Steven D. Galbraith (Ed.)

LNCS 4887

Cryptography and Coding

11th IMA International Conference
Cirencester, UK, December 2007
Proceedings

Springer

Steven D. Galbraith (Ed.)

Cryptography and Coding

11th IMA International Conference
Cirencester, UK, December 18-20, 2007
Proceedings

Springer

Volume Editor

Steven D. Galbraith
Royal Holloway University of London
Mathematics Department
Egham, Surrey, TW20 0EX, UK
E-mail: steven.galbraith@rhul.ac.uk

Library of Congress Control Number: 2007940956

CR Subject Classification (1998): E.3-4, G.2.1, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-77271-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-77271-2 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12203093 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4887

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Preface

The 11th IMA Conference on Cryptography and Coding was held at the Royal Agricultural College, Cirencester, UK during December 18–20, 2007. As usual, the venue provided a relaxed and convivial atmosphere for attendees to enjoy the conference programme and discuss current and future research ideas.

The programme comprised three invited talks and 22 contributed papers. The invited speakers were Jonathan Katz (University of Maryland, USA), Patrick Solé (Ecole Polytechnique de l'Université de Nice-Sophia Antipolis, France) and Whit Diffie (Sun Microsystems, USA). Special thanks are due to these speakers. Two of the invited speakers provided papers, included in this volume, which highlight the connections between cryptography, coding theory and discrete mathematics.

The contributed talks were selected from 48 submissions. The accepted papers cover a range of topics in mathematics and computer science, including symmetric and public key cryptography, Boolean functions, sequences, efficient implementation and side-channel analysis.

I would like to thank all the people who helped with the conference programme and organization. First, I thank the Steering Committee for their guidance on the general format of the conference and for suggestions of members of the Programme Committee. I also heartily thank the Programme Committee and the sub-reviewers listed on the following pages for their thoroughness during the review process. Each paper was reviewed by at least three people. There was significant online discussion about a number of papers.

The submission and review process was greatly simplified by the ichair software developed by Thomas Baignères and Matthieu Finiasz. Thanks also to Jon Hart for running the submissions Web server and Sriram Srinivasan for designing and maintaining the conference Web page.

Thanks go to the authors of all submitted papers. I also thank the authors of accepted papers for revising their papers according to referee suggestions and returning latex source files in good time. The revised versions were not checked by the Programme Committee so authors bear full responsibility for their contents. I thank the staff at Springer for their help with producing the proceedings.

I thank Hewlett-Packard and Vodafone for their sponsorship of this event.

Finally, I wish to thank the conference staff of the Institute for Mathematics and its Applications, especially Lucy Nye and Sammi Lauesen, for their help with running the conference and handling the finances.

October 2007 Steven Galbraith

Cryptography and Coding 2007

Royal Agricultural College, Cirencester, UK
December 18–20, 2007

Sponsored by
The Institute of Mathematics and its Applications

in cooperation with
Hewlett-Packard Laboratories and *Vodafone Ltd.*

Programme Chair

Steven Galbraith	Royal Holloway University of London

Steering Committee

Bahram Honary	Lancaster University
Chris Mitchell	Royal Holloway
Kenny Paterson	Royal Holloway
Fred Piper	Royal Holloway
Nigel Smart	University of Bristol
Mike Walker	Vodafone Ltd. and Royal Holloway

Programme Committee

Steve Babbage	Vodafone Group Services Ltd.
Nigel Boston	South Carolina/Wisconsin
Pascale Charpin	INRIA Rocquencourt
Liqun Chen	Hewlett-Packard
Carlos Cid	Royal Holloway
YoungJu Choie	Postech, Korea
Arjen Lenstra	EPFL, Lausanne
Alexander May	Ruhr Universität Bochum
Gary McGuire	University College Dublin
Alfred Menezes	University of Waterloo
David Naccache	Ecole Normale Supérieure
Matthew Parker	University of Bergen
Matt Robshaw	France Telecom
Ana Sălăgean	Loughborough University
Berry Schoenmakers	Technical University Eindhoven
Michael Scott	Dublin City University
Amin Shokrollahi	EPFL, Lausanne
Nigel Smart	University of Bristol
Frederik Vercauteren	K. U. Leuven
Gilles Zemor	Université Bordeaux

