软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(5):1196−1212 [doi: 10.13328/j.cnki.jos.004693]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

密钥弹性泄漏安全的通配模板层次委托加密机制*

张明武[1], 王春枝[1], 杨 波[2], 高木刚[3]

[1](湖北工业大学 计算机学院,湖北 武汉 430068)

[2](陕西师范大学 计算机学院,陕西 西安 710071)

[3](Institute of Mathematics for Industry, Kyushu University, Fukuoka 819-0395, Japan)

通讯作者: 张明武, E-mail: csmwzhang@gmail.com

摘 要: 传统的密码方案假定密钥对可能的攻击者来说是完全隐藏的(只有算法是公开的),敌手无法获得有关密钥的任何信息.但在实际系统中,攻击者可在噪声信道或由侧信道攻击获得有关密钥的部分信息.密钥弹性泄漏安全的加密方案通过改进密码算法达到在密钥存在可能部分泄漏情况下的语义安全性.设计了一个抗密钥弹性泄漏的可委托层次模板加密方案.在该方案中,用户身份关联到含有通配符的身份模板,并可以实现再次密钥委托.该方案是抗泄漏的层次身份加密方案(hierarchical identity-based encryption,简称 HIBE)和隐藏向量加密方案(hidden vector encryption,简称 HVE)的一般扩展,可有效地抵抗密钥弹性泄漏,并达到自适应语义安全性.同时给出该方案的安全性证明和系统抗泄漏性能,分析显示,该方案具有较好的密钥泄漏容忍性.

关键词: 通配身份基加密;弹性泄漏;密钥委托;身份模板;泄漏率

中图法分类号: TP309

中文引用格式: 张明武,王春枝,杨波,高木刚.密钥弹性泄漏安全的通配模板层次委托加密机制.软件学报,2015,26(5):1196−1212. http://www.jos.org.cn/1000-9825/4693.htm

英文引用格式: Zhang MW, Wang CZ, Yang B, Takagi T. Key leakage-resilient secure cryptosystem with hierarchical wildcard pattern delegation. Ruan Jian Xue Bao/Journal of Software, 2015,26(5):1196−1212 (in Chinese). http://www.jos.org.cn/1000-9825/4693.htm

Key Leakage-Resilient Secure Cryptosystem with Hierarchical Wildcard Pattern Delegation

ZHANG Ming-Wu[1], WANG Chun-Zhi[1], YANG Bo[2], Tsuyoshi TAKAGI[3]

[1](School of Computer Sciences, Hubei University of Technology, Wuhan 430068, China)

[2](School of Computers, Shaanxi Normal University, Xi'an 710071, China)

[3](Institute of Mathematics for Industry, Kyushu University, Fukuoka 819-0395, Japan)

Abstract: In the traditional cryptosystems, secret keys are perfectly hidden for any possible attackers and only the cryptographic algorithms and public parameters are public. However, in practical applications, the attacker can obtain partial information about the matched decryption key from the noise channels or by the side-channel attacks. This study proposes a leakage-resilient hierarchical wildcard pattern encryption in which a user is associated with a wildcard identity pattern. A secret key is derived for a vector of identity strings where entries can be left blank using a wildcard, and this key can then be used to derive keys for any pattern that replaces wildcards with concrete identities. The scheme supports the wildcard pattern key delegation, which is considered as a general extension of leakage-resilient hierarchical IBE (identity-based encryption) and HVE (hidden vector encryption). Moreover, the proposed scheme can tolerate partial key leakage, and the scheme is proven to be leakage-resilient and semantically secure in the standard model under the subgroup decision assumptions.

Key words: wildcard IBE (identity-based encryption); leakage resilience; key delegation; identity pattern; leakage rate

* 基金项目: 国家自然科学基金(61370224, 61272436, 61170135); 湖北省自然科学基金(2013CFA046); 湖北工业大学高层次人才项目; 中国科学院信息工程研究所信息安全国家重点实验实验室开放课题(2014-04)

收稿时间: 2013-04-03; 定稿时间: 2014-07-09

在密钥可委托的层次加密系统中[1,2],所有用户组成一个深度是 L 的树型结构,树根对应系统主密钥持有方(如密钥生成中心 PKG),任何中间节点可为其子节点(或叶子节点)生成密钥.虽然层次加密方案可以机密发送一个消息给多个用户(对应一个子树路径的用户群),但在解密过程中,父节点必须通过密钥委托机制生成与接收用户身份串对应的密钥才能解密.同时,由于树型用户群结构是预先已设计好的,这种层次用户群结构非常不灵活,无法在实际应用中实现弹性的接收者控制.基于通配身份的加密(wildcard identity-based encryption,简称 WIBE)最早由 Abdalla 等人[3]提出,用于控制不同接收群的消息保密方案,允许身份串中部分元素由通配符*代替,只要任何匹配模板的用户使用其密钥就可以解密.WIBE 可以扩展到通配内积加密[4].通配模板加密扩展 WIBE,使得收发双方都采用含通配符的向量模板,其典型应用是安全群邮件收发和生物特征模板身份加密.例如,我们想将一封邮件发送到计算机系的所有人员,则可以通过*@cs.edu.cn 来实现,这里的*就是通配符.利用通配模板,我们可以有效地管理不同类型的用户群.

