抗辅助输入 CCA 安全的 PKE 构造

王志伟[1)] 李道丰[2)] 张 伟[1)] 陈 伟[1)]

[1)](南京邮电大学计算机学院 南京 210023)

[2)](广西大学计算机与电子信息学院 南宁 530004)

摘 要 辅助输入模型是弹性泄露密码学中一个重要的泄露模型,它定义了一族不可逆的函数去模拟一类密钥泄露的情况.目前已有的抗辅助输入公钥加密方案(PKE)、身份基加密方案(IBE)都是选择明文攻击安全(CPA-secure)的,文中提出了一个抗辅助输入选择密文攻击安全(CCA-secure)的 PKE 方案.方案的构造使用了 Qin 等人在亚密 2013 提出的一次泄露过滤函数(one-time lossy filter),并利用 Goldreich-Levin 定理构造抗辅助输入的核心部分.方案的 CCA 安全证明利用了一次泄露过滤函数的泄露模式,在此模式下,由于仅泄露少量的私钥信息,因而攻击者对私钥依然存在很大的不确定性,其查询非法的密文会被挑战者以高概率拒绝.

关键词 弹性泄露密码学;辅助输入;一次泄露过滤函数;选择密文攻击安全

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2016.00562

CCA Secure PKE with Auxiliary Input

WANG Zhi-Wei[1)] LI Dao-Feng[2)] ZHANG Wei[1)] CHEN Wei[1)]

[1)](*School of Computer, Nanjing University of Posts and Telecommunications, Nanjing* 210023)

[2)](*School of Computer, Electronics and Information, Guangxi University, Nanning* 530004)

Abstract The auxiliary input model is an important leakage model in leakage-resilient cryptography, which defines a class of computationally uninvertible function families F to simulate a large class of leakage. Recently, almost all PKE and IBE schemes with auxiliary input are proved CPA secure, such as Dodis et al.'s PKE scheme and Yuen et al.'s IBE scheme. We proposed a CCA secure PKE scheme in this paper, and our construction is based on the one-time lossy filter, which is proposed by Qin et al. in AsiaCrypt 2013. We use the modified Goldreich-Levin theorem to design the hard core, which is the same as other schemes with auxiliary input. One-time lossy filter has two mode: injective mode and leakage mode, and the CCA security proof is mainly relied on the leakage mode. The difference of these two modes is that the one-time lossy filter in injective mode is an injective function, and it discloses all bits of secret key, but it only leaks a little bits of secret key in the leakage mode. So, we use the injective mode for practical and the leakage mode for security proof. Thus, the attacker in security proof cannot determine the secret key by such a little leaked bits and the queried ciphertexts will be rejected with high probability.

Keywords leakage-resilient cryptography; auxiliary input; one-time lossy filter; CCA secure

1 引 言

在传统的密码学中,密码方案的安全性通常基于一个假设,即密钥必须被安全保存,包括其他的中间状态(随机数).但是在实际中,密钥的泄露通常无法避免,例如侧信道攻击就可以得到密码运算的一些特性或者将密钥及随机数重复使用.因此,弹性泄

收稿日期:2014-11-03;最终修改稿收到日期:2015-06-30.本课题得到国家自然科学基金(61373006,61202353,61272422)和安徽大学信息保障技术协同创新中心 2015 年度开放课题资助.**王志伟**,男,1976 年生,博士,副教授,主要研究方向为信息安全与密码学.E-mail:zhwwang@njupt.edu.cn.**李道丰**,男,1974 年生,博士,副教授,主要研究方向为数字签名、网络安全以及密码协议.**张 伟**,男,1973 年生,博士,教授,主要研究领域为网络安全、密码协议.**陈 伟**,男,1979 年生,博士,教授,主要研究领域为网络安全、云安全.

露密码学(Leakage Resilient Cryptography)被提出以应对密钥的泄露问题，即如何在密钥泄露的情况下，保证密码方案的安全性. 弹性泄露密码学已成为密码学的研究热点，目前已提出的一些主要泄露模型如下：

(1) 仅计算泄露(Only computation leaks information). 假设设备在进行密码运算时，内存会泄露部分密钥信息，不参加运算的部件不会发生泄露[1-2].

(2) 泄露受限模型(Bounded leakage model). 不仅仅是运算会发生泄露，而是假设系统整个运行周期内，密钥或者内部状态泄露的比特数有一个最大阈值[3-7]. 如果泄露超过阈值，则希望会被及时发现并中止运行. 其中此类方案最重要的性能参数是泄露比值(leakage rate)，即可泄露的比特数和密钥总比特数的比值.

(3) 连续泄露模型(Continual leakage model). 这个模型假设在两个相继的密钥更新时间段内，密钥泄露的比特数是有限的，密钥需要定期的更新，这样可以承受连续的泄露[8-10].

(4) 辅助输入模型(Auxiliary input model). 由相对泄露模型发展而来，它允许攻击者拥有一类不可逆的辅助输入函数去模拟多种泄露的情况. 通过这些辅助输入函数，攻击者可以获得密钥的泄露信息. 但是无论这些泄露信息有多少，甚至密钥在信息论意义上已被完全泄露，但是这些泄露的信息都无法帮助攻击者恢复出密钥[11-12].

对于抗泄露的公钥加密方案(PKE)，抗选择明文攻击安全(CPA secure)是指概率多项式时间攻击者即使可以进行密钥泄露查询，也无法区分两个等长消息的密文. 如果攻击者还能进行解密查询，只是限制不可以对挑战密文进行查询，并且在生成挑战密文后停止密钥泄露的查询. 这样的安全性称为抗选择密文攻击安全(CCA secure). 哈希证明系统(hash proof sysem)是目前较为实用的构造 CCA 安全的 PKE 的方法，但是对于泄露受限模型下的 PKE，哈希证明系统只能做到密钥泄露比值低于 1/2. Qin 等人[13] 在 Hopfheinz 的泄露代数函数(lossy algebraic filter)[14] 基础上提出了简化版本，即一次泄露过滤函数(one-time lossy filter)，将泄露代数函数的代数特性等忽略，并且不要求函数可逆. Qin 等人[13] 用一次泄露过滤函数和哈希证明系统组合，设计出 CCA 安全的 PKE 方案，并且将密钥的泄露比值提高到 $1-o(1)$.

目前，提出的抗辅助输入的 PKE 方案[11]，包括 IBE 方案[12] 都是 CPA 安全的，我们的思路是利用一次泄露过滤函数将抗辅助输入的 PKE 方案提高到 CCA 安全. 一次泄露函数的特点是泄露模式下，仅泄露私钥有限的信息，安全证明中的挑战者能以很大概率将攻击者不合法的解密查询拒绝，这样做到 CCA 安全. 此外，一次泄露函数构造简单，没有泄露代数函数的代数特性，具有较好的效率，也是我们选用它进行构造的原因. 本文的主要贡献在于：(1) 证明了基于二次剩余群的一次泄露过滤函数 OTLF1 具有泄露性、不可区分性和躲闪性；(2) 基于 OTLF1 构造了一个抗辅助输入的 PKE 方案；(3) 对 PKE 方案给出了 CCA 安全的证明.

本文第 2 节列出和本文方案及证明相关的一些预备知识，包括抗辅助输入的 PKE 安全模型、Goldreich-Levin 定理、一次泄露过滤函数定义、卡梅隆哈希函数以及 DDH 假设；第 3 节给出一个基于二次剩余群的一次泄露过滤函数 OTLF1，并证明了它的特性；第 4 节设计了一个抗辅助输入的 PKE 方案，并给出安全性证明以及效率分析；第 5 节是结论.

