

# 公钥加密系统的可证明安全——新挑战新方法\*

刘胜利

上海交通大学 计算机科学与工程系, 上海 200240

通讯作者: 刘胜利, E-mail: slliu@sjtu.edu.cn

**摘要:** 密码界对公钥加密所广泛接受的安全标准是 IND-CCA2 安全. 但是近年来各种新的攻击手段层出不穷, IND-CCA2 安全已不能应付这些攻击. 本文将对近年来出现的“选择打开攻击”, “密钥泄漏攻击”、“密钥相关信息安全”、“密钥相关攻击”、及“随机数相关攻击”进行阐述, 并介绍如何对这些攻击进行形式化, 如何定义能够抵御这些攻击的更高的安全标准, 包括: 针对“选择打开攻击”的“基于仿真的选择打开 CCA2 安全”(SIM-SO-CCA2)及“基于不可区分的选择打开 CCA2 安全”(IND-SO-CCA2); 针对“密钥泄漏攻击”的“容忍密钥泄漏 CCA2 安全”(LR-CCA2); 依赖密钥的消息的 CCA2 安全(KDM-CCA2); 针对“密钥相关攻击”的“密钥相关 CCA2 安全”(KR-CCA2); 针对“随机数相关攻击”的“随机数相关 CCA2 安全”(RR-CCA2). 此外, 我们还简要介绍了目前达到新标准所使用的技术和方法, 包括交叉认证码技术、Hash Proof System 技术, One-Time Lossy Filter 技术等, 同时指出了目前公钥加密可证明安全所面临的挑战.

**关键词:** 公钥加密; 可证明安全; CCA2 安全

中图法分类号: TP309.7 文献标识码: A DOI: 10.13868/j.cnki.jcr.000050

中文引用格式: 刘胜利. 公钥加密系统的可证明安全——新挑战新方法[J]. 密码学报, 2014, 1(6): 537-550.

英文引用格式: Liu S L. Provable security for public key encryption——challenges and approaches[J]. Journal of Cryptologic Research, 2014, 1(6): 537-550.

## Provable Security for Public Key Encryption——Challenges and Approaches

LIU Sheng-Li

Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Corresponding author: LIU Sheng-Li, E-mail: slliu@sjtu.edu.cn

**Abstract:** The widely acceptable standard security notion for public key encryption is IND-CCA2 security. Many new attacking techniques are proposed in recent years, which impose new security requirements beyond IND-CCA2. In this survey, we describe some recent appeared attacks, i.e., the Selective-Opening Attacks, Key-Leakage Attacks, Key-Dependent Security, Key-Related Attacks and Randomness-Related Attacks. We show how to formalize those attacks to get new security models and set up new security notions resisting those attacks. The formalization of “Selective-Opening Attacks” gives the notion of “Simulation-based Selective Opening

---

\* 基金项目: 国家自然科学基金(61170229, 61373153, 61133014); 高等学校博士学科点专项科研基金(20110073110016); 上海市教委科研创新项目(12ZZ021)

收稿日期: 2014-09-18 定稿日期: 2014-11-26



从上图可以看出, 语义安全和不可区分安全是等价的. 而在敌手的 CCA2 攻击情况下, 三种不同的形式化定义又是等价的. 因此, 在证明 CCA2 安全时, 人们总会选择简洁易证的 IND-CCA2 安全. 在本文中, 为简单起见, 我们将 CCA2 写为 CCA.

## 2 公钥加密的 IND-CCA 安全以及新攻击和新要求

### 2.1 公钥加密与 IND-CCA 安全

一个公钥加密方案包括三个算法: 密钥生成算法  $\text{KeyGen}(1^k) \rightarrow (\text{pk}, \text{sk})$ , 输入安全参数  $k$ , 输出一对公私钥  $(\text{pk}, \text{sk})$ ; 加密算法  $\text{Enc}(\text{pk}, M; R) \rightarrow C$ , 输入公钥  $\text{pk}$  和明文  $M$  以及随机数  $R$ , 输出相应的密文  $C$ ; 解密算法  $\text{Dec}(\text{sk}, C) \rightarrow M/\perp$ , 输入私钥  $\text{sk}$  和密文  $C$ , 输出所恢复的明文  $M$  或者一个解密失败的符号  $\perp$ .

**表 1** 公钥加密方案算法  
Table 1 Algorithms of a Public Key Encryption Scheme

密钥生成算法	加密算法	解密算法
$\text{KeyGen}(1^k) \rightarrow (\text{pk}, \text{sk})$	$\text{Enc}(\text{pk}, M; R) \rightarrow C$	$\text{Dec}(\text{sk}, C) \rightarrow M/\perp$

由于在 CCA2 攻击下, 语义安全、不可区分安全和不可延展安全是等价的. 所以我们介绍最简明的 IND-CCA2(简记为 IND-CCA)安全. IND-CCA 安全模型由下述实验(或者称为 Game)来刻画. 实验中有一个挑战者和一个敌手.

**初始阶段:** 挑战者调用密钥生成算法  $\text{KeyGen}(1^k) \rightarrow (\text{pk}, \text{sk})$  得到公私钥对, 并将公钥  $\text{pk}$  发给敌手.

**解密阶段 1:** 敌手查询密文  $C$ , 挑战者调用解密算法  $\text{Dec}(\text{sk}, C) \rightarrow M/\perp$  回复.

**挑战阶段:** 敌手向挑战者提交两个长度相同的明文  $M_0, M_1$ , 挑战者随机选择一个比特  $b$ , 调用加密算法加密  $M_b$ , 得到挑战密文  $C^* = \text{Enc}(\text{pk}, M_b; R)$ . 挑战者将挑战密文  $C^*$  发给敌手.

**解密阶段 2:** 敌手查询密文  $C$ , 但要限定  $C \neq C^*$ . 挑战者调用解密算法  $\text{Dec}(\text{sk}, C) \rightarrow M/\perp$  回复.

**猜测阶段:** 敌手猜测  $b$  的值  $b'$ .  
如果敌手猜对  $b' = b$ , 则敌人赢得了这个实验.

图 2 PKE 的 IND-CCA 实验及安全模型  
Figure 2 The IND-CCA experiment of PKE and the security model

**定义 1** 给定一个公钥加密方案  $\text{PKE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ . 如果任意的概率多项式时间(ppt)的敌手赢得上述实验的概率都可以忽略的量接近  $1/2$ , 即

$$\left| \text{Prob}[b = b'] - \frac{1}{2} \right| = \text{neg}(k)$$

那么这个 PKE 方案就是 IND-CCA 的.

如果上述实验中没有解密阶段 1 和解密阶段 2, 那么 IND-CCA 安全就退化为 IND-CPA 安全; 如果上

述实验中只有解密阶段 1, 则 IND-CCA 安全退化为 IND-CCA1.

## 2.2 IND-CCA 安全的研究现状

1984 年, Goldwasser 和 Micali<sup>[8]</sup>提出了概率加密的公钥加密算法, 并给出了语义安全的形式化定义, 从此开启了公钥密码的可证明安全的新篇章. 两位学者也因此获得了 2012 年的图灵奖.

