



International InfoSecurity Updates

[illegible]

			46
AES	9	AES-128	48
			50
		MITM	52
Skein	ARX		54
			56
			58
			60
			62
			64
			66
			68
		N	70
			72
TLS			74
		PAKE	76
			78
			80
			82
			84
			86
			88
			90
SIS	LWE		92

				94
LWR				96
LWE				98
-				100
				102
2013	(I)				
		NIZK		104
				106
				108
Q-				110
Weil		GLV		112
		Lemmaover		114
		IP1S		116
				118
				120
				122
				124
SPHF				126
				128
				130
				132
				134
				136
3	Even-Mansour	8	LED-128	AES ² 138

	140
ALE	142
	144
	146
	148
Feistel	150
	152
	154
SPN	SCARE	156
	158
Fiat–Shamir	160
	162

Candidate Multilinear Maps from Ideal Lattices

Sanjam Garg¹, Craig Gentry², and Shai Halevi²

¹ UCLA

² IBM Research

Abstract. We describe plausible lattice-based constructions with properties that approximate the sought-after multilinear maps in hard discrete-logarithm groups, and show an example application of such multi-linear maps that can be realized using our approximation. 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.

Source: EUROCRYPT 2013, LNCS, Vol. 7881, Springer, Heidelberg (2013)

Lossy Codes and a New Variant of the Learning-With-Errors Problem

Nico Dottling and Jorn Muller-Quade
Karlsruhe Institute of Technology, Karlsruhe, Germany
{doettling,mueller-quade}@kit.edu

Abstract. The hardness of the Learning-With-Errors (LWE) Problem has become one of the most useful assumptions in cryptography. It exhibits a worst-to-average-case reduction making the LWE assumption very plausible. This worst-to-average-case reduction is based on a Fourier argument and the errors for current applications of LWE must be chosen from a gaussian distribution. However, sampling from gaussian distributions is cumbersome.

In this work we present the first worst-to-average case reduction for LWE with uniformly distributed errors, which *can* be sampled very efficiently. This new worst-to-average-case connection comes with a slight drawback and we need to use a bounded variant of the LWE problem, where the number of samples is fixed in advance. Most applications of LWE can be based on the bounded variant. The proof is based on a new tool called lossy codes, which might be of interest in the context other lattice/coding-based hardness assumptions.

Keywords: Learning-With-Errors, Worst-Case Reduction, Uniform Interval Error-Distribution

Source: EUROCRYPT 2013, LNCS, Vol. 7881, Springer, Heidelberg (2013)

LWE

LWE

worst to average-case

LWE

worst-to-average case

LWE

LWE worst-to-average

worst-to-average

LWE

LWE

LWE

A Toolkit for Ring-LWE Cryptography

Vadim Lyubashevsky¹, Chris Peikert², and Oded Regev³,

¹INRIA and École Normale Supérieure, Paris

²Georgia Institute of Technology

³Courant Institute, New York University

Abstract. Recent advances in lattice cryptography, mainly stemming from the development of ring-based primitives such as ring-LWE, have made it possible to design cryptographic schemes whose efficiency is competitive with that of more traditional number-theoretic ones, along with entirely new applications like fully homomorphic encryption. Unfortunately, realizing the full potential of ring-based cryptography has so far been hindered by a lack of practical algorithms and analytical tools for working in this context. As a result, most previous works have focused on very special classes of rings such as power-of-two cyclotomics, which significantly restricts the possible applications.

We bridge this gap by introducing a toolkit of fast, modular algorithms and analytical techniques that can be used in a wide variety of ring-based cryptographic applications, particularly those built around ring-LWE. Our techniques yield applications that work in arbitrary cyclotomic rings, with no loss in their underlying worst-case hardness guarantees, and very little loss in computational efficiency, relative to power-of-two cyclotomics. To demonstrate the toolkit’s applicability, we develop two illustrative applications: a public-key cryptosystem and a “somewhat homomorphic” symmetric encryption scheme. Both apply to arbitrary cyclotomics, have tight parameters, and very efficient implementations.

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

-LWE

Regularity of Lossy RSA on Subdomains and Its Applications

Mark Lewko¹, Adam O'Neill², and Adam Smith³

¹University of California, Los Angeles

mlewko@math.ucla.edu

²Boston University

amoneill@bu.edu

³Pennsylvania State University

asmith@cse.psu.edu

Abstract. We build on an approach of Kiltz et al. (CRYPTO '10) and bring new techniques to bear on the study of how “lossiness” of the RSA trapdoor permutation under the Φ -Hiding Assumption (Φ A) can be used to understand the security of classical RSA-based cryptographic systems. In particular, we show that, under Φ A, several questions or conjectures about the security of such systems can be reduced to bounds on the regularity (the distribution of the primitive e -th roots of unity mod N) of the “lossy” RSA map (where e divides $\phi(N)$). Specifically, this is the case for: (i) showing that large consecutive runs of the RSA input bits are simultaneously hardcore, (ii) showing the widely-deployed PKCS #1 v1.5 encryption is semantically secure, (iii) improving the security bounds of Kiltz et al. for RSA-OAEP. We prove several results on the regularity of the lossy RSA map using both classical techniques and recent estimates on Gauss sums over finite subgroups, thereby obtaining new results in the above applications. Our results deepen the connection between “combinatorial” properties of exponentiation in \mathbb{Z}_N and the security of RSA-based constructions.

Keywords: RSA encryption, PKCS#1v1.5, Lossy trapdoor functions, Φ -Hiding Assumption, Gauss sums

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

RSA

- Kiltz Φ - RSA
- (ΦA) RSA “
- ΦA
- ” RSA e divides $\varphi(N)$ e -th N
- i RSA
- (ii) PKCS#1v1.5 iii RSA-OAEP
- Kiltz
- RSA
- ZN “ ” RSA
- PKCS#1v1.5 Φ -

Efficient Cryptosystems from 2^k -th Power Residue Symbols

Marc Joye and Benoît Libert

Technicolor 975 avenue des Champs Blancs, 35576 Cesson-S'evign'e Cedex, France

/marc.joye,benoit.libert/@technicolor.com

Abstract. Goldwasser and Micali (1984) highlighted the importance of randomizing the plaintext for public-key encryption and introduced the notion of semantic security. They also realized a cryptosystem meeting this security notion under the standard complexity assumption of deciding quadratic residuosity modulo a composite number. The Goldwasser-Micali cryptosystem is simple and elegant but is quite wasteful in bandwidth when encrypting large messages. A number of works followed to address this issue and proposed various modifications.

This paper revisits the original Goldwasser-Micali cryptosystem using 2^k -th power residue symbols. The so-obtained cryptosystems appear as a very natural generalization for $k \geq 2$ (the case $k = 1$ corresponds exactly to the Goldwasser-Micali cryptosystem). Advantageously, they are efficient in both bandwidth and speed; in particular, they allow for fast decryption. Further, the cryptosystems described in this paper inherit the useful features of the original cryptosystem (like its homomorphic property) and are shown to be secure under a similar complexity assumption. As a prominent application, this paper describes the most efficient lossy trapdoor function based on quadratic residuosity.

Keywords: Public-key encryption, quadratic residuosity, Goldwasser-Micali cryptosystem,,homomorphic encryption, standard model

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

$$2^k$$

Goldwasser Micali 1984

Goldwasser-Micali

$$2k$$

Goldwasser-Micali

$$k \geq 2$$

$$k=1$$

Goldwasser-Micali

Goldwasser-Micali

Deterministic Public-Key Encryption for Adaptively Chosen Plaintext Distributions

Ananth Raghunathan¹, Gil Segev¹, and Salil Vadhan^{2,†}

¹ Computer Science Department

Stanford University, Stanford, CA 94305, USA

{ananthr,segev}@stanford.edu

² School of Engineering and Applied Sciences

& Center for Research on Computation and Society,

Harvard University, Cambridge, MA 02138, USA

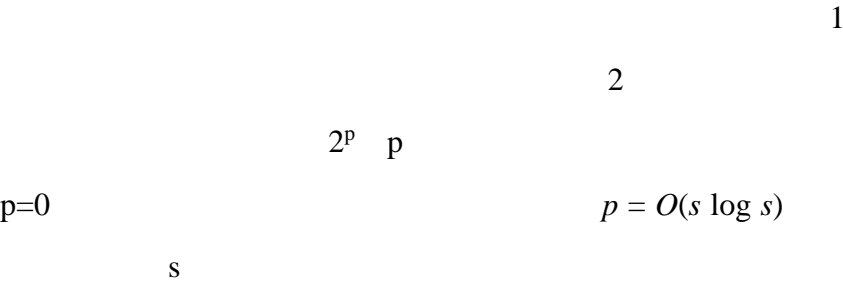
salil@seas.harvard.edu

Abstract. Bellare, Boldyreva, and O’Neill (CRYPTO ’07) initiated the study of deterministic public-key encryption as an alternative in scenarios where randomized encryption has inherent drawbacks. The resulting line of research has so far guaranteed security only for adversarially-chosen plaintext distributions that are independent of the public key used by the scheme. In most scenarios, however, it is typically not realistic to assume that adversaries do not take the public key into account when attacking a scheme.

We show that it is possible to guarantee meaningful security even for plaintext distributions that depend on the public key. We extend the previously proposed notions of security, allowing adversaries to adaptively choose plaintext distributions after seeing the public key, in an interactive manner. The only restrictions we make are that: (1) plaintext distributions are unpredictable (as is essential in deterministic public-key encryption), and (2) the number of plaintext distributions from which each adversary is allowed to adaptively choose is upper bounded by 2^p , where p can be any predetermined polynomial in the security parameter. For example, with $p = 0$ we capture plaintext distributions that are independent of the public key, and with $p = O(s \log s)$ we capture, in particular, all plaintext distributions that are samplable by circuits of size s .

Within our framework we present both constructions in the random oracle model based on any public-key encryption scheme, and constructions in the standard model based on lossy trapdoor functions (thus, based on a variety of number-theoretic assumptions). Previously known constructions heavily relied on the independence between the plaintext distributions and the public key for the purposes of randomness extraction. In our setting,

Bellare, Boldyreva O'Neill CRYPTO'07



Trevisan Vadhan

(FOCS '00) Dodis (PhD Thesis, MIT, '00)

How to Watermark Cryptographic Functions

Ryo Nishimaki

NTT Secure Platform Laboratories

nishimaki.ryo@lab.ntt.co.jp

Abstract. We propose a scheme for watermarking cryptographic functions. Informally speaking, a digital watermarking scheme for cryptographic functions embeds information, called a *mark*, into functions such as (trapdoor) one-way functions and decryption functions of public-key encryption. It is required that a mark-embedded function is functionally equivalent to the original function and it is difficult for adversaries to remove the embedded mark without damaging the function. In spite of its importance and usefulness, there have only been a few theoretical studies on watermarking for functions (or program), and we do not have rigorous and meaningful definitions of watermarking for cryptographic functions and concrete constructions.

To solve the above problem, we introduce a notion of watermarking for cryptographic functions and define its security. We present a lossy trapdoor function (LTF) based on the decisional linear (DLIN) problem and a watermarking scheme for the LTF. Our watermarking scheme is secure under the DLIN assumption in the standard model. We use the techniques of dual system encryption and dual pairing vector spaces (DPVS) to construct our watermarking scheme. This is a new application of DPVS.

Keywords: digital watermarking, dual pairing vector space, dual system encryption, vector decomposition problem

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

(DLIN)

(LTF)

DLIN

(DPVS)

DPVS

Security Evaluations beyond Computing Power

How to Analyze Side-Channel Attacks You Cannot Mount?

Nicolas Veyrat-Charvillon¹, Benoit Gerard², and François-Xavier Standaert¹

¹UCL Crypto Group, Université catholique de Louvain

Place du Levant 3, B-1348, Louvain-la-Neuve, Belgium

²Direction Generale de l'Armement–Maitrise de l'information, France

Abstract. Current key sizes for symmetric cryptography are usually required to be at least 80-bit long for short-term protection, and 128-bit long for long-term protection. However, current tools for security evaluations against side-channel attacks do not provide a precise estimation of the remaining key strength after some leakage has been observed, e.g. in terms of number of candidates to test. This leads to an uncomfortable situation, where the security of an implementation can be anywhere between enumerable values (i.e. 2^{10} – 2^{50} key candidates to test) and the full key size (i.e. 2^{60} – 2^{128} key candidates to test). In this paper, we propose a solution to this issue, and describe a key rank estimation algorithm that provides tight bounds for the security level of leaking cryptographic devices. As a result and for the first time, we are able to analyze the full complexity of “standard” (i.e. divide-and-conquer) side-channel attacks, in terms of their tradeoff between time, data and memory complexity.

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

80

128

$2^{10}-2^{50}$

$2^{60}-2^{128}$

Masking against Side-Channel Attacks: A Formal Security Proof

Emmanuel Prouff¹ and Matthieu Rivain²

¹ ANSSI

emmanuel.prouff@ssi.gouv.fr

² CryptoExperts

matthieu.rivain@cryptoexperts.com

Abstract. Masking is a well-known countermeasure to protect block cipher implementations against side-channel attacks. The principle is to randomly split every sensitive intermediate variable occurring in the computation into $d + 1$ shares, where d is called the masking order and plays the role of a security parameter. Although widely used in practice, masking is often considered as an empirical solution and its effectiveness is rarely proved. In this paper, we provide a formal security proof for masked implementations of block ciphers. Specifically, we prove that the information gained by observing the leakage from one execution can be made negligible (in the masking order). To obtain this bound, we assume that every elementary calculation in the implementation leaks a noisy function of its input, where the amount of noise can be chosen by the designer (yet linearly bounded). We further assume the existence of a leak-free component that can refresh the masks of shared variables. Our work can be viewed as an extension of the seminal work of Chari *et al.* published at CRYPTO in 1999 on the soundness of combining masking with noise to thwart side-channel attacks.

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

Leakage-Resilient Cryptography from Minimal Assumptions

Carmit Hazay¹, Adriana Lopez-Alt²,

Hoeteck Wee³, and Daniel Wichs⁴

¹ Bar-Ilan University

² New York University

³ George Washington University

⁴ Northeastern University

Abstract. We present new constructions of leakage-resilient cryptosystems, which remain provably secure even if the attacker learns some arbitrary partial information about their internal secret key. For any polynomial l , we can instantiate these schemes so as to tolerate up to l bits of leakage. While there has been much prior work constructing such leakage-resilient cryptosystems under concrete number-theoretic and algebraic assumptions, we present the first schemes under general and minimal assumptions. In particular, we construct:

- Leakage-resilient *public-key encryption* from any standard public-key encryption.
- Leakage-resilient *weak pseudorandom functions*, *symmetric-key encryption*, and *message-authentication codes* from any one-way function.

These are the first constructions of leakage-resilient symmetric-key primitives that do not rely on public-key assumptions. We also get the first constructions of leakage-resilient public-key encryption from search assumptions, such as the hardness of factoring or CDH. Although our schemes can tolerate arbitrarily large amounts of leakage, the tolerated rate of leakage (defined as the ratio of leakage-amount to key-size) is rather poor in comparison to prior results under specific assumptions.

As a building block of independent interest, we study a notion of *weak* hash-proof systems in the public-key and symmetric-key settings. While these inherit some of the interesting security properties of standard hashproof systems, we can instantiate them under general assumptions.

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)



l

l

—

—

CDH

Faster Index Calculus for the Medium Prime Case

Application to 1175-bit and 1425-bit Finite Fields

Antoine Joux

CryptoExperts and

Université de Versailles Saint-Quentin-en-Yvelines, Laboratoire PRISM,

45 avenue des États-Unis, F-78035 Versailles Cedex, France

antoine.joux@m4x.org

Abstract. Many index calculus algorithms generate multiplicative relations between smoothness basis elements by using a process called Sieving. This process allows us to quickly filter potential candidate relations, without spending too much time to consider bad candidates. However, from an asymptotic point of view, there is not much difference between sieving and straightforward testing of candidates. The reason is that even when sieving, some small amount of time is spent for each bad candidate. Thus, asymptotically, the total number of candidates contributes to the complexity.

In this paper, we introduce a new technique: Pinpointing, which allows us to construct multiplicative relations much faster, thus reducing the asymptotic complexity of relations' construction. Unfortunately, we only know how to implement this technique for finite fields which contain a medium-sized subfield. When applicable, this method improves the asymptotic complexity of the index calculus algorithm in the cases where the sieving phase dominates. In practice, it gives a very interesting boost to the performance of state-of-the-art algorithms. We illustrate the feasibility of the method with discrete logarithm records in two medium prime finite fields, the first of size 1175 bits and the second of size 1425 bits.

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

1175

1425

Fast Cryptography in Genus 2

Joppe W. Bos¹, Craig Costello¹, Huseyin Hisil², and Kristin Lauter¹

¹ Microsoft Research, Redmond, USA

² Yasar University, Izmir, Turkey

Abstract. In this paper we highlight the benefits of using genus 2 curves in public-key cryptography. Compared to the standardized genus 1 curves, or elliptic curves, arithmetic on genus 2 curves is typically more involved but allows us to work with moduli of half the size. We give a taxonomy of the best known techniques to realize genus 2 based cryptography, which includes fast formulas on the Kummer surface and efficient 4-dimensional GLV decompositions. By studying different modular arithmetic approaches on these curves, we present a range of genus 2 implementations. On a single core of an Intel Core i7-3520M (Ivy Bridge), our implementation on the Kummer surface breaks the 120 thousand cycle barrier which sets a new software speed record at the 128-bit security level for constant-time scalar multiplications compared to all previous genus 1 and genus 2 implementations.

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)



		2							
					2			1	
		2							
					2			Kummer	
		4	GLV						
		2		Intel		i7-3520M	Ivy Bridge		
				Kummer				120,000	
	1	2							
128									

Cryptanalysis of Full RIPEMD-128

Franck Landelle¹ and Thomas Peyrin²,

¹ DGA MI, France

²Division of Mathematical Sciences, School of Physical and Mathematical Sciences,

Nanyang Technological University, Singapore

landelle.franck@laposte.net, thomas.peyrin@gmail.com

Abstract. In this article we propose a new cryptanalysis method for double-branch hash functions that we apply on the standard RIPEMD-128, greatly improving over known results. Namely, we were able to build a very good differential path by placing one non-linear differential part in each computation branch of the RIPEMD-128 compression function, but not necessarily in the early steps. In order to handle the low differential probability induced by the non-linear part located in later steps, we propose a new method for using the freedom degrees, by attacking each branch separately and then merging them with free message blocks. Overall, we present the first collision attack on the full RIPEMD-128 compression function as well as the first distinguisher on the full RIPEMD-128 hash function. Experiments on reduced number of rounds were conducted, confirming our reasoning and complexity analysis. Our results show that 16 years old RIPEMD-128, one of the last unbroken primitives belonging to the MD-SHA family, might not be as secure as originally thought.

