Information Security and Cryptography

For further volumes:
www.springer.com/series/4752

Benny Applebaum

Cryptography in Constant Parallel Time

Springer

Benny Applebaum
School of Electrical Engineering
Tel Aviv University
Tel Aviv, Israel

ISSN 1619-7100 Information Security and Cryptography
ISBN 978-3-642-17366-0 ISBN 978-3-642-17367-7 (eBook)
DOI 10.1007/978-3-642-17367-7
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013945294

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To my parents, my wife and my children.

Foreword

This book provides excellent coverage of the exciting results obtained in the last decade regarding the complexity of doing cryptography.

Cryptography is concerned with the study of the design of systems that are easy to operate but hard to abuse. Thus, a complexity gap between the ease of using such systems and the difficulty of abusing them lies at the heart of cryptography. The question addressed in the current book is how wide can this gap be. In a nutshell, the work presented in this book asserts that the gap may be much wider than one would have thought: The systems may be extremely easy to use (i.e., each output bit can be computed based on *a constant number* of input bits), whereas no efficient procedure may abuse them (i.e., the notion of security is the standard one).

Let me be somewhat more technical. The work provides strong evidence that many cryptographic primitives and tasks can be implemented with very low complexity. For example, it shows that the existence of one-way functions that can be evaluated in $\mathbf{NC}^1$ (and even somewhat above $\mathbf{NC}^1$) implies the existence of one-way functions that can be evaluated in $\mathbf{NC}^0$. Whereas the former are widely believed to exist (e.g., based on the standard factoring assumption), most researchers have previously believed that the latter do not exist. Recall that evaluation in $\mathbf{NC}^0$ means that each output bit only depends on a constant number of input bits. This work further shows that dependence on *four* input bits suffices (whereas dependence on at least *three* input bits is definitely necessary).

Let me briefly discuss the aforementioned beliefs. Recall that all known constructions of cryptographic primitives are based on complexity assumptions. In particular, all these assumptions (and actually also the very existence of these cryptographic primitives) imply $\mathbf{P} \neq \mathbf{NP}$ and thus establishing any of these assumptions would resolve the famous P-vs-NP question. Thus, unless one resolves the P-vs-NP question, a result of the current type must be based on some assumptions. The complexity assumptions used in the current work are among the weakest ones used in cryptographic research.

Actually, the work presents a transformation of implementations of cryptographic primitives, taking any implementation in a class between $\mathbf{NC}^1$ and $\mathbf{NC}^2$, and producing an implementation in $\mathbf{NC}^0$. (Recall that $\mathbf{NC}$ is the class of problems that are solvable by polynomial-size circuits of polylogarithmic depth, and $\mathbf{NC}^i$ denotes the subclass in which the exponent of the polylogarithmic function is i.) The transformation is based on “randomizing polynomials” a notion introduced a few years ago for very different purposes. In particular, the original motivation was the study of *information-theoretic* privacy in multi-party computation, whereas the current context is complexity theoretic in nature.

The centerpiece of the book is presented in Chaps. 3 and 4, where the aforementioned results are proved. Let me stress that these chapters present an amazing breakthrough in the study of the theoretical foundations of cryptography. In particular, they provide extremely efficient implementations of several basic cryptographic tools. As I noted above, this outstanding achievement took almost all experts in the area by surprise. The following chapters (i.e., Chaps. 5–8) provide intriguing follow-ups and extensions of the direction initiated in Chaps. 3 and 4. The book also contains a nice exposition of the relevant background (specifically, Chap. 2).

Weizmann Institute of Science Oded Goldreich
May 2013

Preface

Cryptography is concerned with communication and computation in the presence of adversaries. A fundamental challenge in theoretical and practical cryptography is to minimize the computational complexity of honest parties while providing security against computationally strong attackers. Ideally, one would like to construct cryptographic tools or "primitives" which can be computed extremely fast and retain strong security guarantees. These two targets, *efficiency* and *security*, are somewhat contradictory as highly efficient functions may be too simple to generate cryptographic hardness. Identifying the minimal level of efficiency which still guarantees security is therefore a major research goal.

This book studies this question through the lens of parallel-time complexity. We ask whether basic cryptographic primitives can be computed in constant parallel time. Formally, we consider the possibility of computing instances of these primitives using $\mathbf{NC}^0$ circuits, in which each output bit depends on a constant number of input bits. Despite previous efforts in this direction, there has been no convincing theoretical evidence supporting this possibility, which was posed as an open question in several previous works (e.g., [50, 69, 85, 105, 112]). We essentially settle this question by providing strong evidence for the possibility of cryptography in $\mathbf{NC}^0$. In particular, we derive the following results.

Existence of Cryptographic Primitives in $\mathbf{NC}^0$ We show that many cryptographic primitives can be realized in $\mathbf{NC}^0$ under standard intractability assumptions used in cryptography, such as those related to factoring, discrete logarithm, or lattice problems. This includes one-way functions, pseudorandom generators, symmetric and public-key encryption schemes, digital signatures, message authentication schemes, commitment schemes, collision-resistant hash functions and zero-knowledge proofs. Moreover, we provide a *compiler* that transforms an implementation of a cryptographic primitive in a relatively "high" complexity class into an $\mathbf{NC}^0$ implementation. This compiler is also used to derive new unconditional $\mathbf{NC}^0$ *reductions* between different cryptographic primitives. In some cases, no parallel reductions of this type were previously known, even in $\mathbf{NC}$. Interestingly, we get *non-black-box* reductions.

