抗(持续)辅助输入 CCA 安全的 PKE 构造方案的分析及改进

李素娟[1)] 张明武[2)] 张福泰[3)]

[1)](南京工业大学数理科学学院 南京 211800)

[2)](湖北工业大学计算机学院 武汉 430068)

[3)](南京师范大学计算机科学与技术学院 南京 210023)

摘 要 抗辅助输入适应性选择密文攻击(CCA)安全的公钥加密(PKE)方案是公钥密码体制中一个比较重要的研究课题.目前已有的抗辅助输入公钥加密方案都是选择明文攻击(CPA)安全.在构造抗辅助输入 CCA 安全的 PKE 方案中一个比较有意义的尝试是由王志伟等提出的抗辅助输入 CCA 安全的 PKE 构造.该文对该方案进行了安全分析,指出:(1)该方案基于的困难假设是易解的;(2)该方案不满足选择明文攻击安全;(3)该方案的安全证明是不严谨的.在此基础上,该文对该方案进行了改进,并提出了一个新的抗辅助输入 CCA 安全的 PKE 方案,同时给出了严格的安全证明.另外,该文还对改进的方案进行了拓展,首次提出了抗持续辅助输入 CCA 安全的 PKE 方案.

关键词 辅助输入;一次性有损过滤器;选择密文安全;RSI(Refined Subgroup Indistinguishability)假设;扩展 Goldreich-Levin 定理

中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2018.02823

Security Analysis and Improvement of CCA Secure PKE with (Continual) Auxiliary Input

LI Su-Juan[1)] ZHANG Ming-Wu[2)] ZHANG Fu-Tai[3)]

[1)](*School of Mathematical and Physical Science, Nanjing Tech University, Nanjing* 211800)

[2)](*School of Computer Science, University of Hubei Technology, Wuhan* 430068)

[3)](*School of Computer Science and Technology, Nanjing Normal University, Nanjing* 210023)

Abstract Security primitives of the modern cryptography technology has modeled attackers as having only black-box access to the primitives, and ensure that secret keys must be safely stored and internal states are not leaked to the attackers. But these models do not capture the real circumstance where the adversary can achieve traditional information of the secret inner states through the side channel attack. In order to avoid this type of attacks, the researchers provide two remedial measures to resist the attacks. One way is to reinforce the hardware to eliminate the damage of the kind of attack, which we call hardware-based level way; the other way is to design secure algorithms by some mathematical technology in order to reject this kind of attack, which we call algorithm-based level way. The chosen ciphertext attack (CCA) secure public key encryption (PKE) with auxiliary input is an important research topic in the leakage resilient public key cryptosystem. To the best of our knowledge, the auxiliary input model is the strongest model in the security model of leakage resilient attacks during one key existing period. Recently, there

收稿日期:2016-09-20;在线出版日期:2017-07-04.本课题得到国家自然科学基金(61702259,61802242,61672289,61672010)、江苏省政府留学基金、江苏省博士后基金(1601008A)、江苏省高校自然科学基金(16KJB520018)、江苏省高校哲学社科基金项目(2017SJB0201)资助.**李素娟**(通信作者),女,1978 年生,博士,副教授,中国计算机学会(CCF)会员,主要研究方向为信息安全和密码学.E-mail:lisujuan1978@126.com.**张明武**,男,1970 年生,博士,教授,中国计算机学会(CCF)高级会员,主要研究领域为应用密码技术、安全隐私保护和网络安全协议.**张福泰**,男,1965 年生,博士,教授,主要研究领域为网络安全与密码学.

appear many public key encryption schemes or Identity-based encryption (IBE) schemes against auxiliary input leakage in the literature. However, almost all PKE and IBE schemes with auxiliary input are proved to be chosen plaintext attack (CPA) secure. Compared with CCA secure, as we all know, CPA secure is on a weaker security level. One of the interesting attempts to construct CCA secure public key encryption scheme with auxiliary input is due to Wang et al.'s scheme. However, through our cryptanalysis on their scheme, we find out some mistakes in their scheme. In this paper, we point out these mistakes and try our best to correct these mistakes. There are three mistakes in their scheme. The first one is that the hardness assumption which Wang et al.'s scheme mainly based on is not a difficult hardness assumption in itself. The second one is the security of Wang et al.'s scheme does not meet the basic requirements of the CPA secure public key encryption scheme. Therefore, it is impossible that their scheme can arrive at the much stronger security requirement—CCA secure. The last one is that the security proof of Wang et al.'s scheme is not rigorous. Based on the above analysis, we present an improved CCA secure public key encryption scheme against auxiliary input leakage. In the proceeding, we mainly borrow the ideas of both Boneh et al.'s public key encryption scheme of CRYPTO'08 and Qin et al.'s public key encryption scheme of PKC'14. And with the help of the extended Goldreich-Levin theorem, we give a rigorous security proof of the improved scheme. According to our knowledge, there is not any public key encryption scheme which can resist the continual auxiliary input leakage up to now. By means of the algebraic kernel technology, based on the improved scheme, we also provide the first CCA secure public key encryption scheme against continual auxiliary input leakage in the floppy model.

Keywords auxiliary input; one-time lossy filter; chosen ciphertext secure; the Refined Subgroup Indistinguishability assumption; the extended Goldreich-Levin theorem

1 引 言

在密码世界里,一个系统的任何物理实现都会泄漏系统内部的一些信息.在侧信道攻击中,攻击者通过密码系统的物理实现过程中所泄漏的如计算时间、能量消耗、电磁辐射、噪声、热量辐射等可以获取系统的部分内部秘密状态.文献[1]已经指出了计时攻击对经典的 Diffie-Hellman 密钥交换协议、RSA 加解密、DSS 等密码系统的实现所带来的严重安全威胁;冷启动攻击[2]是近些年发现的一类新的安全泄漏攻击.利用这种攻击,攻击者可以从保存过秘密信息的物理设备,在其刚刚关闭的短时间内获取其内存中的部分秘密信息.文献[2-3]探索了如何利用冷启动攻击来恢复出经典的 DES、AES、RSA 算法的安全密钥.我们把所有企图获取密码系统部分内部秘密状态的攻击统称为密钥泄漏攻击.

目前,在单个密钥的一个有效运行周期内,国内外学者对密钥泄漏攻击建立了 3 种安全模型(如图 1):只有计算泄漏模型、有界泄漏模型和辅助输入模型.

(1) 只有计算泄漏模型[4](Only Computation Leaks Information,OCLI).顾名思义,在该模型中只有参与计算的部分会发生泄漏,没有参与计算的则不会发生泄漏.

(2) 有界(有限)泄漏模型[5](Bounded Leakage Model,BLM),有时又称为相对泄漏模型(Relative Leakage Model,RLM).在这种模型下,攻击者需要事先设定一个泄漏参数值 l,但是 l 必须小于密钥长度 $|sk|$.攻击者只可以获得关于密钥 sk 至多 l 比特长度(或者信息熵).通常情况下,泄漏参数值 l 可以是比特信息,也可以是熵信息.

(3) 辅助输入模型[6](Auxiliary Input Model,AIM).这种模型是比前两种模型更强的安全模型,它是有界泄漏模型的一种延伸.在该模型下,我们允许攻击者拥有一类不可逆的辅助函数 f,将这类不可逆的辅助函数作用于密钥 sk,使攻击者获得 $f(sk)$ 的函数值信息,从而来模拟密钥 sk 的各种泄漏情形.但前提条件是,无论通过这些泄漏函数泄漏的信息有多少(哪怕是信息论意义上可以完全泄漏密钥),攻击者都无法恢复出用户密钥 sk.