Keywords RIPEMD-128, collision, distinguisher, hash function

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

RIPEMD-128

RIPEMD-128

RIPEMD-128

RIPEMD-128

RIPEMD-128

MD-SHA

16

RIPEMD-128

RIPEMD-128

New Collision Attacks on SHA-1

Based on Optimal Joint Local-Collision Analysis

Marc Stevens

CWI, Amsterdam, The Netherlands

marc@marc-stevens.nl

Abstract. The main contributions of this paper are two-fold. Firstly, we present a novel direction in the cryptanalysis of the cryptographic hash function SHA-1. Our work builds on previous cryptanalytic efforts on SHA-1 based on combinations of local collisions. Due to dependencies, previous approaches used heuristic corrections when combining the success probabilities and message conditions of the individual local collisions. Although this leads to success probabilities that are seemingly sufficient for feasible collision attacks, this approach most often does not lead to the maximum success probability possible as desired. We introduce novel techniques that enable us to determine the theoretical maximum success probability for a given set of (dependent) local collisions, as well as the smallest set of message conditions that attains this probability. We apply our new techniques and present an implemented open-source near-collision attack on SHA-1 with a complexity equivalent to $2^{57.5}$ SHA-1 compressions.

Secondly, we present an identical-prefix collision attack and a chosen prefix collision attack on SHA-1 with complexities equivalent to approximately 2^{61} and $2^{77.1}$ SHA-1 compressions, respectively.

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

SHA-1

SHA-1

SHA-1

SHA-1

$2^{57.5}$ SHA-1

SHA-1

2^{61} $2^{77.1}$ SHA-1

Improving Local Collisions: New Attacks on Reduced SHA-256

Florian Mendel, Tomislav Nad, and Martin Schlaffer

IAIK, Graz University of Technology, Austria

florian.mendel@iaik.tugraz.at

Abstract. In this paper, we focus on the construction of semi-free-start collisions for SHA-256, and show how to turn them into collisions. We present a collision attack on 28 steps of the hash function with practical complexity. Using a two-block approach we are able to turn a semi free-start collision into a collision for 31 steps with a complexity of at most $2^{65.5}$. The main improvement of our work is to extend the size of the local collisions used in these attacks. To construct differential characteristics and confirming message pairs for longer local collisions, we had to improve the search strategy of our automated search tool. To test the limits of our techniques we present a semi-free-start collision for 38 steps.

Keywords: hash functions, SHA-2, cryptanalysis, collisions, semi-free-start collisions, differential characteristics, automatic search tool

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

SHA-256

SHA-256

28

$2^{65.5}$ 31

38

SHA-2

Dynamic Proofs of Retrievability via Oblivious RAM*

David Cash^{1,**}, Alptekin Küpçü^{2,***}, and Daniel Wichs^{3,†}

¹ Rutgers University

² Koç University

³ Northeastern University

Abstract. Proofs of retrievability allow a client to store her data on a remote server (e.g., “in the cloud”) and periodically execute an efficient audit protocol to check that all of the data is being maintained correctly and can be recovered from the server. For efficiency, the computation and communication of the server and client during an audit protocol should be significantly smaller than reading/transmitting the data in its entirety. Although the server is only asked to access a few locations of its storage during an audit, it must maintain full knowledge of all client data to be able to pass. Starting with the work of Juels and Kaliski (CCS ’07), all prior solutions require that the client data is static and do not allow it to be efficiently updated. Indeed, they store a redundant encoding of the data on the server, so that the server must delete a large fraction of its storage to ‘lose’ any actual content. Unfortunately, this means that even a single bit modification to the original data will need to modify a large fraction of the server storage, which makes updates highly inefficient.

In this work, we give the first solution providing proofs of retrievability for dynamic storage, where the client can perform arbitrary reads/writes on any location within her data by running an efficient protocol with the server. At any point in time, the client can also execute an audit protocol to ensure that the server maintains the latest version of its data. The computation and communication complexity of the server and client in our protocols is only polylogarithmic in the size of the data. Our main idea is to split up the data into small blocks and redundantly encode each block of data individually, so that an update inside any data block only affects a few codeword symbols. The main difficulty is to prevent the server from identifying and deleting too many codeword symbols belonging to any single data block. We do so by hiding where the various codeword symbols are stored on the server and when they are being accessed by the client, using the techniques of oblivious RAM.

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

RAM

“ ”

/

Juels Kaliski

CCS'07

‘ ’

/

RAM

Message-Locked Encryption and Secure Deduplication

Mihir Bellare¹, Sriram Keelveedhi¹, and Thomas Ristenpart²

¹ Department of Computer Science & Engineering, University of California San Diego

<http://cseweb.ucsd.edu/~mihir/>, <http://cseweb.ucsd.edu/~skeelvec/>

² Department of Computer Sciences, University of Wisconsin-Madison

<http://pages.cs.wisc.edu/~rist/>

Abstract. We formalize a new cryptographic primitive that we call Message-Locked Encryption (MLE), where the key under which encryption and decryption are performed is itself derived from the message. MLE provides a way to achieve secure deduplication (space-efficient secure outsourced storage), a goal currently targeted by numerous cloudstorage providers. We provide definitions both for privacy and for a form of integrity that we call tag consistency. Based on this foundation, we make both practical and theoretical contributions. On the practical side, we provide ROM security analyses of a natural family of MLE schemes that includes deployed schemes. On the theoretical side the challenge is standard model solutions, and we make connections with deterministic encryption, hash functions secure on correlated inputs and the sample-then-extract paradigm to deliver schemes under different assumptions and for different classes of message sources. Our work shows that MLE is a primitive of both practical and theoretical interest.

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

Keccak

Guido Bretoni¹, Joan Daemen¹, Michael Peeters¹, and Gilles Van Assche¹

¹ STMicroelectronics

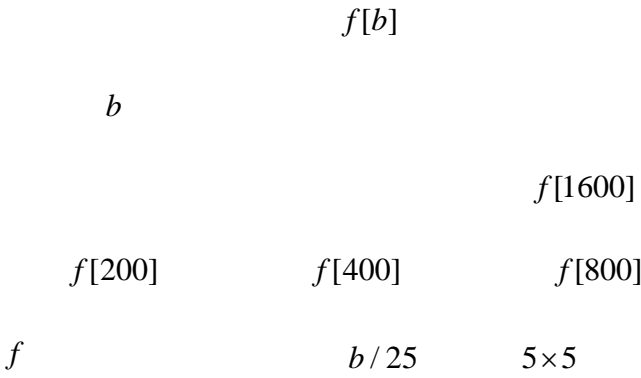
² NXP Semiconductors

Abstract. In October 2012, the American National Institute of Standards and Technology (NIST) announced the selection of Keccak as the winner of the SHA-3 Cryptographic Hash Algorithm Competition [10,11]. This concluded an open competition that was remarkable both for its magnitude and the involvement of the cryptographic community. Public review is of paramount importance to increase the confidence in the new standard and to favor its quick adoption. The SHA-3 competition explicitly took this into account by giving open access to the candidate algorithms and everyone in the cryptographic community could try to break them, compare their performance, or simply give comments. While preparing for the SHA-3 competition, we developed and presented the sponge construction [1]. Our initial goal of this effort was to solve the problem of compactly expressing a comprehensive security claim. It turned out to be a powerful tool for building a hash function and we adopted it for our SHA-3 candidate Keccak. Additionally, with its variable output length it can be used as a mask generating function, a stream cipher or a MAC computation function. To support more sophisticated modes such as single-pass authenticated encryption and reseenable pseudorandom sequence generation, we additionally introduced the duplex construction [3]. We have proven both sponge and duplex constructions sound in the indifferentiability framework [8,2,3]. Our permutation-based modes can be seen as an alternative to the block-cipher based modes that have dominated mainstream symmetric cryptography in the last decades. They are simpler than the traditional block cipher modes and other at the same time more flexibility by allowing to trade in security strength level for speed and vice versa. At the core of Keccak is a set of seven permutations called Keccak- $f[b]$, with width b chosen between 25 and 1600 by multiplicative steps of 2[4]. Depending on b , the resulting function ranges from a toy cipher to a wide function. The instances proposed for SHA-3 use exclusively Keccak- $f[1600]$ for all security levels[5], whereas lightweight alternatives can use for instance Keccak- $f[200]$ or

Keccak- $f[400]$, leaving Keccak- $f[800]$ as an intermediate choice[6]. Inside Keccak- f , the state to process is organized in 5×5 lanes of $b/25$ bits each, or alternatively as $b/25$ slices of 25 bits each. The round function processes the state using a non-linear layer of algebraic degree two (χ), a linear mixing layer (θ), inter- and intra-slice dispersion steps (ρ, π) and the addition of round constants (ι). The choice of operations in Keccak- f makes it very different from the SHA-2 family or even Rijndael (AES) [9,7]. On the implementation side, these operations are efficiently translated into bitwise Boolean operation and circular shifts, they lead to short critical paths in hardware implementations and they are well suited for protections against side-channel attacks.

Source: EUROCRYPT 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

SHA-3



$b/25$

(χ)

(θ)

(ρ, π)

(t)

f

Batch Fully Homomorphic Encryption over the Integers

Jung Hee Cheon¹, Jean-Sebastien Coron², Jinsu Kim¹, Moon Sung Lee¹,

Tancrede Lepoint^{3,4}, Mehdi Tibouchi⁵, and Aaram Yun⁶

¹ CryptoExperts Seoul National University(SNU), Republic of Korea, {jhcheon, kjs2002, moolee}@snu.ac.kr

² Tranef, France, jscoron@tranef.com

³ CryptoExperts, France; ⁴ Ecole Normale Supérieure, France, tancrede.lepoint@cryptoexperts.com

⁵ NTT Secure Platform Laboratories, Japan, tibouchi.mehdi@lab.ntt.co.jp

⁶ Ulsan, National Institute of Science and Technology (UNIST), Republic of Korea, aaramyun@unist.ac.kr

Abstract. We extend the fully homomorphic encryption scheme over the integers of van Dijk et al. (DGHV) into a batch fully homomorphic encryption scheme, i.e. to a scheme that supports encrypting and homomorphically processing a vector of plaintexts as a single ciphertext.

We present two variants in which the semantic security is based on different assumptions. The first variant is based on a new decisional problem, the Decisional Approximate-GCD problem, whereas the second variant is based on the more classical computational Error-Free Approximate-GCD problem but requires additional public key elements.

We also show how to perform arbitrary permutations on the underlying plaintext vector given the ciphertext and the public key. Our scheme offers competitive performance even with the bootstrapping procedure: we describe an implementation of the homomorphic evaluation of AES, with an amortized cost of about 12 minutes per AES ciphertext on a standard desktop computer; this is comparable to the timings presented by Gentry et al. at Crypto 2012 for their implementation of a Ring-LWE based fully homomorphic encryption scheme.

Keywords: Fully Homomorphic Encryption, Batch Encryption, Chinese Remainder Theorem, Approximate GCD, Homomorphic AES

Source: CRYPTO 2013, LNCS, vol. 7881, Springer, Heidelberg (2013)

DGHV

-GCD

-GCD

AES

12

Gentry

2012

AES

-LWE

GCD

AES

Fuming Acid and Cryptanalysis: Handy Tools for Overcoming a Digital Locking and Access Control System

Daehyun Strobel, Benedikt Driessen, Timo Kasper, Gregor Leander,
David Oswald, Falk Schellenberg, and Christof Paar
Horst Gtz Institute for IT-Security
Ruhr-University Bochum, Germany

Abstract. We examine the widespread SimonsVoss digital locking system 3060 G2 that relies on an undisclosed, proprietary protocol to mutually authenticate transponders and locks. For assessing the security of the system, several tasks have to be performed: By decapsulating the used microcontrollers with acid and circumventing their read-out protection with UV-C light, the complete program code and data contained in door lock and transponder are extracted. As a second major step, the multi-pass challenge-response protocol and corresponding cryptographic primitives are recovered via low-level reverse-engineering. The primitives turn out to be based on DES in combination with a proprietary construction. Our analysis pinpoints various security vulnerabilities that enable practical key-recovery attacks. We present two different approaches for unauthorizedly gaining access to installations. Firstly, an attacker having physical access to a door lock can extract a master key, allowing to mimic transponders, in altogether 30 minutes. A second, purely logical attack exploits an implementation flaw in the protocol and works solely via the wireless interface. As the only prerequisite, a valid ID of a transponder needs to be known (or guessed). After executing a few (partial) protocol runs in the vicinity of a door lock, and some seconds of computation, an adversary obtains all of the transponder's access rights.

Keywords: Access control, electronic lock, reverse-engineering, realworld attack, hardware attack, cryptanalysis, wireless door openers

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

SimonsVoss

3060 G2

UV-C

DES

30

ID

Real Time Cryptanalysis of Bluetooth Encryption with Condition Masking

Bin Zhang¹, Chao Xu², and Dengguo Feng²

¹ State Key Laboratory of Information Security, Institute of Information
Engineering, Chinese Academy of Sciences, Beijing, 100093, P.R. China

² Institute of Software, Chinese Academy of Sciences, Beijing 100190, P.R. China

{zhangbin,xuchao}/@is.iscas.ac.cn

Abstract. The Bluetooth standard authorized by IEEE 802.15.1 adopts the two-level E0 stream cipher to protect short range privacy in wireless networks. The best published attack on it at Crypto 2005 requires 238 on-line computations, 238 off-line computations and 233 memory (which amount to about 19-hour, 37-hour and 64GB storage in practice) to restore the original encryption key, given the first 24 bits of 223.8 frames.

In this paper, we describe more threatening and real time attacks against two-level E0 based on condition masking, a new cryptanalytic technique that characterizes the conditional correlation attacks on stream ciphers. The idea is to carefully choose the condition to get better tradeoffs on the time/memory/data complexity curve. It is shown that if the first 24bits of 222.7 frames is available, the secret key can be reliably found with 2^{27} on-line computations, $2^{21.1}$ off-line computations and 4MB memory. Our attacks have been fully implemented on one core of a single PC. It takes only a few seconds to restore the original encryption key. This is the best known-IV attack on the real Bluetooth encryption scheme so far.

Keywords: Stream ciphers, Correlation, Condition masking, Bluetooth two-level E0

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

Structural Evaluation of AES and Chosen-Key Distinguisher of 9-Round AES-128

Pierre-Alain Fouque¹, Jeremy Jean², and Thomas Peyrin³

¹ Universite de Rennes 1, France

² Ecole Normale Supérieure, France

³ Nanyang Technological University, Singapore

Abstract. While the symmetric-key cryptography community has now a good experience on how to build a secure and efficient fixed permutation, it remains an open problem how to design a key-schedule for block ciphers, as shown by the numerous candidates broken in the related-key model or in a hash function setting. Provable security against differential and linear cryptanalysis in the related-key scenario is an important step towards a better understanding of its construction. Using a structural analysis, we show that the full AES-128 cannot be proven secure unless the exact coefficients of the MDS matrix and the S-Box differential properties are taken into account since its structure is vulnerable to a related-key differential attack. We then exhibit a chosen key distinguisher for AES-128 reduced to 9 rounds, which solves an open problem of the symmetric community. We obtain these results by revisiting algorithmic theory and graph-based ideas to compute all the best differential characteristics in SPN ciphers, with a special focus on AES-like ciphers subject to related-keys. We use a variant of Dijkstra's algorithm to efficiently find the most efficient related-key attacks on SPN ciphers with an algorithm linear in the number of rounds.

Keywords: SPN, Block Cipher, AES, Related-Key, Chosen-Key

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

AES

9 AES-128

AES-128

MDS

S

AES-128

9

SPN

AES

Dijkstra

SPN

SPN

SPN

AES

Bounds in Shallows and in Miseries

Céline Blondeau¹, Andrey Bogdanov², and Gregor Leander³

¹ Aalto University, School of Science, Finland

celine.blondeau@aalto.fi

² Technical University of Denmark, Denmark

anbog@dtu.dk

³ Ruhr University Bochum, Germany

gregor.leander@rub.de

Abstract. Proving bounds on the expected differential probability (EDP) of a characteristic over all keys has been a popular technique of arguing security for both block ciphers and hash functions. In fact, to a large extent, it was the clear formulation and elegant deployment of this very principle that helped Rijndael win the AES competition. Moreover, most SHA-3 finalists have come with explicit upper bounds on the EDP of a characteristic as a major part of their design rationale. However, despite the pervasiveness of this design approach, there is no understanding of what such bounds actually mean for the security of a primitive once a key is fixed — an essential security question in practice.

In this paper, we aim to bridge this fundamental gap. Our main result is a quantitative connection between a bound on the EDP of differential characteristics and the highest number of input pairs that actually satisfy a characteristic for a fixed key. This is particularly important for the design of permutation-based hash functions such as sponge functions, where the EDP value itself is not informative for the absence of rekeying. We apply our theoretical result to revisit the security arguments of some prominent recent block ciphers and hash functions. For most of those, we have good news: a characteristic is followed by a small number of pairs only. For Keccak, though, currently much more rounds would be needed for our technique to guarantee any reasonable maximum number of pairs.

Thus, our work — for the first time — sheds light on the fixed-key differential behaviour of block ciphers in general and substitution permutation networks in particular which has been a long-standing fundamental problem in symmetric-key cryptography.