1990 年, Naor 和 Yung<sup>[1]</sup>提出了 CCA1 攻击以及如何实现 IND-CCA1 安全. 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<sup>[9]</sup>提出了 CCA2 攻击, 并指出 Naor-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 Naor-Yung 的方法具有理论价值但缺乏实际意义.

1998 年, Cramer 和 Shoup 提出第一个实用的 IND-CCA 安全的公钥加密方案, 它属于类 ElGamal 体制, 其安全性可以归约为 Decisional Diffie-Hellman(DDH)问题. 之后, Cramer 和 Shoup<sup>[2]</sup>又将其设计思想扩展为 Hash Proof System(HPS). 其构造 PKE 的方法是使用两种类型的 HPS, 一个是 smooth HPS, 另一个是 2-universal HPS. Smooth HPS 用于产生一个一次性密钥来掩盖明文, 而 2-universal HPS 则用于检查密文的合法性. 基于这种方法, 可以构造出多种实用的 IND-CCA2 安全 PKE: 基于 Quadratic Residue 假设的, 基于 Decisional Composite Residue 假设的等.

2006 年, Boneh, Cannetti, Halevi, Katz<sup>[3]</sup>提出如何使用基于身份的加密(IBE)构造公钥加密(PKE)的 BCHK 方法. 假设  $\text{IBE} = (\text{IBE.Gen}, \text{IBE.Der}, \text{IBE.Enc}, \text{IBE.Dec})$  是具有弱的 selective-ID 的 CPA(IND-sID-CPA)安全的基于身份的加密方案. 其中  $\text{IBE.Gen}(1^k) \rightarrow (\text{mpk}, \text{msk})$  产生公开参数 mpk 和主密钥 msk, 其它算法都隐含了将 mpk 作为公共输入;  $\text{IBE.Der}(\text{msk}, \text{ID}) \rightarrow \text{SK}_{\text{ID}}$  对任意一个身份 ID, 利用主密钥产生私钥  $\text{SK}_{\text{ID}}$ ; IBE 的加密算法  $\text{IBE.Enc}(\text{ID}, M) \rightarrow \phi$  输入身份信息和明文, 输出相应的密文; IBE 的解密算法  $\text{IBE.Dec}(\text{SK}_{\text{ID}}, \phi) \rightarrow M/\perp$  输入私钥和密文输出所恢复的明文  $M$  或者  $\perp$ . 使用强的一次性签名方案  $\text{OTS} = (\text{OTS.Gen}, \text{OTS.Sign}, \text{OTS.Ver})$  中的密钥产生算法 OTS.Gen 生成签名私钥和验证密钥对  $(\text{sk}_{\text{sig}}, \text{vk})$ . 同时使得 vk 作为 ID 对明文进行加密得到  $\phi = \text{IBE.Enc}(\text{vk}, M)$ , 再对  $\phi$  进行签名得到  $\sigma = \text{OTS.Sign}(\text{sk}_{\text{sig}}, \phi)$ . 最终加密得到的密文为  $(\text{vk}, \phi, \sigma)$ . 解密时, 先用 vk 验证签名的正确性, 再使用 msk 得到密钥  $\text{sk}_{\text{vk}}$ , 最后使用  $\text{IBE.Dec}(\text{SK}_{\text{vk}}, \phi)$  恢复明文. 所构造的公钥加密方案的安全性归约为 IBE 的 IND-sID-CPA 安全和一次签名的强不可伪造特性.

## 2.3 IND-CCA 安全的局限

但是, IND-CCA 安全有如下的限定:

- (1) 安全模型仅限于两方: 发送方和接收方. 不适用于多用户的网络环境, 因此不会考虑敌人对多用户进行的主动渗透(corruption)攻击;
- (2) 安全模型默认敌人所得到的私钥相关信息仅限于公钥 pk 和解密预言机, 除了公钥信息以及解密服务(解密预言机提供)之外, 敌人没有关于私钥 sk 的其它任何信息;
- (3) 挑战密文  $C^*$  所加密的信息不能是私钥直接参与计算所得到的函数值  $f(\text{sk})$ .
- (4) 敌人不会影响解密算法中私钥 sk 的使用方法.
- (5) 公钥加密中采用的随机数  $R$  是真正随机的.

网络化环境使得信息系统日趋复杂,不同的环境对安全性能的要求也不尽相同,采取的安全策略也具有多样性.比如,在多方安全计算环境中,多个发方会使用公钥加密向同一个收方发送密文信息.而这些密文所对应的明文很可能是相互关联的.敌人可能会进行渗透攻击,得到某些发送方所有的信息,包括密文所对应的明文以及加密所使用的随机数.此外,边信道攻击方法的日新月异,“内存攻击”的出现颠覆了“只有计算才会泄漏信息”这一论断.即使不做任何计算,敌人也可能会通过 Cold-Boots Attack 来得到存储在内存的密钥的一部分信息.这些攻击方法都导致了新的安全要求.

## 2.4 新攻击新要求

复杂环境对保障信息安全的算法提出了更高的安全要求,对信息安全保障理论与技术提出了更高的挑战.具体表现在如下几个方面.

- (1) 网络化环境下的协同计算中可能会有多个实体,他们之间相互通信的信息极有可能是相互关联的.而敌手则可能会窃听到网络上传输的任何信息.同时,敌手也可能会渗透(corrupt)甚至完全掌控某个或多个通信实体.那么如何保障那些没有受到敌人渗透的通信实体所加密的数据的保密性?这样的一个复杂环境下的多方密码系统的安全性,已经不能够由简单的只涉及两方通信的 IND-CCA 安全性来保证了.如何建立新的安全模型,定义新的安全指标,设计加密算法实现并达到这些安全指标?
- (2) 实施密码算法的电子设备在运行的过程中会有功率消耗或电磁辐射.而密码算法中的密钥参与算法运行时,密钥的 0 或 1 比特信息会引起不同的功率消耗或者不同强度的电磁辐射.边信道攻击(side channel attack)正是通过算法运行过程中的时间消耗、功率消耗或电磁辐射之类的信息泄露对密钥进行恢复,进而攻破密码系统.近几年来,边信道已经由简单功耗分析攻击(simple power analysis attacks, SPA)和差分功耗分析攻击(differential power analysis attacks, DPA)发展为零值点攻击(zero-value attack),内存攻击(memory attack)等.这些攻击都是以恢复(部分密钥)为目的.而传统的密码算法的可证明安全总是假设密钥服从均匀分布,敌人(计算意义下)不知道密钥的任何信息.边信道攻击无疑给敌手带来了绝对的密钥泄漏.为了抵御这种攻击,通常会对密钥进行盲化处理,但是本质上并没有改变算法本身,以牺牲效率来换取安全性.这种解决方法具有很强的针对性,只针对特定的算法和特定的攻击,不具有一般性,对新的算法和新的边信道攻击可能无能为力.如何设计一个密码算法,使其从理论上就能抵抗边信道攻击?
- (3) 在网络化的分布式存储中,为了保证数据的安全性,数据一般都需要加密后存储.而在实际应用中,加密存储中的数据中往往还包括了加密数据所使用的密钥.如 Windows 操作系统所提供的 BitLocker 磁盘加密系统,数据和磁盘密钥一起加密后存储在磁盘中.这样做的好处是方便密钥存储和管理.而在信证系统(credential system)中,为了防止用户将自己的某个私钥交给他人代理,系统将每个用户的多个私钥利用循环加密(circular encryption)的方法进行加密存储.泄漏一个私钥意味着泄漏了用户的所有私钥.无论是既成事实上的加密应用,还是为了实现某个功能的主观设计,都产生了“私钥加密私钥”这样一个不争的事实.而 IND-CPA/CCA 安全模型却不能涵盖这种情况,也就是说即使算法是 IND-CPA/CCA 安全的,也不能保证利用私钥加密私钥所产生的密文对敌人而言是安全的.在这种情况下,同样也需要一个更强的安全模型,设计具有更高安全性的密码算法.
- (4) “密钥相关攻击”(related-key attack, RKA)最早是一种常见的分组密码攻击方法.它同样可能实施在公钥加密系统中.敌人可以篡改解密设备中的私钥,知道篡改的方式但不知道篡改前后的密钥值,然后观察篡改后的私钥在解密算法的输出表现提取出有用信息,进而破译整个密码算法.
- (5) “随机数相关攻击”(randomness-related attack, RRA)则是敌人通过对公钥加密所用的随机数进行篡