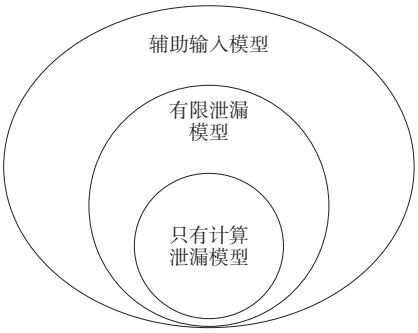


图 1　单个密钥周期内的密钥泄漏模型

如果说前三种分类是从空间角度将密钥泄漏攻击进行了分类，另一方面从时间角度，国内外学者将密钥单个周期内的泄漏模型又进一步拓展至连续多个密钥周期的泄漏模型[7-8]，也即持续泄漏模型(Continual Leakage Model，CLM)．显然，由于可以持续泄漏有关密钥的无限信息，再结合单个周期内最强的辅助输入模型，因而持续辅助输入模型(Continual Auxiliary Input Model，CAIM)是目前所有的泄漏安全模型中安全性最强的安全模型．在这种模型中，通常需要一个可信的抗泄漏的硬件装置来进行密钥的持续更新，并及时销毁更新过的密钥，而在加密的其他阶段，尤其是实际发生密钥泄漏的解密阶段则无需这种硬件装置．文献[9]将在这种状态下的持续泄漏模型又称为柔性模型(the Floppy Model)．

抗密钥泄漏的公钥加密方案是研究允许用户私钥部分泄漏的情况下，方案仍然能够保证安全性．这种安全性又分为抗泄漏选择明文攻击安全(Leakage Resilient Chosen Plaintext Attack Secure，LR-CPA-Secure)和抗泄漏选择密文攻击安全(Leakage Resilient Chosen Ciphertext Attack Secure，LR-CPA-Secure)．选择密文安全比选择明文安全安全性更强，意即概率多项式时间(Probability Polynomial Time，PPT)攻击者不但可以进行密钥泄漏询问，还可以进行密文的解密询问；在挑战密文生成后，除了对挑战密文不能进行解密询问外，仍可以进行其它密文的解密询问，但当挑战密文生成后，对密钥的泄漏询问必须中止．

自从 Naor 和 Segev[10] 构造出第一篇抗泄漏选择密文安全的公钥加密方案后，研究者们对构造高效的和高密钥泄漏率(密钥泄漏长度与密钥长的比率)的抗泄漏选择密文安全的公钥加密方案进行了不断的尝试，并产生了比较好的研究成果[11-21]．

在辅助输入模型下，设计出 CCA 安全的公钥加密(Public Key Encryption，PKE)方案是一个比较有意义的研究方向，其中一个比较有意义的尝试是由王志伟等提出的抗辅助输入 CCA 安全的 PKE 构造[22]．本文对该方案进行了安全分析，认为该方案是不安全的．所以，有必要重新设计一种抗辅助输入 CCA 安全的 PKE 方案．另一方面，本文根据改进方案的代数结构，构造出了首个柔性模型下抗持续辅助输入 CCA 安全的 PKE 方案．

本文的主要贡献在于：

(1) 指出文献[22]中设计的抗辅助输入 CCA 安全的 PKE 方案是不安全的．主要从 3 个方面说明：

(a) 该方案基于的困难假设是易解的；

(b) 该方案不能满足 IND-CPA 安全性；

(c) 该方案的安全证明是不严谨的．

(2) 利用合数阶群上的一次性有损过滤器[13]，借助 BHHO 方案[23] 构造了一个新的 CCA 安全的抗辅助输入的 PKE 方案；

(3) 利用扩展 Goldreich-Levin 定理结合混合证明技术严格给出新方案的安全性证明；

(4) 利用代数中的核技术在改进方案的基础上进行了拓展，首次在柔性模型下提出了抗持续辅助输入 CCA 安全的 PKE 方案．

本文结构如下：

第 2 节给出构造方案所需要的预备知识，如：困难假设、扩展 Goldreich-Levin 定理；第 3 节介绍抗辅助输入 CCA 安全的 PKE 方案的安全模型；第 4 节，借助 Chameleon 哈希函数在合数阶群下构造一个具体的基于 RSI 假设的一次性有损过滤器；第 5 节回顾文献[22]中方案的构造，并进行安全性分析；在此基础上，第 6 节给出一个新的抗辅助输入 CCA 安全的 PKE 方案，并给出严格的安全证明；第 7 节对改进的方案进行拓展，构造一个抗持续辅助输入 CCA 安全的 PKE 方案；最后一节给出结论和后期可以进一步开展的工作．

2　预备知识

2.1　符号表示

(1) 记符号$[n]$表示集合$\{1,2,\cdots,n\}$；

(2) 1^k表示 k 个 1 构成的字符串；

(3) 若 t 是个字符串，则$|t|$表示其长度；

(4) $\mathrm{negl}(k)$表示任意可忽略的函数；

(5) 向量用黑体 $\boldsymbol{r},\boldsymbol{s}$ 等表示；

(6) 符号$\langle \boldsymbol{r},\boldsymbol{s}\rangle$表示向量 $\boldsymbol{r}$ 与向量 $\boldsymbol{s}$ 的内积．

2.2　困难假设

2.2.1　DDH 假设

设$\mathcal{G}(1^k)\rightarrow(G,q,g)$，其中 k 是安全参数，群 G

是一个生成元为 g 的素数 q 阶循环群. DDH(Decisional Diffie-Hellman)假设：

对任意概率多项式时间(PPT)算法 $\mathcal{A}$，区分两个数组 (G,g_1,g_2,g_1^r,g_2^r) 和 $(G,g_1,g_2,g_1^{r_1},g_2^{r_2})$ 的优势 $\mathrm{Adv}_{G,\mathcal{A}}^{\mathrm{DDH}}(k):=|\Pr[\mathcal{A}(G,g_1,g_2,g_1^r,g_2^r)=1]-\Pr[\mathcal{A}(G,g_1,g_2,g_1^{r_1},g_2^{r_2})=1]|$ 是可以忽略的，其中 $r,r_1,r_2\in Z_q$，$g_1,g_2\in G$.

后来，Boneh 等人[23]将标准的 DDH 假设进行了拓展，也即对任意概率多项式时间(PPT)算法 $\mathcal{A}$，区分两个数组 $\mathcal{A}(G,g_1,g_2,\cdots,g_m,g_1^r,g_2^r,\cdots,g_m^r)$ 和 $(G,g_1,g_2,\cdots,g_m,g_1^{r_1},g_2^{r_2},\cdots,g_m^{r_m})$ 的优势

$$\mathrm{Adv}_{G,\mathcal{A}}^{\mathrm{DDH}}(k):=$$
$$|\Pr[\mathcal{A}(G,g_1,g_2,\cdots,g_m,g_1^r,g_2^r,\cdots,g_m^r)=1]-$$
$$\Pr[\mathcal{A}(G,g_1,g_2,\cdots,g_m,g_1^{r_1},g_2^{r_2},\cdots,g_m^{r_m})=1]|$$

是可以忽略的，其中 $r,r_i\in Z_q$，$g_i\in G(i,j\in[m])$.

2.2.2 RSI 假设

设有限可交换乘法群 G 是两个阶分别为素数 t_1，t_2 的循环群的直积，即 $G=G_{t_1}\times G_{t_2}$. 若 $1/t_i=\mathrm{negl}(k)$，RSI(Refined Subgroup Indistinguishability)假设[13]即对 PPT 攻击者 $\mathcal{A}$，

$$\mathrm{Adv}_{G,\mathcal{A}}^{\mathrm{RSI}}(k)=|\Pr[x\in G:\mathcal{A}(1^k,x)=1]-\Pr[x\in G_{t_i}:\mathcal{A}(1^k,x)=1]|=\mathrm{negl}(k),(i=1,2).$$

若令 $T=t_1t_2$，g,h 分别是循环群 G_{t_1}，G_{t_2} 的生成元，则在合数阶群 G 上

$$\Pr[x\in G_{t_1}:\mathcal{A}(1^k,x)=1]-\Pr[x\in G\backslash G_{t_1}:\mathcal{A}(1^k,x)=1]|\leq 2\cdot\mathrm{Adv}_{G,\mathcal{A}}^{\mathrm{RSI}}(k);$$

$$\Pr[x\in G_{t_1}:\mathcal{A}(1^k,x)=1]-\Pr[x\in G_{t_1}:\mathcal{A}(1^k,x\cdot h)=1]|\leq 2\cdot\mathrm{Adv}_{G,\mathcal{A}}^{\mathrm{RSI}}(k).$$

2.3 扩展 Goldreich-Levin 定理

这里只介绍本文中用到的由 Dodis 等人[6]证明的扩展 Goldreich-Levin 定理，与 Goldreich-Levin 定理[24]仅在二元域上成立不同，Dodis 等人将二元域扩展到了任意素数域上.

