Foundations of Cryptography – A Primer

Foundations of Cryptography – A Primer

Oded Goldreich

Department of Computer Science
Weizmann Institute of Science
Rehovot Israel
oded.goldreich@weizmann.ac.il

the essence of knowledge

Boston – Delft

Foundations and Trends® in Theoretical Computer Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1 781 871 0245
www.nowpublishers.com
sales@nowpublishers.com

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

A Cataloging-in-Publication record is available from the Library of Congress

Printed on acid-free paper

ISBN: 1-933019-02-6; ISSNs: Paper version 1551-305X; Electronic version 1551-3068

Contents

1

Introduction and Preliminaries

It is possible to build a cabin with no foundations,
but not a lasting building.

Eng. Isidor Goldreich (1906–1995)

1.1 Introduction

The vast expansion and rigorous treatment of cryptography is one of the major achievements of theoretical computer science. In particular, concepts such as computational indistinguishability, pseudorandomness and zero-knowledge interactive proofs were introduced, classical notions such as secure encryption and unforgeable signatures were placed on sound grounds, and new (unexpected) directions and connections were uncovered. Indeed, modern cryptography is strongly linked to complexity theory (in contrast to "classical" cryptography which is strongly related to information theory).

Modern cryptography is concerned with the construction of information systems that are robust against malicious attempts to make these systems deviate from their prescribed functionality. The prescribed functionality may be the private and authenticated communication of information through the Internet, the holding of tamper-proof and secret electronic voting, or conducting any "fault-resilient" multi-party computation. Indeed, the scope of modern cryptography is very broad, and it stands in contrast to "classical" cryptography (which has focused on the single problem of enabling secret communication over insecure communication media).

The design of cryptographic systems is a very difficult task. One cannot rely on intuitions regarding the "typical" state of the environment in which the system operates. For sure, the adversary attacking the system will try to manipulate the environment into "untypical" states. Nor can one be content with counter-measures designed to withstand specific attacks, since the adversary (which acts after the design of the system is completed) will try to attack the schemes in ways that are different from the ones the designer had envisioned. The validity of the above assertions seems self-evident, but still some people hope that in practice ignoring these tautologies will not result in actual damage. Experience shows that these hopes rarely come true; cryptographic schemes based on make-believe are broken, typically sooner than later.

In view of the foregoing, we believe that it makes little sense to make assumptions regarding the specific *strategy* that the adversary may use. The only assumptions that can be justified refer to the computational *abilities* of the adversary. Furthermore, the design of cryptographic systems has to be based on *firm foundations*; whereas ad-hoc approaches and heuristics are a very dangerous way to go. A heuristic may make sense when the designer has a very good idea regarding the environment in which a scheme is to operate, yet a cryptographic scheme has to operate in a maliciously selected environment which typically transcends the designer's view.

This primer is aimed at presenting the foundations for cryptography. The foundations of cryptography are the paradigms, approaches and techniques used to conceptualize, define and provide solutions to natural "security concerns". We will present some of these paradigms, approaches and techniques as well as some of the fundamental results obtained using them. Our emphasis is on the clarification of fundamental concepts and on demonstrating the feasibility of solving several central cryptographic problems.

Solving a cryptographic problem (or addressing a security concern) is a two-stage process consisting of a *definitional stage* and a *constructional stage*. First, in the definitional stage, the functionality underlying the natural concern is to be identified, and an adequate cryptographic problem has to be defined. Trying to list all undesired situations is infeasible and prone to error. Instead, one should define the functionality in terms of operation in an imaginary ideal model, and require a candidate solution to emulate this operation in the real, clearly defined, model (which specifies the adversary's abilities). Once the definitional stage is completed, one proceeds to construct a system that satisfies the definition. Such a construction may use some simpler tools, and its security is proved relying on the features of these tools. In practice, of course, such a scheme may need to satisfy also some *specific* efficiency requirements.

This primer focuses on several archetypical cryptographic problems (e.g., encryption and signature schemes) and on several central tools (e.g., computational difficulty, pseudorandomness, and zero-knowledge proofs). For each of these problems (resp., tools), we start by presenting the natural concern underlying it (resp., its intuitive objective), then define the problem (resp., tool), and finally demonstrate that the problem may be solved (resp., the tool can be constructed). In the latter step, our focus is on demonstrating the feasibility of solving the problem, not on providing a practical solution. As a secondary concern, we typically discuss the level of practicality (or impracticality) of the given (or known) solution.

