Cryptography (Summer 2015)
Final Program Report

Shafi Goldwasser   Tal Rabin (Chair)   Guy N. Rothblum

Note: Numbered citations refer to the list of publications resulting from the program. Alphanumeric citations refer to the bibliography at the end of this report; these latter publications did not result directly from the program.

Modern Cryptography studies settings where adversarial behavior might be a concern, and aims to circumvent such behavior. Recently, powerful technological trends have created new challenges and opportunities for cryptographic research. We are witnessing an explosive growth in online data stored by third-party providers in "the cloud". There are numerous benefits and applications that can be derived from this paradigm. Together with these benefits, there are also new threats and avenues for adversarial interference. As sensitive data and computations migrate to the cloud, the need to simultaneously guarantee privacy, availability of data and correctness of computations is paramount, and the scale of the challenges is greater than ever.

The Cryptography program at the Simons Institute set out to explore the complex and delicate cryptographic challenges imposed by this emerging digital reality. We aimed to develop and promote a paradigm shift in the goals and the thinking of modern cryptography. Moving beyond the traditional goals of cryptography, namely secure and authenticated communication, and towards efficient solutions that address increasingly sophisticated computational settings and adversaries. The program's scientific goals were organized around several themes:

- **Foundational Advancements in Cryptography for The Cloud.** Recent years have seen tremendously exciting cryptographic advances. Most notably, new techniques for fully homomorphic encryption, program obfuscation, verifiable outsourcing of computations, and differentially private data analysis. These new developments constitute significant strides towards addressing the challenges described above. They hold the potential for expanding the scope of cryptography, providing new and previously unimaginable notions, secure solutions, and protections against adversarial behavior.

  Program participants made foundational advances in the study of verifying the correctness of computations delegated to the cloud (see Section 1.1) and in understanding the building blocks of non-malleable cryptography that can provide strong security guarantees in distributed settings and under tampering attacks (see Section 1.5).

- **Towards Securing Computation Efficiently.** In a complementary trend, more mature cryptographic techniques such as secure multi-party computation, garbling circuits and computer programs, and oblivious RAM are seeing significant advances through increasingly efficient solutions, thus enhancing their practical relevance to addressing real-world problems, and holding the potential for solutions and systems that are simultaneously highly efficient, highly secure and highly functional.

Program participants achieved a breakthrough in constructing efficient secure multi-party computation protocols under discrete-log assumptions (see section 1.2), and the community set forth on a foundational study of the bitcoin protocol and its underpinnings (Section 1.4).

- **The Mathematical Underpinnings of Modern Cryptography.** Many recent exciting developments in cryptography have been based upon relatively new computational problems and assumptions relating to classical mathematical structures. Prominent examples include approximation problems on point lattices, their specializations to structured lattices arising in algebraic number theory, and, more speculatively, problems from noncommutative algebra. The cryptography program brought together cryptographers, mathematicians and cryptanalysts to investigate the algorithmic and complexity-theoretic aspects of these new problems, the relations among them, and the cryptographic applications they enable.

  Program participants made exciting progress on understanding the mathematical objects that allow for secure code obfuscation, with several major works and continued progress (see Section 1.3).

- **Community.** The cryptographic community is large, diverse in scientific background and demographics, and geographically scattered. The cryptography program brought together cryptographers at an unprecedented scale with the goal of fostering new collaborations and interactions, facilitating a rapid and productive exchanges of ideas, and building a richer and more vibrant scientific community.

  Considerable effort was dedicated to community-building, and this was an unqualified success. The program fostered new collaborations and connections, and helped to integrate young researchers into the field. See Section 2 for a summary of some of the community-building aspects of the program.

1 Research Highlights

We believe that the cryptography program was a resounding success, and this was echoed by participants' feedback. A huge part of the community studying the theory of cryptography converged at the Simons Institute. Recent developments and new ideas were exchanged and developed at an astounding rate. The scale of the gathering was unprecedented, and we are confident that its impact will continue to unfold in the coming years. The program's deep and broad research impact is already apparent in an array of beautiful results published by program participants in the past year. Participants have identified 185 works tied to the program. We highlight several of the program's most notable achievements below.

1.1 Proof Systems for Delegating Computation

Proof systems allow a powerful prover to prove complex statements to a weak verifier. The power of efficiently-verifiable proof systems is a central question in the study of computation. The P vs. NP question considers the power of "classical" proof systems with deterministic polynomial-time verifiers. Interactive Proofs [GMR89, BM88] revolutionized cryptography and complexity theory by introducing interactive and probabilistic proof verification. A rich literature has studied the power of such proof systems for proving intractable statements to a polynomial-time verifier.

An exciting new frontier in the study of proof systems considers proofs that *can be generated in polynomial time* and verified super-efficiently, e.g. in near-linear time. This study, initiated in [GKR08, GKR15], focuses on proof systems for *tractable* statements, where verifying the proof should require significantly less resources than it would take to resolve the (tractable) statement

Beyond their theoretical importance, such proof systems are also motivated by real-world applications, such as delegating computation. Here, a powerful server can run a computation for a weak client, and provide an interactive proof of the output's correctness, see [GKR15]. This scenario is increasingly relevant in the era of cloud computing.

Constant-Round Interactive Proofs for Delegating Computation. Reingold, Rothblum and Rothblum [174] obtained a breakthrough in the study of interactive proofs. They showed that every statement that can be evaluated in polynomial time and bounded-polynomial space has an interactive proof that satisfies strict efficiency requirements: (1) the honest prover runs in polynomial time, (2) the verifier is almost linear time (even sublinear under some conditions), and (3) the interaction consists of only a *constant number of communication rounds*. Prior to this work, very little was known about the power of efficient, constant-round interactive proofs. Their work represents significant progress on the round complexity of interactive proofs (even if we ignore the running time of the honest prover), and on the expressive power of interactive proofs with polynomial-time honest prover (even if we ignore the round complexity). This result has several applications, and in particular it can be used for verifiable delegation of computation.

Even beyond this powerful bottom-line guarantee, the work made exciting strides in the study of probabilistic proof systems. The construction leverages several new notions of interactive proofs, which are of independent interest and will (we believe) lead to further study and progress. They also formalize a goal of *amortized proof verification*: designing proof systems for verifying the correctness of k statements much more efficiently than can be done via k independent verifications. They show general theorems for amortizing the verification of rich families of interactive proofs.

This work appeared in STOC 2016, and was invited to the SIAM Journal on Computing special issue for that conference.

Other Highlights. Kalai, Rothblum and Rothblum [136] used recent advances in the study of code obfuscation to present the first family of hash functions that can be used to securely instantiate the Fiat-Shamir methodology [FS86], giving an automatic compiler for reducing interaction in proof systems. Dwork, Naor and Rothblum [93] studied the so-called "spooky" compiler for reducing interaction [ABOR00], showing positive and negative results on instantiating the compiler with standard cryptographic assumptions. Dodis, Halevi, Rothblum and Wichs [85] also studied the spooky compiler and its applicability to multi-prover interactive proof systems. They constructed "spooky encryption schemes", which can be used to make the compiler fail (and also for positive applications), thus resolving another long-standing open question.

1.2 Succinct Secure Computation

Secure computation is a powerful cryptographic tool that enables distrustful parties to jointly emulate the correctness and privacy guarantees of a trusted third party. This provides a means for computing across data owned by separate entities who are unwilling to reveal the data itself, as well as providing a line of defense for data owned by a single individual, company, or government, by requiring attackers to compromise multiple separate entities in order to breach security.