External Reviewers

Joppe Bos
Christophe De Cannière
Anne Canteaut
Claude Carlet
Mahdi Cheraghchi
Alex Dent
Fabien Galand
Philippe Guillot
Darrel Hankerson
Marcelo Kaihara
Cedric Lauradoux
Lorenz Minder
Marine Minier
Stephane Manuel
Ashley Montanaro
Sean Murphy
Dag Arne Osvik
Gregory Neven
Dan Page
Kenny Paterson
Benny Pinkas
Louis Salvail
Amin Shokrollahi
Andrey Sidorenko
Patrick Solé
Martijn Stam
Søren Steffen Thomsen
Eran Tromer
José Villegas

Lecture Notes in Computer Science

Sublibrary 4: Security and Cryptology

Vol. 4887: S.D. Galbraith (Ed.), Cryptography and Coding. XI, 423 pages. 2007.

Vol. 4861: S. Qing, H. Imai, G. Wang (Eds.), Information and Communications Security. XIV, 508 pages. 2007.

Vol. 4859: K. Srinathan, C.P. Rangan, M. Yung (Eds.), Progress in Cryptology – INDOCRYPT 2007. XI, 426 pages. 2007.

Vol. 4856: F. Bao, S. Ling, T. Okamoto, H. Wang, C. Xing (Eds.), Cryptology and Network Security. XII, 283 pages. 2007.

Vol. 4833: K. Kurosawa (Ed.), Advances in Cryptology – ASIACRYPT 2007. XIV, 583 pages. 2007.

Vol. 4817: K.-H. Nam, G. Rhee (Eds.), Information Security and Cryptology - ICISC 2007. XIII, 367 pages. 2007.

Vol. 4812: P. McDaniel, S.K. Gupta (Eds.), Information Systems Security. XIII, 322 pages. 2007.

Vol. 4784: W. Susilo, J.K. Liu, Y. Mu (Eds.), Provable Security. X, 237 pages. 2007.

Vol. 4779: J.A. Garay, A.K. Lenstra, M. Mambo, R. Peralta (Eds.), Information Security. XIII, 437 pages. 2007.

Vol. 4776: N. Borisov, P. Golle (Eds.), Privacy Enhancing Technologies. X, 273 pages. 2007.

Vol. 4752: A. Miyaji, H. Kikuchi, K. Rannenberg (Eds.), Advances in Information and Computer Security. XIII, 460 pages. 2007.

Vol. 4734: J. Biskup, J. López (Eds.), Computer Security – ESORICS 2007. XIV, 628 pages. 2007.

Vol. 4727: P. Paillier, I. Verbauwhede (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2007. XIV, 468 pages. 2007.

Vol. 4691: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. VIII, 285 pages. 2007.

Vol. 4677: A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design IV. VII, 325 pages. 2007.

Vol. 4657: C. Lambrinoudakis, G. Pernul, A.M. Tjoa (Eds.), Trust, Privacy and Security in Digital Business. XIII, 291 pages. 2007.

Vol. 4637: C. Kruegel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.

Vol. 4631: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 347 pages. 2007.

Vol. 4622: A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007. XIV, 631 pages. 2007.

Vol. 4593: A. Biryukov (Ed.), Fast Software Encryption. XI, 467 pages. 2007.

Vol. 4586: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), Information Security and Privacy. XIV, 476 pages. 2007.

Vol. 4582: J. López, P. Samarati, J.L. Ferrer (Eds.), Public Key Infrastructure. XI, 375 pages. 2007.

Vol. 4579: B.M. Hämmerli, R. Sommer (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment. X, 251 pages. 2007.

Vol. 4575: T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (Eds.), Pairing-Based Cryptography – Pairing 2007. XI, 408 pages. 2007.

Vol. 4521: J. Katz, M. Yung (Eds.), Applied Cryptography and Network Security. XIII, 498 pages. 2007.

Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.

Vol. 4499: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security II. IX, 117 pages. 2007.

Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.

Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.

Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.

Vol. 4437: J.L. Camenisch, C.S. Collberg, N.F. Johnson, P. Sallee (Eds.), Information Hiding. VIII, 389 pages. 2007.

Vol. 4392: S.P. Vadhan (Ed.), Theory of Cryptography. XI, 595 pages. 2007.

Vol. 4377: M. Abe (Ed.), Topics in Cryptology – CT-RSA 2007. XI, 403 pages. 2006.

Vol. 4356: E. Biham, A.M. Youssef (Eds.), Selected Areas in Cryptography. XI, 395 pages. 2007.