Computational difficulty

The aforementioned tools and applications (e.g., secure encryption) exist only if some sort of computational hardness exists. Specifically, all these problems and tools require (either explicitly or implicitly) the ability to generate instances of hard problems. Such ability is captured in the definition of one-way functions. Thus, one-way functions are the very minimum needed for doing most natural tasks of cryptography. (It turns out, as we shall see, that this necessary condition is "essentially" sufficient; that is, the existence of one-way functions (or augmentations and extensions of this assumption) suffices for doing most of cryptography.)

Our current state of understanding of efficient computation does not allow us to prove that one-way functions exist. In particular, if $\mathcal{P} = \mathcal{NP}$ then no one-way functions exist. Furthermore, the existence of one-way functions implies that $\mathcal{NP}$ is not contained in $\mathcal{BPP} \supseteq \mathcal{P}$ (not even "on the average"). Thus, proving that one-way functions exist is not easier than proving that $\mathcal{P} \neq \mathcal{NP}$; in fact, the former task seems significantly harder than the latter. Hence, we have no choice (at this stage of history) but to assume that one-way functions exist. As justification to this assumption we may only offer the combined beliefs of hundreds (or thousands) of researchers. Furthermore, these beliefs concern a simply stated assumption, and their validity follows from several widely believed conjectures which are central to various fields (e.g., the conjectured intractability of integer factorization is central to computational number theory).

Since we need assumptions anyhow, why not just assume what we want (i.e., the existence of a solution to some natural cryptographic problem)? Well, first we need to know what we want: as stated above, we must first clarify what exactly we want; that is, go through the typically complex definitional stage. But once this stage is completed, can we just assume that the definition derived can be met? Not really: once a definition is derived, how can we know that it can be met at all? The way to demonstrate that a definition is viable (and that the corresponding intuitive security concern can be satisfied at all) is to construct a solution based on a *better understood* assumption (i.e., one that is more common and widely believed). For example, looking at the definition of zero-knowledge proofs, it is not a-priori clear that such proofs exist at all (in a non-trivial sense). The non-triviality of the notion was first demonstrated by presenting a zero-knowledge proof system for statements, regarding Quadratic Residuosity, which are believed to be hard to verify (without extra information). Furthermore, contrary to prior beliefs, it was later shown that the existence of one-way functions implies that any NP-statement can be proved in zero-knowledge. Thus, facts that were not known to hold at all (and even believed to be false), were shown to hold by reduction to widely believed assumptions (without which most of modern cryptography collapses anyhow). To summarize, not all assumptions are equal, and so reducing a complex, new and doubtful assumption to a widely-believed simple (or even merely simpler) assumption is of great value. Furthermore, reducing the solution of a new task to the assumed security of a well-known primitive typically means providing a construction that, using the known primitive, solves the new task. This means that we do not only know (or assume) that the new task is solvable but we also have a solution based on a primitive that, being well-known, typically has several candidate implementations.

Prerequisites and structure

Our aim is to present the basic concepts, techniques and results in cryptography. As stated above, our emphasis is on the clarification of fundamental concepts and the relationship among them. This is done in a way independent of the particularities of some popular number theoretic examples. These particular examples played a central role in the development of the field and still offer the most practical implementations of all cryptographic primitives, but this does not mean that the presentation has to be linked to them. On the contrary, we believe that concepts are best clarified when presented at an abstract level, decoupled from specific implementations. Thus, the most relevant background for this primer is provided by basic knowledge of algorithms (including randomized ones), computability and elementary probability theory.

The primer is organized in two main parts, which are preceded by preliminaries (regarding efficient and feasible computations). The two parts are Part I – Basic Tools and Part II – Basic Applications. The basic tools consist of computational difficulty (one-way functions), pseudorandomness and zero-knowledge proofs. These basic tools are used for the basic applications, which in turn consist of Encryption Schemes, Signature Schemes, and General Cryptographic Protocols.

In order to give some feeling of the flavor of the area, we have included in this primer a few proof sketches, which some readers may find too terse. We stress that following these proof sketches is *not*

1: Introduction and Preliminaries
Part I: Basic Tools
2: Computational Difficulty (One-Way Functions)
3: Pseudorandomness
4: Zero-Knowledge
Part II: Basic Applications
5: Encryption Schemes
6: Signature and Message Authentication Schemes
7: General Cryptographic Protocols

Fig. 1.1 Organization of this primer

essential to understanding the rest of the material. In general, later sections may refer to definitions and results in prior sections, but not to the constructions and proofs that support these results. It may be even possible to understand later sections without reading any prior section, but we believe that the order we chose should be preferred because it proceeds from the simplest notions to the most complex ones.

