer, pp. 129–140, 1991.

[207] C. Peikert and S. Shiehian, "Noninteractive zero knowledge for NP from (plain) learning with errors," in *Advances in Cryptology – CRYPTO 2019 – 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part I*, A. Boldyreva and D. Micciancio, Eds., ser. Lecture Notes in Computer Science, vol. 11692, pp. 89–114, Springer, 2019.

[208] D. Petersen, (URL: https://math.stackexchange.com/users/677/dan-petersen). How to prove that a polynomial of degree n has at most n roots? Mathematics Stack Exchange. URL: https://math.stackexchange.com/q/25831 (version: 2011-03-08).

[209] N. Pippenger, "On the evaluation of powers and monomials," *SIAM Journal on Computing*, vol. 9, no. 2, pp. 230–250, 1980.

[210] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Trans. Inf. Theory*, vol. 24, no. 1, pp. 106–110, 1978.

[211] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

[212] A. Polishchuk and D. A. Spielman, "Nearly-linear size holographic proofs," in *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing, 23–25 May 1994, Montréal, Québec, Canada*, pp. 194–203, 1994.

[213] J. M. Pollard, "Monte Carlo methods for index computation mod *p*," *Mathematics of Computation*, vol. 32, pp. 918–924, 1978.

[214] O. Reingold, G. N. Rothblum, and R. D. Rothblum, "Constant-round interactive proofs for delegating computation," in *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, ser. STOC '16, pp. 49–62, New York, NY, USA: ACM, 2016.

[215] N. Ron-Zewi and R. Rothblum, "Local proofs approaching the witness length," *Electron. Colloquium Comput. Complex.*, vol. 26, p. 127, 2019, Accepted to Foundations of Computer Science (FOCS), 2020.

[216] G. Rothblum, "Delegating computation reliably : Paradigms and constructions," Ph.D. dissertation, Massachusetts Institute of Technology, 2009.

[217] G. N. Rothblum, S. P. Vadhan, and A. Wigderson, "Interactive proofs of proximity: Delegating computation in sublinear time," in *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1–4, 2013*, pp. 793–802, 2013.

[218] R. Rothblum, "The Fiat-Shamir transformation," Talk at The 9th BIU Winter School on Cryptography – Zero Knowledge. 2019. URL: https://www.youtube.com/watch?v=9cagVtYstyY.

[219] R. Rubinfeld and M. Sudan, "Robust characterizations of polynomials with applications to program testing," *SIAM Journal on Computing*, vol. 25, no. 2, pp. 252–271, 1996.

[220] A. D. Sarma, R. J. Lipton, and D. Nanongkai, "Best-order streaming model," in *Proc. Annual Conference on Theory and Applications of Models of Computation*, 2009.

[221] E. B. Sasson, L. Goldberg, S. Kopparty, and S. Saraf, "DEEP-FRI: sampling outside the box improves soundness," in *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12–14, 2020, Seattle, Washington, USA*, T. Vidick, Ed., ser. LIPIcs, vol. 151, pp. 5: 1–5: 32, 2020.

[222] W. J. Savitch, "Relationships between nondeterministic and deterministic tape complexities," *Journal of Computer and System Sciences*, vol. 4, no. 2, pp. 177–192, 1970.

[223] C.-P. Schnorr, "Efficient identification and signatures for smart cards," in *Conference on the Theory and Application of Cryptology*, Springer, pp. 239–252, 1989.

[224] J. T. Schwartz, "Fast probabilistic algorithms for verification of polynomial identities," *J. ACM*, vol. 27, no. 4, pp. 701–717, 1980.

[225] R. Seidel, "On the all-pairs-shortest-path problem in unweighted undirected graphs," *J. Comput. Syst. Sci.*, vol. 51, no. 3, pp. 400–403, 1995.

[226] S. Setty, "Spartan: Efficient and general-purpose zkSNARKs without trusted setup," in *Annual International Cryptology Conference*, Springer, pp. 704–737, 2020.

[227] S. T. V. Setty, B. Braun, V. Vu, A. J. Blumberg, B. Parno, and M. Walfish, "Resolving the conflict between generality and plausibility in verified computation," in *EuroSys*, Z. Hanzálek, H. Härtig, M. Castro, and M. F. Kaashoek, Eds., pp. 71–84, ACM, 2013.

[228] S. T. V. Setty, R. McPherson, A. J. Blumberg, and M. Walfish, "Making argument systems for outsourced computation practical (sometimes)," in *19th Annual Network and Distributed System Security Symposium, NDSS 2012, San Diego, California, USA, February 5–8, 2012*, 2012.

[229] S. Setty, S. Angel, T. Gupta, and J. Lee, "Proving the correct execution of concurrent services in zero-knowledge," in *13th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pp. 339–356, 2018.

[230] S. Setty and J. Lee, *Quarks: Quadruple-efficient transparent zksnarks*, Cryptology ePrint Archive, Report 2020/1275, 2020. URL: https://eprint.iacr.org/2020/1275.

[231] A. Shamir, "IP = PSPACE," *J. ACM*, vol. 39, pp. 869–877, 1992, Preliminary version in STOC 1990.

[232] A. Shen, "IP = PSPACE: Simplified Proof," *J. ACM*, vol. 39, pp. 878–880, 1992.

[233] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, IEEE, pp. 124–134, 1994.

[234] V. Shoup, "Lower bounds for discrete logarithms and related problems," in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 256–266, 1997.

