On the Foundations of Modern Cryptography

Oded Goldreich
Department of Computer Science and Applied Mathematics
Weizmann Institute of Science, Rehovot, ISRAEL.
Email: oded@wisdom.weizmann.ac.il

June 5, 1997

In our opinion, the Foundations of Cryptography are the paradigms, approaches and techniques used to conceptualize, define and provide solutions to natural cryptographic problems. We survey some of these paradigms, approaches and techniques as well as some of the fundamental results obtained using them. Special effort is made in attempt to dissolve common misconceptions regarding these paradigms and results.

It is possible to build a cabin with no foundations,
but not a lasting building.
Eng. Isidor Goldreich (1906–1995)

Cryptography is concerned with the construction of schemes which are robust against malicious attempts to make these schemes deviate from their prescribed functionality. Given a desired functionality, a cryptographer should design a scheme which not only satisfies the desired functionality under "normal operation", but also maintains this functionality in face of adversarial attempts which are devised after the cryptographer has completed his/her work. The fact that an adversary will devise its attack after the scheme has been specified makes the design of such schemes very hard. In particular, the adversary will try to take actions other than the ones the designer had envisioned. Thus, our approach is that it makes little sense to make assumptions regarding the specific *strategy* that the adversary may use. The only assumptions which can be justified refer to the computational *abilities* of the adversary. Furthermore, it is our opinion that the design of cryptographic systems has to be based on *firm foundations*; whereas ad-hoc approaches and heuristics are a very dangerous way to go. A heuristic may make sense when the designer has a very good idea about the environment in which a scheme is to operate, yet a cryptographic scheme has to operate in a maliciously selected environment which typically transcends the designer's view.

Providing firm foundations to Cryptography has been a major research direction in the last two decades. Indeed, the pioneering paper of Diffie and Hellman [8] should be considered the initiator of this direction. Two major (interleaved) activities have been:

1. **Definitional Activity**: The identification, conceptualization and rigorous definition of cryptographic tasks which capture natural security concerns; and

2. **Constructive Activity**: The study and design of cryptographic schemes satisfying definitions as in (1).

The definitional activity provided a definition of secure encryption [17]. The reader may be surprised: *what is there to define* (beyond the basic setting formulated in [8])? Let us answer with a question (posed by [17]): *should an encryption scheme which leaks the first bit of the plaintext be considered secure?* Clearly, the answer is negative and so some naive conceptions regarding secure encryption (e.g., "a scheme is secure if it is infeasible to obtain the plaintext from the ciphertext when not given the decryption key") turn out to be unsatisfactory. The lesson is that even when a natural concern (e.g., "secure communication over insecure channels") has been identified, work still needs to be done towards a satisfactory (rigorous) definition of the underlying concept. The definitional activity also undertook the treatment of unforgeable signature schemes [19]: One result of the treatment was the refutation of a "folklore theorem" (attributed to Ron Rivest) by which "a signature scheme that is robust against chosen message attack cannot have a proof of security". The lesson here is that unclear/unsound formulations (i.e., those underlying the above folklore paradox) lead to false conclusions.

Another existing concept which was re-examined is the then-fuzzy notion of a "pseudorandom generator". Although ad-hoc "pseudorandom generators" which pass some ad-hoc statistical tests may be adequate for some statistical samplings, they are certainly inadequate for use in Cryptography: For example, sequences generated by linear congruential generators are easy to predict and endanger cryptographic applications even when not given in the clear. The alternative suggested in [7, 17, 26] is a robust notion of pseudorandom generators – such a generator produces sequences which are *computationally indistinguishable* from truly random sequences, and thus, can replace truly random sequences in any practical application. The approach was further extended to pseudorandom functions [13].

The definitional activity has identified concepts which were not known before. One well-known example is the introduction of zero-knowledge proofs [18]. A key paradigm crystallized in making the latter definition is the *simulation paradigm*: A party is said to have gained nothing from some extra information given to it if it can generate (i.e., simulate the receipt of) essentially the same information by itself (i.e., without being given this information). The simulation paradigm plays a central role in the related definitions of secure multi-party computations as well as in different settings.

The definitional activity is an on-going process. Its more recent targets have included mobile adversaries, Electronic Cash, Coercibility, Threshold Cryptography and more.

The constructive activity. As new definitions of cryptographic tasks emerged, the first challenge was to demonstrate that they can be achieved. Thus, the first goal of the constructive activity is to *demonstrate the plausibility* of obtaining certain goals. Thus, standard assumptions such as that the RSA is hard to invert were used to construct secure public-key encryption schemes [17, 26] and unforgeable digital schemes [19]. We stress that assuming that RSA is hard to invert is different from assuming that RSA is a secure encryption scheme. Furthermore, plain RSA (alike any deterministic public-key encryption scheme) is not secure (as one can easily distinguish the encryption of one *predetermined* message from the encryption of another). Yet, RSA can be easily transformed into a secure public-key encryption scheme by using a construction which is reminiscent of a common practice (of padding the message with random noise). We stress that the resulting scheme is not merely believed to be secure but rather its security is linked to a much simpler assumption (i.e., the assumption that RSA is hard to invert). Likewise, although plain RSA signing is vulnerable to "existential forgery" (and other attacks), RSA can be transformed into a signature scheme which is unforgeable (provided RSA is hard to invert). Using the assumption that RSA is hard to invert, one can construct pseudorandom generators [7, 26], zero-knowledge proofs for any NP-statement [15], and multi-party protocols for securely computing any multi-variant function [27, 16].

