New Directions in Cryptography: Twenty Some Years Later

(or Cryptograpy and Complexity Theory: A Match Made in Heaven)

Shafi Goldwasser*

Abstract of Talk

In 1976 Diffie and Hellman published thair fundamental paper on *New Directions in Cryptography*, in which they announced that "we stand on the brink of a revolution in cryptography".

Today, twenty some years later, we will survey some of the progress made in cryptography during this time. We will especially focus on the successful interplay between complexity theory and cryptography, witnessed perhaps most vividly by the developments in interactive and probabilistic proof systems and in pseudo radnom number generation. A list of topics to be touched upon during the talk is included, followed by refereneces in the bibliography.

FOUNDATIONS OF CRYPTOGRAPHY. Complexity theory based cryptography is based on the existence of one-way functions. Reformulated, a one-way function is a problem for which there is an efficiently samplable distribution of instances (to be used by the legal user), which are impossible on the average to solve efficiently by any probabilistic algorithm (the adversary). Taking efficient to mean polynomial time, basing cryptography on complexity theory is thus possible only if $NP \neq BPP$, although it is not known to be a sufficient condition. The existence of an NP-complete problem which can be shown as hard on the average to solve as in the worst case for some efficiently samplable distribution, is an open problem.

In lieu of techniques for proving even worst case non-linear lower bounds for natural NP problem, our goal is construct a theoretical foundation of the field by (1) finding the minimal necessary and sufficient assumption for every cryptographic application, and (2) constructing schemes that can be proven at least as secure as the minimal assumption necessary. The proofs take the form of a "reduction" showing how any break in the security of a system can be transformed into a violation of the underlying assumption.[1]. Defining what it means to be "secure", and what it means to "break" a cryptographic system is an essential first step in establishing these foundations.

IDENTIFYING BUILDING BLOCKS IN CRYPTOGRAPY: Any cryptographic system we know of (e.g encryption, signatures, oblivious transfer, key exchange) can be shown to imply the existence of one way functions. But, whereas

*MIT Laboratory for Computer Science, 545 Technology Square, Cambridge, MA 02139, USA, and the Weizmann Institute, Rehovot, Israel. e-mail: shafi@theory.lcs.mit.edu.

[1]Generally, we take efficient to mean probabilistic polynomial time and inefficient to mean non-polynomial time. We note however that security proofs are generally not affected by changing the definition of 'efficient ' and 'inefficient'. In a line of work initiated by [BKR, BGR], parameterized reductions are used which tightly monitor the cost of reductions made in security proofs, facilitating using arbitrary gaps between 'inefficient' and 'efficient'.

one-way functions are necessary, they are not always sufficient. In addition to one-way functions and trapdoor functions defined already in [DH], one-way predicates, trapdoor predicates [GM], oblivious transfer protocol[CK], bit commitment protocol, secret sharing among n users[SH], and computing with shares of a secret rather than directly with data directly[GMW2, BGW], have been identified as key building tools.It is interesting to investigate the relation between these primitives. In particular, in light of the work of [AD] the question of whether trapdoor predicates imply trapdoor functions is intriguing.

CANDIDATE HARD COMPUTATIONAL PROBLEMS: In order to actually use cryptosystems we need to find natural candidates for the abstract building blocks. The celebrated RSA function [RSA] pointed the way to number theory where several other suitable candidate hard problems can be found such as factoring integers, computing discrete log over finite fields, and distinguishing quadratic residues from quadratic non-residues modlo composite numbers. Other candidate hard problems found suitable are computing elliptic logarithm in a group of points defined by an elliptic curve over a finite field, decoding random linear error correcting codes, and of late an array of computational problems over lattices[AD, A, GGH]. Showing some relation between average case computational difficulty of the above problems and their worst case difficulty, is a central theme in the the field. For example, for fixed n, it can be proved that distinguishing between quadratic residues and non-residues modulo n is as hard on the average as in the worst case [GM]. Recently, [A] showed that computing the shortest vector in lattice (in which the shortest vector is unique upto a polynomial factor) is as hard on the average (taken over a certain samplable distribution of the lattices) as in the worst case. It remains an intriguing open problem to show the existence of an NP-complete problem which is as hard on the average to solve as in the worst case for some samplable distribution. An affirmative resolution would establish the existence of one-way functions on $P \neq NP$.