2　预备知识

我们用 $\boldsymbol{x}\in\{0,1\}^n$ 表示向量，第 i 个分量表示为 x_i. 向量 $\boldsymbol{x},\boldsymbol{y}$ 的内积表示为 $\langle\boldsymbol{x},\boldsymbol{y}\rangle$，即 $\sum x_i y_i$. 我们用 $[n]$ 表示集合 $\{1,2,\cdots,n\}$. 如果 κ 表示安全参数，则 1^κ 表示 κ 个 1 组成的串. 如果 S 表示集合，则 $s\leftarrow S$ 表示从集合 S 均匀随机地选取元素 s. 我们用 $\boldsymbol{y}=A(\boldsymbol{x})$ 表示输入 $\boldsymbol{x}$，运行 A 得到结果 $\boldsymbol{y}$. 我们用 $negl(\kappa)$ 表示任意可忽略函数.

2.1　抗辅助输入 CCA 安全的 PKE

辅助输入模型下，攻击者可以访问私钥的附加信息，但是这种信息无论多少，攻击者都无法恢复私钥. 和泄露受限模型相比，辅助输入模型中攻击者获得的泄露信息从信息论角度转向了可计算性的角度. 令 $PKE=(G,E,D)$ 是一个公钥加密方案，其中 G 为密钥生成算法，E 为加密算法，D 为解密算法，私钥空间为 SK，公钥空间为 PK，消息空间为 M. 对于任意的函数族 $f=\{f_\kappa:SK\times PK\rightarrow\{0,1\}^*\}$，我们定义攻击者 $\mathfrak{A}$ 的求逆胜率为

$$Inv_f Adv[\mathfrak{A}]=\max\{\Pr_{(sk,pk)\leftarrow G(1^\kappa),f_\kappa\leftarrow f}[\mathfrak{A}(1^\kappa,f_\kappa(sk,pk))=sk]\}$$①.

① $Inv_f Adv[\mathfrak{A}]$ 表示攻击者 $\mathfrak{A}$ 对函数族 f 中所有函数求逆成功概率的最大值.

令 l 为私钥的比特长度. 对于任何多项式时间攻击者 $\mathfrak{A}$ 有 $Inv_f Adv[\mathfrak{A}] \leq \varepsilon$，则称多项式时间可计算函数族 f 是 $\varepsilon=\varepsilon(l)$ 求逆困难的. 这种“求逆困难函数”弱于单向函数的定义，因为单向函数需要完整恢复整个私钥.

根据文献[15-16]，对于任意的可计算函数族 f，通过挑战者 $\mathfrak{C}$ 和攻击者 $\mathfrak{A}$ 的交互，我们定义抗辅助输入 CCA 安全的 PKE 如下：

(1) 初始化. 挑战者 $\mathfrak{C}$ 生成公私钥对 $(sk,pk)\leftarrow G(1^\kappa)$，并选择 $b\leftarrow\{0,1\}$[①]，然后将 pk 发送给攻击者 $\mathfrak{A}$.

(2) 辅助输入查询. 挑战者 $\mathfrak{C}$ 任选 $f_\kappa\in f$，并计算 $z\leftarrow f_\kappa(sk,pk)$，发送给 $\mathfrak{A}$.

(3) 解密查询 1. 攻击者 $\mathfrak{A}$ 发送查询密文 CT 给 $\mathfrak{C}$，$\mathfrak{C}$ 利用 sk 返回明文 m 给 $\mathfrak{A}$.

(4) 挑战. 攻击者 $\mathfrak{A}$ 发送两个长度相等的明文 m_0,m_1 给 $\mathfrak{C}$，挑战者 $\mathfrak{C}$ 计算 $CT^*\leftarrow E(m_b)$，并返回给 $\mathfrak{A}$.

(5) 解密查询 2. 攻击者 $\mathfrak{A}$ 继续发送密文查询给 $\mathfrak{C}$，但不可以查询 CT^*.

(6) 输出. 攻击者 $\mathfrak{A}$ 输出猜测 $b'\leftarrow\{0,1\}$.

如果 $b=b'$，则称 $\mathfrak{A}$ 胜出上述游戏，定义 $Aux_f Adv[\mathfrak{A}]$ 为 $\mathfrak{A}$ 胜出的概率. 我们称 PKE 方案是抗辅助输入 CCA 安全的，当且仅当对任意的 ε-不可逆函数族 f 和任意的多项式时间攻击者 $\mathfrak{A}$，都有 $Aux_f Adv[\mathfrak{A}]=negl(\kappa)$.

2.2 Goldreich-Levin 定理

Goldreich 和 Levin[16] 在 1989 年提出了二元域的 Goldreich-Levin 定理，是目前抗辅助输入密码方案的基础.

定理 1. 令 $f:\{0,1\}^n\rightarrow\{0,1\}^*$ 是任意的函数，如果存在一个区分者 $\mathfrak{A}$ 在时间 t 内满足

$$|\Pr[\mathfrak{A}(\boldsymbol{y},\boldsymbol{r},\langle\boldsymbol{x},\boldsymbol{r}\rangle)=1|\boldsymbol{x},\boldsymbol{r}\leftarrow\{0,1\}^n,\boldsymbol{y}=f(\boldsymbol{x})]-\Pr[\mathfrak{A}(\boldsymbol{y},\boldsymbol{r},u)=1|\boldsymbol{x},\boldsymbol{r}\leftarrow\{0,1\}^n,u\leftarrow\{0,1\},\boldsymbol{y}=f(\boldsymbol{x})]|\geq\varepsilon,$$

则存在一个求逆者 $\mathfrak{B}$ 在时间 $t'=t\cdot poly(n,1/\varepsilon)$ 内满足

$$\Pr[\mathfrak{B}(\boldsymbol{y})=\boldsymbol{x}|\boldsymbol{x}\leftarrow\{0,1\}^n,\boldsymbol{y}\leftarrow f(\boldsymbol{x})]\geq\Omega(\varepsilon^3/n).$$

随后，Dodis 等人[11] 又证明了 Goldreich-Levin 定理在大域上也成立.

定理 2. 令 q 是素数，H 是 $GF(q)$ 的任意子集. 令 $f:H^n\rightarrow\{0,1\}^*$ 是任意的函数，如果存在一个区分者 $\mathfrak{A}$ 在时间 t 内满足

$$|\Pr[\mathfrak{A}(\boldsymbol{y},\boldsymbol{r},\langle\boldsymbol{x},\boldsymbol{r}\rangle)=1|\boldsymbol{x}\leftarrow H^n,\boldsymbol{r}\leftarrow GF(q)^n,\boldsymbol{y}=f(\boldsymbol{x})]-\Pr[\mathfrak{A}(\boldsymbol{y},\boldsymbol{r},u)=1|\boldsymbol{x}\leftarrow H^n,\boldsymbol{r}\leftarrow GF(q)^n,u\leftarrow GF(q),\boldsymbol{y}=f(\boldsymbol{x})]|\geq\varepsilon,$$

则存在一个求逆者 $\mathfrak{B}$ 在时间 $t'=t\cdot poly(n,|H|,1/\varepsilon)$ 内满足

$$\Pr[\mathfrak{B}(\boldsymbol{y})=\boldsymbol{x}|\boldsymbol{x}\leftarrow H^n,\boldsymbol{y}\leftarrow f(\boldsymbol{x})]\geq\frac{\varepsilon^3}{512\cdot n\cdot q^2}.$$

