Appendix A

Annotated List of References (compiled Feb. 1989)

Author's Note: *The following list of annotated references was compiled by me more than five years ago. The list was intended to serve as an appendix to class notes for my course on "Foundations of Cryptography" given at the Technion in the Spring of 1989. Thus, a few pointers to lectures given in the course appear in the list.*

Author's Note: *By the way, copies of the above-mentioned class notes, written mostly by graduate students attending my course, can be requested from the publication officer of the Computer Science Department of the Technion, Haifa, Israel. Although I have a very poor opinion of these notes, I was surprised to learn that they have been used by several people. The only thing that I can say in favour of these notes is that they cover my entire (one-semester) course on "Foundations of Cryptography"; in particular, they contain material on encryption and signatures (which is most missing in the current fragments).*

Preface

The list of references is partitioned into two parts: Main References and Suggestions for Further Reading. The Main References consists of the list of papers that I have *extensively* used during the course. Other papers which I mentioned briefly may be found in the list of Suggestions for Further Reading. This second list also contains papers, reporting further developments, which I have not mentioned at all.

Clearly, my suggestions for further reading do not exhaust all interesting works done in the area. Some good works were omitted on purpose (usually when totally superseeded by others) and some were omitted by mistake. Also, no consistent policy was implemented in deciding which version of the work to cite. In most cases I used the reference which I had available on line (as updating all references would have taken too much time).

PART I : Main References

[BM88] Bellare, M., and S. Micali, "How to Sign Given any Trapdoor Function", *Proc. 20th STOC*, 1988.

Simplifies the construction used in [GMR84], using a weaker condition (i.e. the existence of trapdoor one-way permutations).
Readability: reasonable.

[BM82] Blum, M., and Micali, S., "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits", *SIAM Jour. on Computing*, Vol. 13, 1984, pp. 850-864. First version in *FOCS 1982*.

Presents a general method of constructing pseudorandom generators, and the first example of using it. Characterizes such generators as passing all (polynomial-time) prediction tests. Presents the notion of a "hard-core" predicate and the first proof of the existence of such predicate based on the existence of a particular one-way function (i.e. Discrete Logarithm Problem).
Readability: confusing in some places, but usually fine.

[GL89] Goldreich, O., and L.A. Levin, "A Hard-Core Predicate to any One-Way Function", *21st STOC*, 1989, pp. 25-32.

Shows that any "padded" one-way function $f(x,p) = f_0(x) \cdot p$, has a simple hard-core bit, the inner-product mod-2 of x and p.
Readability: STOC version is very elegant and laconic (Levin wrote it). These notes present a more detailed but cumbersome version.

[GMW86] Goldreich, O., S. Micali, and A. Wigderson, "Proofs that Yield Nothing But their Validity and a Methodology of Cryptographic Protocol Design", *Proc. of 27th Symp. on Foundation of Computer Science*, 1986, pp. 174-187. A full version appears as TR-544, Computer Science Dept., Technion, Haifa, Israel.

Demonstrates the generality and the wide applicability of zero-knowledge proofs. In particular, using any bit commitment scheme, it is shown how to construct a zero-knowledge proof for any language in $\mathcal{NP}$. Perfect zero-knowledge proofs are presented for Graph Isomorphism and its complement.

Readability: the full version is very detailed, sometimes to a point of exhausting the reader. A more elegant proof of the main result is sketched in [G89a].

[GMW87] Goldreich, O., S. Micali, and A. Wigderson, "How to Play any Mental Game", *19th STOC*, 1987. A more reasonable version is available from me.

Deals with the problem of cryptographic protocols in its full generality, showing how to automatically generate fault-tolerant protocols for computing any function (using any trapdoor one-way permutation).
Readability: STOC version is too hand-waving. These notes constitute a better source of information.

[GM82] Goldwasser, S., and S. Micali, "Probabilistic Encryption", *JCSS*, Vol. 28, No. 2, 1984, pp. 270-299. Previous version in *STOC 1982*.

Introduces the concept of polynomially indistinguishable probability distributions. Presents notions of secure encryption, demonstrating the inadequency of previous intuitions. Presents a general method for constructing such encryption schemes, and a first application of it. First use of the "hybrid" method.
Readability: Nice introduction. The technical part is somewhat messy.

[GMR85] Goldwasser, S., S. Micali, and C. Rackoff, "The Knowledge Complexity of Interactive Proof Systems", *SIAM J. on Comput.*, Vol. 18, No. 1, 1989, pp. 186-208. Previous version in *STOC 1985*.

Introduces the concepts of an interactive proof and a zero-knowledge proof. Presents the first (non-trivial) example of a zero-knowledge proof. First application of zero-knowledge to the design of cryptographic protocols.
Readability: good.

[GMR84] Goldwasser, S., S. Micali, and R.L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen Message Attacks", *SIAM J on Comput.*, Vol. 17, No. 2, 1988, pp. 281-308. Previous version in *FOCS 1984*.

Surveys and investigates definitions of unforgeable signatures. Presents the first signature scheme which is unforgeable in a very strong sense even under a chosen message attack.
Readability: excellent as an introduction to the problem. Don't read the construction, but rather refer to [BM88].

[Y82] Yao, A.C., "Theory and Applications of Trapdoor Functions", *Proc. of the 23rd IEEE Symp. on Foundation of Computer Science*, 1982, pp. 80-91.

Presents a general definition of polynomially indistinguishable probability distributions. Characterizes pseudorandom generators as passing all (polynomial-time) statistical tests. (This formulation is equivalent to passing all polynomial-time prediction tests.) Given any one-way permutation constructs a pseudorandom generator.
Readability: Most interesting statements are not stated explicitly. Furthermore, contains no proofs.

PART II : Suggestions for Further Reading

My suggestions for further reading are grouped under the following categories:

1. *General:* Papers which deal or relate several of the following categories.
2. *Hard Computational Problems:* Pointers to literature on seemingly hard computational problems (e.g. integer factorization) and to works relating different hardness criteria.
3. *Encryption:* Papers dealing with secure encryption schemes (in the strong sense defined in lecture 5B and 6).
4. *Pseudorandomness:* Papers dealing with the construction of pseudorandom generators, pseudorandom functions and permutations and their applications to cryptography and complexity theory.
5. *Signatures and Commitment Schemes:* Papers dealing with unforable signature schemes (as defined in lecture 10) and secure commitment schemes (mentioned in lecture 13).
6. *Interactive Proofs, Zero-Knowledge and Protocols:* In addition to papers with apparent relevance to cryptography this list contains also papers investigating the complexity theoretic aspects of interactive proofs and zero-knowledge.
7. *Additional Topics:* Pointers to works on software protection, computation with an untrusted oracle, protection against abuse of cryptographic systems, Byzantine Agreement, sources of randomness, and "cryptanalysis".
8. *Historical Background:* The current approach to Cryptography did not emerge "out of the blue". It originates in works that were not referenced in the previous categories (which include only material conforming with the definitions and concepts presented in the course). This category lists some of these pioneering works.

A.1 General

Much of the current research in cryptography focuses on reducing the existence of complex cryptographic primitives (such as the existence of unforgeable signature schemes) to simple complexity assumptions (such as the existence of one-way functions). A first work investigating the limitations of these reductions is [IR89], where a "gap" between tasks implying secret key exchange and tasks reducible to the existence of one-way functions is shown. The gap is in the sense that a reduction of the first task to the second would imply $\mathcal{P} \neq \mathcal{NP}$.