PROBABILISTIC METHODS: The use of probabilistic cryptosystems has emerged as essential for achieving security. It can be shown that probabilistic encryption algorithms are necessary in order to hide partial information about messages and handle arbitrary message spaces [GM]. Probabilistic signature algorithms are needed to achieve unforgeability in face of chosen message attacks [GMRi, 1, DN]. Another example is the replacment of traditional passwords by interactive and probabilistic identification protocols where the key idea behind the security is that the messages exachanged during the protocol are chosen randomly and independently every time the identification protocol is repeated [GMR, FFS, FS]. Interestingly, randomized variants of well-known algorithms such as RSA have made their way by now into tool kits such as SET(sceure elctronic transactions).

TWO-PARTY PROTOCOLS, ZERO KNOWLEDGE : The most exciting developments following public-key cryptography has been the in the area of protocols. First, there is a wide array of new capabilities that have been developed, such as secret-exchange, contract-signing, certified mail [Bsecret, Bcoin, R77, EGL], and more generaly any two-party computation can be performed maintaing correctness and secrecy of the inputs if oblivious transfer exists[Y2, K].

Second, the notion of zero-knowledge [GMR] protocols and proofs [GMR] has trasformed the field from an art form to a science. Zero knowledge yields a formal way to prove security of (or find mistakes in) protocols. Perhaps, more importantly zero knowledge protocols make possible achieving cryptographic tasks deemed impossible before. For example, zero-knowledge identification schemes allow an interactive password method in which all communication between the verifier (checking identity) and prover (being identified) can be sent over an insecure channel as mentioned above [FS]. Another example is that non-interactive zero knowledge enables building an encryption scheme which is provably secure against chosen message attacks if trapdoor functions exist [BFM, BDMP, 1].

More generally, any NP-statement can be proved in zero knowledge if one-way permutations exist [GMW1]. This allows an automatic translation of protocols proved secure for users who follow protocol instructions, into protocols which remain secure even when users may deviate arbitrarily from the legal protocol.

INTERACTIVE AND PROBABILISTIC PROOF SYSTEMS The first zero knowledge protocols were of simple Yes/No statements, in which one party (the prover) convinced another party (the verifier) with overwhelming probability of correctness that certain inputs were well formed (e.g. an integer n was factor of 2 primes, or an integer y was a quadratic residue mod n)[2]. Although simple NP proofs (i.e short witnesses) existed for these particular statements, the protocols made it possible to hide all other knowledge beside the correctness of the statement being proved. It became immediately apparent that these were not only cryptographic tools, but an alterantive way to prove statements correctly with high probability via an interactive process of questions and answers. The name "interactive proof" was coined [GMR][3], and the notion took a life of its own seperate from security applications. What seemed obvious for cryptographic purposes - that without randomization and interaction certain statements cannot be proved - turned out to be of much wider applicability to complexity theory at large. In a famous sequence of works by [GMW2, LFKN, SH2] it was first shown that a hard problem not known to be in NP - graph non-isomorphism - has an interactive proof, and finally that languages which have interactive proofs are exactly the PSPACE languages. Many other studies of the complexity of interactive proofs exist (see references). Curiously, the notion of Arthur-Merlin games which seemed like a restricted form of interactive form orginally, and was developed in [Ba] in order to classify the complexity of certain matrix group membership problems, turned out to coincide with interactive proofs in generality.

An extention of the interactive proof model to the multi-prover interactive proof model [BGKW], where a number of non-communicating provers are available, was made to enable proving that NP statements can be proved in zero knowledge without resorting to any assumptions. This model, has born even more surprising fruit to complexity theory. In [BFL] it is proved that languages which have multi-prover interactive proofs are exactly the NEXPTIME languages. By examining in a quantitative fashion the amount of randomness used by the verifier, and communication exchanged beween provers and verifier in a multi-prover proof it was further shown [BFLS, FGLSS, AS, ALMSS] (some of these works use the oracle formulation of multi-prover proofs [FRS]) that NP can be characterized as languages provable by multi-prover proofs with only logarithmic randomness and constant answer size. A surprising connection between multi-prover proofs with bounded resources and approximation problems was found in [FGLSS], and has subsequently enabled classifying the hardness of approximating a slew of optimization problems.

In return, on occasion, the efficient probabilistic proof checking methods developed for complexity purposes in the above models, have made their way back into cryptography [K2, M2].

PSEDUO RANDOMNESS Randomness for chosing secret keys was always recognized as an essential part of the security of a cryptographic system. Even more so today, when it is an integral part of the algorithms themselves. Thus, very early it became clear that good pseudo random number generators are necessary. From a line of exciting works [SH3, BM, Y] emerged the notion of cryptographically strong pseudo random number generators (cspsrg's) which produce sequences indistinguishable from truly random sequences by any probabilistic polynomial time algorithm. The notion was accompanied by constructions of cspsrg's under the assumption that one-way permutations exist, and particular efficient construction under specific number theoretic assumptions

[2]The fact that the prover knew some auxilary knowledge such as the factorization of n made it possible for him to convince the verifier of these facts withour revealing any extra knowledge

[3]Mike Sipser suggested this name when first hearing of a protocol to distinguish between composite numbers of 2 vs. 3 prime factors, thanks Mike!

