公钥密码是否安全看证明

刘胜利

如何评价一个密码系统是否安全？以前的方法是：密码学家通过各种攻击手段来攻击密码系统，如果这个系统能够经受各种攻击的考验，那么这个密码系统就认为是安全的。但是，我们难以穷尽所有的攻击方法。目前一个密码系统找不到有效的攻击方法，不代表以后也找不到有效的新型攻击。那么我们如何从理论上保证一个密码系统的安全性呢？从上世纪 80 年代末开始，密码学家开始发展可证明安全理论，试图从理论上证明一个密码系统的安全性。在公钥密码的可证明安全理论中，我们首先假设一些困难问题。而密码发展的历史中的确留下了一些公认的困难问题，如：解离散对数 (DL) 问题、判定性 Diffie-Hellman(DDH) 问题、整数分解 (Factoring) 问题、判定性合数剩余 (DCR) 问题等。其次，我们对敌手的能力、对密码系统的安全要求等进行形式化，建立数学模型。定义出什么叫做“敌人攻破了系统”。最后，我们通过安全性归约来证明系统的安全性：如果有一个多项式时间的敌手能够有效地攻破系统，那么我们可以构造出一个多项式时间的算法来解决一个“特定的数学难题”。由于大家公认数学难题不可能在多项式时间内解决，故不可能存在这样的多项式时间的敌手。进而得到如下结论：只要“特定的问题是困难的”，任意多项式时间的敌手都不可能攻破系统，因此“系统是安全的”。

在可证明安全理论中，一个密码系统的安全性向困难问题进行归约的过程中，都会产生一些归约参数来衡量归约的有效性。如果一个概率多项式时间的敌手 A 能在 T_A 时间内以 ε_A 的概率攻破敌手，那么可以构造另外一个概率多项式时间的算法 B 能在 T_B 时间内以 ε_B 的概率解决该困难问题。最理想的安全归约是：$T_A \approx T_B$ 且 $\varepsilon_A \approx \varepsilon_B$。但是大多数的安全证明中都会有 $\varepsilon_A \leqslant L\varepsilon_B$，其中 L 是归约损失因子。在公钥加密中，L 一般都与敌手的解密查询次数以及挑战密文的个数有关。在数字签名中，L 则与敌手的签名查询次数有关。由于敌手的查询次数可以高达 2^{20}，那么为了达到同一安全强度，松散的安全归约会导致密码系统的安全参数增大，密码运算的计算量大幅度提高。如果 L 最多是安全参数的线性因子，则安全归约就是紧致的。本文介绍公钥加密领域的紧归约技术。

1.CPA 安全的紧致归约

一个公钥加密方案 (PKE) 比较容易实现紧致归约的 CPA 安全，现以 ElGamal 与 Paillier 加密方案 [1] 为例。

ElGamal 公钥加密方案对明文 m 加密所得的密文形式为：$C=(g^r, mg^{xr})$，其中公钥为 $y=g^x$。那么由 DDH 问题的困难性假设，

就可以直接得到如下结论：(g, g^x, g^r, g^{xr}) 与 (g, g^x, g^r, g^z) 计算不可区分。因此，$(g, g^x, g^r, m\ g^{xr})$ 与 $(g, g^x, g^r, m\ g^z)$ 不可区分。均匀分布的群元素 g^z 完美地掩盖了消息 m 的信息。所以 ElGamal 公钥加密方案的安全性可以直接归约为 DDH 问题的困难性。

Paillier 公钥加密方案对明文 m 加密所得的密文形式为：$C=(1+N)^m r^N$。这里的群为 $Z^*_{N^2}$。由 DCR 假设，可知当 r 在 $Z^*_{N^2}$ 上均匀分布且 x 在 Z_N 上均匀分布时，r^N 与 $(1+N)^x r^N$ 是计算不可区分的，进而有 $(1+N)^m r^N$ 与 $(1+N)^{x+m} r^N$ 计算不可区分且 $(1+N)^{m'} r^N$ 与 $(1+N)^{x+m'} r^N$ 计算不可区分。而 $(1+N)^{x+m} r^N$ 与 $(1+N)^{x+m'} r^N$ 均在 $Z_{N^2}^*$ 上均匀分布，所以 $(1+N)^m r^N$ 与 $(1+N)^{m'} r^N$ 是计算不可区分的。故而 Paillier 公钥加密方案的安全性可以直接归约为 DCR 问题的困难性。