Keywords: block cipher, hash function, differential cryptanalysis, differential characteristic, expected differential probability, Grøstl

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

EDP

Rijndael

AES

SHA-3

EDP

EDP

EDP

Keccak

Grøstl

Sieve-in-the-Middle: Improved MITM Attacks

Anne Canteaut¹, María Naya-Plasencia¹, and Bastien Vayssière²

¹ Inria Paris-Rocquencourt, Project-Team SECRET, France

{ Anne.Canteaut, Maria.Naya Plasencia } @inria.fr,

² Université de Versailles Saint-Quentin-en-Yvelines, France

bastien.vayssiere.w@gmail.com

Abstract. This paper presents a new generic technique, named sieve-in-the-middle, which improves meet-in-the-middle attacks in the sense that it provides an attack on a higher number of rounds. Instead of selecting the key candidates by searching for a collision in an intermediate state which can be computed forwards and backwards, we look for the existence of valid transitions through some middle sbox. Combining this technique with short bicliques allows to freely add one or two more rounds with the same time complexity. Moreover, when the key size of the cipher is larger than its block size, we show how to build the bicliques by an improved technique which does not require any additional data (on the contrary to previous biclique attacks). These techniques apply to PRESENT, DES, PRINCE and AES, improving the previously known results on these four ciphers. In particular, our attack on PRINCE applies to 8 rounds (out of 12), instead of 6 in the previous cryptanalyses. Some results are also given for theoretically estimating the sieving probability provided by some inputs and outputs of a given sbox.

Keywords: Meet-in-the-middle, bicliques, sbox, matching algorithms

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

MITM

S bicliques

bicliques biclique

PRESENT, DES, PRINCE AES

PRINCE 12 8

6 S

biliciques S

Construction of Differential Characteristics in ARX Designs Application to Skein

Gaëan Leurent

UCL Crypto Group

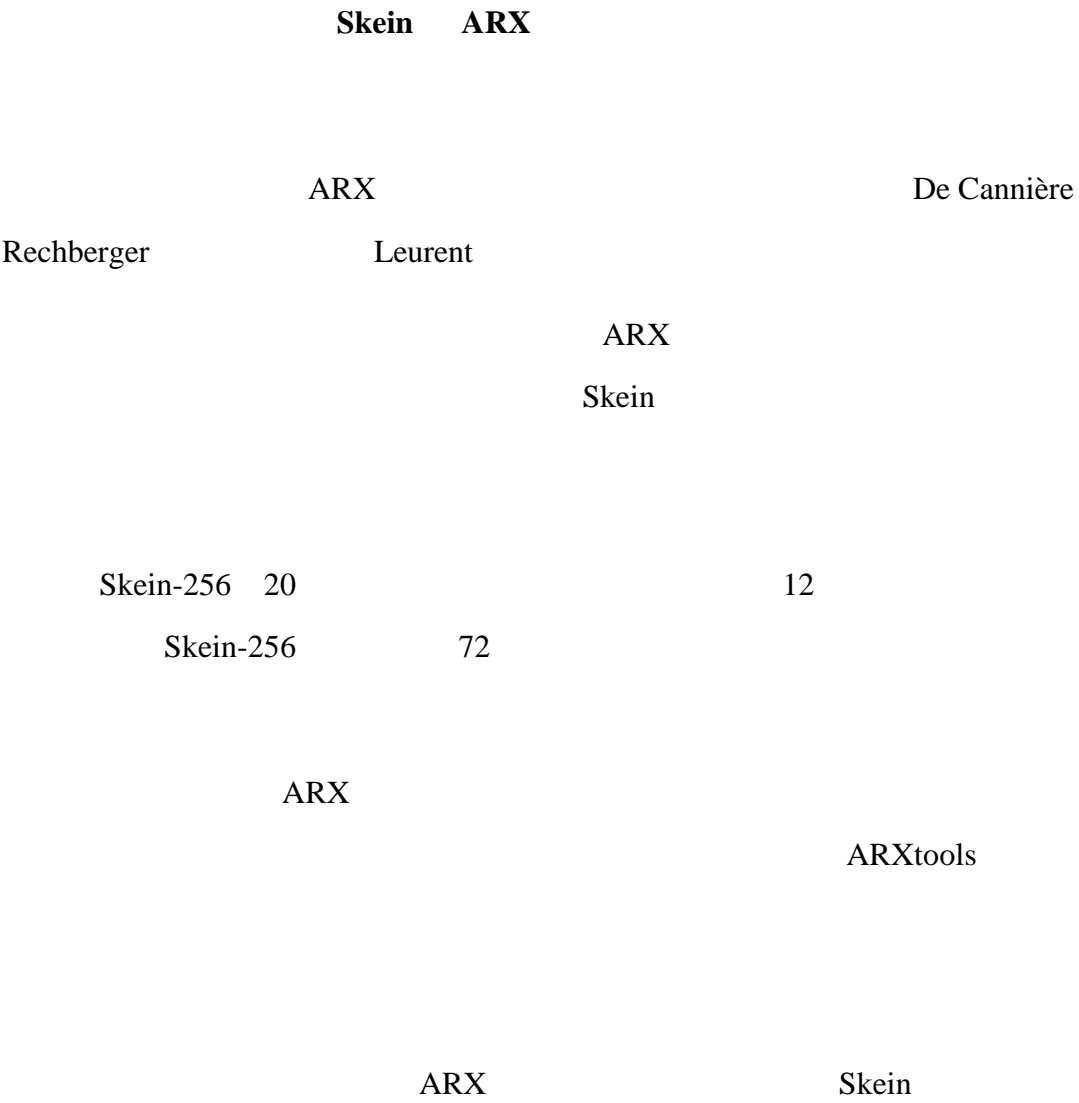
Gaetan.Leurent@uclouvain.be

Abstract. In this paper, we study differential attacks against ARX schemes. We build upon the generalized characteristics of De Canni re and Rechberger and the multi-bit constraints of Leurent.

Our main result is an algorithm to build complex non-linear differential characteristics for ARX constructions, that we applied to reduced versions of the hash function Skein. We present several characteristics for use in various attack scenarios: on the one hand we show attacks with a relatively low complexity, in relatively strong settings; and on the other hand weaker distinguishers reaching more rounds. Our most notable results are practical free-start and semi-free-start collision attacks for 20 rounds and 12 rounds of Skein-256, respectively. Since the full version of Skein-256 has 72 rounds, this result confirms the large security margin of the design. These results are some of the first examples of complex differential trails built for pure ARX designs. We believe this is an important work to assess the security those functions against differential cryptanalysis. Our tools are publicly available from the ARXtools webpage.

Keywords: Symmetric ciphers, Hash functions, ARX, Generalized characteristics, Differential attacks, Skein

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)



On Fair Exchange, Fair Coins and Fair Sampling

Shashank Agrawal and Manoj Prabhakaran
University of Illinois, Urbana-Champaign
{sagraw12,mmp}@illinois.edu

Abstract. We study various classical secure computation problems in the context of fairness, and relate them with each other. We also systematically study fair sampling problems (i.e., inputless functionalities) and discover three levels of complexity for them.

Our results include the following:

- Fair exchange cannot be securely reduced to the problem of fair cointossing by an r -round protocol, except with an error that is $\Omega(1/r)$.

- Finite fair sampling problems with rational probabilities can all be reduced to fair coin-tossing and unfair 2-party computation (or equivalently, under computational assumptions). Thus, for this class of functionalities, fair coin-tossing is complete.

- Only sampling problems which have fair protocols without any fair setup are the trivial ones in which the two parties can sample their outputs independently. Others all have an $\Omega(1/r)$ error, roughly matching an upperbound for fair sampling from [21].

- We study communication-less protocols for sampling, given another sampling problem as setup, since such protocols are inherently fair. We use spectral graph theoretic tools to show that it is impossible to reduce a sampling problem with common information (like fair cointossing) to a sampling problem without (like “noisy” coin-tossing, which has a small probability of disagreement).

The last result above is a slightly sharper version of a classical result by Witsenhausen from 1975. Our proof reveals the connection between the tool used by Witsenhausen, namely “maximal correlation,” and spectral graph theoretic tools like Cheeger inequality.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

—

r-

$$\Omega\left(\frac{l}{r}\right)$$

$$\Omega\left(\frac{l}{r}\right)$$

[21]

“ ”

Witsenhausen 1975
Witsenhausen
Cheeger

Limits on the Power of Cryptographic Cheap Talk

Pavel Hubáček¹, Jesper Buus Nielsen¹, and Alon Rosen²

¹ Aarhus University

² IDC Herzliya

Abstract. We revisit the question of whether cryptographic protocols can replace correlated equilibria mediators in two-player strategic games. This problem was first addressed by Dodis, Halevi and Rabin (CRYPTO 2000), who suggested replacing the mediator with a secure protocol and proved that their solution is stable in the Nash equilibrium (NE) sense, provided that the players are computationally bounded.

We show that there exist two-player games for which no cryptographic protocol can implement the mediator in a sequentially rational way; that is, without introducing empty threats. This explains why all solutions so far were either sequentially unstable, or were restricted to a limited class of correlated equilibria (specifically, those that do not dominate any NE, and hence playing them does not offer a clear advantage over playing any NE).

In the context of computational NE, we classify necessary and sufficient cryptographic assumptions for implementing a mediator that allows to achieve a given utility profile of a correlated equilibrium. The picture that emerges is somewhat different than the one arising in semi-honest secure two-party computation. Specifically, while in the latter case every functionality is either “complete” (i.e., implies Oblivious Transfer) or “trivial” (i.e., can be securely computed unconditionally), in the former there exist some “intermediate” utility profiles whose implementation is equivalent to the existence of one-way functions.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

Dodis Halevi Rabin (CRYPTO 2000)

NE

NE

NE

Accuracy-Privacy Tradeoffs for Two-Party Differentially Private Protocols

Vipul Goyal^{1,_,}, Ilya Mironov^{2,}, Omkant Pandey^{3,_,}, and Amit Sahai^{4,__,}

¹ Microsoft Research India

² Microsoft Research Silicon Valley

³ The University of Texas at Austin

⁴ University of California Los Angeles

Abstract. Differential privacy (DP) is a well-studied notion of privacy that is generally achieved by randomizing outputs to preserve the privacy of the input records. A central problem in differential privacy is how much accuracy must be lost in order to preserve input privacy?

Our work obtains general upper bounds on accuracy for differentially private two-party protocols computing any Boolean function. Our bounds are independent of the number of rounds and the communication complexity of the protocol, and hold with respect to computationally unbounded parties. At the heart of our results is a new general geometric technique for obtaining non-trivial accuracy bounds for any Boolean functionality.

We show that for any Boolean function, there is a constant accuracy gap between the accuracy that is possible in the client-server setting and the accuracy that is possible in the two-party setting. In particular, we show tight results on the accuracy that is achievable for the AND and XOR functions in the two-party setting, completely characterizing which accuracies are achievable for any given level of differential privacy.

Finally, we consider the situation if we relax the privacy requirement to computational differential privacy. We show that to achieve any noticeably better accuracy than what is possible for differentially private two-party protocols, it is essential that one-way functions exist.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

DP

-

AND XOR

Secure Computation against Adaptive Auxiliary Information

Elette Boyle¹, Sanjam Garg², Abhishek Jain³, Yael Tauman Kalai⁴,
and Amit Sahai²

¹ MIT

eboyle@mit.edu

² UCLA

{sanjamg,sahai}@cs.ucla.edu

³ MIT and Boston University

abhishek@csail.mit.edu

⁴ Microsoft Research, New England

yael@microsoft.com

Abstract. We study the problem of secure two-party and multiparty computation (MPC) in a setting where a cheating polynomial-time adversary can corrupt an arbitrary subset of parties and, in addition, learn arbitrary auxiliary information on the entire states of all honest parties (including their inputs and random coins), in an adaptive manner, throughout the protocol execution. We formalize a definition of multiparty computation secure against adaptive auxiliary information (AAIMPC), that intuitively guarantees that such an adversary learns no more than the function output and the adaptive auxiliary information. In particular, if the auxiliary information contains only partial, “noisy,” or computationally invertible information on secret inputs, then only such information should be revealed.

We construct a universally composable AAI two-party and multiparty computation protocol that realizes any (efficiently computable) functionality against malicious adversaries in the common reference string model, based on the linear assumption over bilinear groups and the n -th residuosity assumption. Apart from theoretical interest, our result has interesting applications to the regime of leakage-resilient cryptography.

At the heart of our construction is a new two-round oblivious transfer protocol secure against malicious adversaries who may receive adaptive auxiliary information. This may be of independent interest.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions

Francois-Xavier Standaert¹, Olivier Pereira¹, and Yu Yu²

¹ ICTEAM/ELEN/Crypto Group, Universite Catholique de Louvain, Belgium

² East China Normal University and Tsinghua University, China

Abstract. Leakage-resilient cryptography aims at formally proving the security of cryptographic implementations against large classes of side channel adversaries. One important challenge for such an approach to be relevant is to adequately connect the formal models used in the proofs with the practice of side-channel attacks. It raises the fundamental problem of finding reasonable restrictions of the leakage functions that can be empirically verified by evaluation laboratories. In this paper, we first argue that the previous bounded leakage requirements used in leakage resilient cryptography are hard to fulfill by hardware engineers. We then introduce a new, more realistic and empirically verifiable assumption of simulatable leakage, under which security proofs in the standard model can be obtained. We finally illustrate our claims by analyzing the physical

Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries

David Cash¹, Stanislaw Jarecki², Charanjit Jutla³, Hugo Krawczyk³,
Marcel-Catalin Rosu³, and Michael Steiner³

¹ Rutgers University

david.cash@cs.rutgers.edu

² University of California Irvine

stasio@ics.uci.edu

³ IBM Research

{csjutla,hugokraw,rosu,msteiner}@us.ibm.com

Abstract. This work presents the design and analysis of the first searchable symmetric encryption (SSE) protocol that supports conjunctive search and general Boolean queries on outsourced symmetrically encrypted data and that scales to very large databases and arbitrarily structured data including free text search. To date, work in this area has focused mainly on single-keyword search. For the case of conjunctive search, prior SSE constructions required work linear in the total number of documents in the database and provided good privacy only for structured attribute-value data, rendering these solutions too slow and inflexible for large practical databases.

In contrast, our solution provides a realistic and practical trade-off between performance and privacy by efficiently supporting very large databases at the cost of moderate and well-defined leakage to the outsourced server (leakage is in the form of data access patterns, never as direct exposure of plaintext data or searched values). We present a detailed formal cryptographic analysis of the privacy and security of our protocols and establish precise upper bounds on the allowed leakage. To demonstrate the real-world practicality of our approach, we provide performance results of a prototype applied to several large representative data sets, including encrypted search over the whole English Wikipedia (and beyond).

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

Message-Locked Encryption for Lock-Dependent Messages

Martín Abadi^{1,3}, Dan Boneh², Ilya Mironov¹

Ananth Raghunathan², and Gil Segev²

¹Microsoft Research Silicon Valley

²Stanford University

³University of California, Santa Cruz

Abstract. Motivated by the problem of avoiding duplication in storage systems, Bellare, Keelveedhi, and Ristenpart have recently put forward the notion of Message-Locked Encryption (MLE) schemes which subsumes *convergent encryption* and its variants. Such schemes do not rely on permanent secret keys, but rather encrypt messages using keys de-rived from the messages themselves.

We strengthen the notions of security proposed by Bellare et al. by considering plaintext distributions that may depend on the public parameters of the schemes. We refer to such inputs as lock-dependent messages. We construct two schemes that satisfy our new notions of security for message-locked encryption with lock-dependent messages.

Our main construction deviates from the approach of Bellare et al. by avoiding the use of ciphertext components derived deterministically from the messages. We design a fully randomized scheme that supports an equality-testing algorithm defined on the ciphertexts.

Our second construction has a deterministic ciphertext component that enables more efficient equality testing. Security for lock-dependent messages still holds under computational assumptions on the message distributions produced by the attacker. In both of our schemes the overhead in the length of the ciphertext is only additive and independent of the message length.

Keywords: Deduplication, convergent encryption, message-locked encryption

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

:

Bellare, Keelveedhi Ristenpart

Bellare

Bellare

The Mix-and-Cut Shuffle: Small-Domain Encryption Secure against N Queries

Thomas Ristenpart¹ and Scott Yilek²

¹ University of Wisconsin–Madison

rist@cs.wisc.edu

² University of St. Thomas

syilek@stthomas.edu

Abstract. We provide a new shuffling algorithm, called Mix-and-Cut, that provides a provably-secure block cipher even for adversaries that can observe the encryption of all $N = 2n$ domain points. Such fully secure ciphers are useful for format-preserving encryption, where small domains (e.g., $n = 30$) are common and databases may well include examples of almost all ciphertexts. Mix-and-Cut derives from a general framework for building fully secure pseudorandom permutations (PRPs) from fully secure pseudorandom separators (PRSs). The latter is a new primitive that we treat for the first time. Our framework was inspired by, and uses ideas from, a particular cipher due to Granboulin and Pornin. To achieve full security for Mix-and-Cut using this framework, we give a simple proof that a PRP secure for $(1 - \epsilon)N$ queries (recently achieved efficiently by Hoang, Morris, and Rogaway’s Swap-or-Not cipher) yields a PRS secure for N queries.