[BBS, GMT, HSS, ACGS]. This culminated in the work of [GL, HILL] showing that cspsrg existence is equivalent to the existence of one-way functions. These constructs were shown by [Y] to have immediate consequences on relation betweeen probabilistic and deterministic complexity classed. Pseudo random functions [GGM] again were a reply to a cryptographic need of randomly accessing a cspsrg by many independent users, yet they have been used extensively to establish impossibility results in learning theory.

PROOF TECHNIQUES: A few dominant proof tecqhniques have emerged in security proofs. Among which are, probabilistic polynmial-time reducabilities between problems, simulation proofs, the hybrid method, and random self reducability. The latter was first observed as applied to the number theoretic problems of factoring, discrete log, testing quadratic residuosity, and the RSA function. For all of these problems, one could use the algebraic structure to show how to map a particular input uniformly and randomly to other inputs in such a way that the answer for the original input can be recovered from the answers for the targets of the random mapping. A trivial example is for RSA, fix $n = pq$ product of two prime numbers and $(e, \phi(n)) = 1$, $ed = 1 \bmod n$. Then, given $y = x^e \bmod n$, it is easy to map y to a random instance in Z_n^*, picking $z \in Z_n^*$ at random and setting $w = z^e y \bmod n$, such that from the inverse of w $w^D \bmod n$, x can be recovered by setting it to $x = w^d z^{-1}$. This random mapping can be thus utilized to find out x from y in expected polynomial time, if RSA could be inverted with non-negligible probability over Z_n^* for this n. Showing that polynomials are randomly self reducible over finite fields [BGW] [BF] was applied to the low-degree polynomial representations of Boolean functions, and has been a central and useful technique in probabilistically checkable proofs.

WHAT HAS THEORY OF CRYPTOGRAPHY DONE FOR PRACTICE: Theory of cryptography is inherintly a field which is inspired by practical problems. The underlying setting which we work with involves users and adversaries with varying capabillites, attempting to model real life scenarios. The practice of cryptography may be different than most other fields of applied computer science in that it truly uses theoretical ideas and inventions to operate. The RSA function is, naturaly, the overwhelming example. Other examples applied to practice already are zero knowledge identification schemes, the idea of how to catch double spending in Electronic Cash [CFN], probabilistic signature methods in SET [BRsign], verifiable secret sharing was applied to get split key escrow methods in the key escrow arena [M1].

FUTURE DIRECTIONS IN CRYPTOGRAPHY: Interestingly enough, twenty years later we are again at the brink of a revolution in cryptography. We have moved from the setting of a pair of sender and receiver who want to communicate privately and authenticaly, to the setting of the internet. This presents the challenge and possibility of performing complex distributed computations among a large number of potentially untrusted parties, maintaing correctness, privacy, authenticity, anonymity, and varying degrees of un/traceability. In the last part of this talk, we will discuss the topic of multi-party protocols (or distributed cryptography) which models this situation, and some of the future research directions posed by this setting.

We believe that the field of multi party computations is today where public-key cryptography was ten years ago, namely an extremely powerful tool and rich theory whose real-life usage is at this time only beginning but will become in the future an integral part of our computing reality.

References

[A] M. Ajtai. Generating Hard Instances of Lattice Problems. In *28th STOC*, pages 99–108, 1996.

[AD] M. Ajtai and C. Dwork. A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence, In *29th STOC*, pages 284–293, 1997.

[ACGS] W. Alexi, B. Chor, O. Goldreich and C.P. Schnorr. RSA/Rabin Functions: Certain Parts are As Hard As the Whole. *SICOMP*, Vol. 17, April 1988, pages 194–209.

[ALMSS] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and hardness of approximation problits. In *Proc. 33rd IEEE Symp. on Foundations of Computer Science*, pages 14–23, 1992.

[AS] S. Arora and S. Safra. Probabilistic checking of proofs: a new characterization of NP. In *Proc. 33rd IEEE Symp. on Foundations of Computer Science*, pages 2–13, 1992.

[Ba] L. Babai. Trading Group Theory for Randomness. In *17th STOC*, pages 421–420, 1985.

[BFLS] L. Babai, L. Fortnow, L. Levin, and M. Szegedy. Checking computations in poly-logarithmic time. In *Proc. 23rd ACM Symp. on Theory of Computing*, 1991.