Vol. 4341: P.Q. Nguyên (Ed.), Progress in Cryptology - VIETCRYPT 2006. XI, 385 pages. 2006.

Vol. 4332: A. Bagchi, V. Atluri (Eds.), Information Systems Security. XV, 382 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4298: J.K. Lee, O. Yi, M. Yung (Eds.), Information Security Applications. XIV, 406 pages. 2007.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S.-i. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4258: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies. VIII, 431 pages. 2006.

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4237: H. Leitold, E.P. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.

Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.

Vol. 4219: D. Zamboni, C. Krügel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security – ESORICS 2006. XI, 548 pages. 2006.

Vol. 4176: S.K. Katsikas, J. López, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - CRYPTO 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4107: G. Di Crescenzo, A. Rubin (Eds.), Financial Cryptography and Data Security. XI, 327 pages. 2006.

Vol. 4083: S. Fischer-Hübner, S. Furnell, C. Lambrinoudakis (Eds.), Trust and Privacy in Digital Business. XIII, 243 pages. 2006.

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4047: M.J.B. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages. 2006.

Vol. 3989: J. Zhou, M. Yung, F. Bao (Eds.), Applied Cryptography and Network Security. XIV, 488 pages. 2006.

Vol. 3969: Ø. Ytrehus (Ed.), Coding and Cryptography. XI, 443 pages. 2006.

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T.G. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 pages. 2006.

Vol. 3957: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 325 pages. 2006.

Vol. 3956: G. Barthe, B. Grégoire, M. Huisman, J.-L. Lanet (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 175 pages. 2006.

Vol. 3935: D.H. Won, S. Kim (Eds.), Information Security and Cryptology - ICISC 2005. XIV, 458 pages. 2006.

Vol. 3934: J.A. Clark, R.F. Paige, F.A.C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3919: R. Safavi-Naini, M. Yung (Eds.), Digital Rights Management. XI, 357 pages. 2006.

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3856: G. Danezis, D. Martin (Eds.), Privacy Enhancing Technologies. VIII, 273 pages. 2006.

Vol. 3786: J.-S. Song, T. Kwon, M. Yung (Eds.), Information Security Applications. XI, 378 pages. 2006.

Vol. 3108: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), Information Security and Privacy. XII, 494 pages. 2004.

Vol. 2951: M. Naor (Ed.), Theory of Cryptography. XI, 523 pages. 2004.

Vol. 2742: R.N. Wright (Ed.), Financial Cryptography. VIII, 321 pages. 2003.

¥495.00元

Table of Contents

Invited Papers

Signatures I

Boolean Functions

Block Cipher Cryptanalysis

Side Channels

Linear Complexity

Public Key Encryption

Curves

RSA Implementation

Signatures II

Efficient Cryptographic Protocols Based on the Hardness of Learning Parity with Noise

Jonathan Katz*

Dept. of Computer Science
University of Maryland
jkatz@cs.umd.edu

Abstract. The problem of *learning parity with noise* (The LPN problem), which can be re-cast as the problem of decoding a random linear code, has attracted attention recently as a possible tool for developing highly-efficient cryptographic primitives suitable for resource-constrained devices such as RFID tags. This article surveys recent work aimed at designing efficient authentication protocols based on the conjectured hardness of this problem.

1 Introduction

1.1 The LPN Problem

Fix a binary vector (i.e., a bit-string) $\mathbf{s}$ of length k. Given a sequence of randomly-chosen binary vectors $\mathbf{a}_1, \ldots, \mathbf{a}_\ell$ along with the values of their inner-product $z_i = \langle \mathbf{s}, \mathbf{a}_i \rangle$ with $\mathbf{s}$, it is a simple matter to reconstruct $\mathbf{s}$ in its entirety as soon as ℓ is slightly larger than k. (All that is needed is to wait until the set $\{\mathbf{a}_i\}$ contains k linearly-independent vectors.) In the presence of *noise*, however, where each bit z_i is flipped (independently) with probability ε, determining $\mathbf{s}$ becomes much more difficult. We refer to the problem of learning $\mathbf{s}$ in this latter case as the problem of learning parity with noise, or *the LPN problem*.