2.3 一次泄露过滤函数

Qin 等人[13] 在基于泄露代数过滤函数(lossy algebraic filter)的基础上，提出了一次泄露过滤函数(one-time lossy filter)的概念. 一次泄露过滤函数 (Dom,l_{LF})-OTLF 是一组由公钥 Fpk 和标记 t 确定的函数族，函数 $\mathrm{OTLF}_{Fpk,t}$ 将 $\boldsymbol{x}\in Dom$ 映射到 $\mathrm{OTLF}_{Fpk,t}(\boldsymbol{x})$. 标记集合 $\mathfrak{T}$ 可分为两个不可区分的子集，即单射标记集合 $\mathfrak{T}_{inj}$ 与泄露标记集合 $\mathfrak{T}_{lossy}$. 假如 t 为单射标记，则函数 $\mathrm{OTLF}_{Fpk,t}$ 也是单射函数，它的函数像大小为 $|Dom|$. 如果 t 为泄露标记，则函数 $\mathrm{OTLF}_{Fpk,t}$ 的像大小至多为 $2^{l_{LF}}$. 因此，函数 $\mathrm{OTLF}_{Fpk,t}(\boldsymbol{x})$ 在泄露模式下，只泄露关于 $\boldsymbol{x}$ 的 l_{LF} 比特信息. Qin 等人[17] 又提出了唯一泄露过滤函数(all-but-one lossy filter)，即泄露标记集合 $\mathfrak{T}_{lossy}$ 仅有一个元素，它是一次泄露过滤函数的特例，易于构造，并能和卡梅隆哈希函数组合成一次泄露过滤函数.

一次泄露过滤函数 (Dom,l_{LF})-OTLF 由 3 个概率多项式时将算法组成，即密钥生成、函数计算和泄露标记生成.

(1) 密钥生成(OTLF.Gen). 这个算法生成一次泄露过滤函数的公私钥对 (Fpk,Ftd). 公钥 Fpk 定义了一个标记空间 $\mathfrak{T}=\{0,1\}^*\times\mathfrak{T}_c$，分为单射标记子集 $\mathfrak{T}_{inj}$ 与泄露标记子集 $\mathfrak{T}_{lossy}$. 标记 $t=(t_a,t_c)$ 中，$t_a\in\{0,1\}^*$ 是辅助标记，$t_c\in\mathfrak{T}_c$ 是核心标记. 私钥 Ftd 是计算泄露标记的陷门.

(2) 函数计算(OTLF.Eval). 这个算法输入公钥 Fpk，标记 t 以及 $\boldsymbol{x}\in Dom$，输出 $\mathrm{OTLF}_{Fpk,t}(\boldsymbol{x})$.

(3) 泄露标记生成(OTLF.LTag). 这个算法输入私钥 Ftd，辅助标记 t_a，输出核心标记 t_c，满足 $t=(t_a,t_c)$ 是泄露标记.

一次泄露过滤函数 (Dom,l_{LF})-OTLF 具备 3 种性质：泄露性、不可区分性以及躲闪性.

(1) 泄露性. 假如 t 为单射标记，则函数 $\mathrm{OTLF}_{Fpk,t}$

① b 表示随机比特，CCA 安全定义中，攻击者 $\mathfrak{A}$ 无法区分挑战密文 CT^*. 对应的明文 m_b 是 m_0 还是 m_1.

也是单射函数，它的函数像大小为 $|Dom|$. 如果 t 为泄露标记，则函数 $\mathrm{OTLF}_{Fpk,t}$ 的像大小至多为 $2^{l_{LF}}$.

(2) 不可区分性. 对任意的概率多项式时间攻击者 $\mathfrak{A}$，都难以区分单射标记和泄露标记，其胜出概率满足下式：

$$Adv^{ind}_{\mathrm{OTLF},\mathfrak{A}}(\kappa):=|\Pr[\mathfrak{A}(Fpk,(t_a,t_c))=1]-\Pr[\mathfrak{A}(Fpk,(t_a,t'_c))=1]|,$$

其中 $t_a\leftarrow\mathfrak{A}(Fpk)$，$t'_c$ 由泄露标记生成算法生成，t_c 随机选自 $\mathfrak{T}_c$.

(3) 躲闪性. 对任意的概率多项式攻击者 $\mathfrak{A}$，即使给定一个泄露标记，它也难以计算出另一个非单射标记. 其胜出概率满足下式：

$$Adv^{eva}_{\mathrm{OTLF},\mathfrak{A}}(\kappa):=[(t'_a,t'_c)\neq(t_a,t_c)\wedge(t'_a,t'_c)\notin\mathfrak{T}/\mathfrak{T}_{inj}\mid(t_a,t_c)\in\mathfrak{T}_{lossy};(t'_a,t'_c)\leftarrow\mathfrak{A}(Fpk,(t_a,t_c))].$$

唯一泄露过滤函数(all-but-one lossy filter)[18] 由于只有一个泄露标记，所以只具有泄露性和不可区分性.

2.4　卡梅隆哈希函数

卡梅隆哈希函数[18] CH 是具有公私钥对 $(pk_{\mathrm{CH}},td_{\mathrm{CH}})$ 的特殊哈希函数，如果仅有计算公钥 pk_{CH}，CH 具有抗碰撞性，但是如果有陷门私钥 td_{CH}，则可以找到碰撞. CH 由 3 个概率多项式算法组成，即密钥生成、函数计算以及两可计算.

(1) 密钥生成(CH.Gen). 该算法生成卡梅隆哈希函数 CH 的公私钥对 $(pk_{\mathrm{CH}},td_{\mathrm{CH}})$.

(2) 函数计算(CH.Eval). 这个算法输入计算公钥 pk_{CH} 以及随机数 $r_{\mathrm{CH}}\leftarrow\mathfrak{R}_{\mathrm{CH}}$，将 $\boldsymbol{x}\in\{0,1\}^*$ 映射到 $\boldsymbol{y}\in\mathfrak{y}$. 如果 r_{CH} 在 $\mathfrak{R}_{\mathrm{CH}}$ 上是均匀分布的，则 $\boldsymbol{y}$ 在 $\mathfrak{y}$ 上也是均匀分布的.

(3) 两可计算(CH.Equ). 该算法输入陷门私钥 td_{CH}，$(\boldsymbol{x},r_{\mathrm{CH}})$ 以及 $\boldsymbol{x}'$，输出另一个随机数 $r'_{\mathrm{CH}}\in\mathfrak{R}_{\mathrm{CH}}$，满足函数计算结果相等

$$\mathrm{CH.Eval}(pk_{\mathrm{CH}},\boldsymbol{x};r_{\mathrm{CH}})=\mathrm{CH.Eval}(pk_{\mathrm{CH}},\boldsymbol{x}';r'_{\mathrm{CH}}).$$

其间 r'_{CH} 同样在 $\mathfrak{R}_{\mathrm{CH}}$ 上是均匀分布.