Many of the more complex results in cryptography (e.g. the existence of zero-knowledge interactive proofs for all languages in $\mathcal{NP}$) are stated and proved in terms of non-uniform complexity. As demonstrated throughout the course, this simplifies both the statements and their proofs. An attempt to treat secure encryption and zero-knowledge in uniform complexity measures is reported in [G89a]. In fact, the lectures on secure encryption are based on [G89a].

references

[G89a] Goldreich, O., "A Uniform-Complexity Treatment of Encryption and Zero-Knowledge", TR-568, Computer Science Dept., Technion, Haifa, Israel, 1989.

[IR89] Impagliazzo, R., and S. Rudich, "Limits on the Provable Consequences of One-Way Permutations", *21st STOC*, pp. 44-61, 1989.

A.2 Hard Computational Problems

2.1. Candidates for One-Way functions

Hard computational problems are the basis of cryptography. The existence of adequately hard problems (see lecture 2) is not known. The most popular candidates are from computational number theory: integer factorization (see [P82] for a survey of the best algorithms known), discrete logarithms in finite fields (see [O84] for a survey of the best algorithms known), and the logarithm problem for "Elliptic groups" (cf. [M85]). Additional suggestions are the decoding problem for random linear codes (see [GKL88] and [BMT78]) and *high density* subset-sum ("knapsack") problems (see [CR88, IN89]). Note that *low density* subset-sum problems are usually easy (see survey [BO88]).

Much of the early-80th research in cryptography used the intractability assumption of the Quadratic Residuousity Problem (introduced in [GM82]). The nice structure of the problem was relied upon in constructions as [LMR83], but in many cases further research led to getting rid of the need to rely on the special structure (and to using weaker intractability assumptions).

Attempts to base cryptography on computationally hard combinatorial problems have been less popular. Graph Isomorphism is very appealing (as it has a nice structure as the Quadratic Residuousity Problem), but such a suggestion should not be taken seriously unless one specifies an easily samplable instance distribution for which the problem seems hard.

For details on candidates whose conjectured hardness was refuted see category 7.6.

2.2. Generic Hard Problems

The universal one-way function presented in lecture 3 originates from [L85]. The same ideas were used in [G88a] and [AABFH88], but the context there is of "average case complexity" (originated in [L84] and surveyed in [G88a]). In this context "hard" means intractable on infinitely many instance lengths, rather than intractable on all but finitely many instance lengths. Such problems are less useful in cryptography.

2.3. Hard-Core Predicates

As pointed out in lecture 4, hard-core predicates are a useful tool in cryptography. Such predicates are known to exist for exponentiation modulo a prime [BM82], (more generally) for "repeated addition" in any Abelian group [K88] and for the RSA and Rabin (squaring mod N) functions [ACGS84]. Recall that the general result of [GL89] (see lectures 4-5A) guarantees the existence of hard-core predicates for any "padded" function.

references

[AABFH88] Abadi, M., E. Allender, A. Broder, J. Feigenbaum, and L. Hemachandra, "On Generating Hard, Solved Instances of Computational Problem", *Crypto88* proceedings.

[ACGS84] W. Alexi, B. Chor, O. Goldreich and C.P. Schnorr, "RSA and Rabin Functions: Certain Parts Are As Hard As the Whole", *SIAM Jour. on Computing*, Vol. 17, 1988, pp. 194-209. A preliminary version appeared in *Proc. 25th FOCS*, 1984, pp. 449-457.

[BM82] see main references.

[BMT78] Berlekamp, E.R., R.J. McEliece, and H.C.A. van Tilborg, "On the Inherent Intractability of Certain Coding Problems", *IEEE Trans. on Inform. Theory*, 1978.

[BO88] Brickell, E.F., and A.M. Odlyzko, "Cryptanalysis: A Survey of Recent Results", *Proceedings of the IEEE*, Vol. 76, pp. 578-593, 1988.

[CR88] Chor, B., and R.L. Rivest, "A Knapsack Type Public-Key Cryptosystem Based on Arithmetic in Finite Fields", *IEEE Trans. on Inf. Th.*, Vol. 34, pp. 901-909, 1988.

[G88a] Goldreich, O., "Towards a Theory of Average Case Complexity (a survey)", TR-531, Computer Science Dept., Technion, Haifa, Israel, 1988.

[GKL88] see category 4.

[GL89] see main references.

[GM82] see main references.

[IN89] Impagliazzo, R., and M. Naor, "Efficient Cryptographic Schemes Provable as Secure as Subset Sum", manuscript, 1989.

[K88] B.S. Kaliski, Jr., "Elliptic Curves and Cryptography: A Pseudorandom Bit Generator and Other Tools", Ph.D. Thesis, LCS, MIT, 1988.

[L84] Levin, L.A., "Average Case Complete Problems", *SIAM Jour. of Computing*, 1986, Vol. 15, pp. 285-286. Extended abstract in *16th STOC*, 1984.

[L85] see category 4.

[LW] D.L. Long and A. Wigderson, "How Discreet is Discrete Log?", *Proc. 15th STOC*, 1983, pp. 413-420. A better version ?

[LMR83] see category 6.

[M85] Miller, V.S., "Use of Elliptic Curves in Cryptography", *Crypto85 - Proceedings*, Lecture Notes in Computer Science, Vol. 218, Springer Verlag, 1985, pp. 417-426.

[O84] Odlyzko, A.M., "Discrete Logarithms in Finite Fields and their Cryptographic Significance", *Eurocrypt84* proceedings, Springer-Verlag, Lecture Notes in Computer Science, Vol. 209, pp. 224-314, 1985. manuscript.

[P82] Pomerance, C., "Analysis and Comparison of some Integer Factorization Algorithms", *Computational Methods in Number Theory:* Part I, H.W. Lenstra Jr. and R. Tijdeman eds., Math. Center Amsterdam, 1982, pp. 89-139.

A.3 Encryption

The efficient construction of a secure public-key encryption scheme, presented in lecture 8, originates from [BG84]. The *security* of this scheme is based on the intractability assumption of factoring, while its *efficiency* is comparable with that of the RSA. More generally, the scheme can be based on any trapdoor one-way permutation.

Non-uniform versions of the two definitions of security (presented in lecture 6) were shown equivalent in [MRS88]. These versions were also shown equivalent to a third definition appearing in [Y82].

The robustness of encryption schemes against active adversaries was addressed in [GMT82]. Folklore states that secret communication can be achieved over a channel controlled by an active adversary by use of bi-directional communication: for every message transmission, the communicating parties exchange new authenticated cryptographic keys (i.e. the receiver transmits a new authenticated encryption-key that is used only for the current message). Note that this prevents a chosen message attack on the currently used instance of the encryption scheme. Note that this suggestion does not constitute a public-key encryption scheme, but rather a secure means of private bi-directional communication. It was claimed that "non-interactive zero-knowledge proofs of knowledge" yield the construction of public-key encryption secure against chosen ciphertext attack [BFM88], but no proof of this claim has appeared.

references

[BFM88] see category 6.

[BG84] Blum, M., and S. Goldwasser, "An Efficient Probabilistic Public-Key Encryption Scheme which hides all partial information", *Advances in Cryptology: Proc. of Crypto 84*, ed. B Blakely, Springer Verlag Lecture Notes in Computer Science, vol. 196, pp. 289-302.

[GMT82] Goldwasser, S., S. Micali, and P. Tong, "Why and How to Establish a Private Code in a Public Network", *23rd FOCS*, 1982, pp. 134-144.

[MRS88] Micali, S., C. Rackoff, and B. Sloan, "The Notion of Security for Probabilistic Cryptosystems", *SIAM Jour. of Computing*, 1988, Vol. 17, pp. 412-426.

[Y82] see main references.

A.4 Pseudorandomness

I have partitioned the works in this category into two subcategories: works with immediate cryptographic relevance versus works which have a more abstract (say complexity theoretic) orientation. A survey on Pseudorandomness in contained in [G88b].