Key words: shuffles, small-block encryption, tweakable block ciphers

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

N

Mix-and-Cut ,

$$N = 2n$$

(e.g., $n = 30$)

(PRSs)

(PRPs)

(PRSs)

Granboulin

Pornin

$$1-E \quad N$$

N

Hoang, Morris, and

Rogaway

Key Homomorphic PRFs and Their Applications

Dan Boneh, Kevin Lewi, Hart Montgomery, and Ananth Raghunathan
Computer Science Department,
Stanford University, Stanford, CA 94305

Abstract. A pseudorandom function $F : K \times X \rightarrow Y$ is said to be key homomorphic if given $F(k_1, x)$ and $F(k_2, x)$ there is an efficient algorithm to compute $F(k_1 \oplus k_2, x)$, where \oplus denotes a group operation on k_1 and k_2 such as *xor*. Key homomorphic PRFs are natural objects to study and have a number of interesting applications: they can simplify the process of rotating encryption keys for encrypted data stored in the cloud, they give one round distributed PRFs, and they can be the basis of a symmetric-key proxy re-encryption scheme. Until now all known constructions for key homomorphic PRFs were only proven secure in the random oracle model. We construct the first provably secure key homomorphic PRFs in the standard model.

$$\begin{array}{ccccc}
 & & F(k_1,x) & F(k_2,x) & F(k_1\oplus k_2,x), \\
 & & & & \\
 k_1 & & k_2 & & F:K\times X\rightarrow Y
 \end{array}$$

$$\begin{array}{ccc}
 \text{LWE} & & l
 \end{array}$$

$$\text{LWE}$$

On the Security of the TLS Protocol: A Systematic Analysis

Hugo Krawczyk¹, Kenneth G. Paterson², and Hoeteck Wee³

¹IBM Research

²Royal Holloway, University of London

³George Washington University

Abstract. TLS is the most widely-used cryptographic protocol on the Internet. It comprises the TLS Handshake Protocol, responsible for authentication and key establishment, and the TLS Record Protocol, which takes care of subsequent use of those keys to protect bulk data. In this paper, we present the most complete analysis to date of the TLS Handshake protocol and its application to data encryption (in the Record Protocol). We show how to extract a key-encapsulation mechanism (KEM) from the TLS Handshake Protocol, and how the security of the entire TLS protocol follows from security properties of this KEM when composed with a secure authenticated encryption scheme in the Record Protocol. The security notion we achieve is a variant of the ACCE notion recently introduced by Jager et al. (Crypto '12). Our approach enables us to analyse multiple different key establishment methods in a modular fashion, including the *first proof* of the most common deployment mode that is based on RSA PKCS #1v1.5 encryption, as well as Diffie-Hellman modes. Our results can be applied to settings where mutual authentication is provided and to the more common situation where only server authentication is applied.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

TLS

TLS Internet

TLS

TLS

TLS

TLS

TLS

(KEM)

TLS

ACCE

Jager

12

RSA PKCS #1v1.5

Diffie-Hellman

New Techniques for SPHF and Efficient One-Round PAKE Protocols

Fabrice Benhamouda¹, Olivier Blazy², Céline Chevalier³,

David Pointcheval¹, and Damien Vergnaud¹

¹ ENS, Paris, France*

² Ruhr-Universität Bochum, Germany

³ Université Panéon-Assas, Paris, France

Abstract. Password-authenticated key exchange (PAKE) protocols allow two players to agree on a shared high entropy secret key, that depends on their own passwords only. Following the Gennaro and Lindell's approach, with a new kind of smooth-projective hash functions (SPHFs), Katz and Vaikuntanathan recently came up with the first concrete one-round PAKE protocols, where the two players just have to send simultaneous flows to each other. The first one is secure in the Bellare-Pointcheval-Rogaway (BPR) model and the second one in the Canetti's UC framework, but at the cost of simulation-sound non-interactive zero knowledge (SS-NIZK) proofs (one for the BPR-secure protocol and two for the UC-secure one), which make the overall constructions not really efficient.

This paper follows their path with, first, a new efficient instantiation of SPHF on Cramer-Shoup ciphertexts, which allows to get rid of the SS-NIZK proof and leads to the design of the most efficient one-round PAKE known so far, in the BPR model, and in addition without pairings.

In the UC framework, the security proof required the simulator to be able to extract the hashing key of the SPHF, hence the additional SS-NIZK proof. We improve the way the latter extractability is obtained by introducing the notion of trapdoor smooth projective hash functions (TSPHFs). Our concrete instantiation leads to the most efficient one round PAKE UC-secure against static corruptions to date.

We additionally show how these SPHFs and TSPHFs can be used for blind signatures and zero-knowledge proofs with straight-line extractability.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

PAKE

PAKE

Gennaro Lindell

SPHF_s Katz Vaikuntanathan

1 PAKE

Bellare-Pointcheval-Rogaway BPR

Canetti

UC

SS-NIZK

BPR-

UC-

Cramer-Shoup

SPHF

BPR

SS-NIZK

PAKE

UC

SPHF

SS-NIZK

TSPHF_s

1 PAKE

UC

SPHF_s

TSPHF_s

Practical Multilinear Maps over the Integers

Jean-S'ebastien Coron¹, Tancre`ede Lepoint^{2,3}, and Mehdi Tibouchi⁴

¹ University of Luxembourg

jean-sebastien.coron@uni.lu

² CryptoExperts, France

³ Ecole Normale Sup'erieure, France

tancrede.lepoint@cryptoexperts.com

⁴ NTT Secure Platform Laboratories, Japan

tibouchi.mehdi@lab.ntt.co.jp

Abstract. Extending bilinear elliptic curve pairings to multilinear maps is a long-standing open problem. The first plausible construction of such multilinear maps has recently been described by Garg Gentry and Halevi, based on ideal lattices. In this paper we describe a different construction that works over the integers instead of ideal lattices, similar to the DGHV fully homomorphic encryption scheme. We also describe a different technique for proving the full randomization of encodings: instead of Gaussian linear sums, we apply the classical leftover hash lemma over a quotient lattice. We show that our construction is relatively practical: for reasonable security parameters a one-round 7-party Diffie-Hellman key exchange requires less than 40 seconds per party. Moreover, in contrast with previous work, multilinear analogues of useful, base group assumptions like DLIN appear to hold in our setting.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

Garg Gentry Halevi

DGHV

7 Diffie-Hellman

40

DLIN

Full Domain Hash from (Leveled) Multilinear Maps and Identity-Based

Aggregate Signatures

Susan Hohenberger^{1,*}, Amit Sahai^{2,**} and Brent Waters^{3,***}

¹ Johns Hopkins University

susan@cs.jhu.edu

² UCLA

sahai@cs.ucla.edu

³ University of Texas at Austin

bwaters@cs.utexas.edu

Abstract. In this work, we explore building constructions with full domain hash structure, but with standard model proofs that do not employ the random oracle heuristic. The launching point for our results will be the utilization of a “leveled” multilinear map setting for which Garg, Gentry, and Halevi (GGH) recently gave an approximate candidate. Our first step is the creation of a standard model signature scheme that exhibits the structure of the Boneh, Lynn and Shacham signatures. In particular, this gives us a signature that admits unrestricted aggregation.

We build on this result to offer the first identity-based aggregate signature scheme that admits unrestricted aggregation. In our construction, an arbitrary-sized set of signatures on identity/message pairs can be aggregated into a single group element, which authenticates the entire set. The identity-based setting has important advantages over regular aggregate signatures in that it eliminates the considerable burden of having to store, retrieve or verify a set of verification keys, and minimizes the total cryptographic overhead that must be attached to a set of signer/message pairs. While identity-based signatures are trivial to achieve, their aggregate counterparts are not. To the best of our knowledge, no prior candidate for realizing unrestricted identity-based aggregate signatures exists in either the standard or random oracle models.

A key technical idea underlying these results is the realization of a hash function with a Naor-Reingold-type structure that is publicly computable using repeated application of the multilinear map. We present our results in a generic “leveled” multilinear map setting and then show how they can be translated to the GGH graded algebras analogue of multilinear maps.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)



Garg Gentry Halevi GGH

Boneh Lynn

Shacham

/

/

Naor-Rengold

GGH

Programmable Hash Functions in the Multilinear Setting

Eduarda S.V. Freire^{1,*}, Dennis Hofheinz^{2,**},
Kenneth G. Paterson^{1,***}, and Christoph Striecks²
¹ Royal Holloway, University of London
² Karlsruhe Institute of Technology

Abstract. We adapt the concept of a programmable hash function (PHF, Crypto 2008) to a setting in which a multilinear map is available. This enables new PHFs with previously unachieved parameters.

To demonstrate their usefulness, we show how our (standard-model) PHFs can replace random oracles in several well-known cryptographic constructions. Namely, we obtain standard-model versions of the Boneh- Franklin identity-based encryption scheme, the Boneh-Lynn-Shacham signature scheme, and the Sakai-Ohgishi-Kasahara identity-based noninteractive key exchange (ID-NIKE) scheme. The ID-NIKE scheme is the first scheme of its kind in the standard model.

Our abstraction also allows to derive hierarchical versions of the above schemes in settings with multilinear maps. This in particular yields simple and efficient hierarchical generalizations of the BF, BLS, and SOK schemes. In the case of hierarchical ID-NIKE, ours is the first such scheme with full security, in either the random oracle model or the standard model.

While our constructions are formulated with respect to a generic multilinear map, we also outline the necessary adaptations required for the recent “noisy” multilinear map candidate due to Garg, Gentry, and Halevi.

Keywords: programmable hash functions, multilinear maps, identity based encryption, identity-based non-interactive key exchange, digital signatures

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)



On the Indifferentiability of Key-Alternating Ciphers

Elena Andreeva¹, Andrey Bogdanov², Yevgeniy Dodis³,

Bart Mennin¹, and John P. Steinberger⁴

¹ KU Leuven and iMinds

{elena.andreeva, bart.mennin}@edat.kuleuven.be

² Technical University of Denmark

a.bogdanov@mat.dtu.dk

³ New York University

dodis@cs.nyu.edu

⁴ Tsinghua University

jpsteinb@gmail.com

Abstract. The Advanced Encryption Standard (AES) is the most widely used block cipher. The high level structure of AES can be viewed as a (10-round) key-alternating cipher, where a t -round key-alternating cipher KA_t consists of a small number t of fixed permutations P_i on n bits, separated by key addition:

$$\text{KA}_t(K, m) = k_t \oplus P_t(\dots k_2 \oplus P_2(k_1 \oplus P_1(k_0 \oplus m)) \dots),$$

where (k_0, \dots, k_t) are obtained from the master key K using some key derivation function.

For $t = 1$, KA_1 collapses to the well-known Even-Mansour cipher, which is known to be indistinguishable from a (secret) random permutation, if P_1 is modeled as a (public) random permutation. In this work we seek for stronger security of key-alternating ciphers indifferentiability from an ideal cipher and ask the question under which conditions on the key derivation function and for how many rounds t is the key-alternating cipher KA_t indifferentiable from the ideal cipher, assuming P_1, \dots, P_t are (public) random permutations?

As our main result, we give an affirmative answer for $t = 5$, showing that the 5-round key-alternating cipher KA_5 is indifferentiable from an ideal cipher, assuming P_1, \dots, P_5 are five independent random permutations, and the key derivation function sets all rounds keys $k_i = f(K)$, where $0 \leq i \leq 5$ and f is modeled as a random oracle. Moreover, when $|K| = |m|$, we show we can set $f(K) = P_0(K) \oplus K$, giving an n -bit block cipher with an n -bit key, making only six calls to n -bit permutations $P_0, P_1, P_2, P_3, P_4, P_5$.

Keywords: Even-Mansour, ideal cipher, key-alternating cipher, indifferentiability

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)



AES		AES	
10	t	KA_t	n
P_i	t		
$\text{KA}_t(K,m)=k_t\oplus P_t(\dots k_2\oplus P_2(k_1\oplus P_1(k_0\oplus m))\dots),$			
(k_0,\dots,k_t)		K	
$t=1$	P_1	KA_1	
Even-Mansour			
		-	
P_1,\dots,P_t ()		t	
KA_t			
		$t=5$	5
KA_5		P_1,\dots,P_5	
		$k_i=f(K),\quad 0\leq i\leq 5\quad f$	
$,\quad K = m ,$		$f(K)=P_0(K)\oplus K,$	
n	n	n	P_0,P_1,P_2,P_3,P_4,P_5 6

Even-Mansour

Plain Versus Randomized Cascading-Based Key-Length Extension for Block Cipher

Peter Gazi

ETH Zurich, Switzerland

Department of Computer Science

peter.gazi@inf.ethz.ch

Abstract. Cascading-based constructions represent the predominant approach to the problem of key-length extension for block ciphers. Besides the plain cascade, existing works also consider its modification containing key-whitening steps between the invocations of the block cipher, called randomized cascade or XOR-cascade. We contribute to the understanding of the security of these two designs by giving the following attacks and security proofs, assuming an underlying ideal block cipher with key length κ and block length n :

- For the plain cascade of odd (resp. even) length l we present a generic attack requiring roughly $2^{\kappa + \frac{l-1}{l+1}n}$ (resp. $2^{\kappa + \frac{l-2}{l}n}$) queries, being a generalization of both the meet-in-the-middle attack on double encryption and the best known attack on triple cascade.

- For XOR-cascade of odd (resp. even) length l we prove security up to $2^{\kappa + \frac{l-1}{l+1}n}$ (resp. $2^{\kappa + \frac{l-2}{l}n}$) queries and also an improved bound $2^{\kappa + \frac{l-1}{l}n}$ for the special case $l \in \{3, 4\}$ by relating the problem to the security of key-alternating ciphers in the random-permutation model.

- Finally, for a natural class of sequential constructions where block-cipher encryptions are interleaved with key-dependent permutations, we show a generic attack requiring roughly $2^{\kappa + \frac{l-1}{l}n}$ queries. Since XOR-cascades are sequential, this proves tightness of our above result for XOR-cascades of length $l \in \{3, 4\}$ as well as their optimal security within the class of sequential constructions.

These results suggest that XOR-cascades achieve a better security/efficiency trade-off than plain cascades and should be preferred.

Keywords: Provable security, block ciphers, key-length extension, ideal-cipher model, cascade, XOR-cascade

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)



	κ	n
$\frac{2^{\kappa+\frac{l-2}{l}n}}{2^{\kappa+\frac{l-1}{l+1}n}}$	l	
$\frac{2^{\kappa+\frac{l-2}{l}n}}{2^{\kappa+\frac{l-1}{l+1}n}}$	l	$2^{\kappa+\frac{l-1}{l+1}n}$
	$l \in \{3,4\}$	$2^{\kappa+\frac{l-1}{l}n}$
	$l \in \{3,4\}$	$2^{\kappa+\frac{l-1}{l}n}$
		$/$

Digital Signatures with Minimal Overhead from Indifferentiable Random Invertible Functions

Eike Kiltz¹, Krzysztof Pietrzak², and Mario Szegedy³

¹ Horst-Gortz Institute for IT Security, Ruhr-Universität Bochum, Germany

eike.kiltz@rub.de

² Institute of Science and Technology, Austria

pietrzak@ist.ac.at

³ Rutgers University, USA

szegedy@dragon.rutgers.edu

Abstract. In a digital signature scheme with message recovery, rather than transmitting the message m and its signature σ , a single enhanced signature τ is transmitted. The verifier is able to recover m from τ and at the same time verify its authenticity. The two most important parameters of such a scheme are its security and overhead $|\tau| - |m|$. A simple argument shows that for any scheme with “ n bits security” $|\tau| - |m| \geq n$, i.e., the overhead is lower bounded by the security parameter n . Currently, the best known constructions in the random oracle model are far from this lower bound requiring an overhead of $n + \log q_h$, where q_h is the number of queries to the random oracle. In this paper we give a construction which basically matches the n bit lower bound. We propose a simple digital signature scheme with $n + o(\log q_h)$ bits overhead, where q_h denotes the number of random oracle queries.

Our construction works in two steps. First, we propose a signature scheme with message recovery having optimal overhead in a new ideal model, the random invertible function model. Second, we show that a four-round Feistel network with random oracles as round functions is tightly “public-indifferentiable” from a random invertible function. At the core of our indistinguishability proof is an almost tight upper bound for the expected number of edges of the densest “small” subgraph of a random Cayley graph, which may be of independent interest.

Keywords: digital signatures, indistinguishability, Feistel, Additive combinatorics, Cayley graph

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)



$$\begin{array}{ccccccc} & & & & m & & \sigma \\ & & & & m & & \\ \tau & & \tau & & & & \\ & & & & |\tau| - |m| & & \\ \text{“} n & & \text{”} & & |\tau| - |m| \geq n & & n \\ & & & & & & \\ n + \log q_h & & q_h & & & & \\ & & & & n + o(\log q_h) & & \\ n & & & & & & \\ & & q_h & & & & \end{array}$$

$$\begin{array}{ccccccc} & & & & 4 & & \text{Feistel} \\ & & & & & & \\ \text{“} & & \text{”} & & & & \\ \text{“} & & \text{”} & & & & \end{array}$$

Feistel



Practical Bootstrapping in Quasilinear Time

Jacob Alperin-Sheriff and Chris Peikert

School of Computer Science, Georgia Institute of Technology

Abstract. Gentry’s “bootstrapping” technique (STOC2009) constructs a fully homomorphic encryption (FHE) scheme from a “somewhat homomorphic” one that is powerful enough to evaluate its own decryption function. To date, it remains the only known way of obtaining unbounded FHE. Unfortunately, bootstrapping is computationally very expensive, despite the great deal of effort that has been spent on improving its efficiency. The current state of the art, due to Gentry, Halevi, and Smart (PKC 2012), is able to bootstrap “packed” ciphertexts (which encrypt up to a linear number of bits) in time only quasilinear $\tilde{O}(\lambda) = \lambda \cdot \log^{O(1)} \lambda$ in the security parameter. While this performance is asymptotically optimal up to logarithmic factors, the practical import is less clear: the procedure composes multiple layers of expensive and complex operations, to the point where it appears very difficult to implement, and its concrete runtime appears worse than those of prior methods (all of which have quadratic or larger asymptotic runtimes).

In this work we give simple, practical, and entirely algebraic algorithms for bootstrapping in quasilinear time, for both “packed” and “non-packed” ciphertexts. Our methods are easy to implement (especially in the non-packed case), and we believe that they will be substantially more efficient in practice than all prior realizations of bootstrapping. One of our main techniques is a substantial enhancement of the “ring-switching” procedure of Gentry et al. (SCN 2012), which we extend to support switching between two rings where neither is a subring of the other. Using this procedure, we give a natural method for homomorphically valuating a broad class of structured linear transformations, including one that lets us evaluate the decryption function efficiently.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

Gentry (FHE) ,

“ ”

FHE ,

Gentry,Halevi Smart(PKC 2012)

$\tilde{O}(\lambda) = \lambda \cdot \log^{O(1)} \lambda$

“ ”

,

Gentry “ ”

Hardness of SIS and LWE with Small Parameters

Daniele Micciancio¹, and Chris Peikert²,

¹ University of California, San Diego

² School of Computer Science, Georgia Institute of Technology

Abstract. The Short Integer Solution (SIS) and Learning With Errors (LWE) problems are the foundations for countless applications in lattice-based cryptography, and are provably as hard as approximate lattice problems in the worst case. An important question from both a practical and theoretical perspective is how small their parameters can be made, while preserving their hardness.

We prove two main results on SIS and LWE with small parameters. For SIS, we show that the problem retains its hardness for moduli $q \geq \beta \cdot n^\delta$ for any constant $\delta > 0$, where β is the bound on the Euclidean norm of the solution. This improves upon prior results which required $q > \beta \cdot \sqrt{n \cdot \log n}$, and is close to optimal since the problem is trivially easy for $q \leq \beta$. For LWE, we show that it remains hard even when the errors are small (e.g., uniformly random from $\{0, 1\}$), provided that the number of samples is small enough (e.g., linear in the dimension n of the LWE secret). Prior results required the errors to have magnitude at least \sqrt{n} and to come from a Gaussian-like distribution.

