1. Record Nr. UNINA9910860804003321

Autore	Garg Sanjam
Titolo	Candidate Multilinear Maps
Pubbl/distr/stampa	San Rafael : , : Morgan & Claypool Publishers, , 2015 ©2015
ISBN	1-62705-537-1
Edizione	[1st ed.]
Descrizione fisica	1 online resource (125 pages)
Collana	ACM Bks.
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Contents -- Preface -- 1. Introduction -- Our Results -- Brief Overview -- Organization -- 2. Survey of Applications -- How Flexible Can We Make Access to Encrypted Data? -- Program Obfuscation -- Other Applications -- 3. Multilinear Maps and Graded Encoding Systems -- Cryptographic Multilinear Maps -- Graded Encoding Schemes -- 4. Preliminaries I: Lattices -- Lattices -- Gaussians on Lattices -- Sampling from Discrete Gaussian -- 5. Preliminaries II: Algebraic Number Theory Background -- Number Fields and Rings of Integers -- Embeddings and Geometry -- Ideals in the Ring of Integers -- Prime Ideals-Unique Factorization and Distributions -- Ideal Lattices -- 6. The New EncodingSchemes -- The Basic Graded Encoding Scheme -- Setting the Parameters -- Extensions and Variants -- 7. Security of OurConstructions -- Our Hardness Assumption -- Simplistic Models of Attacks -- Cryptanalysis Beyond the Generic Models -- Some Countermeasures -- Easiness of Other Problems -- 8. Preliminaries III: Computation in a Number Field -- Some Computational Aspects of Number Fields and Ideal Lattices -- Computational Hardness Assumptions over Number Fields -- 9. Survey of LatticeCryptanalysis -- Averaging Attacks -- Gentry-Szydlo: Recovering v from v . v and v -- Nguyen-Regev: A Gradient Descent Attack -- Ducas-Nguyen: Gradient Descent over Zonotopes and Deformed Parallelepipeds -- A New Algorithm for the Closest Principal Ideal Generator Problem --

Coppersmith Attacks -- Dimension Halving in Principal Ideal Lattices -- 10 One-Round Key Exchange -- Definitions -- Our Construction -- A. Generalizing Graded Encoding Systems -- Efficient Procedures-The Dream Version -- Efficient Procedures-The Real-Life Version -- Hardness Assumptions -- Bibliography -- Author's Biography.

Sommario/riassunto

Cryptography to me is the "black magic," of cryptographers, enabling tasks that often seem paradoxical or simply just impossible. Like the space explorers, we cryptographers often wonder, "what are the boundaries of this world of black magic?" This work lays one of the founding stones in furthering our understanding of these edges. We describe plausible lattice-based constructions with properties that approximate the sought after multilinear maps in hard-discrete-logarithm groups. The security of our constructions relies on seemingly hard problems in ideal lattices, which can be viewed as extensions of the assumed hardness of the NTRU function. These new constructions radically enhance our tool set and open a floodgate of applications. We present a survey of these applications. This book is based on my PhD thesis which was an extended version of a paper titled "Candidate Multilinear Maps from Ideal Lattices" co-authored with Craig Gentry and Shai Halevi. This paper was originally published at EUROCRYPT 2013. The aim of cryptography is to design primitives and protocols that withstand adversarial behavior. Information theoretic cryptography, how-so-ever desirable, is extremely restrictive and most non-trivial cryptographic tasks are known to be information theoretically impossible. In order to realize sophisticated cryptographic primitives, we forgo information theoretic security and assume limitations on what can be efficiently computed. In other words we attempt to build secure systems conditioned on some computational intractability assumption such as factoring, discrete log, decisional Diffie-Hellman, learning with errors, and many more. In this work, based on the 2013 ACM Doctoral Dissertation Award-winning thesis, we put forth new plausible lattice-based constructions with properties that approximate the sought after multilinear maps. The
multilinear analog of the decision Diffie-Hellman problem appears to be hard in our construction, and this allows for their use in cryptography. These constructions open doors to providing solutions to a number of important open problems.