Suggestions for further reading

This primer is a brief summary of the author's two-volume work on the subject (65; 67). Furthermore, Part I corresponds to (65), whereas Part II corresponds to (67). Needless to say, the reader is referred to these textbooks for further detail.

Two of the topics reviewed by this primer are zero-knowledge proofs (which are probabilistic) and pseudorandom generators (and functions). A wider perspective on probabilistic proof systems and pseudorandomness is provided in (62, Sections 2–3).

Current research on the foundations of cryptography appears in general computer science conferences (e.g., FOCS and STOC), in cryptography conferences (e.g., Crypto and EuroCrypt) as well as in the newly established *Theory of Cryptography Conference* (TCC).

Practice. The aim of this primer is to introduce the reader to the *theoretical foundations* of cryptography. As argued above, such foundations are necessary for *sound* practice of cryptography. Indeed, practice requires more than theoretical foundations, whereas the current primer makes no attempt to provide anything beyond the latter. However, given a sound foundation, one can learn and evaluate various practical suggestions that appear elsewhere (e.g., in (97)). On the other hand, lack of sound foundations results in inability to critically evaluate practical suggestions, which in turn leads to unsound decisions. Nothing could be more harmful to the design of schemes that need to withstand adversarial attacks than misconceptions about such attacks.

Non-cryptographic references: Some "non-cryptographic" works were referenced for sake of wider perspective. Examples include (4; 5; 6; 7; 55; 69; 78; 96; 118).

1.2 Preliminaries

Modern cryptography, as surveyed here, is concerned with the construction of *efficient* schemes for which it is *infeasible* to violate the security feature. Thus, we need a notion of efficient computations as well as a notion of infeasible ones. The computations of the legitimate users of the scheme ought be efficient, whereas violating the security features (by an adversary) ought to be infeasible. We stress that we do not identify feasible computations with efficient ones, but rather view the former notion as potentially more liberal.

Efficient computations and infeasible ones

Efficient computations are commonly modeled by computations that are polynomial-time in the security parameter. The polynomial bounding the running-time of the legitimate user's strategy is *fixed and typically explicit* (and *small*). Indeed, our aim is to have a notion of efficiency that is as strict as possible (or, equivalently, develop strategies that are as efficient as possible). Here (i.e., when referring to the complexity of the legitimate users) we are in the same situation as in any algorithmic setting. Things are different when referring to our assumptions regarding the computational resources of the adversary, where we refer to the notion of feasible that we wish to be as wide as possible. A common approach is to postulate that feasible computations are polynomial-time too, but here the polynomial is *not a-priori specified* (and is to be thought of as arbitrarily large). In other words, the adversary is restricted to the class of polynomial-time computations and anything beyond this is considered to be infeasible.

Although many definitions explicitly refer to the convention of associating feasible computations with polynomial-time ones, this convention is *inessential* to any of the results known in the area. In all cases, a more general statement can be made by referring to a general notion of feasibility, which should be preserved under standard algorithmic composition, yielding theories that refer to adversaries of running-time bounded by any specific super-polynomial function (or class of functions). Still, for sake of concreteness and clarity, we shall use the former convention in our formal definitions (but our motivational discussions will refer to an unspecified notion of feasibility that covers at least efficient computations).

Randomized (or probabilistic) computations

Randomized computations play a central role in cryptography. One fundamental reason for this fact is that randomness is essential for the existence (or rather the generation) of secrets. Thus, we must allow the legitimate users to employ randomized computations, and certainly (since randomization is feasible) we must consider also adversaries that employ randomized computations. This brings up the issue of success probability: typically, we require that legitimate users succeed (in fulfilling their legitimate goals) with probability 1 (or negligibly close to this), whereas adversaries succeed (in violating the security features) with negligible probability. Thus, the notion of a negligible probability plays an important role in our exposition. One requirement of the definition of negligible probability is to provide a robust notion of rareness: A rare event should occur rarely even if we repeat the experiment for a feasible number of times. That is, in case we consider any polynomial-time computation to be feasible, a function $\mu:\mathbb{N}\to\mathbb{N}$ is called negligible if $1-(1-\mu(n))^{p(n)} < 0.01$ for every polynomial p and sufficiently big n (i.e., μ is negligible if for every positive polynomial p' the function $\mu(\cdot)$ is upper-bounded by $1/p'(\cdot)$). However, if we consider the function $T(n)$ to provide our notion of infeasible computation then functions bounded above by $1/T(n)$ are considered negligible (in n).

