

Contents

1	Introduction	1
1.1	The Basic Question	1
1.1.1	Further Perspectives	2
1.2	Our Research	3
1.2.1	Our Approach	4
1.2.2	Results and Organization	4
1.3	Comparison with Doctoral Thesis Submitted to Technion	8
2	Preliminaries and Definitions	11
2.1	General	11
2.2	Statistical and Computational Indistinguishability	12
2.2.1	Some Useful Facts	12
2.3	Computational Models	14
2.4	Output Locality, Input Locality and Degree	16
3	Randomized Encoding of Functions	19
3.1	Definitions	19
3.2	Basic Properties	23
3.3	More Aspects of Randomized Encoding	27
3.3.1	The Necessity of Randomness	27
3.3.2	The Power of Randomized Encoding	27
3.3.3	Lower Bounds for Locality and Degree	29
4	Cryptography in NC^0	33
4.1	Introduction	33
4.1.1	Previous Work	33
4.1.2	Our Results	34
4.1.3	Overview of Techniques	36
4.1.4	Organization	39
4.2	NC^0 Encoding for Functions in $\oplus\text{L}/\text{poly}$ and NL/poly	39
4.2.1	Degree-3 Randomizing Polynomials from mod-2 BPs	39
4.2.2	Reducing the Locality	42

4.2.3	A Generalization of the Locality Construction	44
4.3	One-Way Functions in \mathbf{NC}^0	45
4.3.1	Key Lemmas	46
4.3.2	Main Results	49
4.4	Pseudorandom Generators in \mathbf{NC}^0	51
4.4.1	Cryptographic Generators	52
4.4.2	ε -Biased Generators	55
4.4.3	Generators for Space-Bounded Computation	57
4.4.4	Pseudorandom Generators—Conclusion	59
4.5	Collision-Resistant Hashing in \mathbf{NC}^0	59
4.6	Encryption in \mathbf{NC}^0	61
4.6.1	Main Results	61
4.6.2	On Decryption in \mathbf{NC}^0	64
4.6.3	Security Against CPA, CCA1 and CCA2 Attacks	65
4.7	Other Cryptographic Primitives	67
4.7.1	Signatures	67
4.7.2	Commitments	68
4.7.3	Zero-Knowledge Proofs	72
4.7.4	Instance Hiding Schemes	74
4.8	Summary and Discussion	74
4.8.1	The Case of PRFs	75
4.8.2	Open Problems	76
4.9	Appendix: On Collections of Cryptographic Primitives	76
5	Computationally Private Randomizing Polynomials and Their Applications	79
5.1	Introduction	79
5.1.1	Overview of Results and Techniques	79
5.1.2	Organization	83
5.2	Computational Encoding in \mathbf{NC}^0 for Efficient Functions	83
5.2.1	From PRG to One-Time Encryption	84
5.2.2	From One-Time Encryption to Computational Encoding	86
5.2.3	Main Results	90
5.2.4	Proof of Lemma 5.4	92
5.3	Applications	96
5.3.1	Relaxed Assumptions for Cryptography in \mathbf{NC}^0	96
5.3.2	Parallel Reductions Between Cryptographic Primitives	98
5.3.3	Secure Multiparty Computation	101
6	One-Way Functions with Optimal Output Locality	107
6.1	Introduction	107
6.1.1	Semi-private Randomized Encoding and Robust OWF	108
6.1.2	Constructing Robust OWF	109
6.2	Preliminaries	109
6.3	Semi-private Randomized Encoding	111
6.3.1	Definition and Construction	111

6.3.2	Encoding a Function via SPRE	113
6.4	Robust One-Way Function	115
6.4.1	A Candidate Robust One-Way Function	115
6.4.2	Proof of Theorem 6.3	117
6.5	Addendum: Notes and Open Questions	120
7	On Pseudorandom Generators with Linear Stretch in \mathbf{NC}^0	123
7.1	Introduction	123
7.1.1	Our Contribution	124
7.1.2	Related Work	125
7.2	Preliminaries	126
7.2.1	Some Useful Facts	126
7.3	LPRG in \mathbf{NC}^0 Implies Hardness of Approximation	127
7.4	A Construction of LPRG in \mathbf{NC}^0	129
7.4.1	Overview	129
7.4.2	The Assumption	130
7.4.3	The Construction	133
7.4.4	ε -Biased Generators in Uniform \mathbf{NC}^0	136
7.4.5	Alekhovich's Assumption Implies Assumption 7.1	139
7.5	The Necessity of Expansion	141
7.5.1	Results	141
7.5.2	Discussion	142
7.6	Addendum: Notes and Open Questions	144
7.6.1	Pseudorandomness of Random Local Functions	144
7.6.2	\mathbf{NC}^0 Randomness Extractors and \mathbf{NC}^0 Sources	145
8	Cryptography with Constant Input Locality	147
8.1	Introduction	147
8.1.1	Results	148
8.1.2	Our Techniques	149
8.1.3	Previous Work	150
8.2	Preliminaries	151
8.2.1	Cryptographic Primitives	151
8.2.2	Extractors	153
8.3	Randomized Encoding with Constant Input Locality	153
8.3.1	Key Lemmas	153
8.3.2	Main Results	155
8.4	Primitives with Constant Input Locality and Output Locality	158
8.4.1	Main Assumption: Intractability of Decoding Random Linear Code	158
8.4.2	Pseudorandom Generator in \mathbf{Local}_3^3	161
8.4.3	Symmetric Encryption	163
8.4.4	Commitment in \mathbf{Local}_3^4	164
8.4.5	Semantically Secure Public-Key Encryption in $\mathbf{Local}_3^{O(1)}$	166
8.4.6	Locality-Preserving Reductions Between Different Primitives	168

8.5	Negative Results for Cryptographic Primitives	171
8.5.1	Basic Observations	171
8.5.2	MACs and Signatures	173
8.5.3	Non-malleable Encryption	175
8.5.4	The Impossibility of Implementing a PRG in Local ₂ . . .	176
8.6	Negative Results for Randomized Encodings	178
8.6.1	A Necessary Condition for Encoding with Low Input Locality	178
8.6.2	Impossibility of Universal Encoding for Linear Functions	182
8.7	Conclusions and Open Questions	183
8.8	Addendum: Cryptography with Physical Locality	183
References	187



<http://www.springer.com/978-3-642-17366-0>

Cryptography in Constant Parallel Time

Applebaum, B.

2014, XVI, 193 p. 3 illus., Hardcover

ISBN: 978-3-642-17366-0