改,知道篡改的方式但不知道篡改前后的随机数的值,对篡改后的加密算法的输出进行分析,以期获得额外的信息.

灵活多样的网络化环境对安全性提出了不同的要求. IND-CCA 安全性对于一些环境(如多方通信环境,密钥加密存储系统,边信道信息泄漏环境等)的安全要求是远远不够的. 因此,必须重新建立复杂环境下的安全模型,定义新环境下的安全定义,并在新模型下对公钥密码体制进行设计,从理论上证明其安全性.

### 3 新模型新方法

我们对上节所介绍的几种新攻击的进行形式化描述,给出相应的安全定义,并指出现有的解决方法.

#### 3.1 选择打开攻击和 SO-CCA 安全

与传统的 IND-CCA 安全模型相比,这里考虑的是多用户环境,同时敌人有更强的能力,表现为渗透(corruption)攻击,即:敌手可以自由选择打开哪些密文,并得到相关的明文和随机数. 见图 3 和图 4.

敌人得到的信息包括:公钥、多个密文组成的挑战密文向量(相应明文向量的概率分布可以由敌手指定)、敌人选择密文向量的一部分并得到相应的密文分量所对应的明文和随机数、敌人可以自适应地访问解密预言机(但是不能查询挑战密文向量中的密文).

SO-CCA 安全与传统的 CCA 安全相比,敌人多了选择打开的能力,目前 CCA 安全的公钥加密不一定是 SO-CCA 安全的. 传统的 CCA 安全有两种主流的形式化定义:基于不可区分意义下的 IND-CCA 安全和基于仿真意义下的 SIM-CCA 语义安全. 而且两种安全是等价的,即 IND-CCA=SIM-CCA. 同样,SO-CCA 也有两种形式化的定义:基于不可区分意义下的 IND-SO-CCA 安全(图 3)和基于仿真意义下的 SIM-SO-CCA 语义安全(图 4). IND-SO-CCA 安全要求是:任意 ppt 的敌人无法区分挑战密文向量所对应的真正明文向量和一个与所打开的明文一致的重新采样的假明文向量. 这里要求明文的概率分布一定是能够条件概率重采样的;SIM-SO-CCA 语义安全则要求: ppt 的敌人可以计算的都可以通过一个只知道打开的明文分量的 ppt 的仿真器所仿真. 由于 SIM-SO-CCA 不需要明文概率分布的条件概率重采样,故更难实现.

**初始阶段:** 挑战者调用密钥生成算法  $\text{KeyGen}(1^k) \rightarrow (\text{pk}, \text{sk})$  得到公私钥对. 将公钥  $\text{pk}$  发给敌手.

**解密阶段 1:** 敌手查询密文  $C$ , 挑战者调用解密算法  $\text{Dec}(\text{sk}, C) \rightarrow M/\perp$  回复.

**挑战阶段:** 敌手向挑战者提交一个可以条件重采样的概率分布  $M$ , 挑战者根据这个概率分布选择出  $n$  个明文构成明文向量  $(M_1, \dots, M_n)$ , 并将其加密得到相应的密文向量  $(C_1, C_2, \dots, C_n)$ , 其中  $C_i = \text{Enc}(\text{pk}, M_i; R_i)$ . 挑战者将挑战密文向量  $(C_1, C_2, \dots, C_n)$  发给敌手.

**打开阶段:** 敌手选择一个集合  $I \subseteq \{1, 2, \dots, n\}$  发送给挑战者. 挑战者打开相应的密文分量得到  $(M_i, R_i)_{i \in I}$ . 挑战者随机选择一个比特  $b$ . 如果  $b=1$ , 则将原明文向量  $(M_1, \dots, M_n)$  和打开的随机数  $(R_i)_{i \in I}$  发送给敌手. 如果  $b=0$ , 则在固定  $(M_i)_{i \in I}$  的值的条件下根据  $M$  概率分布重新采样得到新明文向量  $(M'_1, \dots, M'_n)$ , 并将新的明文向量发给敌手. 对于所有的  $i \in I$  显然有  $M'_i = M_i$ .

**解密阶段 2:** 敌手查询密文  $C$ , 但要限定  $C \notin \{C_1, C_2, \dots, C_n\}$ . 挑战者调用解密算法  $\text{Dec}(\text{sk}, C) \rightarrow M/\perp$  回复.

**猜测阶段:** 敌手猜测  $b$  的值  $b'$ .

如果敌手猜对  $b' = b$ , 则敌人赢得了这个实验.

图 3 PKE 的 IND-SO-CCA 实验及相关安全模型

Figure 3 The IND-SO-CCA experiment of PKE and the security model

**定义 2** 给定一个公钥加密方案  $\text{PKE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ . 如果任意的概率多项式时间(ppt)的敌手赢得图 3 中实验的概率都以可以忽略的量接近  $1/2$ , 即

$$\left| \text{Prob}[b = b'] - \frac{1}{2} \right| = \text{neg}(k)$$

那么这个 PKE 方案就是 IND-SO-CCA 的.

PKE 的 SIM-SO-CCA 安全要求是: 真实实验中 ppt 敌手的输出  $\text{Out}_A$  与理想实验中和 ppt 仿真器的输出  $\text{Out}_S$  计算不可区分. 也就是说找不到一个 ppt 的算法以不可忽略的概率区分出这两个输出的概率分布. SIM-SO-CCA 安全要表达的内容是: 一个敌手从它所看到密文向量、选择打开的明文和随机数、以及解密查询所得到信息中可以 ppt 计算出来的任何内容, 都可以通过一个只看到选择打开的明文的 ppt 仿真器计算出来. 因此, 密文向量, 选择打开的随机数以及解密查询不会给敌手带来任何的收益. 见图 4.