We will also refer to the notion of noticeable probability. Here the requirement is that events that occur with noticeable probability, will occur almost surely (i.e., except with negligible probability) if we repeat the experiment for a polynomial number of times. Thus, a function $\nu : \mathbb{N} \to \mathbb{N}$ is called noticeable if for some positive polynomial p' the function $\nu(\cdot)$ is lower-bounded by $1/p'(\cdot)$.

References

[1] "National institute for standards and technology," 1991. Digital Signature Standard (DSS). *Federal Register* Vol. 56, No.169.

[2] W. Aiello and J. Håstad, "Perfect zero-knowledge languages can be recognized in two rounds," in *28th IEEE Symposium on Foundations of Computer Science*, pp. 439–448, 1987.

[3] W. Alexi, B. Chor, O. Goldreich, and C. Schnorr, "Rsa/rabin functions: certain parts are as hard as the whole," *SIAM Journal on Computing*, pp. 194–209, 1988.

[4] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, "Proof verification and intractability of approximation problems," *Journal of the ACM*, vol. 17, pp. 501–555, 1998. Preliminary version in *33rd FOCS*, 1992.

[5] S. Arora and S. Safra, "Probabilistic checkable proofs: a new characterization of np," *Journal of the ACM*, vol. 45, pp. 70–122, 1998. Preliminary version in *33rd FOCS*, 1992.

[6] L. Babai, L. Fortnow, L. Levin, and M. Szegedy, "Checking computations in polylogarithmic time," in *23rd ACM Symposium on the Theory of Computing*, pp. 21–31, 1991.

[7] L. Babai, L. Fortnow, N. Nisan, and A. Wigderson, "BPP has subexponential time simulations unless exptime has publishable proofs," *Complexity Theory*, vol. 3, pp. 307–318, 1993.

[8] B. Barak, "How to go beyond the black-box simulation barrier," in *42nd IEEE Symposium on Foundations of Computer Science*, pp. 106–115, 2001.

[9] B. Barak, "Constant-round coin-tossing with a man in the middle or realizing the shared random string model," in *43th IEEE Symposium on Foundations of Computer Science*, pp. 345–355, 2002.

[10] B. Barak, R. Canetti, and J. Nielsen, "Universally composable protocols with relaxed set-up assumptions," in *45th IEEE Symposium on Foundations of Computer Science*, pp. 186–195, 2004.

[11] B. Barak and O. Goldreich, "17th ieee conference on computational complexity," in *Universal arguments and their applications*, pp. 194–203, 2002.

[12] B. Barak and Y. Lindell, "Strict polynomial-time in simulation and extraction," *SIAM Journal on Computing*, vol. 33(4), pp. 783–818, 2004.

[13] D. Beaver, *Foundations of secure interactive computing.* Vol. 576, Springer-Verlag, 1991. *Crypto91*, Lecture Notes in Computer Science.

[14] D. Beaver, "Secure multi-party protocols and zero-knowledge proof systems tolerating a faulty minority," *Journal of Cryptology*, vol. 4, pp. 75–122, 1991.

[15] D. Beaver, S. Micali, and P. Rogaway, "The round complexity of secure protocols," in *22nd ACM Symposium on the Theory of Computing*, pp. 503–513, 1990. See details in (113).

[16] M. Bellare, "Electronic commerce and electronic payments," Webpage of a course. http://www-cse.ucsd.edu/users/mihir/cse291-00/.

[17] M. Bellare, R. Canetti, and R. Krawczyk, *Keying hash functions for message authentication.* Vol. 1109, Springer, 1996. *Crypto96* Lecture Notes in Computer Science.

[18] M. Bellare, R. Canetti, and R. Krawczyk, "A modular approach to the design and analysis of authentication and key-exchange protocols," in *30th ACM Symposium on the Theory of Computing*, pp. 419–428, 1998.

[19] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, *Relations among notions of security for public-key encryption schemes.* Vol. 1462, Springer, 1998. *Crypto98* Lecture Notes in Computer Science.

[20] M. Bellare and O. Goldreich, *On defining proofs of knowledge.* Vol. 740, Springer-Verlag, 1992. *Crypto92* Lecture Notes in Computer Science.