Since the seminal feasibility results of the 1980s [Yao86, GMW87, BGW88, CCD88], a major challenge in the area of secure computation has been to break the asymptotic "circuit-size barrier." This barrier refers to the fact that all classical techniques for secure computation required a larger amount of communication than the size of a boolean circuit representing the function to be computed, even when the circuit is much bigger than the inputs. The circuit size barrier applied not only to general circuits, but also to useful restricted classes of circuits such as boolean formulas or branching programs.

The one exception to this emerged in 2009, based on a breakthrough in fully homomorphic encryption (FHE) [RAD78, Gen09]. FHE enables local computations on encrypted inputs, thus providing a general-purpose solution to the problem of low-communication secure computation. However, on the down side, even the best known implementations of FHE [HS15, DM15, CGGI16] are still quite slow. Moreover, while there has been significant progress on basing the feasibility of FHE on more standard or different assumptions [vDGHV10, BV14, GSW13], the set of cryptographic assumptions on which FHE can be based is still very narrow, and in particular it does not include any of the assumptions based on hardness of factoring or the discrete logarithm problem.

Breaking the Circuit-Size Barrier in Secure Computation Under DDH. Program participants Boyle, Gilboa, and Ishai [50] showed how to break the circuit-size communication barrier in secure computation for a large class of functions based on *discrete logarithm type* assumptions. These group-based techniques constitute a completely different mathematical structure from the lattices that underly all known approaches to FHE and succinct secure computation. Their work was given the Best Paper Award at CRYPTO 2016.

More specifically, the work obtained the following applications from the Decisional Diffie-Hellman (DDH) assumption: (1) A secure 2-party computation protocol for evaluating any branching program or formula of size S, where the communication complexity is linear in the input size (and only the running time grows with S), (2) A secure 2-party computation protocol for evaluating leveled boolean circuits of size S with sublinear communication complexity $O(S/\log S)$, and (3) A 1-round 2-server private information retrieval scheme supporting general private database searches expressed by branching programs.

Perhaps most exciting about the work is that it provides a new approach to secure computation design: Homomorphic secret sharing (HSS). HSS is a relaxed form of FHE which enables homomorphic evaluation on a secret input *split* across two parties; it is a dual notion to function secret sharing [51], which was the topic of a reading group presentation at the Simons Cryptography program that sparked many relevant discussions toward this result and others.

1.3 The Building-Blocks of Code Obfuscation

Program Obfuscation. Program obfuscation aims to use software to emulate black-box hardware for hiding secrets and comptuations over secrets. Strong notions of obfuscation notion are known to be unattainable [BGI$^+$12]. Recent breakthroughs, however, have shown that a weaker notion of program obfuscation, known as *Indistinguishability Obufscation* (IO), is potentially achievable [GGH$^+$13b], and has fantastic cryptographic applications (starting with [SW14]).

However, so far, the existence of IO itself remains uncertain. Prior to the Simons cryptography program, all candidate IO constructions were based on so-called *graded encodings* [GGH13a], an abstract framework of algebraic structures. Graded encodings allow for the evaluation of *high (polynomial) degree* polynomials over secret encoded values, revealing only whether the output is zero. Furthermore, the security of these IO constructions rely on strong assumptions on graded encoding schemes. Despite extensive efforts to instantiate graded encodings from integer lattices, vulnerabilities were demonstrated in all instantiations proposed thus far.

IO from Constant-Degree Graded Encodings. Therefore, understanding "*what objects and assumptions are sufficient for achieving IO?*" is a central question in the theory of cryptography. During the Simons summer program, Lin [150] took an exciting step and showed that to achieve IO, we do not necessarily need the full power of general graded encodings: a much weaker version, called *constant-degree* graded encodings, suffice. Constant-degree graded encodings only support the evaluation of *constant-degree* polynomials (her work also assumes the existence of pseudo-random generators with constant locality and polynomial stretch, as well as the hardness of learning with errors). This paper received a Best Paper Honorable Mention at the Eurocrypt 2016 conference (awarded to the top three submissions to that conference). Soon after that, Lin and Vaikuntanathan [152] presented a new IO construction whose security was based on a much weaker assumption on constant-degree graded encodings. This assumption is in the sprit of the classical Decisional Diffie-Hellman (DDH) assumption.

The two above works significantly simplified and weakened the objects and assumptions needed for achieving IO, and natually led us to the question "*how much can we narrow the gap between objects and assumptions that imply IO, and well-studied ones?*" In particular, *bilinear pairing groups*, well-studied mathematical objects, are themselves a weak version of graded encodings, which support evaluation of only *quadratic* polynomials. Two very recent works by program participants [AS16, Lin16] make further strides in narrowing the above gap. They show that graded encodings for just *degree-5* polynomials already suffice for achieving IO (assuming also the existence of pseudo-random generators with output locality 5 and the hardness of learning with errors). In particular, Lin's construction [Lin16] relies on a direct generalization of bilinear pairing groups to degree 5, with the classical DDH assumption.

We believe that these works will lead to further progress in simplifying and weakening the objects and assumptions that imply IO, deepening our understanding of this fundamental object, and moving towards the eventual goal of basing the existence of IO on well-studied assumptions.

Cryptanalysis of Multilinear Maps. Cryptographic multilinear maps (aka graded encoding) are recent and very powerful cryptographic tools. During the special semester in Simons we worked on constructing and breaking recent constructions. Several variations on existing schemes were described in by Halevi [120] Some new variants that we were considered were quickly broken by Brakersky *et al.* [57]. Also the work done as part of the cryptogrpahy program formed the basis for the work on "Annihilation attacks for multilinear maps" by Miles, Sahai and Zhandry [160], which are currently the most potent form of attacks on GGH13-based constructions.

1.4 Moderate Hardness and Its Applications

A new direction fostered and expanded in the program was studying moderate cryptographic hardness and it's applications, especially in light of the recent widepsread adoption of the bitcoin protocol, originally proposed by Nakamoto [Nak08, Nak09]. This burgeoning literature studies the bitcoin protocol itself, models its security properties, suggests alternatives, and considers the theoretical underpinning of moderate hardness.

Analyzing the bitcoin backbone. Studying the security properties of the bitcoin protocol itself has emerged as a central challenge for cryptography. The bitcoin protocol is described by its implementation and, as such, is hard to analyze directly. For this reason, Garay, Kiayias and Leonardos [GKL15] extracted its core consensus building component, the bitcoin "backbone", and then presented an analysis from a provable security point of view. The introduced a formal adversarial model, relevant security properties, and proof techniques suitable for arguing the security of the protocol. Importantly, an explicit problem statement was now available: a blockchain protocol is secure if it satisfies two properties called *persistence* and *liveness*; security properties of the blockchain data structure were also put forth, called *common prefix* and *chain quality*. This work left open a number of questions that were tackled in the course of the program. For instance, Kiayias and Panagiotakos [KP15] studied the necessary requirements for proving persistence and liveness, while Pass, Seeman and Shelat, [PSS16], extended the adversary to the semi-synchronous setting. Finally, the analysis of one of the most intricate aspects of the bitcoin implementation, the way the protocol adjusts itself to accommodate an evolving population of participants was analyzed by Garay, Kiayias and Leonardos in [GKL16].

Alternative blockchain protocols. The above results have provided an initial outline of the problem of blockchain protocol design and in this way motivated further questions regarding the optimality of the bitcoin protocol as a solution to that problem. In this direction, Kiayias and Panagiotakos [KP16] studied the GHOST rule for reaching consensus in blockchain protocols and introduced new proof techniques that take into account trees of blocks (as opposed to chains). Pass and Shi [170] put forth a new blockchain protocol that has a *fair chain* property. This thwarts attacks like "selfish mining", which affect the reward mechanism of the bitcoin blockchain. A second protocol by Pass and Shi [171] scales better than bitcoin, and does so by adopting an innovative hybrid approach.