Keywords: Lattice cryptography, Computational hardness, SIS, LWE

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

SIS LWE

(SIS)

LWE

worst-case

,

SIS LWE

SIS

$$q \geq \beta \cdot n^\delta$$

$$\delta > 0 \quad \beta$$

$$q > \beta \cdot \sqrt{n \cdot \log n}$$

$$q \leq \beta$$

LWE

n LWE

$$\sqrt{n}$$

SIS

LWE

Lattice Signatures and Bimodal Gaussians

Leo Ducas¹, Alain Durmus², ★Tancrede Lepoint³, and Vadim Lyubashevsky⁴,

¹ ENS Paris, France

² ENPC and ENS Cachan, France

³ CryptoExperts and ENS Paris, France

⁴ INRIA and ENS Paris, France

{Leo.Ducas,Alain.Durmus,Tancrede.Lepoint,Vadim.Lyubashevsky}@ens.fr

Abstract. Our main result is a construction of a lattice-based digital signature scheme that represents an improvement, both in theory and in practice, over today's most efficient lattice schemes. The novel scheme is obtained as a result of a modification of the rejection sampling algorithm that is at the heart of Lyubashevsky's signature scheme (Eurocrypt, 2012) and several other lattice primitives. Our new rejection sampling algorithm which samples from a bimodal Gaussian distribution, combined with a modified scheme instantiation, ends up reducing the standard deviation of the resulting signatures by a factor that is asymptotically square root in the security parameter. The implementations of our signature scheme for security levels of 128,160, and 192 bits compare very favorably to existing schemes such as RSA and ECDSA in terms of efficiency. In addition, the new scheme has shorter signature and public key sizes than all previously proposed lattice signature schemes.

As part of our implementation, we also designed several novel algorithms which could be of independent interest. Of particular note, is a new algorithm for efficiently generating discrete Gaussian samples over \mathbb{Z}_n . Current algorithms either require many high-precision floating point exponentiations or the storage of very large pre-computed tables, which makes them completely inappropriate for usage in constrained devices. Our sampling algorithm reduces the hard-coded table sizes from linear to logarithmic as compared to the time-optimal implementations, at the cost of being only a small factor slower.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

2012

Lyubashevsky

RSA	ECDSA	128	160	192
-----	-------	-----	-----	-----

Z_n

Learning with Rounding, Revisited New Reduction, Properties and Applications

Joël Alwen¹ Stephan Krenn² Krzysztof Pietrzak³ Daniel Wichs⁴

¹ETH Zurich, alwenj@inf.ethz.ch;

²IBM Research – Zurich, skr@zurich.ibm.com

³Institute of Science and Technology Austria, pietrzak@ist.ac.at

⁴Northeastern University, wichs@ccs.neu.edu

Abstract. The learning with rounding (LWR) problem, introduced by Banerjee, Peikert and Rosen at EUROCRYPT ’12, is a variant of learning with errors (LWE), where one replaces random errors with deterministic rounding. The LWR problem was shown to be as hard as LWE for a setting of parameters where the modulus and modulus-to-error ratio are super-polynomial. In this work we resolve the main open problem and give a new reduction that works for a larger range of parameters, allowing for a polynomial modulus and modulus-to-error ratio. In particular, a smaller modulus gives us greater efficiency, and a smaller modulus-to-error ratio gives us greater security, which now follows from the worst-case hardness of GapSVP with polynomial (rather than super polynomial) approximation factors.

As a tool in the reduction, we show that there is a “lossy mode” for the LWR problem, in which LWR samples only reveal partial information about the secret. This property gives us several interesting new applications, including a proof that LWR remains secure with weakly random secrets of sufficient min-entropy, and very simple constructions of deterministic encryption, lossy trapdoor functions and reusable extractors

Our approach is inspired by a technique of Goldwasser et al. from ICS ’10, which implicitly showed the existence of a “lossy mode” for LWE. By refining this technique, we also improve on the parameters of that work to only requiring a polynomial (instead of super-polynomial) modulus and modulus-to-error ratio.

Keywords: Learning with Errors, Learning with Rounding, Lossy Trapdoor Functions, Deterministic Encryption

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

LWR

learning with rounding LWR

Banerjee, Peikert

Rosen

2012

LWE

LWR

LWE

,

GAPSVP

LWR

“

”

LWR

LWR

Goldwasser

ICS '10

LWE

“

”

Learning with Errors Learning with Rounding

Homomorphic Encryption from Learning with Errors: Conceptually-Simpler Asymptotically-Faster Attribute-Based

Craig Gentry¹ Amit Sahai² and Brent Waters³

¹ IBM Research, cbgentry@us.ibm.com

² UCLA, sahai@cs.ucla.edu

³ UT Austin, bwaters@cs.utexas.edu

Abstract. We describe a comparatively simple fully homomorphic encryption (FHE) scheme based on the learning with errors (LWE) problem. In previous LWE-based FHE schemes, multiplication is a complicated and expensive step involving “relinearization”. In this work, we propose a new technique for building FHE schemes that we call the *approximate eigenvector* method. In our scheme, for the most part, homomorphic addition and multiplication are just matrix addition and multiplication. This makes our scheme both asymptotically faster and (we believe) easier to understand. In previous schemes, the homomorphic evaluator needs to obtain the user’s “evaluation key”, which consists of a chain of encrypted secret keys. Our scheme has no evaluation key. The evaluator can do homomorphic operations without knowing the user’s public key at all, except for some basic parameters. This fact helps us construct the first identity based FHE scheme. Using similar techniques, we show how to compile a recent attribute-based encryption scheme for circuits by Gorbunov et al. into an attribute-based FHE scheme that permits data encrypted under the same index to be processed homomorphically.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

LWE

LWE

(FHE)

LWE

Gorbunov

Gorbunov

A Uniform Min-Max Theorem with Applications in Cryptography

Salil Vadhan and Colin Jia Zheng

School of Engineering and Applied Sciences, Harvard University

Cambridge, Massachusetts, {salil,colinz}@seas.harvard.edu

Abstract. We present a new, more constructive proof of von Neumann’s Min-Max Theorem for two-player zero-sum game—specifically, an algorithm that builds a near-optimal mixed strategy for the second player from several best-responses of the second player to mixed strategies of the first player. The algorithm extends previous work of Freund and Schapire (Games and Economic Behavior ’99) with the advantage that the algorithm runs in $\text{poly}(n)$ time even when a pure strategy for the first player is a distribution chosen from a set of distributions over $\{0,1\}^n$. This extension enables a number of additional applications in cryptography and complexity theory, often yielding uniform security versions of results that were previously only proved for nonuniform security (due to use of the non-constructive Min-Max Theorem).

We describe several applications, including a more modular and improved uniform version of Impagliazzo’s Hardcore Theorem (FOCS ’95), showing impossibility of constructing succinct non-interactive arguments (SNARGs) via black-box reductions under uniform hardness assumptions (using techniques from Gentry and Wichs (STOC ’11) for the nonuniform setting), and efficiently simulating high entropy distributions within any sufficiently nice convex set (extending a result of Trevisan, Tulsiani and Vadhan (CCC ’09)).

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

Freund Schapire
 $\{0,1\}^n$

(FOCS '95)

Impagliazzo
Gentry Wichs

Trevisan, Tulsiani and Vadhan

Limits of Provable Security for Homomorphic Encryption

Andrej Bogdanov¹, and Chin Ho Lee²

¹Dept. of Computer Science and Engineering and Institute for Theoretical
Computer Science and Communications, Chinese University of Hong Kong
andrejb@cse.cuhk.edu.hk

²Dept. of Computer Science and Engineering, Chinese University of Hong Kong
chlee@cse.cuhk.edu.hk

Abstract. We show that public-key bit encryption schemes which support weak (i.e., compact) homomorphic evaluation of any sufficiently “sensitive” collection of functions cannot be proved message indistinguishable beyond $\text{AM} \cap \text{coAM}$ via general (adaptive) reductions, and beyond statistical zero-knowledge via reductions of constant query complexity. Examples of sensitive collections include parities, majorities, and the class consisting of all AND and OR functions.

We also give a method for converting a strong (i.e., distribution-preserving) homomorphic evaluator for essentially any boolean function (except the trivial ones, the NOT function, and the AND and OR functions) into a randomization algorithm: This is a procedure that converts a ciphertext into another ciphertext which is statistically close to being independent and identically distributed with the original one. Our transformation preserves negligible statistical error.

Source: CRYPTO 2013, LNCS, Vol. 8042, Springer, Heidelberg (2013)

“ ”

$AM \cap co\ AM$

—

Shorter Quasi-Adaptive NIZK Proofs for Linear Subspaces

Charanjit S. Jutla¹ and Arnab Roy²

¹ IBM T. J. Watson Research Center

Yorktown Heights, NY 10598, USA

csjutla@us.ibm.com

² Fujitsu Laboratories of America

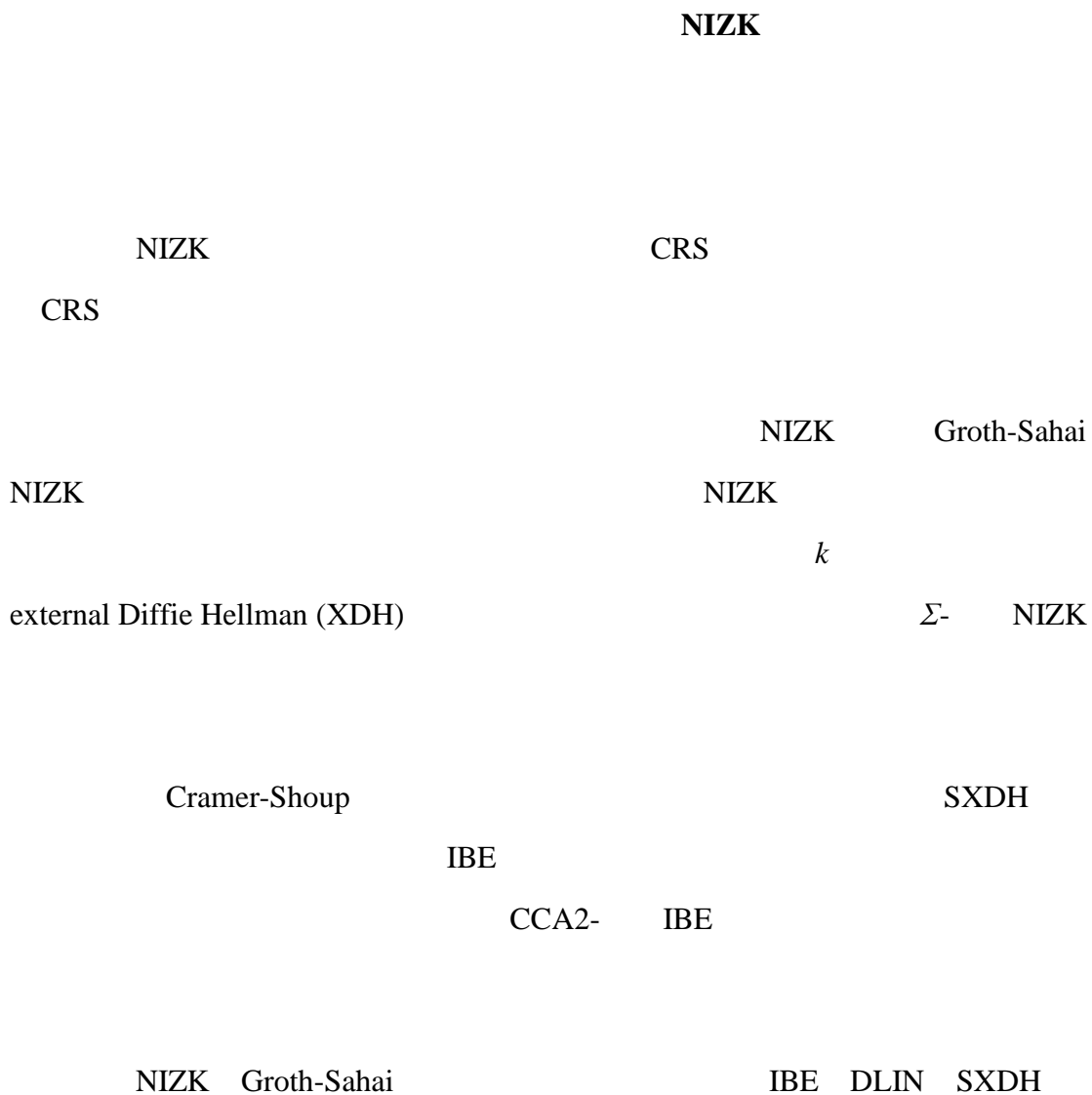
Sunnyvale, CA 94085, USA

arnab@cs.stanford.edu

Abstract. We define a novel notion of quasi-adaptive non-interactive zero knowledge (NIZK) proofs for probability distributions on parametrized languages. It is quasi-adaptive in the sense that the common reference string (CRS) generator can generate the CRS depending on the language parameters. However, the simulation is required to be uniform, i.e., a single efficient simulator should work for the whole class of parametrized languages. For distributions on languages that are linear subspaces of vector spaces over bilinear groups, we give quasi-adaptive computationally sound NIZKs that are shorter and more efficient than Groth-Sahai NIZKs. For many cryptographic applications quasi-adaptive NIZKs suffice, and our constructions can lead to significant improvements in the standard model. Our construction can be based on any k -linear assumption, and in particular under the external Diffie-Hellman (XDH) assumption our proofs are even competitive with Random-Oracle based Σ -protocol NIZK proofs. We also show that our system can be extended to include integer tags in the defining equations, where the tags are provided adaptively by the adversary. This leads to applicability of our system to many applications that use tags, e.g. applications using Cramer-Shoup projective hash proofs. Our techniques also lead to the shortest known (ciphertext) fully secure identity based encryption (IBE) scheme under standard static assumptions (SXDH). Further, we also get a short publicly-verifiableCCA2-secure IBE scheme.

Keywords: NIZK, Groth-Sahai, bilinear pairings, signatures, dual-system IBE, DLIN, SXDH

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)



Constant-Round Concurrent Zero Knowledge in the Bounded Player Model

Vipul Goyal¹, Abhishek Jain², Rafail Ostrovsky³, Silas Richelson⁴,

and Ivan Visconti⁵

¹ Microsoft Research, India

vipul@microsoft.com

² MIT and Boston University, USA

abhishek@csail.mit.edu

³ UCLA, USA

rafail@cs.ucla.edu

⁴ UCLA, USA

sirichel@math.ucla.edu

⁵ University of Salerno, Italy

visconti@dia.unisa.it

Abstract. In [18] Goyal et al. introduced the bounded player model for secure computation. In the bounded player model, there are an a priori bounded number of players in the system, however, each player may execute any unbounded (polynomial) number of sessions. They showed that even though the model consists of a relatively mild relaxation of the standard model, it allows for round-efficient concurrent zero knowledge. Their protocol requires a super-constant number of rounds. In this work we show, constructively, that there exists a *constant-round* concurrent zero-knowledge argument in the bounded player model. Our result relies on a new technique where the simulator obtains a trapdoor corresponding to a player identity by putting together information obtained in multiple sessions. Our protocol is only based on the existence of a collision-resistance hash-function family and comes with a “straight-line” simulator. We note that this constitutes the strongest result known on constant round concurrent zero knowledge in the plain model (under well accepted relaxations) and subsumes Barak’s constant-round bounded concurrent zero-knowledge result. We view this as a positive step towards getting constant round fully concurrent zero-knowledge in the plain model, without relaxations.

Keywords: concurrent zero knowledge, straight-line simulation, bounded player model.

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

: Goyal et al.[18]

“ ”

Barak

Succinct Non-Interactive Zero Knowledge Arguments from Span Programs and Linear Error-Correcting Codes

Helger Lipmaa

Institute of Computer Science, University of Tartu, Estonia

Abstract. Gennaro, Gentry, Parno and Raykova proposed an efficient NIZK argument for Circuit-SAT, based on non-standard tools like conscientious and quadratic span programs. We propose a new linear PCP for the Circuit-SAT, based on a combination of *standard* span programs (that verify the correctness of every individual gate) and high distance linear error-correcting codes (that check the consistency of wire assignments). This allows us to simplify all steps of the argument, which results in significantly improved efficiency. We then construct an NIZK Circuit-SAT argument based on existing techniques.

Keywords: Circuit-SAT, linear error-correcting codes, linear PCP, non interactive zero knowledge, polynomial algebra, quadratic span program, span program, verifiable computation

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

Raykova

CIRCUIT-SAT

NIZK

CIRCUIT-SAT

PCP

NIZK Circuit-SAT

Circuit-SAT

PCP

Families of Fast Elliptic Curves from Q-curves

Benjamin Smith

Team GRACE, INRIA Saclay–Ile-de-France

and Laboratoire d'Informatique de l'Ecole polytechnique (LIX)

Batiment Alan Turing, 1 rue Honor'e d'Estienne d'Orves

Campus de l'Ecole polytechnique, 91120 Palaiseau, France

smith@lix.polytechnique.fr

Abstract. We construct new families of elliptic curves over \mathbb{F}_{p^2} with efficiently computable endomorphisms, which can be used to accelerate elliptic curve-based cryptosystems in the same way as Gallant–Lambert–Vanstone (GLV) and Galbraith–Lin–Scott (GLS) endomorphisms. Our construction is based on reducing quadratic Q-curves (curves defined over quadratic number fields, without complex multiplication, but with isogenies to their Galois conjugates) modulo inert primes. As a first application of the general theory we construct, for every prime $p > 3$, two one-parameter families of elliptic curves over \mathbb{F}_{p^2} equipped with endomorphisms that are faster than doubling. Like GLS (which appears as a degenerate case of our construction), we offer the advantage over GLV of selecting from a much wider range of curves, and thus finding secure group orders when p is fixed. Unlike GLS, we also offer the possibility of constructing twist-secure curves. Among our examples are prime-order curves over \mathbb{F}_{p^2} , equipped with fast endomorphisms, and with almost-prime-order twists, for the particularly efficient primes $p = 2^{127} - 1$ and $p = 2^{255} - 19$.