4.1. Cryptographically oriented works

The theory of pseudorandomness was extended to deal with functions and permutations. Definitions of pseudorandom functions and permutations are presented in [GGM84] and [LR86]. Pseudorandom generators were used to construct pseudorandom functions [GGM84], and these were used to construct pseudorandom permutations [LR86]. Cryptographic applications are discussed in [GGM84b, LR86].

In lecture 9, we proved that the existence of one-way *permutations* implies the existence of pseudorandom generators. Recently, it has been shown that pseudorandom generators exist if and only if one-way functions exist [ILL89, H89]. The construction of pseudorandom generators presented in these works is very complex and inefficient, thus the quest for an efficient construction of pseudorandom generator based on any one-way function is not over yet. A previous construction by [GKL88] might turn out useful in this quest.

A very efficient pseudorandom generator based on the intractability of factoring integers arises from the works [BBS82, ACGS84, VV84]. The generator was suggested in [BBS82] (where it was proved secure assuming intractability of Quadratic Residuousity Problem), and proven secure assuming intractability of factoring in [VV84] (by adapting the techniques in [ACGS84]).

4.2. Complexity oriented works

The existence of a pseudorandom generator implies the existence of a pair of statistically different efficiently constructible probability ensembles which are computationally indistinguishable. This sufficient condition turns out to be also a necessary one [G89b].

The difference between the output distribution of a pseudorandom generator and more commonly considered distributions is demonstrated in [L88]. The "commonly considered" distributions (e.g. all distributions having a polynomial-time computable distribution function) are shown to be *homogenous* while a pseudorandom generator gives rise to distributions which are not homogenous. Homogenous distributions are defined as distributions which allow good average approximation of all polynomial-time invariant characteristics of a string from its Kolmogorov complexity.

The use of pseudorandom generators for deterministic simulation of probabilistic complexity classes was first suggested in [Y82]. A unified approach, leading to better simulations, can be found in [NW88]. Other results concerning the "efficient" generation of sequences which "look random" to machines of various complexity classes can be found in [RT85, BNS89, Ni89].

The existence of sparse and evasive pseudorandom distributions is investigated in [GKr89a]. A sparse distribution (unlike a distribution statistically close to the uniform one) ranges over a negligible fraction of the strings. Evasiveness is the infeasibility of hitting an element in the distribution's support. Applications of some results to zero-knowledge are presented in [GKr89b].

references

[ACGS84] see category 2.

[BNS89] Babai, L., N. Nisan, and M. Szegedy, "Multi-party Protocols and Logspace-Hard Pseudorandom Sequences", *21st STOC*, pp. 1-11, 1989.

[BBS82] L. Blum, M. Blum and M. Shub, *A Simple Secure Unpredictable Pseudo-Random Number Generator*, *SIAM Jour. on Computing*, Vol. 15, 1986, pp. 364-383. Preliminary version in *Crypto82*.

[BM82] see main references.

[G88b] Goldreich, O., "Randomness, Interactive Proofs, and Zero-Knowledge - A Survey", *The Universal Turing Machine - A Half-Century Survey*, R. Herken ed., Oxford Science Publications, pp. 377-406, 1988.

[G89b] Goldreich, O., "A Note on Computational Indistinguishability", TR-89-051, ICSI, Berkeley, USA, (1989).

[GGM84] Goldreich, O., S. Goldwasser, and S. Micali, "How to Construct Random Functions", *Jour. of ACM*, Vol. 33, No. 4, 1986, pp. 792-807. Extended abstract in *FOCS84*.

[GGM84b] Goldreich, O., S. Goldwasser, and S. Micali, "On the Cryptographic Applications of Random Functions", *Crypto84*, proceedings, Springer-Verlag, Lecture Notes in Computer Science, vol. 196, pp. 276-288, 1985.

[GKr89a] Goldreich, O., and H. Krawczyk, "Sparse Pseudorandom Distributions", *Crypto89* proceedings, to appear.

[GKr89b] see category 6.

[GKL88] Goldreich, O., H. Krawczyk, and M. Luby, "On the Existence of Pseudorandom Generators", *29th FOCS*, 1988.

[GM82] see main references.

[H89] Hastad, J., "Pseudo-Random Generators with Uniform Assumptions", preprint, 1989.

[ILL89] Impagliazzo, R., L.A. Levin, and M. Luby, "Pseudorandom Generation from One-Way Functions", *21st STOC*, pp. 12-24, 1989.

[L85] L.A. Levin, "One-Way Function and Pseudorandom Generators", *Combinatorica*, Vol. 7, No. 4, 1987, pp. 357-363. A preliminary version appeared in *Proc. 17th STOC*, 1985, pp. 363-365.

[L88] L.A. Levin, "Homogenous Measures and Polynomial Time Invariants", *29th FOCS*, pp. 36-41, 1988.

[LR86] M. Luby and C. Rackoff, "How to Construct Pseudorandom Permutations From Pseudorandom Functions", *SIAM Jour. on Computing*, Vol. 17, 1988, pp. 373-386. Extended abstract in *FOCS86*.

[NW88] Nisan, N., and A. Wigderson, "Hardness vs. Randomness", *Proc. 29th FOCS*, pp. 2-11, 1988.

[Ni89] Nisan, N., "Pseudorandom Generators for Bounded Space Machines", private communication, 1989.

[RT85] Reif, J.H., and J.D. Tygar, "Efficient Parallel Pseudo-Random Number Generation", *Crypto85*, proceedings, Springer-Verlag, Lecture Notes in Computer Science, vol. 218, pp. 433-446, 1985.

[Y82] see main references.

[VV84] Vazirani, U.V., and V.V. Vazirani, "Efficient and Secure Pseudo-Random Number Generation", *25th FOCS*, pp. 458-463, 1984.

A.5 Signatures and Commitment Schemes

Recent works reduce the existence of these important primitives to assumptions weaker than ever conjectured.

5.1. Unforgeable Signatures Schemes

Unforgeable signature schemes can be constructed assuming the existence of one-way permutations [NY89]. The core of this work is a method for constructing "cryptographically strong" hashing functions. Further improvements and techniques are reported in [G86, EGM89]: in [G86] a technique for making schemes as [GMR84, BM88, NY89] "memoryless" is presented; in [EGS89] the concept of "on-line/off-line" signature schemes is presented and methods for constructing such schemes are presented as well.

5.2. Secure Commitment Schemes

Secure commitment schemes can be constructed assuming the existence of pseudorandom generator [N89]. In fact, the second scheme presented in lecture 13 originates from this paper.

references

[BM88] see main references.

[EGM89] Even, S., O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signature Schemes", *Crypto89* proceedings, to appear.

[G86] Goldreich, O., "Two Remarks concerning the Goldwasser-Micali-Rivest Signature Scheme", *Crypto86*, proceedings, Springer-Verlag, Lecture Notes in Computer Science, vol. 263, pp. 104-110, 1987.

[GMR84] see main references.

[N89] M. Naor, "Bit Commitment Using Pseudorandomness", IBM research report. Also to appear in *Crypto89* proceedings, 1989.

[NY89] M. Naor and M. Yung, "Universal One-Way Hash Functions and their Cryptographic Applications", *21st STOC*, pp. 33-43, 1989.

A.6 Interactive Proofs, Zero-Knowledge and Protocols

This category is subdivided into three parts. The first contains mainly cryptographically oriented works on zero-knowledge, the second contains more complexity oriented works on interactive proofs and zero-knowledge. The third subcategory lists works on the design of cryptographic protocols. Surveys on Interactive Proof Systems and Zero-Knowledge Proofs can be found in [G88b, Gw89].