Formally, let Ber_ε be the Bernoulli distribution with parameter $\varepsilon \in (0, \frac{1}{2})$ (so if $\nu \sim \mathsf{Ber}_\varepsilon$ then $\Pr[\nu = 1] = \varepsilon$ and $\Pr[\nu = 0] = 1 - \varepsilon$), and let $A_{\mathbf{s},\varepsilon}$ be the distribution defined by:

$$\left\{\mathbf{a} \leftarrow \{0,1\}^k; \nu \leftarrow \mathsf{Ber}_\varepsilon : (\mathbf{a}, \langle \mathbf{s}, \mathbf{a} \rangle \oplus \nu)\right\}.$$

Let $A_{\mathbf{s},\varepsilon}$ also denote an oracle which outputs (independent) samples according to this distribution. Algorithm M is said to (t, q, δ)*-solve the* LPN_ε *problem* if

$$\Pr\left[\mathbf{s} \leftarrow \{0,1\}^k : M^{A_{\mathbf{s},\varepsilon}}(1^k) = \mathbf{s}\right] \geq \delta,$$

and furthermore M runs in time at most t and makes at most q queries to its oracle. (This formulation of the LPN problem follows [18]; an alternative but

* Supported in part by NSF CyberTrust grant #0627306 and NSF CAREER award #0447075.

S.D. Galbraith (Eds.): Cryptography and Coding 2007, LNCS 4887, pp. 1–15, 2007.

essentially equivalent formulation allows M to output any $\mathbf{s}$ satisfying at least a $(1-\varepsilon)$ fraction of the equations returned by $A_{\mathbf{s},\varepsilon}$.) In asymptotic terms, the LPN_ε problem is "hard" if every probabilistic polynomial-time algorithm M solves the LPN_ε problem with only negligible probability (where the algorithm's running time and success probability are functions of k).

Note that ε is usually taken to be a fixed constant independent of k, as we will assume here. The value of ε to use depends on a number of tradeoffs and design decisions: although, roughly speaking, the LPN_ε problem becomes "harder" as ε increases, a larger value of ε also affects the error rate (for honest parties) in schemes based on the LPN problem; this will becomes more clear in the sections that follow. For concreteness, the reader can think of $\varepsilon \approx \frac{1}{8}$.

The hardness of the LPN_ε problem, for any constant $\varepsilon \in (0, \frac{1}{2})$, has been studied in many previous works. It can be formulated also as the problem of decoding a random linear code, and is known to be $\mathcal{NP}$-complete [2] as well as hard to approximate within a factor better than 2 (where the optimization problem is phrased as finding an $\mathbf{s}$ satisfying the most equations) [12]. These worst-case hardness results are complemented by numerous studies of the average-case hardness of the problem [3,4,6,20,13,14,24]. Currently, the best algorithms for solving the LPN_ε problem [4,9,23] require $t, q = 2^{\Theta(k/\log k)}$ to achieve $\delta = \mathcal{O}(1)$. We refer the reader to [23] for additional heuristic improvements, as well as a tabulation of the time required to solve the LPN_ε problem (for various settings of the parameters) using the best-known algorithm.

The LPN problem can be generalized to fields other than $\mathbb{F}_2$ (or even other algebraic structures such as rings), and these generalizations have interesting cryptographic consequences also [24]. Such extensions will not be discussed here.

1.2 Cryptographic Applications of the LPN Problem

It is not too difficult to see that hardness of the LPN_ε problem implies the existence of a one-way function. More interesting is that such hardness would imply *efficient* and *direct* constructions of pseudorandom generators [3,24]; see Lemma 1 for an indication of the basic underlying ideas. Furthermore, generating an instance of the distribution $A_{\mathbf{s},\varepsilon}$ is extremely "cheap", requiring only k bit-wise "AND" operations and $k - 1$ "XOR" operations.[1] Finally, as mentioned earlier, the best-known algorithms for solving the LPN_ε problem are only slightly sub-exponential in the length k of the hidden vector. Taken together, these observations suggest the possibility of using the LPN_ε problem to construct efficient cryptographic primitives and protocols, as first suggested in [3].

Actually, if the LPN_ε problem is indeed "hard" enough, there is the potential of using it to construct *extremely* efficient cryptographic primitives, suitable either for implementation by humans (using pencil-and-paper) [13,14] or for implementation on low-cost radio-frequency identification (RFID) tags [17] or sensor nodes. Focusing on the case of RFID tags, Juels and Weis [17,25] estimate

[1] This assumes that generating the appropriate random coins is "free", which may not be a reasonable assumption in practice.

that current RFID tags contain, in the best case, $\approx$ 2000 gate equivalents that can be dedicated to performing security functions; even optimized block cipher implementations may require many more gates than this (see [8,1] for current state-of-the-art).