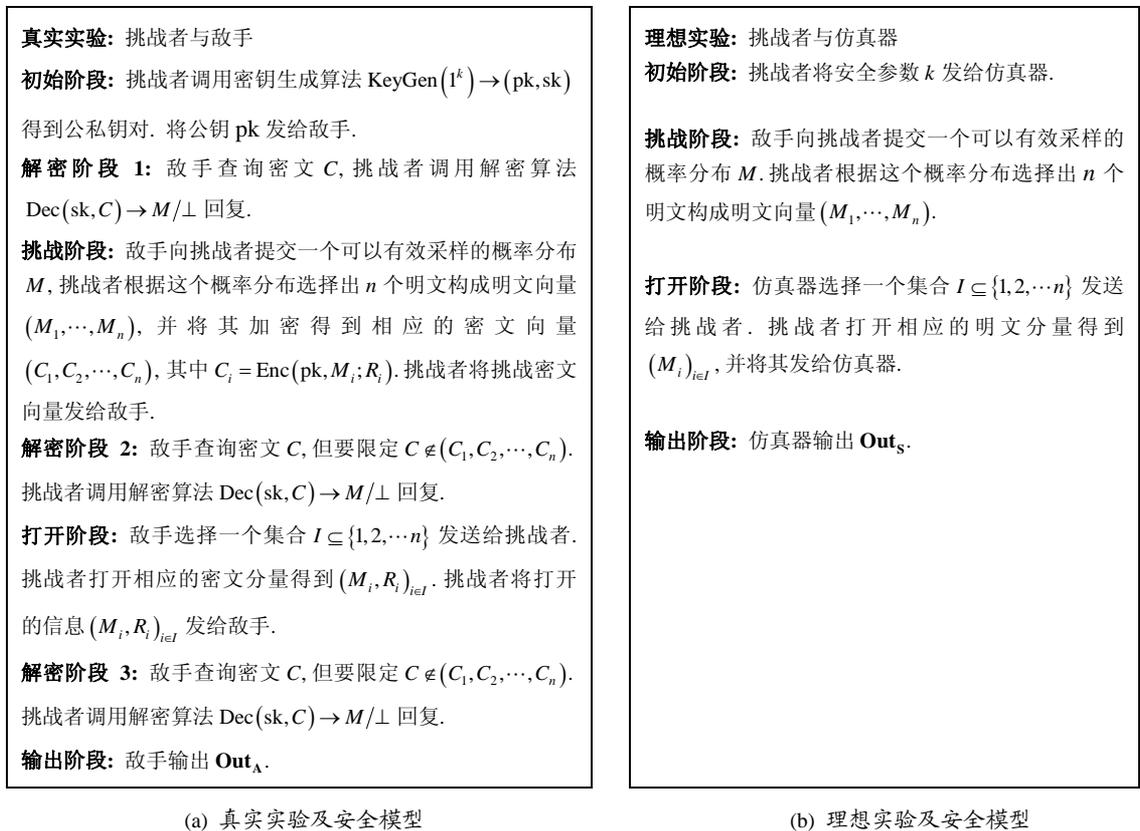


图 4 PKE 的 SIM-SO-CCA 实验及安全模型  
Figure 4 The SIM-SO-CCA experiments of PKE and the security model

**定义 3** 给定一个公钥加密方案  $\text{PKE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ . 如果任意的概率多项式时间(ppt)的区分器  $D$  都不能区分图 4 中两个实验的输出, 即

$$\left| \text{Prob}[D(\text{Out}_A) = 1] - \text{Prob}[D(\text{Out}_S) = 1] \right| = \text{neg}(k)$$

则 PKE 就是 SIM-SO-CCA 安全的.

在 2014 年, Hofheniz 和 Rupp 证明了 IND-SO-CCA 安全性严格高于 IND-CCA 安全<sup>[10]</sup>. 实现 IND-SO-CCA 安全的方法: 可以借用 Waters 用 Lossy Trapdoor Functions(LTDF)<sup>[6,11]</sup>+ABO-TDF+One Time Signature 来构造 CCA 安全 PKE 思想. 由于考虑的挑战密文向量有多个分量, 故需要可以 All-but-N<sup>[12]</sup>, All-but-many lossy trapdoor function<sup>[13]</sup>等技术, 其目的是在安全证明中将挑战密文变为 lossy encryption, 而敌人向解密 oracle 查询的密文不是 lossy encryption, 进而识别出不合法的密文以拒绝解密. 需要指出的是, 在选择打开环境下, 我们不能使用一次签名来验证密文的合法性, 原因在于, 敌人可以通过选择打开攻击得到挑战密文中签名所用的随机数(即签名密钥), 进而伪造合法密文, 从解密预言机中得到有关挑战明文的所有信息. 解决这个问题一个很好的方法是使用变色龙 Hash 函数与 All-but-N(All-but-many)TDF 的结合使用. Bellare 等在文献[14]中提出了如何实现 SIM-SO-CPA 安全的基于身份的公钥加密.

实现 SIM-SO-CCA 安全的挑战性则更高. 在公钥加密(PKE)方面, Fehr<sup>[15]</sup>等人在 EuroCrypt 2010 提出使用 2-universal Hash Proof System (HPS)和交叉认证码(Cross Authentication Codes)相结合实现 SIM-SO-CCA 安全. 在 PKC 2013, Huang 等<sup>[16]</sup>指出单纯的交叉认证码不足以证明所构造的 PKE 的 SIM-SO-CCA 安全性, 而实现一比特的 SIM-SO-CCA 安全的 PKE 则无需交叉认证码. 在 INCoS2013 会议上, Huang 等<sup>[17]</sup>提出了一个加强版的交叉认证码, 成功地修复了 Fehr 等人在 EuroCrypt 2010 论文中的 SIM-SO-CCA 安全证明. 在基于身份的加密(IBE)方面, 现在可行的方法是使用特殊的一比特的 IBE 加密和交叉认证码来实现<sup>[18]</sup>. 一比特的公钥加密的特点是: 加密比特“1”是一个合法的密文, 而加密比特“0”是随机密文(随机选择出的几乎都不是合法密文). 此外, 加密这一比特的密文同时还封装一个密钥. 封闭密钥则是交叉认证码的输入. 多个比特的加密对应的密文通过交叉认证码粘合在一起, 生成共同的认证符. 这样就有效的防止的 Quoting Attack. 这种实现方法的缺点是效率比较低, 但却是一种可以达到 SIM-SO-CCA 安全的通用构造.

### 3.2 密钥泄漏攻击和 IND-LR-CCA 安全

与传统的 IND-CCA 安全模型相比, 敌手有更强的能力, 因为敌手可以额外得到密钥泄漏的一些信息.

