内部资料 注意保存

国际密码学与信息安全研究动态

International InfoSecurity Updates

主　编：封化民

副主编：郎永清　　李晓明

编　者：（以姓氏笔画为序）

王　玮　　巴雪静　　刘伟伟　　刘　妍

严京生　　李天宇　　李新华　　杨厚琴

张武江　　张艳硕　　陈茜芸　　宫启生

解献芬

北京电子科技学院 密码与信息安全情报研究室

目　　录

2012 年欧密会论文摘要（II）

2012 年美密会论文摘要（II）

2012 年亚密会论文摘要（II）

Narrow-Bicliques: Cryptanalysis of Full IDEA

Dmitry Khovratovich[1], Ga¨etan Leurent[2], and Christian Rechberger[3]
[1]Microsoft Research, USA
[2]University of Luxembourg, Luxembourg
[3] DTU, Denmark

Abstract. We apply and extend the recently introduced biclique frame-work to IDEA and for the first time describe an approach to noticeably speed-up key-recovery for the full 8.5 round IDEA.

We also show that the biclique approach to block cipher cryptanalysis not only obtains results on more rounds, but also improves time and data complexities over existing attacks. We consider the first 7.5 rounds of IDEA and demonstrate a variant of the approach that works with practical data complexity.

The conceptual contribution is the narrow-bicliques technique: the recently introduced independent-biclique approach extended with ways to allow for a significantly reduced data complexity with everything else being equal. For this we use available degrees of freedom as known from hash cryptanalysis to narrow the relevant differential trails. Our cryptanalysis is of high computational complexity, and does not threaten the practical use of IDEA in any way, yet the techniques are practically verified to a large extent.

Key words: block ciphers, bicliques, meet-in-the-middle, IDEA, key recovery.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

对全轮 IDEA 的密码分析

摘要：我们将最近引入的 biclique 工作框架应用并扩展到 IDEA 上，并第一次介绍一个明显提高全 8.5 轮 IDEA 的密钥恢复的快速方法。

我们还表明，将 biclique 方法应用于分组加密不仅在更多轮上得出结果，同时还在已有的攻击方法上提高了时间和数据复杂度。考虑 IDEA 的前 7.5 轮并证明这个方法的变体适应实际数据复杂度。

我们在概念上的贡献就是窄 biclique 技术：在最近介绍的独立-双派方法在同等情况下显著降低数据复杂度，对此，我们使用从哈希密码分析得知的可用自由度来窄化相关差分路径。我们的密码分析计算复杂度很高，且从任何一方面都没有威胁到 IDEA 的实际使用，但技术在实际中很大程度上得到了验证。

关键词：分组密码；biclique 方法；中间相遇；IDEA；密钥恢复

Statistical Tools Flavor Side-Channel Collision Attacks

Amir Moradi
Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany
moradi@crypto.rub.de

Abstract. By examining the similarity of side-channel leakages, collision attacks evade the indispensable hypothetical leakage models of multi-query based side-channel distinguishers like correlation power analysis and mutual information analysis attacks. Most of the side-channel collision attacks compare two selective observations, what makes them similar to simple power analysis attacks. A multi-query collision attack detecting several collisions at the same time by means of comparing the leakage averages was presented at CHES 2010. To be successful this attack requires the means of the side-channel leakages to be related to the processed intermediate values. It therefore fails in case the mean values and processed data are independent, even though the leakages and the processed values follow a clear relationship. The contribution of this article is to extend the scope of this attack by employing additional statistics to detect the colliding situations. Instead of restricting the analyses to evaluation of means, we propose to employ higher-order statistical moments and probability density functions as the figure of merit to detect collisions. Thus, our new techniques remove the shortcomings of the existing correlation collision attacks using first-order moments. In addition to the theoretical discussion of our approach, practical evidence of its suitability for side-channel evaluation is provided. We provide four case studies, including three FPGA-based masked hardware implementations and a software implementation using boolean masking on a microcontroller, to support our theoretical groundwork.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

统计工具偏侧信道碰撞攻击

摘要：通过检查相似的侧信道泄漏、碰撞攻击躲避了不必要的多查询的假设泄漏模型，这些模型是基于侧信道区分器，如相关能量分析和互信息分析攻击,大多数侧信道碰撞攻击比较两个选择性的实验观察,即是什么让他们类似于简单的能量分析攻击。CHES 2010 提出了多查询碰撞攻击，通过比较泄露平均值同时检测几个碰撞。要想成功，这一攻击要求侧信道泄漏平均值与被处理的中间值相关，因此如果平均值和被处理数据是独立的，这一攻击就会失败，即使是泄漏和被处理值遵循一个明确的关系。本文的贡献是通过额外统计研究碰撞的情况从而扩大了攻击的范围。我们建议采用高阶统计时机和概率密度函数作为性能因素来检测碰撞，而不是限制对平均值评估的分析，这样,我们的新技术去除了使用一阶时刻的现有相关碰撞攻击的缺点。除了对我们的方法理论上的讨论,我们也提供了这一技术对边信道评估的适用性的实践证明。我们提供四个案例研究,包括三个基于 FPGA 的掩蔽硬件实现和一个利用在微控制器上进行布尔掩蔽的软件实现，以此来支持我们的理论基础。

Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers

Jean-S´ebastien Coron[1], David Naccache[2], and Mehdi Tibouchi[3]

[1] Universit´ du Luxembourg jean-sebastien.coron@uni.lu2´

[2]Ecole normale sup´erieure

david.naccache@ens.fr

[3] NTT Information Sharing Platform Laboratories tibouchi.mehdi@lab.ntt.co.jp

Abstract. We describe a compression technique that reduces the public key size of van Dijk, Gentry, Halevi and Vaikuntanathan's (DGHV) fully homomorphic scheme over the integers from O˜(ë7) to O˜(ë5). Our variant remains semantically secure, but in the random oracle model. We obtain an implementation of the full scheme with a 10.1 MB public key instead of 802 MB using similar parameters as in . Additionally we show how to extend the quadratic encryption technique of to higher degrees, to obtain a shorter public-key for the basic scheme.

This paper also describes a new modulus switching technique for the DGHV scheme that enables to use the new FHE framework without boot-strapping from Brakerski, Gentry and Vaikuntana than with the DGHV scheme. Finally we describe an improved attack against the approximate GCD Problem on which the DGHV scheme is based, with complexity O˜(2ñ) instead of O˜(23ñ/2).

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

整数上完全同态加密的公钥压缩和模数转换

摘要：我们介绍了一种,在从 O~(λ7) 到 O~(λ5)的整数范围内降低 Dijk, Gentry, Halevi and Vaikuntanathan’s (DGHV)公钥大小的完全同态方案。但在随机预言模型里，我们仍然是语义安全的变体。

我们实施了一个 10.1 MB 公共密钥完整方案，而不是使用其他类似的参数，如 802 MB。此外，我们展示了如何将二次加密技术扩展到更高的程度，以此来获得一个较短的公开密钥的基本方案。

本文还描述了一种用于 DGHV 方案的新的模数转换技术，这种技术能够使用一个新的 FHE 框架而无需 DGHV 的 Brakerski、Gentry 和 Vaikuntanathan 绑定启动。最后我们介绍一种复杂度为 O~(2ρ)而不是 O~(23ρ/ 2)的针对 DGHV 方案基础的 Approximate GCD 问题的改进攻击。

Multiparty Computation with Low Communication, Computation and Interaction via Threshold FHE

Gilad Asharov[1], Abhishek Jain[2], Adriana L′opez-Alt[3], Eran Tromer[4]
Vinod Vaikuntanathan[5], and Daniel Wichs[6]
[1] Bar-Ilan University
[2] University of California Los Angeles (UCLA)
[3] New York University (NYU)
[4] Tel Aviv University
[5] University of Toronto
[6] IBM Research, T.J. Watson

Abstract. Fully homomorphic encryption (FHE) enables secure computation over the encrypted data of a single party. We explore how to extend this to multiple parties, using threshold fully homomorphic encryption(TFHE). In such scheme, the parties jointly generate a common FHE public key along with a secret key that is shared among them; they can later cooperatively decrypt ciphertexts without learning anything but the plaintext. We show how to instantiate this approach efficiently, by extending the recent FHE schemes of Brakerski, Gentry and Vaikuntanathan (CRYPTO ’11, FOCS ’11, ITCS ’12) based on the (ring) learning with errors assumption. Our main tool is to exploit the property that such schemes are additively homomorphic over their keys.

Using TFHE, we construct simple multiparty computation protocols secure against fully malicious attackers, tolerating any number of corruptions, and providing security in the universal composability framework. Our protocols have the following properties: Low interaction: 3 rounds of interaction given a common random string, or 2 rounds with a public-key infrastructure. Low communication: independent of the function being computed (proportional to just input and output sizes).Cloud-assisted computation: the bulk of the computation can be efficiently outsourced to an external entity (e.g. a cloud service) so that the computation of all other parties is independent of the complexity of the evaluated function.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

通过门限全同态加密的低通信，计算和交互的多方计算

摘要：全同态加密（FHE）可以确保单一方加密的数据的安全计算。本文探讨使用门限全同态加密（TFHE）的方法扩展到多方计算。在这种方案中，多方共同生成一个共同的 FHE 公钥及一个共享密钥,仅仅通过分析明文即可对密文解密。我们拓展了三位研究者 Brakerski，Gentry 和 Vaikuntanathan(CRYPTO ’11, FOCS’11, ITCS ’12)最近提出的基于 LWE（环）的 FHE 方案， 证明了如何有效地对这种方法给出例示。我们的主要工具是利用方案是附加同态密钥这一性质。

通过使用 TFHE，我们构建了简单的安全多方计算协议用以防范那些极度恶意的攻击者，容忍任何数量的损毁，并提供通用可组合框架安全保障。我们构建的协议具有以下特性：第一，低交互， 在一个共同的随机字符串中仅有 3 轮互动，或在公钥基础框架中只有 2 轮。第二，低通信：独立于函数计算（仅与输入输出的大小成比例）。第三，云计算：海量的计算可以有效地外包给一个外部实体（如一个云服务机构），以保证其他各方计算不依赖复杂的评价函数。

Faster Algorithms for Approximate Common Divisors:

Breaking Fully-Homomorphic-Encryption Challenges over the Integers

Yuanmi Chen[1] and Phong Q. Nguyen[2]
[1] ENS, Dept. Informatique, 45 rue d'Ulm, 75005 Paris, France
http://www.eleves.ens.fr/home/ychen/
[2] INRIA, France and Tsinghua University, Institute for Advanced Study, China
http://www.di.ens.fr/˜pnguyen/

Abstract. At EUROCRYPT '10, van Dijk et al. presented simple fully homomorphic encryption (FHE) schemes based on the hardness of approximate integer common divisors problems, which were introduced in 2001 by Howgrave-Graham. There are two versions for these problems: the partial version (PACD) and the general version (GACD). The seemingly easier problem PACD was recently used by Coron et al. at CRYPTO '11 to build a more efficient variant of the FHE scheme by van Dijk et al.. We present a new PACD algorithm whose running time is essentially the "square root" of that of exhaustive search, which was the best attack in practice. This allows us to experimentally break the FHE challenges proposed by Coron et al. Our PACD algorithm directly gives rise to a new GACD algorithm, which is exponentially faster than exhaustive search. Interestingly, our main technique can also be applied to other settings, such as noisy factoring and attacking low-exponent RSA.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

更快的近似公因子算法：打破对整数的完全同态加密挑战

摘要：在2010年的欧密会上，van Dijk等人基于近似整数公因子分解问题的困难性提出了简单的完全同态加密方案(FHE)，而近似整数公因子分解问题是由Howgrave-Graham在2001年提出的。它们有两个版本：部分版本(PACD)和通用版本(GACD)。看似更简单的版本PACD最近被Coron等人在2011年的美密会上使用过，他们创建了比van Dijk等人的方案更有效的一个FHE方案升级版。我们则在本文中提出了一个新的PACD算法，该算法的运行时间是穷举搜索所需时间的“平方根”，而穷举搜索是实践中最好的攻击手段。这允许我们在实证上能够打破由Coron等人提出的FHE挑战。我们的PACD算法可以直接产生一个新的GACD算法，它拥有比穷举搜索快指数级的速度。有趣的是,我们的主要技术也可以应用到其他方面,比如噪声分解和低指数攻击RSA。

Decoding Random Binary Linear Codes in2n/20：

How 1+1 = 0 Improves Information Set Decoding

Anja Becker1, Antoine Joux[1, 2], Alexander May[3], and Alexander Meurer[3]

[1]Universit´e de Versailles Saint-Quentin, Laboratoire PRISM

[2]DGA

[3]Ruhr-University Bochum, Horst G ¨ortz Institute for IT-Security

anja.becker@prism.uvsq.fr, antoine.joux@m4x.org

{alex.may,alexander.meurer}@rub.de

Abstract. Decoding random linear codes is a well studied problem with many applications in complexity theory and cryptography. The security of almost all coding and LPN/LWE-based schemes relies on the assumption that it is hard to decode random linear codes. Recently, there has been progress in improving the running time of the best decoding algorithms for binary random codes. The ball collision technique of Bernstein, Lange and Peters lowered the complexity of Stern's information set decoding algorithm to $2^{0.\,0556n}$. Using representations this bound was improved to $2^{0.\,0537n}$ by May, Meurer and Thomae. We show how to further increase the number of representations and propose a new information set decoding algorithm with running time $2^{0.\,0494n}$.

Keywords: Information Set Decoding, Representation Technique

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

2n/20 范围内的随机二元线性码译码：如何通过 1+1=0 提高信息集译码

摘要：在复杂性理论和密码学中，随机线性码译码是受到充分关注并研究的一个问题。几乎所有的编码和基于 LPN/LWE 的方案的安全性都是基于随机线性码难于破解这一假设。最近，二进制随机码的译码的最佳算法的运行时间得到了很大改善。Bernstein, Lange 和 Peters 的球碰撞技术把斯特恩（Stern）的信息集的解码算法复杂性降低到 20.0556n。May,Meurer 和 Thomae 等人使用表示技术（representation）把边界提高到了 20.0537n。我们将证明如何进一步增加表示（respresentation）的数量,并提出一个新的运行时间为 20.0494n 的信息集译码算法，。

关键词：信息集译码；表示技术

On the Exact Security of Schnorr-TypeSignatures in the Random Oracle Model

YannickSeurin

ANSSI, Paris, France

yannick.seurin@m4x.org

Abstract. The Schnorr signature scheme has been known to be provably secure in the Random Oracle Model under the Discrete Logarithm(DL) assumption since the work of Pointcheval and Stern (EUROCRYPT'96), at the price of a very loose reduction though: if there is a forger making at most q_h random oracle queries, and forging signatures with probability ε_F , then the Forking Lemma tells that one can compute discrete logarithms with constant probability by rewinding the forger $O(q_h/\varepsilon_F)$times. In other words, the security reduction loses a factor $O(q_h$)inits time-to-success ratio. This is rather unsatisfactory since may be quite large. Yet Paillier and Vergnaud (ASIACRYPT 2005) later showed that under the One More Discrete Logarithm (OMDL) assumption, any algebraic reduction must lose a factor at least $q_h^{1/2}$in its time-to-success ratio.This was later improved by Garget al. (CRYPTO 2008) to a factor$q_h^{2/3}$.Up to now, the gap between$q_h^{2/3}$ and qh remained open. In this paper, we show that the security proof using the Forking Lemma is essentially the best possible. Namely, under the OMDL assumption, any algebraic reduction must lose a factor $f(\varepsilon_F)q_h$ in its time-to-success ratio, whereof $\leqslant$ 1 is a function that remains close to 1 as long as ε F is noticeably smaller than 1. Using a formulation in terms of expected-time and queries algorithms, we obtain an optimal loss factorΩ (q_h), independently ofε_F. These results apply to other signature schemes based on one-way group homomorphisms, such as the Guillou-Quisquater signature scheme.

Keywords: Schnorr signatures, discrete logarithm, Forking Lemma, Random Oracle Model, meta-reduction, one-way group homomorphism.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

随机预言模型中 Schnorr 型签名的精确安全性

摘要：自 Pointcheval 和 Stern 在 1996 年欧密会提出 Schnorr 签名以来，尽管以松散规约为代价，Schnorr 签名方案已被普遍证明在随机预言模型下用离散对数算法是安全的。如果有一个伪造者攻击随机预言查询最多 qh 次，伪造签名的概率是εF，然后根据分叉引理，可以通过反复常数概率 O(qh/εF)次计算出离散对数。换句话说，安全规约在时间/成功比率上损失一个因子 O(qh)。这个损失可能很大，所以不令人满意。然而在 2005 亚密会上 Paillier 和 Vergnaud 证明用 OMDL（One More Discrete Logarithm）算法，任何代数规约在时间/成功比率上必须损失 qh 1/ 2 因子。这个后来被 Garg 等人在 2008 年美密会上证明到了 qh 2/ 3。直到现在 qh 2/ 3 和 qh 之间的差距依然是公开的。本论文中，我们证明使用分叉引理安全性本质上是最好的。也就是用 OMDL 算法，任何代数规约在时间/成功比率上必须损失一个因子 *f*(εF) qh。只要εF 明显小于 1，f ≤ 1 就是一个保持接近 1 的函数。使用以预期时间和查询算法的公式，我们可以得到一个最优的损失因子 Ω(qh)，并独立于εF。这些结果可应用在其他的基于单向的群同态签名算法，例如 Guillou-Quisquater 签名算法等。

关键字：Schnorr 签名；离散对数；分叉引理；随机预言模型；元规约（meta-reduction）；单向群同态

Tightly-Secure Signatures from Lossy Identification Schemes

Michel Abdalla[1], Pierre-Alain Fouque[1],
Vadim Lyubashevsky[1], and Mehdi Tibouchi[2]
[1] ′Ecole Normale Sup′erieure
{michel.abdalla,pierre-alain.fouque,vadim.lyubashevsky}@ens.fr
[2] NTT Information Sharing Platform Laboratories
tibouchi.mehdi@lab.ntt.co.jp

Abstract. In this paper we present three digital signature schemes with tight security reductions. Our first signature scheme is a particularly efficient version of the short exponent discrete log based scheme of Girault et al. (J. of Cryptology 2006). Our scheme has a tight reduction to the *decisional* Short Discrete Logarithm problem, while still maintaining then on-tight reduction to the *computational* version of the problem upon which the original scheme of Girault et al. is based. The second signature scheme we construct is a modification of the scheme of Lyubashevsky (Asiacrypt 2009) that is based on the worst-case hardness of the shortest vector problem in ideal lattices. And the third scheme is a very simple signature scheme that is based directly on the hardness of the Subset Sum problem. We also present a general transformation that converts, what we term *lossy* identification schemes, into signature schemes with tight security reductions. We believe that this greatly simplifies the task of constructing and proving the security of such signature schemes.

Keywords: Signature schemes, tight reductions, Fiat-Shamir.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

基于有损身份认证方案的紧安全性签名

摘要：:本文中我们提出了三个具有紧安全性规约的数字签名方案。我们的第一个签名方案是基于 Girault 等人在 2006 年密码学学报上的方案，它是一个特别有效的短指数离散对数版本。我们的方案对于决定性的短离散对数问题有一个紧规约， 同时也保留了 Girault 原方案中对于计算性问题的紧规约。第二个签名方案是对 2009 年亚密会 Lyubashevsky 方案的修订,该方案基于理想格上最短向量问题的最坏硬度情况。第三个方案是一个非常简单的签名方案,是直接基于子集和问题的难解度。我们也提出了一个通用转换，它可以将我们所定义的有损身份认证方案转换成为紧安全规约的签名方案。我们相信,这大大简化了方案的构建并证明了签名方案的安全性。

关键词： 签名方案,紧规约,Fiat-Shamir

Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption

Tatsuaki Okamoto[1] and Katsuyuki Takashima[2]

[1] NTT

okamoto.tatsuaki@lab.ntt.co.jp

[2] Mitsubishi Electric

Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

Abstract： This paper proposes the first inner product encryption (IPE) scheme that is adaptively secure and fully attribute-hiding (attribute-hiding in the sense of the definition by Katz, Sahai and Waters), while the existing IPE schemes are either fully attribute-hiding but selectively secure or adaptively secure but weakly attribute-hiding. The proposed IPE scheme is proven to be adaptively secure and fully attribute-hiding under the decisional linear assumption in the standard model. The IPE scheme is comparably as efficient as the existing attribute-hiding IPE schemes. We also present a variant of the proposed IPE scheme with the same security that achieves shorter public and secret keys. A hierarchical IPE scheme can be constructed that is also adaptively secure and fully attribute-hiding under the same assumption. In this paper, we extend the dual system encryption technique by Waters into a more general manner, in which new forms of ciphertext and secret keys are employed and new types of information theoretical tricks are introduced along with several forms of computational reduction.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

具有适应性属性隐藏性（等级的）的内积加密

摘要：本文第一次提出了内积加密（IPE）方案是自适应安全的，并具完全隐藏属性（属性隐藏的含义参考了 Katz, Sahai 和 Waters 所做的定义），而现有 IPE 方案要么是虽具完全隐藏属性但其安全性是选择性，要么其安全性是自适应的但只具有弱属性隐藏。这里提出的 IPE 方案被证明在标准模型中决策性线性假设条件下，该方案是自适应安全的并且具有完全隐藏属性。 IPE 的方案跟现存的有属性隐藏 IPE 方案比具有同等效率。我们提出的 IPE 方案还给出了一个变量，该变量具有相同的安全性，并且能实现使用较短的公钥和秘密密钥。在相同的假设下一个具有自适应安全性和完全隐藏属性的分层 IPE 方案可以构造出来。本文中，我们将 Waters 的双系统加密技术扩展为一个个更普遍的方式，其中用到了密文和密钥的新形式，且引入了新型的信息理论技巧以及几种形式的计算缩减。

Scalable Group Signatures with Revocation

Benoˆıt Libert[1], Thomas Peters[1], and Moti Yung[2]

[1] Universit′e Catholique de Louvain, ICTEAM Institute, Belgium

[2] Google Inc. and Columbia University, USA

Abstract. Group signatures are a central cryptographic primitive, simultaneously supporting accountability and anonymity. They allow users to anonymously sign messages on behalf of a group they are members of. The recent years saw the appearance of several constructions with security proofs in the standard model (i.e., without appealing to the random oracle heuristic). For a digital signature scheme to be adopted, an efficient revocation scheme (as in regular PKI) is absolutely necessary. Despite over a decade of extensive research, membership revocation remains a non-trivial problem in group signatures: all existing solutions are not truly scalable due to either high overhead (e.g., large group public key size), or limiting operational requirement (the need for all users to follow the system’s entire history).