卡梅隆哈希函数 CH 在仅有计算公钥 pk_{CH} 情况下，具有抗碰撞性，即对于任何概率多项式时间攻击者 $\mathfrak{A}$，难以找到 $(\boldsymbol{x},r_{\mathrm{CH}})\neq(\boldsymbol{x}',r'_{\mathrm{CH}})$，使得它们函数值相等. $\mathfrak{A}$ 的胜出概率为

$$Adv^{cr}_{\mathrm{CH},\mathfrak{A}}(\kappa):=\Pr[(\boldsymbol{x},r_{\mathrm{CH}})\neq(\boldsymbol{x}',r'_{\mathrm{CH}})\wedge\mathrm{CH.Eval}(pk_{\mathrm{CH}},\boldsymbol{x};r_{\mathrm{CH}})=\mathrm{CH.Eval}(pk_{\mathrm{CH}},\boldsymbol{x}';r'_{\mathrm{CH}})\mid(\boldsymbol{x},r_{\mathrm{CH}},\boldsymbol{x}',r'_{\mathrm{CH}})\leftarrow\mathfrak{A}(pk_{\mathrm{CH}})].$$

2.5　DDH 假设

确定性 Diffie-Hellman(DDH)假设：令素数阶 q 群 G 的生成元 g，任意选择 G 的生成元 g_1,g_2 以及随机数 $r\in\mathbb{Z}_q$ 和 $r'\in\mathbb{Z}_q\backslash\{r\}$，DDH 假设成立当且仅当对任意概率多项式时间攻击者 $\mathfrak{D}$，

$$Adv^{\mathrm{ddh}}_{G,\mathfrak{D}}(\kappa)=|\Pr[\mathfrak{D}(g_1,g_2,g_1^r,g_2^r)=1]-\Pr[\mathfrak{D}(g_1,g_2,g_1^r,g_2^{r'})=1]|$$

是可忽略的.

Naor 等人[19] 将 DDH 假设扩展到 $m>2$ 个生成元，并证明等价于 DDH 假设，即任意选择 G 的生成元 $g_1,\cdots,g_m$ 以及随机数 $r\in\mathbb{Z}_q$ 和 $r_1,\cdots,r_m\in\mathbb{Z}_q$，DDH 假设成立当且仅当对任意概率多项式时间攻击者 $\mathfrak{D}$，

$$Adv^{\mathrm{ddh}}_{G,\mathfrak{D}}(\kappa)=|\Pr[\mathfrak{D}(g_1,\cdots,g_m,g_1^r,\cdots,g_m^r)=1]-\Pr[\mathfrak{D}(g_1,\cdots,g_m,g_1^{r_1},\cdots,g_m^{r_m})=1]|$$

是可忽略的.

假设 $\varpi_1=d\log_g g_1,\cdots,\varpi_m=d\log_g g_m$，其中 $\varpi_1,\cdots,\varpi_m\in\mathbb{Z}_q$，DDH 假设中任意概率多项式时间攻击者 $\mathfrak{D}$ 胜出概率可变为

$$Adv^{\mathrm{ddh}}_{G,\mathfrak{D}}(\kappa)=|\Pr[\mathfrak{D}(\varpi_1,\cdots,\varpi_m,r\varpi_1,\cdots,r\varpi_m)=1]-\Pr[\mathfrak{D}(\varpi_1,\cdots,\varpi_m,r_1\varpi_1,\cdots,r_m\varpi_m)=1]|$$

是可忽略的.

3　一次泄露函数的构造

3.1　子群不可区分假设

Brakerski 等人[20] 提出了子群不可区分假设，即有限可交换乘法群 G 是两个群的直积 $G=G_{\tau_1}\times G_{\tau_2}$，其中 G_{τ_1} 为循环群且阶为 τ_1，G_{τ_2} 的阶为 τ_2，G 的阶为 $\tau_1\cdot\tau_2$，要求 $gcd(\tau_1,\tau_2)=1$. 如果 $1/\tau_2=negl(\kappa)$，则对于任意概率多项式时间攻击者 $\mathfrak{A}$ 均有

$$Adv^{sg}_{\mathfrak{A}}(\kappa)=|\Pr[\boldsymbol{x}\leftarrow G:\mathfrak{A}(1^\kappa,\boldsymbol{x})=1]-\Pr[\boldsymbol{x}\leftarrow G_{\tau_2}:\mathfrak{A}(1^\kappa,\boldsymbol{x})=1]|=negl(\kappa).$$

Qin 等人[17] 又提出了改进的子群不可区分假设，即要求 G_{τ_2} 也为循环群，则 G 也为循环群. 对于任意概率多项式时间攻击者 $\mathfrak{A}$ 均有

$$Adv^{rsg}_{\mathfrak{A}}(\kappa)=|\Pr[\boldsymbol{x}\leftarrow G:\mathfrak{A}(1^\kappa,\boldsymbol{x})=1]-\Pr[\boldsymbol{x}\leftarrow G_{\tau_1}:\mathfrak{A}(1^\kappa,\boldsymbol{x})=1]|=negl(\kappa).$$

令 g,h 分别为 G_{τ_1} 和 G_{τ_2} 的生成元. 定义一个上界 $T\geq\tau_1\cdot\tau_2$，随机选取 $\boldsymbol{x}\leftarrow_R\mathbb{Z}_T$，则 $g^{\boldsymbol{x}}$ 均匀分布于 G_{τ_1}，$h^{\boldsymbol{x}}$ 均匀分布于 G_{τ_2}. 令 $\mathfrak{G}=(G,T,g,h)$ 是如上所述的有

限交换乘法群,可以得出如下引理.

引理 1. 如果改进的子群不可区分假设在 G 上成立,则对于任意的概率多项式时间攻击者 $\mathfrak{B}$,都有

$$|\Pr[\boldsymbol{x}\leftarrow G_{\tau_1}:\mathfrak{B}(\mathfrak{G},\boldsymbol{x})=1]-\Pr[\boldsymbol{x}\leftarrow G/G_{\tau_1}:\mathfrak{B}(\mathfrak{G},\boldsymbol{x})=1]|\leq 2\cdot Adv^{rsg}_{\mathfrak{A}}(\kappa),$$

$$|\Pr[\boldsymbol{x}\leftarrow G_{\tau_1}:\mathfrak{B}(\mathfrak{G},\boldsymbol{x})=1]-\Pr[\boldsymbol{x}\leftarrow G_{\tau_1}:\mathfrak{B}(\mathfrak{G},\boldsymbol{x}\cdot h)=1]|\leq 2\cdot Adv^{rsg}_{\mathfrak{A}}(\kappa).$$

3.2 基于二次剩余群的一次泄露函数

选取 3 个不同的大素数 p,q,P,满足 $P=2pq+1$,则二次剩余群 $\mathbb{QR}_P=G_p\times G_q$,阶为 $T=|\mathbb{QR}_P|=pq$. 二次剩余群 $\mathbb{QR}_P=G_p\times G_q$ 满足 3.1 节的改进的子群不可区分假设,如果不能分解 T,则任意概率多项式时间的攻击者 $\mathfrak{A}$ 都无法区分 $\boldsymbol{x}\in\mathbb{QR}_P$ 和 $\boldsymbol{x}\in G_p$. 令 g,h 分别为 G_p 和 G_q 的生成元,定义一次泄露函数 OTLF1[16] 如下:

(1) 密钥生成. 任意选择 $s\in\mathbb{Z}_p$,$(t_a^*,t_c^*)\in\{0,1\}^*\times\mathfrak{R}_{\mathrm{CH}}$,计算 $\beta^*=\mathrm{CH.Eval}(pk_{\mathrm{CH}},t_a^*;t_c^*)$. 计算公钥 $Fpk=(g,h,\mathbb{QR}_P,T,EK=g^sh^{-\beta^*})$,陷门私钥为 $Ftd=(td_{\mathrm{CH}},(t_a^*,t_c^*))$. 标记空间为 $\mathfrak{T}=\{0,1\}^*\times\mathfrak{R}_{\mathrm{CH}}$,泄露标记子集为

$$\mathfrak{T}_{lossy}=\{(t_a,t_c)|(t_a,t_c)\in\mathfrak{T}\wedge\beta^*=\mathrm{CH.Eval}(pk_{\mathrm{CH}},t_a;t_c)\}.$$

单射标记子集为

$$\mathfrak{T}_{inj}=\{(t_a,t_c)|(t_a,t_c)\in\mathfrak{T}\wedge\beta^*\neq\mathrm{CH.Eval}(pk_{\mathrm{CH}},t_a;t_c)\}.$$

(2) 函数计算. 对于 $\boldsymbol{x}\in\mathbb{Z}_T$ 和标记 $(t_a,t_c)\in\{0,1\}^*\times\mathfrak{R}_{\mathrm{CH}}$,计算 $\beta=\mathrm{CH.Eval}(pk_{\mathrm{CH}},t_a;t_c)$,再计算 $\boldsymbol{y}=(g^s\cdot h^{-\beta^*}\cdot h^{\beta})^{\boldsymbol{x}}$.