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

[BeGr] M. Bellare and O. Goldreich. On Defining Proofs of Knowledge. In *CRYPTO92*, Springer-Verlag LNCS (Vol. 740), pages 390–420.

[BGG1] M. Bellare, O. Goldreich and S. Goldwasser. Incremental Cryptography: the Case of Hashing and Signing. In *CRYPTO94*, Springer-Verlag LNCS (Vol. 839), pages 216–233, 1994.

[BGG2] M. Bellare, O. Goldreich and S. Goldwasser. Incremental Cryptography and Application to Virus Protection. In *27th STOC*, pages 45–56, 1995.

[BGR] M. Bellare, R. Guerin and P. Rogaway. XOR MACs: New Methods for Message Authentication using Finite Pseudorandom Functions. In *CRYPTO95*, Springer-Verlag LNCS (Vol. 963), pages 15–28.

[BKR] M. Bellare, J. Kilian and P. Rogaway. The Security of Cipher Block Chaining. In *CRYPTO94*, Springer-Verlag LNCS (Vol. 839), pages 341–358.

[BeM] M. Bellare and S. Micali. How to Sign Given Any Trapdoor Function. *J. of the ACM*, Vol. 39, pages 214–233, 1992.

[BRsign] M. Bellare and P. Rogaway. The Exact Security of Digital Signatures: How to Sign with RSA and Rabin. In *EuroCrypt96*, Springer LNCS (Vol. 1070), pages 399–416.

[Betal] M. Ben-Or, O. Goldreich, S. Goldwasser, J. Håstad, J. Kilian, S. Micali and P. Rogaway. Everything Provable is Probable in Zero-Knowledge. In *CRYPTO88*, Springer-Verlag LNCS (Vol. 403), pages 37–56, 1990.

[BGKW] M. Ben-or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi prover interactive proofs: How to remove intractability. In *Proc. 20th ACM Symp. on Theory of Computing*, pages 113–131, 1988.

[BGW] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation. In *20th STOC*, pages 1–10, 1988.

[Blk] G. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings*, June 1979.

[BBS] L. Blum, M. Blum and M. Shub. A Simple Secure Unpredictable Pseudo-Random Number Generator. *SIAM J. on Comput.*, Vol. 15, 1986, pages 364–383.

[Bsecret] M. Blum. How to Exchange Secret Keys. *ACM Trans. Comput. Sys.*, Vol. 1, pages 175–193, 1983.

[Bcoin] M. Blum. Coin Flipping by Phone. *IEEE Spring COMPCOM*, pages 133–137, February 1982. See also *SIGACT News*, Vol. 15, No. 1, 1983.

[BDMP] M. Blum, A. De Santis, S. Micali, and G. Persiano. Non-Interactive Zero-Knowledge Proof Systems. *SIAM J. on Comput.*, Vol. 20, No. 6, pages 1084–1118, 1991. (Considered the journal version of [BFM].)

[BFM] M. Blum, P. Feldman and S. Micali. Non-Interactive Zero-Knowledge and its Applications. In *20th STOC*, pages 103–112, 1988. See [BDMP].

[BlGw] M. Blum and S. Goldwasser. An Efficient Probabilistic Public-Key Encryption Schite which hides all partial information. In *CRYPTO84*, LNCS (Vol. 196) Springer-Verlag, pages 289–302.

[BM] M. Blum and S. Micali. How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits. *SIAM J. on Comput.*, Vol. 13, pages 850–864, 1984. Preliminary version in *23rd FOCS*, 1982.

[BDL] D. Boneh, R. DeMillo and R. Lipton. On the Importance of Checking Cryptographic Protocols for Faults. In *EuroCrypt97*, Springer LNCS (Vol. 1233), pages 37–51, 1997.

[BHZ] R. Boppana, J. Hastad, and S. Zachos. Does Co-NP Have Short Interactive Proofs? *IPL*, 25, May 1987, pp. 127-132.

[Bo] J. B. Boyar. Inferring Sequences Produced by Pseudo-Random Number Generators. *J. of the ACM*, Vol. 36, pages 129–141, 1989.

[BCC] G. Brassard, D. Chaum and C. Crépeau. Minimum Disclosure Proofs of Knowledge. *J. of Comp. and Sys. Sci.*, Vol. 37, No. 2, pages 156–189, 1988. Preliminary version by Brassard and Crépeau in *27th FOCS*, 1986.

[BC] G. Brassard and C. Crépeau. Zero-Knowledge Simulation of Boolean Circuits. In *CRYPTO86*, Springer-Verlag LNCS (Vol. 263), pages 223–233, 1987.