定理 1. q 是大素数，H 是 GF(q)的任意子群，设 $f:H^n\to\{0,1\}^*$ 是任意随机函数. 若存在一个区分器 $\mathcal{D}$ 满足 $|\Pr[\mathcal{D}(f(\boldsymbol{s}),\boldsymbol{t},\langle\boldsymbol{s},\boldsymbol{t}\rangle)=1]-\Pr[\mathcal{D}(f(\boldsymbol{s}),\boldsymbol{t},z)=1]|\geq\varepsilon$，其中 $\boldsymbol{s}\leftarrow H^n$，$\boldsymbol{t}\leftarrow\mathrm{GF}(q)^n$，$z\leftarrow\mathrm{GF}(q)$，且 $\langle\boldsymbol{s},\boldsymbol{t}\rangle$ 是在 GF(q)上的内积运算. 则存在一个求逆算法在时间 $\mathrm{poly}(n,1/\varepsilon)$ 内使得

$$\Pr[\mathcal{A}(f(\boldsymbol{s}))=\boldsymbol{s}]\geq\frac{\varepsilon^3}{512\cdot n\cdot q^2}.$$

特别地，当向量 $\boldsymbol{t}$ 为指数向量 $\boldsymbol{g}^r$ 时，Wee 在文献[25]第 4 节中指出，该结论仍然成立.

3 抗辅助输入 CCA 安全的 PKE 的安全模型

辅助输入模型是一类比抗泄漏模型更强的安全模型. 在抗泄漏模型中，攻击者仅可以获得有关密钥的有限的比特信息或者信息熵；而在辅助输入模型中，将泄漏信息由信息论意义升级为可计算角度，意即攻击者可以获得有关私钥的任何辅助信息，可是无论获得多少相关信息，攻击者都不可能求得私钥.

记公钥加密算法为 $\mathrm{PKE}=(Gen,Enc,Dec)$，$PK,SK$ 分别为公钥、私钥空间，M 是消息空间. 设 $\mathcal{F}=\{f_k:SK\times PK\to\{0,1\}^*\}$①为任意不可逆函数集合，给定关于私钥和公钥的相关信息 $f_k(sk,pk)$，求出 sk 是不可行的，意即该函数族在多项式时间内可求逆的概率几乎是可以忽略的.

借助 Dodis 等人[6]抗辅助输入 IND-CPA 安全的安全模型，再进行适当的拓展，我们可以得到抗辅助输入 CCA 安全的 PKE 的安全模型.

定义 1. 公钥加密方案为 $\mathrm{PKE}=(Gen,Enc,Dec)$ 是抗辅助输入 CCA 安全的，若对任意 PPT 的攻击者 $\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)$，对 $\forall f\in\mathcal{F}$，优势 $\mathrm{Adv}_{\mathrm{PKE},\mathcal{A}}^{\mathrm{AI\text{-}CCA}}(k):=|\Pr[\mathrm{Exp}_{\mathrm{PKE},\mathrm{A}}^{\mathrm{AI\text{-}CCA}}(k,0)=1]-\Pr[\mathrm{Exp}_{\mathrm{PKE},\mathcal{A}}^{\mathrm{AI\text{-}CCA}}(k,1)=1]|$ 是可以忽略的，其中 $\mathrm{Exp}_{\mathrm{PKE},\mathrm{A}}^{\mathrm{AI\text{-}CCA}}(k,\beta)$ 定义为：

(1) $(SK,PK)\leftarrow Gen(1^k)$；

(2) $(M_0,M_1,\mathrm{st})\leftarrow\mathcal{A}_1^{f(SK,PK),Dec(SK,\cdot)}(PK)$，s.t. $|M_0|=|M_1|$；

(3) $C\leftarrow Enc_{pk}(M_\beta)$；

(4) $\beta'\leftarrow\mathcal{A}_2^{Dec\neq C(SK,\cdot)}(C,\mathrm{st})$；

(5) 输出 β'.

4 合数阶群上构造一次性有损过滤器

4.1 一次性有损过滤器

一次性有损过滤器(One-time Lossy Filter，OTLF)是 Qin 等人[12]为了证明抗泄漏 PKE 方案的 CCA 安全性提出的新概念. 和有损陷门函数(Lossy Trapdoor Functions，LTFs)一样，一次性有损过滤器也有两种模式：单射模式和有损模式.

① 就攻击目标而言，不可逆函数与单向函数的区别在于[6]：对于前者，攻击者给定 $f_k(sk,pk)$，攻击者力图可以求出原像 sk；而对于后者，攻击者只需要输出一个 sk'，使得 $f_k(sk,pk)=f_k(sk',pk)$. 因此，当函数 f_k 无法进行输出求逆时，该函数便是不可逆函数，而非单向函数. Dodis 等人在文献[8]中指出，若 k 代表私钥 sk 的长度，则这类辅助输入不可逆函数至多以概率 2^{-k^ξ} 可求逆(对任意 $\xi>0$). 显然，当 k 越大，这类函数可求逆的概率就越低.

一次性有损过滤器(Dom,l)-OTLF 由以下 3 个算法构成[12]：

(1) 密钥生成算法(OTLF.Gen). 该算法生成一对公私钥对(F_{pk},F_{td}).

(a) 公钥 F_{pk} 定义了一个标记空间 $\mathcal{T}=\{0,1\}^*\times\mathcal{T}_c=\{t=(t_a,t_c)\mid t_a\in\{0,1\}^*$ 是辅助标记，$t_c\in\mathcal{T}_c$ 是核心标记$\}$. 同时，标记空间 $\mathcal{T}$ 也是由单射标记空间 $\mathcal{T}_{inj}$ 和有损标记空间 $\mathcal{T}_{loss}$ 形成的完备空间，即

$$\mathcal{T}=\mathcal{T}_{inj}\cup\mathcal{T}_{loss},\text{且}\mathcal{T}_{inj}\cap\mathcal{T}_{loss}=\varnothing.$$

(b) F_{td} 是用来计算有损标记的陷门.

(2) 函数计算算法(OTLF.Eval). 该算法输入公钥 F_{pk}，标记 t 和变量 $x\in Dom$，输出 $\mathrm{OTLF}_{F_{pk},t}(x)$. 在有损标记 $t=(t_a,t_c)$ 下，函数 $\mathrm{OTLF}_{F_{pk},t}(x)\in\{0,1\}^l$ 就是有损模式；此时，$|Dom|-l$ 称为像的损失(lossiness).

(3) 有损标记生成(OTLF.LTag). 该算法输入陷门 F_{td}，辅助标记 t_a，输出核心标记 t_c，其中 $t=(t_a,t_c)$ 是有损标记.

一次性有损过滤器(Dom,l)-OTLF 具有以下两个性质：

(1) 不可区分性(Indistinguishability). 对任意的 PPT 攻击者 $\mathcal{A}$ 都难以从随机标记空间中区分出有损标记，也即攻击者在以下区分过程中的优势是可以忽略的，即

$$\mathrm{Adv}^{\mathrm{IND}}_{\mathrm{OTLF},\mathcal{A}}(k):=|\Pr[\mathcal{A}(F_{pk},(t_a,t_c^{(0)}))=1]-\Pr[\mathcal{A}(F_{pk},(t_a,t_c^{(1)}))=1]|\leq\mathrm{negl}(k),$$

其中 $t_a\in\mathcal{A}(F_{pk})$，$t_c^{(0)}\in\mathrm{OTLF.LTag}(F_{td},t_a)$ 并且 $t_c^{(1)}\in_R\mathcal{T}_c$.

(2) 躲闪性(Evasiveness). 对任意 PPT 的攻击者 $\mathcal{A}$，给定一个有损标记 $t=(t_a,t_c)$ 很难生成一个非单射标记 $t'=(t'_a,t'_c)$，意即

$$\mathrm{Adv}^{\mathrm{EVA}}_{\mathrm{OTLF},\mathcal{A}}(k):=\Pr[(t'_a,t'_c)\neq(t_a,t_c)\wedge(t'_a,t'_c)\in\mathcal{T}\setminus\mathcal{T}_{inj}\mid t_a\leftarrow\mathcal{A}(F_{pk}),t_c\leftarrow\mathrm{OTLF.LTag}(F_{td},t_a);(t'_a,t'_c)\leftarrow\mathcal{A}(F_{pk},(t_a,t_c))]\leq\mathrm{negl}(k).$$

4.2　Chameleon 哈希函数

Chameleon 哈希函数是一类特殊的哈希函数，和一般的哈希函数一样具有抗碰撞性，但是，在已知陷门情况下，是可以找到碰撞的. 它主要由 3 个算法构成：

(1) 密钥生成算法(CH.Gen). 该算法生成一对哈希函数的公私钥对(pk_{CH},td_{CH}).

(2) 函数计算算法(CH.Eval). 该算法输入公钥 pk_{CH} 和随机数 $r_{CH}\leftarrow R_{CH}$，将变量 $x\in\{0,1\}^*$ 映射到 $y\in\mathcal{Y}$.