Keywords: Elliptic curve cryptography, endomorphisms, GLV, GLS, exponentiation, scalar multiplication, Q-curves

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

Four-Dimensional GLV via the Weil Restriction

Aurore Guillevic^{1,2} and Sorina Ionica¹

¹ Crypto Team – DI – Ecole Normale Supérieure

45 rue d'Ulm – 75230 Paris Cedex 05 – France

² Laboratoire Chiffre – Thales Communications and Security

4 Avenue des Louvresses – 92622 Gennevilliers Cedex – France

aurore.guillevic@ens.fr, sorina.ionica@m4x.org

Abstract. The Gallant-Lambert-Vanstone (GLV) algorithm uses efficiently computable endomorphisms to accelerate the computation of scalar multiplication of points on an abelian variety. Freeman and Satoh proposed for cryptographic use two families of genus 2 curves defined over F_p which have the property that the corresponding Jacobians are $(2, 2)$ -isogenous over an extension field to a product of elliptic curves defined over F_{p^2} . We exploit the relationship between the endomorphism rings of isogenous abelian varieties to exhibit efficiently computable endomorphisms on both the genus 2 Jacobian and the elliptic curve. This leads to a four-dimensional GLV method on Freeman and Satoh's Jacobians and on two new families of elliptic curves defined over F_{p^2} .

Keywords: GLV method, elliptic curves, genus 2 curves, isogenies

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

GLV

$$Fp$$

(2, 2)

2

Sato

$$\mathbb{F}p^2$$

2

Discrete Gaussian Leftover Hash Lemma over Infinite Domains

Shweta Agrawal¹, Craig Gentry², Shai Halevi², and Amit Sahai¹

¹ UCLA

² IBM Research

Abstract. The classic Leftover Hash Lemma (LHL) is often used to argue that certain distributions arising from modular subset-sums are close to uniform over their finite domain. Though very powerful, the applicability of the leftover hash lemma to lattice based cryptography is limited for two reasons. First, typically the distributions we care about in lattice-based cryptography are discrete Gaussians, not uniform. Second, the elements chosen from these discrete Gaussian distributions lie in an infinite domain: a lattice rather than a finite field.

In this work we prove a “lattice world” analog of LHL over infinite domains, proving that certain “generalized subset sum” distributions are statistically close to well behaved discrete Gaussian distributions, even without any modular reduction.

Specifically, given many vectors $\{x_i\}_{i=1}^m$ from some lattice $L \subseteq \mathbb{R}^n$, we analyze the

probability distribution $\sum_{i=1}^m z_i x_i$ where the integer vector $z \in \mathbb{Z}^m$ is chosen from a

discrete Gaussian distribution. We show that when the x_i ’s are “random enough” and the Gaussian from which the z ’s are chosen is “wide enough”, then the resulting distribution is statistically close to a near-spherical discrete Gaussian over the lattice L . Beyond being interesting in its own right, this “lattice-world” analog of LHL has applications for the new construction of multilinear maps [5], where it is used to sample Discrete Gaussians obliviously. Specifically, given encoding of the x_i ’s, it is used to produce an encoding of a near-spherical Gaussian distribution over the lattice. We believe that our new lemma will have other applications, and sketch some plausible ones in this work.

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

Lemmaover

$$\{x_i\}_{i=1}^m$$

?

$$\sum_{i=1}^m z_i x_i$$

New Insight into the Isomorphism of Polynomial Problem IP1S and Its Use in Cryptography

Gilles Macario-Rat¹, Jerome Plut², and Henri Gilbert²

¹ Orange Labs

38–40, rue du General Leclerc, 92794 Issy-les-Moulineaux Cedex 9, France gilles.macariorat@orange.com

² ANSSI,

51 Boulevard de la Tour-Maubourg, 75007 Paris, France

{henri.gilbert, jerome.plut}@ssi.gouv.fr

Abstract. This paper investigates the mathematical structure of the “Isomorphism of Polynomial with One Secret” problem (IP1S). Our purpose is to understand why for practical parameter values of IP1S most random instances are easily solvable (as first observed by Bouillaguet et al.). We show that the structure of the equations is directly linked to a matrix derived from the polar form of the polynomials. We prove that in the likely case where this matrix is cyclic, the problem can be solved in polynomial time-using an algorithm that unlike previous solving techniques is not based upon Grobner basis computation.

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

IP1S

“ ” (IP1S)

IP1S (

Bouillaguet)

Grobner

Constructing Confidential Channels from Authenticated Channels—Public-Key Encryption

Revisited

Sandro Coretti, Ueli Maurer, and Björn Tackmann

Department of Computer Science, ETH Zürich, Switzerland

{coretti,maurer,bjoernt}@inf.ethz.ch

Abstract. The security of public-key encryption (PKE), a widely-used cryptographic primitive, has received much attention in the cryptology literature. Many security notions for PKE have been proposed, including several versions of CPA-security, CCA-security, and non-malleability. These security notions are usually defined via a game that no efficient adversary can win with non-negligible probability or advantage.

If a PKE scheme is used in a larger protocol, then the security of this protocol is proved by showing a reduction of breaking a certain security property of the PKE scheme to breaking the security of the protocol. A major problem is that each protocol requires in principle its own tailormade security reduction. Moreover, which security notion of the PKE scheme should be used in a given context is a priori not evident; the employed games model the use of the scheme abstractly through oracle access to its algorithms, and the sufficiency for specific applications is neither explicitly stated nor proven.

In this paper we propose a new approach to investigating the application of PKE, based on the constructive cryptography framework [24,25]. The basic use of PKE is to enable confidential communication from a sender A to a receiver B, assuming A is in possession of B's public key. One can distinguish two relevant cases: The (non-confidential) communication channel from A to B can be authenticated (e.g., because messages are signed) or non-authenticated. The application of PKE is shown to provide the construction of a secure channel from A to B from two (assumed) authenticated channels, one in each direction, or, alternatively, if the channel from A to B is completely insecure, the construction of a confidential channel without authenticity. Composition then means that the assumed channels can either be physically realized or can themselves be constructed cryptographically, and also that the resulting channels can directly be used in any applications that require such a channel. The composition theorem of constructive cryptography guarantees the soundness of this approach, which eliminates the need for separate reduction proofs.

We also revisit several popular game-based security notions (and variants thereof) and give them a constructive semantics by demonstrating which type of construction is achieved by a PKE scheme satisfying which notion. In particular, the necessary and sufficient security notions for the above two constructions to work are CPA-security and a variant of CCA security, respectively.

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

PKE

CPA

CCA

PKE

PKE

PKE

PKE

PKE

A

B

A

B

(

)

A

B

(

)

PKE

(

)

A B

A B

PKE

CPA

CCA

Reset Indifferentiability and Its Consequences

Paul Baecher¹, Christina Brzuska², and Arno Mittelbach¹

¹ Darmstadt University of Technology, Germany

² Tel-Aviv University, Israel

Abstract. The equivalence of the random-oracle model and the ideal cipher model has been studied in a long series of results. Holenstein, Kunzler, and Tessaro (STOC, 2011) have recently completed the picture positively, assuming that, roughly speaking, equivalence is indifferentiability from each other. However, under the stronger notion of reset indifferentiability this picture changes significantly, as Demay et al. (EUROCRYPT, 2013) and Luykx et al. (ePrint, 2012) demonstrate.

We complement these latter works in several ways. First, we show that any simulator satisfying the reset indifferentiability notion must be stateless and pseudo deterministic. Using this characterization we show that, with respect to reset indifferentiability, two ideal models are either equivalent or incomparable, that is, a model cannot be strictly stronger than the other model. In the case of the random-oracle model and the ideal-cipher model, this implies that the two are incomparable. Finally, we examine weaker notions of reset indifferentiability that, while not being able to allow composition in general, allow composition for a large class of multi-stage games. Here we show that the seemingly much weaker notion of 1-reset indifferentiability proposed by Luykx et al. is equivalent to reset indifferentiability. Hence, the impossibility of coming up with a reset-indifferentiable construction transfers to the setting where only one reset is permitted, thereby re-opening the quest for an achievable and meaningful notion in between the two variants.

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

Holenstein,
Kunzler, and Tessaro (STOC, 2011)

Demay Luykx

,

Luykx

1

Computational Fuzzy Extractors

Benjamin Fuller¹, Xianrui Meng², and Leonid Reyzin²

¹Boston University and MIT Lincoln Laboratory

²Boston University

Abstract. Fuzzy extractors derive strong keys from noisy sources. Their security is defined information-theoretically, which limits the length of the derived key, sometimes making it too short to be useful. We ask whether it is possible to obtain longer keys by considering computational security, and show the following.

– Negative Result: Noise tolerance in fuzzy extractors is usually achieved using an information reconciliation component called a “se-cure sketch.” The security of this component, which directly affects the length of the resulting key, is subject to lower bounds from coding theory. We show that, even when defined computationally, secure sketches are still subject to lower bounds from coding theory. Specifically, we consider two computational relaxations of the information-theoretic security requirement of secure sketches, using conditional HILL entropy and unpredictability entropy. For both cases we show that computational secure sketches cannot outperform the best information-theoretic secure sketches in the case of high-entropy Hamming metric sources.

– Positive Result: We show that the negative result can be overcome by analyzing computational fuzzy extractors directly. Namely, we show how to build a computational fuzzy extractor whose output key length equals the entropy of the source (this is impossible in the information-theoretic setting). Our construction is based on the hardness of the Learning with Errors (LWE) problem, and is secure when the noisy source is uniform or symbol-fixing (that is, each dimension is either uniform or fixed). As part of the security proof, we show a result of independent interest, namely that the decision version of LWE is secure even when a small number of dimensions has no error.

Key words: Fuzzy extractors, secure sketches, key derivation, Learning with Errors, error-correcting codes, computational entropy, randomness

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

HILL

LWE

LWE

Efficient One-Way Secret-Key Agreement and Private Channel Coding via Polarization

Joseph M. Renes, Renato Renner, and David Sutter

Institute for Theoretical Physics,

ETH Zurich, Switzerland

{renes, renner, suttetdav}@phys.ethz.ch

Abstract. We introduce explicit schemes based on the polarization phenomenon for the task of secret-key agreement from common information and one-way public communication as well as for the task of private channel coding. Our protocols are distinct from previously known schemes in that they combine two practically relevant properties: they achieve the ultimate rate—defined with respect to a strong secrecy condition—and their complexity is essentially linear in the blocklength. However, we are not able to give an efficient algorithm for code construction.

Keywords: One-way secret-key agreement, private channel coding, one-way secret-key rate, secrecy capacity, wiretap channel scenario, more capable, less noisy, degraded, polarization phenomenon, polar codes, practically efficient, strongly secure

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

Polar

SPHF-Friendly Non-interactive Commitments

Michel Abdalla¹, Fabrice Benhamouda¹, Olivier Blazy², Céline Chevalier³,
and David Pointcheval¹

¹ École Normale Supérieure, CNRS-INRIA, Paris, France

² Ruhr-Universität Bochum, Germany

³ Université Panthéon-Assas, Paris, France

Abstract. In 2009, Abdalla et al. proposed a reasonably practical password-authenticated key exchange (PAKE) secure against adaptive adversaries in the universal composability (UC) framework. It exploited the Canetti-Fischlin methodology for commitments and the Cramer-Shoup smooth projective hash functions (SPHFs), following the Gennaro-Lindell approach for PAKE. In this paper, we revisit the notion of non-interactive commitments, with a new formalism that implies UC security. In addition, we provide a quite efficient instantiation. We then extend our formalism to SPHF-friendly commitments. We thereafter show that it allows a blackbox application to one-round PAKE and oblivious transfer (OT), still secure in the UC framework against adaptive adversaries, assuming reliable erasures and a single global common reference string, even for multiple sessions. Our instantiations are more efficient than the Abdalla et al. PAKE in Crypto 2009 and the recent OT protocol proposed by Choi et al. in PKC 2013. Furthermore, the new PAKE instantiation is the first one-round scheme achieving UC security against adaptive adversaries.

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

SPHF

2009 Abdalla PAKE
UC
Canetti-Fischlin Cramer-Shoup SPHF
PAKE Gennaro-Lindell
UC
SPHF
1 PAKE
OT UC
Abdalla 2009
Choi 2013 PKC OT
PAKE 1-
UC

Self-Updatable Encryption: Time Constrained Access Control with Hidden Attributes and Better Efficiency

Kwangsue Lee¹, Seung Geol Choi², Dong Hoon Lee¹,

Jong Hwan Park^{1,3}, and Moti Yung⁴

¹CIST, Korea University, Korea

²US Naval Academy, USA

³Sangmyung University, Korea

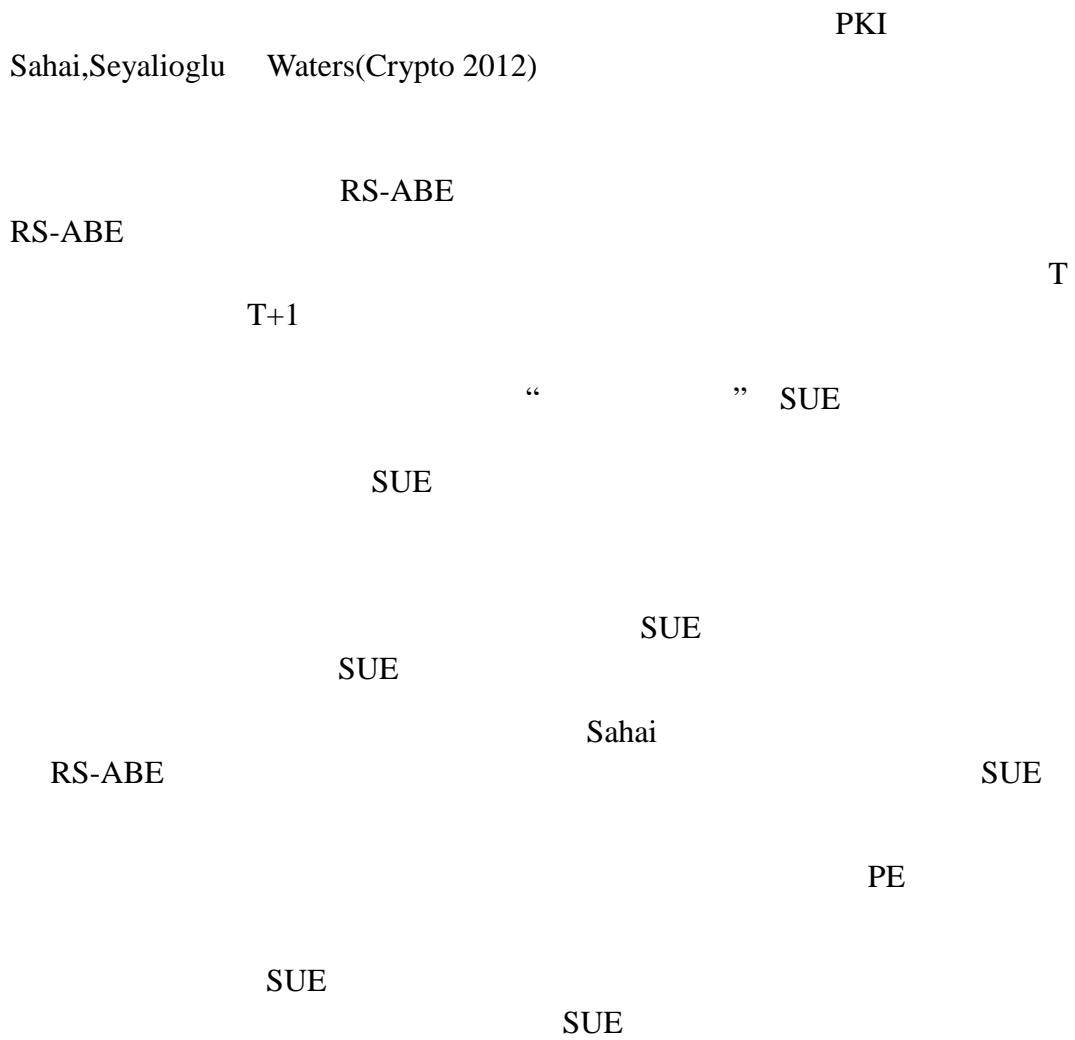
⁴Google Inc. and Columbia University, USA

Abstract. Revocation and key evolving paradigms are central issues in cryptography, and in PKI in particular. A novel concern related to these areas was raised in the recent work of Sahai, Seyalioglu, and Waters (Crypto 2012) who noticed that revoking past keys should at times (e.g., the scenario of cloud storage) be accompanied by revocation of past ciphertexts (to prevent unread ciphertexts from being read by revoked users). They introduced revocable-storage attribute-based encryption (RS-ABE) as a good access control mechanism for cloud storage. RSABE protects against the revoked users not only the future data by supporting key-revocation but also the past data by supporting ciphertext-update, through which a ciphertext at time T can be updated to a new ciphertext at time $T+1$ using only the public key. Motivated by this pioneering work, we ask whether it is possible to have a modular approach, which includes a primitive for time managed ciphertext update as a primitive. We call encryption which supports this primitive a “self-updatable encryption” (SUE). We then suggest a modular cryptosystems design methodology based on three sub-components: a primary encryption scheme, a key-revocation mechanism, and a time-evolution mechanism which controls the ciphertext self-updating via an SUE method, coordinated with the revocation (when needed). Our goal in this is to allow the self-updating ciphertext component to take part in the design of new and improved cryptosystems and protocols in a flexible fashion. Specifically, we achieve the following results:

- We first introduce a new cryptographic primitive called self-updatable encryption (SUE), realizing a time-evolution mechanism. We also construct an SUE scheme and prove its full security under static assumptions.
- Following our modular approach, we present a new RS-ABE scheme with shorter ciphertexts than that of Sahai et al. and prove its security. The length efficiency is mainly due to our SUE scheme and the underlying modularity.
- We apply our approach to predicate encryption (PE) supporting attribute-hiding property, and obtain a revocable-storage PE (RS-PE) scheme that is selectively-secure.
- We further demonstrate that SUE is of independent interest, by showing it can be used for timed-release encryption (and its applications), and for augmenting key-insulated encryption with forward-secure storage.