敌手得到的信息包括: 公钥、挑战密文、解密预言机、以及一个密钥泄漏预言机. 其中, 挑战密文是从敌人提供的长度相同的两个明文中随机选出并加密得到的.

密钥泄漏的安全模型又可分为两种: 有界泄漏模型(bounded model)和辅助输入模型(auxiliary input model). 在有界泄漏模型中, 敌人可以自适应地询问密钥泄漏预言机某个函数  $f_i$ , 预言机则回复  $f_i(\text{sk})$ . 但是, 要求所泄漏的所有  $f_i(\text{sk})$  关于私钥 sk 的信息不超过 sk 的长度. 在辅助输入模型中, 对  $f_i(\text{sk})$  的仅要求函数值求逆的是计算困难的. 因此, 这种模型更为通用. IND-LR-CCA 安全要求敌人不能区分挑战密文是他所选择的两个明文中哪个明文的加密.

**初始阶段:** 挑战者调用密钥生成算法  $\text{KeyGen}(1^k) \rightarrow (\text{pk}, \text{sk})$  得到公私钥对. 将公钥 pk 发给敌手.

**解密及密钥泄漏阶段 1:** 若敌手查询密文  $C$ , 挑战者调用解密算法  $\text{Dec}(\text{sk}, C) \rightarrow M/\perp$  回复. 若敌手查询函数  $f_i$ , 则挑战者回复  $f_i(\text{sk})$ . 但如果历次泄漏的  $f_i(\text{sk})$  累积信息达到上界  $\lambda$ , 则回复  $\perp$ .

**挑战阶段:** 敌手向挑战者提交两个长度相同的明文  $M_0, M_1$ , 挑战者随机选择一个比特  $b$ , 调用加密算法加密  $M_b$ , 得到挑战密文  $C^* = \text{Enc}(\text{pk}, M_b; R)$ . 挑战者将挑战密文  $C^*$  发给敌手.

**解密阶段 2:** 敌手查询密文  $C$ , 但要限定  $C \neq C^*$ . 挑战者调用解密算法  $\text{Dec}(\text{sk}, C) \rightarrow M/\perp$  回复.

**猜测阶段:** 敌手猜测  $b$  的值  $b'$ .

如果敌手猜对  $b' = b$ , 则敌人赢得了这个实验.

图 5 PKE 的 IND-LR-CCA 实验及安全模型

Figure 5 The IND-LR-CCA experiment of PKE and the security model

**定义 4** 给定一个公钥加密方案  $\text{PKE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ . 如果任意的概率多项式时间(ppt)的敌手赢得图 5 中实验的概率都以可以忽略的量接近  $1/2$ , 即

$$\left| \text{Prob}[b = b'] - \frac{1}{2} \right| = \text{neg}(k)$$

那么这个 PKE 方案就是  $\lambda$ -IND-LR-CCA 安全的.

实现 IND-LR-CCA 安全的有效技术是提取器. 提取器可以将一个不是均匀分布但熵很大的字符串变为一个接近均匀分布的短字符串. 例如使用提取器可以将 Cramer-Shoup 方案转变为容忍密钥泄漏的版本<sup>[19-21]</sup>; 结合 Hash Proof System 和 Naor-Yung 两把密钥的方法即可得到容忍密钥泄漏的 LR-CCA 安全的 PKE<sup>[21]</sup>. 但是, 目前的方法中, 要么私钥所容忍泄漏比例较小, 要么所实现效率太低. 最新的方法<sup>[22,23]</sup>是将 Hash Proof System(HPS)与 One-Time Lossy Filter 相结合, 同时达到了高效和密钥泄漏比例接近 1 的两个要求. 其思想是: HPS 封装一个密钥, 该密钥既用于掩盖明文, 又用于有效密文的验证. 而 One-Time Lossy Filter 在挑战密文中表现为 Lossy, 即泄漏关于封装密钥很少的信息, 而敌人生成的密文中 One-Time Lossy Filter 则表现为单射函数, 进而使敌人提交的不合法密文被解密预言机有效地拒绝. 以上方案均只适用于有界泄漏模型.

辅助输入(Auxiliary-Input)密钥泄漏模型是对有界泄漏模型的推广. 回忆有界指的是所有的泄漏信息量不得超过私钥的长度. 但是在辅助输入模型下, 对于敌人查询的私钥泄漏函数  $f$  只有如下要求: 已知数值  $f(\text{sk})$ , 在计算意义上求  $\text{sk}$  具有困难性. 这实际是要求函数  $f$  的单向性. 例如: 如果  $f$  是一个单向置换, 那么在信息论意义下,  $f(\text{sk})$  已经泄漏了关于  $\text{sk}$  的信息, 但是任何的 ppt 的敌手却只能以约  $1/2$  的概率猜中它的 hard-core 比特.

实现辅助输入密钥泄漏模型下的 PKE, 一个重要的技术是广义的 Goldreich-Levin(GL)定理<sup>[24]</sup>, 指的是在素数域  $\text{GF}(p)$  上如何产生单向函数的 Hard-Core. 由于广义的 GL 定理所使用的 Hard Core 函数是线性函数, 故仅有 BHHO 方案<sup>[1]</sup>和基于 LWE 的 PKE 方案<sup>[10]</sup>可以实现 IND-LR-CPA 安全. 目前还没有实现 IND-LR-CCA 安全的 PKE 高效的实例.

### 3.3 密钥相关信息的加密和 KDM-CCA 安全

与传统的 IND-CCA 安全模型相比, 敌人拿到的挑战密文可能是与私钥  $\text{sk}$  紧密联系的消息的加密. 这些消息可能是只有知道私钥  $\text{sk}$  才可以有效计算出来的关于  $\text{sk}$  的函数值.

敌人得到的信息包括: 公钥、加密预言机、挑战密文、解密预言机. 其中, 敌人可以多次询问加密预言机, 而挑战密文是加密预言机的输出: 要么每次都对一个固定明文的加密, 如对  $11\dots 1$  的加密, 要么每次都是对  $f_i(\text{sk})$  的加密. 而  $f_i$  可以由敌人从某个固定的函数集合  $\Psi$  中自由挑选, 函数值的长度应该和固定明文的长度相同.

**定义 5** 给定一个公钥加密方案  $\text{PKE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ . 如果任意的概率多项式时间(ppt)的敌手赢得图 6 中实验的概率都以可以忽略的量接近  $1/2$ , 即

$$\left| \text{Prob}[b = b'] - 1/2 \right| = \text{neg}(k)$$

那么这个 PKE 方案就是 KDM-CCA 安全的.

KDM-CCA 安全要求: ppt 的敌人不能区分挑战密文向量是对  $f_i(\text{sk})$  的加密还是对固定明文的加密. 如

果  $f_i(\text{sk})$  是一个常函数, 那么 KDM-CCA 安全就退化成了 IND-CCA 安全. 可见 KDM-CCA 安全比传统的 IND-CCA 安全要求更高<sup>[25]</sup>.