以上考虑的一个挑战密文的 CPA 安全性。当考虑多个挑战密文时，我们对所依赖的困难性问题有更高的要求：问题必须具有 random-self-reducible 的特性。困难问题的实例之间可以多项式时间内进行归约，即一个困难问题可以有效地变为多个统计独立的困难问题。如 DDH,DCR 问题均为有 Self-Random-Reducible 性质的困难问题。所以 ElGamal 与 Paillier 加密方案可以实现多挑战密文的紧致归约 CPA 安全。

2.CCA 安全的紧致归约

在公钥加密领域，有效地实现了紧致归约 CCA2 安全的是 Cramer-Shoup 公钥加密方案 [CS98]，其单个挑战密文的 CCA 安全性可以紧致归约为 DDH 问题。如果有 Q 个挑战密文，其 CCA 安全性只能通过 Hybrid Argument 进行归约，由于需要 Q 次 Hybrid Argument，所以归约因子至少为 Q。也就是说 Cramer-Shoup 公钥加密方案的多个挑战密文难以实现 CCA2 安全的紧致归约。

关于紧致归约 CCA2 安全，近年来的研究工作如下：

2.1 CPA 安全的紧致归约的 IBE

2004 年，Canetti 等人提出了 CHK 转换 [CHK04]。通过 CHK 转换，CPA 安全（可能弱化为选择性 CPA 安全，即 sCPA 安全）的 IBE 可以转换为一个 CCA 安全的公钥加密方案。由于 CHK 转换不损失归约因子，所以只要能够实现具有紧致归约 CPA 安全的 IBE，CHK 转换后就可以得到一个具有紧致归约 CCA 安全的公钥加密方案。

2013 年 Chen 和 Wee 通过 Noar-Reingold 的 PRF 技术设计了 IBE 方案，并实现了 CPA 安全的紧致归约 [CW13]。因此也得到一个具有紧致归约 CCA 安全的公钥加密方案。之后 2014 年，Blake,Kiltz,Pan 重新用 affine MAC 的技术对 IBE 方案进行设计，得到一个效率更高的具有紧致归约的 IBE[BKP14]。

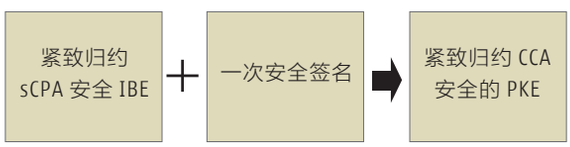

图 1：CHK 转换

2016 年，Gong 等人将单个挑战密文的 IBE 扩展为多个挑战密文的 IBE，进而实现了多挑战密文紧致归约 CCA 安全的公钥加密

方案 [6]。

2.2 Noar Yung 通用转换方案

1990 年，Naor 和 Yung 提出如何将 CPA 安全的公钥加密转变为 CCA1 安全的公钥加密 [7]，所采取的技术为非交互零知识证明（NIZK）。其思想是使用两把“密钥”对同一个明文进行加密，也就是说，用两个 IND-CPA 安全的公钥加密算法对同一个明文进行加密得两个密文，同时使用非交互零知识证明（NIZK）来说明两个密文是对同一个明文的加密。1991 年 Rackoff 和 Simon 提出了 CCA2 攻击，并指出 Noar-Yung 的方法可以扩展实现 IND-CCA2 安全，只需要 NIZK 具有 Simulation-Soundness 性质即可。但是，由于非交互零知识证明没有高效的实现方法，所以 Noar-Yung 的方法具有理论价值但缺乏实际意义。2008 年，Groth-Sahai 基于配对群设计出了高效的 NIZK[8]，使 Noar-Yung 转换最终成为一个有效可用的方法。

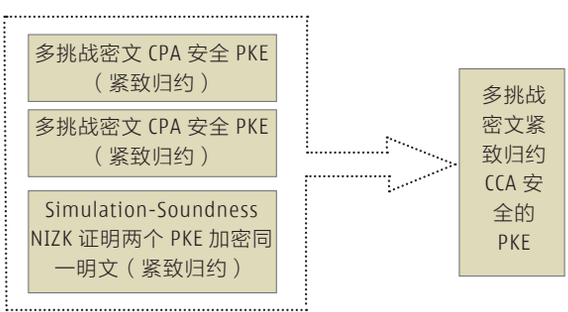

图 2：Noar-Yung 转换

根据 Noar-Yung 转换，只要构件中的 PKE 具有多挑战密文紧致归约 CPA 安全，NIZK 的 Simulation-Soundness 和零知识性质均具有紧致归约特性，那么所得到的 PKE 就具有多挑战密文紧致归约 CCA 安全性。具有多挑战密文紧致归约 CPA 安全 PKE 有多个选择，如 ElGamal 和 Paillier 公钥加密方案。但是 Simulation-Soundness 和 Zero-Knowledge 的紧致归约性很难达到。