Keywords: Public-key encryption, Attribute-based encryption, Predicate encryption, Self-updatable encryption, Revocation, Key evolving systems, Cloud storage

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)



Function-Private Subspace-Membership Encryption and Its Applications

Dan Boneh¹, Ananth Raghunathan¹, and Gil Segev²

¹Stanford University

{dabo,ananthr}@cs.stanford.edu

²Hebrew University

segev@cs.huji.ac.il

Abstract. Boneh, Raghunathan, and Segev (CRYPTO '13) have recently put forward the notion of function privacy and applied it to identity-based encryption, motivated by the need for providing predicate privacy in public-key searchable encryption. Intuitively, their notion asks that decryption keys reveal essentially no information on their corresponding identities, beyond the absolute minimum necessary. While Boneh et al. showed how to construct function-private identity-based encryption (which implies predicate-private encrypted keyword search), searchable encryption typically requires a richer set of predicates. In this paper we significantly extend the function privacy framework. First, we consider the notion of subspace-membership encryption, a generalization of inner-product encryption, and formalize a meaningful and realistic notion for capturing its function privacy. Then, we present a generic construction of a function-private subspace-membership encryption scheme based on any inner-product encryption scheme. This is the first generic construction that yields a function-private encryption scheme based on a non-function-private one.

Finally, we present various applications of function-private subspace-membership encryption. Among our applications, we significantly improve the function privacy of the identity-based encryption schemes of Boneh et al.: whereas their schemes are function private only for identities that are highly unpredictable (with min-entropy of at least $\lambda + \omega(\log \lambda)$ bits, where λ is the security parameter), we obtain function-private schemes assuming only the minimal required unpredictability (i.e., min-entropy of only $\omega(\log \lambda)$ bits). This improvement offers a much more realistic function privacy guarantee.

Keywords: Function privacy, functional encryption

Source: Asiacypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

Boneh,Raghunathan

Segev

Boneh

,

,

Boneh

$\lambda+\omega(\log\lambda)$

λ

$\omega(\log\lambda)$

Random Projections, Graph Sparsification, and Differential Privacy

Jalaj Upadhyay

David R. Cheriton School of Computer Science

University of Waterloo,

200, University Avenue West

Waterloo, ON, Canada–N2L 3G1

jkupadhy@cs.uwaterloo.ca

Abstract. This paper initiates the study of preserving differential privacy (DP) when the data-set is sparse. We study the problem of constructing efficient sanitizer that preserves DP and guarantees high utility for answering cut-queries on graphs. The main motivation for studying sparse graphs arises from the empirical evidences that social networking sites are sparse graphs. We also motivate and advocate the necessity to include the efficiency of sanitizers, in addition to the utility guarantee, if one wishes to have a practical deployment of privacy preserving sanitizers.

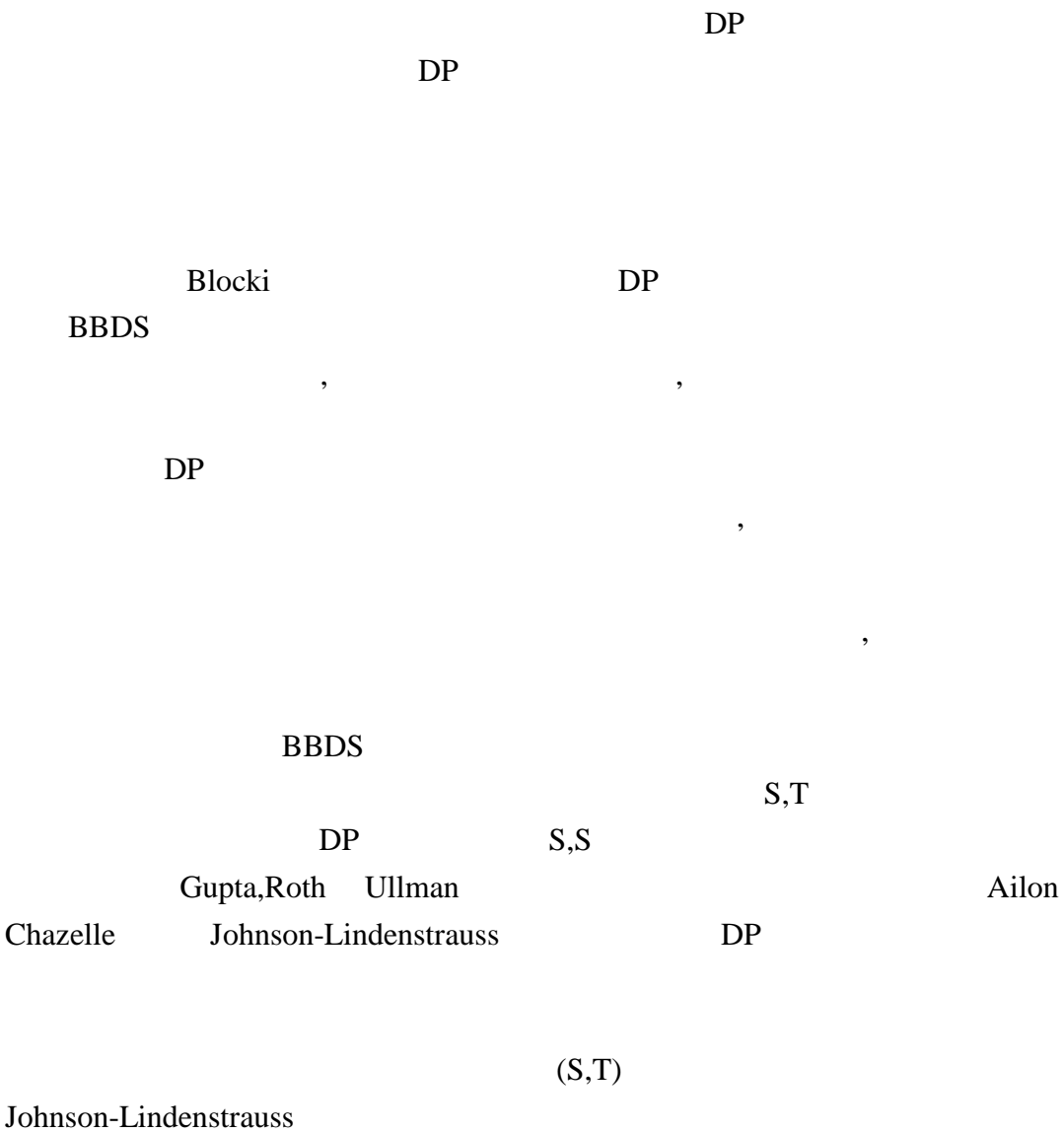
We show that the technique of Blocki et al. can be adapted to preserve DP for answering cut-queries on sparse graphs, with an asymptotically efficient sanitizer than BBDS. We use this as the base technique to construct an efficient sanitizer for arbitrary graphs. In particular, we use a preconditioning step that preserves the spectral properties (and therefore, size of any cut is preserved), and then apply our basic sanitizer. We first prove that our sanitizer preserves DP for graphs with high conductance. We then carefully compose our basic technique with the modified sanitizer to prove the result for arbitrary graphs. In certain sense, our approach is complementary to the Randomized sanitization for answering cut queries: we use graph sparsification, while Randomized sanitization uses graph densification.

Our sanitizers almost achieves the best of both the worlds with the same privacy guarantee, i.e., it is almost as efficient as the most efficient sanitizer and it has utility guarantee almost as strong as the utility guarantee of the best sanitization algorithm.

We also make some progress in answering few open problems by BBDS. We make a combinatorial observation that allows us to argue that the sanitized graph can also answer (S,T)-cut queries with same asymptotic efficiency, utility, and DP guarantee as our sanitization algorithm for S, S-cuts. Moreover, we achieve a better utility guarantee than Gupta, Roth, and Ullman. We give further optimization by showing that fast Johnson-Lindenstrauss transform of Ailon and Chazelle also preserves DP.

Keywords: Differential privacy, Graph sparsification, (S,T)-cut queries, Fast Johnson-Lindenstrauss transform

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)



Notions of Black-Box Reductions, Revisited

Paul Baecher¹, Christina Brzuska², and Marc Fischlin¹

Department of Computer Science, Darmstadt University of Technology, Germany

² Tel-Aviv University, Israel

Abstract. Reductions are the common technique to prove security of cryptographic constructions based on a primitive. They take an allegedly successful adversary against the construction and turn it into a successful adversary against the underlying primitive. To a large extent, these reductions are black-box in the sense that they consider the primitive and/or the adversary against the construction only via the input-output behavior, but do not depend on internals like the code of the primitive or of the adversary. Reingold, Trevisan, and Vadhan (TCC, 2004) provided a widely adopted framework, called the RTV framework from hereon, to classify and relate different notions of black-box reductions.

Having precise notions for such reductions is very important when it comes to black-box separations, where one shows that black-box reductions cannot exist. An impossibility result, which clearly specifies the type of reduction it rules out, enables us to identify the potential leverages to bypass the separation. We acknowledge this by extending the RTV framework in several respects using a more fine-grained approach. First, we capture a type of reduction—frequently ruled out by so-called meta-reductions—which escapes the RTV framework so far. Second, we consider notions that are “almost black-box”, i.e., where the reduction receives additional information about the adversary, such as its success probability. Third, we distinguish explicitly between efficient and inefficient primitives and adversaries, allowing us to determine how relativizing reductions in the sense of Impagliazzo and Rudich (STOC, 1989) fit into the picture.

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

Reingold, Trevisan	Vadhan	2004	TCC
			RTV

RTV

RTV

Impagliazzo Rudich (STOC, 1989)

Adaptive and Concurrent Secure Computation from New Adaptive, Non-malleable Commitments

Dana Dachman-Soled^{1, *} Tal Malkin² Mariana Raykova^{3, **}

and Muthuramakrishnan Venkitasubramaniam⁴

¹ University of Maryland, College Park, MD 20742, USA

danadach@ece.umd.edu

² Columbia University, New York, NY 10027, USA

tal@cs.columbia.edu

³ IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA, and

SRI, Menlo Park, CA 94025, USA

mariana@cs.columbia.edu

⁴ University of Rochester, Rochester, NY 14627, USA

muthuv@cs.rochester.edu

Abstract. We present a unified approach for obtaining general secure computation that achieves adaptive-Universally Composable (UC)-security. Using our approach we essentially obtain all previous results on adaptive concurrent secure computation, both in relaxed models (e.g., quasi-polynomial time simulation), as well as trusted setup models (e.g., the CRS model, the imperfect CRS model). This provides conceptual simplicity and insight into what is required for adaptive and concurrent security, as well as yielding improvements to set-up assumptions and/or computational assumptions in known models. Additionally, we provide the first constructions of concurrent secure computation protocols that are adaptively secure in the timing model, and the non-uniform simulation model. As a corollary we also obtain the first adaptively secure multiparty computation protocol in the plain model that is secure under bounded-concurrency.

Conceptually, our approach can be viewed as an adaptive analogue to the recent work of Lin, Pass and Venkitasubramaniam [STOC '09], who considered only non-adaptive adversaries. Their main insight was that the non-malleability requirement could be decoupled from the simulation requirement to achieve UC security. A main conceptual contribution of this work is, quite surprisingly, that it is still the case even when considering adaptive security.

A key element in our construction is a commitment scheme that satisfies a strong definition of non-malleability. Our new primitive of concurrent equivocal non-malleable commitments, intuitively, guarantees that even when a man-in-the-middle adversary observes concurrent equivocal commitments and decommitments, the binding property of the commitments continues to hold for commitments made by the adversary. This definition is stronger than previous ones, and may be of independent interest. Previous constructions that satisfy our definition have been constructed in setup models, but either require existence of stronger encryption schemes such as CCA-secure encryption or require independent “trapdoors” provided by the setup for every pair of parties to ensure non-malleability. A main technical contribution of this work is to provide a construction that eliminates these requirements and requires only a single trapdoor.

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

UC -

CRS

CRS

/

-

Lin Pass Venkitasubramaniam [STOC

‘09]

UC-

CCA-

“ ”

Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES²

Itai Dinur¹, Orr Dunkelman^{1,2,*}, Nathan Keller^{1,3,**}, and Adi Shamir¹

¹ Computer Science department, The Weizmann Institute, Rehovot, Israel

² Computer Science Department, University of Haifa, Israel

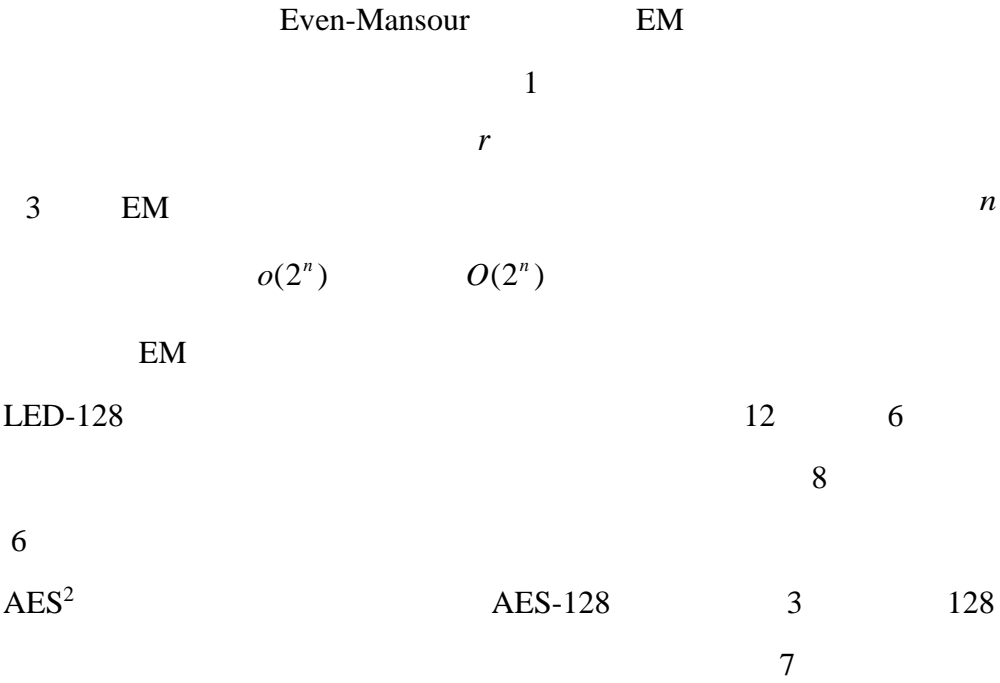
³ Department of Mathematics, Bar-Ilan University, Israel

Abstract. The Even-Mansour (EM) encryption scheme received a lot of attention in the last couple of years due to its exceptional simplicity and tight security proofs. The original 1-round construction was naturally generalized into r -round structures with one key, two alternating keys, and completely independent keys. In this paper we describe the first key recovery attack on the one-key 3-round version of EM which is asymptotically faster than exhaustive search (in the sense that its running time is $o(2^n)$ rather than $O(2^n)$ for an n -bit key). We then use the new cryptanalytic techniques in order to improve the best known attacks on several concrete EM-like schemes. In the case of LED-128, the best previously known attack could only be applied to 6 of its 12 steps. In this paper we develop a new attack which increases the number of attacked steps to 8, is slightly faster than the previous attack on 6 steps, and uses about a thousand times less data. Finally, we describe the first attack on the full AES²(which uses two complete AES-128 encryptions and three independent 128-bit keys, and looks exceptionally strong) which is about 7 times faster than a standard meet-in-the-middle attack, thus violating its security claim.

Keywords: Cryptanalysis, key recovery attacks, iterated Even-Mansour, LED encryption scheme, AES2 encryption scheme

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

3 Even-Mansour 8 LED-128 AES²



Even-Mansour LED AES²

Key Difference Invariant Bias in Block Ciphers

Andrey Bogdanov¹, and Christina Boura¹, Vincent Rijmen²,

Meiqin Wang³, LongWen³, Jingyuan Zhao³,

¹ Technical University of Denmark, Denmark

² KU Leuven ESAT/SCD/COSIC and iMinds, Belgium

³ Shandong University, Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China

Abstract. In this paper, we reveal a fundamental property of block ciphers: There can exist linear approximations such that their biases ε are deterministically invariant under key difference. This behaviour is highly unlikely to occur in idealized ciphers but persists, for instance, in 5-round AES. Interestingly, the property of key difference invariant bias is independent of the bias value ε itself and only depends on the form of linear characteristics comprising the linear approximation in question as well as on the key schedule of the cipher.

We propose a statistical distinguisher for this property and turn it into an key recovery. As an illustration, we apply our novel cryptanalytic technique to mount related-key attacks on two recent block ciphers —LBlock and TWINE. In these cases, we break 2 and 3 more rounds, respectively, than the best previous attacks.

Keywords: block ciphers, key difference invariant bias, linear crypt-analysis, linear hull, key-alternating ciphers, LBlock, TWINE

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

ϵ

5 AES

ϵ

-LBlock TWINE

2 3

LBlock TWINE

Leaked-State-Forgery Attack against the Authenticated Encryption

Algorithm ALE

Shengbao Wu^{1,3}, Hongjun Wu², Tao Huang², Mingsheng Wang⁴,
and Wenling Wu¹

¹Trusted Computing and Information Assurance Laboratory, Institute of Software,
Chinese Academy of Sciences, Beijing 100190, P.O. Box 8718, China

²Division of Mathematical Sciences, School of Physical and Mathematical Sciences,
Nanyang Technological University, Singapore

³Graduate School of Chinese Academy of Sciences, Beijing 100190, China

⁴State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China

{wushengbao, wwl}@tca.iscas.ac.cn

{wuhj, huangtao}@ntu.edu.sg

wangmingsheng@iie.ac.cn

Abstract. ALE is a new authenticated encryption algorithm published at FSE 2013. The authentication component of ALE is based on the strong Pelican MAC, and the authentication security of ALE is claimed to be 128-bit. In this paper, we propose the leaked-state-forgery attack (LSFA) against ALE by exploiting the state information leaked from the encryption of ALE. The LSFA is a new type of differential cryptanalysis in which part of the state information is known and exploited to improve the differential probability. Our attack shows that the authentication security of ALE is only 97-bit. And the results may be further improved to around 93-bit if the whitening key layer is removed. We implemented our attacks against a small version of ALE (using 64-bit block size instead of 128-bit block size). The experimental results match well with the theoretical results.

Keywords: authenticated encryption, forgery attack, ALE

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

ALE

2013 ALE FSE ALE
Pelican MAC ALE 128
ALE LSFA ALE
LSFA
ALE 97
93 ALE 64
128

ALE

A Modular Framework for Building Variable-Input-Length Tweakable Ciphers

Thomas Shrimpton and R. Seth Terashima
Dept. of Computer Science, Portland State University
{teshrim, seth}@cs.pdx.edu

Abstract. We present the Protected-IV construction (PIV) a simple, modular method for building variable-input-length tweakable ciphers. At our level of abstraction, many interesting design opportunities surface. For example, an obvious pathway to building beyond birthday-bound secure tweakable ciphers with performance competitive with existing birthday-bound-limited constructions. As part of our design space exploration, we give two fully instantiated PIV constructions, TCT_1 and TCT_2 ; the latter is fast and has beyond birthday-bound security, the former is faster and has birthday-bound security. Finally, we consider a generic method for turning a VIL tweakable cipher (like PIV) into an authenticated encryption scheme that admits associated data, can with-stand nonce-misuse, and allows for multiple decryption error messages.

