抗选择密文攻击公钥密码体制的研究*

梅其祥[1,2,3]，唐小虎[1]，何大可[1]

(1.西南交通大学 计算机与通信工程学院，四川 成都 610031；2.中国科学院 研究生院 信息安全国家重点实验室，北京 100039；3.中南大学 信息工程学院，湖南 长沙 410075)

摘　要：抗选择密文攻击公钥密码体制是安全性很高的密码体制,它是设计抗主动攻击的协议非常有用的工具。总结该体制的构造与应用的主要研究成果,并指出了几个值得进一步研究的问题。

关键词：加密；选择密文安全性；密码协议

中图法分类号：TP309　　**文献标识码**：A　　**文章编号**：1001-3695(2006)02-0019-03

Study of Public Key Encryption Secure Against Chosen Ciphertext Attacks

MEI Qi-xiang[1,2,3], TANG Xiao-hu[1], HE Da-ke[1]

(1. *School of Computer Science & Communication Engineering, Southwest Jiaotong University, Chengdu Sichuan* 610031, *China*; 2. *State Key Laboratory of Information Security, Graduate School, Chinese Academy of Sciences, Beijing* 100039, *China*; 3. *School of Information Science & Engineering, Central South University, Changsha Hunan* 410075, *China*)

Abstract: The public key cryptosystem secure against chosen ciphertext attacks is a very strong secure cryptosystem and is a useful primitive for designing protocols that resisting active adversary. This paper surveys the main results about its construction and applications available in the literature. The authors also point out some important problems that deserve to be further studied.

Key words: Encryption; Chosen Ciphertext Security; Cryptography Protocol

Internet 的飞速发展,给人们展现了非常美好的前景。然而由于黑客事件和病毒事件发生频繁,信息安全问题成为信息产业的瓶颈。网络安全和信息安全保障能力也是国家综合国力的体现,是世界各国奋力攀登的制高点。

公钥密码技术[20]是现代密码技术的最重要的组成研究内容之一。传统对称密码的加密密钥与解密密钥相同,加/解密简单、高效,但是传送、保管密钥是一个难题,也无法构造有效率的数字签名方案。而公钥密码的加密密钥与解密密钥不同,虽然加/解密速度较慢,但是很好地解决了密钥管理问题,并能用于数字签名、身份认证,可以为电子商务、电子政务等提供有力的密码技术保障。

在公钥密码体制中,攻击者拥有公钥,可以随便选择明文进行加密,所以一个公钥密码体制起码应该能抗选择明文攻击。另外,在开放的网络环境中,攻击者还会利用各种途径获得密文,并获得相应的解密,相比传统对称密码体制,公钥密码更易受到选择密文攻击。

抗选择密文攻击密码体制[31]是一种安全性很高的体制。现在它已是被密码学家们普遍接受的概念。研究表明,利用抗选择密文攻击密码体制,可以设计许多安全强度很高的、重要的密码协议,如密钥传输、密钥交换、公平交换协议等等。Bellare 和 Rogaway 提出的 OAEP(1994)体制[9]成为 SET 协议的新的加密标准。抗选择密文攻击是当今公钥加密候选标准的最重要的要求之一,2004 年最新的几个候选标准[25]的原型就是几个重要的抗选择密文攻击公钥加密方案。

收稿日期：2005-03-25；修返日期：2005-05-06

基金项目：国家自然科学基金资助项目(60302015)；信息安全国家重点实验室 2004 年第一批开放课题(01-01)

1　公钥密码体制安全性概念

公钥密码体制的安全性按照可能的攻击目标,可以分为:①单向性(OW)安全。由密文不能恢复相应的明文,这是一个加密方案最基本的要求。②不可区分性(IND)安全。对攻击者给定的两个明文,加密者随机一致地选择其中一个进行加密,攻击者无法从密文中知道是对哪个明文的加密。③非延展性(NM)安全。攻击者无法构造与已给密文相关的新密文。这些安全性概念依次加强:NM 比 IND 强,IND 比 OW 强。

密码体制的安全性也是根据抗攻击的能力来确定的,而攻击按照模型可分为:①选择明文(CPA)攻击。攻击者可以先适应地选择明文,获得相应的密文。在公钥密码中,攻击者拥有公钥,可以随便加密,进而实现选择明文攻击。②非适应性选择密文(CCA1)攻击。攻击者除了可以适应地选择明文攻击外,在给定挑战密文前,还可以适应地选择密文获得相应的解密。③适应性选择密文(CCA2)攻击。攻击者的唯一限制就是不可以直接用挑战密文获得相应的明文,即还可以在给定挑战密文后,适应地选择密文获得相应的解密。