[21] M. Bellare, R. Impagliazzo, and M. Naor, "Does parallel repetition lower the error in computationally sound protocols?," in *38th IEEE Symposium on Foundations of Computer Science*, pp. 374–383, 1997.

[22] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," in *1st Conf. on Computer and Communications Security*, pp. 62–73, 1993.

[23] M. Ben-Or, R. Canetti, and O. Goldreich, "Asynchronous secure computation," in *25th ACM Symposium on the Theory of Computing.* See details in (35).

[24] M. Ben-Or, O. Goldreich, S. Goldwasser, J. Håstad, J. Kilian, S. Micali, and P. Rogaway, *Everything provable is probable in zero-knowledge.* Vol. 403, Springer-Verlag, 1990. *Crypto88* Lecture Notes in Computer Science.

[25] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," in *20th ACM Symposium on the Theory of Computing*, pp. 1–10, 1988.

[26] M. Ben-Or, B. Kelmer, and T. Rabin, "Asynchronous secure computations with optimal resilience," in *13th ACM Symposium on Principles of Distributed Computing*, pp. 183–192, 1994.

[27] C. Bennett, G. Brassard, and J. Robert, "Privacy amplification by public discussion," *SIAM Journal on Computing*, vol. 17, pp. 210–229, 1998. Preliminary version in *Crypto85*, titled "How to reduce your enemy's information".

[28] M. Blum, "Coin flipping by phone," *IEEE Sprig COMPCOM*, pp. 133–137, 1982. See also *SIGACT News*, Vol. 15, No. 1, 1983.

[29] M. Blum, B. Feldman, and T. Micali, "Non-interactive zero-knowledge proof systems," in *20th ACM Symposium on Principles of Distributed Computing*, pp. 103–112, 1988. See (32).

[30] M. Blum and S. Goldwasser, *An efficient probabilistic public-key encryption scheme which hides all partial information*. Vol. 196, Springer-Verlag, 1985. *Crypto84* Lecture Notes in Computer Science.

[31] M. Blum and S. Micali, "How to generate cryptographically strong sequences of pseudo-random bits," *SIAM Journal on Computing*, vol. 13, pp. 850–864, 1984. Preliminary version in *23rd FOCS*, 1982.

[32] M. Blum, A. D. Santis, S. Micali, and G. Persiano, "Non-interactive zero-knowledge proof systems," *SIAM Journal on Computing*, vol. 20(6), pp. 1084–1118, 1991. (Considered the journal version of (29).

[33] G. Brassard, D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge," *Journal of Computer and System Science*, vol. 37(2), pp. 156–189, 1988. Preliminary version by Brassard and Crépeau in *27th FOCS*, 1986.

[34] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," in *42nd IEEE Symposium on Foundations of Computer Science*, pp. 136–145. Full version (with different title) is available from *Cryptology ePrint Archive*, Report 2000/067.

[35] R. Canetti, *Studies in secure multi-party computation and applications*. PhD thesis, Weizmann Institute of Science, Rehovot, Israel, June 1995. Available from http://www.wisdom.weizmann.ac.il/ oded/PS/ran-phd.ps.

[36] R. Canetti, "Security and composition of multi-party cryptographic protocols," *Journal of Cryptology*, vol. 13(1), pp. 143–202, 2000.

[37] R. Canetti, U. Feige, O. Goldreich, and M. Naor, "Adaptively secure multi-party computation," in *28th ACM Symposium on the Theory of Computing*, pp. 639–648, 1996.

[38] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," in *30th ACM Symposium on the Theory of Computing*, pp. 209–218, 1998.

[39] R. Canetti and A. Herzberg, *Maintaining security in the presence of transient faults*. Vol. 839, Springer-Verlag, 1994. *Crypto94* Lecture Notes in Computer Science.

[40] R. Canetti, J. Kilian, E. Petrank, and A. Rosen, "Black-box concurrent zero-knowledge requires $\tilde{\Omega}(\log n)$ rounds," in *33rd ACM Symposium on the Theory of Computing*, pp. 494–503, 2002.

[41] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai, "Universally composable two-party and multi-party secure computation," in *34th ACM Symposium on the Theory of Computing*, pp. 494–503, 2002.

[42] D. Chaum, C. Crépeau, and I. Damgård, "Multi-party unconditionally secure protocols," in *20th ACM Symposium on Principles of Distributed Computing*, pp. 260–268, 1987.

[43] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," in *20th ACM Symposium on the Theory of Computing*, pp. 11–19, 1988.