(3) 泄露标记生成. 对于辅助标记 t_a,用陷门私钥 Ftd 计算核心标记 $\mathrm{CH.Equ}(td_{\mathrm{CH}},t_a^*,t_c^*,t_a)$.

定理 3. OTLF1 是一个基于二次剩余群的 $(\mathbb{Z}_T,\log p)$一次泄露过滤函数.

证明. 假如 $t=(t_a,t_c)$为单射标记,则 $\beta\neq\beta^*$,$(g^s\cdot h^{\beta-\beta^*})^{\boldsymbol{x}}$ 是一个 $\mathbb{QR}_P$ 上的单射函数. 假如 $t=(t_a,t_c)$是泄露标记,则 $\beta=\beta^*$,$(g^s\cdot h^{\beta-\beta^*})^{\boldsymbol{x}}=g^{s\cdot\boldsymbol{x}}\in G_p$,只泄露 $\log p$ 比特的信息. 因此 OTLF1 的泄露性成立.

$s\in\mathbb{Z}_p$是随机数,且$(t_a^*,t_c^*)\in\{0,1\}^*\times\mathfrak{R}_{\mathrm{CH}}$也是随机的,则 β^* 也是随机数. 对于 $\boldsymbol{x}\in\mathbb{Z}_T$,$g^{s\cdot\boldsymbol{x}}$均匀分布于 G_p,$(g^s\cdot h^{\beta-\beta^*})^{\boldsymbol{x}}$均匀分布于 $\mathbb{QR}_P$. 由于二次剩余群 $\mathbb{QR}_P=G_p\times G_q$满足 3.1 节的改进的子群不可区分假设,可由引理 1 得到

$$Adv^{ind}_{\mathrm{OTLF1},\mathfrak{A}}(\kappa)\leq 2\cdot Adv^{rsg}_{\mathbb{QR}_P,\mathfrak{A}}(\kappa).$$

因此 OTLF1 的不可区分性成立.

由 OTLF1 的构造可知,它是由唯一泄露过滤函数和卡梅隆哈希函数组合而成,其中 β^* 是其中唯一泄露过滤函数仅有的泄露标记,因此 OTLF1 的躲闪性仅依赖于卡梅隆哈希函数的抗碰撞性,即

$$Adv^{eva}_{\mathrm{OTLF1},\mathfrak{A}}(\kappa)\leq Adv^{cr}_{\mathrm{CH},\mathfrak{A}}(\kappa).$$ 证毕.

综上所述,OTLF1 是一个基于二次剩余群的 $(\mathbb{Z}_T,\log p)$一次泄露过滤函数.

4 抗辅助输入 CCA 安全的 PKE 方案

Dodis 等人[11] 提出了一种抗辅助输入的 PKE 方案,但是其安全是 CPA 安全. 在本节中,我们利用 3.2 节的 OTLF1 函数将其改进为 CCA 安全方案. PKE 方案由 3 个概率多项式时间算法组成:密钥生成、加密和解密.

(1) 密钥生成$(1^\kappa,\varepsilon)$. 选择至少为 κ 比特的大素数 p,q,计算 $P=2pq+1$,则 $\mathbb{Z}_P^*$ 是阶为 $T=pq$ 的二次剩余群,记为 $\mathbb{QR}_P$. 那么 $\mathbb{QR}_P$ 也是两个循环群的直积 $\mathbb{QR}_P=G_p\times G_q$. 令 $m=(4\log T)^{1/\varepsilon}$,选择 $\mathbb{QR}_P$ 中的生成元 g 以及 $r_1,\cdots,r_m\in\mathbb{Z}_N$. 令向量 $\boldsymbol{r}=(r_1,\cdots,r_m)$,$\boldsymbol{g}=(g^{r_1},\cdots,g^{r_m})$,选择 m 比特的随机串 $\boldsymbol{s}=(s_1,\cdots,s_m)\in\{0,1\}^m$,再选择随机标记$(t_a^*,t_c^*)\in\{0,1\}^*\times\mathfrak{R}_{\mathrm{CH}}$以及具有公私钥对$(pk_{\mathrm{CH}},td_{\mathrm{CH}})$的卡梅隆哈希函数CH,计算$\beta^*=\mathrm{CH.Eval}(pk_{\mathrm{CH}},t_a^*;t_c^*)$. 选择 G_p中的生成元$\tilde{g}$,G_q中的生成元$\tilde{h}$ 以及$v\in\mathbb{Z}_p$,计算 $EK=\tilde{g}^v\tilde{h}^{-\beta^*}$. 公钥为 $PK=(N,g,\mathbb{QR}_P,T,\boldsymbol{r},\boldsymbol{g},\langle\boldsymbol{r},\boldsymbol{s}\rangle,\tilde{g},\tilde{h},EK,pk_{\mathrm{CH}})$. 私钥为 $SK=(\boldsymbol{s})$.

(2) 加密(PK,M). 输入公钥 PK 和明文 $M\in\mathbb{QR}_P$,选择$\varpi\in\mathbb{Z}_T$,计算

$$C=\varpi\cdot\boldsymbol{r},\ K=\varpi\cdot\langle\boldsymbol{r},\boldsymbol{s}\rangle,$$

$$\psi=g^K\cdot M,\ \Pi=(EK\cdot\tilde{h}^{\beta})^K,$$

其中 $\beta=\mathrm{CH.Eval}(pk_{\mathrm{CH}},t_a;t_c)$,辅助标记 $t_a=(C,\psi)$,随机选择核心标记 $t_c\in\mathfrak{R}_{\mathrm{CH}}$. 密文为 $CT=(C,\psi,\Pi,t_c)\in\mathbb{Z}_T^m\times\mathbb{QR}_P\times\mathbb{QR}_P\times\mathfrak{R}_{\mathrm{CH}}$.

(3) 解密(SK,CT). 输入密文$CT=(C,\psi,\Pi,t_c)$以及私钥$SK=(\boldsymbol{s})$,计算 $K'=(\boldsymbol{C},\boldsymbol{s})$和 $\Pi'=(EK\cdot\tilde{h}^{\beta})^{K'}$,其中$\beta=\mathrm{CH.Eval}(pk_{\mathrm{CH}},(C,\psi);t_c)$. 校验 $\Pi'=\Pi$ 是否成立,如果不成立,则拒绝解密并返回 $\perp$. 如果成立,则返回明文 $M=\psi/K'$.