6.1. Cryptographically oriented works on Zero-Knowledge

An important measure for the "practicality" of a zero-knowledge proof system is its *knowledge tightness*. Intuitively, tightness is (the supremum taken over all probabilistic polynomial-time verifiers of) the ratio between the time it takes the simulator to simulate an interaction with the prover and the complexity of the corresponding verifier [G87a]. The definition of zero-knowledge only guarantees that the knowledge-tightness can be bounded by any function growing faster than every polynomial. However, the definition does not guarantee that the knowledge-tightness can be bounded above by a *particular* polynomial. It is easy to see that the knowledge-tightness of the proof system for Graph Isomorphism (presented in lecture 12) is 2, while the tightness of proof system for Graph colouring (lecture 13) is m (i.e., the number of edges). I believe that the knowledge-tightness of a protocol is an important aspect to be considered, and that it is very desirable to have tightness be a constant. Furthermore, using the notion of knowledge-tightness one can introduce more refined notions of zero-knowledge and in particular the notion of constant-tightness zero-knowledge. Such refined notions may be applied in a non-trivial manner also to languages in $\mathcal{P}$.

Two standard efficiency measures associated with interactive proof systems are the *computational complexity* of the proof system (i.e., number of steps taken by either or both parties) and the *communication complexity* of the proof system (here one may consider the number of rounds, and/or the total number of bits exchanged). Of special importance to practice is the question whether the (honest) prover's program can be a probabilistic polynomial-time when an auxiliary input is given (as in the case of the proof system, presented in lecture 13, for Graph Colouability). An additional measure, the importance of which has been realized only recently, is the number of strings to which the commitment scheme is applied individually (see [KMO89]). The zero-knowledge proof system for graph colourability presented in lecture 13 is not the most practical one known. Proof systems with constant knowledge-tightness, probabilistic polynomial-time provers and a number of iterations which is merely super-logarithmic exist for all languages in $\mathcal{NP}$ (assuming, of course, the existence of secure commitment) [IY87]. This proof system can be modified to yield a zero-knowledge proof with $f(n)$ iterations, for every unbounded function f. Using stronger intractability assumptions (e.g. the existence of claw-free one-way permutations), constant-round zero-knowledge proof systems can be presented for every language in $\mathcal{NP}$ [GKa89].

Perfect zero-knowledge *arguments*[1] were introduced in [BC86a, BCC88] and shown to exist for all languages in $\mathcal{NP}$, assuming the intractability of factoring integers. The differ-

[1] The term "argument" has appeared first in [BCY89]. The authors of [BCC88] create an enormous

ence between arguments and interactive proofs is that in a argument the soundness condition is restricted to probabilistic polynomial-time machines (with auxiliary input). Hence, it is *infeasible* (not impossible) to fool the verifier into accepting (with non-negligible probability) an input not in the language. Assuming the existence of any commitment scheme, it is shown that any language in $\mathcal{NP}$ has a constant-round zero-knowledge argument [FS88].

The limitations of zero-knowledge proof systems and the techniques to demonstrate their existence are investigated in [GO87, GKr89b]. In particular, zero-knowledge proofs with deterministic verifier (resp. prover) exist only for languages in $\mathcal{RP}$ (resp. $\mathcal{BPP}$), constant-round proofs of the AM-type (cf. [B85]) can be demonstrated zero-knowledge by an oblivious simulation only if the language is in $\mathcal{BPP}$. Thus, the "parallel versions" of the interactive proofs (presented in [GMW86]) for Graph Isomorphism and every $L \in \mathcal{NP}$ are unlikely to be demonstrated zero-knowledge. However, modified versions of these interactive proofs yield constant-round zero-knowledge proofs (see [GKa89] for $\mathcal{NP}$ and [BMO89] for Graph Isomorphism). These interactive proofs are, of course, not of the AM-type.

The concept of a "proof of knowledge" was introduced and informally defined in [GMR85]. Precise formalizations following this sketch has appeared in [BCC88, FFS87, TW87]. This concept is quite useful in the design of cryptographic protocols and zero-knowledge proof systems. In fact, it has been used implicitly in [GMR85, GMW87, CR87] and explicitly in [FFS87, TW87]. However, I am not too happy with the current formalizations and intend to present a new formalization.

"Non-interactive" zero-knowledge proofs are known to exist assuming the existence of trapdoor one-way permutations [KMO89]. These are two-phase protocols. The first phase is a preprocessing which uses bi-directional communication. In the second phase, zero-knowledge proofs can be produced via one-directional communication from the prover to the verifier. The number of statements proven in the second phase is a polynomial in the complexity of the first phase (this polynomial is arbitrarily fixed *after* the first phase is completed).

Historical remark: Using a stronger intractability assumption (i.e. the intractability of Quadratic Residuousity Problem) [BC86b] showed that every language in $\mathcal{NP}$ has a zero-knowledge interactive proof system. This result has been obtained independently of (but subsequently to) [GMW86].

amount of confusion by insisting to refer to arguments by the term interactive proofs. For example, the result of [For87] does not hold for perfect zero-knowledge *arguments*. Be careful not to confuse arguments with interactive proofs in which the completeness condition is satisfied by a probabilistic polynomial-time prover (with auxiliary input).

6.2. Complexity oriented works on Interactive Proofs and Zero-Knowledge

The definition of interactive proof systems, presented in lecture 12, originates from [GMR85]. A special case, in which the verifier sends the outcome of all its coin tosses to the prover was suggested in [B85] and termed *Arthur Merlin* (*AM*) games. AM games are easier to analyze, while general interactive proof systems are easier to design. Fortunately, the two formalizations coincide in a strong sense: for every polynomial Q, the classes $\mathcal{IP}(Q(n))$ and $\mathcal{AM}(Q(n))$ are equal [GS86], where $\mathcal{IP}(Q(n))$ denotes the class of languages having $Q(n)$-round interactive proof system. It is also known, that for every $k \geq 1$ and every polynomial Q, the class $\mathcal{AM}(Q(n))$ and $\mathcal{AM}(k \cdot Q(n))$ coincide [BaMo88]. A stronger result does not "relativize" (i.e. there exists an oracle A such that for every polynomial Q and every unbounded function g the class $\mathcal{AM}(Q(n))^A$ is strictly contained in $\mathcal{AM}(g(n) \cdot Q(n))^A$) [AGH88].

> **Author's Note:** *However, in light of the results of* `[LFKN,S]` *(see* `FOCS90`*), this means even less than ever. See also Chang et. al. (*`JCSS`*, Vol. 49, No. 1).*

> **Author's Note:** *This list was compiled before the fundamental results of Lund, Fortnow, Karloff and Nisan* `[LFKN]` *and Shamir* `[S]` *were known. By these results every language in $\mathcal{PSPACE}$ has an interactive proof system. Since $\mathcal{IP} \subseteq \mathcal{PSPACE}$ [folklore], the two classes collide.*

Every language $L \in \mathcal{IP}(Q(n))$ has a $Q(n)$-round interactive proof system in which the verifier accepts every $x \in L$ with probability 1, but only languages in $\mathcal{NP}$ have interactive proof systems in which the verifier never accepts $x \notin L$ [GMS87]. Further developments appear in [BMO89].

The class $\mathcal{AM}(2)$ is unlikely to contain co$\mathcal{NP}$, as this will imply the collapse of the polynomial-time hierarchy [BHZ87]. It is also known that for a random oracle A, $\mathcal{AM}(2) = \mathcal{NP}^A$ [NW88].