In the standard model, the situation is even worse as many existing solutions are not readily adaptable. To fill this gap and tackle this challenge, we describe a new revocation approach based, perhaps somewhat unexpectedly, on the Naor-Naor-Lotspiech framework which was introduced for a different problem (namely, that of broadcast encryption). Our mechanism yields efficient and scalable revocable group signatures in the standard model. In particular, the size of signatures and the verification cost are independent of the number of revocations and the maximal cardinality N of the group while other complexities are at most poly logarithmic in N. Moreover, the schemes are history-independent: unrevoked group members do not have to update their keys when a revocation occurs.

Keywords: Group signatures, revocation, standard model, efficiency.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

使用撤销来实现的可扩展集体签名

摘要：集体签名是一个核心密码学原语，可同时支持匿名性和问责性。他们允许用户代表他们组的成员匿名进行消息签名。近年来出现了几个标准模型（不需要随机预言启发）下具有安全证明的方案。要采用一种数字签名，高效率的撤回方案（如普通 PKI 中）是绝对必要的。尽管经过十年的广泛研究，在集体签名中成员资格撤销仍然是一个重点问题：所有现存解决方案由于高额日常管理（即大群公钥长度）或者由于限制操作要求（需要所有用户遵照系统的全部历史记录）做不到真正意义上的可扩展。

在标准模式下，由于很多现存解决方案不是随时可自适应的，这种情况会更糟糕。为了解决这个差距，应对这个挑战，我们使用了一种新的撤销方法，该方法基于 Naor-Naor-Lotspiech 框架。我们之前没预期使用该框架是因为它原本是来解决另外一个问题的（即广播加密问题）。在标准的模型下，我们的机制产生高效的、可扩展的可撤销的群签名。特别要指出的是，签名的长度和花费验证不受撤销数和群的最大基数 N 的限制，而其他方案的复杂操作是集中在 N 中多数多重对数上。而且，我们的方案是独立于历史记录的：当一个撤销发生时，未撤销的集体成员不必更新他们的密钥。

关键词：集体签名，撤回，标准模型，效率

Incremental Deterministic Public-Key Encryption

Ilya Mironov[1], Omkant Pandey[2], Omer Reingold[1],andGilSegev[1]

[1]Microsoft Research Silicon Valley, Mountain View, CA 94043, USA

{mironov,gil.segev,omer.reing old} @mic rosof t.co m

[2]Microsoft, Redmond, USA and Microsoft Research, Bangalore, India

omkantp@microsoft.com

Abstract. Motivated by applications in large storage systems, we initiate the study of incremental deterministic public-key encryption. Deterministic public-key encryption, introduced by Bellare, Boldyreva, and O'Neill (CRYPTO '07), provides a realistic alternative to randomized public-key encryption in various scenarios where the latter exhibits inherent drawbacks. A deterministic encryption algorithm, however, can-not satisfy any meaningful notion of security for low-entropy plaintexts distributions, and Bellare et al. demonstrated that a strong notion of security can in fact be realized for relatively high-entropy plaintext distributions.

In order to achieve a meaningful level of security, a deterministic en-cryption algorithm should be typically used for encrypting rather long plaintexts for ensuring a sufficient amount of entropy. This requirement may be at odds with efficiency constraints, such as communication complexity and computation complexity in the presence of small updates. Thus, a highly desirable property of deterministic encryption algorithms is incrementality: small changes in the plaintext translate into small changes in the corresponding ciphertext.

We present a framework for modeling the incrementality of deter-ministic public-key encryption. Within our framework we propose two schemes, which we prove to enjoy an optimal tradeoff between their security and incrementality up to small polylogarithmic factors. Our first scheme is a generic method which can be based on any deterministic public-key encryption scheme, and in particular, can be instantiated with any semantically-secure (randomized) public-key encryption scheme in the random oracle model. Our second scheme is based on the Decisional Diffie-Hellman assumption in the standard model.

The approach underpinning our schemes is inspired by the fundamental "sample-then-extract" technique due to Nisan and Zuckerman (JCSS'96) and refined by Vadhan (J.Cryptology'04),and by the closely related notion of "locally-computable extractors" due to Vadhan. Most notably, whereas Vadhan used such extractors to construct private-key encryption schemes in the bounded-storage model, we show that techniques along these lines can also be used to construct incremental public-key encryption schemes.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

高确定性的公钥密码

摘要：由于大存储系统的使用，我们开始研究高确定性的公钥密码。确定性的公钥密码，由Bellare, Boldyreva, 和O’Neill提出(CRYPTO ’07)。它提供了一个逼真的替代物，对于随机的公钥密码在各种各样的情况。后者存在固有的缺陷。然而，对于低熵的明文分布来说,一个确定性的加密算法不能够满足任何有意义的安全性的概念。并且，Bellare等人证明，对于相对高熵的明文分布来说，强安全性是可以实现的。

为了获得一个有意义的安全性的标准。确定性的加密算法应该被用来加密相当长的明文来确保获得足够大的熵。这个要求可能有一定的效率约束。比如，在小的更新中的通信复杂度和计算复杂度。因此，确定性算法的高满意度性质是渐进性的：明文中的少量变化将会带来密文中的少量变化。

确定性公钥加密的渐进性的建模，我们给出了一个框架。在我们的框架里我们建议两个方案。由于多重对数因素，我们证明了一个安全性和渐进性的折中方案。第一个方案是一种通用的方法，可以用在任何的确定性加密方案上。尤其是，在随机的oracle模型中的任意随机的确定性加密方案都可以被实例化。我们的第二个方案基于标准模式中的Diffie-Hellman假设。

我们方案的基础从基本的“抽样-提取”技术中得到的启发。这个技术是Nisan and Zuckerman (JCSS’96)提出的。Vadhan (J. Cryptology ’04)对其进行了精炼。,也从 Vadhan 提出的“局部可计算性提取器”技术中得到启发。非常明显的是,鉴于Vadhan用这种提取器在有限存储模式中构造私钥加密方案,我们表述的是顺着这一条线上的技术也可以被用来构造增强性的公钥加密方案。

Standard Security Does Not Imply Security against Selective-Opening

Mihir Bellare[1], Rafael Dowsley[1], Brent Waters[2], and Scott Yilek[3]
[1]Department of Computer Science & Engineering, University of California San Diego
http://cseweb.ucsd.edu/~mihir, http://cseweb.ucsd.edu/~rdowsley
[2]Department of Computer Science, University of Texas at Austin
http://www.cs.utexas.edu/~bwaters
[3]Department of Computer and Information Sciences, University of St. Thomas
http://personal.stthomas.edu/yile5901

Abstract: We show that no commitment scheme that is hiding and binding according to the standard definition is semantically-secure under selective opening attack (SOA), resolving a long-standing and fundamental open question about the power of SOAs. We also obtain the first examples of IND-CPA encryption schemes that are not secure under SOA, both for sender corruptions where encryption coins are revealed and receiver corruptions where decryption keys are revealed. These results assume only the existence of collision-resistant hash functions.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

标准安全并不意味对选择性开放安全

摘要：本文指出根据标准定义没有一个隐藏和绑定的承诺方案在选择性开放攻击(SOA)下是语义安全的，这解决了一个关于 SOA 的长期存在的和基本的悬而未决的问题。同时我们给出了第一个基于 IND—CPA 的加密方案，对于发送双方突发的密钥泄露在 SOA 下是均是不安全的。这些结果假设只存在于抗碰撞散列函数的情况下。

Detecting Dangerous Queries: A New Approach for Chosen Ciphertext Security

Susan Hohenberger[1] ,*, Allison Lewko[2] ,**, and Brent Waters[3] ,***

[1]Johns Hopkins University

susan@cs.jhu.edu

[2]University of Texas at Austin

{alewko,bwaters}@cs.utexas.edu

Abstract. We present a new approach for creating chosen ciphertext secure encryption. The focal point of our work is a new Abstraction that we call Detectable Chosen Ciphertext Security(DCCA). Intuitively, this notion is meant to capture systems that are not necessarily chosen ciphertext attack (CCA) secure, but where we can detect whether a certain query CT can be useful for decrypting (or distinguishing) a challenge ciphertext CT*.

We show how to build chosen ciphertext secure systems from DCCA security. We motivate our techniques by describing multiple examples of DCCA systems including creating them from 1-bit CCA secure encryption — capturing the recent Myers-shelat result (FOCS 2009). Our work identifies DCCA as a new target for building CCA secure systems.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

检测危险查询：选择密文安全的新方法

摘要: 我们对创建选择密文攻击安全加密我们提出了一个新的方法。我们研究的焦点是建立一个新的抽象，我们称之为可检测的选择密文安全（DCCA）。直观地看，这一概念意味着去捕获不一定选择的密文攻击（CCA）安全的系统，但是，在这里我们可以检测目标的查询 CT 对解密（或区分）一个有挑战的密文 CT 是否是有用的。

我们证明如何从 DCCA 安全系统构建选择密文安全系统。我们推动我们的技术通过描述多种 DCCA 系统的例子，包括从 1 比特 CCA 安全加密创建他们 -捕获最近 Myers-shelat 的结果（FOCS2009）。我们的工作是把 DCCA 当作建立 CCA 安全系统的一个新目标。

Security of Symmetric Encryption in the Presence of Ciphertext Fragmentation

Alexandra Boldyreva[1], Jean Paul Degabriele[2], Kenneth G.Paterson[2],
and Martijn Stam[3]
[1] Georgia Institute of Technology
[2] Royal Holloway, University of London
[3] University of Bristol

Abstract. In recent years, a number of standardized symmetric encryption schemes have fallen foul of attacks exploiting the fact that in some real world scenarios ciphertexts can be delivered in a fragmented fashion. We initiate the first general and formal study of the security of symmetric encryption against such attacks. We extend the SSH-specific work of Paterson and Watson (Eurocrypt 2010) to develop security models for the fragmented setting. We also develop security models to formalize the additional desirable properties of ciphertext boundary hiding and robustness against Denial-of-Service (DoS) attacks for schemes in this setting. We illustrate the utility of each of our models via efficient constructions for schemes using only standard cryptographic components, including constructions that simultaneously achieve confidentiality, ciphertext boundary hiding and DoS robustness.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

密文碎片环境下对称加密的安全性

摘要：: 最近几年，一些标准对称加密体制正面临利用实际环境中密文碎片传送这一特点的攻击。我们对防止这类攻击的对称密码算法安全性进行首次全面和正规的研究。我们将 Paterson 和 Watson (Eurocrypt 2010)提出的针对 SSH 的工作扩展为碎片场景条件下的安全性模型。同时在这一场景下，提出密文边界隐匿和抗 DoS 攻击所需附加性质的形式化安全模型。我们仅仅使用标准的密码部件，包括同时获得机密性、密文边界隐匿和 DoS 强健性的构件，构建相应密码体制来阐明我们所提出的几种模型的实用性。

Trapdoors for Lattices:

Simpler, Tighter, Faster, Smaller

Daniele Micciancio[1],and Chris Peikert[2]

[1] University of California, San Diego

[2] Georgia Institute of Technology

Abstract. We give new methods for generating and using “strong trapdoors” in cryptographic lattices, which are simultaneously simple, efficient, easy to implement (even in parallel), and asymptotically optimal with very small hidden constants. Our methods involve a new kind of trapdoor, and include specialized algorithms for inverting LWE, randomly sampling SIS preimages, and securely delegating trapdoors. These tasks were previously the main bottleneck for a wide range of cryptographic schemes, and our techniques substantially improve upon the prior ones, both in terms of practical performance and quality of the produced outputs. Moreover, the simple structure of the new trapdoor and associated algorithms can be exposed in applications, leading to further simplifications and efficiency improvements. We exemplify the applicability of our methods with new digital signature schemes and CCA-secure encryption schemes, which have better efficiency and security than the previously known lattice-based constructions.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

格的陷门更简单、更紧凑、速度更快、体积更小

摘要：我们给出新的生成和使用密码格的“强陷门”的方法，该方法简单、高效、易于实现（即使在并行情况），并且在小的隐藏常量条件下接近最优。我们的方法涉及一种新型的陷门，给出了 LWE 求逆、随机选取 SIS 原像和安全委托限门的专门算法。这些任务是原来很多密码方案的主要瓶颈。无论是在实用性能还是产生输出的质量上，我们的技术都在已有结果基础上有了较大的改进。而且，新陷门的简单结构和相关算法可以应用于实际，这有利于方案的进一步简化和效率的改进。我们举例说明了新方法在一个新数字签名方案和一些 CCA 安全加密方案的应用性能，新方案比现存的基于格的体制有更好的安全性和效率。

Pseudorandom Functions and Lattices

Abhishek Banerjee[1], Chris Peikert[1], and Alon Rosen[2],

[1] Georgia Institute of Technology

[2] IDC Herzliya

Abstract. We give direct constructions of pseudorandom function (PRF) families based on conjectured hard lattice problems and learning problems. Our constructions are asymptotically efficient and highly parallelizable in a practical sense, i.e., they can be computed by simple, relatively small low-depth arithmetic or boolean circuits (e.g., in NC^1 or even TC^0). In addition, they are the first low-depth PRFs that have no known attack by efficient quantum algorithms. Central to our results is a new "derandomization" technique for the learning with errors (LWE) problem which, in effect, generates the error terms deterministically.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

伪随机函数和格

摘要：. 我们给出基于假定的困难格问题和学习问题的伪随机函数（PRF）族的直接构造方法。我们的构造在实际意义上是渐进有效且高度并行的，也就是说，它们可以用简单和相对小的低深度算术和布尔电路（比如，NC^1 或甚至 TC^0）进行计算。并且，它们是首批低深度伪随机函数，不受已知高效量子算法的攻击。我们的研究结果的核心是针对确定性产生错误项的错误学习问题（LWE）的一个新的“去随机”技术。

Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting

Allison Lewko_
The University of Texas at Austin
alewko@cs.utexas.edu

Abstract. In this paper, we explore a general methodology for converting composite order pairing-based cryptosystems into the prime order setting. We employ the dual pairing vector space approach initiated by Okamoto and Takashima and formulate versatile tools in this framework that can be used to translate composite order schemes for which the prior techniques of Freeman were insufficient. Our techniques are typically applicable for composite order schemes relying on the canceling property and proven secure from variants of the subgroup decision assumption, and will result in prime order schemes that are proven secure from the decisional linear assumption. As an instructive example, we obtain a translation of the Lewko-Waters composite order IBE scheme. This provides a close analog of the Boneh-Boyen IBE scheme that is proven fully secure from the decisional linear assumption. In the full version of this paper, we also provide a translation of the Lewko-Waters unbounded HIBE scheme.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

素数阶设置中模拟合数阶双线性群特性的工具

摘要：在本文中,我们开发了一个通用方法将合数阶双线性对密码系统转变成为素数阶的设置。我们采用由 Okamoto and Takashima 提出的对偶对向量空间方法形成了一些通用工具，可用来转换合数阶方案， 而以前 Freeman 的技术对这类方案存在很多不充分之处。我们的技术很典型地适用于一些依赖于消去特性和在各类子群决策假设下证明安全的合数阶方案。作为一个展示性例子,我们获得一个 Lewko-Waters 合数阶 IBE 方案的转换。这提供了一个与 Boneh-Boyen IBE 方案很近似的对应物，且被证明在决策线性假设下是完全安全的。在本文的完整版,我们也提供一个 Lewko-Waters 无界 HIBE 方案的转换。

Minimalism in Cryptography: The Even-Mansour Scheme Revisited

Orr Dunkelman[1,2], Nathan Keller[2,3], and Adi Shamir[2]

[1] Computer Science Department, University of Haifa, orrd@cs.haifa.ac.il, [2] Faculty of Mathematics and Computer Science, Weizmann Institute of Science, [3] Department of Mathematics, Bar-Ilan University, Israel

Abstract. In this paper we consider the following fundamental problem: What is the simplest possible construction of a block cipher which is provably secure in some formal sense? This problem motivated Even and Mansour to develop their scheme in 1991, but its exact security remained open for more than 20 years in the sense that the lower bound proof considered known plaintexts, whereas the best published attack (which was based on differential cryptanalysis) required chosen plaintexts. In this paper we solve this open problem by describing the new Slidex attack which matches the $T = \Omega(2n/D)$ lower bound on the time T for any number of known plaintexts D. Once we obtain this tight bound, we can show that the original two-key Even-Mansour scheme is not minimal in the sense that it can be simplified into a single key scheme with half as many key bits which provides exactly the same security, and which can be argued to be the simplest conceivable provably secure block cipher. We then show that there can be no comparable lower bound on the memory requirements of such attacks, by developing a new memoryless attack which can be applied with the same time complexity but only in the special case of $D = 2n/2$. In the last part of the paper we analyze the security of several other variants of the Even-Mansour scheme, showing that some of them provide the same level of security while in others the lower bound proof fails for very delicate reasons.

Keywords: Even-Mansour block cipher, whitening keys, minimalism, provable security, tight security bounds, slide attacks, slidex attack.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

密码学极简主义:依文-曼苏尔计划回顾

摘要：在本文中,我们考虑以下基本问题:一个在某些形式化意义上可证安全的分组密码的尽可能简单的构造是什么？这一问题促使依文和曼苏尔在 1991 年开发了他们的方案。但是，他们的下界论证考虑的是已知明文而以差分密码分析为基础的最好的已知攻击需要选择明文。在此意义上，这一方案的确切安全性 20 多年仍然无法确定。在本文中,我们通过描述新的 Slidex 攻击来解决这个开放问题，这种攻击与任何已知明文 D 数量的时间下界 T $=\Omega(2^n/D)$相匹配。一旦取得此紧界,我们可以表明,最初的两个密钥的依文-曼苏尔方案不是最简化的，它可以被简化成一个单密钥方案，只要一半数量的密钥比特就能提供完全相同的安全性,可以认为这是最简单的可证安全的分组密码。然后,通过开发一个新的具有相同时间复杂度但仅在 D = 2n/2 特例下的无内存攻击,我们表明：此类攻击的内存需求没有与之相当的下界。在论文的最后一部分，我们分析了依文-曼苏尔方案中其他几个变型的安全性，指出其中一些提供相同级别的安全性,而另一些的下界证明则由于非常微妙的原因失败了。

关键词:依文-曼苏尔分组密码，白化密钥，极简主义，可证安全,安全紧界,滑动攻击,slidex攻击

Message Authentication, Revisited

Yevgeniy Dodis[1], Eike Kiltz[2],□, Krzysztof Pietrzak[2],□□, and Daniel Wichs[4]

1 New York University

2 Ruhr-Universit¨at Bochum

[3] IST Austria

[4] IBM T.J. Watson Research Center

Abstract. Traditionally, symmetric-key message authentication codes (MACs) are easily built from pseudorandom functions (PRFs). In this work we propose a wide variety of other approaches to building efficient MACs, without going through a PRF first. In particular, unlike deterministic PRF-based MACs, where each message has a unique valid tag, we give a number of probabilistic MAC constructions from various other primitives/assumptions. Our main results are summarized as follows:

– We show several new probabilistic MAC constructions from a variety of general assumptions, including CCA-secure encryption, Hash Proof Systems and key-homomorphic weak PRFs. By instantiating these frameworks under concrete number theoretic assumptions, we get several schemes which are more efficient than just using a state-of-the-art PRF instantiation under the corresponding assumption.