[44] B. Chor and E. Kushilevitz, "A zero-one law for boolean privacy," *SIAM Journal of Discrete Mathematics*, vol. 4, pp. 36–47, 1991.

[45] B. Chor and M. Rabin, "Achieving independence in logarithmic number of rounds," in *6th ACM Symposium on Principles of Distributed Computing*, pp. 260–268, 1987.

[46] R. Cleve, "Limits on the security of coin flips when half the processors are faulty," in *18th ACM Symposium on the Theory of Computing*, pp. 364–369, 1986.

[47] I. Damgård, *Collision free hash functions and public key signature schemes*. Vol. 304, Springer-Verlag, 1988. *EuroCryp87* Lecture Notes in Computer Science.

[48] I. Damgard and J. Nielsen, *Improved non-committing encryption schemes based on general complexity assumption*. Vol. 1880, Springer-Verlag, 2000. *Crypto00* Lecture Notes in Computer Science.

[49] W. Diffie and M. Hellmann, "New directions in cryptography," *IEEE Trans. on Info. Theory*, pp. 644–654, 1976. IT-22.

[50] D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography," *SIAM Journal on Computing*, vol. 30, no. 2, pp. 391–437, 2000. Preliminary version in *23rd STOC*, 1991.

[51] D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly secure message transmission," *Journal of the ACM*, vol. 40(1), pp. 17–47, 1993.

[52] D. Dolev and H. Strong, "Authenticated algorithms for byzantine agreement," *SIAM Journal on Computing*, vol. 12, pp. 656–666, 1983.

[53] C. Dwork, M. Naor, and A. Sahai, "Concurrent zero-knowledge," in *30th ACM Symposium on the Theory of Computing*, pp. 409–418, 1998.

[54] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Communications of the ACM*, vol. 28, no. 6, pp. 637–647, 1985.

[55] U. Feige, S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy, "Approximating clique is almost np-complete," *Journal of the ACM*, vol. 43, pp. 268–292, 1996. Preliminary version in *32nd FOCS*, 1991.

[56] U. Feige, D. Lapidot, and A. Shamir, "Multiple non-interactive zero-knowledge proofs under general assumptions," *SIAM Journal on Computing*, vol. 29(1), pp. 1–28, 1999.

[57] U. Feige and A. Shamir, "Witness indistinguishability and witness hiding protocols," in *22nd ACM Symposium on the Theory of Computing*, pp. 416–426, 1990.

[58] A. Fiat and A. Shamir, *How to prove yourself: practical solution to identification and signature problems*. Vol. 263, Springer-Verlag, 1987. *Crypto86* Lecture Notes in Computer Science.

[59] L. Fortnow, "The complexity of perfect zero-knowledge," in *19th ACM Symposium on the Theory of Computing*, pp. 204–209, 1987.

[60] P. Gemmell, *An introduction to threshold cryptography*. Vol. 2(3), RSA Lab, 1997. *CryptoBytes*.

[61] R. Gennaro, M. Rabin, and T. Rabin, "Simplified vss and fast-track multiparty computations with applications to threshold cryptography," in *17th ACM Symposium on Principles of Distributed Computing*, pp. 101–112, 1998.

[62] O. Goldreich, *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*. Vol. 17 of *Algorithms and Combinatorics series*, Springer, 1998.

[63] O. Goldreich, "Secure multi-party computation," 1998. Working Draft, Available from http://www.wisdom.weizmann.ac.il/ oded/pp.html.

[64] O. Goldreich, "A uniform complexity treatment of encryption and zero-knowledge," *Journal of Cryptology*, vol. 6(1), pp. 21–53, 1998.

[65] O. Goldreich, *Foundations of Cryptography – Basic Tools*. Cambridge University Press, 2001.

[66] O. Goldreich, "Concurrent zero-knowledge with timing, revisited," in *34th ACM Symposium on the Theory of Computing*, pp. 332–340, 2002.

[67] O. Goldreich, *Foundations of Cryptography – Basic Applications*. Cambridge University Press, 2004.

[68] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *Journal of the ACM*, vol. 33(4), pp. 792–807, 1986.

[69] O. Goldreich and J. Håstad, "On the complexity of interactive proofs with bounded communication," *IPL*, vol. 67(4), pp. 205–214, 1998.

[70] O. Goldreich and A. Kahan, "How to construct constant-round zero-knowledge proof systems for np," *Journal of Cryptology*, vol. 9(2), pp. 167–189, 1996.