The complexity of languages having zero-knowledge proof systems seems to depend on whether these systems are *perfect* or only *computational* zero-knowledge. On one hand, it is known that perfect (even almost-perfect) zero-knowledge proof systems exist only for languages inside $\mathcal{AM}(2) \cap$co$\mathcal{AM}(2)$ [For87, AH87]. On the other hand, assuming the existence of commitment schemes (the very assumption used to show "NP in ZK") every languages in $\mathcal{IP}$ has a computational zero-knowledge proof system [IY87] (for a detailed proof see [Betal88]). Returning to perfect zero-knowledge proof systems, it is worthwhile mentioning that such systems are known for several computational problems which are considered hard (e.g. Quadratic Residuousity Problem [GMR85], Graph Isomorphism [GMW86], membership in a subgroup [TW87], and a problem computationally equivalent to Discrete Logarithm [GKu88]).

The concept of the knowledge complexity of a languages was introduced in [GMR85], but the particular formalization suggested there is somewhat ad-hoc and unnatural.[2] The *knowledge complexity* of a language is the minimum number of bits released by an interactive proof system for the language. Namely, a language $L \in \mathcal{IP}$ has knowledge complexity $\leq k(\cdot)$ if there exists an interactive proof for L such that the interaction of the prover on $x \in L$ can be simulated by a probabilistic polynomial-time *oracle* machine on input x and up to $k(|x|)$ Boolean queries (to an oracle of "its choice"). More details will appear in a forthcoming paper of mine.

An attempt to get rid of the intractability assumption used in the "NP in ZK" result of [GMW86], led [BGKW88] to suggest and investigate a model of *multi-prover* interactive proof systems. It was shown that two "isolated" provers can prove statements in $\mathcal{NP}$ in a perfect zero-knowledge manner. A different multi-prover model, in which one unknown prover is honest while the rest my interact and cheat arbitrarily, was suggested and investigated in [FST88]. This model is equivalent to computation with a "noisy oracle".

6.3. On the Design of Cryptographic Protocols

The primary motivation for the concept of zero-knowledge proof systems has been their potential use in the design of cryptographic protocols. Early examples of such use can be found in [GMR85, FMRW85, CF85]. The general results in [GMW86] allowed the presentation of automatic generators of two-party and multi-party cryptographic protocols (see [Y86][3] and [GMW87], respectively). Further improvements are reported in [GHY87, GV87, IY87].

Two important tools in the construction of cryptographic protocols are Oblivious Transfer and Verifiable Secret Sharing. *Oblivious Transfer*, introduced in [R81], was further investigated in [EGL82, FMRW85, BCR86, Cre87, CK88, Kil88]. *Verifiable Secret Sharing*, introduced in [CGMA85], was further investigated in [GMW86, Bh86a, Fel87]. Other useful techniques appear in [Bh86b, CR87].

An elegant model for investigations of multi-party cryptographic protocols was suggested in [BGW88]. This model consists of processors connected in pairs via *private channels*. The bad processors have infinite computing resources (and so using computationally hard problems is useless). Hence, computational complexity restrictions and assumptions are substituted by assumptions about the communication model. An automatic generator of protocols for this model, tolerating up to $\frac{1}{3}$ malicious processors, has been presented in [BGW88, CCD88]. Augmenting the model by a broadcast channel, tolerance can be

[2] In particular, according to that formalization a prover revealing with probability $\frac{1}{2}$ a Hamiltonian circuit in the input gragh yields one one bit of knowledge.

[3] It should be stressed that [Y86] improves over [Y82b]. The earlier paper presented two-party cryptographic protocols allowing semi-honest parties to compute privately functions ranging over "small" (i.e. polynomially bounded) domains.

improved to $\frac{1}{2}$ [BR89]. (The augmentation is necessary, as there are tasks which cannot be performed if a third of the processors are malicious (e.g. Byzantine Agreement).) Beyond the $\frac{1}{2}$ bound, only functions of special type (i.e. the exclusive-or of locally computed functions) can be privately computed [CKu89].

references

[AGH86] Aiello, W., S. Goldwasser, and J. Hastad, "On the Power of Interaction", *Proc. 27th FOCS*, pp. 368-379, 1986.

[AH87] Aiello, W., and J. Hastad, "Perfect Zero-Knowledge Languages can be Recognized in Two Rounds", *Proc. 28th FOCS*, pp. 439-448, 1987.

[AGY85] Alon, N., Z. Galil, and M. Yung, "A Fully Polynomial Simultaneous Broadcast in the Presence of Faults", unpublished manuscript, 1985.

[B85] Babai, L., "Trading Group Theory for Randomness", *Proc. 17th STOC*, 1985, pp. 421-429.

[BKL] Babai, L., W.M. Kantor, and E.M. Luks, "Computational Complexity and Classification of Finite Simple Groups", *Proc. 24th FOCS*, pp. 162-171, 1983.

[BaMo88] Babai, L., and S. Moran, "Arthur-Merlin Games: A Randomized Proof System, and a Hierarchy of Complexity Classes", *JCSS*, Vol. 36, No. 2, pp. 254-276, 1988.

[BMO89] Bellare, M., S. Micali, and R. Ostrovsky, "On Parallelizing Zero-Knowledge Proofs and Perfect Completeness Zero-Knowledge", manuscript, April 1989.

[Bh86a] Benaloh, (Cohen), J.D., "Secret Sharing Homomorphisms: keeping shares of a secret secret", *Crypto86*, proceedings, Springer-Verlag, Lecture Notes in Computer Science, vol. 263, pp. 251-260, 1987.

[Bh86b] Benaloh, (Cohen), J.D., "Cryptographic Capsules: A Disjunctive Primitive for Interactive Protocols", *Crypto86*, proceedings, Springer-Verlag, Lecture Notes in Computer Science, vol. 263, pp. 213-222, 1987.

[Betal88] Ben-Or, M., O. Goldreich, S. Goldwasser, J. Hastad, J. Killian, S. Micali, and P. Rogaway, "Every Thing Provable is provable in ZK", to appear in the proceedings of *Crypto88*, 1988.

[BGW88] Ben-Or, M., S. Goldwasser, and A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation", *20th STOC*, pp. 1-10, 1988.

[BGKW88] Ben-Or, M., S. Goldwasser, J. Kilian, and A. Wigderson, "Multi-Prover Interactive Proofs: How to Remove Intractability", *20th STOC*, pp. 113-131, 1988.

[BT89] Ben-Or, M., and T. Rabin, "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority", *21st STOC*, pp. 73-85, 1989.

[Bk] Blakley, G.R., "Safeguarding Cryptographic Keys", *Proc. of National Computer Conf.*, Vol. 48, AFIPS Press, 1979, pp. 313-317.

[BFM88] Blum, M., P. Feldman, and S. Micali, "Non-Interactive Zero-Knowledge and its Applications", *20th STOC*, pp. 103-112, 1988.

[BHZ87] Boppana, R., J. Hastad, and S. Zachos, "Does Co-NP Have Short Interactive Proofs?", *IPL*, 25, May 1987, pp. 127-132.

[BCC88] Brassard, G., D. Chaum, and C. Crepeau, "Minimum Disclosure Proofs of knowledge", *JCSS*, Vol. 37, No. 2, Oct. 1988, pp. 156-189.

[BC86a] Brassard, G., and C. Crepeau, "Non-Transitive Transfer of Confidence: A Perfect Zero-Knowledge Interactive Protocol for SAT and Beyond", *Proc. 27th FOCS*, pp. 188-195, 1986.

[BC86b] Brassard, G., and C. Crepeau, "Zero-Knowledge Simulation of Boolean Circuits", *Advances in Cryptology - Crypto86 (proceedings)*, A.M. Odlyzko (ed.), Springer-Verlag, Lecture Notes in Computer Science, vol. 263, pp. 223-233, 1987.

[BCR86] Brassard, G., C. Crepeau, and J.M. Robert, "Information Theoretic Reductions Among Disclosure Problems", *Proc. 27th FOCS*, pp. 168-173, 1986.