层次加密系统密钥委托过程假定委托者与受委托者之间存在传送密钥的可信秘密信道[1,5,6],同时假定密钥对可能的攻击者来说是完全隐藏的(密码算法是公开的),敌手无法获得有关密钥的任何信息[7−9].在安全性方面,传统方案中允许敌手询问非匹配挑战身份密钥,无法获得匹配挑战密文身份的解密密钥的任何信息.即使匹配挑战身份的密钥被部分地泄漏(即使是一个比特),可证明安全也将失效.

在实际应用系统中,攻击者可在噪声信道或由侧信道攻击获得有关密钥的部分信息[10−12].例如,在层次密钥委托系统中,每个用户都可为其子树节点用户生成委托密钥,但要保证用户与其所有子节点间存在可传输密钥的秘密且可信的信道,这在大规模开放式网络系统,如云计算、物联网及 Mesh 网等,是非常困难的.进一步来讲,即使密钥被安全地分发,系统密码算法在执行过程中,密钥都必须调入内存被相关算法调用,这极易被攻击以通过冷启动的方法获得密钥的部分信息.密钥弹性泄漏安全的加密方案通过改进密码算法达到在密钥存在可能部分泄漏情况下的语义安全性[10,13−15].在密钥委托系统中,每个用户都可生成其子树的密钥,因此更容易受到这类攻击[16−18].

Akavia 等人[19]于 2009 年首次引入密钥泄漏下可证明安全的概念,并设计由侧信道攻击产生的抗对称密钥的内存泄漏,引起信息安全领域的高度重视.为了模拟泄漏,设定攻击者能够访问泄漏寓言机(leakage oracle),从而获得关于密钥的任何多项式时间可计算函数的输出.Alwen 等人[10]改进了文献[19]的工作,首次构建了基于边界检索模型的抗泄漏公钥加密方案,采用在硬件上不同的存储区来组织密钥,并要求多个密钥存储模块不能同时被泄漏.Dodis 等人[20]和 Chow 等人[13]采用哈希证明系统(Hash proof system,简称 HPS),分别扩展到了基于公钥和基于身份的抗弹性泄漏的加密方案,但建立在哈希证明系统上的方案不支持主(根)密钥泄漏安全性.虽然 HPS 提供一般的公钥加密到抗泄漏的转化技术,但在密钥可委托的方案中,无法提供密钥委托的构建[13,15];同时,HPS 需要理论模型的随机提取器,在现实中不容易构造[21].Liu 等人[15]改进了 HPS 的构建方法,使其达到更好的抗泄漏性.Lewko 等人[16]提出了利用双系统加密技术达到容忍密钥有界泄漏.文献[18]设计了仿射空间作为密钥角色的容忍主密钥和用户密钥连续泄漏的加密方案.

本文了设计一个基于通配模板抗密钥弹性泄漏的加密方案.在该方案中,用户身份关联到含有通配符的身份模板,并可以实现再次密钥委托.加密过程中,接收者定义为含有通配符的身份模板,用以灵活地控制多个不同接收者.本方案可以看作是密钥弹性泄漏安全的层次身份加密 HIBE(hierarchical identity-based encryption)[13,16]、模糊身份基加密 FIBE(fuzzy identity-based encryption)[22]、隐藏向量加密 HVE(hidden vector encryption)[23]等方案的一般扩展.

由于本方案要支持在弹性泄漏条件下的模板密钥委托功能,因此不能直接采用哈希证明系统来构建.要解决的关键问题是:如何保证密钥在部分被泄漏情况下,密钥熵损是可忽略的.为此,借助于代数空间正交向量弹性泄漏容忍映射性质(引理 1),我们扩展合数阶双线性群到多维,以实现有界弹性泄漏安全;同时,借助于多维子群向量空间组织双系统空间[16],以实现对方案的自适应性安全性证明.文献[24,25]提出了入侵容忍的加密和签名方案.该系统中密钥可以在整个生命周期被分割成离散的时间阶段,并可行演化解密密钥.