同时考虑攻击目标和攻击模型,可以获得不同的安全,其中强度最大也最重要的是 IND-CCA2 和 NM-CCA2 安全[5],而两者被证明是等价的,所以加密中通常所说的选择密文安全是指 IND-CCA2 安全。

2 研究现状

1991 年, Rackoff 和 Simon[31] 首先提出 IND-CCA2 概念。由于抗选择密文攻击的重要意义, 吸引了一大批国际著名的密码学家对其进行大量的研究, 下面进行介绍。

(1) IND-CCA2 安全公钥加密方案

1994 年, Bellare 和 Rogaway 提出的 OAEP(Optimal Asymmetric Encryption Padding) 体制, 将任意陷门置换转换为 IND-CCA2, 第一次将较弱的体制转换为 IND-CCA2。OAEP 是第一个可被证明且可以实用的 IND-CCA2 方案, 具有非常重要的地位。但是, 它要求假设 Hash 函数是理想的, 即是在 "Random Oracle Model"[8] 意义下的。

1998 年 Cramer 和 Shoup 提出了一种实用的 IND-CCA2 方案(CS98 方案)[17], 该方案是第一个 "真实世界"(在标准的数论假设下) 的(而不是 "Random Oracle Model" 意义下的) 方案, 而且具有实用价值, 因而具有重要的意义, 被广泛引用; 其安全性基于决定性 Diffi-Hellman (DDH) 假设, 该假设被认为比标准的计算性 Diffi-Hellman CDH 假设强。该方案相对 Random Oracle 模型中基于 Diffie-Hellman 问题的 IND-CCA2 方案, 加密、解密速度, 以及密钥长度都大约是它们的两倍。所以, Random Oracle 模型中的方案有效率高的优势, 但标准模型中的方案不需假设 Hash 函数是理想的。

1999 年, Fujisaki 和 Okamoto[22] 将任何抗选择明文攻击(IND-CPA) 的方案转换为其 IND-CCA2 方案, 它的特点是具有通用性, 相对被转换的方案, 其加密速度、密文长度都不变, 但解密中的验证过程要求重新加密。

2000 年, Pointchaval[30] 提出了将单向陷门函数转换为 IND-CCA2 的方法, 也具有通用性, 且比 FO99 的通用转换的范围更广, 其效率与 FO99 转换基本相同, 解密中的验证过程也要求重新加密。

2000 年, Shoup[33] 对 CS98 方案进一步改进, 一方面, 当 DDH 假设成立, 该方案在真实世界依然是 IND-CCA2 安全的; 另一方面, 当 DDH 假设成立不成立, 该方案在 Random Oracle Model 中, 在 CDH 假设下是 IND-CCA2 安全的, 而且效率较 CS98 方案高。2002 年 Cramer 和 Shoup[18] 对 CS98 方案、S00 方案进一步改进提高, 并推广成平滑 Hash 证明系统, 给出了基于另外假设的几个方案。

2001 年, Okamoto 和 Pointcheval [29] 的 REACT 转换中首次提出了公钥和私钥相结合的方法, 将在明密文检测攻击下单向性安全(OW-PCA) 的加密转换为 IND-CCA2, 其解密验证不需重新加密, 效率很高, 而且可以处理长消息。

2001 年, Shoup 在 ISO(2001) 公钥加密标准草案[35] 中提出了密钥封装的模式, 即将抗选择密文攻击的公钥系统和抗选择密文攻击的私钥系统结合, 这样公钥部分专门用来封装会话密钥, 私钥系统专门用来处理实际要加密的数据。

2001 年, Abdalla, Bellare 和 Rogway 提出了 DHIES 方案[1]。该方案将 ElGamal 加密和消息认证码、私钥密码系统结合。其效率非常高, 不需要 Random Oracle, 其安全性基于 Oracle Diffie-Hellman 假设, 这是一种不太标准的数论假设, 在 Random Oracle 模型中, 这种假设等价于 Gap Diffie-Hellman(GDH) 假设[28]。

2004 年, Kurosawa 和 Desmedt [26] 提出了一种新的标准模型中的 IND-CCA2 加密, 该方案以 CS98 方案为基础, 但减少了密文长度, 提高了计算效率, 是目前为止标准模型的效率最高的方案。

2004 年, Canetti 等人[15] 提出了利用基于身份加密来构造 IND-CCA2 加密的新思想, 与 Boneh 和 Boyen 2004 年提出的两个高效的基于身份加密结合, 可以得到标准模型的新的方案[10]。