Memory hard functions. *Proofs of Work* [DN92] are at the core of many blockchain protocols. An important primitive for realizing proofs of work is memory hard functions such as "scrypt." Analyses of memory hard functions often use tools from graph pebbling, as pioneered by [DGN03]. Alwen, Chen, Kamath, Kolmogorov, Pietrzak, and Tessaro [8] proved the memory hardness of Scrypt under a set of well defined assumptions. Subsequently, program participants Alwen and Blocki, [7], put forth techniques for analyzing the security of practical memory hard functions and presented attacks against recent proposals for such functions including Argon2i and Balloon Hashing.

1.5 Non-Malleable Cryptography

The goal of non-malleable cryptography is developing the tools and techniques required to secure computer systems against tampering attacks. Non-malleable commitments [DDN91] require that a man-in-the-middle (MIM) attacker should not be able to tamper with a given commitment and produce a commitment to a related value. Commitments are often used as the paragon example for non-malleable primitives because of their ability to almost "universally" secure higher-level protocols against MIM attacks. Non-malleable commitments have been foundational to designing round-efficient secure computation protocols, secure computation protocols over the internet, and even in areas as diverse as position-based cryptography. Somewhat surprisingly, techniques from the area of non-malleable commitments have even found application is designing information theoretic objects such non-malleable extractors and codes [CGL16], which in turn, have been found useful in resolving a long-standing open problem regarding designing two-source randomness extractors [CZ16]. A key measure of efficiency for non-malleable commitments is the number of rounds (i.e., the number of messages exchanged) the commitment protocol requires. Over the past two decades, several work have studied the round complexity of non-malleable commitments.

Program participants Goyal, Pandey, and, Richelson [116] obtained a new protocol with the following features, resolving a long standing open problem.

- The protocol has only *three rounds* of interaction. Pass [Pas13] showed an impossibility result for a two-round non-malleable commitment scheme w.r.t. a black-box reduction to any "standard" intractability reduction. Thus, this resolves the round complexity of non-malleable commitment at least w.r.t. black-box security reductions. Their construction is secure as per the standard notion of non-malleability w.r.t. commitment.

- Their protocol is truly efficient. In their basic protocol, the entire computation of the committer is dominated by just three invocations of a non-interactive statically binding commitment scheme, while, the receiver computation (in the commitment stage) is limited to just sampling a random string. Unlike many previous works, they directly construct a protocol for large tags and hence avoid any non-malleability amplification steps.

- Their basic protocol is based on a black-box use of any non-interactive statistically binding commitment scheme. Such schemes, in turn, can be based on any one-to-one one-way function (or any one-way function at the cost of an extra initialization round). The basic protocol is secure against synchronizing adversaries, which is sufficient in application like secure multi-party computation. The construction against general adversaries requires a slightly stronger assumption and a higher number of invocations of the underlying commitment scheme.

- Their construction is public-coin and makes use of only black-box simulation. Prior to their work, no public-coin constant round non-malleable commitment schemes were known based on black-box simulation.

The techniques used are of independent interest as well. As a main technical tool, they rely on non-malleable codes in the split state model. In addition, they also present a (different) simple construction of constant-round non-malleable commitments from any one-way function. While this result is not new, the main feature is its simplicity compared to *any* previous construction of non-malleable commitments (in any number of rounds). The simple construction uses non-malleable codes in the split state model in a black-box way.

Given the lower bound of Pass [Pas13], three rounds could be considered to be a natural "barrier" on the round efficiency of non-malleable commitments. In their recent work, Goyal, Khurana, and, Sahai [115] construct only two-round non-malleable commitments, thus bypassing this barrier. Their protocol consists of two unidirectional messages by the committer (with no message from the receiver), and is secure against all polynomial-time adversaries in the synchronous setting. The protocol assumes only one-to-one one-way functions and achieves the notion of non-malleability w.r.t. opening. Their techniques depart significantly from the commit-challenge-response structure followed by nearly all prior works on non-malleable protocols in the standard model. In addition, the techniques gives renewed hope that a non-interactive (i.e., 1-round) non-malleable commitment scheme may finally be within reach.

2 Program Activities

The program was anchored by a successful "Bootcamp", offering a whirlwind tour of the latest and greatest developments in the field, as well as workshops on "Securing Computation" and "The Mathematics of Cryptography", developing the themes outlined above. These were all extremely well attended. Throughout the program, the Simons Institute was positively buzzing with scientific activity. On most days, every corner of the building was taken over by different groups working on exciting new projects and collaborations. While much of this energetic activity was unstructured, several structured activities added richness and depth to the program.

- **Historical Papers.** This weekly series consisted of talks about seminal papers that had, and continue to have, long-lasting impact in cryptography and beyond. The talks discussed not only the works themselves, but also their historical context and, more broadly, the field's evolution and the works' impact both in and out of cryptography. The talks were recorded and accessible to a wide audience.
- **Reading Groups: Cryptography, Obfuscation, Differential Privacy.** A weekly (and occasionally twice-weekly) reading group encompassed talks on wide-ranging topics in cryptography. A second weekly reading group focused on differential privacy. Shai Halevi organized an obfuscation reading group, whose goal was to fish out a simple obfuscation construction from the literature at that time that is implementable. These reading groups were well-attended and successfully provided a venue for participants to delve deeper into specific questions and results.
- **Student and Fellows lunches.** A weekly lunch provided an opportunity for students to network with the more senior programs participants. Small groups of students were randomly assigned to share a table with an experienced researcher, providing them with a valuable opportunity to receive guidance and advice, and to network among themselves. The weekly fellows lunch provided an excellent venue for the fellows to get to learn about each others' work, building collaborations and community.
- **Student Mentoring.** An initiative by program participant Alon Rosen brought together students and senior researchers to discuss interesting papers in the format of a one-on-one (or many-on-one) presentation and conversation. This facilitated interactions between participants and provided an opportunity for the students and the researchers to get to know each other and a new topic.

Finally, a reunion workshop in August 2016 showcased the deep and broad scientific contributions made by program participants. The emphasis was on "deep dives" into central results, but all participants had an opportunity to present their works. Two panel discussions generated set the stage for discussion and contemplation of progress made and directions for the future. Most importantly, this workshop provided ample opportunities for new and continued collaborations, setting the stage for further scientific progress.

3 Acknowledgements

We thank Elette Boyle, Vipul Goyal, Shai Halevi, Aggelos Kiayias and Huijia (Rachel) Lin for contributing to the writing of this report.

References

[ABOR00] William Aiello, Sandeep N. Bhatt, Rafail Ostrovsky, and Sivaramakrishnan Rajagopalan. Fast verification of any remote procedure call: Short witness-indistinguishable one-round proofs for NP. In *ICALP*, pages 463–474, 2000.

[AS16] Prabhanjan Ananth and Amit Sahai. Projective arithmetic functional encryption and indistinguishability obfuscation from degree-5 multilinear maps. Cryptology ePrint Archive, Report 2016/1097, 2016. `http://eprint.iacr.org/2016/1097`.

[BGI+12] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. *J. ACM*, 59(2):6, 2012.

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *STOC*, pages 1–10, 1988.

[BM88] László Babai and Shlomo Moran. Arthur-merlin games: A randomized proof system, and a hierarchy of complexity classes. *JCSS*, 36(2):254–276, 1988.

[BV14] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. *SIAM J. Comput.*, 43(2):831–871, 2014.

[CCD88] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *STOC*, pages 11–19, 1988.

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Proceedings, Part I*, pages 3–33, 2016.

[CGL16] Eshan Chattopadhyay, Vipul Goyal, and Xin Li. Non-malleable extractors and codes, with their many tampered extensions. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 285–298, 2016.

[CZ16] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 670–683, 2016.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, pages 542–552, 1991.