[235] StarkWare, *EthSTARK documentation*, Cryptology ePrint Archive, Paper 2021/582, 2021. URL: https://eprint.iacr.org/2021/582,

[236] H. Sun, H. Sun, K. Singh, A. S. Peddireddy, H. Patil, J. Liu, and W. Chen, *The inspection model for zero-knowledge proofs and efficient zerocash with secp256k1 keys*, Cryptology ePrint Archive, Paper 2022/1079, 2022. URL: https://eprint.iacr.org/2022/1079,

[237] J. Thaler, "Time-optimal interactive proofs for circuit evaluation," in *Proceedings of the 33rd Annual Conference on Advances in Cryptology*, ser. CRYPTO'13, Berlin, Heidelberg: Springer-Verlag, 2013.

[238] J. Thaler, *A note on the GKR protocol*, 2015. URL: http://people.cs.georgetown.edu/jthaler/GKRNote.pdf.

[239] P. Valiant, "Incrementally verifiable computation or proofs of knowledge imply time/space efficiency," in *Theory of Cryptography Conference*, Springer, pp. 1–18, 2008.

[240] A. Vlasov and K. Panarin, "Transparent polynomial commitment scheme with polylogarithmic communication complexity.," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 1020, 2019.

[241] V. Vu, S. T. V. Setty, A. J. Blumberg, and M. Walfish, "A hybrid architecture for interactive verifiable computation," in *2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19–22, 2013*, pp. 223–237, 2013.

[242] R. S. Wahby, Y. Ji, A. J. Blumberg, A. Shelat, J. Thaler, M. Walfish, and T. Wies, "Full accounting for verifiable outsourcing," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp. 2071–2086, 2017.

[243] R. S. Wahby, S. Setty, Z. Ren, A. J. Blumberg, and M. Walfish, "Efficient ram and control flow in verifiable outsourced computation," in *NDSS*, 2015.

[244] R. S. Wahby, I. Tzialla, A. Shelat, J. Thaler, and M. Walfish, "Doubly-efficient zkSNARKs without trusted setup," in *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21–23 May 2018, San Francisco, California, USA*, pp. 926–943, IEEE Computer Society, 2018.

[245] A. Waksman, "A permutation network," *Journal of the ACM*, vol. 15, no. 1, pp. 159–163, 1968.

[246] H. Wee, "On round-efficient argument systems.," in *ICALP*, pp. 140–152, 2005.

[247] H. Wee, "Zero knowledge in the random oracle model, revisited," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 417–434, 2009.

[248] C. Weng, K. Yang, J. Katz, and X. Wang, "Wolverine: Fast, scalable, and communication-efficient zero-knowledge proofs for Boolean and arithmetic circuits," in *2021 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 1074–1091, 2021.

[249] D. Wikström, *Special soundness in the random oracle model*, Cryptology ePrint Archive, Report 2021/1265, URL: https://ia.cr/2021/1265, 2021.

[250] H. Wu, W. Zheng, A. Chiesa, R. A. Popa, and I. Stoica, "DIZK: A distributed zero knowledge proof system," in *27th USENIX Security Symposium* (USENIX Security), pp. 675–692, 2018.

[251] T. Xie, J. Zhang, Y. Zhang, C. Papamanthou, and D. Song, "Libra: Succinct zero-knowledge proofs with optimal prover computation," in *Annual International Cryptology Conference*, Springer, pp. 733–764, 2019.

[252] T. Xie, J. Zhang, Z. Cheng, F. Zhang, Y. Zhang, Y. Jia, D. Boneh, and D. Song, "Zkbridge: Trustless cross-chain bridges made practical," *arXiv preprint arXiv:2210.00264*, 2022.

[253] T. Xie, Y. Zhang, and D. Song, "Orion: Zero knowledge proof with linear prover time," in *Annual International Cryptology Conference*, Springer, pp. 299–328, 2022.

[254] R. Yuster, "Computing the diameter polynomially faster than APSP," *arXiv preprint arXiv:1011.6181*, 2010.

[255] J. Zhang, T. Liu, W. Wang, Y. Zhang, D. Song, X. Xie, and Y. Zhang, "Doubly efficient interactive proofs for general arithmetic circuits with linear prover time," in *CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15–19, 2021*, Y. Kim, J. Kim, G. Vigna, and E. Shi, Eds., pp. 159–177, ACM, 2021.

[256] J. Zhang, T. Xie, Y. Zhang, and D. Song, "Transparent polynomial delegation and its applications to zero knowledge proof," in *2020 IEEE Symposium on Security and Privacy*, IEEE, pp. 859–876, 2020.

[257] Y. Zhang, D. Genkin, J. Katz, D. Papadopoulos, and C. Papamanthou, "A zero-knowledge version of vSQL," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 1146, 2017.

[258] Y. Zhang, D. Genkin, J. Katz, D. Papadopoulos, and C. Papamanthou, "VSQL: Verifying arbitrary SQL queries over dynamic outsourced databases," in *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22–26, 2017*, pp. 863–880, 2017.

[259] Y. Zhang, D. Genkin, J. Katz, D. Papadopoulos, and C. Papamanthou, "VRAM: Faster verifiable RAM with program-independent preprocessing," in *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21–23 May 2018, San Francisco, California, USA*, pp. 908–925, IEEE Computer Society, 2018.

[260] R. Zippel, "Probabilistic algorithms for sparse polynomials," in *EUROSAM*, E. W. Ng, Ed., ser. Lecture Notes in Computer Science, vol. 72, pp. 216–226, Springer, 1979.

[261] ZKProof Community Reference, Version 0.3, 2022. URL: https://docs.zkproof.org/pages/reference/versions/ZkpComRef-0-3.pdf.