– For probabilistic MACs, unlike deterministic ones, unforgeability against a chosen message attack (uf-cma) alone does not imply security if the adversary can additionally make verification queries (uf-cmva). We give an efficient generic transformation from any uf-cma secure MAC which is “message-hiding” into a uf-cmva secure MAC. This resolves the main open problem of Kiltz et al. From Eurocrypt’11; By using our transformation on their constructions, we get the first efficient MACs from the LPN assumption.

– While all our new MAC constructions immediately give efficient actively secure, two-round symmetric-key identification schemes, we also show a very simple, three-round actively secure identification protocol from any weak PRF. In particular, the resulting protocol is much more efficient than the trivial approach of building a regular PRF from a weak PRF.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

消息认证之回顾

摘要：传统上，对称密钥的消息认证码（MAC）很容易由伪随机函数（PRF）构建。在这项工作中，我们提出了不必先通过 PRF 而建立有效 MAC 的多种其他方法。以 PRF 为基础的确定性 MAC 的每个消息都有唯一的有效标签，与此不同，我们基于其它各种基元/假设给出了一些概率性 MAC 构造。我们的主要结果如下：

---- 我们展示了一些基于普通假设的若干新的概率性 MAC 结构，包括 CCA 安全的加密、哈希证明系统和弱的密钥同态 PRF。通过在具体数论假设下实例化这些结构，我们得到了几个方案，它们比在相同假设下仅使用当今最好 PRF 的实例更有效。

---- 与确定性 MAC 不同，对概率性 MAC 来说，如果敌手可以另外做验证查询（UF-CMVA），针对选择消息攻击（UF-CMA）的不可伪造性自身并不意味着安全性。我们可把任一个“消息隐藏”的 UF-CMA 安全 MAC 有效转化成一个 UF-CMVA 安全 MAC。这解决了基尔茨等人在 Eurocrypt’11 提出的主要开放性问题。通过对它们的结构的转化，我们从 LPN 假设得到了第一批有效的 MAC。

---- 尽管我们所有的新的 MAC 结构可以立刻给出有效的主动安全的两轮对称密钥身份验证方案，我们还展示了一个非常简单的来自于任一弱 PRF 的三轮主动安全的身份验证协议。特别是，该协议比从弱 PRF 建立常规 PRF 的平凡方法更有效。

Property Preserving Symmetric Encryption

Omkant Pandey[1] and Yannis Rouselakis[2]

[1] Microsoft, Redmond, USA and Microsoft Research, Bangalore, India

omkantp@microsoft.com

[2] The University of Texas at Austin

jrous@cs.utexas.edu

Abstract. Processing on encrypted data is a subject of rich investigation. Several new and exotic encryption schemes, supporting a diverse set of features, have been developed for this purpose. We consider encryption schemes that are suitable for applications such as data clustering on encrypted data. In such applications, the processing algorithm needs to learn certain properties about the encrypted data to make decisions. Often these decisions depend upon multiple data items, which might have been encrypted individually and independently. Current encryption schemes do not capture this setting where computation must be done on multiple ciphertexts to make a decision.

In this work, we seek encryption schemes which allow public computation of a pre-specified property P about the encrypted messages. That is, such schemes have an associated property P of fixed arity k, and a publicly computable algorithm Test, such that Test (ct1, . . . , ctk) =P(m1, . . . ,mk), where cti is an encryption of mi for i = 1, . . . , k. Further, this requirement holds even if the ciphertexts ct1, . . . , ctk were generated individually and independently. We call such schemes property preserving encryption schemes. Property preserving encryption (PPEnc) makes most sense in the symmetric setting due to the requirement that Test is publicly computable.

In this work, we present a thorough investigation of property preserving symmetric encryption. We start by formalizing several meaningful notions of security for PPEnc. Somewhat surprisingly, we show that there exists a hierarchy of security notions for PPEnc, indexed by integers η ∈ N, whi
symmetric PPEnc scheme for encrypting vectors in ZN of polynomial length. This construction supports the orthogonality property: for every two vectors (□x, □y) it is possible to publicly learn whether □x · □y = 0 mod p. Our scheme is based on bilinear groups of composite order.

Source: EUROCRYPT 2012, LNCS, vol. 7237, Springer, Heidelberg (2012)

保持性能的对称加密

摘要：处理加密数据是一个具有丰富研究内容的课题。为此，人们开发了一些支持不同特性的新奇的加密方案。我们研究了适合于某些应用的加密方案，例如加密数据的数据聚类。在这样的应用中，处理算法需要了解加密数据的某些性能来做出决策。这些决策通常取决于多个数据项，这些数据项可能已被个别和独立地加密。因此决策需要对多密文进行计算，而目前的加密方案不适用这种设定。

在这项研究中，我们寻找允许对密文的预指定性能 P 进行公开计算的加密方案。即这种方案有一个含不变参数数量 K 的相关性能 P 和一个公开可计算的算法 Test，使得$\boldsymbol{Test}\left(ct_1,...,ct_k\right)=P\left(m_1,..,m_k\right)$，其中$ct_i$是一个对$m_i$的加密，i=0, 1, …k。而且即使密文$ct_1,ct_2,...,ct_k$是个别和独立产生的仍然满足这一要求。我们称这样的方案为保持性能的加密方案。由于要求 Test 算法是公开可计算的，保持性能的加密（PPEnc）在对称密码设定环境中最有意义。

在这项研究中，我们对保持性能的对称加密进行了充分探讨。我们从形式化 PPEnc 的几个有意义安全概念入手。有些出人意料的是，PPEnc 存在一个不会发生矛盾的安全概念的阶层结构，以整数η∈N 为索引。我们还提出了一种多项式长度的Z_n中加密向量的对称 PPEnc 加密方案。该结构支持正交性：对于任何两个向量□x, □y，它能公开得知是否□$x\cdot$□$y = 0 \bmod p$。我们的方案基于合数阶的双线性群。

Multi-instance Security and Its Application to Password-Based Cryptography

Mihir Bellare[1], Thomas Ristenpart[2], and Stefano Tessaro[3]

[1] Department of Computer Science & Engineering, University of California San Diego
cseweb.ucsd.edu/~mihir/

[2] Department of Computer Sciences, University of Wisconsin - Madison
pages.cs.wisc.edu/~rist/

[3] CSAIL, Massachusetts Institute of Technology
people.csail.mit.edu/tessaro/

Abstract. This paper develops a theory of multi-instance (mi) security and applies it to provide the first proof-based support for the classical practice of salting in password-based cryptography. Mi-security comes into play in settings (like password-based cryptography) where it is computationally feasible to compromise a single instance, and provides a second line of defense, aiming to ensure (in the case of passwords, via salting) that the effort to compromise all of some large number *m* of instances grows linearly with *m*. The first challenge is definitions, where we suggest LORX-security as a good metric for mi security of encryption and support this claim by showing it implies other natural metrics, illustrating in the process that even lifting simple results from the si setting to the mi one calls for new techniques. Next we provide a composition-based framework to transfer standard single-instance (si)security to mi-security with the aid of a key-derivation function. Analyzing password-based KDFs from the PKCS#5 standard to show that they meet our indifferentiability-style mi-security definition for KDFs, we are able to conclude with the first proof that per password salts amplify mi-security as hoped in practice. We believe that mi-security is of interest in other domains and that this work provides the foundation for its further theoretical development and practical application.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

多实例安全及其在基于口令的密码学中的应用

摘要：本文提出一种多实例（mi）安全理论，并首次为基于口令的密码学中传统加盐法提供证据支持。在单一实例容易破解的设定中，比如基于口令的密码学，mi 安全可以发挥作用，并提供第二道防线，以保证（在口令的情况下，通过加盐）破解所有的大数 m 个实例的代价与 m 呈线性增长。首先面对的挑战是定义，通过表明它包含其他自然度量，并在此过程中展示即使提升从 si 设定到 mi 设定的简单结果也需要新技术，我们建议用 LORX 安全作为加密的安全 mi 的度量。接下来，我们提供一个基于合成的框架，在密钥推导函数的帮助下，把标准的单实例（si）安全转移为 mi 安全。通过分析 PKCS#5 标准中基于口令的 KDF，表明它们符合我们对 KDF 的不区分 mi 安全的定义，我们可以得出第一次证明：正如实践中期望的那样，每个口令盐增强了 mi 安全。我们相信，mi 安全在其他领域也有用途，本研究为其进一步的理论发展和实际应用提供了基础。

Hash Functions Based on Three Permutations: A Generic Security Analysis

Dept. Electrical Engineering, ESAT/COSIC, KU Leuven, and IBBT, Belgium
{bart.mennink,bart.preneel}@esat.kuleuven.be

Abstract. We consider the family of 2n-to-n-bit compression functions that are solely based on at most three permutation executions and on XOR-operators, and analyze its collision and preimage security. Despite their elegance and simplicity, these designs are not covered by the results of Rogaway and Steinberger (CRYPTO 2008). By defining a carefully chosen equivalence relation on this family of compression functions, we obtain the following results. In the setting where the three permutations π1, π2, π3 are selected independently and uniformly at random, there exist at most four equivalence classes that achieve optimal 2n/2 collision resistance. Under a certain extremal graph theory based conjecture, these classes are then proven optimally collision secure. Three of these classes allow for finding preimages in 2n/2 queries, and only one achieves optimal 22n/3 preimage resistance (with respect to the bounds of Rogaway and Steinberger, EUROCRYPT 2008). Consequently, a compression function is optimally collision and preimage secure if and only if it is equivalent to $F(x1, x2) = x1 \oplus \pi1(x1) \oplus \pi2(x2) \oplus \pi3(x1 \oplus x2 \oplus \pi1(x1))$. For compression functions that make three calls to the same permutation we obtain a surprising negative result, namely the impossibility of optimal 2n/2 collision security: for any scheme, collisions can be found with 22n/5 queries. This result casts some doubt over the existence of any (larger) secure permutation-based compression function built only on XOR-operators and (multiple invocations of) a single permutation.

Keywords: Hash function, Permutation-based, Collision resistance, Preimage resistance.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

基于三置换的哈希函数：一个通用的安全分析

摘要：我们研究仅以最多三个置换和 XOR 运算符为基础的 2n-to-n-bit 压缩函数族，分析其碰撞和原象安全性。尽管这些设计优美简洁，但不是 Rogaway 和 Steinberger (CRYPTO 2008) 的研究结果所能涵盖的。通过定义此类压缩函数族的一个精心挑选的等价关系，我们获得如下结果：在随机独立均匀地选择三置换 π1， π2， π3 的设定中，最多存在四个能达到最优 2n/2 抗碰撞性的等价类。在一个以极值图论为基础的猜想下，这些等价类被证明碰撞安全性最优。其中三类在 2n/2 询问中能寻找到原象，只有一类达到最优 22n/3 抗原象性（就 EUROCRYPT 2008 Rogaway 和 Steinberger 的界限而言）。因此，当且仅当一个压缩函数等同于 F(x1, x2) = x1⊕π1(x1)⊕π2(x2)⊕π3(x1⊕x2⊕π1(x1))时，它的碰撞和原象安全性最优。对那些三次调用同样置换的压缩函数，我们得到的是令人惊讶的负面结果，即不可能达到最优 2n/2 碰撞安全：在任意方案中，用 22n/5 询问都能发现碰撞。这一结果使人对仅建立在 XOR 运算和（多重调用）单一置换基础上任何安全的基于（较大）置换的压缩函数产生怀疑。

关键词：哈希函数，基于置换的，抗碰撞性，抗原象性

To Hash or Not to Hash Again?

(In)Differentiability Results for H2 and HMAC

Yevgeniy Dodis[1], Thomas Ristenpart[2], John Steinberger[3], and Stefano Tessaro[4]

[1]New York University

dodis@cs.nyu.edu

[2]University of Wisconsin–Madison

rist@cs.wisc.edu

[3]Tsinghua University

jpsteinb@gmail.com

[4]Massachusetts Institute of Technology

tessaro@csail.mit.edu

Abstract. We show that the second iterate H2(M)= H(H(M)) of a random oracle H cannot achieve strong security in the sense of indifferentiability from a random oracle. We do so by proving that indifferentiability for H2 holds only with poor concrete security by providing a lower bound (via an attack) and a matching upper bound (via a proof requiring new techniques) on the complexity of any successful simulator. We then investigate HMAC when it is used as a general-purpose hash function with arbitrary keys (and not as a MAC or PRF with uniform, secret keys). We uncover that HMAC's handling of keys gives rise to two types of weak key pairs. The first allows trivial attacks against its indifferentiability; the second gives rise to structural issues similar to that which ruled out strong indifferentiability bounds in the case of H2. However, such weak key pairs do not arise, as far as we know, in any deployed applications of HMAC. For example, using keys of any fixed length shorter than d − 1, where d is the block length in bits of the underlying hash function, completely avoids weak key pairs. We therefore conclude with a positive result: a proof that HMAC is indifferentiable from a RO (with standard, good bounds) when applications use keys of a fixed length less than d−1.

Keywords: Indifferentiability, Hash functions, HMAC.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

是否需要再次计算哈希值？H2 和 HMAC 的（不）可区分性结论

摘要：从与随机预言不可区分性的意义上说，我们认为一个随机预言 H 的第二轮迭代值 $H^2(M)= H(H(M))$，无法达到强安全性。通过给任何成功模拟器的复杂度提供一个下界（通过攻击）和一个相匹配的上界（通过采用新技术的证明），我们证明了 H^2 的不可区分性仅在比较差的具体安全性方面成立。我们还研究了带有任意密钥的（不作为 MAC 或带有均匀密钥的 PRF）被用作一般用途哈希函数的 HMAC。我们发现，HMAC 处理密钥过程会产生两种类型的弱密钥对。第一种允许对它的不可区分性进行平凡攻击；第二种引起类似于在 H^2 时不存在强不可区分性界限的结构问题。然而，据我们所知,在任何 HMAC 应用中这样的弱密钥对不会出现。例如使用任何固定长度短于 d−1 的密钥时（其中 d 是以比特为单位的底层的哈希函数的块长度）就可完全避免出现弱密钥对。因此,我们得出一个结论：当某个应用使用固定长度短于 d−1 的密钥时，HMAC 是与随机预言不可区分的（（有标准良好界限）。

关键词：不可区发性，哈希函数，HMAC

New Preimage Attacks against Reduced SHA-1

Simon Knellwolf[1], and Dmitry Khovratovich[2]
[1]ETH Zurich and FHNW, Switzerland
[2]Microsoft Research Redmond, USA

Abstract. This paper shows preimage attacks against reduced SHA-1 up to 57 steps. The best previous attack has been presented at CRYPTO 2009 and was for 48 steps finding a two-block preimage with incorrect padding at the cost of 2159.3 evaluations of the compression function. For the same variant our attacks find a one-block preimage at 2150.6 and a correctly padded two-block preimage at 2151.1 evaluations of the compression function. The improved results come out of a differential view on the meet-in-the-middle technique originally developed by Aoki and Sasaki. The new framework closely relates meet-in-the-middle attacks to differential cryptanalysis which turns out to be particularly useful for hash functions with linear message expansion and weak diffusion properties.

Keywords: SHA-1, preimage attack, differential meet-in-the-middle

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

对减少轮数的 SHA-1 的新型原象攻击

摘要：此文展示了对 57 轮 SHA-1 的新型原象攻击。之前最好的攻击在 CRYPTO 2009 中提出，它们是针对 48 轮的，以 $2^{159.3}$ 次压缩函数计算得到了一个不正确填充下的两消息块的原象。对于同样轮数，我们的攻击在对压缩函数的 $2^{150.6}$ 次运算中发现一个单消息块的原象，在对压缩函数的 $2^{151.1}$ 次运算后发现一个正确填充的两消息块的原象。这些改进结果来自于对 Aoki 和 Sasaki 提出的中间相遇技术的不同视角处理方法。新型框架把中间相遇攻击和差分密码分析紧密联系在一起，结果证明这对具有线性消息扩展和弱性扩散性能的哈希函数尤其有用。

关键词：SHA-1；原象攻击；差分中间相遇

Universal Composability from Essentially Any Trusted Setup

Mike Rosulek*
Department of Computer Science, University of Montana
mikero@cs.umt.edu

Abstract. It is impossible to securely carry out general multi-party computation in arbitrary network contexts like the Internet, unless protocols have access to some trusted setup. In this work we classify the power of such trusted (2-party) setup functionalities. We show that nearly every setup is either useless (ideal access to the setup is equivalent to having no setup at all) or else complete (composably secure protocols for tasks exist in the presence of the setup). We further argue that those setups which are neither complete nor useless are highly unnatural. The main technical contribution in this work is an almost-total characterization of completeness for 2-party setups. Our characterization treats setup functionalities as black-boxes, and therefore is the first work to classify completeness of arbitrary setup functionalities (i.e., randomized, reactive, and having behavior that depends on the global security parameter).

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

针对几乎任何可信设置的一般可组合性

摘要：除非协议能够访问一些可信设置，否则在任意网络环境下，比如互联网，安全地执行一般多方计算是不可能的。在本论文中，我们将可信设置（两方的）的功能强度进行分类，指出几乎每一个设置要么是无用的(理想访问该设置相当于没有设置)，要么是完备的(设置中存在任务的可组合安全协议)。我们进一步指出那些既不完备也没用的设置是相当不合常理的。本文的主要技术贡献是一个对两方设置完备性的几乎完全的特征描述。我们的特征描述将设置的功能视为黑箱，因此这是首次将任意设置功能（即随机的、有反应的、有取决于全局安全参数的行为的）的完备性进行分类。

Impossibility Results for Static Input Secure Computation

Sanjam Garg[1], Abishek Kumarasubramanian[1],
Rafail Ostrovsky[1], and Ivan Visconti[2]
[1] UCLA, Los Angeles, CA
{sanjamg,abishekk,rafail}@cs.ucla.edu
[2] University of Salerno, Italy
visconti@dia.unisa.it

Abstract. Consider a setting of two mutually distrustful parties Alice and Bob who want to securely evaluate some function on pre-specified inputs. The well studied notion of two-party secure computation allows them to do so in the stand-alone setting. Consider a deterministic function (e.g., 1-out-of-2 bit OT) that Alice and Bob can not evaluate trivially and which allows only Bob to receive the output. We show that Alice and Bob can not securely compute any such function in the concurrent setting even when their inputs are pre-specified. Our impossibility result also extends to all deterministic functions in which both Alice and Bob get the same output. Our results have implications in the bounded concurrent setting as well.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

静态输入安全计算的不可能结果

摘要：考虑如下设置：两个相互不信任参与者爱丽丝和鲍勃，二者打算在预先确定的输入下安全地计算一些函数。经过充分研究的双方安全计算的概念允许他们在独立设置环境下完成上述任务。考虑一个确定性的函数(如 2 比特中 1 比特的不经意传播)，爱丽丝和鲍勃不能简单计算它，而只有鲍勃才能得到输出。研究表明，即使他们的输入是预先定义的，在并发设置中爱丽丝和鲍勃不能安全地计算任何这样的函数。我们不可能的结果可以扩展到所有可使爱丽丝和鲍勃得到相同的输出的确定性函数。我们的结果在有界的并发设置中也具有广泛的意义。

New Impossibility Results for Concurrent Composition and a Non-interactive Completeness Theorem for Secure Computation

Shweta Agrawal[1], Vipul Goyal[2], Abhishek Jain[1],Manoj Prabhakaran[3], and Amit Sahai1, [1] UCLA

[2] Microsoft Research, India, [3] UIUC

Abstract： We consider the client-server setting for the concurrent composition of secure protocols: in this setting, a single server interacts with multiple clients concurrently, executing with each client a specified protocol where only the client should receive any nontrivial output. Such a setting is easily motivated from an application standpoint. There are important special cases for which positive results are known － such as concurrent zero knowledge protocols － and it has been an open question whether other natural functionalities such as Oblivious Transfer (OT) are possible in this setting.

In this work:

• We resolve this open question by showing that unfortunately, even in this very limited concurrency setting, broad new impossibility results hold, ruling out not only OT, but in fact all nontrivial finite asymmetric functionalities. Our new negative results hold even if the inputs of all honest parties are fixed in advance, and the adversary receives no auxiliary information.

