Preface to Shafi & Silvio's book*

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

March 29, 2019

There are no privileges without duties

Adv. Klara Goldreich-Ingwer (1912–2004)

Cryptography is concerned with the construction of schemes that withstand any abuse: A cryptographic scheme is constructed so as to maintain a desired functionality, even under malicious attempts aimed at making it deviate from its prescribed behavior. The design of cryptographic systems must be based on firm foundations, whereas ad-hoc approaches and heuristics are a very dangerous way to go. These foundations were developed mostly in the 1980's, in works that are all co-authored by Shafi Goldwasser and/or Silvio Micali. These works have transformed Cryptography from an engineering discipline, lacking sound theoretical foundations, into a scientific field possessing a well-founded theory, which influences practice as well as contributes to other areas of Theoretical Computer Science. The current book celebrates these works, which were the basis for bestowing the 2012 Turing Award upon Shafi Goldwasser and Silvio Micali.

♢ ♢ ♢

Cryptography as we know it today is based entirely on concepts, definitions, techniques, and feasibility results put forward and developed in the works of Goldwasser and/or Micali. A significant portion of this book reproduces some of these works, whose contents is briefly outlined next.

Probabilistic Encryption (see Chapter 7). The pivot of the aforementioned body of work is the pioneering work *Probabilistic Encryption*, whose title reflects the realization that a robust notion of secure encryption requires the use of randomization in the process of encrypting each message (and not only in the process of generating cryptographic keys). This work of Goldwasser and Micali defined the mind-set of the field by establishing conceptual frameworks and demonstrating their usefulness. In particular:

*To appear in an ACM book celebrating the work of Goldwasser and Micali.

- This work suggested viewing computationally indistinguishable objects as equivalent. This revolutionary suggestion has played a key role in all standard cryptographic definitions and has served as the pivot of the acclaimed theory of pseudorandomness (to be briefly reviewed below).

- This work suggested interpreting security as the ability to emulate an ideal setting. This suggestion, further clarified by Goldwasser and Micali in early versions of *The Knowledge Complexity of Interactive Proof Systems* (briefly reviewed below). has been adopted as the basic approach to defining security in almost all cryptographic settings. This approach, known as the simulation paradigm, *resolves the Gordian Knot that has frustrated previous attempts to define security by trying to enumerate all desired properties*. The simulation paradigm bypasses this enumeration by asserting that security means that anything that can be efficiently obtained by an attack on the cryptographic system can be essentially obtained (as efficiently) without attacking the system. Thus, any gain that an attacker claims is actually not due to the use of the cryptographic system.

- This work demonstrated the fruitfulness of the aforementioned paradigm shift by providing robust definitions for the most basic cryptographic primitive (i.e., encryption schemes) and by constructing a secure encryption scheme based on a standard complexity assumption. In addition to demonstrating the viability of the new-at-the-time approach, this paper set the standard for the two-step process to be followed by all subsequent works:

  1. First, a robust definition is developed, based on the aforementioned approach.
  2. Next, schemes satisfying this definition are proven to exist (and actually explicitly constructed) based on much better understood assumptions.

  For example, once defined, it was not *a priori* clear whether zero-knowledge proofs exist at all, and thus relating this question to well-known conjectures demonstrated the viability of zero-knowledge.

- This work also introduced important techniques, one being later termed *the hybrid argument*, which found numerous applications in cryptography and in the theory of pseudorandomness. Notably, this work also heralded worst-case to average-case reductions (a.k.a random self-reducibility).

The Knowledge Complexity of Interactive Proof Systems (Chapter 8). The second most influential work of Goldwasser and Micali is their joint work on zero-knowledge, which after not being understood by most researchers for three years, and being revised several times, appeared in the "formal verification" session of STOC'85 (indicating that it was misunderstood even by the program committee that accepted it for presentation). I can testify to the fact that the lack of understanding has not been due to a poor presentation of the ideas, but rather to their revolutionary nature. (By the way, their earlier work "Probabilistic Encryption" also faced lack of understanding for a couple of years.)