(2) IND-CCA2 安全门限密码方案

1998 年, Shoup 和 Gennaro[36] 提出了建立抗选择密文攻击密码门限体制的安全性模型, 并在 Random Oracle Model 中提出了两个高效的方案, 其安全性分别基于 DDH 假设和 CDH 假设; 1999 年, Canetti 和 Goldwasser[14] 基于 CS98 方案, 提出了在标准模型中的门限 IND-CCA2, 但由于 CS98 方案中的密文的合法性不能公开验证, 使得 CG99 方案需要预先计算大量的随机数和进行大量的交互。另外, 由于 CHK04 方案可以公开验证, 可以将它们转换为标准模型中的门限 IND-CCA2 方案, 而且是非交互式的。

(3) IND-CCA2 加密与其他密码协议

Bellare 等探讨与密钥传输[4]、认证密钥交换[6] 的关系、其他公钥加密概念之间[7] 的关系, Canetti 和 Krawczk 考虑与安全(认证且保密) 信道[16]、基于口令的认证密钥交换[24] 的关系, Asokan 等人[2] 探索了与公平交换的关系。用 CCA2 加密来设计认证密钥交换协议, 可以实现 Bellare 等人提出的安全模型, 而该模型可以抵抗所有已知的各种攻击, 如字典攻击、中间人攻击、抗已知会话密钥攻击(指已经被攻破的会话密钥不会对未被恢复的会话密钥产生不利影响)。用 CCA2 加密可以实现 Canetti 提出的理想加密函数[13], 该理想加密函数在与其他协议并发、复合时仍然是安全的。在 Asokan 的公平交换协议中需要用到带验证的加密来实现公平交换, 当发生冲突时, 需要第三方将密文进行解密来解决冲突, 这使得加密必须具有 IND-CCA2 安全性, 而 Asokan 等人也证明了 IND-CCA2 加密是充分的。

(4) 对已有标准的攻击

1998 年, Bleichenbacher[12] 对原先的 RSA 标准进行了有效的攻击, 这种攻击能实现是因为实际密码系统中可以回答解密请求, 使得攻击者可以得到解密; 2000 年(后来发表在 2002 年的 Journal of Cryptography), Shoup[34] 指出 OAEP 在一般情形是不安全的, 并提出了 $OAEP^{+}$; Fujisaki 等人[23] 在 2001 年指出, 虽然 OAEP 一般情形是不安全的, 但由于 RSA 的特殊代数结构, OAEP-RSA 是安全的。

(5) 新的公钥候选标准

2004 年 ISO 最新的几个候选标准[25] 的原型就是几个重要的抗选择密文攻击公钥加密密码方案, 其中包括 BR94(RSA-based), CS98 和 CS01(EI Gamal-based), FO99 和 OP01(EPOC-based), ABR01(EI Gamal-based)。

(6) IND-CCA2 加密的存在性构造

以上实际上是针对具有实用价值的方案来介绍的, 但在抗选择密文攻击的发展过程中, 有一些构造方法, 它们具有一般性, 不依赖于特殊的数论假设和理想的 Hash 函数, 只需要假设存在单向函数。但这种构造由于太具有一般性, 结果效率不

高,不具有实用性,可以看作是 IND-CCA2 加密的存在性构造。这些构造包括 Sahai 99[32], DDN 00[19] 和 Lindell 03[27]。

3　进一步研究的问题

抗选择密文攻击密码体制的研究是一个非常重要方向,正在产生很多新的思想和方法,还有非常多的工作值得去做。下面列出我们认为值得继续研究的几个问题,供对该领域有兴趣的研究人员参考:

(1) 对已有的方案进行进一部优化、论证、具体实现。除了尽可能地直接提高加/解密速度,减少密文长度外,对其安全性进一步论证,弱化该方案的假设条件,使其规约为所基于的假设时更加紧致,从而可以选择更小的参数。已有方案的具体实现也是不容忽视的问题,因为每个实用的方案都是基于一定的数论假设的,而且大多数还假设 Hash 函数是理想的,这样,首先必须选取合理的群以及合理的参数,使得该群上这种数论假设是成立的。另外,如何选取这种 Hash 函数也显得特别重要,至少要求利用已有的方法,不能找出明显的缺陷,选用后还要密切关注最新的攻击手段并作出相应调整。

(2) 设计标准模型中高效适用的 IND-CCA2 加密体制。目前大多数 IND-CCA2 加密都是在理想的 Random Oracle 模型中证明其安全性,但这种理想 Hash 函数实际是不存在的,当用实际的密码学 Hash 函数来实现时,该方案不一定是安全的,所以,在标准模型中的方案安全性更可靠。但现在只有很少的方案其安全性能在标准模型中得到证明,而且效率明显地低于 Random Oracle 模型中的方案,一个重要但富有挑战性的问题是寻求标准模型中的设计、证明的新方法、新思想,设计出能与 Random Oracle 模型中效率相当的方案。