Key words: tweakable blockciphers, beyond-birthday-bound security, authenticated encryption, associated data, full-disk encryption

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

IV

PIV

PIV

TCT1

TCT2

VIL

PIV

-

Parallelizable and Authenticated Online Ciphers

Elena Andreeva^{1,2}, Andrey Bogdanov³, Atul Luykx^{1,2}, Bart Mennink^{1,2},
Elmar Tischhauser^{1,2}, and Kan Yasuda^{1,4}

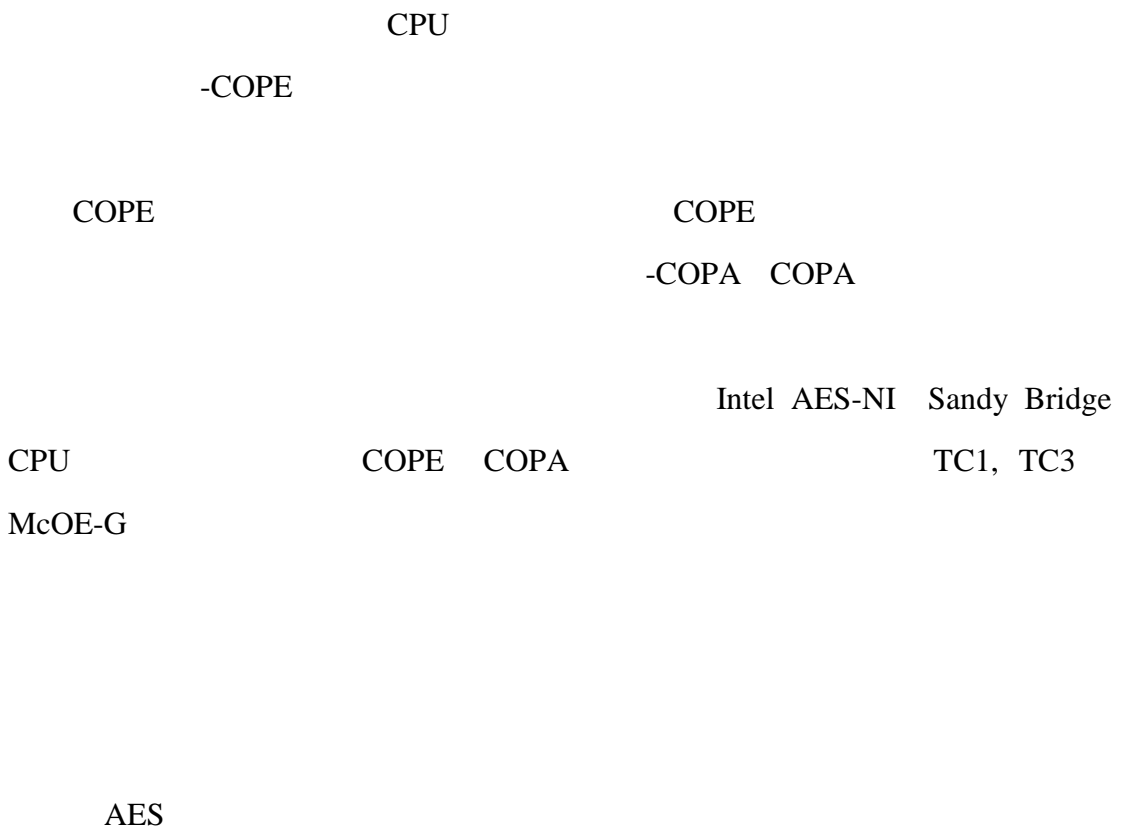
¹ Department of Electrical Engineering, ESAT/COSIC, KU Leuven, Belgium

² iMinds, Belgium

³ Department of Mathematics, Technical University of Denmark, Denmark

⁴ NTT Secure Platform Laboratories, Japan

Abstract. Online ciphers encrypt an arbitrary number of plaintext blocks and output ciphertext blocks which only depend on the preceding plaintext blocks. All online ciphers proposed so far are essentially serial, which significantly limits their performance on parallel architectures such as modern general-purpose CPUs or dedicated hardware. We propose the first parallelizable online cipher, COPE. It performs two calls to the underlying block cipher per plaintext block and is fully parallelizable in



How to Construct an Ideal Cipher from a Small Set of Public Permutations

Rodolphe Lampe¹ and Yannick Seurin²

¹ University of Versailles, France

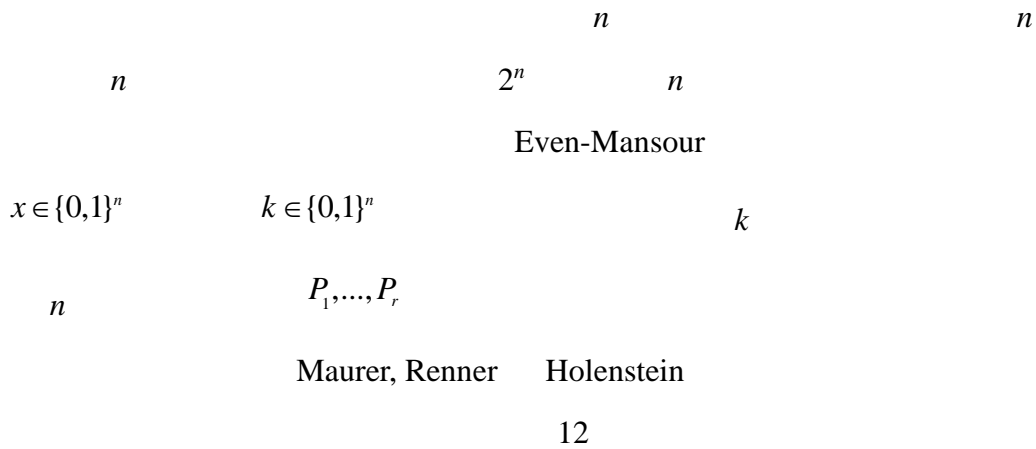
² ANSSI, Paris, France

rodolphe.lampe@gmail.com, yannick.seurin@m4x.org

Abstract. We show how to construct an ideal cipher with n -bit blocks and n -bit keys (*i.e.* a set of 2^n public n -bit permutations) from a small constant number of n -bit random public permutations. The construction that we consider is the *single-key iterated Even-Mansour cipher*, which encrypts a plaintext $x \in \{0,1\}^n$ under a key $k \in \{0,1\}^n$ by alternatively xoring the key k and applying independent random public n -bit permutations P_1, \dots, P_r (this construction is also named a *key alternating cipher*). We analyze this construction in the plain indistinguishability framework of Maurer, Renner, and Holenstein (TCC 2004), and show that twelve rounds are sufficient to achieve indistinguishability from an ideal cipher. We also show that four rounds are necessary by exhibiting attacks for three rounds or less.

Keywords: block cipher, ideal cipher, iterated Even-Mansour cipher, key-alternating cipher, indistinguishability

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)



Generic Key Recovery Attack on Feistel Scheme

Takanori Isobe and Kyoji Shibutani

Sony Corporation

1-7-1 Konan, Minato-ku, Tokyo 108-0075, Japan

{Takanori.Isobe,Kyoji.Shibutani}@jp.sony.com

Abstract. We propose new generic key recovery attacks on Feistel-type block ciphers. The proposed attack is based on the all subkeys recovery approach presented in SAC 2012, which determines all subkeys instead of the master key. This enables us to construct a key recovery attack without taking into account a key scheduling function. With our advanced techniques, we apply several key recovery attacks to Feistel-type block ciphers. For instance, we show 8-, 9- and 11-round key recovery attacks on n -bit Feistel ciphers with $2n$ -bit key employing random keyed F-functions, random F-functions, and SP-type F-functions, respectively. Moreover, thanks to the meet-in-the-middle approach, our attack leads to *low-data complexity*. To demonstrate the usefulness of our approach, we show a key recovery attack on the 8-round reduced CAST-128, which is the best attack with respect to the number of attacked rounds. Since our approach derives the lower bounds on the numbers of rounds to be secure under the single secret key setting, it can be considered that we unveil the limitation of designing an efficient block cipher by a Feistel scheme such as a low-latency cipher.

Keywords: block cipher, key scheduling function, all-subkeys-recovery attack, meet-in-the-middle attack, key recovery attack, low-data complexity attack

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

Feistel

Feistel

SAC2012

Feistel

F

F

SP F

$2n$

n

Feistel

8

9

11

CAST-128

8

Feistel

Dose My Device Leak Information? An a priori Statistical Power Analysis of Leakage Detection Tests

Luke Mather¹, Elisabeth Oswald², Joe Bandenburg³ and Marcin Wojcik⁴

¹ University of Bristol, Department of Computer Science,

Merchant Venturers Building, Woodland Road, BS8 1UB Bristol UK

^{1,2,3,4} {Luke.Mather, Elisabeth.Oswald, Marcin.Cojcik}@bris.ac.uk,

joe@bandenburg.com

Abstract. The development of a leakage detection testing methodology for the side-channel resistance of cryptographic devices is an issue that has received recent focus from standardisation bodies such as NIST. Statistical techniques such as hypothesis and significance testing appear to be ideally suited for this purpose. In this work we evaluate the candidacy of three such detection tests: a t-test proposed by Cryptography Research Inc., and two mutual information-based tests, one in which data is treated as continuous and one as discrete. Our evaluation investigates three particular areas: statistical power, the effectiveness of multiplicity corrections, and computational complexity. To facilitate a fair comparison we conduct a novel apriori statistical power analysis of the three tests in the context of side-channel analysis, finding surprisingly that the continuous mutual information and t-tests exhibit similar levels of power. We also show how the inherently parallel nature of the continuous mutual information test can be leveraged to reduce a large computational cost to insignificant levels. To complement the apriori statistical power analysis we include two real-world case studies of the tests applied to software and hardware implementations of the AES.

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

NIST

t

t

AES

90

/

CMOS

350 130 90

SCARE of Secret Ciphers with SPN Structure

Matthieu Rivain¹ and Thomas Roche²

¹ CryptoExperts, France

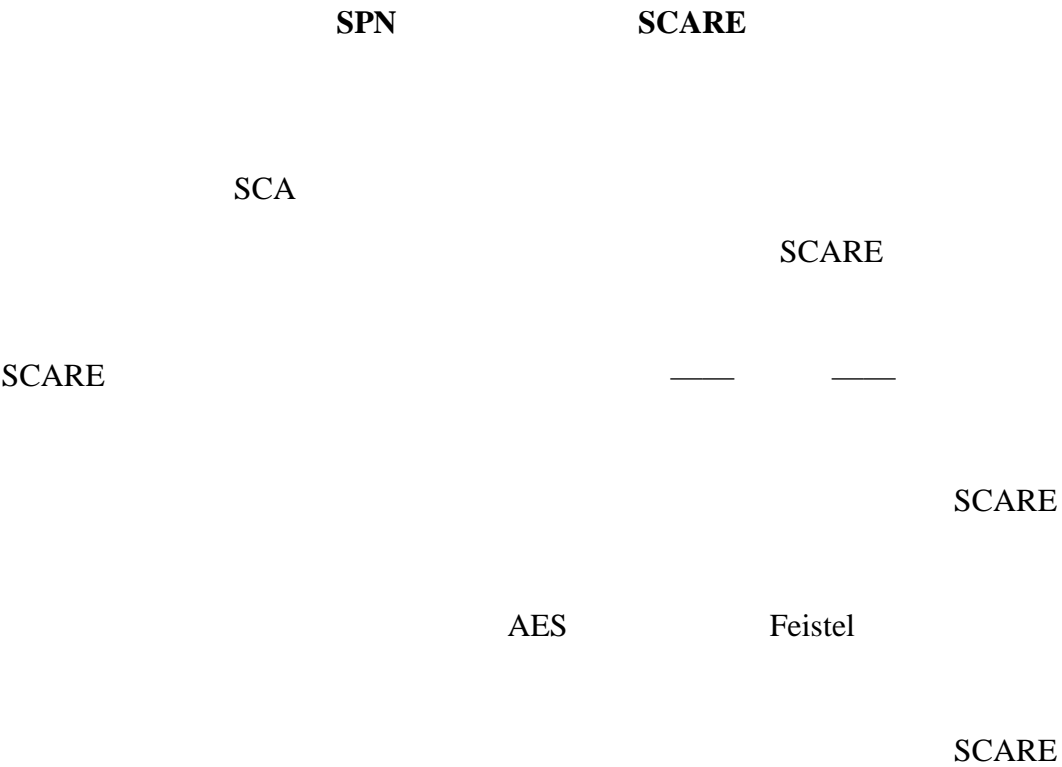
matthieu.rivain@cryptoexperts.com

² ANSSI, France

thomas.roche@ssi.gouv.fr

Abstract. Side-Channel Analysis (SCA) is commonly used to recover secret keys involved in the implementation of publicly known cryptographic algorithms. On the other hand, Side-Channel Analysis for Reverse Engineering (SCARE) considers an adversary who aims at recovering the secret design of some cryptographic algorithm from its implementation. Most of previously published SCARE attacks enable the recovery of some secret parts of a cipher design--the substitution box(es)--assuming that the rest of the cipher is known. Moreover, these attacks are often based on idealized leakage assumption where the adversary recovers noise-free side-channel information. In this paper, we address these limitations and describe a generic SCARE attack that can recover the full secret design of any iterated block cipher with common structure. Specifically we consider the family of Substitution-Permutation Networks with either a classical structure (as the AES) or with a Feistel structure. Based on a simple and usual assumption on the side-channel leakage we show how to recover all parts of the design of such ciphers. We then relax our assumption and describe a practical SCARE attack that deals with noisy side-channel leakages.

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)



Lattice-Based Group Signatures with Logarithmic Signature Size

Fabien Laguillaumie^{1,3}, Adeline Langlois^{2,3}

Benoît Libert⁴, and Damien Stehle^{2,3}

¹Universite Claude Bernard Lyon 1

²Ecole Normale Supérieure de Lyon

³LIP(U.Lyon,CNRS,ENS Lyon,INRIA,UCBL),

46 Allée d'Italie, 69364 Lyon Cedex 7, France

⁴Technicolor, 975 Avenue des Champs Blancs, 35510 Cesson-sevigne, France

Abstract. Group signatures are cryptographic primitives where users can anonymously sign messages in the name of a population they belong to. Gordon et al. (Asiacrypt 2010) suggested the first realization of group signatures based on lattice assumptions in the random oracle model. A significant drawback of their scheme is its linear signature size in the cardinality N of the group. A recent extension proposed by Camenisch et al. (SCN 2012) suffers from the same overhead. In this paper, we describe the first lattice-based group signature schemes where the signature and public key sizes are essentially logarithmic in N (for any fixed security level). Our basic construction not only satisfies a relaxed definition of anonymity (just like the Gordon et al. system) but readily extends into a fully anonymous group signature (i.e., that resists adversaries equipped with a signature opening oracle). We prove the security of our schemes in the random oracle model under the SIS and LWE assumptions.

Keywords: Lattice-based cryptography, group signatures, anonymity

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

Gordonet Asiacrypt 2010

N

Camenisch (SCN 2012)

N

Gordonet

SIS LWE

The Fiat–Shamir Transformation in a Quantum World

Özgür Dagdelen, Marc Fischlin, and Tommaso Gagliardoni

Technische Universität Darmstadt, Germany

oezguer.dagdelen@cased.de, marc.fischlin@gmail.com,

tommaso@gagliardoni.net

www.cryptoplexity.de

Abstract. The Fiat-Shamir transformation is a famous technique to turn identification schemes into signature schemes. The derived scheme is provably secure in the random-oracle model against classical adversaries. Still, the technique has also been suggested to be used in connection with quantum-immune identification schemes, in order to get quantum-immune signature schemes. However, a recent paper by Boneh et al. (Asiacrypt 2011) has raised the issue that results in the random-oracle model may not be immediately applicable to quantum adversaries, because such adversaries should be allowed to query the random oracle in superposition. It has been unclear if the Fiat-Shamir technique is still secure in this quantum oracle model (QROM).

Here, we discuss that giving proofs for the Fiat-Shamir transformation in the QROM is presumably hard. We show that there cannot be black-box extractors, as long as the underlying quantum-immune identification scheme is secure against active adversaries and the first message of the prover is independent of its witness. Most schemes are of this type. We then discuss that for some schemes one may be able to resurrect the Fiat-Shamir result in the QROM by modifying the underlying protocol first. We discuss in particular a version of the Lyubashevsky scheme which is provably secure in the QROM.

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

Fiat-Shamir

Fiat-Shamir

oracle

Boneh

2011

oracle

Fiat-Shamir

QROM

QROM

Fiat-Shamir


QROM

Fiat-Shamir

QROM

Lyubashevsky

On the Security of One-Witness Blind Signature Schemes

Foteini Baldimtsi and Anna Lysyanskaya 

Department of Computer Science, Brown University, Providence, RI, USA

/foteini,anna/@cs.brown.edu

Abstract. Blind signatures have proved an essential building block for applications that protect privacy while ensuring unforgeability, i.e., electronic cash and electronic voting. One of the oldest, and most efficient blind signature schemes is the one due to Schnorr that is based on his famous identification scheme. Although it was proposed over twenty years ago, its unforgeability remains an open problem, even in the random oracle model. In this paper, we show that current techniques for proving security in the random oracle model do not work for the Schnorr blind signature by providing a meta-reduction which we call “personal nemesis adversary”. Our meta-reduction is the first one that does not need to reset the adversary and can also rule out reductions to interactive assumptions. Our results generalize to other important blind signatures, such as the one due to Brands. Brands’ blind signature is at the heart of Microsoft’s newly implemented UProve system, which makes this work relevant to cryptographic practice as well.

Keywords: Blind signatures, meta-reduction technique, unforgeability, random oracle model

Source: Asiacrypt 2013, LNCS, Vol.8269, Springer, Heidelberg (2013)

Schnorr

oracle

“ ”

oracle

Schnorr

Brands

Brands

uprove

Oracle