(3) 碰撞生成算法(CH.Equiv). 该算法输入陷门 td_{CH} 和 $(x,r_{CH};x')$. 在陷门 td_{CH} 的帮助下，已知 (x,r_{CH}) 和 x'，可找到 (x,r_{CH}) 的碰撞 (x',r'_{CH})，有 $\mathrm{CH.Eval}(pk_{CH},x,r_{CH})=\mathrm{CH.Eval}(pk_{CH},x',r'_{CH})$.

在未知陷门的前提下，该函数具有抗碰撞性. 即对任意 PPT 攻击者 $\mathcal{A}$，很难找到 $(x,r_{CH})\neq(x',r'_{CH})$，使得哈希函数值相等，其找到碰撞的优势

$$\mathrm{Adv}^{\mathrm{CR}}_{\mathrm{CH},\mathcal{A}}(k):=\Pr[(x,r_{CH})\neq(x',r'_{CH})\wedge\mathrm{CH.Eval}(pk_{CH},x,r_{CH})=\mathrm{CH.Eval}(pk_{CH},x',r'_{CH}):(x,r_{CH};x',r'_{CH})\leftarrow\mathcal{A}(pk_{CH})]\leq\mathrm{negl}(k).$$

4.3　合数阶群上构造一次性有损过滤器

借助 Qin 等人[13]利用 Chameleon 函数构造合数阶群上构造一次性有损过滤器的方法，借助 RSI 假设在大整数因子分解困难假设的基础上我们构造出适合本方案的具体的一次性有损过滤器如下：

设 $N=2pq+1$，其中 p,q 是大素数. 令 $T=pq$，则二次剩余群 QR_N 的阶为 T，且是两个阶分别为素数 p,q 的群 G_p 和 G_q 的直积，即 $QR_N=G_p\times G_q$，设两个素数阶群的生成元分别为 g,h. 显然，若 T 难分解，则 RSI 假设在群 QR_N 上是成立的. 在群 QR_N 上，结合 Chameleon 哈希函数 CH=(CH.Gen,CH.Eval,CH.Equiv)给出一个一次性有损陷门函数$(Z_N,\log p)$-OTLF，其结构如下：

(1) 密钥生成算法(OTLF.Gen)，具体步骤如下：

(a) 运行 $\mathrm{CH.Gen}(1^k)$ 算法得到 Chameleon 哈希函数的公私钥对(pk_{CH},td_{CH})；

(b) 随机选择标记 $(t_a^*,t_c^*)\in\{0,1\}^*\times R_{CH}$，计算 $\beta^*=\mathrm{CH.Eval}(pk_{CH},t_a^*,t_c^*)$；

(c) 随机选择 $u\in\mathbb{Z}_p^*$，计算 $E=g^uh^{-\beta^*}$；

(d) 标记空间 $\mathcal{T}=\{0,1\}^*\times R_{CH}=\mathcal{T}_{inj}\cup\mathcal{T}_{loss}$，其中单射标记空间 $\mathcal{T}_{inj}=\{(t_a,t_c)\mid(t_a,t_c)\in\mathcal{T}\wedge\mathrm{CH.Eval}(pk_{CH},t_a,t_c)=\beta^*\}$；有损标记空间 $\mathcal{T}_{loss}=\{(t_a,t_c)\mid(t_a,t_c)\in\mathcal{T}\wedge\mathrm{CH.Eval}(pk_{CH},t_a,t_c)\neq\beta^*\}$.

(e) 输出公钥 F_{pk} 和陷门 F_{td}，分别为

$$F_{pk}=(QR_N,T,g,h,E,pk_{CH}),$$
$$F_{td}=(td_{CH},(t_a^*,t_c^*)).$$

(2) 函数计算算法(OTLF.Eval)，具体步骤如下：

(a) 给定标记 $t=(t_a,t_c)$ 和变量 $x\in Z_N$，计算 $\beta=\mathrm{CH.Eval}(pk_{CH},t_a,t_c)$；

(b) 计算

$$y=(E\cdot h^{\beta})^x=(g^uh^{-\beta^*}\cdot h^{\beta})^x=(g^uh^{\beta-\beta^*})^x.$$

(3) 有损标记生成算法(OTLF.LTag). 对辅助标记 t_a，利用陷门 $F_{td}=(td_{CH},(t_a^*,t_c^*))$ 输出核心标记 $t_c=\mathrm{CH.Equiv}(td_{CH},(t_a^*,t_c^*),t_a)$，使得 $t=(t_a,t_c)$ 是有损标记.

定理 2. 在 T 难分解的前提下，基于合数阶群 QR_N 构造的 OTLF 是一个 $(Z_N, \log p)$ 的一次性有损过滤器.

证明.

(1) 有损性. 对函数 $y=(g^u h^{\beta-\beta^*})^x$，当 β 是单射标记，即 $\beta\neq\beta^*$ 时，该函数是群 QR_N 上的单射函数；当 β 是有损标记，即 $\beta=\beta^*$ 时，$y=(g^u)^x\in G_p$，故原像损失至少 $\log q$ 比特信息.

(2) 不可区分性. 因为标记 $(t_a^*, t_c^*)\in\{0,1\}^*\times R_{CH}$ 是随机选取的，则 β^* 也是随机的；又 $x\in Z_N$ 且随机数 $u\in Z_T$，所以，$(g^u)^x$ 是群 G_p 上的均匀分布，$(g^u h^{\beta-\beta^*})^x$ 是 QR_N 上的均匀分布. 根据在 T 难分解的前提下，合数阶群 $QR_N=G_p\times G_q$ 上 RSI 假设成立，所以有损模式下的函数 $y=(g^u)^x$ 与单射模式下的函数 $y=(g^u h^{\beta-\beta^*})^x$ 不可区分，也即从随机标记空间中分辨出有损标记是困难的，有

$$\mathrm{Adv}^{\mathrm{IND}}_{\mathrm{OTLF},\mathcal{A}}(k)\leq 2\mathrm{Adv}^{\mathrm{RSI}}_{\mathrm{QR}_N,\mathcal{B}}(k).$$

(3) 躲闪性. 显然，一次性有损过滤器的躲闪性取决于 Chameleon 哈希函数的抗碰撞性，因此 $\mathrm{Adv}^{\mathrm{EVA}}_{\mathrm{OTLF},\mathcal{A}}(k)=\mathrm{Adv}^{\mathrm{CR}}_{\mathrm{CH},\mathcal{B}}(k)$. 证毕.

5 文献[22]中方案的回顾和分析

5.1 文献[22]中方案基于的困难假设

在 DDH 假设的基础上，文献[22]中方案认为：若令

$w_1=d\log_g g_1, w_2=d\log_g g_2, \cdots, w_m=d\log_g g_m$，

其中 $w_1, w_2, \cdots, w_m\in Z_q$，DDH 假设中任意概率多项式时间攻击者 $\mathcal{A}$ 胜出的概率 $\mathrm{Adv}^{\mathrm{DDH}}_{\mathrm{G},\mathcal{A}}(k):=|\Pr[\mathcal{A}(w_1, w_2, \cdots, w_m, rw_1, rw_2, \cdots, rw_m)=1]-\Pr[\mathcal{A}(w_1, w_2, \cdots, w_m, r_1w_1, r_2w_2, \cdots, r_mw_m)=1]|$ 是可以忽略的.

5.2 文献[22]中方案描述

该方案包括密钥生成中心，消息的发送方和密文的接受方. 主要包括如下 3 个算法：

(1) 密钥生成算法 $(1^k, \varepsilon)$. 选择至少为 k 比特的大素数，计算 $P=2pq+1$，则 Z_P^* 是阶为 $T=pq$ 的二次剩余群，记为 QR_P. 那么 QR_P 也是两个循环群的直积 $QR_P=G_p\times G_q$. 令 $m=(4\log T)^{1/\varepsilon}$，选择 QR_P 中的生成元 g 以及 $r_1, \cdots, r_m\in Z_N$. 令向量 $\boldsymbol{r}=(r_1, r_2, \cdots, r_m)$，$\boldsymbol{g}=(g^{r_1}, g^{r_2}, \cdots, g^{r_m})$，选择 m 比特的随机串 $\boldsymbol{s}=(s_1, s_2, \cdots, s_m)\in\{0,1\}^m$，再选择随机标记 $(t_a^*, t_c^*)\in\{0,1\}^*\times R_{CH}$ 及具有公私钥对 (pk_{CH}, td_{CH}) 的卡梅隆哈希函数 CH，计算 $\beta^*=\mathrm{CH.Eval}(pk_{CH}, t_a^*, t_c^*)$. 选择 G_p 中的生成元 $\tilde{g}$，G_q 中的生成元 $\tilde{h}$ 以及 $v\in Z_p$，计算 $EK=\tilde{g}^v\tilde{h}^{-\beta^*}$. 公钥为 $PK=(N, g, QR_P, T, \boldsymbol{r}, \boldsymbol{g}, \langle\boldsymbol{r},\boldsymbol{s}\rangle, \tilde{g}, \tilde{h}, EK, pk_{CH})$，私钥为 $SK=\boldsymbol{s}$.