Nowadays, it is well-understood that this work introduced two fascinating and highly influential concepts: the concept of interactive proofs and the concept of zero-knowledge. The concept of interactive proofs had a vast impact on complexity theory, to be briefly reviewed below. The concept of zero-knowledge, on top of being very intriguing (once one stops being confused by

it), became a central tool in cryptography, and led to fundamental discoveries regarding general secure multi-party computation. Initial indications to the vast potential impact of these concepts were provided by the results and discussions in the conference version of this work (reproduced in Chapter 8).

How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits (Chapter 9). This work defined pseudorandom generators as producing a sequence of unpredictable bits. This definition was later shown to be equivalent to being computationally indistinguishable from the uniform distribution over bit-strings of adequate length. The notion of computational indistinguishably used here is the same as the notion introduced in *Probabilistic Encryption*, but subsequent works introduced a variety of alternative definitions yielding a host of notions of pseudorandom generators. This work also defined the notion of a hard-core predicate of a one-way function, and established its existence for the modular exponentiation function.

How to Construct Random Functions (Chapter 10). This work extended the theory of pseudorandomness to functions, and showed how to construct pseudorandom functions based on any pseudorandom generator. The notion of a pseudorandom function found numerous applications in cryptography, starting from the construction of message authentication codes and private-key encryption schemes that withstand chosen ciphertext attacks.

A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks (Chapter 11). The result proved by this paper was considered impossible or at least "paradoxical" at the time, because it was (falsely) believed that a "constructive proof of unforgeability" (under passive attacks) implies a successful chosen-message attack.

Proofs that Yield Nothing but their Validity or All Languages in NP Have Zero-Knowledge Proof Systems (Chapter 12). This work demonstrated the generality and wide applicability of zero-knowledge proofs. In particular, assuming the existence of secure commitment schemes, it showed how to construct zero-knowledge interactive proof systems for any set in NP, yielding a powerful tool for the design of various cryptographic schemes. Loosely speaking, zero-knowledge proofs offer a way for a party to prove that it has behaved according to a predetermined protocol, *without revelaing its own secrets*, and so they can be used to force parties to behave in "honest-but-curious" manner.

How to Play any Mental Game – A Completeness Theorem for Protocols with Honest Majority (Chapter 13). This work presented constructions of secure protocols for any multi-party computation problem. In other words, it shows how a trusted party can be emulated by a set of mutually distrustful parties. This result combines the construction of "privacy-preserving" protocols for the "honest-but-curious" model with a method (presented in Chapter 12) of forcing parties to behave in an honest-but-curious. The privacy-preserving protocols rely on the existence of a public-key encryption scheme and an Oblivious Transfer protocol, which can both be based on the existence of trapdoor permutations.

Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Chapter 15). This work obtained the general results similar to those of the foregoing

work (of Chapter 13), except that it uses no intractability assumptions. Instead this work presumes the existence of private channels between each pair of parties (and a larger percentage of honest parties).

Multi-Prover Interactive Proofs: How to Remove Intractability (Chapter 16). Motivated by the desire to construct zero-knowledge proof systems without relying on intractability assumptions, this work presented a model of multi-prover interactive proofs in which the provers cannot interact with one another during their interaction with the verifier. This model, denoted MIP, turned out to be closely related to the PCP model, which was introduced later and is briefly reviewed below.

Non-Interactive Zero-Knowledge (NIZK) Proof Systems (Chapter 14). The model of non-interactive proof systems introduced in this work includes a common random string provided from the outside and available to both the prover and the verifier. The work showed how to provide zero-knowledge (non-interactive) proofs for any NP-assertion. Such NIZKs have been used as a building blocks in many subsequent works (e.g., in constructing public-key encryption schemes that withstand chosen-ciphertext attacks).

Part II of this book reproduces the conference versions of the ten foregoing works (while using the titles of their journal versions, which are different in few of the cases). These conference versions are extended abstracts that lack many of the details that support the claims made in them, but they best portray the spirit of innovation, boldness, and freshness that is characteristic of Shafi Goldwasser and Silvio Micali.