[DGN03] Cynthia Dwork, Andrew V. Goldberg, and Moni Naor. On memory-bound functions for fighting spam. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 426–444, 2003.

[DM15] Léo Ducas and Daniele Micciancio. FHEW: bootstrapping homomorphic encryption in less than a second. In *Advances in Cryptology - EUROCRYPT 2015, Proceedings*, pages 617–640, 2015.

[DN92] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, pages 139–147, 1992.

[FS86] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*, pages 186–194, 1986.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *STOC*, pages 169–178, 2009.

[GGH13a] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In *EUROCRYPT*, pages 1–17, 2013.

[GGH+13b] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *FOCS*, pages 40–49, 2013.

[GKL15] Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. 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*, pages 281–310, 2015.

[GKL16] Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol with chains of variable difficulty. Cryptology ePrint Archive, Report 2016/1048, 2016. `http://eprint.iacr.org/2016/1048`.

[GKR08] Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum. Delegating computation: interactive proofs for muggles. In *STOC*, pages 113–122, 2008. To appear in *J. ACM*.

[GKR15] Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum. Delegating computation: Interactive proofs for muggles. *J. ACM*, 62(4):27:1–27:64, 2015.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *STOC*, pages 218–229, 1987.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, pages 75–92, 2013.

[HS15] Shai Halevi and Victor Shoup. Bootstrapping for helib. 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 I*, pages 641–670, 2015.

[KP15] Aggelos Kiayias and Giorgos Panagiotakos. Speed-security tradeoffs in blockchain protocols. *IACR Cryptology ePrint Archive*, 2015:1019, 2015.

[KP16] Aggelos Kiayias and Giorgos Panagiotakos. On trees, chains and fast transactions in the blockchain. *IACR Cryptology ePrint Archive*, 2016:545, 2016.

[Lin16] Huijia Lin. Indistinguishability obfuscation from ddh on 5-linear maps and locality-5 prgs. Cryptology ePrint Archive, Report 2016/1096, 2016. `http://eprint.iacr.org/2016/1096`.

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf, 2008.

[Nak09] Satoshi Nakamoto. Bitcoin open source implementation of p2p currency. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source, February 2009.

[Pas13] Rafael Pass. Unprovable security of perfect NIZK and non-interactive non-malleable commitments. In *TCC*, pages 334–354, 2013.

[PSS16] Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the blockchain protocol in asynchronous networks. *IACR Cryptology ePrint Archive*, 2016:454, 2016.

[RAD78] Ronald L. Rivest, Len Adleman, and Michael L. Dertouzos. On data banks and privacy homomorphisms. In *Foundations of secure computation (Workshop, Georgia Inst. Tech., Atlanta, Ga., 1977)*, pages 169–179. Academic, New York, 1978.

[SW14] Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 475–484, 2014.

[vDGHV10] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In *Advances in Cryptology - EUROCRYPT 2010. Proceedings*, pages 24–43, 2010.

[Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In *FOCS*, pages 162–167, 1986.

Cryptography, Summer 2015

[1] D. AGGARWAL, S. AGRAWAL, D. GUPTA, H. K. MAJI, O. PANDEY, and M. PRABHAKARAN. Optimal Computational Split State Non-malleable Codes. In submission.
[2] S. AGRAWAL, M. PRABHAKARAN, and C.-H. YU. Virtual Grey-Boxes Beyond Obfuscation: A Statistical Security Notion for Cryptographic Agents. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[3] S. AGRAWAL. Interpolating Predicate and Functional Encryption from Learning With Errors. *IACR Cryptology ePrint Archive 2016/654,* 2016.
[4] S. AGRAWAL. Functional Encryption for Bounded Collusions, Revisited. *IACR Cryptology ePrint Archive 2016/361,* 2016.
[5] S. AGRAWAL, B. LIBERT, and D. STEHLÉ. Fully secure functional encryption for inner products, from standard assumptions. In *Advances in Cryptology -- CRYPTO*, 2016.
[6] J. ALWEN and J. BLOCKI. Efficiently computing data-independent memory-hard functions. In *Advances in Cryptology -- CRYPTO*, 2016.
[7] J. ALWEN and J. BLOCKI. Towards practical attacks on argon2i and balloon hashing. *Cryptology ePrint Archive, Report 2016/759,* 2016.
[8] J. ALWEN, B. CHEN, C. KAMATH, V. KOLMOGOROV, K. PIETRZAK, and S. TESSARO. On the complexity of scrypt and proofs of space in the parallel random oracle model. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 358–387, 2016.
[9] J. ALWEN, R. OSTROVSKY, H.-S. ZHOU, and V. ZIKAS. Incoercible Multi-party Computation and Universally Composable Receipt-Free Voting. In *Advances in Cryptology -- CRYPTO*, vol. 2, pp. 763–780, 2015.
[10] P. ANANTH, Y.-C. CHEN, K.-M. CHUNG, H. LIN, and W.-K. LIN. Delegating RAM computations with adaptive soundness and privacy. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[11] P. ANANTH, A. COHEN, and A. JAIN. Cryptography with Updates. Manuscript, in preparation.
[12] P. ANANTH, A. JAIN, M. NAOR, A. SAHAI, and E. YOGEV. Universal constructions and robust combiners for indistinguishability obfuscation and witness encryption. In *Advances in Cryptology -- CRYPTO*, pp. 491–520, 2016.
[13] P. ANANTH, A. JAIN, and A. SAHAI. Patchable Indistinguishability Obfuscation: iO for Evolving Software. Manuscript, in preparation.
[14] P. ANANTH, A. JAIN, and A. SAHAI. Patchable obfuscation. *Cryptology ePrint Archive, Report 2015/1084,* 2015.
[15] P. ANANTH, A. JAIN, and A. SAHAI. Achieving Compactness Generically: Indistinguishability Obfuscation from Non-Compact Functional Encryption. Manuscript. 2015. Available at https://eprint.iacr.org/2015/730.pdf.
[16] D. APON, X. FAN, and F.-H. LIU. Bi-deniable inner product encryption from LWE. *IACR Cryptology ePrint Archive, 2015/993,* 2015.
[17] D. APON, X. FAN, and F.-H. LIU. Deniable Attribute Based Encryption for Branching Programs from LWE. In preparation.
[18] B. APPLEBAUM. On the Complexity of Collision Resistance Hash Functions. In preparation.
[19] B. APPLEBAUM. From Private Simultaneous Messages to Zero-Information Arthur-Merlin Protocols and Back. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, 2016.
[20] B. APPLEBAUM. On the Relationship between Non-Interactive Statistical Zero-Knowledge and Randomized Encodings. In *Advances in Cryptology -- CRYPTO*, 2016.
[21] F. ARMKNECHT, D. MORIYAMA, A.-R. SADEGHI, and M. YUNG. Towards a unified security model for physically unclonable functions. In *Cryptographers' Track at the RSA Conference (CT-RSA)*, pp. 271–287, 2016.
[22] P. D. AZAR, S. GOLDWASSER, and S. PARK. How to Incentivize Data-Driven Collaboration Among Competing Parties. In *Proceedings of the 7th Annual Innovations in Theoretical Computer Science (ITCS)*, pp. 213–225, 2016.
[23] S. BADRINARAYANAN, E. MILES, A. SAHAI, and M. ZHANDRY. Post-Zeroizing Obfuscation: new mathematical tools, and the case of evasive circuits. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 764–791, 2016.
[24] M. BALL, D. DACHMAN-SOLED, M. KULKARNI, and T. MALKIN. Non-Malleable Codes for Bounded Depth, Bounded Fan-In Circuits. In *Proceedings of the 35th Annual International Conference on the Theory and*