• Along the way, we establish a new unconditional completeness result for asymmetric functionalities, where we characterize functionalities that are non-interactively complete secure against active adversaries. When we say that a functionality F is non-interactively complete, we mean that every other asymmetric functionality can be realized by parallel invocations of several copies off with no other communication in any direction. Our result subsumes a completeness result of Kilian [STOC’00] that uses protocols which require additional interaction in both directions.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

并发复合的新不可能性结果和安全计算的非交互完备性定理

摘要：我们考虑实现安全协议并发复合的客户端 - 服务器设置，在此设置中，一台服务器上同时与多个客户端进行交互，与每一个客户执行一个只有客户能够收到非平凡输出的协议。从应用程序的角度来看这样的设置是很容易出现的。有一些存在积极结论的重要的特殊情况，例如并发零知识协议，但在此设置下是否还可能有其他的自然功能，如不经意传输（OT），一直是一个悬而未决的问题。

在这篇论文中：

•我们解决了这个悬而未决的问题。不幸的是，即使是在这个限制严格的并发设置中，存在大量的新的不可能结果。我们不仅排除了不经意传输，而且去除了所有非平凡的非对称密码学功能。，即使诚实各方的输入是先固定的，对手也没有收到辅助信息，我们新的负面结果也是成立的。

•按照这个思路，我们针对非对称功能建立了一套新的无条件完整性结果。在此结果中，我们把抗主动攻击的非交互完备安全功能特征化。当我们说一个功能 F 具有非交互完备性时，我们是指其他任意的非对称功能在没有其它任意方向通信时可以通过并行调用多个副本实现。我们的结果可归入 Kilian [STOC’00] 的完整性结果。后一结果使用的协议需要额外双向交互。

Black-Box Constructionsof Composable Protocols without Set-Up

Huijia Lin[1],_ and Rafael Pass[2],
[1] MIT and Boston University
huijia@csail.mit.edu
[2] Cornell University
rafael@cs.cornell.edu

Abstract. We present the first black-box construction of a secure multi-party computation protocol that satisfies a meaningful notion of concurrent security in the plain model (without any set-up, and withoutassuming an honest majority). Moreover, our protocol relies on the minimal assumption of the existence of a semi-honest OT protocol, and our security notion “UC with super-polynomial helpers” (Canetti etal, STOC’10) is closed under universal composition, and implies super polynomial-time simulation security.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

无设置可复合协议的黑箱构造

摘要：我们提出第一个安全多方计算协议的黑箱构造,这个协议在平凡模型（无设置和无多数人诚实的假设）下满足有意义的并发安全性。而且，我们的协议依赖于存在一种半诚实不经意传播协议的最小假设。我们的“具有超级多项式帮手的 UC”（Canetti etal, STOC’10）安全概念在一般复合下是封闭的，这意味着超多项式的模拟安全性。

Crowd-Blending Privacy

Johannes Gehrke, Michael Hay, Edward Lui, and Rafael Pass
Department of Computer Science, Cornell University
{johannes,mhay,luied,rafael }@cs .cor nell. Edu

Abstract. We introduce a new definition of privacy called crowd-blending privacy that strictly relaxes the notion of differential privacy. Roughly speaking, k-crowd blending private sanitization of a database requires that each individual i in the database "blends" with k other individuals in the database, in the sense that the output of the sanitizer is "indistinguishable" if i's data is replaced by j 's.

We demonstrate crowd-blending private mechanisms for histograms and for releasing synthetic data points, achieving strictly better utility than what is possible using differentially private mechanisms. Additionally, we demonstrate that if a crowd-blending private mechanism is combined with a "pre-sampling" step, where the individuals in the database are randomly drawn from some underlying population (as is often the case during data collection), then the combined mechanism satisfies not only differential privacy, but also the stronger notion of zero-knowledge privacy. This holds even if the pre-sampling is slightly biased and an adversary knows whether certain individuals were sampled or not. Taken together, our results yield a practical approach for collecting and privately releasing data while ensuring higher utility than previous approaches.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

拥挤-混合保密性

摘要：我们介绍一种新的保密性定义，叫做拥挤-混合保密性，它严格放宽了差分保密性的概念。概括的说，一个数据库的 k 位拥挤-混合保密性处理，要求每个个体 i 和数据库中的 K 个个体 j 混合，当 i 的数据被 j 的数据替代时，处理的输出是不能分辨的。

我们用直方图和释放综合数据点证明了拥挤-混合保密性机制，并且相对于差分保密性而言，实用性更好。此外，我们还证明了当拥挤-混合保密机制和预取样相结合时，此时数据库中的个体将被从潜在的群体中随机的获取（数据采集中常出现此种情况），这个结合机制不仅仅满足差分保密性，而且满足更严格的零知识保密性。即使预取样存在些微小偏差或者敌手知道某一特定的个体是否被取样，结果依然成立。综合以上，在确保比之前方法更具使用性的同时，我们在采集和秘密释放数据方面得出了更加实用的方法。

Differential Privacy with Imperfect Randomness

Yevgeniy Dodis[1], Adriana Lo´ pez-Alt[2], Ilya Mironov, and Salil Vadhan[3]

[1]New York University

{dodis,lopez}@cs.nyu.edu

[2]Microsoft Research Silicon Valley

mironov@microsoft.com

[3]Harvard University

salil@seas.harvard.edu

Abstract.：In this work we revisit the question of basing cryptography on imperfect randomness. Bosley and Dodis (TCC'07) showed that if a source of randomness R is "good enough" to generate a secret key capable of encrypting k bits, then one can deterministically extract nearly k almost uniform bits from R, suggesting that traditional privacy notions(namely, indistinguishability of encryption) requires an "extractable" source of randomness. Other, even stronger impossibility results are known for achieving privacy under specific "non-extractable" sources of randomness, such as the γ-Santha-Vazirani (SV) source, where each next bit has fresh entropy, but is allowed to have a small bias $\gamma < 1$(possibly depending on prior bits).

We ask whether similar negative results also hold for a more recent notion of privacy called differential privacy (Dwork et al., TCC'06),concentrating, in particular, on achieving differential privacy with the Santha-Vazirani source. We show that the answer is no. Specifically, we give a differentially private mechanism for approximating arbitrary "low sensitivity" functions that works even with randomness coming from aγ-Santha-Vazirani source, for any $\gamma < 1$. This provides a somewhat surprising "separation" between traditional privacy and differential privacy with respect to imperfect randomness.

Interestingly, the design of our mechanism is quite different from the traditional "additive-noise" mechanisms (e.g., Laplace mechanism) successfully utilized to achieve differential privacy with perfect randomness. Indeed, we show that any (non-trivial) "SV-robust" mechanism for our problem requires a demanding property called consistent sampling, which is strictly stronger than differential privacy, and cannot be satisfied by any additive-noise mechanism.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

具有不完美随机性的差分保密性

摘要：本文重新讨论了将密码学建立在不完美随机性的问题。Bosley 和 Dodis(TCC’07)指出：如果一个随机信源 R 能形成加密 k 比特（信息）的足够好的密钥，那么就能确信地从该信源 R 中抽取几乎均匀的 k 比特，这就表明传统的关于保密性的观点（即就是，加密的不可区分性）需要一个 “可抽取的”随机信源。另外，存在一些在“非抽取”随机源获得保密性的更强的不可能结果，例如γ-Santha-Vazirani (SV) 信源，它的每下一个比特具有不同的熵，但允许有一个满足γ < 1（可能取决于前面比特）的误差。

我们讨论了一个较新的关于保密性的概念，叫做差分保密性（Dwork et al., TCC’06），是否具有类似的负面结果，并特别关注利用 SV 信源实现差分保密性问题。结果是没有这样结论。我们特别给出一个差分保密性机制，它可以无限近似一些“低灵敏度”函数，这些函数甚至可以在随机性的任何满足γ < 1 的γ-Santha-Vazirani (SV) 信源下工作。这就使传统保密性和差分保密性在不完美随机性方面出现了一个有点出人意料的“分歧”。

有趣的是，这种机制的设计与传统的“加性噪声”机制（例如，拉普拉斯机制）大为不同，后一机制被成功地用于实现完美随机性的差分保密性。事实上，我们展示了对于这个问题的任何（非平凡）“SV-稳健”机制需要一个称为持续抽样的特殊性质，这个性质比差分保密性要求更加严格，而任何加性噪声机制都不能满足。

Tamper and Leakage Resilience in the Split-State Model

Feng-Hao Liu and Anna Lysyanskaya
Brown University
{fenghao,anna}@cs.brown.edu

Abstract. It is notoriously difficult to create hardware that is immune from side channel and tampering attacks. A lot of recent literature, therefore, has instead considered algorithmic defenses from such attacks. In this paper, we show how to algorithmically secure any cryptographic functionality from continual split-state leakage and tampering attacks. A split-state attack on cryptographic hardware is one that targets separate parts of the hardware separately. Our construction does not require the hardware to have access to randomness. In contrast, prior work on protecting from continual combined leakage and tampering [23] required true randomness for each update. Our construction is in the common reference string (CRS) model; the CRS must be hard-wired into the device. We note that prior negative results show that it is impossible to algorithmically secure a cryptographic functionality against a combination of arbitrary continual leakage and tampering attacks without true randomness; therefore restricting our attention to the split-state model is justified. Our construction is simple and modular, and relies on a new construction, in the CRS model, of non-malleable codes with respect to split-state tampering functions, which may be of independent interest.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

Split-State 模型中的防篡改性和防泄漏性

摘要：周众所周知，构建一个能抵抗旁路攻击和篡改攻击的硬件是十分困难的。因此，许多目前的文献已经考虑此类攻击的算法防御措施。在本文中，我们将分析如何从算法的角度确保密码功能在面对持续分裂状态泄露和篡改攻击干扰下的安全性。加密硬件所遭遇的分裂状态攻击就是针对每个单独部分的分别攻击。我们的构造不需要硬件访问随机源。然而，在以前的保护措施中，每一次刷新都需要真正的随机源。我们的构造是在公共参考串（CRS）模型下的，CRS 必须硬链入到设备。我们注意到，以前的负面结果表明：在没有真正的随机源条件下，防止任意持续泄漏和篡改的组合攻击而算法上确保加密功能安全性是不可能的，因此，我们的注意力集中在分裂—状态模型上是合理的。我们的构造是简单的和模块化的，在 CRS 模型下，依赖于一个相对分裂状态篡改函数的不可锻造码的新构造，这或许会引起人们的额外兴趣。

Securing Circuits against Constant-Rate Tampering

Dana Dachman-Soled and Yael Tauman Kalai
Microsoft Research New England

Abstract. We present a compiler that converts any circuit into one that remains secure even if a constant fraction of its wires are tampered with. Following the seminal work of Ishai et. al. (Eurocrypt 2006), we consider adversaries who may choose an arbitrary set of wires to corrupt, and may set each such wire to 0 or to 1, or may toggle with the wire. We prove that such adversaries, who continuously tamper with the circuit, can learn at most logarithmically many bits of secret information (in addition to black-box access to the circuit). Our results are information theoretic.

Keywords: side-channel attacks；tampers；circuit complier；PCP of proximity

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

抗电路的恒率篡改

摘要：：我们给出一种编译器，它能把任何电路进行转化，即使该电路的一个恒定的部分线路被篡改仍能保持其安全。根据 Ishai 等人 (Eurocrypt 2006)基础性的研究，我们考虑这样的敌手：她可能选择任意线路集合进行篡改，同时能把线路设为 0 或设为 1，或者用这些线路进行切换。我们证明这样持续篡改电路的敌手，能获取最多对数数量级的秘密信息比特（除了对电路的黑盒访问）。我们的结论是信息理论层面上的。

关键词: 侧信道攻击；篡改；电路编译器；PCP近似问题

How to Compute under AC0 Leakage without Secure Hardware

Guy N. Rothblum

Microsoft Research, Silicon Valley Campus

Abstract. We study the problem of computing securely in the presence of leakage on the computation's internals. Our main result is a general compiler that compiles any algorithm P, viewed as a boolean circuit, into a functionally equivalent algorithm P'. The compiled P' can then be run repeatedly on adversarially chosen inputs in the presence of leakage on its internals: In each execution of P', an AC0 adversary can (adaptively) choose any leakage function that can be computed in AC0 and has bounded output length, apply it to the values on P''s internal wires in that execution, and view its output. We show that no such leakage adversary can learn more than P's input-output behavior. In particular, the internals of P are protected.

Security does not rely on any secure hardware, and is proved under a computational intractability assumption regarding the hardness of computing inner products for AC0 circuits with pre-processing. This new assumption has connections to long-standing open problems in complexity theory.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

在无安全硬件的 AC0 泄漏下如何计算

摘要：: 我们研究了在计算内核组件上存在泄漏时的计算安全性问题。我们的主要成果是一个通用的编译器，它能编译任何算法 *P*，将 P 视为一个布尔电路，并转化成一个功能等价的算法 *P'*。已编译的 *P'*能在有泄漏的内部组件上对敌手选择的输入进行重复运行：每次执行 *P'时*，一个 AC^0 敌手能（自适应地）选择任何泄漏函数，这些函数能在 AC^0 下计算，有有限的输出长度，能应用于 *P'*的内部组件线路在本次执行的取值上，然后观测输出结果。我们说明没有这样的敌手能获取比算法 *P* 的输入输出行为更多的信息。特别是算法 *P* 的内部组件是受到保护的。

其安全性并不依赖于安全硬件，并在一个关于含预处理 AC^0 电路的内积难解性的计算困难性假设下得到了证明。这种新的假设和由来已久的计算复杂性理论中的开放性难题是相联系的。

Recent Advances and Existing Research Questions in Platform Security

Ernie Brickell
Chief Security Architect for Intel Corporation, USA

Abstract. In this talk I will provide a description of recent uses Intel has made of cryptography in our platforms, including providing a hardware random number generator, using anonymous signatures, and improving performance of cryptographic algorithms. I will discuss how processor capabilities could be used more effectively by cryptographic algorithms. I will then discuss research questions in cryptographic protocols and platform security that are motivated by our goals.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

平台安全研究的最新进展和存在问题

摘要：这次报告中，我将介绍 Intel 在我们平台上一些密码学的应用，包括提供硬件的随机数产生器、使用匿名签名和改进密码算法的性能。我还将讨论密码算法如何更有效地应用处理器容量。接下来再讨论与我们研究目标有关的密码协议以及平台安全研究上存在的一些问题。

Tightly Secure Signatures and Public-Key Encryption

Dennis Hofheinz and TiborJager
Karlsruhe Institute of Technology, Germany
{dennis.hofheinz,tibor.jager}@kit.edu

Abstract. We construct the first public-key encryption scheme whose chosen-ciphertext (i.e., IND-CCA) security can be proved under a standard assumption and does not degrade in either the number of users or the number of ciphertexts. In particular, our scheme can be safely deployed in unknown settings in which no a-priori bound on the number of encryptions and/or users is known.

As a central technical building block, we construct the first structure preserving signature scheme with a tight security reduction. (This signature scheme may be of independent interest.) Combining this scheme with Groth-Sahai proofs yields a tightly simulation-sound non-interactive zero-knowledge proof system for group equations. If we use this proof system in the Naor-Yung double encryption scheme, we obtain a tightly IND-CCA secure public-key encryption scheme from the Decision Linear assumption.

We point out that our techniques are not specific to public-key encryption security. Rather, we view our signature scheme and proof system as general building blocks that can help to achieve a tight security reduction.

Keywords: Tight security proofs, structure-preserving signatures, public-key encryption, Groth-Sahaiproofs.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

紧归约的安全签名和公钥加密

摘要：我们构造了首个公钥加密方案, 在一个标准假设和不随用户数量或密文数量降低性能的条件下，可以证明其选择密文(即：IND-CCA)安全性。特别是, 我们的方案可以安全地部署在不知加密和/或用户数的先验界值的未知环境当中。

作为一个核心技术构建模块, 我们构造了首个具有紧归约的保持结构的签名方案(这个签名方案可能具有自身的被关注价值)。该方案与 Groth-Sahai 证明结合则可生成一个关于群方程的紧模拟正确性的非交互式零知识证明系统。如果我们将这个证明系统应用在 Naor-Yung 双重加密方案上, 那我们会由决策线性假设获得一个紧的 IND-CCA 安全的公钥加密方案。我们的技术不是特定于公钥加密安全性。相反, 我们认为我们的签名方案和证据体系能作为一般的构建模块, 可以帮助实现紧的安全规约。

关键词：紧安全性证明，结构保持签名，公钥加密，Groth-Sahai证明

Efficient Padding Oracle Attacks on Cryptographic Hardware

Romain Bardou[1], Riccardo Focardi[2], Yusuke Kawamoto[3], Lorenzo Simionato[2], Graham Steel[1], and Joe-Kai Tsay[4],

[1] INRIA Project ProSecCo, Paris, France, [2] DAIS, Universit`a Ca' Foscari, Venezia, Italy

[3] School of Computer Science, University of Birmingham, UK, [4] Department of Telematics, NTNU, Norway

Abstract. We show how to exploit the encrypted key import functions of a variety of different cryptographic devices to reveal the imported key. The attacks are padding oracle attacks, where error messages resulting from incorrectly padded plaintexts are used as a side channel. In the asymmetric encryption case, we modify and improve Bleichenbacher's attack on RSA PKCS#1v1.5 padding, giving new cryptanalysis that al-lows us to carry out the 'million message attack' in a mean of 49000 and median of 14500 oracle calls in the case of cracking an unknown valid ciphertext under a 1024 bit key (the original algorithm takes a mean of 215000 and a median of 163 000 in the same case). We show how implementation details of certain devices admit an attack that requires only 9400 operations on average (3800 median). For the symmetric case, we adapt Vaudenay's CBC attack, which is already highly efficient. We demonstrate the vulnerabilities on a number of commercially available cryptographic devices, including security tokens, smartcards and the Estonian electronic ID card. The attacks are efficient enough to be practical: we give timing details for all the devices found to be vulnerable, showing how our optimizations make a qualitative difference to the practicality of the attack. We give mathematical analysis of the effectiveness of the attacks, extensive empirical results, and a discussion of countermeasures.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

对密码硬件的有效填充预言攻击

摘要：我们将展示如何利用加密密钥导入功能的各种不同的加密设备,揭示了进口的关键。此次袭击是填充预言攻击,造成不正确的错误的填充明文并用作侧频道。非对称加密的情况下,我们修改和改善 Bleichenbacher 的攻击 RSA PKCS#1v1.5 填充,给新密码分析,艾尔低点使我们开展“百万消息攻击”，在平均 49000 和 14500 的 14 位的中位数的预测，调用破解未知有效的密文在一个 1024 位的密钥(原算法以平均 215 和中位数 163 在相同的情况下)。我们展示了如何实现细节承认攻击的某些设备只需要 9400 次运算（中位数为 3800）。我们证明了一些市售加密设备，包括安全令牌，智能卡和爱沙尼亚电子身份证上的漏洞。这些攻击在实践中是足够有效的，我们给所有设备的定时细节都被发现是脆弱的,我们展示如何优化引起质变到实用性的攻击。我们给出有效攻击和大量实证结果的数学分析 ,并讨论了相应对策。

我们研究了如何利用各种不同密码设备中加密的密钥输入函数来恢复输入密钥。 这种攻击为填充预言攻击，此时由不正确填充的明文导致的错误消息被当作侧信道。在非对称加密情况，我们修正和提高了 Bleichenbacher 关于 RSA PKCS#1v1.5 填充方式的攻击，得到的新分析结果可使我们发动平均 49000 次预言调用的“百万消息攻击”和平均 13500 预言调用的 1024 比特密钥的未知有效密文的破译（原来的攻击算法分别需要 215000 次和 163000 次）。我们展示了完成攻击平均仅需 9400 次（中间值为 3800）运算的特定设备的实现细节。在对称情况，我们修改了原本已很高效的 Vaudenay 的 CBC 攻击。我们展示了一些可商业购买的密码设备的脆弱性，包括安全令牌、智能卡和 Estonian 电子身份卡。攻击是有效的，足以在现实中实现：我们给出所有发现脆弱性的设备的定时细节，指出我们的优化过程如何给出实践攻击能力的质量差异。我们给出了攻击效率的数学分析、扩展的经验结果和反测量的一个讨论。

Public Keys

Arjen K. Lenstra[1], James P. Hughes[2], Maxime Augier[1], JoppeW. Bos[1],
Thorsten Kleinjung[1], and Christophe Wachter[1]
[1] EPFL IC LACAL, Station 14, CH-1015 Lausanne, Switzerland
[2] Self, Palo Alto, CA, USA

Abstract. We performed a sanity check of public keys collected on the web and found that the vast majority works as intended. Our main goal was to test the validity of the assumption that different random choices are made each time keys are generated. We found that this is not always the case, resulting in public keys that offer no security. Our conclusion is that generating secure public keys in the real world is challenging. We did not study usage of public keys.