(3) 构造适合于某些特殊应用的 CCA2 加密体制。如在防火墙中,需要设计可以公开检测的加密,而且这些验证过程要求速度很高,那么可以将已有的公开检测加密进行改进,甚至可以牺牲其他方面,如加密速度、密文长度来提高验证过程的效率;而有些环境中,需要特别短的密文,可以考虑满足这种条件的方案。

(4) 进一步探讨与其他密码协议的关系,寻找新的应用背景。除了可以用 IND-CCA2 加密设计前面介绍提到的协议外,怎样用它来设计群签名、电子拍卖等协议非常值得研究。它与零知识证明、陷门承诺之间的关系值得考虑,并反过来用它们设计 IND-CCA2 加密。

4　结束语

抗选择密文攻击公钥密码体制是一种安全性很高的密码体制,具有重要的研究意义。该概念自从被提出后,受到了密码学界的普遍关注,已经取得了大量的研究成果。本文介绍了该领域取得的研究成果,并指出了几个值得进一步研究的问题。

参考文献:

[1] Abdalla, M Bellare, P Rogaway. The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES[C]. Berlin: Springer-Verlag, Topics in Cryptology CT-RSA 2001, 2001. 143-158.

[2] N Asokan, V Shoup, M Waidner. Optimistic Fair Exchange of Digital Signatures[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 593-610.

[3] J Baek, R Steinfeld, Y Zheng. Formal Proofs for the Security of Signcryption[M]. Berlin: Springer-Verlag, Public Key Cryptography, 2002. 81-98.

[4] M Bellare, R Canetti, H Krawczyk. A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols[C]. New York: ACM, the 30th Annual ACM Symposium on Theory of Computing, 1998. 419-428.

[5] M Bellare, A Desai, D Pointcheval, *et al*. Relations Among Notions of Security for Public Key Encryption Schemes[C]. Berlin: Springer-Verlag, Advances in Cryptology CRYPTO'98, 1998. 26-45.

[6] M Bellare, D Pointcheval, P Rogaway. Authenticated Key Exchange Secure Against Dictionary Attacks[C]. Berlin: Springer-Verlag, Advances in Cryptology - Proceedings of EUROCRYPT 2000, 2000. 139-155.

[7] M Bellare, P Rogaway. Entity Authentication and Key Distribution [C]. Berlin: Springer-Verlag, Advances in Cryptology CRYPTO'93, 1994. 232-249.

[8] M Bellare, P Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols[C]. New York: ACM, the 1st ACM Conference on Computer and Communications Security, 1993. 62-73.

[9] M Bellare, P Rogaway. Optimal Asymmetric Encryption[C]. Berlin: Springer-Verlag, Advances in Cryptology-EUROCRYPT'94, 1994. 92-111.

[10] D Boneh, X Boyen. Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles[C]. Berlin: Springer-Verlag, Advances in Cryptology EUROCRYPT 2004, 2004. 223-238.

[11] D Boneh, M Franklin. Identity-based Encryption from the Weil Pairing[C]. Berlin: Springer-Verlag, Advances in Cryptology -CRYPTO'01, 2001. 213-229.

[12] D Bleichenbacher. Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1 [C]. Berlin: Springer-Verlag, Advances in Cryptology CRYPTO'98, 1998. 1-12.

[13] R Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols[C]. Washington: IEEE, the 42nd IEEE Symposium on Foundations of Computer Science, 2001. 136-145.

[14] R Canetti, S Goldwasser. An Efficient Threshold Public Key Cryptosystem Secure Against Adaptive Chosen Ciphertext Attack[C]. Berlin: Springer-Verlag, Advances in Cryptology EUROCRYPT'99, 1999. 90-106.

[15] R Canetti, S Halevi, J Katz. Chosen-Ciphertext Security from Identity-based Encryption[C]. Berlin: Springer-Verlag, Advances in Cryptology EUROCRYPT 2004, 2004. 207-222.

[16] R Canetti, H Krawczyk. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels[C]. Berlin: Springer-Verlag, Advances in Cryptology EUROCRYPT 2001, 2001. 453-474.

[17] R Cramer, V Shoup. A Practical Public-Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack[C]. Berlin: Springer-Verlag, Advances in Cryptology CRYPTO'98, 1998. 13-25.

[18] R Cramer, V Shoup. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption[C]. Berlin: Springer-Verlag, Advances in Cryptology EUROCRYPT 2002, 2002. 45-64.

[19] D Dolev, C Dwork, M Naor. Non-malleable Cryptography[J]. SIAM Journal of Computing, 2000, 30(2): 391-437.

(下转第 30 页)