1.3 Efficient Authentication Based on the LPN Problem

In the remainder of this work, we survey recent work directed toward developing authentication protocols based on the LPN problem; these protocols have been suggested as suitable for the secure identification of RFID tags. All protocols we will consider are intended for the shared-key (i.e., symmetric-key) setting, and provide unidirectional authentication only; typically, this would permit an RFID tag, acting as a *prover*, to authenticate itself to a tag reader acting as a *verifier*. We begin with a brief outline of the history of the developments, and defer all technical details to the sections that follow.

The first protocol we will present — following [17], we will refer to it as the *HB protocol* — was introduced by Hopper and Blum [13,14] and provides security against a passive (eavesdropping) adversary. Juels and Weis [17,25] were the first to rigorously prove security of the HB protocol, and to suggest its use for RFID authentication. (Hopper and Blum proposed it as a way to authenticate humans using pencil-and-paper only.) Juels and Weis also proposed a second protocol, called HB$^+$, that could be proven secure against an active attacker who can impersonate the tag reader to an RFID tag. In each case, Juels and Weis focus on a single, "basic authentication step" of the protocol and prove that a computationally-bounded adversary cannot succeed in impersonating a tag in this case with probability noticeably better than 1/2; that is, a single iteration of the protocol has *soundness error* 1/2. The implicit assumption is that repeating these "basic authentication steps" sufficiently-many times yields a protocol with negligible soundness error, though this intuition was not formally proven by Juels and Weis.

Two papers of my own [18,19] (along with Ji-Sun Shin and Adam Smith) provide a simpler and improved analysis of the HB and HB$^+$ protocols. Besides giving what is arguably a cleaner framework for analyzing the security of these protocols, the proofs in these works also yield the following concrete improvements: (1) they show that the HB$^+$protocol remains secure under arbitrary concurrent executions of the protocol; this, in particular, means that the HB$^+$ protocol can be *parallelized* so as to run in 3 rounds (regardless of the desired soundness error); (2) the proofs explicitly incorporate the dependence of the soundness error on the number of iterations of a "basic authentication step"; and (3) the proofs deal with the inherent error probability in even honest executions of the protocol. (The reader is referred to [18] for further detailed discussion of these points.) The initial work [18] was limited to the case of $\varepsilon < 1/4$; subsequent work [19] extended these results to the case of arbitrary $\varepsilon < 1/2$.

In work tangential to the above, Gilbert et al. [10] show that the HB$^+$ protocol is not secure against a man-in-the-middle attack, in the sense that a man-in-the-middle attacker is able to reconstruct the entire secret key of the RFID tag after sufficiently-many interactions. (The reader is additionally referred to the work of Wool et al. [21,22], for an illuminating discussion on the feasibility of man-in-the-middle attacks in RFID systems.) This has motivated numerous proposals (e.g., [5]) of HB-variants that are claimed to be secure against the specific attack of Gilbert et al., but I am not aware of any HB-variant that is provably-secure against *all* man-in-the-middle attacks. To my mind, the existence of a man-in-the-middle attack on the HB$^+$ protocol shows that the protocol must be used with care, but does not rule out its usefulness; specifically, I view the aim of the line of research considered here to be the development of protocols which are *exceptionally* efficient while still guaranteeing *some* useful level of (provable) security. The possibility of man-in-the-middle attacks does *not* mean that it is useless to explore the security of authentication protocols in weaker attack models. Furthermore, as a practical matter, Juels and Weis [17, Appendix A] note that the man-in-the-middle attack of [10] does not apply in a *detection-based* system where numerous failed authentication attempts immediately raise an alarm. Nevertheless, the design of an HB-variant with provable security against man-in-the-middle attacks remains an interesting open problem.

1.4 Overview of This Paper

The remainder of this paper is devoted to a description of the HB and HB$^+$ protocols, as well as the technical proofs of security for these protocols (adapted from [18,19]). It is not the goal of this paper to replace [18,19]; instead, the main motivation is to give a high-level treatment of the proofs with a focus on those aspects that might be of greatest interest to coding-theorists. Proof steps that are "technical" but otherwise uninteresting will be glossed over, and some proofs are omitted entirely. The interested reader can find full details of all proofs in [18,19].