Applications of Cryptographic Techniques (EUROCRYPT), pp. 881–908, 2016.
[25] M. BALL, T. MALKIN, and M. ROSULEK. Garbling Gadgets for Boolean and Arithmetic Circuits. In *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)*, 2016.
[26] A. BEIMEL, A. GABIZON, Y. ISHAI, and E. KUSHILEVITZ. Distribution Design. In *Proceedings of the 7th Annual Innovations in Theoretical Computer Science (ITCS)*, 2016.
[27] A. BEIMEL, Y. ISHAI, and E. KUSHILEVITZ. Ad hoc PSM protocols. In preparation.
[28] M. BELLARE, D. J. BERNSTEIN, and S. TESSARO. Hash-function based PRFs: AMAC and its multi-user security. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 566–595, 2016.
[29] M. BELLARE, G. FUCHSBAUER, and A. SCAFURO. NIZKs with an Untrusted CRS: Security in the Face of Parameter Subversion. In *Proceedings of the 22nd Annual International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT)*, 2016.
[30] M. BELLARE and A. LYSYANSKAYA. Symmetric and Dual PRFs from Standard Assumptions: A Generic Validation of an HMAC Assumption. *Cryptology ePrint Archive Report 2015/1198,* 2015.
[31] M. BELLARE and I. STEPANOVS. Point-function obfuscation: a framework and generic constructions. In *Theory of Cryptography Conference*, pp. 565–594, 2016.
[32] M. BELLARE, I. STEPANOVS, and S. TESSARO. Contention in Cryptoland: Obfuscation, Leakage and UCE. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, pp. 542–564, 2016.
[33] A. BENIN, S. TOLEDO, and E. TROMER. Secure Association for the Internet of Things. In *International Workshop on Secure Internet of Things (SIOT)*, pp. 25–34, 2015.
[34] A. BISHOP, V. PASTRO, R. RAJARAMAN, and D. WICHS. Essentially optimal robust secret sharing with maximal corruptions. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 58–86, 2016.
[35] N. BITANSKY, Z. BRAKERSKI, Y. KALAI, O. PANETH, and V. VAIKUNTANATHAN. 3-Message Zero Knowledge Against Human Ignorance. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[36] N. BITANSKY, A. DEGWEKAR, and V. VAIKUNTANATHAN. Structure vs Hardness through the Obfuscation Lens. Preprint. 2016.
[37] N. BITANSKY, S. GOLDWASSER, A. JAIN, O. PANETH, V. VAIKUNTANATHAN, and B. WATERS. Time-lock puzzles from randomized encodings. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science (ITCS)*, pp. 345–356, 2016.
[38] N. BITANSKY, O. PANETH, and D. WICHS. Perfect Structure on the Edge of Chaos. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, 2016.
[39] N. BITANSKY and V. VAIKUNTANATHAN. Indistinguishability Obfuscation: from Approximate to Exact. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, 2016.
[40] J. BLOCKI. Client CASH. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (AsiaCCS)*, 2016.
[41] J. BLOCKI, A. DATTA, and J. BONNEAU. Differentially Private Password Frequency Lists. In *Proceedings of the Networking and Distributed System Security Symposium (NDSS)*, 2016.
[42] J. BLOCKI and A. DATTA. CASH: A Cost Asymmetric Secure Hash Algorithm for Optimal Password Protection. In *Proceedings of the Computer Security Foundations Symposium (CSF)*, 2016.
[43] J. BLOCKI and H. ZHOU. Designing Proof of Human-work Puzzles for Cryptocurrency. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[44] J. BLOCKI and V. ZIKAS. Modeling Password Attacks using Rational Protocol Design. In preparation.
[45] A. BOGDANOV, S. GUO, D. MASNY, S. RICHELSON, and A. ROSEN. On the Hardness of Learning with Rounding over Small Modulus. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, 2016.
[46] A. BOGDANOV, Y. ISHAI, E. VIOLA, and C. WILLIAMSON. Bounded Indistinguishability and the Complexity of Recovering Secrets. In *Advances in Cryptology -- CRYPTO*, 2016.
[47] D. BONEH. Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks. In *Proceedings of the 22nd Annual International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT)*, 2016.
[48] D. BONEH, K. LEWI, and D. J. WU. Constraining Pseudorandom Functions Privately. *IACR Cryptology ePrint Archive, 2015/1167,* 2015.
[49] E. BOYLE, K.-M. CHUNG, and R. PASS. Oblivious Parallel RAM and Applications. In *Proceedings of the 13th*

Theory of Cryptography Conference (TCC-A), 2016.
[50] E. BOYLE, N. GILBOA, and Y. ISHAI. Breaking the Circuit-Size Barrier Under DDH. In *Advances in Cryptology -- CRYPTO*, 2016. Best paper award.
[51] E. BOYLE, N. GILBOA, and Y. ISHAI. Function Secret Sharing: Improvements and Extensions. In *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)*, 2016.
[52] E. BOYLE, Y. ISHAI, and A. POLYCHRONIADOU. Limits of Practical Sublinear Secure Computation. Manuscript. 2016.
[53] E. BOYLE, A. JAIN, M. PRABHAKARAN, and C.-H. YU. Communication Complexity of Large-Scale Multiparty Computation. Manuscript. 2016.
[54] E. BOYLE and M. NAOR. Is there an Oblivious RAM Lower Bound? In *Proceedings of the 7th Annual Innovations in Theoretical Computer Science (ITCS)*, pp. 357–368, 2016.
[55] E. BOYLE and R. PASS. Limits of Extractability Assumptions with Distributional Auxiliary Input. In *Proceedings of the 10th ACM on Asia Conference on Computer and Communications Security (AsiaCCS)*, 2015.
[56] Z. BRAKERSKI, D. CASH, R. TSABARY, and H. WEE. Targeted Homomorphic Attribute Based Encryption. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[57] Z. BRAKERSKI, C. GENTRY, S. HALEVI, T. LEPOINT, A. SAHAI, and M. TIBOUCHI. Cryptanalysis of the Quadratic Zero-Testing of GGH. *Cryptology ePrint Archive, Report 2015/845,* 2015.
[58] Z. BRAKERSKI, V. VAIKUNTANATHAN, H. WEE, and D. WICHS. Obfuscating conjunctions under entropic ring LWE. In *Proceedings of the 7th Annual Innovations in Theoretical Computer Science (ITCS)*, pp. 147–156, 2016.
[59] R. CANETTI, Y. CHEN, J. HOLMGREN, and M. RAYKOVA. Adaptive Succinct Garbled RAM or: How To Delegate Your Database. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[60] R. CANETTI, Y. CHEN, and L. REYZIN. On the Correlation Intractability of Obfuscated Pseudorandom Functions. *IACR Cryptology ePrint Archive,* 334, 2015.
[61] R. CANETTI and J. HOLMGREN. Fully succinct garbled RAM. In *Proceedings of the 7th Annual Innovations in Theoretical Computer Science (ITCS)*, pp. 169–178, 2016.
[62] R. CANETTI, O. POBURINNAYA, and M. RAYKOVA. Optimal-Rate Non-Committing Encryption in a CRS Model. *IACR Cryptology ePrint Archive 2016/511,* 2016.
[63] D. CASH, P. GRUBBS, J. PERRY, and T. RISTENPART. Leakage-Abuse Attacks Against Searchable Encryption CCS 2015. In *Proceedings of the 2015 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2015.
[64] D. CASH, E. KILTZ, and S. TESSARO. Two-round man-in-the-middle security from LPN. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, pp. 225–248, 2016.
[65] S. CHAKRABORTY, G. PAUL, and C. P. RANGAN. Forward-Secure Authenticated Symmetric Key Exchange Protocols: New Security Model and Secure Constructions. In *The 9th International Conference on Provable Security (ProvSec)*, pp. 149–166, 2015.
[66] H. CHAN, K. CHUNG, W.-K. LIN, F. LIU, R. PASS, and E. SHI. Circuit OPRAM: Tight Upper and Lower Bounds for Oblivious Parallel RAM. In preparation.
[67] B. CHEN, H. LIN, and S. TESSARO. Oblivious Parallel RAM: Improved Efficiency and Generic Constructions. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, 2016.
[68] K.-M. CHUNG, Y.-C. CHEN, S. S. M. CHOW, R. W. F. LAI, W.-K. LIN, and H.-S. ZHOU. Cryptography for Parallel RAM from Indistinguishability Obfuscation. In *The 7th Annual Innovations in Theoretical Computer Science (ITCS)*, 2016.
[69] M. CIAMPI, R. OSTROVSKY, L. SINISCALCHI, and I. VISCONTI. Concurrent Non-Malleable Commitments (and More) in 3 Rounds. In *Advances in Cryptology -- CRYPTO*, 2016.
[70] M. CIAMPI, G. PERSIANO, A. SCAFURO, L. SINISCALCHI, and I. VISCONTI. Improved OR-Composition of Sigma-Protocols. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, pp. 112–141, 2016.
[71] M. CIAMPI, G. PERSIANO, A. SCAFURO, L. SINISCALCHI, and I. VISCONTI. Online/Offline OR Composition of Sigma Protocols. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, 2016.
[72] A. COHEN, J. HOLMGREN, R. NISHIMAKI, V. VAIKUNTANATHAN, and D. WICHS. Watermarking Cryptographic Capabilities. In *Proceedings of the 48th Annual Symposium on the Theory of Computing (STOC)*, 2016.