[Br] G. Brassard. Relativized Cryptography. In *20th FOCS*, pages 383–391, 1979.

[ran95] R. Canetti. *Studies in Secure Multi-Party Computation and Applications.* Ph.D. Thesis, Department of Computer Science and Applied Mathitatics, Weizmann Institute of Science, Rehovot, Israel, June 1995. Available from `http://theory.lcs.mit.edu/tcryptol/BOOKS/ran-phd.html`.

[CDNO] R. Canetti, C. Dwork, M. Naor and R. Ostrovsky. Deniable Encryption. In *CRYPTO97*, Springer LNCS (Vol. 1294).

[CG] R. Canetti and R. Gennaro. Incoercible Multiparty Computation. In *37th FOCS*, pages 504–513, 1996.

[CHH] R. Canetti, S. Halevi and A. Herzberg. How to Maintain Authenticated Communication in the Presence of Break-Ins. In *16th Symp. on Principles of Distributed Computing*, 1997.

[CH] R. Canetti and A. Herzberg. Maintaining Security in the Presence of Transient Faults. In *CRYPTO94*, Springer-Verlag LNCS (Vol. 839), pages 425–439.

[C82] D. Chaum. Blind Signatures for Untraceable Payments. In *CRYPTO82*, Plenum Press, pages 199–203, 1983.

[CCD] D. Chaum, C. Crépeau and I. Damgård. Multi-party unconditionally Secure Protocols. In *20th STOC*, pages 11–19, 1988.

[CFN] D. Chaum, A. Fiat and M. Naor. Untraceable Electronic Cash. In *CRYPTO88*, Springer-Verlag LNCS (Vol. 403), pages 319–327.

[cpir] B. Chor and N. Gilboa. Computationally Private Information Retrieval. In *29th STOC*, pages 304–313, 1997.

[pir] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, Private Information Retrieval. In *36th FOCS*, pages 41–50, 1995.

[CGMA] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. In *26th FOCS*, pages 383–395, 1985.

[Cl] R. Cleve. Limits on the Security of Coin Flips when Half the Processors are Faulty. In *18th STOC*, pages 364–369, 1986.

[CDP] R. Cramer, I. Damgård, and T. Pedersen. Efficient and provable security amplifications. In *Proc. of 4th Cambridge Security Protocols Workshop*, Springer, LNCS (Vol. 1189), pages 101–109.

[CK] C. Crepeau and J. Kilian. "Achieving Oblivious Transfer Using Weakened security Assumptions", *29th FOCS*, pp. 42-52.

[D87] I. Damgård. Collision Free Hash Functions and Public Key Signature Schites. In *EuroCrypt87*, Springer-Verlag, LNCS (Vol. 304), pages 203–216.

[DDFY] A. De-Santis, Y. Desmedt, Y. Frankel and M. Yung. How to Share a Function Securely. In *26th STOC*, pages 522–533, 1994.

[DF89] Y. Desmedt and Y. Frankel. Threshold Cryptosystems. In *CRYPTO89*, Springer-Verlag LNCS (Vol. 435), pages 307–315.

[DH] W. Diffie, and M.E. Hellman. New Directions in Cryptography. *IEEE Trans. on Info. Theory*, IT-22 (Nov. 1976), pages 644–654.

[DDN] D. Dolev, C. Dwork, and M. Naor. Non-Malleable Cryptography. In *23rd STOC*, pages 542–552, 1991. Full version available from authors.

[DN] C. Dwork, and M. Naor. An Efficient Existentially Unforgeable Signature Schite and its Application. To appear in *J. of Cryptography.* Preliminary version in *Crypto94*.

[EG83] S. Even and O. Goldreich. On the Security of Multi-party Ping-Pong Protocols. *24th FOCS*, pages 34–39, 1983.

[EGL] S. Even, O. Goldreich, and A. Litpel. A Randomized Protocol for Signing Contracts. *CACM*, Vol. 28, No. 6, 1985, pages 637–647.

[EGM] S. Even, O. Goldreich and S. Micali. On-line/Off-line Digital signatures. *J. of Crypto.*, Vol. 9, 1996, pages 35–67.

[ESY] S. Even, A.L. Selman, and Y. Yacobi. The Complexity of Promise Problits with Applications to Public-Key Cryptography. *Inform. and Control*, Vol. 61, pages 159–173, 1984.

[EY80] S. Even and Y. Yacobi. Cryptography and NP-Completeness. In proceedings of *7th ICALP*, Springer-Verlag LNCS (Vol. 85), pages 195–207, 1980. See [ESY].