Keywords: Sanity check, public keys, (batch) factoring, discrete logarithm, Euclidean algorithm, seeding random number generators

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

公钥

摘要：我们对网上收集的公钥进行了正确性检查，发现绝大多数按照预期的那样工作。我们的主要目的是检验这一假设的有效性：每次密钥生成都是不同的随机选择。我们发现并不总是这样的情况，有时会导致不提供安全性的公钥。我们的结论的是，在现实世界中产生安全的公钥是具有挑战性的。我们没有研究使用公钥的问题。

关键词：正确性检查，公钥，（批量）构造，离散对数，欧几里德算法，种子随机数发生器

Multiparty Computation from Somewhat Homomorphic Encryption

Ivan Damg˚ard[1], Valerio Pastro1, Nigel Smart[2], and Sarah Zakarias[1]

[1] Department of Computer Science, Aarhus University

[2] Department of Computer Science, Bristol University

Abstract. We propose a general multiparty computation protocol secure against an active adversary corrupting up to $n-1$ of the n players. The protocol may be used to compute securely arithmetic circuits over any finite field Fpk . Our protocol consists of a preprocessing phase that is both independent of the function to be computed and of the inputs, and a much more efficient online phase where the actual computation takes place. The online phase is unconditionally secure and has total computational (and communication) complexity linear in n, the number of players, where earlier work was quadratic in n. Moreover, the work done by each player is only a small constant factor larger than what one would need to compute the circuit in the clear. We show this is optimal for computation in large fields. In practice, for 3 players, a secure 64-bit multiplication can be done in 0.05 ms. Our preprocessing is based on a somewhat homomorphic cryptosystem. We extend a scheme by Brakerski et al., so that we can perform distributed decryption and handle many values in parallel in one ciphertext. The computational complexity of our preprocessing phase is dominated by the public-key operations, we need $O(n2/s)$ operations per secure multiplication where s is a parameter that increases with the security parameter of the cryptosystem. Earlier work in this model needed $\Omega(n2)$ operations. In practice, the preprocessing prepares a secure 64-bit multiplication for 3 players in about 13 ms.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

由 Somewhat 同态加密实现的多方计算

摘要：我们提出了一个通用安全多方计算协议，它在一个主动攻击的敌手从 n 个参与者中拉拢人数达到 $n-1$ 个的情况下仍然是安全的。该协议可以用于安全地计算任何有限域 $\mathrm{F}pk$ 上的算术电路。我们的协议中包含了一个预处理阶段和一个更效在线阶段，预处理阶段是与被计算函数和输入独立的，，在线阶段是实际计算发生的地方。在线阶段是无条件安全的，总的计算（通信）复杂性与参与者数量 n 呈线性关系，而以前的工作中复杂性是 n 的二次方关系。此外，每个参与者所做的工作只比计算空闲电路多一个很小的常数因子。我们指出这对于大的域而言是最优的。实际的有 3 名参与者的计算中，安全的 64 位乘法可以在 0.05 毫秒完成。我们的预处理是基于一个 samewhat 同态加密系统。我们扩展了 Brakerski 等人的方案，使我们能够用分布式解密，并行处理一个密文中的多个值。预处理阶段的计算复杂度主要由公钥运算产生，每次安全乘法需要 $O\left(n^2/s\right)$ 次运算，其中 s 是与加密安全参数同时增加的参数。在这个模型中，早期的工作需要 $\Omega\left(n^2\right)$ 运算。在实践中，预处理可以在 13 毫秒内为一个有 3 名参与者的安全 64 位乘法做好准备。

Near-Linear Unconditionally-Secure Multiparty Computation with a Dishonest Minority

Eli Ben-Sasson[1],SergeFehr[2], and Rafail Ostrovsky[3]

[1]Department of Computer Science, Technion, Haifa, Israel,
and Microsoft Research New-England, Cambridge, MA
eli@cs.technion.ac.il

[2]Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands
serge.fehr@cwi.nl

[3]Department of Computer Science and Department of Mathematics, UCLA
rafail@cs.ucla.edu

Abstract. In the setting of unconditionally-secure MPC, where dishonest players are unbounded and no cryptographic assumptions are used, it was known since the 1980's that an honest majority of players is both necessary and sufficient to achieve privacy and correctness, assuming secure point-to-point and broadcast channels. The main open question that was left is to establish the exact communication complexity.

We settle the above question by showing an unconditionally-secure MPC protocol, secure against a dishonest minority of malicious players that matches the communication complexity of the best known MPC protocol in the honest-but-curious setting. More specifically, we present a new n-player MPC protocol that is secure against a computationally- unbounded malicious adversary that can adaptively corrupt t<n/2 of the players. For polynomially-large binary circuits that are not too unshaped, our protocol has an amortized communication complexity of $O(n \log n+\kappa/n^{\mathrm{const}})$ bits per multiplication (i.e. AND) gate, where κ denotes the security parameter and const ∈ Z is an arbitrary non-negative constant. This improves on the previously most efficient protocol with the same security guarantee, which offers an amortized communication complexity of $O(n^2K)$ bits per multiplication gate. For any κ polynomial in n, the amortized communication complexity of our protocol matches the O(n log n) bit communication complexity of the best known MPC protocol with passive security.

We introduce several novel techniques that are of independent interest and we believe will have wider applicability. One is a novel idea of computing authentication tags by means of a mini MPC, which allows us to avoid expensive double-sharings; the other is a batch-wise multiplication verification that allows us to speedup Beaver's "multiplication triples".

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

少数不诚实参与者的近似线性无条件安全多方计算

摘要：在无条件安全的 MPC 中，不诚实参与者的计算能力是受限制的，并且不使用密码学假设。自 80 年代以来众所周知的一个结论是：假设存在安全的点对点和广播信道时，多数诚实参与者是实现保密性和正确性的充要条件。留待解决的开放问题是如何确立准确的通信复杂性。

我们通过展示一个无条件安全的 MPC 协议，解决了上述问题，该协议可抵御少数不诚实的恶意攻击者，其通信复杂性可以与诚实但好奇设置下已知最好的 MPC 协议相比。更具体地说,我们提出一个新的 n 个参与者的 MPC 协议，该协议可以免受计算能力不受限制的恶意攻击者的攻击，该攻击者可以自适应地腐蚀 $t < n / 2$ 个参与者。对于多项式规模的不是过于无形的二进制电路来说，该协议具有一个每乘法门 $O(n \log n+\kappa/n^{const})$比特的消减通信复杂度， 其中 k 是安全参数，const∈ Z 是一个任意的非负整数。这改善了以往拥有相同安全性的最有效的协议，后者提供每个乘法门 $O(n^2K)$比特的消减通信复杂度。对于任意以 n 为变量的多项式规模的 k，该协议的消减通信复杂度能够堪比著名的拥有被动安全的 MPC 协议，它的通信复杂度为 $O(n \log n)$比特。

本文介绍了一些新颖的技术，这些技术具有各自独立价值并且我们相信它们将会得到更广泛的应用。其中一项是借助迷你 MPC 计算认证标签的思路，它可以让我们避免昂贵的双倍秘钥共享；另一项技术是分批的乘法验证,可以通过它来加速 Beaver 的“乘法三元组”。

A New Approach to Practical Active-Secure Two-Party Computation

Jesper Buus Nielsen[1], Peter Sebastian Nordholt[1], Claudio Orlandi[2],
and Sai Sheshank Burra[3]
[1]Aarhus University
[2]Bar-Ilan University
[3]Indian Institute of Technology Guwahati

Abstract. We propose a new approach to practical two-party computation secure against an active adversary. All prior practical protocols were based on Yao's garbled circuits. We use an OT-based approach and get efficiency via OT extension in the random oracle model. To get a practical protocol we introduce a number of novel techniques for relating the outputs and inputs of OTs in a larger construction.

We also report on an implementation of this approach, that shows that our protocol is more efficient than any previous one: For big enough circuits, we can evaluate more than 20000 Boolean gates per second. As an example, evaluating one oblivious AES encryption (～34000 gates) takes 64 seconds, but when repeating the task 27 times it only takes less than 3 seconds per instance.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

一种实用的主动安全双方计算新方法

摘要：针对主动安全攻击，我们提出了一个新的实用的双方计算安全方法。先前的所有实用协议都是基于Yao的乱码电路。我们运用一个基于OT（不经意传输）的方法，并通过OT在随机预言模型中的扩展获得高效率。为了得到一个实用的协议，我们引入了一些新颖的技术，在一个较大结构中把OT的输入和输出联系起来。

我们还报告了本方法的一种实现方案，表明我们的协议比以前任何一个都更高效：对于一个足够大的电路，我们可以完成每秒超过 20000 布尔门的计算。比如说，计算一个不经意AES加密（ ~34000门）需要64秒，但当该任务重复27次后每次只需要不到3秒钟。

Efficient Dissection of Composite Problems, with Applications to Cryptanalysis, Knapsacks, and Combinatorial Search Problems

Itai Dinur[1], Orr Dunkelman[1,2], Nathan Keller[1,3], and Adi Shamir[1]
[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. In this paper we show that a large class of diverse problems have a bicomposite structure which makes it possible to solve them with a new type of algorithm called dissection, which has much better time/memory tradeoffs than previously known algorithms. A typical example is the problem of finding the key of multiple encryption schemes with r independent n-bit keys. All the previous error-free attacks required time T and memory M satisfying TM =2rn, and even if “false negatives” are allowed, no attack could achieve TM < 23rn/4. Our new technique yields the first algorithm which never errs and finds all the possible keys with a smaller product of TM, such as T =24n time and M =2n memory for breaking the sequential execution of r =7block ciphers. The improvement ratio we obtain increases in an unbounded way as r increases, and if we allow algorithms which can sometimes miss solutions, we can get even better tradeoffs by combining our dissection technique with parallel collision search. To demonstrate the generality of the new dissection technique, we show how to use it in a generic way in order to attack hash functions with a rebound attack, to solve hard knapsack problems, and to find the shortest solution to a generalized version of Rubik’s cube with better time complexities (for small memory complexities) than the best previously known algorithms.

Keywords: Cryptanalysis, TM-tradeoff, multi-encryption, knapsacks, bicomposite, dissection, rebound.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

复合问题的有效分离及其在密码分析、背包和组合搜索问题的应用

摘要：在本论文中我们指出：一大类分散问题具有双复合结构，使得它们可用一种称为分离算法的新算法进行求解。此算法较以前的算法有更好的时间/内存的权衡能力。一个典型的例子就是找到具有 r 个 比特独立密钥的多重加密方案的密钥问题。所有之前的无错误攻击需要满足 TM=2 的时间 和内存   。即使允许漏报率，没有攻击可以达到 TM<2。我们的新技术产生第一个没有错误的算法，并可以用一个较小的积找到可能的秘钥，例如用 T=24n 的时间和 M=2n 的存储破解 r =7 的顺序执行的分组密码。随着 r 值的增长，我们获得的改进率会无限提高。如果允许算法有时可以无解的话，我们可以通过结合分离技术和并行碰撞搜索得到更好的权衡能力。为了证明新分离技术的普遍性，我们展示了如何用它以一般方式攻击存在反弹攻击的哈希函数、求解背包困难问题，以及用比已知最好算法还优的时间复杂度发现推广 Rubik 魔方问题的最短解。

关键字：密码分析；TM 权衡；多重加密；背包；双复合；分离；反弹

Resistance against Iterated Attacks by Decorrelation Revisited

Aslı Bay, Atefeh Mashatan, and Serge Vaudenay
EPFL, Switzerland
{asli.bay,atefeh.mashatan,serge.vaudenay}@epfl.ch

Abstract.: Iterated attacks are comprised of iterating adversaries who can make *d* plaintext queries, in each iteration to compute a bit, and are trying to distinguish between a random cipher *C* and the ideal random cipher *C** based on all bits. In EUROCRYPT '99, Vaudenay showed that a 2*d*-decorrelated cipher resists to iterated attacks of order *d* when iterations make almost no common queries. Then, he first asked what the necessary conditions are for a cipher to resist a non-adaptive iterated attack of order *d*. Secondly, he speculated that repeating a plaintext query in different iterations does not provide any advantage to a non-adaptive distinguisher. We close here these two long-standing open problems.

We show that, in order to resist non-adaptive iterated attacks of order *d*, decorrelation of order $2d-1$ is not sufficient. We do this by providing a counterexample consisting of a cipher decorrelated to the order $2d-1$ and a successful non-adaptive iterated attack of order *d* against it.

Moreover, we prove that the aforementioned claim is wrong by showing that a higher probability of having a common query between different iterations can translate to a high advantage of the adversary in distinguishing *C* from *C**. We provide a counterintuitive example consisting of a cipher decorrelated to the order 2*d* which can be broken by an iterated attack of order 1 having a high probability of common queries.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

再论通过解相关抵抗迭代攻击

摘要：迭代攻击由一些迭代敌手组成，他们可以询问 d 个明文。在每次迭代中计算一个比特，然后基于所有的比特试图区分一个随机密码 C 和理想的随机密码 C*。在 99 年的欧密会中 Vaudenay 指出：当迭代几乎不做相同询问时，2d 解相关密码可以对抗阶为 d 的迭代攻击。然后，他首先提出什么必要条件可以使一个密码来抵制非自适应 d 阶迭代攻击这一问题。其次，他推测在不同的迭代重复一个明文询问并不能够为非自适应区分器提供任何优势。我们在此解决这两个长期存在的开放性问题。

我们表明，为了抵制阶为 d 的非自适应迭代攻击，阶为 2d-1 的解相关是不充分的。为此，我们提供一个反例，它由解相关至阶为 2d-1 的一个密码和一个对其进行成功的阶为 d 的非自适应迭代攻击构成。

此外，我们通过论证不同迭代之间具有一个相同询问的高概率可以转化为敌手从 C*中区分 C 的高优势，证明上述推测是错误的。我们提供一个违反直觉的例子，包括一个解相关至阶为 2d 的密码，它可以被一个具有高概率相同询问的阶为 1 的迭代攻击所破译。

Secure Identity-Based Encryption in the Quantum Random Oracle Model

Mark Zhandry

Stanford University, USA

Abstract. We give the first proof of security for an identity-based encryption scheme in the quantum random oracle model. This is the first proof of security for any scheme in this model that requires no additional assumptions. Our techniques are quite general and we use them to obtain security proofs for two random oracle hierarchical identity-based encryption schemes and a random oracle signature scheme, all of which have previously resisted quantum security proofs, even using additional assumptions. We also explain how to remove the extra assumptions from prior quantum random oracle model proofs. We accomplish these results by developing new tools for arguing that quantum algorithms cannot distinguish between two oracle distributions. Using a particular class of oracle distributions, so called semi-constant distributions, we argue that the aforementioned cryptosystems are secure against quantum adversaries.

Keywords: Quantum, Random Oracle, IBE, Signatures

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

量子随机预言模型下安全的基于身份加密

摘要：我们首次在量子随机预言模型下证明一个基于身份的加密方案的安全性。这是在该模型下对任意方案安全性的首次证明，而不需要任何额外假设。我们的技术具有相当好的普遍性，我们利用它们证明了两个基于身份的随机预言分层加密方案和一个随机预言签名方案的安全性，而所有这些方案先前都没有量子安全性证明，即使在采用额外假设的条件下也是如此。我们还说明了如何从之前的量子随机预言模型证明中去除额外的假设。我们通过开发新的工具，来证明量子算法不能在两个量子分布中做出识别，从而实现以上结果。使用一类特殊的预言分布，即半常数分布，我们证明上述密码系统对于量子敌手具有安全性。

关键词：量子，随机预言，IBE，签名

Quantum to Classical Randomness Extractors_

Mario Berta[1], Omar Fawzi[2], and Stephanie Wehner[3]

[1] Institute for Theoretical Physics, ETH Zurich

berta@phys.ethz.ch

[2] School of Computer Science, McGill University

ofawzi@cs.mcgill.ca

[3] Centre for Quantum Technologies, National University of Singapore

wehner@nus.edu.sg

Abstract. he goal of randomness extraction is to distill (almost) perfect randomness from a weak source of randomness. When the source outputs a classical string X, many extractor constructions are known. Yet, when considering a physical randomness source, X is itself ultimately the result of a measurement on an underlying quantum system. When characterizing the power of a source to supply randomness it is hence a natural question to ask, how much classical randomness we can extract from a quantum system. To tackle this question we here take on the study of quantum-to-classical randomness extractors (QC-extractors).

We provide constructions of QC-extractors based on measurements in a full set of mutually unbiased bases (MUBs), and certain single qubit measurements. The latter are particularly appealing since they are not only easy to implement, but appear throughout quantum cryptography. We proceed to prove an upper bound on the maximum amount of randomness that we could hope to extract from any quantum state. Some of our QC-extractors almost match this bound. We show two applications of our results.

First, we show that any QC-extractor gives rise to entropic uncertainty relations with respect to quantum side information. Such relations were previously only known for two measurements. In particular, we obtain strong relations in terms of the von Neumann (Shannon) entropy as well as the min-entropy for measurements in (almost) unitary 2-designs, a full set of MUBs, and single qubit measurements in three MUBs each.

Second, we finally resolve the central open question in the noisy storage model Wehner et al., PRL 100, 220502 (2008)] by linking security to the quantum capacity of the adversary's storage device. More precisely, we show that any two-party cryptographic primitive can be implemented securely as long as the adversary's storage device has sufficiently low quantum capacity. Our protocol does not need any quantum storage to implement, and is technologically feasible using present-day technology.

Keywords: randomness extractors, randomness expansion, entropic uncertainty relations, mutually unbiased bases, quantum side information, two-party quantum cryptography, noisy-storage model.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

针对经典随机性提取器的量子论

摘要：随机性提取的目的是为了从弱随机性中提取（几乎）完美的随机性。当数据源输出一个经典字符串 X，许多提取器的构造方法是已知的。然而当考虑物理随机源时，X 本身就是对所涉及量子系统的一个最终测量结果。当描述提供随机性的数据源的能力时，一个很自然的问题就是我们能从一个量子系统中提取出多少经典随机性。为了解决这个问题，我们进行量子至经典随机性提取器（QC-提取器）的研究。

基于相互无偏基（MUB）的一个全集测量和某些单量子比特测量，我们提供了 QC 提取器的一些构造。基于后一种测量的构造更具吸引力，它不仅仅因为易于操作，而且遍及于量子密码学中。我们继续证明了从任意量子状态中希望提取的随机性最大值的上限。一些 QC-提取器几乎匹配这个上限。我们还展示了研究结果的两个应用。

首先，我们指出任何一个 QC 提取器能给出关于量子侧信息的熵的不确定关系，这种关系之前只对两种测量方式是已知的。尤其是我们利用最小熵和冯•诺依曼(Shannon)熵的概念，对（几乎）单一 2 设计测量、MUB 的一个全集和三个 MUB 中单量子比特测量值获得了较强的关系。

其次，我们将敌手存储设备的量子容量和安全性结合起来，解决了噪声存储模型中核心的开放性问题[Wehner et al., PRL 100, 220502 (2008)]。更精确地讲，我们证明了：只要敌手存储设备的量子容量充分低，任意双方密码学部件就可以安全地被实现。我们的协议实施不需要任何量子存储，使用当前技术就可方便实现。

关键词：随机性提取器，随机性扩展，熵的不确定性关系，相互无偏性，量子侧信息，双方量子加密，噪音存储模型

Actively Secure Two-Party Evaluation of Any Quantum Operation

Fr´ed´eric Dupuis[1], Jesper Buus Nielsen[2], and Louis Salvail[3]

[1]Institute for Theoretical Physics, ETH Zurich, Switzerland

dupuis@phys.ethz.ch

[2]Department of Computer Science, Aarhus University, Denmark

jbn@cs.au.dk

[3]Universit´e de Montr´eal (DIRO), QC, Canada

salvail@iro.umontreal.ca

Abstract. We provide the first two-party protocol allowing Alice and Bob to evaluate privately even against active adversaries any completely positive, trace-preserving map F $L(A_{in} \otimes B_{in}) \rightarrow L(A_{out} \otimes B_{out})$, given as a quantum circuit, upon their joint quantum input state ρ in $D(A_{in} \otimes B_{in})$. Our protocol leaks no more to any active adversary than an ideal functionality for F provided Alice and Bob have the cryptographic resources for active secure two-party classical computation. Our protocol is constructed from the protocol for the same task secure against specious adversaries presented in [4].