[71] O. Goldreich and H. Krawczyk, "On the composition of zero-knowledge proof systems," *SIAM Journal on Computing*, vol. 25(1), pp. 169–192, 1996.

[72] O. Goldreich and L. Levin, "Hard-core predicates for any one-way function," in *21st ACM Symposium on the Theory of Computing*, pp. 25–32, 1989.

[73] O. Goldreich and L. Levin, *Fair computation of general functions in presence of immoral majority*. Vol. 537, Springer-Verlag, 1991. *Crypto90* Lecture Notes in Computer Science.

[74] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game – a completeness theorem for protocols with honest majority," in *19th ACM Symposium on the Theory of Computing*, pp. 218–229, 1987. See details in (63).

[75] 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*, vol. 38(1), pp. 691–729, 1991. Preliminary version in *27th FOCS*, 1986.

[76] O. Goldreich and Y. Oren, "Definitions and properties of zero-knowledge proof systems," *Journal of Cryptology*, vol. 7(1), pp. 1–32, 1994.

[77] O. Goldreich, A. Sahai, and S. Vadhan, "Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge," in *30th ACM Symposium on the Theory of Computing*, pp. 399–408, 1998.

[78] O. Goldreich, S. Vadhan, and A. Wigderson, "On interactive proofs with a laconic provers," *Computational Complexity*, vol. 11, pp. 1–53, 2002.
[79] O. Goldreich and R. Vainish, *How to solve any protocol problem – an efficiency improvement*. Vol. 293, Springer-Verlag, 1988. *Crypto87* Lecture Notes in Computer Science.
[80] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Science*, vol. 28(2), pp. 270–299, 1984. Preliminary version in *14th STOC*, 1982.
[81] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on Computing*, vol. 18, pp. 186–208, 1989. Preliminary version in *17th STOC*, 1985.
[82] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, pp. 281–308, 1988.
[83] S. Golomb, *Shift Register Sequences*. Aegean Park Press, revised edition ed., 1982. Holden-Dat, 1967.
[84] R. Greenstadt, "Electronic voting bibliography," 2000. http://theory.lcs.mit.edu/ cis/voting/greenstadt-voting-bibligraphy.html.
[85] J. Håstad, R. Impagliazzo, L. Levin, and M. Luby, "A pseudorandom generator from any one-way function," *SIAM Journal on Computing*, vol. 28(4), pp. 1364–1396, 1999.
[86] M. Hirt and U. Maurer, "Complete characterization of adversaries tolerable in secure multi-party computation," *Journal of Cryptology*, vol. 13(1), pp. 31–60, 2000.
[87] R. Impagliazzo, L. Levin, and M. Luby, "Pseudorandom generation from one-way functions," in *21st ACM Symposium on the Theory of Computing*, pp. 12–24, 1989.
[88] R. Impagliazzo and M. Yung, *Direct zero-knowledge computations*. Vol. 293, Springer-Verlag, 1987. *Crypto87* Lecture Notes in Computer Science.
[89] J. Katz and M. Yung, "Complete characterization of security notions for probabilistic private-key encryption," in *32nd ACM Symposium on the Theory of Computing*, pp. 245–254, 2000.
[90] J. Kilian, "A note on efficient zero-knowledge proofs and arguments," in *24th ACM Symposium on the Theory of Computing*, pp. 723–732, 1992.
[91] J. Kilian and E. Petrank, "Concurrent and resettable zero-knowledge in polylogarithmic rounds," in *33rd ACM Symposium on the Theory of Computing*, pp. 560–569, 2001.
[92] D. Knuth, *The Art of Computer Programming*. Vol. 2, Addison-Wesley Publishing Company Inc, first edition ed., 1969.
[93] H. Krawczyk, *LFSR-based hashing and authentication*. Vol. 839, Springer-Verlag, 1994. *Crypto94* Lecture Notes in Computer Science.
[94] Y. Lindell, *Parallel coin-tossing and constant-round secure two-party computation*. Vol. 2139, Springer-Verlag, 2001. *Crypto01* Lecture Notes in Computer Science.
[95] Y. Lindell, A. Lysyanskaya, and T. Rabin, "On the composition of authenticated byzantine agreement," in *34th ACM Symposium on the Theory of Computing*, pp. 514–523, 2002.