(2) 加密算法 (PK, M). 输入公钥 PK 和明文 $M\in QR_P$，选择 $w\in Z_T$，计算 $K=w\cdot\langle\boldsymbol{r},\boldsymbol{s}\rangle$，$C=w\cdot\boldsymbol{r}$，$\psi=g^K\cdot M$，$\Pi=(EK\cdot\tilde{h}^{\beta})^K$，其中 $\beta=\mathrm{CH.Eval}(pk_{CH}, t_a; t_c)$，辅助标记 $t_a=(C,\psi)$ 随机选择核心标记 $t_c\in R_{CH}$，密文为 $CT=(C,\psi,\Pi,t_c)\in Z_T^m\times QR_P\times QR_P\times R_{CH}$.

(3) 解密算法 (SK, CT). 输入密文 $CT=(C,\psi,\Pi,t_c)$ 及私钥 $SK=\boldsymbol{s}$，计算 $K'=\langle C,\boldsymbol{s}\rangle$ 和 $\Pi'=(EK\cdot\tilde{h}^{\beta})^{K'}$，其中 $\beta=\mathrm{CH.Eval}(pk_{CH}, (C,\psi); t_c)$. 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 $M=\psi/K'$.

5.3 对文献[22]中方案的安全性分析

本节主要从 3 个方面入手，论述了文献[22]中方案安全的脆弱性.

(1) 该方案基于的困难假设是易解的. 针对文献[22]中方案构造的 DDH 假设的等价形式，因为 $w_i, rw_i, r_iw_i\in Z_q$，所以 $r=rw_i/w_i$，$r_i=r_iw_i/w_i$ $(i\in[m])$. 从而区分两个数组 $(w_1, w_2, \cdots, w_m, rw_1, rw_2, \cdots, rw_m)$ 和 $(w_1, w_2, \cdots, w_m, r_1w_1, r_2w_2, \cdots, r_mw_m)$ 的概率是 1. 也即文献[22]中方案基于的困难假设是易解的.

(2) 该方案不满足选择明文攻击(IND-CPA)的安全性. 给定公钥 $PK=(N, g, QR_P, T, \boldsymbol{r}, \boldsymbol{g}, \langle\boldsymbol{r},\boldsymbol{s}\rangle, \tilde{g}, \tilde{h}, EK, pk_{CH})$ 和密文 $CT=(C,\psi,\Pi,t_c)$，因为向量 $\boldsymbol{r}=(r_1, r_2, \cdots, r_m)\in Z_N^m$ 是公开的，已知密文向量 $\boldsymbol{C}=(c_1, c_2, \cdots, c_m)=w\cdot\boldsymbol{r}\in Z_N^m$，故可以计算出常系数 $w=\boldsymbol{C}/\boldsymbol{r}$(即向量 $\boldsymbol{C}$ 和向量 $\boldsymbol{r}$ 成比例). 又因为内积 $\langle\boldsymbol{r},\boldsymbol{s}\rangle$ 公开，从而可以计算出被封装的密钥 $K=w\cdot\langle\boldsymbol{r},\boldsymbol{s}\rangle$，最后可以恢复出明文消息 $M=\psi/g^K$.

(3) 该方案的安全性证明不严谨. 文献[22]构造的抗辅助输入 CCA 安全的 PKE 方案安全的理论基础是由 Dodis 等人[6]证明的扩展 Goldreich-Levin 定理. 该定理是用来描述素数阶有限域 $GF(q)$(其中 q 是素数)上的向量内积 $\langle\boldsymbol{r},\boldsymbol{s}\rangle$ 和素数阶有限域 $GF(q)$ 上任意元素 u 的不可区分属性. 在文献[22]方案的安全证明 Game_5 中，在利用扩展 Goldreich-Levin 定理进行不可区分证明时随机元素 u 是取自非素数阶有限域 Z_T(其中 $T=pq$，p, q 是素数).

6 改进的抗辅助输入 CCA 安全的 PKE 方案

6.1 构造思路

目前，构造抗泄漏的 CCA 安全的 PKE 方案效

率较好的是 Qin 等人[12]提出的利用哈希证明系统(Hash Proof System，HPS)结合 OTLF 的方法，HPS 保证了 PKE 方案的 IND-CPA 安全性，而 OTLF 在提供 IND-CCA 安全性的同时还能够维持 PKE 方案较高的密钥泄漏率. 新的构造方案借助 BHHO 方案的封装密钥的思想(隐含了一个基于 DDH 困难假设的 HPS)保证方案的 IND-CPA 安全，再将封装的密钥作为 OTLF 的输入，将封装密钥的密文和隐藏明文消息的密文作为 OTLF 的辅助标签，从而来验证密文的有效性，使方案达到 IND-CCA 安全.

6.2　改进的方案

(1) 密钥生成算法 PKE.KG$(1^k,\varepsilon)$. 具体步骤如下：

(a) 选择至少为 k 比特的大素数 p,q，计算 $N=2pq+1$，则 Z_N^* 有一个阶为 $T=pq$ 模 N 的二次剩余群，记为 QR_N. 另外，QR_N 也是两个循环群的直积 $QR_N=G_p\times G_q$；

(b) 令 $m=(4\log T)^{1/\varepsilon}$，随机选择向量 $\boldsymbol{r}=(r_1',r_2',\cdots,r_m')\in Z_T^m$，选择 m 维的随机串 $\boldsymbol{s}=(s_1',s_2',\cdots,s_m')\in Z_T^m$；

(c) 选择素数 P 阶群 $G_P(P\geq N)$ 中的一个生成元 g，计算 $g^{\boldsymbol{r}}=(g^{r_1'},\cdots,g^{r_m'})=(g_1,\cdots,g_m)$，$g^{\langle \boldsymbol{r},\boldsymbol{s}\rangle}=g^{\sum_{i=1}^m r_i'\cdot s_i'}=\Pi_{i=1}^m g^{r_i'\cdot s_i'}=\Pi_{i=1}^m g_i^{s_i'}$. $Inj:G_P\rightarrow Z_N$.

(d) 选择随机标记$(t_a^*,t_c^*)\in\{0,1\}^*\times R_{CH}$ 以及具有公私钥对(pk_{CH},td_{CH})的 Chameleon 哈希函数 CH，计算 $\beta^*=$CH.Eval(pk_{CH},t_a^*,t_c^*)；

(e) 选择 G_p 中的生成元 $\tilde{g}$，G_q 中的生成元 $\tilde{h}$，计算 $E=\tilde{g}^u\tilde{h}^{-\beta^*}(u\in_R\mathbb{Z}_T^*)$；

(f) 输出公钥 $PK=(QR_N,T,g^{\boldsymbol{r}},g^{\langle \boldsymbol{r},\boldsymbol{s}\rangle},\tilde{g},\tilde{h},E,pk_{CH})$，私钥 $SK=\boldsymbol{s}$.

(2) 加密算法 PKE.Enc(PK,M). 具体步骤如下：

(a) 输入公钥 PK 和明文 $M\in Z_N$；

(b) 随机选择 $w\in Z_T$，计算 $\boldsymbol{C}=g^{\boldsymbol{r}\cdot w}$；

(c) 计算 $K=g^{\langle \boldsymbol{r},\boldsymbol{s}\rangle\cdot w}$，$\psi=K\cdot M=g^{\langle \boldsymbol{r},\boldsymbol{s}\rangle\cdot w}\cdot M$；

(d) 计算 $\Pi=(E\cdot\tilde{h}^{\beta})^{Inj(K)}$，其中 $\beta=$CH.Eval$(pk_{CH},t_a;t_c)$，辅助标记 $t_a=(\boldsymbol{C},\psi)$，随机选择核心标记 $t_c\in R_{CH}$；

(e) 输出密文 $CT=(\boldsymbol{C},\psi,\Pi,t_c)$.