Part III of this book presents scientific surveys of the works of Shafi Goldwasser and Silvio Micali and of works that were directly inspired by their work. This part starts with a survey of the foundations of cryptography.

On the foundations of cryptography. Before spelling out what these foundations are, let us briefly reflect on the significance of such theoretical foundations to cryptographic practice. While the following argument is widely accepted nowadays, it required a convincing advocation in the 1980's. Needless to say, Shafi Goldwasser and Silvio Micali provided such advocation when presenting their pioneering work.

Surely, providing sound theoretical foundations is of great importance for any discipline, but more so for cryptography, since cryptography is concerned with the construction of schemes that should be robust against malicious attempts to make these schemes deviate from their prescribed functionality. 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 that typically transcends the designer's view. In fact, the adversary is likely to take the very actions that were dismissed or ignored by the designer. Thus, the design of cryptographic systems has to be based on *firm foundations*, as provided by the research project lead by Goldwasser and Micali in the 1980's.

The foundations of cryptography are the main paradigms, approaches and techniques used to conceptualize, define and provide solutions to natural cryptographic problems. These foundations

will be reviewed in Chapter 17, starting with a presentation some of the central tools used in cryptography; that is, computational difficulty (in the form of one-way functions), pseudorandomness, and zero-knowledge proofs. Based on these tools, the survey treats basic cryptographic applications such as encryption and signature schemes as well as the design of general secure cryptographic protocols. It is striking to note that the entire exposition is rooted directly or indirecting in works of Goldwasser and Micali. Indeed, the history of laying the foundations of cryptography is the story of the works of Goldwasser and Micali.

Impact on Complexity Theory. The revolutionary evolution of cryptography in the 1980's had a great impact on other areas of Computer Science most notably on Complexity Theory. Some of this impact will be reviewed in Chapter 18. Among the direct contributions of the cryptographic evolution to Computer Science, I wish to highlight the theory of pseudorandomness and the study of probabilistic proof systems. Notably, Goldwasser and Micali played a key role also in the development of these specific areas.

A fresh view at the "question of randomness" was taken in the Theory of Computing: It has been postulated that a distribution is *pseudorandom* if it cannot be told apart from the uniform distribution by any efficient procedure. This paradigm, which was introduced in cryptography where efficient procedures were associated with polynomial-time algorithms that may be stronger than the (purported pseudorandom) generator, has been applied also with respect to a variety of limited classes of such distinguishing procedures including polynomial-size circuits that are smaller than the running time of the generator, constant-depth circuits, space-bounded machines, local tests (cf., limited independence generators), linear tests (cf., small bias generators), non-deterministic polynomial-time machines, and more. Indeed, this paradigm has been the basis of a vast body of intriguing research concerned with the role of randomness in computation. Also worth noting are the application of pseudorandom functions (e.g., to hardness of *PAC learning* and to "Natural Proofs").

Various types of *probabilistic* proof systems have played a central role in the development of Computer Science in the last decades. Such non-traditional formulations of proof systems, which allow for a bounded probability of error and view the proof as a dynamic process rather than as a static object, have many advantages over the classical formulation of proof systems (which underlies NP). These advantages are demonstrated by the known results regarding Interactive Proofs, Zero-Knowledge Proofs, and Probabilistically Checkable Proofs (PCP). The fruitful connection between PCPs and the complexity of natural approximation problems was also discovered in such a work. This connection has provided a breakthrough in the study of approximation algorithms, which has been almost literally stuck for two decades.

On some other works of Goldwasser and Micali. Although the main topic of this book is the contributions of Goldwasser and Micali to the foundations of cryptography, it will be inappropriate not to mention their direct contributions to other areas within the theory of computation. Some of these contributions are surveyed in Chapter 18, where the perspective is of the impact of cryptography on complexity theory. In addition, Chapter 19 surveys a few other contributions, without mentioning the relations of some of them to cryptography. The selection of titles includes:

- *An $O(\sqrt{|V|} \cdot |E|)$-time algorithm for finding maximum matching in general graphs*, which still holds the record for the fastest algorithm for this central computational problem.