注意:在 CCA 安全证明中,如果攻击者解密查

询的密文都是合法的，则攻击者能够获得额外的密钥信息和公钥泄漏的私钥信息是完全一样的. 如果攻击者提交非法密文解密询问且通过验证的话，那么从理论角度，攻击者可以完全确定密钥信息. 因此，必须提供一种机制将敌手所有解密查询的非法密文拒绝解密. 在上述方案中，我们加入了 3.2 节的一次泄露过滤函数 OTLF1，作为对密文的认证. 在证明中，当攻击者$\mathfrak{A}$进行解密查询时，挑战者$\mathfrak{C}$可以利用一次泄露过滤的性质，将非法的密文拒绝. 其原因是$\mathfrak{A}$的查询密文以很大的概率，是带单射标记，如果不合法，那么$\mathfrak{A}$必须了解私钥的全部信息. 但是，挑战密文中又带的是泄露标记，其泄露的私钥信息非常有限，因此$\mathfrak{A}$查询的非法密文会被拒绝，从而做到 CCA 安全.

定理 4.　如果改进的子群不可区分假设在$\mathbb{QR}_P$上成立，CH 是一个卡梅隆哈希函数，则本节 PKE 方案是抗辅助输入 CCA 安全(AI-CCA)的，且概率多项式时间攻击者$\mathfrak{A}$的胜出概率如下：

$$Adv_{\mathrm{PKE},\mathfrak{A}}^{\mathrm{AI\text{-}CCA}}\leq 2\cdot Adv_{\mathbb{QR}_P,\mathfrak{B}_1}^{rsg}(\kappa)+Adv_{\mathbb{QR}_P,\mathfrak{B}_1}^{\mathrm{ddh}}(\kappa)+$$
$$Q(\kappa)\cdot\left(Adv_{\mathrm{CH},\mathfrak{B}_4}^{cr}(\kappa)+\frac{2^{\log p}}{2^{\log T}-Q(\kappa)}+\frac{\varepsilon^3}{512\cdot m\cdot T^2}\right)+\varepsilon,$$

其中$Q(\kappa)$为$\mathfrak{A}$进行的解密查询次数.

证明.　我们将通过挑战者$\mathfrak{C}$和概率多项式时间攻击者$\mathfrak{A}$之间的系列交互游戏 $\mathrm{Game}_0,\cdots,\mathrm{Game}_5$ 来证明上述定理. 在每个游戏中，$\mathfrak{C}$选定一个比特 b，$\mathfrak{A}$输出一个比特 b'作为对 b 的猜测. 令 E_i 表示在 Game_i 中 $b'=b$ 的事件.

Game_0. 这是初始的抗辅助输入 CCA 安全的游戏，挑战者$\mathfrak{C}$首先产生公私钥对(PK,SK)，将公钥 PK 发送给攻击者$\mathfrak{A}$. 当$\mathfrak{A}$进行解密查询或者私钥泄露查询时，$\mathfrak{C}$利用(PK,SK)返回解密结果，或者泄露值 $f(PK,SK)$. 接着，$\mathfrak{A}$提供两个等长的明文 M_0,M_1给$\mathfrak{C}$，$\mathfrak{C}$选择 b 并对 M_b返回挑战密文 CT^*. 接着，$\mathfrak{A}$继续进行解密查询，但是不能查询 CT^*. 最后，$\mathfrak{A}$输出对 b 的猜测 b'. 我们有 $Adv_{\mathrm{PKE},\mathfrak{A}}^{\mathrm{AI\text{-}CCA}}=|\Pr[E_0]-1/2|$.

Game_1. 这个游戏和 Game_0相似，不同的是挑战密文 CT^* 中的核心标记 t_c. 在 Game_1中，挑战者$\mathfrak{C}$利用卡梅隆函数的陷门私钥 td_{CH}和一次泄露过滤函数 OTLF1 的泄露标记生成算法 $\mathrm{CH.Equ}(td_{\mathrm{CH}},t_a^*,t_c^*,t_a)$产生 t_c，使得(t_a,t_c)是一个泄露标记. 而在 Game_0中，挑战密文 CT^* 中的核心标记 t_c随机选自$\mathfrak{T}_c$. 由于 OTLF1 中泄露标记和随机标记的不可区分性，对于 OTLF1 不可区分性任意概率多项式时间的攻击者$\mathfrak{B}_1$，我们有

$$|\Pr[E_1]-\Pr[E_0]|=Adv_{\mathrm{OTLF1},\mathfrak{B}_1}^{ind}(\kappa)$$
$$\leq 2\cdot Adv_{\mathbb{QR}_P,\mathfrak{B}_1}^{rsg}(\kappa).$$

Game_2. 这个游戏和 Game_1类似，除了$\mathfrak{A}$在做解密查询时，如果查询密文中的标记拷贝了挑战密文的泄露标记，此时，挑战者$\mathfrak{C}$要立即停止并输出 $\perp$. 在 Game_2中，假设查询密文中的标记拷贝了挑战密文的泄露标记，如果 $\Pi=\Pi'$，则暗示 $CT=CT^*$，在这种情况下，Game_1和 Game_2中，$\mathfrak{A}$都是被拒绝做密文查询的. 如果 $\Pi\neq\Pi'$，但是由于$(t_a,t_c)=((C,\Psi),t_c)=((\boldsymbol{C}^*,\Psi^*),t_c^*)=(t_a^*,t_c^*)$，所以 $K=K^*$，$\mathrm{OTLF}_{Fpk,t}(K)=\mathrm{OTLF}_{Fpk,t^*}(K^*)=\Pi^*$，那么这样的解密查询也会在 Game_1中被拒绝. 综上，$\Pr[E_2]=\Pr[E_1]$.

Game_3. 这个游戏类似于 Game_2，除了挑战密文 CT^* 中的 $\boldsymbol{C}^*=\varpi\cdot\boldsymbol{r}=(\varpi r_1,\cdots,\varpi r_m)$替换为 $\boldsymbol{C}^*=(\varpi_1 r_1,\cdots,\varpi_m r_m)$，则 CT^* 中的向量 $\boldsymbol{C}^*$ 各分量独立，且随机选自 $\mathbb{Z}_T$. 对于 DDH 假设的攻击者$\mathfrak{B}_3$，$|\Pr[E_3]-\Pr[E_2]|\leq Adv_{\mathbb{QR}_P,\mathfrak{B}_1}^{\mathrm{ddh}}(\kappa)$.

Game_4. 这个游戏类似于 Game_3，除了一个解密查询拒绝的规则，即$\mathfrak{A}$提交的查询密文 CT 中的向量 $\boldsymbol{C}$ 不合法，那么挑战者$\mathfrak{C}$要立即停止并输出 $\perp$. 令 $\bar{E}$ 表示被查询密文 Game_4拒绝但是被 Game_3接受的事件，我们有$|\Pr[E_4]-\Pr[E_3]|\leq\Pr[\bar{E}]$. $\Pr[\bar{E}]$必须是可忽略的，证明如下：

令 F 表示在 Game_4中，存在一个解密查询，密文中的标记$(t_a,t_c)=((C,\Psi),t_c)$是一个非单射，非拷贝的标记. 我们有

$$\Pr[\bar{E}]=\Pr[\bar{E}\wedge F]+\Pr[\bar{E}\wedge\neg F]$$
$$\leq\Pr[F]+\Pr[\bar{E}|\neg F].$$