(3) 解密算法 PKE.Dec(SK,CT). 步骤如下：

(a) 输入密文 $CT=(\boldsymbol{C},\psi,\Pi,t_c)$及私钥 $SK=\boldsymbol{s}$；

(b) 计算 $K'=\langle \boldsymbol{s},\boldsymbol{C}\rangle$；

(c) 计算 $\Pi'=(E\cdot\tilde{h}^{\beta})^{Inj(K')}$，其中

$\beta=$ CH.Eval$(pk_{CH},(\boldsymbol{C},\psi);t_c)$；

(d) 校验 $\Pi'=\Pi$ 是否成立？

如果不成立，则返回⊥并拒绝解密；

如果成立，则返回明文 $M=\psi/K'$.

6.3　正确性和安全证明

6.3.1　正确性

$$K'=\langle \boldsymbol{s},\boldsymbol{C}\rangle=\langle \boldsymbol{s},g^{w\cdot \boldsymbol{r}}\rangle=g^{\langle \boldsymbol{s},w\cdot \boldsymbol{r}\rangle}=g^{\langle \boldsymbol{s},\boldsymbol{r}\rangle\cdot w};$$

$$\frac{\psi}{K'}=\frac{g^{\langle \boldsymbol{s},\boldsymbol{r}\rangle\cdot w}\cdot M}{K'}=M.$$

6.3.2　安全性

定理 3.　设 DDH 困难假设成立，且 RSI 假设在二次剩余群 QR_N 中也成立，CH 是一个卡梅隆哈希函数，根据扩展 Goldreich-Levin 定理(第 2 节定理 1)，改进的新的 PKE 方案是抗辅助输入 IND-CCA 安全的，PPT 攻击者 $\mathcal{A}$ 获胜的优势如下：

$$\mathrm{Adv}_{\mathrm{PKE},\mathcal{A}}^{\mathrm{AI\text{-}CCA}}(k)\leq 2\mathrm{Adv}_{\mathrm{QR}_N,\mathcal{B}}^{\mathrm{RSI}}(k)+\mathrm{Adv}_{\mathrm{G},\mathcal{B}_4}^{\mathrm{DDH}}(k)+$$

$$Q(k)\left(\mathrm{Adv}_{\mathrm{CH},\mathcal{B}_5}^{\mathrm{CR}}(k)+\frac{\varepsilon^3}{512\cdot n\cdot q^2}+\frac{2^{\log p}}{2^{\log T}-Q(k)}\right)+\varepsilon,$$

其中 $Q(k)$是攻击者 $\mathcal{A}$ 进行解密询问的次数.

证明.　我们首先定义挑战者 $\mathcal{B}$ 与 PPT 攻击者 $\mathcal{A}$ 之间的一系列交互式游戏 $\mathrm{Game}_0,\mathrm{Game}_1,\cdots,\mathrm{Game}_6$ 来进行安全性证明. 在第 i 轮游戏 $\mathrm{Game}_i(i=0,1,\cdots,6)$中，挑战者 $\mathcal{B}$ 随机选定比特 b 的值，攻击者 $\mathcal{A}$ 输出 b' 作为对 b 的猜测，记事件 S_i 为“第 i 轮游戏 Game_i 中，$b'=b$”，记挑战密文为 $CT^*=(\boldsymbol{C}^*,\psi^*,\Pi^*,t_c^*)$.

Game_0. 这是最初定义的抗辅助输入 IND-CCA 安全的游戏(第 3 节定义 1). 挑战者 $\mathcal{B}$ 产生一对公/私钥对(PK,SK)，并将公钥 PK 发送给攻击者 $\mathcal{A}$. 当 $\mathcal{A}$ 进行解密询问或者私钥泄漏查询时，$\mathcal{B}$ 利用 SK 进行解密，或者将泄漏函数 f_i 作用于私钥 SK. 同时，返回解密结果和泄漏值 $f_i(SK)$. 对等长的消息 M_0,M_1，$\mathcal{B}$ 随机选择 $b\in\{0,1\}$，并将对 M_b 加密产生的挑战密文 CT^* 发送给 $\mathcal{A}$. 挑战密文产生后，$\mathcal{A}$ 仍可继续对除了挑战密文 CT^* 以外的任何密文进行解密询问. 最后，$\mathcal{A}$ 输出 b'. 所以，

$$\mathrm{Adv}_{\mathrm{PKE},\mathcal{A}}^{\mathrm{AI\text{-}CCA}}(k)=\left|\Pr[S_0]-\frac{1}{2}\right|.$$

Game_1. 这个游戏与游戏 Game_0 不同之处在于：挑战密文中的核心标记 t_c^* 的选择. 在游戏 Game_0 中核心标记 t_c^* 是从标记集合 $\mathcal{T}_c$ 中随机选择的，而游戏 Game_1 中的 t_c^* 是挑战者 $\mathcal{B}$ 根据 OTLF 的有损标记生成算法 OTLF.LTag(F_{td},t_a^*) 计算出 t_c^*，其中 $t_a^*=(\boldsymbol{C}^*,\psi^*)$. 根据 OTLF 中随机标记与有损标记的不可区分性以及合数阶群中 OTLF 的属性(定理 2)，有 $|\Pr[S_1]-\Pr[S_0]|\leq\mathrm{Adv}_{\mathrm{OTLF},\mathcal{B}_1}^{\mathrm{IND}}(k)\leq 2\mathrm{Adv}_{\mathrm{QR}_N,\mathcal{B}}^{\mathrm{RSI}}(k)$.

Game_2. 这个游戏与游戏 Game_1 类似，不同之处

在于:解密询问时,若密文 CT 中的标记 t 与挑战密文 CT^* 中的标记 t^* 相同(又可称为拷贝标记),即 $t=(t_a,t_c)=(t_a^*,t_c^*)=t^*$,挑战者 $\mathcal{B}$ 立即输出"$\perp$"并停止解密.通过下面的分析可以看出,带有拷贝 OTLF 标记的密文在游戏 Game_1 和游戏 Game_2 中被拒绝.这是因为,当 $t=t^*$ 时,会出现两种情形:

(1) $\Pi=\Pi^*$,也即 $CT=CT^*$.这种情形在 Game_1 和游戏 Game_2 即会被挑战者当作挑战密文拒绝;

(2) $\Pi\neq\Pi^*$.因为 $t=t^*$,故 $t_a=t_a^*$,即 $(\boldsymbol{C},\psi)=(\boldsymbol{C}^*,\psi^*)$,故 $K=K^*$,$OTLF_{F_{pk},t}(K)=OTLF_{F_{pk},t^*}(K^*)=\Pi^*$.这种情形也会在 Game_1 中被挑战者拒绝.

综上,$\Pr[S_2]=\Pr[S_1]$.

Game_3.这个游戏与游戏 Game_2 类似,不同之处在于:封装密钥 K^* 是由挑战者 $\mathcal{B}$ 根据私钥 $SK=\boldsymbol{s}$ 计算 $\langle\boldsymbol{C}^*,\boldsymbol{s}\rangle=K^*$ 产生,而不是 Game_2 中利用公钥 $g^{\langle\boldsymbol{r},\boldsymbol{s}\rangle}$ 计算 $K^*=(g^{\langle\boldsymbol{r},\boldsymbol{s}\rangle})^{w^*}$ 产生,由方案的正确性,有 $\Pr[S_3]=\Pr[S_2]$.

Game_4.这个游戏与游戏 Game_3 类似,不同之处在于:挑战密文 $CT^*=(\boldsymbol{C}^*,\psi^*,\Pi^*,t_c^*)$ 中的 $\boldsymbol{C}^*$ 不再是封装密钥 K^* 的"有效密文",而是随机取自封装密钥 K^* 的"无效密文"集合 $\boldsymbol{C}^*=(g_1^{w_1},\cdots,g_m^{w_m})$.根据 DDH 困难假设,因此

$$|\Pr[S_4]-\Pr[S_3]|\leq \text{Adv}_{\text{G},\mathcal{B}_4}^{\text{DDH}}(k).$$

Game_5.这个游戏与游戏 Game_4 类似,不同之处在于:在解密询问中,若 $\boldsymbol{C}$ 是封装密钥 K 的"无效密文"(密文随机选择,指数互不相等),则挑战者 $\mathcal{B}$ 也立即输出"$\perp$"并且停止解密询问.记 E 为事件"密文 CT 在游戏 Game_5 中被拒绝,但在游戏 Game_4 中却未被拒绝".换言之:当 $\boldsymbol{C}$ 为封装密钥 K 的"无效密文"时,CT 在游戏 Game_4 中却被解密 Oracle 接受,这样,攻击者 $\mathcal{A}$ 就容易从挑战者 $\mathcal{B}$ 返回的信息中获得有用信息.所以,$|\Pr[S_5]-\Pr[S_4]|\leq\Pr(\text{E})$.