[96] C. Lund, L. Fortnow, A. Karloff, and N. Nisan, "Algebraic methods for interactive proof systems," *Journal of the ACM*, vol. 39(4), pp. 859–868, 1992. Preliminary version in *31st FOCS*, 1990.
[97] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.
[98] R. Merkle, "Protocols for public key cryptosystems," in *Proc. of the 1980 Symposium on Security and Privacy*, 1980.
[99] S. Micali, "Computationally sound proofs," *SIAM Journal on Computing*, vol. 30(4), pp. 1253–1298, 2000. Preliminary version in *35th FOCS*, 1994.
[100] S. Micali and P. Rogaway, *Secure computation*. Vol. 576, Springer-Verlag, 1991. *Crypto91* Lecture Notes in Computer Science. Elaborated working draft available from the authors.
[101] M. Naor, "Bit commitment using pseudorandom generators," *Journal of Cryptology*, vol. 4, pp. 151–158, 1991.
[102] M. Naor and K. Nissin, "Communication preserving protocols for secure function evaluation," in *33rd ACM Symposium on the Theory of Computing*, pp. 590–599, 2001.
[103] M. Naor and M. Yung, "Universal one-way hash functions and their cryptographic application," in *21st ACM Symposium on the Theory of Computing*, pp. 33–43, 1989.
[104] M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," in *22nd ACM Symposium on the Theory of Computing*, pp. 427–437, 1990.
[105] R. Ostrovsky and A. Wigderson, "One-way functions are essential for non-trivial zero-knowledge," in *2nd Israel Symp. on Theory of Computing and Systems*, pp. 3–17, 1993. IEEE Comp. Soc. Press.
[106] R. Ostrovsky and M. Yung, "how to withstand mobile virus attacks," in *10th ACM Symposium on Principles of Distributed Computing*, pp. 51–59, 1991.
[107] M. Prabhakaran, A. Rosen, and A. Sahai, "Concurrent zero-knowledge proofs in logarithmic number of rounds," in *43rd IEEE Symposium on Foundations of Computer Science*, pp. 366–375, 2002.
[108] M. Rabin. Academic Press, 1977. *Foundations of Secure Computation* (R.A. DeMillo et al, eds).
[109] M. Rabin, "Digitalized signatures and public key functions as intractable as factoring," 1979. MIT/LCS/TR-212.
[110] T. Rabin and M. Ben-Or, "Verifiable secret sharing and multi-party protocols with honest majority," in *21st ACM Symposium on the Theory of Computing*, pp. 73–85, 1989.
[111] R. Richardson and J. Kilian, *On the concurrent composition of zero-knowledge proofs*. Vol. 1592, Springer, 1999. *EuroCrypt99* Lecture Notes in Computer Science.
[112] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, 1978.
[113] P. Rogaway, *The round complexity of secure protocols*. PhD thesis, MIT, 1991. Available from `http://www.cs.ucdavis.edu/~rogaway/papers`.

[114] J. Rompel, "One-way functions are necessary and sufficient for secure signatures," in *22nd ACM Symposium on the Theory of Computing*, pp. 387–394, 1990.

[115] A. Sahai and S. Vadhan, "A complete promise problem for statistical zero-knowledge," *Journal of the ACM*, vol. 50(2), pp. 1–54, 2003.

[116] A. D. Santis, G. D. Crescenzo, R. Ostrovsky, G. Persiano, and A. Sahai, *Robust non-interactive zero-knowledge*. Vol. 2139, Springer-Verlag, 2001. *Crypto01* Lecture Notes in Computer Science.

[117] A. Shamir, "How to share a secret," *Journal of the ACM*, vol. 22, pp. 612–613, 1979.

[118] A. Shamir, "Ip =pspace," *Journal of the ACM*, vol. 39(4), pp. 869–877, 1992. Preliminary version in *31st FOCS*, 1990.

[119] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1983.

[120] M. Sipser, "A complexity theoretic approach to randomness," in *15th ACM Symposium on the Theory of Computing*, pp. 330–335, 1983.

[121] S. Vadhan, *A Study of Statistical Zero-Knowledge Proofs*. PhD thesis, Department of Mathematics, MIT, 1999. Available from `http://www.eecs.harvard.edu/ salil/papers/phdthesis-abs.html`.

[122] S. Vadhan, "An unconditional study of computational zero knowledge," in *45th IEEE Symposium on Foundations of Computer Science*, pp. 176–185, 2004.

[123] A. Yao, "Theory and application of trapdoor functions," in *23rd IEEE Symposium on Foundations of Computer Science*, pp. 80–91, 1982.

[124] A. Yao, "How to generate and exchange secrets," in *27th IEEE Symposium on Foundations of Computer Science*, pp. 162–167, 1986.