[FFS] U. Feige, A. Fiat and A. Shamir. Zero-Knowledge Proofs of Identity. *J. of Crypto.*, Vol. 1, 1988, pages 77–94.

[FLS] U. Feige, D. Lapidot, and A. Shamir. Multiple Non-Interactive Zero-Knowledge Proofs Based on a Single Random String. In *31th FOCS*, pages 308–317, 1990. To appear in *SIAM J. on Comput.*.

[FGLSS] U. Feige, S. Goldwasser, L. Lovasz, S. Safra, and M. Szegedi. Approximating clique is almost NP-complete. In *Proc. 32nd IEEE Symp. on Foundations of Computer Science*, pages 2–12, 1991.

[FeSm] U. Feige and A. Shamir. Witness Indistinguishability and Witness Hiding Protocols. In *22nd STOC*, pages 416–426, 1990.

[Fel] P. Feldman. A Practical Scheme for Non-interactive Verifiable Secret Sharing. In *28th FOCS*, pages 427–437, 1987.

[FS] A. Fiat and A. Shamir. How to Prove Yourself: Practical Solution to Identification and Signature Problits. In *CRYPTO86*, Springer-Verlag LNCS (Vol. 263), pages 186–189, 1987.

[FrSt] J.B. Fischer and J. Stern. An Efficient Pseudorandom Generator Provably as Secure as Syndrome Decoding. In *EuroCrypt96*, Springer LNCS (Vol. 1070), pages 245–255.

[FnSn] R. Fischlin and C.P. Schnorr. Stronger Security Proofs for RSA and Rabin Bits. In *EuroCrypt97*, Springer LNCS (Vol. 1233), pages 267–279, 1997.

[FRS] L. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. In *Proc. 3rd STRUCTURES*, pages 156–161, 1988.

[G89] O. Goldreich. *Lecture Notes on Encryption, Signatures and Cryptographic Proto-col.* Spring 1989. Available from `http://theory.lcs.mit.edu/oded/ln89.html`.

[G95] O. Goldreich. *Foundation of Cryptography–Fragments of a Book.* ed. Dept. of Computer Science and Applied Mathematics, Weizmann Institute, February 1995. Available from `http://theory.lcs.mit.edu/oded/frag.html`.

[GGH] O. Goldreich, S. Goldwasser and S. Halevi. Public-Key Cryptosystems from Lattice Reduction Problems. In *Crypto97*, Springer LNCS, Vol. 1294, pp. 112–131.

[GGM] O. Goldreich, S. Goldwasser, and S. Micali. How to Construct Random Functions. *J. of the ACM*, Vol. 33, No. 4, pages 792–807, 1986.

[GGM2] O. Goldreich, S. Goldwasser, and S. Micali. On the Cryptographic Applications of Random Functions. In *CRYPTO84*, Springer-Verlag LNCS (Vol. 263), pages 276–288, 1985.

[GILVZ] O. Goldreich, R. Impagliazzo, L.A. Levin, R. Venkatesan, and D. Zuckerman. Security Preserving Amplification of Hardness. In *31st FOCS*, pages 318–326, 1990.

[GK] O. Goldreich and H. Krawczyk. On the Composition of Zero-Knowledge Proof Systems. *SIAM J. on Comput.*, Vol. 25, No. 1, February 1996, pages 169–192.

[GL] O. Goldreich and L.A. Levin. Hard-core Predicates for any One-Way Function. In *21st STOC*, pages 25–32, 1989.

[GMW1] O. Goldreich, S. Micali and A. Wigderson. Proofs that Yield Nothing but their Validity or All Languages in NP Have Zero-Knowledge Proof Systems. *J. of the ACM*, Vol. 38, No. 1, pages 691–729, 1991. Preliminary version in *27th FOCS*, 1986.

[GMW2] O. Goldreich, S. Micali and A. Wigderson. How to Play any Mental Game – A Completeness Theorit for Protocols with Honest Majority. In *19th STOC*, pages 218–229, 1987.

[Gw] S. Goldwasser. Fault Tolerant Multi Party Computations: Past and Present. In *16th Symp. on Principles of Distributed Computing*, 1997. Also available from `http://www.cs.cornell.edu/Info/People/chandra/podc97/newProgram.html`.

[GwL] S. Goldwasser and L. A. Levin. Fair Computation of General Functions in Presence of Immoral Majority. In *CRYPTO90*, Springer-Verlag LNCS (Vol. 537), pages 77–93.

[GM] S. Goldwasser and S. Micali. Probabilistic Encryption. *J. of Comp. and Sys. Sci.*, Vol. 28, No. 2, pages 270–299, 1984. Preliminary version in *14th STOC*, 1982.