- *Certifying almost all primes using elliptic curves*, which presented a randomized polynomial-time algorithm that produces (absolute) certificates of primality for almost all primes.
- *Private coins versus public coins in interactive proof systems*, which provided a transformation of general interactive proof systems into ones in which the verifier only poses totally random challenges.
- *An optimal randomized protocol for synchronous Byzantine Agreement*, which provided a constant-round protocol for this central problem.
- *PCPs and the hardness of approximating the size of maximum cliques*, which provided a PCP system of almost logarithmic randomness and query complexity for NP, and linked such systems to the complexity of a central approximation problem.
- *Computationally Sound proofs*, which presented natural notions of computationally-sound proof systems.
- *Property Testing and its connection to learning and approximation*, which initiated a general study of approximate decision problems that can be solved in sublinear time, while focusing on testing properties of (dense) graphs.
- *Pseudo-deterministic algorithms*, which initiated the study of probabilistic algorithms for solving search problems in a consistent manner (i.e., almost always return the same canonical solution).

For each of these selected works, the original abstract is reproduced, and a few additional comments about the work are made. It should be stressed that although Chapters 17–19 review many of the most influential works of Goldwasser and Micali, they are far from exhausting this list, as illustrated by Chapters 21, 24 and 26.

Scientific vinettes by some of their former students. Few of Goldwasser's and Micali's former students were asked to write chapters about topics of their choice. Most of them agreed, and some of them delivered. Certainly, Shafi and Silvio do not educate their students to be timely. In their defense, one may say that they don't preach what they don't practice.

Zvika Brakerski's survey (Chapter 20), *Fundamentals of Fully Homomorphic Encryption*, reviews a topic that was not pioneered by Goldwasser and Micali. In fact, the partial homomorphic property of the Goldwasser-Micali encyption scheme was considered more as a bug than as a feature, which led them to suggest using it only for the establishing of a key for a symmetric encryption scheme (see their work *Why and How to Establish a Private Code on a Public Network*, with Po Tong in FOCS 1982). Nevertheless, perspectives have changed, and the potential benefits of fully homomorphic encryption, envisioned by Rivest *et al.* (in 1978), have been materialized by the surprising discovery of fully homomorphic encryption schemes whose security are based on computational problems regarding lattices.

Computational problems regarding lattices are also the pivot of Daniele Micciancio's survey (Chapter 21), *Interactive Proofs for Lattice Problems*. The starting point of this survey is a work of Goldreich and Goldwasser that presented perfect zero-knowledge interactive proof systems for central problems regarding lattices (in order to demonstrate that they are unlikely to be NP-hard). The survey provides the basic background for the computational aspects of lattices, and

focuses on several interactive proof systems for various claims regarding lattices, while exposing their underlying ideas.

Johan Hastad's survey (Chapter 22), *Following a tangent of proofs*, also starts with interactive proof systems, but its actual focus is on the non-approximability results that can be derived from *probabilistically checkable proofs* (PCPs), which in turn arised from multi-prover interactive proof systems. Hastad confesses that, at the time, he considered the multi-prover model to be "artificial" and doubted the justification of introducing an esoteric complexity class that corresponds to it. His past reaction was reminiscent of the reactions that other notions introduced previously by Goldwasser and Micali have received (cf., e.g., probabilistic encryption and zero-knowledge). Needless to say, in all cases, these skeptic reactions were proved wrong.

Rafael Pass's *Tutorial on Concurrent Zero Knowledge* (Chapter 23) addresses the issue of preserving the zero-knowledge feature under "concurrent composition". The point is that the original definition of zero-knowledge refers to a stand-alone execution, and the preservation of security under sequential, parallel, and even concurrent executions is far from clear. While augmenting the original definition with auxiliary inputs suffices for sequential composition, preservation of security under parallel and concurrent executions requires some work. Dealing with concurrent executions is most challenging, and the tutorial presents the simplest known solution, which did not appear is isolation before.