(1) 如果 F 发生，则存在一个查询密文中的标记(t_a,t_c)是泄露标记. 假设$\mathfrak{B}_4$是一次泄露过滤函数 OTLF1 的攻击者，它的目标是在不知道陷门私钥 Ftd 的情况下，输出泄露标记. 同时$\mathfrak{B}_4$在 Game_4扮演挑战者，对$\mathfrak{A}$的解密查询作应答，当需要产生挑战密文时，$\mathfrak{B}_4$将作泄露标记查询，OTLF1 的挑战者返回泄露标记(t_a^*,t_c^*). 当攻击者$\mathfrak{A}$的 $Q(\kappa)$次解密查询中，有一次发生了 F 事件，即(t_a,t_c)是一个泄露标记，则$\mathfrak{B}_4$可以将(t_a,t_c)作为它的最终输出. 由 OTLF1 的构造可知，它是由唯一泄露过滤函数和卡梅隆哈希函数组合而成，其中 β^* 是唯一泄露过

滤函数仅有的泄露标记. 因此,如果(t_a,t_c)是泄露标记,则表示卡梅隆哈希函数 CH 产生了碰撞 $\mathrm{CH.Eval}(pk_{\mathrm{CH}},t_a;t_c)=\mathrm{CH.Eval}(pk_{\mathrm{CH}},t_a^*;t_c^*)$,因此

$$\begin{aligned}\Pr[F]&\leq Q(\kappa)\cdot Adv^{eva}_{\mathrm{OTLF1},\mathfrak{B}_4}(\kappa)\\&\leq Q(\kappa)\cdot Adv^{cr}_{\mathrm{CH},\mathfrak{B}_4}(\kappa).\end{aligned}$$

(2) 如果 F 未发生,则所有查询密文中的标记(t_a,t_c)都是单射标记. 假设 $CT=(C,\psi,\Pi,t_c)$是给定$\neg F$,使得 $\bar{E}$ 事件发生的第一个查询密文,其中的向量 $\boldsymbol{C}$ 不合法,但是 $\Pi=\mathrm{OTLF1}_{PK,t}(\langle\boldsymbol{C},\boldsymbol{s}\rangle)$,其中$t=((C,\psi),t_a)$. 攻击者 $\mathfrak{A}$ 能获知公钥 PK,挑战密文 CT^* 以及辅助输入 $f(\boldsymbol{r},\boldsymbol{s})$. 由于向量 $\boldsymbol{C}$ 不合法,则 PK 和 C 对获知 K 没有帮助,即 $\Pr[K\mid PK,C]=\Pr[K]$. 挑战密文 CT^* 中,仅有 Π^* 泄露了有关 K 的 $\log p$ 比特,ψ^* 中的 K 隐藏于 g^K. $K\in\mathbb{Z}_T$ 有 $2^{\log T}$ 种取值,$\mathfrak{A}$ 共进行了 $Q(\kappa)$ 次解密查询,因此 $\Pr[K\mid CT^*]=\frac{2^{\log p}}{2^{\log T}-Q(\kappa)}$. 由 Goldreich-Levin 定理可知,辅助输入 $f(\boldsymbol{r},\boldsymbol{s})$和公钥 PK 对恢复私钥 $\boldsymbol{s}$ 的帮助可忽略,概率为$\frac{\varepsilon^3}{512\cdot m\cdot T^2}$. 综上,

$$\Pr[\bar{E}\mid\neg F]\leq Q(\kappa)\cdot\left(\frac{2^{\log p}}{2^{\log T}-Q(\kappa)}+\frac{\varepsilon^3}{512\cdot m\cdot T^2}\right).$$

我们有

$$\begin{aligned}\Pr[\bar{E}]&\leq\Pr[F]+\Pr[\bar{E}\mid\neg F]\\&\leq Q(\kappa)\cdot\left(Adv^{cr}_{\mathrm{CH},\mathfrak{B}_4}(\kappa)+\frac{2^{\log p}}{2^{\log T}-Q(\kappa)}+\frac{\varepsilon^3}{512\cdot m\cdot T^2}\right).\end{aligned}$$

Game_5. 这个游戏类似于 Game_4,除了 ψ^* 的产生方式. 在这个游戏中,挑战者 $\mathfrak{C}$ 在 $\mathbb{QR}_P$ 上随机选择 ψ^*,而不是用 $g^{\langle\boldsymbol{C}^*,\boldsymbol{s}\rangle}M_b$ 产生. 挑战者 $\mathfrak{C}$ 将对辅助输入 $f(\boldsymbol{r},\boldsymbol{s})$求逆的任务归约为以不可忽略的概率 ε 区分 Game_5 和 Game_4. $\mathfrak{C}$ 希望构建一个有效的算法,在给定公钥和辅助输入 $f(\boldsymbol{r},\boldsymbol{s})$ 之下,依据 Goldreich-Levin 定理至少以概率$\frac{\varepsilon^3}{512\cdot m\cdot T^2}$输出 $\boldsymbol{s}$,其中 ε 是区分$(PK,f(\boldsymbol{r},\boldsymbol{s}),\boldsymbol{r},\langle\boldsymbol{r},\boldsymbol{s}\rangle)$和$(PK,f(\boldsymbol{r},\boldsymbol{s}),\boldsymbol{r},u)$①. 的优势概率. 显而易见,$\mathfrak{C}$ 如果输入 $z=\langle\boldsymbol{r},\boldsymbol{s}\rangle\in\mathbb{Z}_T$,则它可以模拟 Game_4,如果 $\mathfrak{C}$ 选择随机的 z,则它可以模拟 Game_5. 因此,$|\Pr[E_5]-\Pr[E_4]|\leq\varepsilon$. 综合 $\mathrm{Game}_{0\sim5}$,在 Game_5 中,挑战密文 $CT^*=(\boldsymbol{C}^*,\psi^*,\Pi^*,t_c^*)$中的向量 $\boldsymbol{C}^*$,各分量独立且随机选自 $\mathbb{Z}_T$ (Game_3中完成转换),挑战密文中的 ψ^* 随机选自 $\mathbb{QR}_P$,与 M_b 完全独立(Game_5 中完成转换). 因此,在 Game_5 中,攻击者 $\mathfrak{A}$ 所看到的挑战密文 CT^* 已完全随机,和挑战者 $\mathfrak{C}$ 选择的加密明文 M_b 已经完全独立. 所以,$\Pr[E_5]=1/2$.

综上所述,定理得证. 证毕.

效率分析:定理 4 证明了本节的抗泄露 PKE 方案为辅助输入模型下 CCA 安全. 辅助输入模型和泄露受限模型不同之处在于,即使攻击者拥有的不可逆辅助输入函数能够在信息论意义上完全泄露密钥,攻击者也不能恢复密钥信息. 因此,抗辅助输入的 PKE 方案不存在密钥泄露比值这个衡量标准. 目前尚无辅助输入模型下 CCA 安全的 PKE 可于本节方案相比较,在表 1 中,我们将本节方案与目前 2 个泄露受限模型下基于 DDH 问题,CCA 安全的 PKE 方案[6-7]作效率比较. 我们假定在阶为 q 的群 G 中元素会被编码成长度为 $\log q$ 的比特串.

表 1 效率比较

方案名	密钥长度/bit	密文长度/bit
NS09[6]	$6\log q'$	$3\log q$
LZSS[7]	$4\log q'$	$3\log q$
本节方案	m	$(m+2)\log T+\log\lvert\mathfrak{R}_{\mathrm{CH}}\rvert$

表 1 中的 q',q 都表示群的阶,根据文献[11]中的分析,方案 NS09[6] 和 LZSS[7] 如果要获得较高的密钥泄露比值,则需要大幅提高群的阶,那么也会相应增大密钥长度和密文长度. 而本节方案的密钥长度和密文长度则与辅助输入函数的求逆成功概率 ε 以及二次剩余群的阶 T 相关.