[GMR] S. Goldwasser, S. Micali and C. Rackoff. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. on Comput.*, Vol. 18, pages 186–208, 1989. Preliminary version in *17th STOC*, 1985.

[GMRi] S. Goldwasser, S. Micali, and R. L. Rivest. A Digital Signature Schite Secure Against Adaptive Chosen-Message Attacks. *SIAM J. on Comput.*, April 1988, pages 281–308.

[GMT] S. Goldwasser, S. Micali and P. Tong. Why and How to Establish a Private Code in a Public Network. In *23rd FOCS*, 1982, pages 134–144.

[GMY] S. Goldwasser, S. Micali and A.C. Yao. Strong Signature Schites. In *15th STOC*, pages 431–439, 1983.

[GS] S. Goldwasser and M. Sipser. Private Coins versus Public Coins in Interactive Proof Systems. In *18th STOC*, pages 59–68, 1986.

[HILL] J. Håstad, R. Impagliazzo, L.A. Levin and M. Luby. Construction of Pseudorandom Generator from any One-Way Function. To appear in *SIAM J. on Comput.*. Preliminary versions by Impagliazzo et. al. in *21st STOC* (1989) and Håstad in *22nd STOC* (1990).

[HSS] J. Håstad, A. Schrift and A. Shamir. The Discrete Logarithm Modulo a Composite Hides $O(n)$ Bits. *J. of Comp. and Sys. Sci.*, Vol. 47, pages 376–404, 1993.

[HJKY] A. Herzberg, S. Jarecki, H. Krawczyk and M. Yu. Proactive Secret Sharing, or How to Cope with Perpetual Leakage. In *CRYPTO95*, Springer-Verlag LNCS (Vol. 963), pages 339–352.

[IL] R. Impagliazzo and M. Luby. One-Way Functions are Essential for Complexity Based Cryptography. In *30th FOCS*, pages 230-235, 1989.

[IN] R. Impagliazzo and M. Naor. Efficient Cryptographic Schemes Provable as Secure as Subset Sum. *J. of Crypto.*, Vol. 9, 1996, pages 199–216.

[IR] R. Impagliazzo and S. Rudich. Limits on the Provable Consequences of One-Way Permutations. In *21st STOC*, pages 44–61, 1989.

[JLO] A. Juels, M. Luby and R. Ostrovsky. Security of Blind Digital Signatures. In *CRYPTO97*, Springer LNCS (Vol. 1294).

[K] J. Kilian. "Founding Cryptography on Oblivious Transfer", *STOC 88,* pp. 20-31.

[K2] J. Kilian. A Note on Efficient Zero-Knowledge Proofs and Arguments. In *24th STOC*, pages 723–732, 1992.

[KP] J. Kilian and E. Petrank. An Efficient Non-Interactive Zero-Knowledge Proof System for NP with General Assumptions. To appear in *J. of Crypto.*.

[KO] E. Kushilevitz and R. Ostrovsky. Replication is not Needed: A Single Database, Computational PIR. TR CS0906, Department of Computer Science, Technion, May 1997. To appear in *38th FOCS*, 1997.

[L79] A. Litpel. Cryptography in Transition. *Computing Surveys*, Dec. 1979.

[L87] L. A. Levin. One-Way Function and Pseudorandom Generators. *Combinatorica*, Vol. 7, pages 357–363, 1987.

[L] M. Luby. *Pseudorandomness and Cryptographic Applications.* Princeton University Press, 1996.

[LR] M. Luby and C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. on Comput.*, Vol. 17, 1988, pages 373–386.

[LFKN] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *JACM*, 39 (1992), 859–868.

[LY] C. Lund and M. Yannakakis. On the hardness of approximating minimization problits. *JACM*, 41(5):960–981, 1994.

[M1] S. Micali. Fair Public-Key Cryptosystems. In *CRYPTO92*, Springer-Verlag LNCS (Vol. 740), pages 113–138.

[M2] S. Micali. CS Proofs. In *35th FOCS*, pages 436–453, 1994.

[M80] R.C. Merkle. Protocols for public key cryptoystems. In *Proc. of the 1980 Symposium on Security and Privacy.*

[M87] R.C. Merkle. A Digital Signature Based on a Conventional Encryption Function. In *CRYPTO87*, Springer-Verlag LNCS (Vol. 293), 1987, pages 369-378.

[M89] R.C. Merkle. A Certified Digital Signature Schite. In *CRYPTO89*, Springer-Verlag LNCS (Vol. 435), pages 218–238.