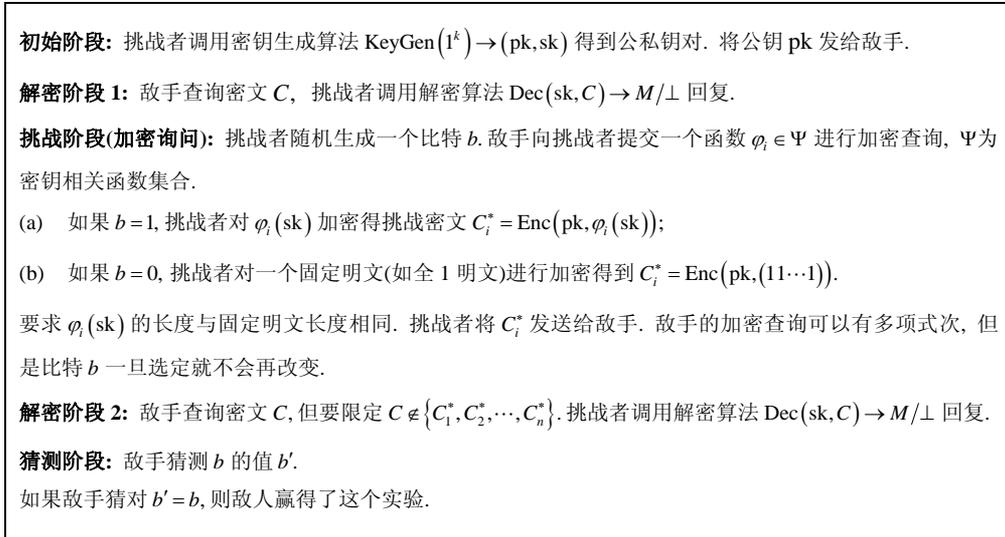


图 6 PKE 的 KDM-CCA 实验及安全模型

Figure 6 The KDM-CCA experiment of PKE and the security model

实现 KDM-CCA 的安全更具有挑战性, 现有的方法主要有: 利用 BHHO 方案<sup>[26]</sup>实现 KDM-CPA 安全, 再用 Noar-Yung 的两把密钥的方法将 KDM-CPA 安全的 PKE 转化为 KDM-CCA 安全的 PKE<sup>[27]</sup>; 使用 lossy algebraic filters<sup>[28]</sup>实现 KDM-CCA 安全. 另一种简单的方法则是直接使用 Cramer-Shoup 方案来实现 KDM-CCA, 但是不能使用私钥加密自身<sup>[29]</sup>.

敌手可以选择的密钥函数集合  $\Psi$  越大, 则密钥相关安全性就越好. 目前, 敌手所可以选择的密钥函数集合仅限于“仿射函数集合”, 如何扩大该集合是一个新的挑战.

### 3.4 “密钥相关攻击”(Related-Key Attack, 简称 RKA)及密钥相关安全(RK-CCA)

与传统的 IND-CCA 安全模型相比, 敌人得到的解密服务更为强大. 敌人可以选择函数  $\phi$ , 迫使解密算法用  $\phi(\text{sk})$  进行解密. 也就是解密预言机必须使用  $\text{Dec}(\phi(\text{sk}), C)$  使用对所提交的密文  $C$  进行解密. 如果函数为常函数  $\phi(\text{sk}) = \text{sk}$ , 则密钥相关的 RK-CCA 安全退化为传统的 IND-CCA 安全.

敌人得到的信息包括: 公钥、挑战密文、特殊的解密预言机. 其中, 特殊的解密预言机的功能更加强大. 敌人在询问特殊解密预言机时, 提交的是一个密文/函数对  $(C, f)$ , 解密预言机使用  $f(\text{sk})$  对密文  $C$  进行解密. 而函数  $f$  是敌人在某个函数集合中自由挑选. 挑战密文则是从敌人自己选择的长度相同的两个明文随机选出并加密得到的.

**定义 6** 给定一个公钥加密方案  $\text{PKE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ . 如果任意的概率多项式时间(ppt)的敌手赢得图 7 中实验的概率都可以忽略的量接近  $1/2$ , 即

$$\left| \text{Prob}[b = b'] - \frac{1}{2} \right| = \text{neg}(k)$$

那么这个 PKE 方案就是  $\Psi$ -IND-RK-CCA 安全的.

IND-RK-CCA 安全要求: 敌人不能区分挑战密文是他所选择的两个明文中哪个明文的加密. 如果敌人解密查询时提交的函数总是  $f(\text{sk}) = \text{sk}$  这样的特殊函数, 那么 IND-RK-CCA 安全就退化成为了传统的 IND-CCA 安全.

Wee<sup>[30]</sup>通过 finger-print 和 key homomorphism 的技术得到了基于各种标准困难性假设的 RKA-CCA 安全的 PKE, 但是密钥相关的函数集合仅限于线性函数. 其思路是: 如果一个具有 IND-CCA 安全的 PKE 还有 finger-print 和 key homomorphism 两种性质, 那么 RKA-CCA 安全就可以归约为 IND-CCA 安全. 原因是, 进行 RKA-CCA 攻击的敌手的所有密文查询  $(C, f)$  都可以通过 key homomorphism 技术转换为一个新的密文  $C'$ , 而 finger-print 性质又保证了  $C'$  与挑战密文  $C^*$  不同. 因此, 原 IND-CCA 安全的敌手就可以对  $C'$  进行解密查询, 进而完美回答了  $(C, f)$  的解密查询. Bellare, Paterson, Thomson<sup>[31]</sup>在 AsiaCrypt2012 中提出如何实现 RKA-CPA 安全的 IBE, 使用(B)CHK 转换即可得到 RKA-CCA 安全的 PKE, 其函数集合扩展到了私钥的多项式.

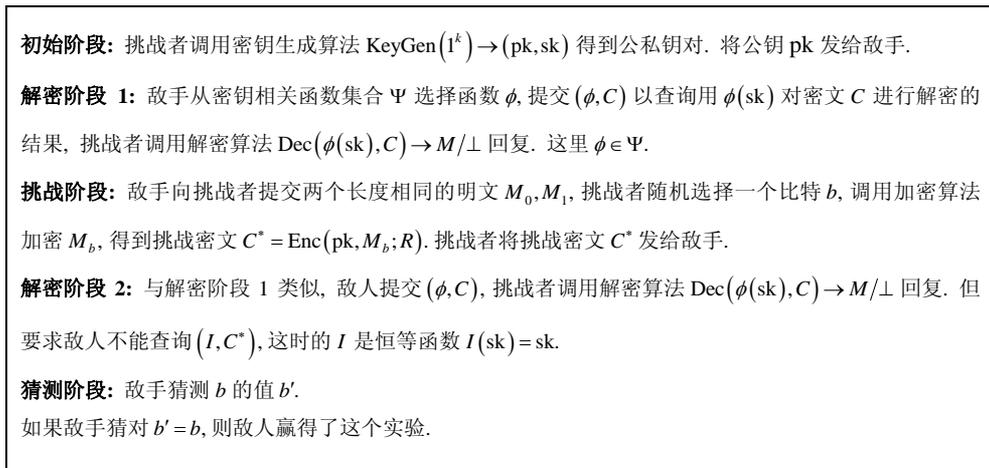


图 7 PKE 的  $\Psi$ -IND-RK-CCA 实验及安全模型

Figure 7 The  $\Psi$ -IND-RK-CCA experiment of PKE and the security model

新的挑战是如何继续扩大密钥相关的函数集合.