2016 年，Hofheiz 设计了第一个具有紧致归约特性的 NIZK[9]，所使用的组件如下：(1) 具有紧归约安全特性的签名方案。方案的安全性要求是：具有非自适应的选择明文攻击下的不可伪造性 (Non-adaptive EUF-CMA 安全性)；(2) 具有紧归约安全特性的一次签名方案。方案的安全性要求是：具有针对多验证密钥的一次强不可伪造安全性 (strongly one-time EUF-CMA)；(3) 完美 WI 及可提取 Groth-Sahai NIZK。Groth-Sahai 证明系统需要证明要么命题成立，要么知道对一次签名验证秘钥的签名。

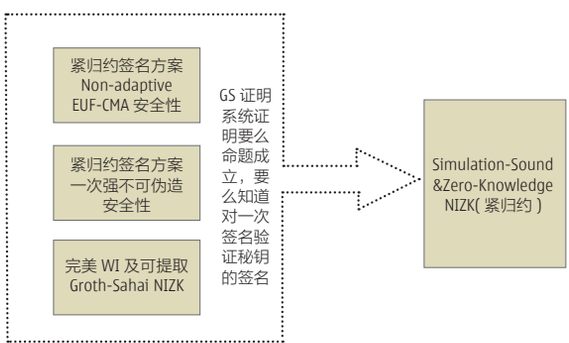

图 3：紧归约 NIZK 的构造 [Hofheinz16]

2.3 基于 MDDH 及 DCR 假设的公钥加密方案

Groth-Sahai 所提出的 NIZK 是建立在配对群（G，G_T，e）上的，而且依赖于配对群中的双线性配对运算 e 的线性性质以及 2-LIN 困难假设。双线性配对运算 e 比一般的群运算要复杂得多，且 DDH 问题在群 G 上并不成立。如何不使用双线性配对实现多挑战密文的

紧归约是一个公开问题。

Gay 等人 [10] 在 2016 年解决了这个公开问题。在 EuroCrypt2016 上，他们提出使用 MDDH 问题的 Random Self-Reducibility 特性，设计了一个公钥加密方案，使其 CCA2 安全性能够（几乎）紧致归约为 MDDH 安全假设。此论文为 EuroCrypt2016 的最佳论文。但是方案的安全性仅限于 MDDH 假设，不能扩展为其它的假设。同时，方案的公钥和密文长度与安全参数成正比。

在 2017 年 的 EuroCrypt2017 中，Hofheinz 提出了 Adaptive Partitioning 技术 [11]，提出了一个称为 Benign Proof System 的系统，并使用此技术和系统成功地设计了一个公钥加密的通用构造方法。所构造的公钥加密的安全性不但可以实现几乎紧致归约，而且其公钥和密文的长度仅为常数级。通过实例化，不但可以基于 MDDH 假设得到具有（几乎）紧致归约的安全归约，还实现了公钥和密文长度的紧致性。此外，论文的另一实例还可以得到第一个基于 DCR 假设的紧归约公钥加密。

附：参考文献

[1] Junqing Gong, Xiaolei Dong, Jie Chen, Zhenfu Cao: Efficient IBE with Tight Reduction to Standard Assumption in the Multi-challenge Setting. ASIACRYPT (2) 2016: 624-654

[2] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Advances in Cryptology—CRYPTO 1998, volume 1462 of LNCS, 1998.

[3] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. In Advances in Cryptology—EUROCRYPT 2004. Springer-Verlag, 2004.

[4] Jie Chen and Hoeteck Wee. Fully, (almost) tightly secure IBE and dual system groups. In Advances in Cryptology – CRYPTO 2013 – Part II, pages 435 – 460, 2013

[5] Romain Gay, Dennis Hofheinz, Eike Kiltz, Hoeteck Wee: Tightly CCA-Secure Encryption Without Pairings. EUROCRYPT (1) 2016: 1-27

[6] Dennis Hofheinz: Adaptive partitioning. IACR Cryptology ePrint Archive 2016: 373 (2016)

[7] M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In 22nd ACM STOC, pages 427{437. ACM Press, May 1990.

[8] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. P. Smart, editor, EUROCRYPT 2008, volume 4965 of LNCS, pages 415{432. Springer, Apr. 2008.

[9] Dennis Hofheinz: Algebraic Partitioning: Fully Compact and (almost) Tightly Secure Cryptography. TCC (A1) 2016: 251-281

[10] Pascal Paillier: Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. EUROCRYPT 1999: 223-238

[11] Olivier Blazy, Eike Kiltz, and Jiaxin Pan. (hierarchical) identity-based encryption from affine message authentication. In Advances in Cryptology – CRYPTO 2014, pages 408 – 425. Springer, 2014.