5 结 论

辅助输入模型是弹性泄露密码学中一种较强的泄露模型,它允许攻击者拥有一类不可逆的辅助输入函数去模拟各种泄露情形,即使私钥在信息论意义上被完全泄露,从辅助输入函数值恢复私钥依然不可能. 我们提出了一种抗辅助输入 CCA 安全的公钥加密方案,在构造中使用了一次泄露过滤函数去认证隐藏消息的密钥. 我们的一次泄露过滤函数采用了唯一泄露过滤函数加卡梅隆哈希函数的构造方式,当工作在单射模式时,它是个单射函数,当 CCA 安全证明中需要切换到泄露模式时,它仅泄露 $\log p$ 比特的私钥信息. 因此,攻击者对私钥依然存

① u 随机取自 $\mathbb{Z}_T$.

在很大的不确定性，从而其查询非法的密文会被挑战者以高概率拒绝. 目前提出的抗辅助输入的身份基加密方案(IBE)依然是 CPA 安全的，如何利用一次泄露过滤函数实现 CCA 安全的抗辅助输入 IBE 方案依然是一个公开问题.

参 考 文 献

[1] Dziembowski S, Pietrzak K. Leakage-resilient cryptography//Proceedings of the FOCS 2008. Philadelphia, USA, 2008: 293-302

[2] Faust S, Kiltz E, Pietrzak K, Rothblum G N. Leakage-resilient signatures//Proceedings of the TCC 2010. Zurich, Switzerland, 2010: 343-360

[3] Alwen J, Dodis Y, Naor M, et al. Public-key encryption in the bounded-retrieval model//Proceedings of the EUROCRYPT 2010, Riviera, France, 2010: 113-134

[4] Alwen J, Dodis Y, Wichs D. Leakage-resilient public-key cryptography in the bounded-retrieval model//Proceedings of the CRYPTO 2009. Santa Barbara, USA, 2009: 36-54

[5] Di Crescenzo D, Lipton R J, Wallsh S. Perfectly secure password protocols in the bounded retrieval model//Proceedings of the TCC 2006. Manhattan, USA, 2006: 225-244

[6] Naor M, Segev G. Public-key cryptosystems resilient to key leakage//Proceedings of the CRYPTO 2009. Santa Barbara, USA, 2009: 18-35

[7] Li S, Zhang F, Sun Y, Shen L. A new variant of the cramer-shoup leakageresilient public key encryption//Proceedings of the INCoS 2012. Bucharest, Romania, 2012: 342-346

[8] Dodis Y, Haralambiev K, Lopez-Alt A, Wichs D. Cryptography against continuous memory attacks//Proceedings of the FOCS 2010. Las Vegas, USA, 2010: 511-520

[9] Lewko A, Rouselakis Y, Waters B. Achieving leakage resilience through dual system encryption//Proceedings of the TCC 2011. Rhode Island, USA, 2011: 70-88

[10] Zhang Mingwu, Shi Wei, Wang Chunzhi, et al. Leakage-resilient attribute-based encryption with fast decryption: Models, analysis and constructions//Proceedings of the ISPEC 2013. Lanzhou, China, 2013: 75-90

[11] Dodis Y, Goldwasser S, Kalai Y T, et al. Public key encryption schemes with auxiliary inputs//Proceedings of the TCC 2010. Zurich, Switzerland, 2010: 361-381

[12] Yuen T H, Chow S S M, Zhang Y, Yiu S M. Identity-based encryption resilient to continual auxiliary leakage//Proceedings of the EUROCRYPT 2012. Cambridge, UK, 2012: 117-134

[13] Qin Baodong, Liu Shengli. Leakage-resilient chosen-ciphertext secure public-key encryption from hash proof system and one-time lossy filter//Proceedings of the ASIACRYPT (2) 2013. Bangalore, India, 2013: 381-400

[14] Hofheinz D. Circular chosen-ciphertext security with compact ciphertexts//Proceedings of the EUROCRYPT 2013. Athens, Greece, 2013: 520-536

[15] Naor M, Segev G. Public-key cryptosystems resilient to key leakage. SIAM Journal on Computing, 2012, 41(4): 772-814

[16] Goldreich O, Levin L A. A hard-core predicate for all one-way functions//Proceedings of the STOC 1989. Seattle, USA, 1989: 25-32

[17] Qin Baodong, Liu Shengli. Leakage-flexible CCA-secure public-key encryption: Simple construction and free of pairing //Proceedings of the Public Key Cryptography 2014. Buenos Aires, Argentina, 2014: 19-36

[18] Krawczyk H, Rabin T. Chameleon signatures//Proceedings of the NDSS 2000. San Diego, USA, 2000: 1-8

[19] Naor M, Reingold O. Number-theoretic constructions of efficient pseudo-random functions. Journal of the ACM, 2004, 51(2): 231-262

[20] Brakerski Z, Goldwasser S. Circular and leakage resilient public-key encryption under subgroup indistinguishability//Proceedings of the CRYPTO 2010. Santa Barbara, USA, 2010: 1-20

WANG Zhi-Wei, born in 1976, Ph.D., associate professor. His research interests include digital signatures, provable security, cryptographic protocols and network and cloud security.

LI Dao-Feng, born in 1974, Ph. D., associate professor. His research interests include digital signatures, network security, cryptographic protocols.

ZHANG Wei, born in 1973, Ph. D., professor. His research interests include network security, cryptographic protocols.

CHEN Wei, born in 1979, Ph.D., professor. His research interests include network security and cloud security.

Background

In practice, many cryptosystems are difficult to avoid the side-channel attacks, which allow attackers to learn partial information about secret by observing physical properties of a cryptographic execution such as timing, power assumption, temperature, radiation, etc. A new notion called "leakage resilient cryptography" has been proposed, which has led to construction of many cryptographic primitives which can be proved secure even against adversaries who can obtain partial information of secret keys and other initial state. Leakage resilience has been studied in many previous works under a variety of leakage models. Auxiliary input model is a very strong model among these models.

Auxiliary input model is developed from the relative leakage model, which allow any uninvertible function f that no PPT adversary can compute the actual pre-image with non-negligible probability. That is to say, although such a function information-theoretically reveals the entire secret key SK, it still computationally infeasible to recover SK from $f(SK)$. If an encryption scheme that is secure w. r. t. any auxiliary input, then user's secret and public key pair can be used for multiple tasks. Dodis et al. firstly introduced the notion of auxiliary input, and proposed the public key encryption schemes in this model. Yuen et al. proposed the first IBE scheme that is proved secure even when the adversary is equipped with auxiliary input.

However, all these schemes with auxiliary input are chosen plaintext attacks (CPA) secure. In the proof of CPA secure, the attacker cannot make the decryption queries. However, the attacker can obtain many ciphertext/plaintext pairs to recover the messages or keys in practical. Obviously, schemes resist the chosen ciphertexts attacks (CCA secure) is much better than CPA secure schemes, and how to construct the CCA secure PKE scheme with auxiliary input is a great challenge.

In this paper, we construct a CCA secure PKE scheme with auxiliary input by using the one-time lossy filter. One-time lossy filter is a new technical tool developed from lossy algebraic filter, which is a good solution for the CCA security. We proved our scheme that it is CCA secure with auxiliary input (AI-CCA) by using the properties of one-time lossy filter. This is the first PKE scheme with AI-CCA secure.

This research is supported by the National Natural Science Foundation of China under Grant Nos. 61373006, 61202353, 61272422.