[73] A. COHEN and S. KLEIN. The GGM Function Family is a Weakly One-Way Family of Functions. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[74] R. COHEN, S. CORETTI, J. GARAY, and V. ZIKAS. Probabilistic Termination and Composability of Cryptographic Protocols. In *Advances in Cryptology -- CRYPTO*, pp. 240–269, 2016.
[75] S. CORETTI, J. GARAY, M. HIRT, and V. ZIKAS. Constant-Round Asynchronous Multi-Party Computation. In *Proceedings of the 22nd Annual International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT)*, 2016.
[76] D. DACHMAN-SOLED. Towards Non-Black-Box Separations of Public Key and Symmetric Key Encryption. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[77] D. DACHMAN-SOLED. Leakage-Resilient Public-Key Encryption from Obfuscation. In *Proceedings of the 19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC)*, 2016.
[78] D. DACHMAN-SOLED, J. KATZ, and A. THIRUVENGADAM. 10-round feistel is indifferentiable from an ideal cipher. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 649–678, 2016.
[79] I. DAMGAARD, J. B. NIELSEN, A. POLYCHRONIADOU, and M. RASKIN. On the Communication required for Unconditionally Secure Multiplication. In *Advances in Cryptology -- CRYPTO*, 2016.
[80] I. DAMGAARD, A. POLYCHRONIADOU, and V. RAO. Adaptively Secure Multi-Party Computation from LWE (via Equivocal FHE). In *Proceedings of the 19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC)*, 2016.
[81] A. DEGWEKAR, V. VAIKUNTANATHAN, and P. N. VASUDEVAN. Fine-grained Cryptography. In *Advances in Cryptology -- CRYPTO*, vol. 3, pp. 533–562, 2016.
[82] Y. DENG, J. GARAY, S. LING, H. WANG, and M. YUNG. On the implausibility of constant-round public-coin zero-knowledge proofs. In *Proceedings of the 10th International Conference on Security and Cryptography for Networks (SCN)*, pp. 237–253, 2016.
[83] A. DESHPANDE, V. KOPPULA, and B. WATERS. Constrained Pseudorandom Functions for Unconstrained Inputs. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, 2016.
[84] I. D. DINUR. Mildly exponential reduction from gap 3SAT to polynomial-gap label-cover. In *Electronic Colloquium on Computational Complexity (ECCC)*, 2016.
[85] Y. DODIS, S. HALEVI, R. D. ROTHBLUM, and D. WICHS. Spooky encryption and its applications. In *Advances in Cryptology -- CRYPTO*, 2016.
[86] Y. DODIS, I. MIRONOV, and N. STEPHENS-DAVIDOWITZ. Message Transmission with Reverse Firewalls--Secure Communication on Corrupted Machines. In *Advances in Cryptology - CRYPTO*, 2016.
[87] S. DOLEV, K. E. DEFRAWY, J. LAMPKINS, R. OSTROVSKY, and M. YUNG. Proactive Secret Sharing with a Dishonest Majority. In *Proceedings of the 10th Conference on Security and Cryptography for Networks (SCN)*, pp. 529–548, 2016.
[88] B. DOWLING, M. FISCHLIN, F. GÜNTHER, and D. STEBILA. A Cryptographic Analysis of the TLS 1.3 Handshake Protocol Candidates. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, 2015.
[89] C. DWORK. Strengthening Data Science Methods for Department of Defense Personnel and Readiness Missions. To be published by the National Academies Press. 2016.
[90] C. DWORK, V. FELDMAN, M. HARDT, T. PITASSI, O. REINGOLD, and A. ROTH. Generalization in adaptive data analysis and holdout reuse. In *Advances in Neural Information Processing Systems (NIPS)*, pp. 2350–2358, 2015.
[91] C. DWORK, V. FELDMAN, M. HARDT, T. PITASSI, O. REINGOLD, and A. ROTH. The reusable holdout: Preserving validity in adaptive data analysis. *Science,* 349, 6248, pp. 636–638, 2015.
[92] C. DWORK, M. NAOR, O. REINGOLD, and G. N. ROTHBLUM. Pure Differential Privacy for Rectangle Queries via Private Partitions. In *Proceedings of the 21st Annual International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT)*, 2015.
[93] C. DWORK, M. NAOR, and G. N. ROTHBLUM. Spooky Interaction and its Discontents: Compilers for Succinct Two-Message Argument Systems. In *Advances in Cryptology -- CRYPTO*, 2016.
[94] C. DWORK and G. N. ROTHBLUM. Concentrated Differential Privacy. *arXiv preprint arXiv:1603.01887v2,* 2016.
[95] C. DWORK, W. SU, and L. ZHANG. Private False Discovery Rate Control. *arXiv preprint arXiv:1511.03803v1,*