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

主动安全的任意量子运算的双方计算

摘要：:我们提出了第一个双方协议，在存在主动敌手的情况下，允许 Alice 和 Bob 秘密计算任何完全正定的、迹保持的映射 $F \in L(Ain \otimes Bin) \rightarrow L(Aou\ t \otimes Bou\ t)$。上述映射以量子线路形式给出，其联合量子输入状态 $\rho \in D(Ain \otimes Bin)$ 。假设 Alice 和 Bob 具有经典的主动安全双方计算的密码学资源，我们的协议对任何主动敌手不泄露除 F 的理想函数功能以外的其他信息。我们的协议是从完成同样任务、能抵御[4]中提出的假冒敌手的协议来构建的。

On the Impossibility of Constructing Efficient Key Encapsulation and Programmable Hash Functions in Prime Order Groups

Goichiro Hanaoka, Takahiro Matsuda, and Jacob C.N. Schuldt
Research Institute for Secure Systems,
National Institute of Advanced Industrial Science and Technology
{hanaoka-goichiro,t-matsuda,jacob.schuldt}@aist.go.jp

Abstract. In this paper, we discuss the (im)possibility of constructing chosen ciphertext secure (CCA secure) key encapsulation mechanisms (KEMs) with low ciphertext overhead. More specifically, we rule out the existence of algebraic black-box reductions from the (bounded) CCA security of a natural class of KEMs to any non-interactive problem. The class of KEMs captures the structure of the currently most efficient KEMs defined in standard prime order groups, but restricts an encapsulation to consist of a single group element and a string. This result suggests that we cannot rely on existing techniques to construct a CCA secure KEM in standard prime order groups with a ciphertext overhead lower than two group elements. Furthermore, we show how the properties of an (algebraic) programmable hash function can be used to construct a simple, efficient and CCA secure KEM based on the hardness of the decisional Diffie-Hellman problem with a ciphertext overhead of just a single group element. Since this KEM construction is covered by the above mentioned impossibility result, this enables us to derive a lower bound on the hash key size of an algebraic programmable hash function, and rule out the existence of algebraic (poly, n)-programmable hash functions in prime order groups for any integer n. The latter result answers an open question posed by Hofheinz and Kiltz (CRYPTO’08) in the case of algebraic programmable hash functions in prime order groups.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

在素数阶群中构造高效密钥封装和可编程哈希函数的不可能性

摘要：本文我们讨论了构造具有低密文开销的选择密文安全（CCA 安全）的密钥封装机制（KEMs）的（不）可能性。更具体的说，我们排除了从一个 KEMs 自然类的（有界）CCA 安全性到任何非交互式问题的代数黑箱归约的存在性。这些 KEMs 类具有当前最有效的定义在标准素数阶群上的 KEMs 结构，但是它们是将一个封装构成限制为单一群元素和单字符串。这个结果表明我们不能仅仅依靠现有的技术构造一个 CCA 安全的 KEM，使其工作在标准素数阶群中且其密文开销低于两个群元素。进一步，我们展示了如何利用一个（对称）可编程哈希函数的性质来构造一个简单有效的 CCA 安全的 KEM，使其基于决策性 Diffie-Hellman 问题并且密文开销仅仅为一个群元素。由于这种 KEM 构造属于上述提到的不可能性结果，这就得出代数可编程哈希函数的哈希密钥大小的一个更低界限，排除了任何整数 n 的素数阶群中代数（poly, n）可编程哈希函数的存在性。后一个结果回答了由 Hofheinz and Kiltz（CRYPTO’08）提出的针对素数阶群中代数可编程哈希函数的一个开放性问题。

Hardness of Computing Individual Bits for One-Way Functions on Elliptic Curves

Alexandre Duc[1]and Dimitar Jetchev[2]

[1]LASEC,

[2]LACAL,

EPFL, 1015 Lausanne, Switzerland

Abstract. We prove that if one can predict any of the bits of the input to an elliptic curve based one-way function over a finite field, then we can invert the function. In particular, our result implies that if one can predict any of the bits of the input to a classical pairing-based one-way function with non-negligible advantage over a random guess then one can efficiently invert this function and thus, solve the Fixed Argument Pairing Inversion problem (FAPI-1/FAPI-2). The latter has implications on the security of various pairing-based schemes such as the identity-based encryption scheme of Boneh–Franklin, Hess' identity-based sig-nature scheme, as well as Joux'sthree-party one-round key agreement protocol. Moreover, if one can solve FAPI-1 and FAPI-2 in polynomial time then one can solve the Computational Diffie–Hellman problem (CDH) in polynomial time.

Our result implies that all the bits of the functions defined above are hard-to-compute assuming these functions are one-way. The argument is based on a list-decoding technique via discrete Fourier transforms due to Akavia–Goldwasser–Safra as well as an idea due to Boneh–Shparlinski.

Key words: One-way function, hard-to-compute bits, bilinear pairings, elliptic curves, fixed argument pairing inversion problem, Fourier trans-form, list decoding.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

椭圆曲线上单向函数的单个比特计算的难度

摘要：我们证明了：如果可以预测基于有限域上椭圆曲线的单向函数的任何比特位输入，那么我们可以反转该函数。特别是我们的结论意味着：如果能以超过随机猜测的非微小概率预测经典双线性对单向函数的任何位输入，那么就可以有效地反转此函数，因而可解决固定变量对反演问题（FAPI-1/FAPI-2）。后者意味着多个基于双线性对的方案的安全性，例如 Boneh–Franklin 的基于身份的加密方案、Hess 的基于身份的签名方案和 Joux 的三方单轮密钥协商协议。此外，如果能在多项式时间解决 FAPI-1 与 FAPI-2 问题，也就能在多项式时间内解决计算迪菲—赫尔曼问题（CDH）。

我们的结果表明：如果假定上述定义的这些函数是单向的，则它们的所有比特都是难解的。这些论证是基于 Akavia–Goldwasser–Safra 提出的利用离散傅里叶变换的列表译码技术以及 Boneh–Shparlinski 提出的一个思路。

关键词：单向函数，难解比特，双线性映射，椭圆曲线，固定参数对反演问题，傅立叶变换形式，列表译码。

Homomorphic Evaluation of the AES Circuit

Craig Gentry[1], ShaiHalevi[1], and Nigel P. Smart[2]

[1] IBM Research

[2] University of Bristol

Abstract. We describe a working implementation of leveled homomorphic encryption (without bootstrapping) that can evaluate the AES-128 circuit in three different ways. One variant takes under over 36 hours to evaluate an entire AES encryption operation, using NTL (over GMP) as our underlying software platform, and running on a large-memory machine. Using SIMD techniques, we can process over 54 blocks in each evaluation, yielding an amortized rate of just under 40 minutes per block. Another implementation takes just over two and a half days to evaluate the AES operation, but can process 720 blocks in each evaluation, yielding an amortized rate of just over five minutes per block. We also detail a third implementation, which theoretically could yield even better amortized complexity, but in practice turns out to be less competitive.

For our implementations we develop both AES-specific optimizations as well as several “generic” tools for FHE evaluation. These last tools include (among others) a different variant of the Brakerski-Vaikuntanathan key-switching technique that does not require reducing the norm of the ciphertext vector, and a method of implementing the Brakerski-Gentry-Vaikuntanathan modulus switching transformation on ciphertexts in CRT representation.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

AES 电路的同态计算

摘要：我们描述了一个分层同态加密算法（无自启动）的实现，可以用三种不同方式计算分组长为 128bit 的 AES 算法。第一个实现中，我们将 NTL（GMP 上）作为软件平台，在一个大容量存储的计算机上完成整个的 AES 加密运算需要花费 36 个小时。采用单指令多数据流 SIMD 技术，每一次计算可以处理超过 54 块数据，产生消减处理率不到 40 分钟/块。另一种实现只花了两天半的时间来计算 AES 运算,但在每次评估中可以处理 720 块数据，产生的消减处理率仅仅超过 5 分钟/块。我们还详细描述了第三个实现，在理论上这个可以产生更好的消减处理复杂性，但在实践上证明它不是很有竞争力。

为了我们的实现，我们提出了特定的 AES 优化方法以及几个“通用”工具进行 FHE 全同态计算。这些工具包括（除了其他现存的之外）一个不需要减少密文向量范数的 Brakerski-Vaikuntanathan 密钥转换技术的一个变体，和一个针对 CRT 表示的密文的 Brakerski-Gentry-Vaikuntanathan 模转换变换的实现方法。

Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP

Zvika Brakerski
Stanford University
zvika@stanford.edu

Abstract. We present a new tensoring technique for LWE-based fully homomorphic encryption. While in all previous works, the ciphertext noise grows quadratically ($B \to B^2 \cdot poly(n)$) with every multiplication (before “refreshing”), our noise only grows linearly $B \to B \cdot poly(n)$.

We use this technique to construct a *scale-invariant* fully homomorphic encryption scheme, whose properties only depend on the ratio between the modulus *q* and the initial noise level *B*, and not on their absolute values.

Our scheme has a number of advantages over previous candidates: It uses the same modulus throughout the evaluation process (no need for “modulus switching”), and this modulus can take arbitrary form. In addition, security can be *classically* reduced from the worst-case hardness of the GapSVP problem (with quasi-polynomial approximation factor)，whereas previous constructions could only exhibit a quantum reduction from GapSVP.

Source: CRYPTO 2012, LNCS, vol. 7417, Springer, Heidelberg (2012)

经无模数转换的基于经典 GapSVP 的全同态加密体制

摘要：我们提出了一种新的应用于基于 LWE 问题的全同态密码体制的张量化技术。在先前的工作中，密文噪声随着每一次乘法操作（在密文更新之前）都是平方增长的（$B \to B^2 \cdot poly(n)$），而在本文中，我们的噪声是线性增长的（$B \to B \cdot poly(n)$）。

我们利用这项技术来构造一个尺度不变的全同态加密方案，该方案的性能仅仅依赖于模数 q 和初始噪声水平 B 的比值，而不依赖于它们的绝对值。

与以前的候选算法相比，我们的体制有下述优点：计算过程自始至终使用相同的模数（不用进行模数转换），这个模数可以采用任意形式。而且，方案安全性可以从 GapSVP 困难问题的最差难度进行经典规约得到（在含拟多项式近似因子），但是之前的体制都只能从 GapSVP 困难问题进行量子规约。

Understanding Adaptivity: Random Systems Revisited

Dimitar Jetchev[1], Onur Özen[1], and Martijn Stam[2]

[1] EPFL IC IIF LACAL, Station 14, CH-1015 Lausanne, Switzerland

dimitar.jetchev@epfl.ch, oezen.onur@gmail.com

[2] Department of Computer Science, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol BS8 1UB, UK

stam@compsci.bristol.ac.uk

Abstract. We develop a conceptual approach for probabilistic analysis of adaptive adversaries via Maurer's methodology of random systems (Eurocrypt'02).We first consider a well-known comparison theorem of Maurer according to which, under certain hypotheses, adaptivity does not help for achieving a certain event. This theorem has subsequently been misinterpreted, leading to a misrepresentation with one of Maurer's hypotheses being omitted in various applications. In particular, the only proof of (a misrepresentation of) the theorem available in the literature contained a flaw. We clarify the theorem by pointing out a simple example illustrating why the hypothesis of Maurer is necessary for the comparison statement to hold and provide a correct proof. Furthermore, we prove several technical statements applicable in more general settings where adaptivity might be helpful, which can be seen as the random system analogue of the game-playing arguments recently proved by Jetchev, Özen and Stam (TCC'12).

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

可理解自适应性：随机系统回顾

摘要：依据 Maurer 在 Eurocrypt’02 上所提出的随机系统方法论，我们开发出了一种针对不同敌手进行概率分析的理论方法。首先认为一个众所周知的 Maurer 比较定理, 在一定的假设下, 其自适应性无助于一个特定的事件实现。这一理论随后即被歪曲了，因为在各种各样的应用中人们忽略了 Maurer 所做的假设。尤其是在文献中可查阅到的（被歪曲的）一些定理中，它们的证明过程都包含着这一缺陷。通过一个简单的例子，我们说明为什么 Maurer 所建立的假设对于比较定理证明的正确性是不可或缺的，以此来使该定理变得更为清晰明了。而且，我们证明了一些适用于自适应性可能会有用的更一般环境下的技术声明，这可以被看做是由 Jetchev、Özen 和 Stam 在 TCC’12 上所证明的与博弈论相类似的随机系统。

RKA Security beyond the Linear Barrier:

IBE, Encryption and Signatures

Mihir Bellare[1], Kenneth G. Paterson[2], and Susan Thomson[3]
[1]Department of Computer Science & Engineering,
University of California San Diego
mihir@eng.ucsd.edu
cseweb.ucsd.edu/~mihir/
[2]Information Security Group, Royal Holloway, University of London
kenny.paterson@rhul.ac.uk
www.isg.rhul.ac.uk/~kp
[3]Information Security Group, Royal Holloway, University of London
s.thomson@rhul.ac.uk

Abstract. We provide a framework enabling the construction of IBE schemes that are secure under related-key attacks (RKAs). Specific instantiations of the framework yield RKA-secure IBE schemes for sets of related key derivation functions that are non-linear, thus overcoming a current barrier in RKA security. In particular, we obtain IBE schemes that are RKA secure for sets consisting of all affine functions and all polynomial functions of bounded degree. Based on this we obtain the first constructions of RKA-secure schemes for the same sets for the following primitives: CCA-secure public-key encryption, CCA-secure symmetric encryption and Signatures. All our results are in the standard model and hold under reasonable hardness assumptions.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

超出线性屏障的相关密钥攻击的安全性：IBE，加密和签名

摘要：我们提出了一种实现 IBE 方案构建的框架，这种方案在相关密钥攻击下是安全的。这种框架的具体例子是相关密钥派生函数集的相关密钥攻击下安全 IBE 方案，这种方案是非线性的，从而克服相关密钥攻击下安全的障碍。尤其是，得到的相关密钥攻击下安全 IBE 方案的集合由仿射函数和多项式函数的边界组成。在此基础上，我们得到了对于相同的集合的相关密钥攻击下安全方案的新结构，即，CCA 安全公钥加密，CCA 安全的对称加密和签名。所有的结果都是基于标准模型并符合合理的假设。

Computing on Authenticated Data: New PrivacyDefinitions and Constructions

Nuttapong Attrapadung[1],*,Beno˘ ıt Libert[2],**, and Thomas Peters[2],***

[1]Research Institute for Secure Systems, AIST (Japan)

[2]Universit´ e Catholique de Louvain, ICTEAM Institute (Belgium)

Abstract. Homomorphic signatures are primitives that allow for public computations on authenticated data. At TCC 2012, Ahn et al. defined a framework and security notions for such systems. For a predicate P, the irnotion of P-homomorphic signature makes it possible, given signatures on a message set M, to publicly derive a signature on any message m’ such that P(M,m) = 1. Beyond unforgeability, Ahn et al. considered a strong notion of privacy – called strong context hiding – requiring that derived signatures be perfectly indistinguishable from signatures newly generated by the signer. In this paper, we first note that the definition of strong context hiding may not imply unlinkability properties that can

be expected from homomorphic signatures in certain situations. We then suggest other definitions of privacy and discuss the relations among them. Our strongest definition, called complete context hiding security, is shown to imply previous ones. In the case of linearly homomorphic signatures, we only attain a slightly weaker level of privacy which is nevertheless stronger than in previous realizations in the standard model. For subsetpredicates, we prove that our strongest notion of privacy is satisfiable and describe a completely context hiding system with constant-size public keys. In the standard model, this construction is the first one that allows signing messages of arbitrary length. The scheme builds on techniques that are very different from those of Ahn et al.

Keywords: Homomorphic signatures, provable security, privacy, un-linkability, standard model.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

认证数据的计算:新的隐私定义和结构

摘要：同态签名是允许公众认证数据计算的原语。对于这样的体系，Ahn等人在TCC 2012上，定义了一个框架和安全的概念。对于谓词p，其p的同态签名理念使得给任何信息m公开得到在信息集合M的签名P（M，m’）=1成为可能。Ahn等人，超越不可伪造性，考量了强隐私的概念－称为强语境隐藏－要求得到签名的签名者和新生成的签名完全不可区分。在本文中，我们首先注意到定义强语境隐藏可能并不意味着不可链接性，可以期望在一定情况下得到同态签名。然后我们提出了其他的隐私定义并讨论了它们之间的关系。我们最强的定义称之为完整语境隐藏安全性的提出是隐含前面已经提到概念的。在线性同态签名的情况下，只能达到一个较弱的隐私级别，但是比在以前实现的标准模型还是要更强一些。对于子集谓词，我们证明了隐私权的概念和定义能满足最强描述的具有恒定大小的公钥完全语境隐藏系统。在标准模型中，这种结构是第一个允许任意长度消息签名的。该模型是建立在基于不同于Ahn等人的技术之上的。

关键字：同态签名；可证明安全性；隐私；不可链接；标准模型

A Coding-Theoretic Approach to Recovering Noisy RSA Keys

Kenneth G. Paterson, Antigoni Polychroniadou, and Dale L. Sibborn
Information Security Group, Royal Holloway, University of London

Abstract. Inspired by cold boot attacks, Heninger and Shacham (Crypto2009) initiated the study of the problem of how to recover an RSA private key from a noisy version of that key. They gave an algorithm for the case where some bits of the private key are known with certainty. Their ideas were extended by Henecka, May and Meurer (Crypto 2010) to produce an algorithm that works when all the key bits are subject to error. In this paper, we bring a coding-theoretic viewpoint to bear on the problem of noisy RSA key recovery. This viewpoint allows us to cast the previous work as part of a more general framework. In turn, this enables us to explain why the previous algorithms do not solve the motivating cold boot problem, and to design a new algorithm that does (and more).In addition, we are able to use concepts and tools from coding theory– channel capacity, list decoding algorithms, and random coding techniques– to derive bounds on the performance of the previous and our new algorithm.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

一个用来恢复有噪声的 RSA 密钥的编码理论方法

摘要：本文的灵感来自于冷启动攻击。Heninger 和 Shacham(Crypto 2009)发起了如何从冗余的密钥中恢复一个 RSA 私钥的研究。他们为有些私钥的信息是确知的情况给出了算法。他们的想法得到 Henecka,May 和 Meurer(Crypto 2010)的进一步的延伸，共同提出了一个算法,该算法在所有密钥比特都可能错误的情况下仍有效。在本文中,我们用编码理论的观点来解决有噪声的 RSA 密钥恢复问题。这个观点让我们把以前的工作作为一个更广泛的框架的一部分。反过来,这可以解释为什么前面的算法不能解决激励冷启动,并要设计一种新的算法的问题。另外,我们还可依据编码理论使用概念和工具——信道容量、列表译码算法,随机编码技术——以获得之前的性能界限和我们新算法。

Certifying RSA

Faculty of Mathematics

Horst-Görtz Institute for IT Security

Ruhr-University Bochum, Germany

{saqib.kakvi,eike.kiltz,alex.may}@rub.de

Abstract. We propose an algorithm that, given an arbitrary N of un-known factorization and prime e ⩾ $N^{1/4+\varepsilon}$, certifies whether the RSA function $RSA_{N,e}(x):=x^e \bmod N$ defines a permutation over Z^*_N or not.

The algorithm uses Coppersmith’s method to find small solutions of poly-nomial equations and runs in time $O(\varepsilon^{-8}\log^2 N)$. Previous certification techniques required e >N.

Keywords: RSA, certified trapdoor permutations, Coppersmith.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

RSA 认证

摘要：我们提出了一个算法。对任意未知的分解 N 和素数 e $\geqslant N^{1/4+\varepsilon}$情况下，该算法证明了 RSA 函数 $RSA_{N,e}(x):=x^{e}\bmod N$ 是否是关于 Z^{*}_{N} 的一个置换。

该算法使用了 Coppersmith 的方法来求解多项式方程的小解,在 $O(\varepsilon^{-8}\log^{2}N)$ 时间内。而先前的认证技术要求 e>N.