2 Definitions and Preliminaries

We have already formally defined the LPN problem in the Introduction. Here, we state and prove the main technical lemma on which we will rely. We also define notion(s) of security for identification; these are standard, but some complications arise due to the fact that the HB/HB$^+$ protocols do not have perfect completeness.

2.1 A Technical Lemma

In this section we prove a key technical lemma due to Regev [24, Sect. 4] (though without the explicit dependence on the parameters given below, which is taken from [18]): hardness of the LPN_ε problem implies "pseudorandomness" of $A_{\mathbf{s},\varepsilon}$. Specifically, let U_{k+1} denote the uniform distribution on $(k+1)$-bit strings. The following lemma shows that oracle access to $A_{\mathbf{s},\varepsilon}$ (for randomly-chosen $\mathbf{s}$) is indistinguishable from oracle access to U_{k+1}.

Lemma 1. *Say there exists an algorithm D making q oracle queries, running in time t, and such that*

$$\left|\Pr\left[\mathbf{s} \leftarrow \{0,1\}^k : D^{A_{\mathbf{s},\varepsilon}}(1^k) = 1\right] - \Pr\left[D^{U_{k+1}}(1^k) = 1\right]\right| \geq \delta.$$

Then there exists an algorithm M making $q' = O\left(q \cdot \delta^{-2} \log k\right)$ oracle queries, running in time $t' = O\left(t \cdot k\delta^{-2} \log k\right)$, and such that

$$\Pr\left[\mathbf{s} \leftarrow \{0,1\}^k : M^{A_{\mathbf{s},\varepsilon}}(1^k) = \mathbf{s}\right] \geq \delta/4.$$

(Various tradeoffs are possible between the number of queries/running time of M and its success probability in solving LPN_ε; see [24, Sect. 4]. We do not discuss these here.)

Proof (Sketch). Algorithm $M^{A_{\mathbf{s},\varepsilon}}(1^k)$ proceeds as follows:

1. Fix random coins for D.
2. Estimate the probability that D outputs 1 when it interacts with oracle U_{k+1}. Call this estimate p.
3. For $i \in [k]$ do:
   (a) Estimate the probability that D outputs 1 when it interacts with an oracle implementing the following distribution:

   $$\mathsf{hyb}_i \stackrel{\text{def}}{=} \left\{\mathbf{a} \leftarrow \{0,1\}^k; c \leftarrow \{0,1\}; \nu \leftarrow \mathsf{Ber}_\varepsilon : (\mathbf{a} \oplus (c \cdot \mathbf{e}_i), \langle \mathbf{s}, \mathbf{a} \rangle \oplus \nu)\right\},$$

   where $\mathbf{e}_i$ is the vector with 1 at position i and 0s elsewhere. Note that M can generate this distribution using its own access to oracle $A_{\mathbf{s},\varepsilon}$. Call the estimate obtained in this step p_i.

   (b) If $|p_i - p| \geq \delta/4$ set $s'_i = 0$; else set $s'_i = 1$.
4. Output $\mathbf{s}' = (s'_1, \ldots, s'_k)$.

Let us analyze the behavior of M. First, note that with "high" probability over choice of $\mathbf{s}$ and random coins for D it holds that

$$\left|\Pr\left[D^{A_{\mathbf{s},\varepsilon}}(1^k) = 1\right] - \Pr\left[D^{U_{k+1}}(1^k) = 1\right]\right| \geq \delta/2, \tag{1}$$

where the probabilities are now taken only over the answers D receives from its oracle. We restrict our attention to $\mathbf{s}, \omega$ for which Eq. (1) holds and show that in this case M outputs $\mathbf{s}' = \mathbf{s}$ with probability at least 1/2. The lemma follows.

Setting the accuracy of our estimations appropriately, we can ensure that

$$\left|\Pr\left[D^{U_{k+1}}(1^k; \omega) = 1\right] - p\right| \leq \delta/16 \tag{2}$$

except with probability at most $O(1/k)$. Now focus on a particular iteration i of steps 3(a) and 3(b). We may once again ensure that

$$\left|\Pr\left[D^{\mathsf{hyb}_i}(1^k; \omega) = 1\right] - p_i\right| \leq \delta/16 \tag{3}$$

except with probability at most $O(1/k)$. Applying a union bound (and setting parameters appropriately) we see that with probability at least 1/2 both Eqs. (2)