我们期望 $\Pr(\text{E})$ 的值是可忽略的.记 F 为事件"在游戏 Game_4 中存在解密询问密文 $CT=(\boldsymbol{C},\psi,\Pi,t_c)$,其中 $t=((\boldsymbol{C},\psi),t_c)$ 是一个非单射、非拷贝的标签".根据全概公式,有

$$\begin{aligned}\Pr(\text{E})&=\Pr[\text{E}\wedge\text{F}]+\Pr[\text{E}\wedge\overline{\text{F}}]\\&\leq\Pr[\text{F}]+\Pr[\text{E}\mid\overline{\text{F}}].\end{aligned}$$

要说明 $\Pr(\text{E})$ 是可忽略的,可以从以下两个方面来证明.设攻击者 $\mathcal{A}$ 进行了至多 $Q(k)$ 次解密询问.

(a) $\Pr[\text{F}]\leq Q(k)\,\text{Adv}_{\text{CH},\mathcal{B}_5}^{\text{CR}}(k)$.若事件 F 发生,产生的标签 t 是非单射、非拷贝(Game_2 中的情形)取决于 OTLF 在给定有损标记的前提下给出非单射标签的碰撞率.在游戏 Game_4 中,为了能够模拟挑战密文(其中 OTLF 的标记必须是有损模式),挑战者 $\mathcal{B}$ 利用挑战密文 CT^* 中的辅助标记 $t_a^*=(\boldsymbol{C}^*,\psi^*)$ 对有损标记生成 Oracle 询问(仅一次)得到有损核心标记 t_c^*,此时,合数阶群上 OTLF 中的 Chameleon 哈希函数发生了碰撞,这个概率为 $\text{Adv}_{\text{OTLF},\mathcal{B}_5}^{\text{EVA}}(k)=\text{Adv}_{\text{CH},\mathcal{B}_5}^{\text{CR}}(k)$.攻击者 $\mathcal{A}$ 进行至多 $Q(k)$ 次解密询问,则事件 F 发生的概率至多为 $Q(k)\,\text{Adv}_{\text{OTLF},\mathcal{B}_5}^{\text{EVA}}(k)=Q(k)\,\text{Adv}_{\text{CH},\mathcal{B}_5}^{\text{CR}}(k)$.

(b) $\Pr[\text{E}|\overline{\text{F}}]\leq Q(k)\left(\dfrac{\varepsilon^3}{512\cdot n\cdot q^2}+\dfrac{\log p}{\log T-Q(k)}\right)$.

设事件 F 未发生前提下,CT 是使得事件 E 发生的第一个密文,即若 $\boldsymbol{C}$ 是封装密钥 K 的"无效密文",且 $\Pi=\text{OTLF}_{F_{pk},t}(K)=\text{OTLF}_{F_{pk},t}(\langle\boldsymbol{C},\boldsymbol{s}\rangle)$.在第一个无效密文 CT 被接受之前,从攻击者 $\mathcal{A}$ 的角度,$\mathcal{A}$ 能获得的与私钥 $SK=\boldsymbol{s}$ 相关的信息为 $PK=(g^{\langle\boldsymbol{r},\boldsymbol{s}\rangle},g^{\boldsymbol{r}})$,$CT^*=(\boldsymbol{C}^*,\psi^*,\Pi^*,t_c^*)$ 以及关于私钥 $\boldsymbol{s}$ 的辅助输入 $f(\boldsymbol{s},\boldsymbol{r})$.

(1)挑战密文 CT^* 中的 ψ^* 和 Π^* 中隐含了密钥 K^* 的信息($t_c^*=\text{OTLF.LTag}(F_{td},(\boldsymbol{C}^*,\psi^*))$ 中已经包含了 ψ^* 的信息),ψ^* 中封装密钥 K^* 至多有 $\log T$ 种可能,而 Π^* 中透露的关于 K^* 的信息至多为其有损模式下像的大小 $\log p$.所以,猜对密钥的概率至多为 $\dfrac{2^{\log p}}{2^{\log T}-Q(k)}$;

(2)已知 $PK=(g^{\boldsymbol{r}},\langle\boldsymbol{s},g^{\boldsymbol{r}}\rangle=g^{\langle\boldsymbol{r},\boldsymbol{s}\rangle})$ 和关于私钥 $\boldsymbol{s}$ 的辅助输入 $f(\boldsymbol{s},\boldsymbol{r})$,根据抗辅助输入模型的属性:不论这些辅助泄漏信息有多少,攻击者都仅以可忽略的概率恢复出用户私钥.由扩展 Goldreich-Levin 定理(第 2 节定理 1),攻击者恢复出私钥 $\boldsymbol{s}$ 的概率至多为 $\dfrac{\varepsilon^3}{512\cdot n\cdot q^2}$.故 $\Pr[\text{E}|\overline{\text{F}}]\leq Q(k)\left(\dfrac{\varepsilon^3}{512\cdot n\cdot q^2}+\dfrac{2^{\log p}}{2^{\log T}-Q(k)}\right)$.

综上可知,$|\Pr[S_5]-\Pr[S_4]|\leq\Pr(\text{E})\leq Q(k)\left(\text{Adv}_{\text{CH},\mathcal{B}_5}^{\text{CR}}(k)+\dfrac{\varepsilon^3}{512\cdot n\cdot q^2}+\dfrac{2^{\log p}}{2^{\log T}-Q(k)}\right)$.

Game_6.这个游戏与游戏 Game_5 类似,不同之处在于:挑战密文 CT^* 中的 ψ^* 不是由封装密钥 K^* 与消息 M_b 相乘得到 $\psi^*=K^*\cdot M_b=\langle\boldsymbol{C}^*,\boldsymbol{s}\rangle\cdot M_b=\langle\boldsymbol{s},\boldsymbol{C}^*\cdot M_b\rangle$,而是任取 $z\in Z_P$,$\psi^*=z\cdot M_b$.在攻击者 $\mathcal{A}$ 看来,这即是扩展 Goldreich-Levin 定理(第 2 节定理 1)中区分 $\langle\boldsymbol{C}^*,\boldsymbol{s}\rangle$ 与 $z\in Z_P$,其概率为 ε.当 $z=\langle\boldsymbol{C}^*,\boldsymbol{s}\rangle$ 时,即为 Game_5;当 $z\in Z_P$ 时,即为 Game_6.所以 $|\Pr[S_6]-\Pr[S_5]|\leq\varepsilon$.

因此,在 Game_6 中挑战密文 CT^* 中各分量

$CT^*=(\boldsymbol{C}^*,\psi^*,\Pi^*,t_c^*)$均独立，与消息$M_b$无关. 所以，$\Pr[S_6]=\frac{1}{2}$.

综上，即可得证.　　证毕.

6.4　改进方案的拓展

在上一节抗辅助输入 IND-CCA 安全 PKE 方案(PKE. KG，PKE.Enc，PKE. Dec)的基础上，利用代数中的核技术进行适当拓展，我们首次提出柔性模型下 IND-CCA 安全的抗持续辅助输入的 PKE 方案(PKE$_1$.KG，PKE$_1$.Enc，PKE$_1$.Dec，PKE$_1$.Update). 具体构造如下：

(1) PKE$_1$.KG，PKE$_1$.Enc，PKE$_1$.Dec：这 3 个与原算法 PKE.KG，PKE.Enc 和 PKE.Dec 分别一致.

(2) PKE$_1$. Update(UK，SK)：系统输入可更新密钥$UK=\boldsymbol{r}$和用户原有私钥$SK=\boldsymbol{s}$，随机选择$\boldsymbol{s}'\in Ker(\boldsymbol{r})$，输出更新后的用户私钥$SK=\boldsymbol{s}+\boldsymbol{s}'$.

6.4.1　正确性

因为$\boldsymbol{s}'\in Ker(\boldsymbol{r})$，所以$\langle \boldsymbol{s}',\boldsymbol{r}\rangle=0$. 因此，

$$K'=\langle \boldsymbol{s}+\boldsymbol{s}',\boldsymbol{C}\rangle=\langle \boldsymbol{s}+\boldsymbol{s}',g^{w\cdot r}\rangle=g^{\langle s+s',w\cdot r\rangle}$$
$$=g^{\langle s+s',r\rangle\cdot w}=g^{(\langle s,r\rangle+\langle s',r\rangle)\cdot w}=g^{\langle s,r\rangle\cdot w};$$

$$\psi/K'=g^{\langle s,r\rangle\cdot w}\cdot M/K'=M.$$

6.4.2　安全性

由于柔性模型中密钥更新的过程是在一个可信的抗泄漏的硬件装置中实施的，且更新前的密钥会及时销毁，故该方案的安全性证明只需要证明单个周期内的抗辅助输入 IND-CCA 安全性. 即上一节改进方案的安全性证明.