关键词：RSA , 认证陷门置换 ,Coppersmith

Faster Gaussian Lattice SamplingUsing Lazy Floating-Point Arithmetic

L′ eo Ducas[1] and Phong Q. Nguyen[2]

[1] ENS, Dept. Informatique, 45 rue d’Ulm, 75005 Paris, France

http://www.di.ens.fr/~ducas/

[2] INRIA, France and Tsinghua University, Institute for Advanced Study, China

http://www.di.ens.fr/~pnguyen/

Abstract. Many lattice cryptographic primitives require an efficient algorithm to sample lattice points according to some Gaussian distribution. All algorithms known for this task require long-integer arithmetic at some point, which may be problematic in practice. We study how much lattice sampling can be sped up using floating-point arithmetic. First, we show that a direct floating-point implementation of these algorithms does not give any asymptotic speedup: the floating-point precision needs to be greater than the security parameter, leading to an overall complexity˜O(n^3) where n is the lattice dimension. However, we introduce a laziness technique that can significantly speed up these algorithms. Namely, in certain cases such as NTRUSign lattices, laziness can decrease the complexity to ˜O(n^2) or even ˜O(n). Furthermore, our analysis is practical: for typical parameters, most of the floating-point operations only require the double-precision IEEE standard.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

使用浮点数算法实现更快高斯格抽样

摘要：很多格加密体制主体在依据高斯分布抽样格点时需要高效的算法。为此，所有已知的算法在某些情况下都需要长整型计算。这可能在实际操作上会出现问题。我们对格抽样如何能加快浮点数运算进行了研究。首先，我们认为直接使用浮点数操作不会给任何渐进加速，浮点数的精度需要大于安全参数，实现了一个 n 为格维度的复杂度 O(n^3)。然而，我们提出的惰性技术却大大提高了这些算法的速度。即：在一些特定的情况下如 NTRUSign 格（数字签名技术)，惰性可以将其复杂度减少到˜O(n^2)，甚至到˜O(n)。此外，我们的分析有实用性：对于典型的参数而言，大多数浮点数操作只要求双精度 IEEE 的标准。

Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures

L′eo Ducas[1] and Phong Q. Nguyen[2]

[1] ENS, Dept. Informatique, 45 rue d’Ulm, 75005 Paris, France

http://www.di.ens.fr/~ducas/

[2]INRIA, France and Tsinghua University, Institute for Advanced Study, China

http://www.di.ens.fr/~pnguyen/

Abstract. NTRUSign is the most practical lattice signature scheme.Its basic version was broken by Nguyen and Regev in 2006: one can efficiently recover the secret key from about 400 signatures. However, countermeasures have been proposed to repair the scheme, such as the perturbation used in NTRUSign standardization proposals, and the deformation proposed by Hu *et al.* at IEEE Trans. Inform. Theory in 2008. These two countermeasures were claimed to prevent the NR attack. Surprisingly, we show that these two claims are incorrect by revisiting the NR gradient-descent attack: the attack is more powerful than previously expected, and actually breaks both countermeasures in practice, *e.g.* 8,000 signatures suffice to break NTRUSign-251 with one perturbation as submitted to IEEE P1363 in 2003. More precisely, we explain why the Nguyen-Regev algorithm for learning a parallelepiped is heuristically able to learn more complex objects, such as zonotopes and deformed parallelepipeds.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

了解 Zonotope 及更多:NTRUSign 干扰的密码分析方法

摘要：NTRUSign 是一种非常实用的格签名策略。它的基本版本在 2006 年被 Nguyen and Regev 破解：他们可以从 400 个签名中恢复出密钥。然而，已经有对策出台修复这个策略，比如扰动技术在 NTRUSign 标准中的应用，以及 HU 等人 2008 年在 IEEE Trans. Inform. Theory 上提出的变形技术。这两种干扰对策被宣称可以有效的抵抗 NR 攻击。意外的是，我们阐述了这么一个事实：重新研究 NR 的梯度下降攻击，会发现这两种宣称是错误的。这种攻击比之前估计的更加厉害，而且，可以破解两种干扰策略。比如说：对 8000 个签名进行 2003 年在 IEEE P1363 上提出的扰动就可以有效的破解 NTRUSign-251。更准确地说，我们解释了为什么 Nguyen-Regev 算法对于学习平行六面体可以启发式地研究更复杂的物体，比如 zonotopes 和变形的平行六边形。

On Polynomial Systems Arising from a Weil Descent

Christophe Petit and Jean-Jacques Quisquater
UCL Crypto Group,
Universit´ e catholique de Louvain
Place du Levant 3
1348 Louvain-la-Neuve (Belgium)
{christophe.petit,jjq}@uclouvain.be

Abstract. In the last two decades, many computational problems arising in cryptography have been successfully reduced to various systems of polynomial equations. In this paper, we revisit a class of polynomial systems introduced by Faug`ere, Perret, Petit and Renault. Based on new experimental results and heuristic evidence, we conjecture that their degrees of regularity are only slightly larger than the original degrees of the equations, resulting in a very low complexity compared to generic systems. We then revisit the application of these systems to the elliptic curve discrete logarithm problem (ECDLP) for binary curves. Our heuristic analysis suggests that an index calculus variant due to Diem requires a sub-exponential number of bit operations $O(2^{cn^{2/3}\log n})$, where c is a constant smaller than F_{2^n} .According to our estimations, generic discrete logarithm methods are outperformed for any n > N where N ≈ 2000, but elliptic curves of currently recommended key sizes (n ≈ 160) are not immediately threatened. The analysis can be easily generalized to other extension fields.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

Weil Descent 中的多项式系统

摘要：在过去的二十年里，许多密码学中的计算问题已经成功地减少为由多项式方程组成的各种系统。在本文中，我们重新研究了由Faug`ere, Perret, Petit和Renault提出的一类多项式系统。基于新的实验结果和启发性的证据，我们猜想这些系统呈现规律性的程度只是略大于原来方程的程度，这就导致了比一般系统更低的复杂度。然后我们重新研究了这些系统在二进制曲线的椭圆曲线离散对数问题(ECDLP)上的应用。我们的启发式分析表明指数级的微积分变量需要亚指数位操作的数量级为$O(2^{cn^{2/3}\log n})$，这里c是比F_{2^n}小的一个常量。通过我们的估计，对于任何n > N并且N ≈ 2000通用离散对数方法更具优势，但是现行的椭圆曲线的推荐密钥大小（n ≈ 160）暂时并没有受到威胁。这些分析可以很容易的推广到其它扩域。

ECM at Work

Joppe W. Bos[1] and Thorsten Kleinjung[2]
[1]Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA
[2]Laboratory for Cryptologic Algorithms, EPFL, Lausanne, Switzerland

Abstract. The performance of the elliptic curve method (ECM) for integer factorization plays an important role in the security assessment of RSA-based protocols as a cofactorization tool inside the number field sieve. The efficient arithmetic for Edwards curves found an application by speeding up ECM. We propose techniques based on generating and combining addition-subtracting chains to optimize Edwards ECM in terms of both performance and memory requirements. This makes our approach very suitable for memory-constrained devices such as graphics processing units (GPU). For commonly used ECM parameters we are able to lower the required memory up to a factor 55compared to the state-of-the-art Edwards ECM approach. Our ECM implementation on a GTX 580 GPU sets a new throughput record, outperforming the best GPU, CPU and FPGA results reported in literature.

Key words: Elliptic curve factorization, cofactorization, addition-subtraction chains, twisted Edwards curves, parallel architectures.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

椭圆曲线的工作方式

摘要：椭圆曲线方法的性能表现作为在数域筛法的一个内外分解工具方面对整数分解在基于 RSA 协议的安全性评估方面扮演了一个重要的角色。通过加速椭圆曲线方法，发现了 Edwards 曲线的高效运算的一种应用。我们在性能与内存要求方面提出了基于产生与结合加减链达到优化椭圆曲线方法的技术方法。这使得我们的方法非常适合于内存受限的设备，如图形处理单元（GPU）。相较于最先进的 Edwards 椭圆曲线方式，我们能把一般的 Edwards 椭圆曲线方法应用参数降低达到设备的 55%。我们在 GTX 580 GPU 上的应用创造了一个新的吞吐率记录，跑赢了有文献记载的最好的 GPU，CPU，FPGA。

关键字：椭圆曲线分解；内外分解；加减链；扭曲的 Edwards 曲线；平行架构

IND-CCA Secure Cryptography Based on a Variant of the LPN Problem

Nico Dottling1, Jorn Muller-Quade[1] , and Anderson C.A. Nascimento[2]

[1] Karlsruhe Institute of Technology, Karlsruhe, Germany

[2] University of Brasilia, Brasilia, Brazil

andclay@ene.unb.br

Abstract. In 2003 Michael Alekhnovich (FOCS 2003) introduced a novel variant of the learning parity with noise problem and showed that it implies IND-CPA secure public-key cryptography. In this paper we introduce the first public-key encryption-scheme based on this assumption which is IND-CCA secure in the standard model. Our main technical tool to achieve this is a novel all-but-one simulation technique based on the correlated products approach of Rosen and Segev (TCC 2009). Our IND-CCA1 secure scheme is asymptotically optimal with respect to ciphertext-expansion. To achieve IND-CCA2 security we use a technique of Dolev, Dwork and Naor (STOC 1991) based on one-time-signatures. For practical purposes, the efficiency of the IND-CCA2 scheme can be substantially improved by the use of additional assumptions to allow for more efficient signature schemes. Our results make Alekhnovich’ s variant of the learning parity with noise problem a promising candidate to achieve post quantum cryptography.

Keywords:IND-CCA2 Security, Learning Parity with Noise, All-But-One Decryption.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

基于 LPN 问题变体的 IND-CCA 安全的密码体制

摘要：：2003 年，Michael Alekhnovich (FOCS 2003)提出一种新的 LPN 问题（Learning Parity with Noise problem）的变体，并说明它是满足 IND-CCA 安全的公钥密码体制。本文我们介绍标准模型下 IND-CCA 安全的基于该假设的第一个公钥加密体制。基于 Rosen 和 Segev (TCC 2009)方法的相关产品，我们主要的方法是新颖且可重复性的可仿真技术。对于密文扩展来说，我们的 IND-CCA1 安全体制是近乎理想的。为了获得 IND-CCA2 安全，我们使用了 Dolev, Dwork and Naor (STOC 1991)的一种方法，该方法基于一次一签名。为了更加实用，对于更高效的签名方案采用一些额外的假设，满足 IND-CCA2 安全的密码体制的效率能有实质上的提升。我们的结论使得 Alekhnovich 的 LPN 问题变体成为后量子密码体制中颇有前景的候选算法。

关键词：IND-CCA2 安全；噪声奇偶性学习问题（LPN 问题）；可重复性加密

Provable Security of the Knudsen-Preneel Compression Functions

Jooyoung Lee
Faculty of Mathematics and Statistics
Sejong University, Seoul, Korea 143-747
jlee05@sejong.ac.kr

Abstract. This paper discusses the provable security of the compression functions introduced by Knudsen and Preneel[11,12,13] that use linear error-correcting codes to build wide-pipe compression functions from underlying block ciphers operating in Davies-Meyer mode. In the information theoretic model, we prove that the Knudsen-Preneel compression function based on an $[r,k,d]_{2^e}$ code is collision resistant up to $2^{\frac{(r-d+1)n}{2r-3d+3}}$ query complexity if $2d \le r+1$ and collision resistant up to $2^{\frac{rn}{2r-2d+2}}$ query complexity if $2d > r+1$. For MDS code based Knudsen-Preneel compression functions, this lower bound matches the upper bound recently given by ¨Ozen and Stam[23].

A preimage security proof of the Knudsen-Preneel compression functions has been first presented by ¨Ozen et al. (FSE ’10). In this paper, we present two alternative proofs that the Knudsen-Preneel compression functions are preimage resistant up to $2^{\frac{rn}{k}}$ query complexity. While the first proof, using a wish list argument, is presented primarily to illustrate an idea behind our collision security proof, the second proof provides a tighter security bound compared to the original one.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

Knudsen-Preneel 压缩函数的可证明安全

摘要：本文探讨了由 Knudsen 和 Preneel 提出的压缩函数的可证明安全性，利用线性纠错码，从以 Davies-Meyer 形式操作的密文里构造宽管道的压缩函数。在信息论模型下，我们证明 Knudsen 和 Preneeldev 基于$[r,k,d]_{2^e}$码的压缩函数在$2d \le r+1$的情况下，其查询复杂性直到$2^{\frac{(r-d+1)n}{2r-3d+3}}$是抗碰撞的，在$2d > r+1$的情况下，其查询复杂性直到$2^{\frac{rn}{2r-2d+2}}$是抗碰撞的，对基于 MDS 码的 Knudsen-Preneel 压缩函数，这个下限与 Ozen 和 Stam 给出的上限相匹配。

Knudsen-Preneel 压缩函数的原像安全的证明最初是由 Ozen et al(FSE ’10)给出的。在本文中，我们给出了 Knudsen-Preneel 压缩函数对直到$2^{\frac{rn}{k}}$的询问复杂性都抗原像攻击的两种证明。在第一种证明中，使用一个之前提到的愿望参数列表来列举我们的碰撞安全性证明的思路。第二种证明提供了一个比原来的那个更严格的安全界限。

Optimal Collision Security in Double Block Length Hashing with Single Length Key

Bart Mennink
Dept. Electrical Engineering, ESAT/COSIC, KU Leuven, and IBBT, Belgium
bart.mennink@esat.kuleuven.be

Abstract. The idea of double block length hashing is to construct a compression function on 2n bits using a block cipher with an n-bit block size. All optimally secure double length hash functions known in the literature employ a cipher with a key space of double block size, 2n-bit.On the other hand, no optimally secure compression functions built from a cipher with an n-bit key space are known. Our work deals with this problem. Firstly, we prove that for a wide class of compression functions with two calls to its underlying n-bit keyed block cipher collisions can be found in about $2^{n/2}$queries. This attack applies, among others, to functions where the output is derived from the block cipher outputs in a linear way. This observation demonstrates that all security results of designs using a cipher with 2n-bit key space crucially rely on the presence of these extra key bits. The main contribution of this work is a proof that this issue can be resolved by allowing the compression function to make one extra call to the cipher. We propose a family of compression functions making three block cipher calls that asymptotically achieves optimal collision resistance up to$2^{n(1-\varepsilon)}$queries and preimage resistance up to $2^{3n(1-\varepsilon)/2}$queries, for any ε>0. To our knowledge, this is the first optimally collision secure double block length construction using a block cipher with single length key space.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

单长度密钥下双分组长度哈希运算的最优碰撞安全性

]摘要：双分组长度哈希是指用一个分组长度为 n 比特的分组密码来构造一个 2n 比特的压缩函数。现文献中所有已知安全性最佳的双分组长度哈希函数，其密钥空间均为双分组长度，即 2n 比特。另一方面，还没有密钥空间为 n 比特的压缩函数是最佳安全性的。我们的工作就是处理这个问题。首先，我们证明对于一大类压缩函数，调用两次它所依托的 n 比特键控分组密码，经过 2n/2 次查询后可以找到碰撞。这个攻击还适用于输出线性来源于分组密码输出的算法。这个结论证明了密钥空间为 2n 比特的算法的安全性结果严重依赖于额外的 n 个密钥比特。这项工作的主要贡献在于证明了用压缩函数额外调用一次密码算法就可以解决这个问题。我们提出了一个压缩函数族，访问调用三次分组密码，对任意 ε>0，可渐进达到抗 2n(1−ε)次查询的最佳抗碰撞性和抗 23n(1−2ε)次查询的抗原像性。据我们所知，这是第一个使用单密钥空间分组密码达到碰撞安全性最佳的双分组长度构造。

Investigating Fundamental Security Requirements on Whirlpool: Improved Preimage and Collision Attacks

Yu Sasaki[1], Lei Wang[2,3], ShuangWu[4], and Wenling Wu[4]
[1]NTT Corporation
[2]The University of Electro-Communications
[3]Nanyang Technological University
wushuang@is.iscas.ac.cn
[4] Institute of Software, Chinese Academy of Sciences

Abstract. In this paper, improved cryptanalysis for the ISO standard hash function Whirlpool are presented with respect to the fundamental security notions. While a subspace distinguisher was presented on full version (10 rounds) of the compression function, its impact to the security of the hash function seems limited. In this paper, we discuss the (second) preimage and collision attacks for the hash function and the compression function of Whirlpool. Regarding the preimage attack, 6rounds of the hash function are attacked with 2481 computations while the previous best attack is for 5 rounds with 2481.5 computations. Regarding the collision attack, 8 rounds of the compression function are attacked with 2120 computations, while the previous best attack is for7 rounds with 2184 computations. To verify the correctness, especially for the rebound attack on the Sbox with an unbalanced Differential Distribution Table (DDT), the attack is partially implemented, and the differences from attacking the Sbox with balanced DDT are reported.

Keywords: Whirlpool, preimage, collision, meet-in-the-middle, guess and determine, local collision.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

探索漩涡散列函数的基本安全要求:改进原象及碰撞攻击

摘要：本文就 ISO 散列函数标准 Whirlpool 进行**研究**，针对其基本安全概念展开进一步密码分析，提出了子空间辨义成分在完整版(10 轮)的压缩功能,其影响的安全散列函数似乎是有限的。在本文中,我们讨论对漩涡散列函数和压缩函数的(二)原象和碰撞攻击。对于原象攻击,用 2481 次计算则 6 轮的散列函数即被攻击，而之前最佳攻击是用 2481.5 计算且只 5 轮。对于碰撞攻击,2120 次计算 8 轮压缩函数被攻击,而之前最好的攻击是 2184 计算 7 轮。为了验证其准确性,尤其是针对不平衡的微分分布 s-盒(DDT）的反弹攻击，攻击仅仅实现了一部分。本文还就攻击平衡微分分布 s-盒(DDT）的各种不同情况做了报告。

关键词：Whirlpool；原象；碰撞；中间相遇；猜测和决定；局部碰撞

Generic Related-Key Attacks for HMAC

Thomas Peyrin[1], Yu Sasaki[2], and Lei Wang[1,3]

[1]Division of Mathematical Sciences, School of Physical and Mathematical Sciences,
Nanyang Technological University, Singapore thomas.peyrin@gmail.com, wang.lei@ntu.edu.sg

[2]NTT Secure Platform Laboratories, NTT Corporation sasaki.yu@lab.ntt.co.jp

[3]The University of Electro-Communications

Abstract. In this article we describe new generic distinguishing and forgery attacks in the related-key scenario (using only a single related-key) for the HMAC construction. When HMAC uses a k-bit key, outputs an n-bit MAC, and is instantiated with an l-bit inner iterative hash function processing m-bit message blocks where m = k, our distinguishing-R attack requires about 2n/2 queries which improves over the currently best known generic attack complexity 2l/2 as soon as l > n. This means that contrary to the general belief, using wide-pipe hash functions as internal primitive will not increase the overall security of HMAC in the related-key model when the key size is equal to the message block size. We also present generic related-key distinguishing-H, internal state recovery and forgery attacks. Our method is new and elegant, and uses a simple cycle-size detection criterion. The issue in the HMAC construction (not present in the NMAC construction) comes from the non-independence of the two inner hash layers and we provide a simple patch in order to avoid this generic attack. Our work finally shows that the choice of the opad and ipad constants value in HMAC is important.

Keywords: HMAC, hash function, distinguisher, forgery, related-key.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

HMAC 的通用相关密钥攻击

摘要：在本文中,我们描述了在 HMAC 构建的关键环节中的新的泛型区分分析和伪造攻击。当 HMAC 使用 k 位键,输出一个 n 位 MAC,是与一个 1 位的内部实例化迭代散列函数处理位信息块,在这个信息块中 m = k,我们区分 r 攻击需要约 $2^n/2$ 次查询,当 l> n 时，它比当前最著名的通用攻击提高复杂度 $2^l/2$ 有提高。这意味着与一般观点相反,当键尺寸等于消息块大小时，在项关键模型中使用宽管散列函数作为内部原始不会增加 HMAC 的整体安全性。我们也提出了通用的相关密钥的区别-H，内部状态恢复和伪造攻击。我们的方法是前沿并且细致的,使用一个简单的循环周期检测标准。HMAC 构造中的问题（NMAC 建设中的不存在）来源于两个非独立的的内哈希层，而且我们还提供了简单的补丁来防止这种泛型攻击。我们的工作终于表明选择 opad 和 ipad 常量值在 HMAC 是非常重要的。

关键词：HMAC,哈希函数，区分，伪造，相关密钥

The Five-Card Trick Can Be Done with Four Cards

Takaaki Mizuki, Michihito Kumamoto, and Hideaki Sone
Cyberscience Center, Tohoku University,
Aramaki-Aza-Aoba 6-3, Aoba-ku, Sendai 980-8578, Japan

Abstract. The “five-card trick” invented by Boer allows Alice and Bob to securely compute the AND function of their secret inputs using five cards—three black cards and two red cards—with identical backs. This paper shows that such a secure computation can be done with only four cards. Specifically, we give a protocol to achieve a secure computation of AND using only four cards—two black and two red. Our protocol is optimal in the sense that the number of required cards is minimum.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

“五张卡牌花招”可用四张卡牌实现

摘要：波尔（Boer）发明的“五张卡牌技巧”使爱丽丝（Alice ）和鲍勃（Bob）能够用相同背面图案的三黑两红的五张卡牌来安全计算他们的秘密输入的 AND 函数。这篇文章描述了这样的安全计算可以同样用四张卡牌来完成。具体说来，我们给出一个协议来实现只用两红两黑四张卡牌就可以完成 AND 函数的安全计算。在所需卡牌数量最小的情况下，我们的协议是最佳的。

A Mix-Net from Any CCA2 Secure Cryptosystem

Shahram Khazaei, TalMoran, and Douglas Wikstr¨om
KTH Royal Institute of Technology
IDC Herzliya

Abstract. We construct a provably secure mix-net from any CCA2 secure cryptosystem.

The mix-net is secure against active adversaries that statically corrupt less than out of k mix-servers, where λ is a threshold parameter, and it is robust provided that at most min(λ − 1, k − λ) mix-servers are corrupted.

The main component of our construction is a mix-net that outputs the correct result if all mix-servers behaved honestly, and aborts with probability 1 −O(H−(t−1)) otherwise (without disclosing anything about the inputs), where t is an auxiliary security parameter and H is the number of honest parties. The running time of this protocol for long messages is roughly 3tc, where c is the running time of Chaum's mix-net (1981).