### 3.5 “随机数相关攻击”(Randomness-Related Attack, RRA)和随机数相关安全(RR-CCA)

在密码算法和协议中会用到大量的随机数, 而在安全分析中, 我们总是认为随机数永远是均匀独立选择的. 但是现实中的随机数并非如此完美, 甚至还会受到敌手的影响, 详见文献[32–38]等论文. 那么使用不完善的随机数进行公钥加密的话, 如何保证加密消息的安全性呢? 这就是随机数相关安全所要研究的.

在“随机数相关攻击”中, 敌手可以在某种程度上影响加密算法中使用的随机数的取值. 其影响的程度可以用一个函数集合  $\Psi$  来表示. 如果  $\Psi$  是恒等函数, 则“随机数相关攻击”下的 RR-CCA 就弱化为了 IND-CCA 安全.

**定义 7** 给定一个公钥加密方案  $PKE = (\text{KeyGen}, \text{Enc}, \text{Dec})$ . 如果任意的概率多项式时间(ppt)的敌手赢得图 8 中实验的概率都可以忽略的量接近  $1/2$ , 即

$$|\text{Prob}[b = b'] - 1/2| = \text{neg}(k)$$

那么这个 PKE 方案就是  $\psi$ -IND-RR-CCA 安全的.

敌人得到的信息包括: 公钥、挑战密文、特殊的加密预言机、解密预言机. 挑战密文则是从敌人自己选择的长度相同的两个明文中随机选出并加密得到的.

**IND-RR-CCA 安全要求:** 敌人不能区分挑战密文是他所选择的两个明文中哪个明文的加密.

对于随机数相关攻击, 最早由 Yilek 在 2010 年研究<sup>[39]</sup>. 目前最新的结果是 2014 年 Paterson, Schuldt, Sibborn 等<sup>[40]</sup>使用 Correlated-Input Secure Hash 以及可以抵抗 Related-key Attack 的伪随机函数构造的<sup>[23]</sup>. 然而目前可抵抗 Related-key Attack 的伪随机函数新的构造仅限于基于 DDH 类假设的构造. 其挑战是如何得到更多的构造以及如何扩大随机数相关函数集合  $\Psi$ .

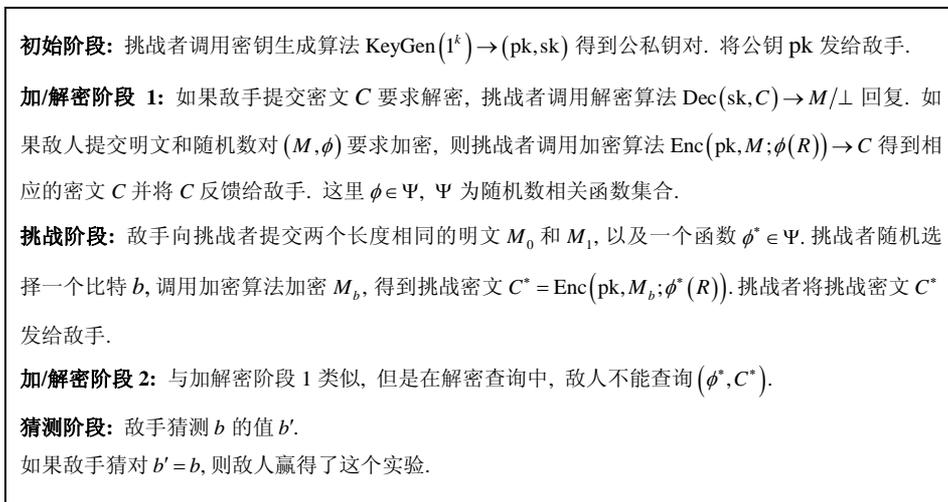


图 8 PKE 的  $\psi$ -IND-RR-CCA 实验及安全模型

Figure 8 The  $\psi$ -IND-RR-CCA experiment of PKE and the security model

## 4 结论

本文综合讨论了现在公钥加密系统面临的新的挑战, 包括: 选择打开攻击、密钥泄漏攻击、密钥相关消息加密、密钥相关攻击及随机数相关攻击. 并介绍了现有的各种新安全模型和新安全模型下的公钥加密系统实现可证明安全所需要的理论技术. 这些新的安全概念都比传统的 IND-CCA 安全要强. 如何设计出一个公钥加密方案使其同时满足上述各种新的安全属性则是一个更大的挑战.

## References

- [1] Naor M, Yung M. Public-key cryptosystems provably secure against chosen ciphertext attacks[C]. In: Proceedings of the 22nd Annual ACM Symposium on Theory of Computing—STOC '90. ACM, 1990: 427–437.
- [2] Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption[C]. In: Advances in Cryptology—EUROCRYPT 2002. Springer Berlin Heidelberg, 2002: 45–64.