[MH78] R.C. Merkle and M.E. Hellman. Hiding Information and Signatures in Trapdoor Knapsacks. *IEEE Trans. Inform. Theory*, Vol. 24, pages 525–530, 1978.

[DSS] National Institute for Standards and Technology. **Digital Signature Standard** (DSS), *Federal Register*, Vol. 56, No. 169, August 1991.

[N] M. Naor. Bit Commitment using Pseudorandom Generators. *J. of Crypto.*, Vol. 4, pages 151–158, 1991.

[NOVY] M. Naor, R. Ostrovsky, R. Venkatesan and M. Yung. Zero-Knowledge Arguments for NP can be Based on General Assumptions. In *CRYPTO92*, Springer-Verlag LNCS (Vol. 740), pages 196–214.

[NR] M. Naor and O. Reingold. Synthesizers and their Application to the Parallel Construction of Pseudo-Random Functions. In *36th FOCS*, pages 170–181, 1995.

[NR2] M. Naor and O. Reingold. On the Construction of Pseudo-Random Permutations: Luby-Rackoff Revisited. In *29th STOC*, pages 189–199, 1997.

[NR3] M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudo-random functions and other cryptographic primitives. To appear in *38th FOCS*, 1997.

[1] M. Naor and M. Yung. Universal One-Way Hash Functions and their Cryptographic Application. *21st STOC*, 1989, pages 33–43.

[NY90] M. Naor and M. Yung. Public-Key Cryptosystems Provably Secure Against Chosen Ciphertext Attacks. In *22nd STOC*, pages 427-437, 1990.

[OW] 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*, IEEE Comp. Soc. Press, pages 3–17, 1993.

[OY] R. Ostrovsky and M. Yung. How to Withstand Mobile Virus Attacks. In *10th Symp. on Principles of Distributed Computing*, pages 51–59, 1991.

[P] B. Pfitzmann. *Digital Signature Schemes (General Framework and Fail-Stop Signatures)*. Springer LNCS (Vol. 1100), 1996.

[R77] M.O. Rabin. Digitalized Signatures. In *Foundations of Secure Computation* (R.A. DeMillo et. al. eds.), Academic Press, 1977.

[R79] M.O. Rabin. Digitalized Signatures and Public Key Functions as Intractable as Factoring. MIT/LCS/TR-212, 1979.

[R81] M.O. Rabin. How to Exchange Secrets by Oblivious Transfer. Tech. Mito TR-81, Aiken Computation Laboratory, Harvard U., 1981.

[TRa] T. Rabin. "Robust Sharing of Secrets When The Dealer is Honest or Faulty", *Journal of the ACM*, No. 6, Vol. 41, 1994, pp. 1089-1109.

[RB] T. Rabin and M. Ben-Or. Verifiable Secret Sharing and Multi-party Protocols with Honest Majority. In *21st STOC*, pages 73–85, 1989.

[RSA] R. Rivest, A. Shamir and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *CACM*, Vol. 21, Feb. 1978, pages 120–126.

[R90] J. Rompel. One-way Functions are Necessary and Sufficient for Secure Signatures. In *22nd STOC*, 1990, pages 387–394.

[S] C.E. Shannon. Communication Theory of Secrecy Systems. *Bell Sys. Tech. J.*, Vol. 28, pages 656–715, 1949.

[SH] A. Shamir. "How to share a secret", *CACM, Vol. 22, No. 11,* 1979, pp. 612-613.

[SH2] A. Shamir. IP=PSPACE. *JACM*, 39 (1992), 869–877.

[SH3] Adi Shamir. The generation of cryptographically strong pseudo-random sequences. In Allen Gersho, editor, *Advances in Cryptology: A Report on CRYPTO 81*, pages 1–1. U.C. Santa Barbara Dept. of Elec. and Computer Eng., 1982. Tech Report 82-04.

[SRA] A. Shamir, R. L. Rivest, and L. Adlitan. Mental Poker. MIT/LCS Report TM-125, 1979.

[VV] U. V. Vazirani and V. V. Vazirani. Efficient and Secure Pseudo-Random Number Generation. *25th FOCS*, pages 458–463, 1984.

[WC] M. Wegman and L. Carter. New Hash Functions and their Use in Authentication and Set Equality. *JCSS*, Vol. 22, 1981, pages 265–279.

[Y] A. C. Yao. Theory and Application of Trapdoor Functions. In *23rd FOCS*, pages 80–91, 1982.

[Y1] A. C Yao. "Protocols for Secure Computation", *23th FOCS,* 1982, pp. 160-164.

[Y2] A. C. Yao. How to Generate and Exchange Secrets. In *27th FOCS*, pages 162–167, 1986.