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

一个来自 CCA2 安全加密系统的混合网

摘要：我们构造了一个可证的来自 CCA2 安全加密系统的安全混合网。这个混合网能防御静态腐败小于出自 k 混合服务器的 λ 的主动攻击，其中 λ 是一个阈值参数，假如至多最小量(λ － 1, k － λ)的混合服务器被损坏时，此参数最强健。我们结构的主要成分是一个混合网，如果所有的混合服务器表现公正那么它就输出正确的结果，出现1-O$\left(H^{-(t-1)}\right)$的概率时则就中止（不透露任何输入），其中 t 是一个辅助的安全参数，H 是一诚信群的一个数字。该此协议的运行长消息的时间大致是 3tc，其中 c 是 Chaum 的混合网的运行时间（1981 年）。

How Not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios

David Bernhard[1], Olivier Pereira[2], and Bogdan Warinschi[1]

[1] University of Bristol

[2] Universit′ e Catholique de Louvain

Abstract. The Fiat-Shamir transformation is the most efficient construction of non-interactive zero-knowledge proofs.

This paper is concerned with two variants of the transformation that appear but have not been clearly delineated in existing literature. Both variants start with the prover making a commitment. The strong variant then hashes both the commitment and the statement to be proved, whereas the weak variant hashes only the commitment. This minor change yields dramatically different security guarantees: in situations where malicious provers can select their statements adaptively, the weak Fiat-Shamir transformation yields unsound/unextractable proofs.

Yet such settings naturally occur in systems when zero-knowledge proofs are used to enforce honest behavior. We illustrate this point by showing that the use of the weak Fiat-Shamir transformation in the Helios cryptographic voting system leads to several possible security breaches: for some standard types of elections, under plausible circumstances, malicious parties can cause the tallying procedure to run indefinitely and even tamper with the result of the election.

On the positive side, we define a form of adaptive security for zero-knowledge proofs in the random oracle model (essentially simulation-sound extractability), and show that a variant which we call strong Fiat-Shamir yields secure non-interactive proofs.

This level of security was assumed in previous works on Helios and our results are then necessary for these analyses to be valid. Additionally, we show that strong proofs in Helios achieve non-malleable encryption and satisfy ballot privacy, improving on previous results that required CCA security.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

如何不去证明你自己：Fiat-Shamir 启发式教育法的陷阱及其对 Helios 的应用

摘要：菲亚特-沙米尔（Fiat-Shamir）转换是最有效的非交互式零知识的证明的构建。

本文涉及进行转换的两个变量，其在现有的文献中还没有较为清晰的描述。两个变量都从证明者做出承诺开始。强变量计算该承诺的哈希值以及需证明的陈述数值，然而弱变量只是计算承诺的哈希值而已。这个微小的改变产生了明显不同的安全保障：在恶意证明者选择适配的陈述数值的情况时，弱的Fiat-Shamir转换会给出不完全的/不可推断的证明。

然而这种情况只有当零知识证明被用作执行诚实行为的时候才会在系统中自然而然的发生。我们通过弱的Fiat-Shamir转换在Helios加密投票系统中的使用导致了一些可能的安全漏洞来说明这一点:对于一些标准类型的选举,在貌似合理的情况下,恶意方可以使计数程序无限制的一直运行下去,甚至可以篡改选举的结果。

从积极的一面来看, 在随机预言模型中我们对于零知识证明定义了一个自适应安全的形式(实质上是伪完全提取性),并且展示了我们称之为强Fiat-Shamir的一个变量给出安全的无交互式的证明。

这种级别的安全假设是在以往对 Helios 的研究中提出的，那么我们的研究结果对于这些分析的正确性就是必需的。此外，我们还表明通过改善需要达到 CCA 安全的以前的选举结果，Helios 已被强有力地证明可实现不可扩展的加密并满足选举隐私的需要。

Sequential Aggregate Signatures with Lazy Verification from Trapdoor Permutations (Extended Abstract)

Kyle Brogle[1],Sharon Goldberg[2], and Leonid Reyzin[2]

[1]Stanford University Department of Computer Science
Stanford, CA 94305 USA
broglek@stanford.edu

[2]Boston University Department of Computer Science
Boston, MA 02215 USA
{goldbe,reyzin }@cs.bu.edu

Abstract. Sequential aggregate signature schemes allow n signers, in order, to sign a message each, at a lower total cost than the cost of n individual signatures. We present a sequential aggregate signature scheme based on trapdoor permutations (e. g. , RSA). Unlike prior such proposals, our scheme does not require a signer to retrieve the keys of other signers and verify the aggregate-so-far before adding its own signature. Indeed, we do not even require a signer to know the public keys of other signers!

Moreover, for applications that require signers to verify the aggregate anyway, our schemes support lazy verification: a signer can add its own signature to an unverified aggregate and forward it along immediately, postponing verification until load permits or the necessary public keys are obtained. This is especially important for applications where signers must access a large, secure, and current cache of public keys in order to verify messages. The price we pay is that our signature grows slightly with the number of signers.

We report a technical analysis of our scheme (which is provably secure in the random oracle model), a detailed implementation-level specification, and implementation results based on RSA and OpenSSL. To evaluate the performance of our scheme, we focus on the target application of BGPsec (formerly known as Secure BGP), a protocol designed for securing the global Internet routing system. There is a particular need for lazy verification with BGPsec, since it is run on routers that must process signatures extremely quickly, while being able to access tens of thousands of public keys. We compare our scheme to the algorithms currently proposed for use in BGPsec, and find that our signatures are considerably shorter non-aggregate RSA (with the same sign and verify times) and have an order of magnitude faster verification than non-aggregate ECDSA, although ECDSA has shorter signatures when the number of signers is small.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

基于陷门置换的连续聚合签名的懒惰验证 (扩展摘要)

摘要：允许 n 个签名者依次签一个消息的连续聚合签名方案总花费比 n 个个人签名的总花费要低。我们展示了一个建立在陷门置换（例如，RSA）的基础上的连续聚合签名方案。与之前的方案不同，在添加自己签名的之前，该方案不需要签名者检索其他签名者的秘钥，到目前为止，也不需要核实其他集合。实际上，我们甚至不需要签名者知道其他签名者的公钥。

此外，对于那些无论如何都需要签名者验证集合的应用来说，我们的方案是懒惰验证：一个签名者可以把自己的签名添加到未经核实的集合上，然后立刻传送它，可将验证延迟到负载许可或获得必要的公钥时。这对那些签名者为了证实信息而必须获取大量安全现有的公钥储藏的应用来说尤其重要。我们要付出的代价是随着签名者数量的增加我们的签名也略微增长。

我们展示了我们方案的一个技术分析（在随机预言模型里这可能是安全的），一份详细的操作级别的规格，和基于 RSA 和 OpenSSL 的操作结果。为了鉴定方案的性能，我们专注于 BGPsec 的目标应用（原来的安全边界网关协议），这个协议的设计是为了保护全球互联网路由系统的安全。BGPsec 特别需要懒惰核实，因为它运行在在能获得成千上万个公钥时就必须快速处理签名的路由器上。我们把该方案和现有的用在 BGPsec 上的算法进行比较，发现我们的签名是相当短的（有相同标志和验证时）无集合 RSA，还拥有比无集合 ECDSA 快一个数量级的验证，尽管当签名者的数量很小时，ECDSA 有更少的签名。

Calling Out Cheaters: Covert Security with Public Verifiability

Gilad Asharov[1] and Claudio Orlandi[2,**]
[1] Department of Computer Science, Bar-Ilan University, Israel
[2]Department of Computer Science, Aarhus University, Denmark
asharog@cs.biu.ac.il, orlandi@cs.au.dk

Abstract. We introduce the notion of covert security with public verifiability, building on the covert security model introduced by Aumannand Lindell (TCC 2007). Protocols that satisfy covert security guarantee that the honest parties involved in the protocol will notice any cheating attempt with some constant probability . The idea behind the model is that the fear of being caught cheating will be enough of a deterrent to prevent any cheating attempt. However, in the basic covert security model, the honest parties are not able to persuade any third party (say, a judge) that a cheating occurred. We propose (and formally define) an extension of the model where, when an honest party detects cheating, it also receives a certificate that can bepublished and used to persuade other parties, without revealing any information about the honest party’s input. In addition, malicious parties cannot create fake certificates in the attempt of framing innocents. Finally, we construct a secure two-party computation protocol for any functionality f that satisfies our definition and our protocol is almost as efficient as the one of Aumann and Lindell. We believe that the fear of a public humiliation or even legal consequences vastly exceeds the deterrent given by standard covert security. Therefore, even a small value of the deterrent factor will suffice in discouraging any cheating attempt.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

呼唤欺骗者：公开验证的秘密安全

摘要：我们介绍了建立在由 Aumannand Lindell (TCC 2007)提出的隐蔽安全模型基础上的公开验证的秘密安全性的概念。能满足秘密安全性的协议确保在协议中涉及到的可信各方都会注意到任何一些常数概率的欺骗尝试。该模型背后的理念是，作弊时会被抓到的恐惧将成为足够预防作弊的威慑。然而，在最基本的秘密安全模型中，可信方不能说服作弊出现时的任何一个第三方（比如一个法官）。我们提出(正式定义)模型的一个扩展,当可信方发现作弊行为时，也会收到一个可以发布和用来说服其他方的证书,而不需透露可信方的任何信息。而且，在构造无辜者尝试中恶意者不能伪造证书。最后，我们，为可以满足我们定义的任何值函数 f 构建了一个安全的双方计算协议,本协议和 Lindell Aumann 之一几乎是一样有效。我们相信对公开羞辱或者法律后果的恐惧远远超过标准的秘密安全的带来的威慑。因此，在阻止任何作弊的尝试中，即使一个小值的威慑因素就足够了。

A Unified Framework for UC from Only OT

Rafael Pass[1], Huijia Lin[2], and Muthuramakrishnan Venkitasubramaniam[3]

[1] Cornell University, Ithaca NY 14850, USA

[2] MIT and Boston University, Boston, MA, 02138, USA

[3] University of Rochester, Rochester, NY 14611, USA

Abstract. In [1], the authors presented a unified framework for constructing Universally Composable (UC) secure computation protocols, assuming only enhanced trapdoor permutations. In this work, we weaken the hardness assumption underlying the unified framework to only the existence of a stand-alone secure semi-honest Oblivious Transfer (OT) protocol. The new frame work directly implies new and improved UC feasibility results from only the existence of a semi-honest OT protocol in various models. Since in many models, the existence of UC-OT implies the existence of a semi-honest OT protocol.

Furthermore, we show that by relying on a more fine-grained analysis of the unified framework, we obtain concurrently secure computation protocols with super-polynomial-time simulation (SPS), based on the necessary assumption of the existence of a semi-honest OT protocol that can be simulated in super-polynomial times. When the underlying OT protocol has constant rounds, the SPS secure protocols constructed also have constant rounds. This yields the first construction of constant round secure computation protocols that satisfy a meaningful notions of concurrent security (i.e., SPS security) based on tight assumptions.

A notable corollary following from our new unified frame work is that standalone(or bounded-concurrent) password authenticated key-exchange protocols(PAKE) can be constructed from only semi-honest OT protocols; combined with the result of [2] that the existence of PAKE protocols implies that of OT, we derive a tight characterization of PAKE protocols.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

一个来自只有 OT 的 UC 的统一框架

摘要：在[1]中,假设只有增强活板门的排列，作者提出了一个统一的框架来构建普遍可组合(UC)的安全计算协议。在我们的文章中，我们削弱了作为统一框架的基础的硬度假设，让它只剩一个独立的安全转移(OT)半诚实的无视协议。新的支架直接意味着新的和改进过的来自于仅存的 OT 协议中的半诚实各种模型的可行性结果。因为在许多模型中 UC-OT 的存在意味着半诚实的 OT 协议的存在。

此外,我们表明,依靠对统一框架的更细粒度的分析,我们同时获得了具有超级多项式时间仿真(SPS)的安全计算协议,基于一种半诚实 OT 协议的存在的必要假设，此协议可以用超级多项式模拟。当底层 OT 协议有常数轮,SPS 安全协议构造的也有常数轮。这就产生了常数轮安全计算协议的第一个构建，此协议满足了基于严谨假设上的并发安全的有意义概念。

在我们的新的研究中有一个显著的推论是独立的(或有界并发)密码认证密钥交换协议(PAKE)可由有半诚实 OT 协议构成;结合[2]的结果,PAKE 协议的存在意味着,我们从 OT 中得到了一个 PAKE 协议的紧密的特征。

Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication

Patrick Longa[1] and Francesco Sica[2], [1] Microsoft Research, USA, plonga@microsoft.com

[2] Nazarbayev University, Kazakhstan, francesco.sica@nu.edu.kz

Abstract. The GLV method of Gallant, Lambert and Van-stone (CRYPTO 2001) computes any multiple kP of a point P of prime order n lying on an elliptic curve with a low-degree endomorphism Φ(called GLV curve) over Fp as $k P = k1P+k2\Phi(P)$,with $\max\{|k1|,|k2|\} \leq C1\sqrt{n}$,for some explicit constant C1>0.

Recently, Galbraith, Lin and Scott (EUROCRYPT 2009) extended this method to all curves over Fp2 which are twists of curves defined over Fp. We show in this work how to merge the two approaches in order to get, for twists of any GLV curve over Fp2, a four-dimensional decomposition together with fast endomorphisms Φ, Ψ over Fp2 acting on the group generated by a point P of prime order n, resulting in a proven decomposition for any scalar

$k \in [1,n]$ given by $kP =k1P+k2\Phi(P)+k3(P)+k4\Psi\Phi(P)$ with $maxi(|ki |) <C2n1/4$,

for some explicit C2>0. Remarkably, taking the best C1,C2,we obtain C2/C1<412, independently of the curve, ensuring in theory an almost constant relative speedup. In practice, our experiments reveal that the use of the merged GLV-GLS approach supports a scalar multiplication that runs up to 50% times faster than the original GLV method. We then improve this performance even further by exploiting the Twisted Edwards model and show that curves originally slower may become extremely efficient on this model. In addition, we analyze the performance of the method on a multicore setting and describe how to efficiently protect GLV-based scalar multiplication against several side-channel at-tacks. Our implementations improve the state-of-the-art performance of point multiplication for a variety of scenarios including side-channel protected and unprotected cases with sequential and multicore execution.

Keywords: Elliptic curves, GLV-GLS method, scalar multiplication, Twisted Edwards curve, side-channel protection, multicore computation

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

四维 Gallant-Lambert-Vanstone 标量乘法

摘要：Gallant, Lambert 和 Van-stone 提出的 GLV 方法(CRYPTO 2001) 是用来计算任意 kP 的乘积的，其中点 p 是一个基于椭圆曲线低阶自同构的 n 阶素数，其中Φ（GLV 曲线）对于 Fp 有 k P = k1P+k2Φ(P)，max{|k1|,|k2|} ≤ C1$\sqrt{n}$，其中一些常数 C1>0。

近期，Galbraith, Lin 和 Scott (EUROCRYPT 2009)对这种方法做了进一步扩展使它适用所有 Fp2 上所有的曲线都适用，Fp2 是定义在 Fp 上的曲率。在这项工作中我们展示如何合并这两种方法去得到 Fp2 上任意 GLV 曲线的曲率；一种四维的分解与快速同态Φ,Ψ 在 由 n 阶素数 P 生成的 Fp2 上的任何标量 k ∈ [1,n] , Kp=k1P+k2Φ(P)+k3(P)+k4ΨΦ(P),maxi(|ki |) <C2n1/4，其中一些常数 C2>0.。值得注意的是，最好的 C1，C2，我们得到 C2/C1<412，独立的曲线，确保在理论上几乎恒定的相对加速比。在实践中，我们的实验揭示了，使用合并后的 GLV GLS 方法支持标量乘比原来的 GLV 方法最多可多运行 50%次。之后我们利用扭 Edwards 模型进一步改善了这种性能，我们发现这种模型使原本比较慢的曲线变得非常高效。此外，我们分析了这种方法在多核设置的表现，并介绍了如何有效地保护基于 GLV 的标量乘法对抗几个侧信道的攻击。我们的方法改善了当前各种情况下的点乘计算，包括在侧通道保护和未受保护的情况下和连续的多核点乘。

关键词：椭圆曲线，GLV-GLS 方法，标乘，扭 Edwards 曲线，侧信道保护，多核计算

Shuffling against Side-Channel Attacks:

A Comprehensive Study with Cautionary Note

Nicolas Veyrat-Charvillon, Marcel Medwed,
St′ephanie Kerckhof, and Francois-Xavier Standaert
Universit′e Catholique de Louvain, UCL Crypto Group,
B-1348 Louvain-la-Neuve, Belgium

Abstract. Together with masking, shuffling is one of the most frequently considered solutions to improve the security of small embedded devices against side-channel attacks. In this paper, we provide a comprehensive study of this countermeasure, including improved implementations and a careful information theoretic and security analysis of its different variants. Our analyses lead to important conclusions as they moderate the strong security improvements claimed in previous works. They suggest that simplified versions of shuffling (e.g. using random start indexes) can be significantly weaker than their counterpart using full permutations. We further show with an experimental case study that such simplified versions can be as easy to attack as unprotected implementations. We finally exhibit the existence of “indirect leakages” in shuffled implementations that can be exploited due to the different leakage models of the different resources used in cryptographic implementations. This suggests the design of fully shuffled (and efficient) implementations, were both the execution order of the instructions and the physical resources used are randomized, as an interesting scope for further research.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

对抗侧信道攻击的扰乱方案：作为警示的综合研究

摘要：连同伪装方式，扰乱是最经常被考虑的提高小型嵌入式设备应对侧信道攻击的安全性的解决方案之一。在这篇文章中，我们提供这一对抗方法的综合研究，包括改进的方法及对不同变量的详细信息理论分析和安全分析。我们的分析得出的重要结论是以前研究中声称的这种方案的极大的安全改进并不完善，分析表明简化了的扰乱（如使用随机开始索引）会比对手使用全排列薄弱很多，我们进一步用实验案例研究表明,使用这种简化方式其受攻击的容易程度相当于那些没有保护的设备，我们最后展示了扰乱方案中“间接泄露”的存在，从而被加密方案中使用的不同资源的不同泄露模式所利用。这表明完全扰乱（及有效的）方案的设计中指令的执行顺序和所用的物理资源都是随机的，这可作为进一步研究的兴趣方向。

Theory and Practice of a Leakage Resilient Masking Scheme

Josep Balasch[1], Sebastian Faust[2],
Benedikt Gierlichs[1], and Ingrid Verbauwhede[2]
[1] KU Leuven Dept. Electrical Engineering-ESAT/SCD-COSIC and IBBT
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be
[2] Aarhus University
Abogade 34, DK-8200 Aarhus, Denmark
sfaust@cs.au.dk

Abstract. A recent trend in cryptography is to formally prove the leakage resilience of cryptographic implementations – that is, one formally shows that a scheme remains provably secure even in the presence of side channel leakage. Although many of the proposed schemes are secure in a surprisingly strong model, most of them are unfortunately rather inefficient and come without practical security evaluations nor implementation attempts. In this work, we take a further step towards closing the gap between theoretical leakage resilient cryptography and more practice-oriented research. In particular, we show that masking countermeasures based on the inner product do not only exhibit strong theoretical leakage resilience, but moreover provide better practical security or efficiency than earlier masking countermeasures. We demonstrate the feasibility of inner product masking by giving a secured implementation of the AES for an 8-bit processor.

Keywords: Inner product masking, AES, Leakage resilience.

Source: ASIACRYPT 2012, LNCS, vol. 7658, Springer, Heidelberg (2012)

泄漏弹性的掩蔽策略的理论和实践

摘要：密码学研究最近趋势是正式证明加密方案的泄漏弹性，也就是说，要正式表明一种方案即使存在信道泄漏也是可证明安全的。尽管许多已提出的方案在极强的模式中都是安全的。但遗憾的是许多方法相当低效，并且没有实际性的安全评估，也没有尝试实现。在本文，我们进一步缩短了理论泄漏弹性密码和更具有实际导向的研究之间的差距。我们特别展示了基于内部产品的掩蔽对抗不仅具有较强的理论泄漏适应性，而且，相比较于之前的掩蔽对抗提供了更好的实际安全性或有效性，通过一个 8 位处理器的 AES 的安全实现，我们证明了内部产品掩蔽的可行性，。

关键词：内部产品掩蔽,AES,泄漏弹性

敬告读者

本刊已在北京电子科技学院数字图书馆平台上建立了中英文摘要：及原文数据库，欢迎读者检索查询原文及其他详细信息。

网址： http://www.lib.besti.edu.cn/

本刊的创办需要各方面的关怀，更需要同行专家学者的赐教。我们衷心欢迎大家的意见与建议，请将您的宝贵建议通过以下方式转给我们：

联系人：郎永清

电话：010-83635200， 13522687802

电子邮件：lance@besti.edu.cn

北京电子科技学院
密码与信息安全情报研究室
2013年10月25日