[BCY89] Brassard, G., C. Crepeau, and M. Yung, "Everything in $\mathcal{NP}$ can be argued in perfect zero-knowledge in a bounded number of rounds", *Proc. of the 16th ICALP*, July 1989.

[CCD88] Chaum, D., C. Crepeau, I. Dangard, "Multi-party Unconditionally Secure Protocols", *20th STOC*, pp. 11-19, 1988.

[Cha] Chaum, D., "Demonstrating that a Public Predicate can be Satisfied Without Revealing Any Information About How", *Advances in Cryptology - Crypto86 (proceedings)*, A.M. Odlyzko (ed.), Springer-Verlag, Lecture Notes in Computer Science, vol. 263, pp. 195-199, 1987.

[CGMA85] Chor, B., S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults", *Proc. 26th FOCS*, 1985, pp. 383-395.

[CKu89] Chor, B., and E. Kushilevitz, "A Zero-One Law for Boolean Privacy", *21st STOC*, pp. 62-72, 1989.

[CR87] Chor, B., and M.O, Rabin, "Achieving Independence in Logarithmic Number of Rounds", *6th PODC*, pp. 260-268, 1987.

[CGG] Chor, B., O. Goldreich, and S. Goldwasser, "The Bit Security of Modular Squaring given Partial Factorization of the Modulos", *Advances in Cryptology - Crypto85 (proceedings)*, H.C. Williams (ed.), Springer-Verlag, Lecture Notes in Computer Science, vol. 218, 1986, pp. 448-457.

[CF85] Cohen, J.D., and M.J. Fischer, "A Robust and Verifiable Cryptographically Secure Election Scheme", *Proc. 26th FOCS*, pp. 372-382, 1985.

[Cre87] Crepeau, C., "Equivalence between two Flavour of Oblivious Transfer", *Crypto87* proceedings, Lecture Notes in Computer Science, Vol. 293, Springer-Verlag, 1987, pp. 350-354.

[CK88] Crepeau, C., and J. Kilian, "Weakening Security Assumptions and Oblivious Transfer", *Crypto88* proceedings.

[EGL82] see category 8.

[Fel87] Feldman, P., "A Practical Scheme for Verifiable Secret Sharing", *Proc. 28th FOCS*, pp. 427-438, 1987.

[FFS87] Feige, U., A. Fiat, and A. Shamir, "Zero-Knowledge Proofs of Identity", *Proc. of 19th STOC*, pp. 210-217, 1987.

[FST88] Feige, U., A. Shamir, and M. Tennenholtz, "The Noisy Oracle Problem", *Crypto88* proceedings.

[FS88] Feige, U., and A. Shamir, "Zero-Knowledge Proofs of Knowledge in Two Rounds", manuscript, Nov. 1988.

[FMRW85] Fischer, M., S. Micali, C. Rackoff, and D.K. Wittenberg, "An Oblivious Transfer Protocol Equivalent to Factoring", unpublished manuscript, 1986. Preliminary versions were presented in *EuroCrypt84* (1984), and in the *NSF Workshop on Mathematical Theory of Security*, Endicott House (1985).

[For87] Fortnow, L., "The Complexity of Perfect Zero-Knowledge", *Proc. of 19th STOC*, pp. 204-209, 1987.

[GHY85] Galil, Z., S. Haber, and M. Yung, "A Private Interactive Test of a Boolean Predicate and Minimum-Knowledge Public-Key Cryptosystems", *Proc. 26th FOCS*, 1985, pp. 360-371.

[GHY87] Galil, Z., S. Haber, and M. Yung, "Cryptographic Computation: Secure Fault-Tolerant Protocols and the Public-Key Model" *Crypto87*, proceedings, Springer-Verlag, Lecture Notes in Computer Science, vol. 293, pp. 135-155, 1987.

[G87a] Goldreich, O., "Zero-Knowledge and the Design of Secure Protocols (an exposition)", TR-480, Computer Science Dept., Technion, Haifa, Israel, 1987.

[G88b] see category 4.

[GKu88] Goldreich, O., and E. Kushilevitz, "A Perfect Zero-Knowledge Proof for a Decision Problem Equivalent to Discrete Logarithm", *Crypto88*, proceedings.

[GKa89] Goldreich, O., and A. Kahan, "Using Claw-Free Permutations to Construct Zero-Knowledge Proofs for NP", in preparation, 1989.

[GKr89b] Goldreich, O., and H. Krawczyk, "On Sequential and Parallel Composition of Zero-Knowledge Protocols", preprint, 1989.

[GV87] Goldreich, O., and R. Vainish, "How to Solve any Protocol Problem - an Efficiency Improvement", *Crypto87*, proceedings, Springer-Verlag, Lecture Notes in Computer Science, vol. 293, pp. 73-86, 1987.

[GMS87] Goldreich, O., Y. Mansour, and M. Sipser "Interactive Proof Systems: Provers that Never Fail and Random Selection", *28th FOCS*, pp. 449-461, 1987.

[GMW86] see main references.

[GMW87] see main references.

[GO87] Goldreich, O., and Y. Oren, "On the Cunning Power of Cheating Verifiers: Some Observations about Zero-Knowledge Proofs", in preparation. Preliminary version, by Y. Oren, in *FOCS87*.

[Gw89] Goldwasser, S., "Interactive Proof Systems", *Proc. of Symposia in Applied Mathematics*, AMS, Vol. 38, 1989.

[GMR85] see main references.

[GS86] Goldwasser, S., and M. Sipser, "Private Coins vs. Public Coins in Interactive Proof Systems", *Proc. 18th STOC*, 1986, pp. 59-68.

[IY87] Impagliazzo, R., and M. Yung, "Direct Minimum-Knowledge Computations", *Advances in Cryptology - Crypto87 (proceedings)*, C. Pomerance (ed.), Springer-Verlag, Lecture Notes in Computer Science, vol. 293, 1987, pp. 40-51.

[Kil88] Kilian, J., "Founding Cryptography on Oblivious Transfer", *20th STOC*, pp. 20-31, 1988.

[LMR83] Luby, M., S. Micali, and C. Rackoff, *24th FOCS*, 1983.

[KMO89] Kilian, J., S. Micali, and R. Ostrovsky, "Simple Non-Interactive Zero-Knowledge Proofs", *30th FOCS*, to appear, 1989.

[NW88] see category 4.

[R81] see category 8.

[TW87] Tompa, M., and H. Woll, "Random Self-Reducibility and Zero-Knowledge Interactive Proofs of Possession of Information", *Proc. 28th FOCS*, pp. 472-482, 1987.

[Y82b] Yao, A.C., "Protocols for Secure Computations", *23rd FOCS*, 1982, pp. 160-164.

[Y86] Yao, A.C., "How to Generate and Exchange Secrets", *Proc. 27th FOCS*, pp. 162-167, 1986.

A.7 Additional Topics

This category provides pointers to topics which I did not address so far. These topics include additional cryptographic problems (e.g. software protection, computation with an untrusted oracle, and protection against "abuse of cryptographic systems"), lower level primitives (e.g. Byzantine Agreement and sources of randomness) and "cryptanalysis".

7.1. Software Protection

A theoretical framework for discussing software protection is suggested in [G87b]. Recently, the solution in [G87b] has been dramatically improved [O89].

7.2. Computation with an Untrusted Oracle

Computation with an untrusted oracle raises two problems: the oracle may fail the computation by providing wrong answers, and/or the oracle can gain information on the input of the machine which uses it. The first problem can be identified with recent research on "program checking" initiated in [BK89]. Note that the definition of "program checking" is more refined than the one of an interactive proof (in particular it does not trivialize polynomial-time computations and does not allow infinitely powerful provers) and thus is more suitable for the investigation. The results in [BK89, BLR89] are mainly encouraging as they provide many positive examples of computations which can be sped-up (and yet confirmed) using an oracle. A formalization of the second problem, presented in [AFK87], seems to have reached a dead-end with the negative results of [AFK87]. Other formalizations appear in [BF89] and [BLR89].