- [3] Boneh D, Canetti R, Halevi S, et al. Chosen-ciphertext security from identity-based encryption[J]. *SIAM Journal on Computing*, 2006, 36(5): 1301–1328.
- [4] Canetti R, Halevi S, Katz J. Adaptively-secure, non-interactive public-key encryption[C]. In: *Theory of Cryptography Conference—TCC 2005*. Springer Berlin Heidelberg, 2005: 150–168.
- [5] Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption[C]. In: *Advances in Cryptology—EUROCRYPT 2004*. Springer Berlin Heidelberg, 2004: 207–222.
- [6] Peikert C, Waters B. Lossy trapdoor functions and their applications[C]. In: *Proceedings of the 40th Annual ACM Symposium on Theory of Computing—STOC 2008*. ACM Press, 2008: 187–196.
- [7] Watanabe Y, Shikata J, Imai H. Equivalence between semantic security and indistinguishability against chosen ciphertext attacks[C]. In: *Public Key Cryptography—PKC 2003*. Springer Berlin Heidelberg, 2002: 71–84.
- [8] Goldwasser S, Micali S. Probabilistic encryption[J]. *Journal of Computer and System Sciences*, 1984, 28(2): 270–299.
- [9] Rackoff C, Simon D R. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack[C]. In: *Advances in Cryptology—CRYPTO '91*. Springer Berlin Heidelberg, 1992: 433–444.
- [10] Hofheinz D, Rupp A. Standard versus selective opening security: separation and equivalence results[C]. In: *Theory of Cryptography Conference—TCC 2014*. Springer Berlin Heidelberg, 2014: 591–615.
- [11] Hemenway B, Ostrovsky R. Lossy trapdoor functions from smooth homomorphic hash proof systems[C]. In: *Electronic Colloquium on Computational Complexity—ECCC. 2009*: 127–127.
- [12] Hemenway B, Libert B, Ostrovsky R, et al. Lossy encryption: constructions from general assumptions and efficient selective opening chosen ciphertext security[C]. In: *Advances in Cryptology—ASIACRYPT 2011*. Springer Berlin Heidelberg, 2011: 70–88.
- [13] Hofheinz D. All-but-many lossy trapdoor functions[C]. In: *Advances in Cryptology—EUROCRYPT 2012*. Springer Berlin Heidelberg, 2012: 209–227.
- [14] Bellare M, Waters B, Yilek S. Identity-based encryption secure against selective opening attack[C]. In: *Theory of Cryptography Conference—TCC 2011*. Springer Berlin Heidelberg, 2011: 235–252.
- [15] Fehr S, Hofheinz D, Kiltz E, et al. Encryption schemes secure against chosen-ciphertext selective opening attacks[C]. In: *Advances in Cryptology—EUROCRYPT 2010*. Springer Berlin Heidelberg, 2010: 381–402.
- [16] Huang Z, Liu S, Qin B. Sender-equivocable encryption schemes secure against chosen-ciphertext attacks revisited[C]. In: *Public-Key Cryptography—PKC 2013*. Springer Berlin Heidelberg, 2013: 369–385.
- [17] Huang Z, Liu S, Qin B, et al. Fixing the sender-equivocable encryption scheme in Eurocrypt 2010[C]. In: *5th International Conference on Intelligent Networking and Collaborative Systems—INCoS 2013*. IEEE, 2013: 366–372.
- [18] Lai J, Deng R H, Liu S, et al. Identity-Based Encryption Secure against Selective Opening Chosen-Ciphertext Attack[C]. In: *Advances in Cryptology—EUROCRYPT 2014*. Springer Berlin Heidelberg, 2014: 77–92.
- [19] Kiltz E, Mohassel P, O'Neill A. Adaptive trapdoor functions and chosen-ciphertext security[C]. In: *Advances in Cryptology—EUROCRYPT 2010*. Springer Berlin Heidelberg, 2010: 673–692.
- [20] Liu S, Weng J, Zhao Y. Efficient public key cryptosystem resilient to key leakage chosen ciphertext attacks[C]. In: *Topics in Cryptology—CT-RSA 2013*. Springer Berlin Heidelberg, 2013: 84–100.
- [21] Naor M, Segev G. Public-key cryptosystems resilient to key leakage[C]. In: *Advances in Cryptology—CRYPTO 2009*. Springer Berlin Heidelberg, 2009: 18–35.
- [22] Qin B, Liu S. Leakage-resilient chosen-ciphertext secure public-key encryption from hash proof system and one-time lossy filter[C]. In: *Advances in Cryptology—ASIACRYPT 2013*. Springer Berlin Heidelberg, 2013: 381–400.
- [23] Qin B, Liu S. Leakage-flexible CCA-secure public-key encryption: simple construction and free of pairing[C]. In: *Public-Key Cryptography—PKC 2014*. Springer Berlin Heidelberg, 2014: 19–36.
- [24] Dodis Y, Goldwasser S, Kalai Y T, et al. Public-key encryption schemes with auxiliary inputs[C]. In: *Theory of Cryptography Conference—TCC 2010*. Springer Berlin Heidelberg, 2010: 361–381.
- [25] Cash D, Green M, Hohenberger S. New definitions and separations for circular security[C]. In: *Public Key Cryptography—PKC 2012*. Springer Berlin Heidelberg, 2012: 540–557.
- [26] Boneh D, Halevi S, Hamburg M, et al. Circular-secure encryption from decision diffie-hellman[C]. In: *Advances in Cryptology—CRYPTO 2008*. Springer Berlin Heidelberg, 2008: 108–125.
- [27] Camenisch J, Chandran N, Shoup V. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks[C]. In: *Advances in Cryptology—EUROCRYPT 2009*. Springer Berlin Heidelberg, 2009: 351–368.
- [28] Hofheinz D. Circular chosen-ciphertext security with compact ciphertexts[C]. In: *Advances in Cryptology—EUROCRYPT. 2013*: 520–536.

- [29] Qin B, Liu S, Huang Z. Key-dependent message chosen-ciphertext security of the Cramer-Shoup Cryptosystem[C]. In: Australasian Conference on Information Security and Privacy—ACISP 2013. Springer Berlin Heidelberg, 2013: 136–151.
- [30] Wee H. Public key encryption against related key attacks[C]. In: Public Key Cryptography—PKC 2012. Springer Berlin Heidelberg, 2012: 262–279.
- [31] Bellare M, Paterson K G, Thomson S. RKA security beyond the linear barrier: IBE, encryption and signatures[C]. In: Advances in Cryptology—ASIACRYPT 2012. Springer Berlin Heidelberg, 2012: 331–348.
- [32] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes[C]. In: Advances in Cryptology—CRYPTO '99. Springer Berlin Heidelberg, 1999: 537–554.
- [33] Goyal V, O'Neill A, Rao V. Correlated-input secure hash functions[C]. In: Theory of Cryptography Conference—TCC 2011. Springer Berlin Heidelberg, 2011: 182–200.
- [34] Guterman Z, Pinkas B, Reinman T. Analysis of the linux random number generator[C]. In: IEEE Symposium on Security and Privacy, 2006. IEEE, 2006: 371–385.
- [35] Heninger N, Durumeric Z, Wustrow E, et al. Mining your Ps and Qs: detection of widespread weak keys in network devices[C]. In: 21st USENIX Security Symposium. 2012: 205–220.
- [36] Debian: Debian Security Advisory DSA-1571-1: OpenSSL—Predictable Random Number Generator[OL]. <http://www.debian.org/security/2008/dsa-1571>.
- [37] Stamos A, Becherer A, Wilcox N. Cloud computing security—raining on the trendy new parade[C]. In: Black Hat USA, 2009.
- [38] Dorrendorf L, Guterman Z, Pinkas B. Cryptanalysis of the random number generator of the windows operating system[J]. ACM Transactions on Information and System Security, 2009, 13(1): 10.
- [39] Yilek S. Resettable public-key encryption: how to encrypt on a virtual machine[C]. In: Topics in Cryptology—CT-RSA 2010. Springer Berlin Heidelberg, 2010: 41–56.
- [40] Paterson K G, Schuldt J C N, Sibborn D L. Related randomness attacks for public key encryption[C]. In: Public-Key Cryptography—PKC 2014. Springer Berlin Heidelberg, 2014: 465–482.

#### 作者信息



刘胜利(1974–), 河北石家庄人, 博士, 上海交通大学教授. 在西安电子科技大学获学士、硕士和博士学位, 在荷兰爱因霍芬技术大学获密码学博士学位. 主要研究领域为公钥密码学、信息理论安全.

E-mail: slliu@sjtu.edu.cn