A major misconception regarding theoretical work in Cryptography stems from not distinguishing work aimed at demonstrating the plausibility of obtaining certain goals from work aimed at suggesting paradigms and/or constructions which can be used in practice. For example, the results concerning zero-knowledge proofs and multi-party protocols [15, 27, 16] mentioned above are merely *claims of plausibility*: What they say is that any problem of the above type (i.e., any protocol problem) can be solved in principle. This is a very valuable piece of information. Thus, if you have a specific problem which falls into the above category then you should know that the problem is solvable in principle. However, if you need to construct a real system then you should probably construct a solution from scratch (rather than employing the above general results). Typically, *some* tools developed towards solving the general problem may be useful in solving the specific problem. Thus, we distinguish three types of results:

1. *Plausibility results:* Here we refer to mere statements of the type "any NP-language has a zero-knowledge proof system" (cf., [15]).

2. *Introduction of paradigms and techniques which may be applicable in practice:* Typical examples include construction paradigms as the "choose n out of $2n$ technique" of [24], the "authentication tree" of [21, 22], the "randomized encryption" paradigm of [17], proof techniques as the "hybrid argument" of [17] (cf., [12, Sec. 3.2.3]), and many others.

3. *Presentation of schemes which are suitable for practical applications:* Typical examples include the public-key encryption schemes of [6], the digital signature schemes of [9, 10], the session-key protocols of [3, 4], and many others.

Typically, it is quite easy to determine to which of the above categories a specific technical contribution belongs. Unfortunately, the classification is not always stated in the paper; however, it is typically evident from the construction. We stress that all results we are aware of (and in particular all results cited here), come with an explicit construction. Furthermore, the security of the resulting construction is explicitly related to the complexity of certain intractable tasks. In contrast to some uninformed beliefs, for each of these results there is an explicit translation of concrete intractability assumptions (on which the scheme is based) into lower bounds on the amount of work required to violate the security of the resulting scheme.[1] We stress that this translation can be invoked for any value of the security parameter. Doing so determines whether a specific construction is adequate for a specific application under specific reasonable intractability assumptions. In many cases the answer is in the affirmative, but in general this does depend on the specific construction as well as on the specific value of the security parameter and on what is reasonable to assume for this value. When we say that a result is suitable for practical applications (i.e., belongs to Type 3 above), we mean that it offers reasonable security for reasonable values of the security parameter and reasonable assumptions.

Other activities. This brief summary is focused on the definitional and constructive activities mentioned above. Other activities in the foundations of cryptography include the exploration of new directions and the marking of limitations. For example, we mention novel modes of operation such as split-entities [5, 23], batching operations [11], off-line/on-line signing [10] and Incremental Cryptography [1, 2]. On the limitation side, we mention [20, 14]. In particular, [20] indicates that

[1] The only exception to the latter statement is Levin's observation regarding the existence of a *universal one-way function* (cf., [12, Sec. 2.4.1]).

certain tasks (e.g., secret key exchange) are unlikely to be achieved by using a one-way function in a "black-box manner".

Bibliographic Notes

This is a brief summary of an essay which will appear in the proceedings of Crypto97 (to be published in Springer's LNCS series). Suggestions for further reading appear in Section 10 of the essay. Revised versions of the essay will be available from `http://theory.lcs.mit.edu/~oded/tfoc.html`.

Bibliographic Abbreviations

- STOC is *ACM Symposium on the Theory of Computing.*
- FOCS is *IEEE Symposium on Foundations of Computer Science.*

References

[1] 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.

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

[3] M. Bellare and P. Rogaway. Entity Authentication and Key Distribution. In *Crypto93*, Springer-Verlag LNCS (Vol. 773), pages 232–249, 1994.

[4] M. Bellare and P. Rogaway. Provably Secure Session Key Distribution: The Three Party Case. In *27th STOC*, pages 57–66, 1995.

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

[6] M. Blum and S. Goldwasser. An Efficient Probabilistic Public-Key Encryption Scheme which hides all partial information. In *Crypto84*, LNCS (Vol. 196) Springer-Verlag, pages 289–302.

[7] 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.

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

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

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

[11] A. Fiat. Batch RSA. *J. of Crypto.*, Vol. 10, 1997, pages 75–88.

[12] O. Goldreich. *Foundation of Cryptography – Fragments of a Book.* February 1995. Available from `http://theory.lcs.mit.edu/~oded/frag.html`

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

[14] 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.

[15] 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. See also preliminary version in *27th FOCS*, 1986.

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

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

[18] S. Goldwasser, S. Micali and C. Rackoff. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. on Comput.*, Vol. 18, pages 186–208, 1989.

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

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

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

[22] R.C. Merkle. A Certified Digital Signature Scheme. In *Crypto89*, Springer-Verlag LNCS (Vol. 435), pages 218–238.

[23] S. Micali. Fair Public-Key Cryptosystems. In *Crypto92*, Springer-Verlag LNCS (Vol. 740), pages 113–138.

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

[25] 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.

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

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