7.3. Protection Against Abuse of Cryptographic Systems

How can a third party prevent the abuse of a two-party cryptographic protocol executed through a channel he controls? As an example consider an attempt of one party to pass information to his counterpart by using a signature scheme. This old problem (sometimes referred to as *the prisoners' problem* or *the subliminal channel*) is formalized and solved, using active intervention of the third party, in [D88].

7.4. Byzantine Agreement

In lectures 14-15 we have assumed the existence of a *broadcast channel* accessable by all processors. In case such a channel does not exist in the network (i.e., in case we are using a point-to-point network), such a channel can be implemented using *Byzantine Agreement*. Using private channel, randomized Byzantine Agreement protocols with expected $O(1)$ rounds can be implemented [FM88]. This work builds on [R83]. Additional insight can be gained from the pioneering works of [Be83, Br85], and from the survey of [CD89].

7.5. Sources of Randomness

A subject related to cryptography is the use of weak sources of randomness in applications requiring perfect coins. Models of weak sources are presented and investigated in [B84, SV84, CG85, Cetal85, LLS87]. Further developments are reported in [V85, VV85, V87].

7.6. Cryptanalysis

In all the famous examples of successful cryptanalysis of a proposed cryptographic scheme, the success revealed a explicit or implicit assumption made by the designers of the cryptosystem. This should serve as experimental support to the thesis underlying the course that assumptions have to be made explicitly.

Knapsack cryptosystems, first suggested in [MH78], were the target of many attacks. The first dramatic success was the breaking of the original [MH78] scheme, using the existence of a trapdoor super-increasing sequence [S82]. An alternative attack applicable against *low density* knapsack (subset sum) problems was suggested in [LO85]. For more details see [BO88]. *It seems that the designers conjectured that subset sum problems with a trapdoor (resp. with low density) are as hard as random high density subset sum problems. It seems that this conjecture is false.*

Another target for many attacks were the linear congruential number generators and their generalizations. Although these generators are known to pass many statistical tests [K69], they do not pass all polynomial-time statistical tests [Boy82]. Generalizations to polynomial congruential recurrences and linear generators which output only part of the bits of the numbers produced can be found in [Kr88] and [S87], respectively. *The fact that a proposed scheme passes some tests or attacks does not mean that it will pass all efficient tests.*

Another famous cryptographic system which triggered interesting algorithmic research is the [OSS84] signature scheme. This scheme was based on the conjecture, latter refuted in [Pol84], that it is hard to solve a modular quadratic equation in two variables. Other variants (e.g. [OSS84b, OS85]) were broken as well (in [EAKMM85, BD85], resp.). *Proving that one cannot find the trapdoor information used by the legal signer does not mean that one cannot forge signatures.*[4]

references

[AFK87] Abadi, M., J. Feigenbaum, and J. Kilian, "On Hiding Information from an Oracle", *19th STOC*, pp. 195-203, 1987.

[BF89] Beaver, D., and J. Feigenbaum, "Encrypted Queries to Multiple Oracles", manuscript, 1989.

[B84] Blum, M., "Independent Unbiased Coin Flips from a Correlated Biased Source: a Finite State Markov Chain", *25th Symp. on Foundation of Computer Science*, pp. 425-433, 1984.

[Be83] Ben-Or, M., "Another Advantage of Free Choice: Completely Asynchronous Agreement Protocols", *2nd PODC*, pp. 27-30, 1983.

[BK89] Blum, M., and S. Kannan, "Designing Programs that Check their Work", *21st STOC*, pp. 86-97, 1989.

[BLR89] Blum, M., M. Luby, and R. Rubinfeld, in preparation.

[Boy82] Boyar, J.B., "Inferring Sequences Produced by Pseudo-Random Number Generators", *JACM*, Vol. 36, No. 1, pp. 129-141, 1989. Early version in *FOCS82* (under previous name: Plumstead).

[Br85] Bracha, G., "An $O(\log n)$ Expected Rounds Randomized Byzantine Generals Protocol", *JACM*, Vol. 34, No. 4, pp. 910-920, 1987. Extended abstract in *STOC85*.

[4] To further stress this point, consider a signature scheme "based on composites" where the signature of a message m relative to the public-key N is $2m \bmod N$. The infeasibility of retrieving the trapdoor (i.e. the factorization of N) is a poor guarantee for security.

[BD85] Brickell, E.F., and J.M. DeLaurentis, "An Attack on a Signature Scheme Proposed by Okamoto and Shiraishi", *Crypto85*, proceedings, Springer-Verlag, Lecture Notes in Computer Science, vol. 218, pp. 28-32, 1985.

[LO85] Lagarias, J.C., and A.M. Odlyzko, "Solving Low-Density Subset Sum Problems", *JACM*, Vol. 32, (1985), pp. 229-246. *24th FOCS*, pp. 1-10, 1983.

[BO88] see category 2.

[CD89] Chor, B., and C. Dwork, "Randomization in Byzantine Agreement", *Advances in Computing Research*, Vol. 5, S. Micali, ed., JAI Press, in press.

[Cetal85] Chor, B., J. Freidmann, O. Goldreich, J. Hastad, S. Rudich, and R. Smolensky, "The Bit Extraction Problem or t-Resilient Functions", *26th FOCS*, pp. 396-407, 1985.

[CG85] Chor, B., and O. Goldreich, "Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity", *26th Symp. on Foundation of Computer Science*, pp. 427-443, 1985.

[D88] Desmedt, Y., "Abuses in Cryptography and How to Fight Them", *Crypto88* proceedings, to appear.

[EAKMM85] Estes, D., L. Adleman, K. Kompella, K. McCurley, and G. Miller, "Breaking the Ong-Schnorr-Shamir Signature Scheme for Quadratic Number Fields", *Crypto85*, proceedings, Springer-Verlag, Lecture Notes in Computer Science, vol. 218, pp. 3-13, 1985.

[FM88] Feldman, P., and S. Micali, "Optimal Algorithms for Byzantine Agreement", *20th STOC*, pp. 148-161, 1988.

[FHKLS] Frieze, A.M., J. Hastad, R. Kannan, J.C. Lagarias, and A. Shamir, "Reconstructing Truncated Integer Variables Satisfying Linear Congruences", *SIAM J. Comput.*, Vol. 17, No. 2, pp. 262-280, 1988. Combines early papers from *FOCS84* and *STOC85* (by Frieze, Kannan and Lagarias, and Hastad and Shamir, resp.).

[G87b] Goldreich, O., "Towards a Theory of Software Protection and Simulation by Oblivious RAMs", *19th STOC*, pp. 182-194, 1987.

[K69] Knuth, D.E., *The Art of Computer Programming*, Vol. 2, Addison-Wesley, Reading, Mass., 1969.

[Kr88] Krawczyk, H., "How to Predict Congruential Generators", TR-533, Computer Science Dept., Technion, Haifa, Israel, 1988. To appear in *J. of Algorithms.*

[LR88] J.C. Lagarias, and J. Reeds, "Unique Extrapolation of Polynomial Recurrences", *SIAM J. Comput.*, Vol. 17, No. 2, pp. 342-362, 1988.

[LLS87] Lichtenstein, D., N. Linial, and M. Saks, "Imperfect Random Sources and Discrete Control Processes", *19th STOC*, pp. 169-177, 1987.

[MH78] see category 8.

[OS85] Okamoto, T., and A. Shiraishi, "A Fast Signature Scheme Based on Quadratic Inequalities", *Proc. of 1985 Symp. on Security and Privacy*, April 1985, Oakland, Cal.