Guy Rothblum's survey (Chapter 24), *Doubly-Efficient Interactive Proofs*, revisits the notion of interactive proof systems with a focus on more strict complexity requirements. In particular, the (honest) prover strategy is required to run in polynomial-time, and the verifier strategy is required to run in almost linear time. Such interactive proof systems, later termed *doubly-efficient*, were first defined and constructed by Goldwasser, Kalai, and Rothblum. Interestingly, this notion was considered by Shafi, Silvio, and myself in the mid 1980s, but we failed to find any appealing example (i.e., one in which interaction speeds-up verification).

The starting point of Salil Vadhan's survey (Chapter 25), *Computational Entropy*, is the notion of computational indistinguishability, put forward by Goldwasser and Micali (see Chapter 7), as applied in the theory of pseudorandomness. This starting point leads to the introduction of computational analogues of other statistical notions such as entropy, min-entropy, KL-divergence, and more. These notions play a major role in the constructions of pseudorandom generators and statistically hiding commitment schemes, which are surveyed in this chapter.

Deviating for the framework that underlies all the foregoing, Yael Tauman Kalai and Leonid Reyzin's *Survey of Leakage-Resilient Cryptography* (Chapter 26) considers cases in which the computing devices used by the honest parties may leak partial information about the their computation or storage. That is, whereas the foregoing views algorithms and strategies as functions (which, once feed with inputs, return adequate outputs), the leakage models attempt to account for the fact that computation is taking place on a physical device that may be subject to various physical measurements, and leakage-resilient schemes attempt to protect against corresponding physical attacks. As noted in the survey, Goldwasser and Micali have contributed significantly also to this research direction.

In contrast to this preface, which started with a review of the works of Goldwasser and Micali, the book starts with their lives and voices. Specifically, Part I contains a brief personal biography

of each of them, an interview with each of them, which touches on both the personal and the professional, and revised transcripts of their Turing award lectures.

Brief biographies. Given the timidness of the theory of computation community, writing personal biographies of its pioneers seems quite challenging. On top of this, I was quite curious to see how a professional writer, who has no background in computer science, will view and portray Shafi and Silvio. I feel that both challenges were well-addressed by Michelle Waitzman. It is quite remarkable that Michelle was able to identify key features of their personalities and link these features to characteristics of their scientific research. Her success is well reflected in the titles she choose for the personal biographies – *Shafi Goldwasser: A story behind every problem* and *Silvio Micali: One obsession at a time*.

Interviews. Given that both Shafi and Silvio are very interactive personalities, interviewing them must have been a pleasure. The pleasure was shared among Alon Rosen, who interviewed Shafi Goldwasser, while building on his expertise in cryptography, and Stephen Ibaraki, who interviewed Silvio Micali (as part of an interview series with outstanding computer professionals). The interviews refer both to the personal life and professional work of Goldwasser and Micali, and the former aspects have some overlap with the biographies, where a common theme is indeed the relation of the personal and the professional. Lightly edited extracts from the two interviews are included in this volume.

The Turing Lectures. Lastly, this volume includes lightly edited versions of the Turing lectures given by Shafi Goldwasser and Silvio Micali during the *46th Annual Symposium on the Theory of Computing*, which took place in New York, in June 2014. Shafi's lecture focused on the influence of cryptographic research on the rest of computer science, whereas Silvio's lecture focused on the evolution of the notion of proofs.

♡ ♡ ♡

I believe that the work of Shafi Goldwasser and Silvio Micali is of historical dimension. Its impact on the development of Cryptography and related areas in complexity theory has the flavor of a scientific revolution (in Kuhn's sense). Hence, whoever performs research in these areas is living in a world created and shaped by their work. In light of the above, it is our professional and personal duty to acknowledge our debt to these works. This assertion definitely holds about myself, having had also the privilege of benefiting from numerous interactions with Shafi and Silvio.