Pseudorandom Generators with Linear Stretch in $\mathbf{NC}^0$ The aforementioned constructions of pseudorandom generators (PRGs) were limited to stretching a seed of n bits to $n + o(n)$ bits. This leaves open the existence of a PRG with a linear (let alone superlinear) stretch in $\mathbf{NC}^0$. We construct a linear-stretch PRG in $\mathbf{NC}^0$ under a relatively new intractability assumption presented by Alekhnovich [5]. We also identify a new connection between such pseudorandom generators and hardness of approximations for combinatorial optimization problems. In particular, we show that an $\mathbf{NC}^0$ pseudorandom generator with linear stretch implies that Max 3SAT cannot be efficiently approximated to within some multiplicative constant. Our argument is quite simple and does not rely on PCP machinery.

Cryptography with Constant Input Locality After studying $\mathbf{NC}^0$ functions, in which each output bit depends on a constant number of input bits, we move on to study functions in which each *input* bit affects a constant number of output bits, i.e., functions with constant *input* locality. We characterize what cryptographic tasks can be performed with constant input locality. On the negative side, we show that primitives that require some form of non-malleability (such as digital signatures, message authentication, or non-malleable encryption) *cannot* be realized with constant input locality. On the positive side, assuming the intractability of certain problems from the domain of error correcting codes, we obtain new constructions of one-way functions, pseudorandom generators, commitments, and semantically secure public-key encryption schemes whose input locality is constant. Moreover, these constructions also enjoy constant *output locality*. Therefore, they give rise to cryptographic hardware that has constant-depth, constant fan-in and constant *fan-out*.

A Study of Randomizing Polynomials Most of our results make use of the machinery of *randomizing polynomials*, which were introduced by Ishai and Kushilevitz [92] in the context of information-theoretic secure multiparty computation. Randomizing polynomials allow us to represent a function $f(x)$ by a low-degree randomized mapping $\hat{f}(x, r)$ whose output distribution on an input x is a *randomized encoding* of $f(x)$. We present several variants of this notion along with new constructions. Our new variants have applications not only in the domain of parallel cryptography. For example, by extending the notion of randomizing polynomials to the computational setting, we show that, assuming a PRG in $\mathbf{NC}^1$, the task of computing an *arbitrary* (polynomial-time computable) function with computational security can be reduced to the task of securely computing degree-3 polynomials (say, over $\mathbb{F}_2$) without further interaction. This gives rise to new, conceptually simpler, constant-round protocols for general functions.

This Version This book is based on the author's doctoral dissertation which was submitted to the Technion in 2007. Some of the sections and proofs have been extended to provide more details and intuition. The content has also been updated to reflect the main recent developments in the field of parallel-time cryptography. A detailed chapter-by-chapter description of the contents and a high-level list of updates appear in Sects. 1.2.2 and 1.3.

Tel Aviv, Israel Benny Applebaum

Acknowledgements

I am greatly indebted to Yuval Ishai and Eyal Kushilevitz, my advisors, for their guidance and friendship. Over the years, I have spent many hours in conversations with Yuval and Eyal. These long discussions have taught me invaluable lessons regarding many aspects of the scientific work and have shaped my scientific outlook. For the enjoyable collaboration which led to this book, for their insightful and knowledgeable advice, and for all their patience and help, I am deeply grateful to Yuval and Eyal.

I am greatly indebted to Oded Goldreich for closely accompanying this research. I was fortunate to have Oded as the editor of the journal versions of some of the works that appear in this book, and was even more fortunate to collaborate with him on some follow-up works. Oded's numerous suggestions and comments have significantly improved this monograph in many ways, and I am most grateful to him for sharing his wisdom and insights with me.

During my graduate studies, I had the opportunity to discuss research topics with many friends and colleagues. These interactions have been pleasant and fruitful. For this, I would like to thank Omer Barkol, Rotem Bennet, Eli Ben-Sasson, Eli Biham, Iftach Haitner, Danny Harnik, Moni Naor, Erez Petrank, Omer Reingold, Ronny Roth, Amir Shpilka, Amnon Ta-Shma, Enav Weinreb and Emanuele Viola. I am also thankful to Eli Biham, Oded Goldreich, Erez Petrank, and Omer Reingold for serving on my thesis committee.

I would like to thank all the people from the Computer Science department in the Technion, with whom I have worked and studied, for making my time at the Technion so pleasant. Special thanks go to my office partner, Boris Kapchits, and my floor mates, Rotem Bennet, Niv Buchbinder, Oren Katzengold, Jonathan Naor and Sharon Shoham—I really liked all these endless coffee breaks!

Since my graduation, I have spent wonderful years in the CS departments of Princeton University and the Weizmann Institute of Science. My sincere thanks to the theory groups at these institutes, and especially to Boaz Barak, Oded Goldreich, Moni Naor and Avi Wigderson for memorable times and priceless lessons from which I have learned so much.

I would like to acknowledge my current academic home, Tel Aviv University's School of Electrical Engineering. Special thanks go to my close colleagues Guy Even, Boaz Patt-Shamir and Dana Ron, for their kind support and lovely company.

Finally, I am grateful to my family and friends for their love and support. Most significantly, I would like to thank my parents, Arie and Elka, and my wife, Hilla. Some feelings cannot be expressed with words, but I can sincerely say that none of this would have been possible without you!

Contents