[OSS84] Ong, H., C.P. Schnorr, and A. Shamir, "An Efficient Signature Scheme Based on Quadratic Equations", *16th STOC*, pp. 208-216, 1984.

[OSS84b] Ong, H., C.P. Schnorr, and A. Shamir, "Efficient Signature Schemes Based on Polynomial Equations", *Crypto84*, proceedings, Springer-Verlag, Lecture Notes in Computer Science, vol. 196, pp. 37-46, 1985.

[O89] Ostrovsky, R., "An Efficient Software Protection Scheme", in preparations.

[Pol84] Pollard, J.M., "Solution of $x^2 + ky^2 \equiv m \,(mod\, n)$, with Application to Digital Signatures", preprint, 1984.

[R83] Rabin, M.O., "Randomized Byzantine Agreement", *24th FOCS*, pp. 403-409, 1983.

[SV84] Santha, M., and U.V. Vazirani, "Generating Quasi-Random Sequences from Slightly-Random Sources", *25th Symp. on Foundation of Computer Science*, pp. 434-440, 1984.

[S82] Shamir, A., "A Polynomial-Time Algorithm for Breaking the Merkle-Hellman Cryptosystem", *23rd FOCS*, pp. 145-152, 1982.

[S87] Stern, J., "Secret Linear Congruential Generators are not Cryptographically Secure", *28th FOCS*, pp. 421-426, 1987.

[V85] U.V. Vazirani, "Towards a Strong Communication Complexity Theory or Generating Quasi-Random Sequences from Two Communicating Slightly-Random Sources", *Proc. 17th ACM Symp. on Theory of Computing*, 1985, pp. 366-378.

[V87] U.V. Vazirani, "Efficiency Considerations in Using Semi-random Sources", *Proc. 19th ACM Symp. on Theory of Computing*, 1987, pp. 160-168.

[VV85] U.V. Vazirani, and V.V. Vazirani, "Random Polynomial Time is equal to Slightly-Random Polynomial Time", *26th Symp. on Foundation of Computer Science*, pp. 417-428, 1985.

A.8 Historical Background

An inspection of the references listed above reveals that all these works were initiated in the 80's and began to appear in the literature in 1982 (e.g. [GM82]). However, previous work had tremendous influence on these works of the 80's. The influence took the form of setting intuitive goals, providing basic techniques, and suggesting potential solutions which served as a basis for constructive criticism (leading to robust approaches).

8.1. Classic Cryptography

Answering the fundamental question of classic cryptography in a gloomy way (i.e. it is *impossible* to design a code that cannot be broken), Shannon suggested a modification to the question [S49]. Rather than asking whether it is *possible* to break the code, one should ask whether it is *feasible* to break it. A code should be considered good if it cannot be broken when investing work which is in reasonable proportion to the work required of the legal parties using the code.

8.2. New Directions in Cryptography

Prospects of commercial application were the trigger for the beginning of civil investigations of encryption schemes. The DES designed in the early 70's has adopted the new paradigm: it is clearly *possible* but supposely *infeasible* to break it.

Following the challenge of constructing and analyzing new encryption schemes came new questions like how to exchange keys over an insecure channel [M78]. New concepts were invented: *digital signatures* [R77, DH76], *public-key cryptosystems* and *one-way functions* [DH76]. First implementations of these concepts were suggested in [MH78, RSA78, R79].

Cryptography was explicitly related to complexity theory in [Br79, EY80, Lem79]: it was understood that problems related to breaking a cryptographic scheme cannot be $\mathcal{NP}$-complete and that $\mathcal{NP}$-hardness is a poor evidence for cryptographic security. Techniques as "n-out-of-$2n$ verification" [R77] and secret sharing [S79] were introduced (and indeed were used extensively in subsequent research).

8.3. At the Dawn of a New Era

Early investigations of cryptographic protocols revealed the inadequacy of imprecise notions of security and the subtleties involved in designing cryptographic protocols. In particular, problems as *coin tossing over telephone* [B82a], *exchange of secrets* and *oblivious transfer* were formulated [R81, B82b] (cf. [EGL82]). Doubts concerning the security of "mental poker" protocol of [SRA79] led to the current notion of secure encryption [GM82] and to concepts as computational indistinguishability. Doubts concerning the Oblivious Transfer protocol of [R81] led to the concept of zero-knowledge [GMR85] (early versions date to March 1982).

An alternative approach to the security of cryptographic protocols was suggested in [DY81] (see also [DEK82]), but it turned out that it is much too difficult to test whether a protocol is secure [EG83]. Fortunately, tools for constructing secure protocols do exist (see [Y86, GMW87])!

references

[B82a] Blum, M., "Coin Flipping by Phone", *IEEE Spring COMPCOM*, pp. 133-137, February 1982. See also *SIGACT News*, Vol. 15, No. 1, 1983.

[B82b] Blum, M., "How to Exchange Secret Keys", Memo. No. UCB/ERL M81/90. *ACM Trans. Comput. Sys.*, Vol. 1, pp. 175-193, 1983.

[Br79] Brassard, G., "A Note on the Complexity of Cryptography", *IEEE Trans. on Inform. Th.*, Vol. 25, pp. 232-233, 1979.

[DH76] W. Diffie, and M. E. Hellman, "New Directions in Cryptography", *IEEE transactions on Info. Theory*, IT-22 (Nov. 1976), pp. 644-654

[DEK82] Dolev, D., S. Even, and R. Karp, "On the Security of Ping-Pong Protocols", *Advances in Cryptology: Proceedings of Crypto82*, Plenum Press, pp. 177-186, 1983.

[DY81] Dolev, D., and A.C. Yao, "On the Security of Public-Key Protocols", *IEEE Trans. on Inform. Theory*, Vol. 30, No. 2, pp. 198-208, 1983. Early version in *FOCS81*.

[EGL82] Even, S., O. Goldreich, and A. Lempel, "A Randomized Protocol for Signing Contracts", *CACM*, Vol. 28, No. 6, 1985, pp. 637-647. Extended abstract in *Crypto82*.

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

[EY80] Even, S., and Y. Yacobi, "Cryptography and NP-Completeness", *7th ICALP* proceedings, Lecture Notes in Computer Science, Vol. 85, Springer Verlag, pp. 195-207, 1980. See also later version by Even, Selman, and Yacobi (titled: "The Complexity of Promise Problems with Applications to Public-Key Cryptography") in *Inform. and Control*, Vol. 61, pp. 159-173, 1984.

[GMW87] see main references.

[GM82] see main references.

[GMR85] see main references.

[Lem79] Lempel, A., "Cryptography in Transition", *Computing Surveys*, Dec. 1979.

[M78] Merkle, R.C., "Secure Communication over Insecure Channels", *CACM*, Vol. 21, No. 4, pp. 294-299, 1978.

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

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

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

[R81] Rabin, M.O., "How to Exchange Secrets by Oblivious Transfer", unpublished manuscript, 1981.

[RSA78] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *Comm. ACM*, Vol. 21, Feb. 1978, pp 120-126

[S79] Shamir, A., "How to Share a Secret", *CACM*, Vol. 22, 1979, pp. 612-613.

[S83] A. Shamir, "On the Generation of Cryptographically Strong Pseudorandom Sequences", *ACM Transaction on Computer Systems*, Vol. 1, No. 1, February 1983, pp. 38-44.

[SRA79] Shamir, A., R.L. Rivest, and L. Adleman, "Mental Poker", MIT/LCS report TM-125, 1979.

[S49] Shannon, C.E., "Communication Theory of Secrecy Systems", *Bell Sys. Tech. J.*, 28, pp. 656-715, 1949.

[Y86] see category 6.