2015.
[96] S. DZIEMBOWSKI, S. FAUST, and F.-X. STANDAERT. Hardware Trojan-Resilience via Testing Amplification. In *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)*, 2016.
[97] V. FEHR and M. FISCHLIN. Sanitizable Signcryption: Sanitization over Encrypted Data. *IACR Cryptology ePrint Archive 2015/765,* 2015.
[98] J. GARAY, B. TACKMANN, and V. ZIKAS. Fair distributed computation of reactive functions. In *Proceedings of the 29th International Symposium on Distributed Computing (DISC)*, pp. 497–512, 2015.
[99] S. GARG, Y. ISHAI, E. KUSHILEVITZ, R. OSTROVSKY, and A. SAHAI. Cryptography with One-Way Communication. In *Advances in Cryptology -- CRYPTO*, vol. 2, pp. 191–208, 2015.
[100] S. GARG, P. MOHASSEL, and C. PAPAMANTHOU. Efficient Oblivious RAM in Two Rounds with Applications to Searchable Encryption. In *Advances in Cryptology -- CRYPTO*, 2016.
[101] S. GARG, P. MUKHERJEE, O. PANDEY, and A. POLYCHRONIADOU. The exact round complexity of secure computation. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 448–476, 2016.
[102] S. GARG and O. PANDEY. Incremental Program Obfuscation. *IACR Cryptology ePrint Archive 2015/997,* 2015.
[103] S. GARG, O. PANDEY, and A. SRINIVASAN. Revisiting the cryptographic hardness of finding a nash equilibrium. In *Advances in Cryptology -- CRYPTO*, pp. 579–604, 2016.
[104] S. GARG, O. PANDEY, A. SRINIVASAN, and M. ZHANDRY. Breaking the sub-exponential barrier in obfustopia. Manuscript. 2016.
[105] S. GARG and A. POLYCHRONIADOU. Efficient Black-box Garbled Data Structures. Manuscript. 2016
[106] R. GAY, D. HOFHEINZ, E. KILTZ, and H. WEE. Tightly CCA-Secure Encryption without Pairings. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 1–27, 2016.
[107] D. GENKIN, Y. ISHAI, and M. WEISS. Binary AMD Circuits from Secure Multiparty Computation. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[108] D. GENKIN, L. PACHMANOV, I. PIPMAN, A. SHAMIR, and E. TROMER. Physical key extraction attacks on PCs. *Communications of the ACM,* 59, 6, pp. 70–79, 2016.
[109] D. GENKIN, L. PACHMANOV, I. PIPMAN, and E. TROMER. ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs. In *Cryptographers' Track at the RSA Conference (CT-RSA)*, pp. 219–235, 2016.
[110] D. GENKIN, L. PACHMANOV, I. PIPMAN, E. TROMER, and Y. YAROM. ECDSA key extraction from mobile devices via nonintrusive physical side channels. In *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)*, 2016. CCS 2016, to appear.
[111] D. GENKIN, A. SHAMIR, and E. TROMER. Acoustic cryptanalysis. *Journal of Cryptography,* 2016. To appear.
[112] S. GOLDWASSER and Y. T. KALAI. Cryptographic assumptions: A position paper. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, pp. 505–522, 2016.
[113] V. GOYAL, Y. ISHAI, H. K. MAJI, A. SAHAI, and A. SHERSTOV. Bounded-Communication Leakage Resilience via Parity-Resilient Circuits. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2016.
[114] V. GOYAL, D. KHURANA, I. MIRONOV, O. PANDEY, and A. SAHAI. Do Distributed Differentially-Private Protocols Require Oblivious Transfer? In *Proceedings of the 43rd International Colloquium on Automata, Languages, and Programming (ICALP)*, vol. 29, pp. 1–15, 2016.
[115] V. GOYAL, D. KHURANA, and A. SAHAI. Breaking the Three Round Barrier for Non-Malleable Commitments. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2016.
[116] V. GOYAL, O. PANDEY, and S. RICHELSON. Textbook Non-Malleable Commitments. In *Proceedings of the 48th Annual Symposium on the Theory of Computing (STOC)*, 2016.
[117] J. GROTH. On the Size of Pairing-Based Non-interactive Arguments. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 305–326, 2016.
[118] S. GUO, P. HUBACEK, A. ROSEN, and M. VALD. Rational Sumchecks. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, 2016.
[119] I. I. HAITNER. Fair Coin Flipping: Tighter Analysis and the Many-Party Case. Manuscript. 2016.
[120] S. HALEVI. Graded encoding, variations on a scheme. *Cryptology ePrint Archive, Report 2015/866,* 2015.

[121] S. HALEVI, Y. ISHAI, A. JAIN, E. KUSHILEVITZ, and T. RABIN. Secure Multiparty Computation with General Interaction Patterns. In *Proceedings of the 7th Annual Innovations in Theoretical Computer Science (ITCS)*, 2016.
[122] C. HAZAY, A. POLYCHRONIADOU, and M. VENKITASUBRAMANIAM. Composable Security in the Tamper-Proof Hardwire Model under Minimal Complexity. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[123] B. HEMENWAY, Z. JAFARGHOLI, R. OSTROVSKY, A. SCAFURO, and D. WICHS. Adaptively secure garbled circuits from one-way functions. In *Advances in Cryptology -- CRYPTO*, 2016.
[124] B. HEMENWAY, R. OSTROVSKY, S. RICHELSON, and A. ROSEN. Adaptive Security with Quasi-Optimal Rate. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, 2016.
[125] M. HIRT, U. MAURER, D. TSCHUDI, and V. ZIKAS. Network-Hiding Communication and Applications to Multi-Party Protocols. In *Advances in Cryptology -- CRYPTO*, vol. 9816, pp. 335-–365, 2016.
[126] D. HOFHEINZ, V. RAO, and D. WICHS. Standard security does not imply indistinguishability under selective opening. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[127] C. K. HOSDURG. On the security of Scrypt and Proofs of Space in the pROM model. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, 2016.
[128] R. IMPAGLIAZZO, R. JAISWAL, V. KABANETS, B. M. KAPRON, V. KING, and S. TESSARO. Simultaneous Amplification of Secrecy and Unreliability for an Unknown Channel. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[129] Y. ISHAI, E. KUSHILEVITZ, M. PRABHAKARAN, A. SAHAI, and C.-H. YU. Secure Protocol Transformations. In *Advances in Cryptology -- CRYPTO*, vol. 2, pp. 430–458, 2016.
[130] Y. ISHAI, M. WEISS, and G. YANG. Making the Best of a Leaky Situation: Zero-Knowledge PCPs from Leakage-Resilient Circuits. In *Theory of Cryptography Conference (TCC)*, 2016A.
[131] Z. JAFARGHOLI and D. WICHS. Adaptive Security of Yao's Garbled Circuits. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[132] S. JARECKI, A. KIAYIAS, H. KRAWCZYK, and J. XU. Highly-Efficient and Composable Password-Protected Secret Sharing. In preparation.
[133] C. S. JUTLA. Upending Stock Market Structure Using Secure Multi-Party Computation. *IACR eprint archive,* July 2015.
[134] Y. T. KALAI and O. PANETH. Delegating RAM computations. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[135] Y. T. KALAI, R. RAZ, and O. REGEV. On the Space Complexity of Linear Programming with Preprocessing. In *Proceedings of the 7th Annual Innovations in Theoretical Computer Science (ITCS)*, 2016.
[136] Y. T. KALAI, G. N. ROTHBLUM, and R. D. ROTHBLUM. From obfuscation to the security of Fiat-Shamir for proofs. *Cryptology ePrint Archive, Report 2016/303,* 2016.
[137] S. KASIVISWANATHAN, K. NISSIM, and H. JIN. Private Incremental Regression. In submission.
[138] D. KHURANA, D. KRASCHEWSKI, H. MAJI, M. PRABHAKARAN, and A. SAHAI. All Complete Functionalities are Reversible. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 213–242, 2016.
[139] A. KIAYIAS, J. GARAY, and N. LEONARDOS. The Bitcoin Backbone: Full Analysis in the Dynamic Setting. In preparation.
[140] A. KIAYIAS, V. TEAGUE, T. ZACHARIAS, and V. ZIKAS. Incoercible and Verifiable Computation. In preparation.
[141] A. KIAYIAS, H.-S. ZHOU, and V. ZIKAS. Fair and robust multi-party computation using a global transaction ledger. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 705–734, 2016.
[142] V. KOLESNIKOV, H. KRAWCZYK, Y. LINDEL, A. MALOZEMOFF, and T. RABIN. Attribute-Based Key Exchange with General Policies. In *The 23rd ACM Conference on Computer and Communications Security (CCS)*, 2016.
[143] A. KOSBA, A. MILLER, E. SHI, Z. WEN, and C. PAPAMANTHOU. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In *IEEE Symposium on Security and Privacy (SP)*, 2016.
[144] H. KRAWCZYK and H. WEE. The OPTLS Protocol and TLS 1.3. In preparation.
[145] K. LEWI, A. J. MALOZEMOFF, D. APON, B. CARMER, A. FOLTZER, D. WAGNER, D. W. ARCHER, D.