7　结束语

本文从基于的困难假设易解、不能抵抗选择明文安全等几个方面指出了文献[22]安全的脆弱性. 在此基础上，借助 BHHO 方案[23]和合数阶群下一次性有损函数重新构造了一个抗辅助输入 IND-CCA 安全的 PKE 方案，并利用扩展 Goldreich-Levin 定理给出了严格的安全性证明. 另外，我们对改进的方案进行拓展，首次提出了抗持续辅助输出 IND-CCA 安全的 PKE 方案. 但是，由于本文的方案是在柔性模型下的方案，也即密钥更新必须在一个抗泄漏的封闭的硬件装置中进行. 如何摆脱这个限制条件，做到真正意义上的抗持续辅助输入，是后续仍然可以深究的工作；另一方面，本文在定理 3 的安全证明中，攻击者对无效密文的选择限定在随机选取范围内，取消这个限制，让攻击者可以非随机选取，也是一个后续仍然可以值得探究的工作.

致　谢　审稿人提出了中肯的意见，付出了辛勤的工作，在此表示感谢！

参　考　文　献

[1] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems//Proceedings of the CRYPTO'96. Santa Barbara, USA, 1996: 104-113

[2] Halderman J A, Schoen S D, Heninger N, et al. Lest we remember: Cold boot attacks on encryption keys//Proceedings of the Usenix Security Symposium. San Jose, USA, 2009: 45-60

[3] Heninger H, Shacham H. Reconstructing RSA private keys from random key bits//Proceedings of the CRYPTO'09. Santa Barbara, USA, 2009: 1-17

[4] Micali S, Reyzin L. Physically observable cryptography//Proceedings of the TCC 2004. Cambridge, USA, 2004: 278-296

[5] Alwen J, Dodis Y, Naor M, et al. Public-key encryption in the bounded-retrieval model//Proceedings of the EUROCRYPT'10. French Riviera, France, 2010: 113-134

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

[7] Dodis Y, Haralambiev K, Lopez-Alt A, Wichs D. Cryptography against continuous memory attacks//Proceedings of the FOCS'10. Las Vegas, USA, 2010: 511-520

[8] Brakerski Z, et al. Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage//Proceedings of the FOCS'10. Las Vegas, USA, 2010: 501-510

[9] Agrawal S, Dodis Y, Vaikuntanathan V, Wichs D. On continual leakage of discrete log representations//Proceedings of the ASIACRYPT'13. Bangalore, India, 2013: 401-420

[10] Naor M, Segev G. Public-key cryptosystems resilient to key leakage//Proceedings of the CRYPTO'10. Santa Barbara, USA, 2010: 18-35

[11] Brakerski Z, Goldwasser S. Circular and leakage resilient public-key encryption under subgroup indistinguishability (or: Quadratic residuosity strikes back)//Proceedings of the CRYPTO'10. Santa Barbara, USA, 2010: 1-20

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

[13] Qin Q, Liu S. Leakage-flexible CCA-secure public-key encryption: Simple construction and free of pairing//Proceedings of the PKC'14. Buenos Aires, Argentina, 2014: 19-36

[14] Li S, Mu Y, Zhang M, Zhang F. Continuous leakage resilient lossy trapdoor functions. Information, 2017, 8(2): 38; doi: 10.3390

[15] Li Su-Juan, Mu Yi, Zhang Ming-Wu, Zhang Fu-Tai. Updatable

lossy trapdoor functions and its application in continuous leakage//Proceedings of the ProvSec'16. Nanjing, China, 2016: 309-319

[16] Li Su-Juan, Zhang Fu-Tai, Sun Yin-Xia, Shen Li-Min. Efficient leakage-resilient public key encryption from DDH assumption. Cluster Computing, 2013, 16(4): 797-806

[17] Dodis Y, Haralambiev K, López-Alt A, Wichs D. Efficient public-key cryptography in the presence of key leakage// Proceedings of the ASIACRYPT'10. Santa Barbara, USA, 2010: 613-631

[18] Galindo D, Herranz J, Villar JL. Identity-based encryption with master key-dependent message security and leakage-resilience// Proceedings of the ESORICS'12. Pisa, Italy, 2012: 627-642

[19] Zhang Ming-Wu, Chen Mi-Wen, He De-Biao, Yang Bo. An efficient leakage resilient and CCA2-secure PKE system. Chinese Journal of Computers, 2016, 39(3): 492-502(in Chinese)
(张明武，陈泌文，何德彪，杨波. 高效弹性泄漏下 CCA 安全的公钥加密体制. 计算机学报，2016，39(3)：492-502)

[20] Li Su-Juan, Zhang Fu-Tai. Leakage-resilient identity-based encryption scheme. International Journal of Grid and Utility Computing, 2013, 4(2/3): 187-196

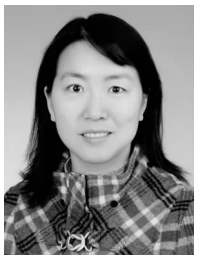
[21] Dachman-Soled D, Dov Gordon S, Liu FH, et al. Leakage-resilient public-key encryption from obfuscation//Proceedings of the PKC'16. Taipei, China, 2016: 101-128

[22] Wang Zhi-Wei, Li Dao-Feng, Zhang Wei, Chen Wei. CCA secure PKE with auxiliary input. Chinese Journal of Computers, 2016, 39(3): 562-570(in Chinese)
(王志伟，李道丰，张伟，陈伟. 抗辅助输入 CCA 安全的 PKE 构造. 计算机学报，2016，39(3)：562-570)

[23] Boneh D, Halevi S, Hamburg M, Ostrovsky R. Circular-secure encryption from decision Diffie-Hellman//Proceedings of the CRYPTO'08. Santa Barbara, USA, 2008: 108-125

[24] Goldreich O, Levin LA. A hard-core predicate for all one-way functions//Proceedings of the STOC'89. Washington, USA, 1989: 25-32

[25] Wee H. Dual projective hashing and its applications—Lossy trapdoor functions and more//Proceedings of the EUROCRYPT'12. Cambridge, UK, 2012: 246-262



LI Su-Juan, born in 1978, Ph. D., associate professor. Her main research interests are information security and cryptography.

ZHANG Ming-Wu, born in 1970, Ph. D., professor. His main research interests include applied cryptography, security and privacy preservation and the protocol of network security.

ZHANG Fu-Tai, born in 1965, Ph. D., professor. His main research interests include network security and cryptography.

Background

Security primitives of modern cryptography technology has modeled attackers as having only black-box access to the primitives, and ensure that secret keys must be safely stored and internal states are not leaked to the attackers. But these models do not capture the real circumstance where the adversary can achieve traditional information of the secret inner states through side-channel attack. In order to avoid this type of attacks, the researchers provide two remedial measures to resist the attacks. One way is to reinforce the hardware to eliminate the damage of the kind of attack, which we call hardware-based level way; the other way is to design secure algorithms by mathematical technology in order to reject this kind of attack, which we call algorithm-based level way.

The chosen ciphertext attack (IND-CCA) secure public key encryption with auxiliary input is an important research topic in the leakage resilient public key cryptosystem. The auxiliary input model is the strongest model in the security model of leakage resilient attacks during one key existing period. According to what we know almost all public key encryption schemes with auxiliary input are proved to be chosen plaintext attack (IND-CPA) secure. One of the more interesting attempts to construct IND-CCA-secure public key encryption with auxiliary input is due to Wang et al. [Wang Zhi-Wei, Li Dao-Feng, Zhang Wei, Chen Wei. CCA Secure PKE with Auxiliary Input. Chinese Journal of Computers. 2016, 39(4): 562-570]. However, by giving concrete attacks we find that their proposal is not secure. The hardness assumption of their scheme is not difficult and their scheme does not satisfy the IND-CPA secure. By the crypto-analysis, we improve their scheme and achieve a new IND-CCA secure public key encryption scheme with (continual) auxiliary input which is proved to be secure rigorously.

This research is supported partially by the National Natural Science Foundation of China under Grant Nos. 61702259, 61802242, 61672289 and 61672010, the Jiangsu Government Scholarship for Overseas Studies, the Postdoctoral Science Foundation of Jiangsu Province (No. 1601008A), the Natural Science Fund for Colleges and Universities of Jiangsu Province (No. 16KJB520018) and the Philosophy and Social Science Fund for Colleges and Universities of Jiangsu Province (2017SJB0201).