BONEH, J. KATZ, and M. RAYKOVA. 5Gen: A Framework for Prototyping Applications Using Multilinear Maps and Matrix Branching Programs. In *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)*, 2016.
[146] B. LI and D. MICCIANCIO. Compactness vs Collusion Resistance in Functional Encryption. In *Proceedings of the 14th Theory of Cryptography Conference (TCC-B)*, 2016.
[147] B. LI and D. MICCIANCIO. Equational Security Proofs of Oblivious Transfer Protocols. *IACR ePrint 2016/624,* 2016.
[148] B. LIBERT, F. MOUHARTEM, T. PETERS, and M. YUNG. Practical Signatures with Efficient Protocols from Simple Assumptions. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (AsiaCCS)*, pp. 511–522, 2016.
[149] B. LIBERT, S. RAMANNA, and M. YUNG. Functional Commitment Schemes: From Polynomial Commitments to Pairing-Based Accumulators from Simple Assumptions. In *Proceedings of the 43rd International Colloquium on Automata, Languages and Programming (ICALP)*, 2016.
[150] H. LIN. Indistinguishability obfuscation from constant-degree graded encoding schemes. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 28–57, 2016.
[151] H. LIN, R. PASS, K. SETH, and S. TELANG. Output-Compressing Randomized Encodings and Applications. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, 2016.
[152] H. LIN and V. VAIKUNTANATHAN. Indistinguishability Obfuscation from DDH-like Assumptions on Constant-Degree Graded Encodings. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2016.
[153] R. J. LIPTON, R. OSTROVSKY, and V. ZIKAS. Provably secure virus detection: Using the observer effect against malware. In *Proceedings of the 43rd International Colloquium on Automata, Languages, and Programming (ICALP)*, 2016.
[154] T. LIU. On Basing Search SIVP on NP-Hardness. In preparation.
[155] T. LIU and V. VAIKUNTANATHAN. On Basing Private Information Retrieval on NP-Hardness. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, pp. 372–386, 2016.
[156] T. LIU and V. VAIKUNTANATHAN. On the Impossibility of Private Information Retrieval from NP Hardness. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, 2016.
[157] M. MAHMOODY, A. MOHAMMED, and S. NEMATIHAJI. More on Impossibility of Virtual Black-Box Obfuscation in Idealized Models. *Cryptology ePrint Archive, Report 2015/632,* 2015.
[158] M. MAHMOODY, A. MOHAMMED, S. NEMATIHAJI, R. PASS, and A. SHELAT. Lower bounds on assumptions behind indistinguishability obfuscation. In *Proceedings of the 13th Theory of Cryptography Conference (TCC-A)*, pp. 49–66, 2016.
[159] P. MIAO. Cut-and-choose for Garbled RAM. In preparation.
[160] E. MILES, A. SAHAI, and M. ZHANDRY. Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over GGH13. In *Advances in Cryptology -- CRYPTO*, vol. 2, pp. 629–658, 2016.
[161] A. MILLER, Y. XIA, K. CROMAN, E. SHI, and D. SONG. The honey badger of BFT protocols. In *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)*, 2016.
[162] A. NAVEH and E. TROMER. PhotoProof: Cryptographic Image Authentication for Any Set of Permissible Transformations. In *IEEE Symposium on Security and Privacy (SP)*, pp. 255–271, 2016.
[163] K. NAYAK, S. KUMAR, A. MILLER, and E. SHI. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. *IACR Cryptology ePrint Archive 2015/796,* 2015. Available at https://eprint.iacr.org/2015/796.pdf.
[164] R. OSTROVSKY, G. PERSIANO, and I. VISCONTI. Impossibility of black-box simulation against leakage attacks. In *Advances in Cryptology -- CRYPTO*, pp. 130–149, 2015.
[165] R. OSTROVSKY, S. RICHELSON, and A. SCAFURO. Round-Optimal Black-Box Two-Party Computation. In *Advances in Cryptology -- CRYPTO*, vol. 2, pp. 339–358, 2015.
[166] O. PANETH and G. N. ROTHBLUM. Publicly Verifiable Non-Interactive Arguments for Delegating Computation. Preprint.
[167] O. PANETH and A. SAHAI. On the Equivalence of Obfuscation and Multilinear Maps. Preprint. 2015.
[168] S. PARK, K. PIETRZAK, J. ALWEN, G. FUCHSBAUER, and P. GAŽI. Spacecoin: A cryptocurrency based on proofs of space. *IACR Cryptology ePrint Archive, 2015/528,* 2015.
[169] S. PARK and R. L. RIVEST. Towards Secure Quadratic Voting. *Cryptology ePrint Archive, Report 2016/400,*

2016. Commissioned to appear in Public Choice 2017.
[170] R. PASS and E. SHI. Fruitchains: A Fair Blockchain. In preparation.
[171] R. PASS and E. SHI. Hybrid Consensus: Efficient Consensus in the Permissionless Model. In preparation.
[172] R. PASS, E. SHI, and F. TRAMER. Formal Abstractions for Attested Execution Processors. In preparation.
[173] C. PEIKERT and H. WEE. New HIBE constructions from lattices. In preparation.
[174] O. REINGOLD, G. N. ROTHBLUM, and R. D. ROTHBLUM. Constant-round interactive proofs for delegating computation. In *Proceedings of the 48th Annual Symposium on Theory of Computing (STOC)*, pp. 49–62, 2016.
[175] R. L. RIVEST and S. TESSARO. "Termutation" Ciphers: Lightweight Symmetric Searchable Encryption. In submission.
[176] A. RUSSELL, Q. TANG, M. YUNG, and H.-S. ZHOU. Destroying Steganography via Amalgamation: Kleptographically CPA Secure Public Key Encryption. *IACR Cryptology ePrint Archive 2016/530,* 2016. To be submitted.
[177] A. RUSSELL, Q. TANG, M. YUNG, and H.-S. ZHOU. Cliptography: Clipping the power of kleptographic attacks. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (AsiaCCS)*, 2016.
[178] A. SRINIVASAN and C. P. RANGAN. Efficiently Obfuscating Re-Encryption Program under DDH Assumption. Submitted to CT-RSA.
[179] N. STEPHENS-DAVIDOWITZ. Discrete Gaussian Sampling Reduces to CVP and SVP. In *Proceedings of the 27th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2016.
[180] S. S. VIVEK, S. D. SELVI, A. SRINIVASAN, and C. P. RANGAN. Stronger Public Key Encryption System Withstanding RAM Scraper Like Attacks. *Security and Communication Networks,* 9, 12, pp. 1650–1662, 2016.
[181] R. WAHBY, M. HOWALD, S. GARG, ABHI SHELAT, and M. WALFISH. Verifiable ASICs. In *Proceedings of the 37th IEEE Symposium on Security and Privacy (SP)*, 2016. Distinguished Student Paper Award.
[182] A. YOUNG and M. YUNG. Cryptography as an Attack Technology: Proving the RSA/Factoring Kleptographic Attack. In *The New Codebreakers*, 243–255. Springer, 2016.
[183] M. YUNG. From Mental Poker to Core Business: Why and How to Deploy Secure Computation Protocols? Invited talk at ACM CCS Conference. October 2015.
[184] M. YUNG. The Mobile Adversary Paradigm in Distributed Computation and Systems. In *Proceedings of the 2015 ACM Symposium on Principles of Distributed Computing*, pp. 171–172, 2015.
[185] S. ZAHUR, X. WANG, M. RAYKOVA, A. GASCÓN, J. DOERNER, D. EVANS, and J. KATZ. Revisiting Square-Root ORAM Efficient Random Access in Multi-Party Computation. In *Proceedings of the 37th IEEE Symposium on Security and Privacy (SP)*, 2016.