为了证明本文方案的安全性,利用子群正交性特性隐藏部分向量空间实现抗泄漏性.在实际的构造方案中,

密钥和密文都处于正常形态(normal),在证明安全时,我们定义半功能化(semi-functional)的密钥和密文.事实上,半功能化密钥和密文类似 HPS 中的无效密钥生成器,仅用于安全性证明.根据双系统加密的性质,一个半功能密钥解密一个半功能密文是计算上不可行的.为了达到方案构造中正常形态挑战密文不能被正常形态密钥解密,我们首先将正常形态密文转换为半功能化形式,然后将敌手所询问的正常形态密钥(非匹配密钥)逐步地转换为半功能形式,并将泄漏条件下的密钥转换为支配型半功能形式,最后得到半功能化的挑战密文和密钥.我们证明这一系列转换在计算上是不可区分的.最后,我们证明在敌手获得匹配密文模板的部分密钥后,仍不能构建有效可解密挑战密文的支配型密钥.

1 预备知识

1.1 基本知识

$F_p=\{1,2,\ldots,p-1\}$.$r\leftarrow F_p$ 定义为从 F_p 上随机选取一元素赋值给 r.设 $P=(a_1,a_2,\ldots,a_L)$是 L 个元素的有序集合.对 $0\leqslant \ell\leqslant L$, $P_{\leqslant \ell}$ 是 P 中前ℓ个元素集合,即 $P_{\leqslant \ell}=(a_1,a_2,...,a_\ell)$.为方便表述,本文以 P 来定义模板.本文中,$\upsilon(\lambda)$定义为对安全参数λ在计算上是可忽略的函数.设 S 表示一有限集合,$|S|$表示 S 的元素个数;设 $X\in\chi$,$Y\in\gamma$是两个分别在概率总体 X 和 Y 上选取的随机变量,随机变量 X 的最小熵定义为 $H_\infty(X)=-\log\max_{x\in\chi}[X=x]$.在已知 Y 下的 X 条件最小熵定义为 $H_\infty(X\mid Y)=-\log(E_{y\leftarrow\gamma}[2^{-H_\infty(X|Y=y)}])$.若 $X_1,X_2\in X$,则 X_1 与 X_2 的统计距离为

$$SD(X_1,X_2)=\frac{1}{2}\sum_{x\in X}|\Pr[X_1=x]-\Pr[X_2=x]|=\max_A \Pr[X_1\in A]-\Pr[X_2\in A] \tag{1}$$

定义 1(计算性不可区分). 对任一概率多项式时间算法 A,两个概率总体χ,γ满足:

$$|\Pr[A(\lambda,\chi)=1]-\Pr[A(\lambda,\gamma)=1]|\leqslant\upsilon(\lambda),$$

则称χ和γ对算法 A 在安全参数λ上是计算不可区分的.

引理 1[12]. 设 p 是素数,$m,l,d\in\mathbf{N}$ 满足 $2\leqslant 2d\leqslant l\leqslant m$, $X_1\leftarrow F_p^{m\times l}$,$X_2\leftarrow F_p^{m\times d}$.$T\leftarrow Rk_d(F_p^{l\times d})$ 是在 F_p 随机选取秩是 d 的矩阵.设 $f:F_p^{m\times d}\to\{0,1\}^J$ 是矩阵 $F_p^{m\times d}$ 上输出长度 $2^J\leqslant 4p^{l-2d}(p-1)\cdot\upsilon(\cdot)^2$ 的任意映射,则

$$SD((X_1,f(X_1T)),(X_1,f(X_2)))\leqslant\upsilon(\cdot) \tag{2}$$

特别地,若 $d=1$,$m\approx l$,则 $f(X_2)$可以近似泄漏全部的 X_2.

显然,定理中$|X_2|=m\log p$,允许泄漏大小 $J=(l-1)\log p-2\log(1/\upsilon(\cdot))$,此时,$f(X_2)$以 $\upsilon(\cdot)$的统计距离隐藏子空间 X_1.假定 p 是超多项式时间的安全参数,$\upsilon(p)=1/p$ 是 p 上的可忽略函数,此时,在 $f(X_2)$泄漏允许最大值是$(l-3)\log p$ 比特时,随机变量 X_2 的函数泄漏 $f(X_2)$可以隐藏子空间 X_1.

推论 1. 设 m 是大于 2 的整数,p 是一大素数.设 $\vec{\Delta},\vec{\pi}\leftarrow F_p^m,\vec{\pi}'\leftarrow V_p^\perp(\vec{\Delta})$ ($V^\perp(\vec{\pi})$ 是由基 $\vec{\pi}$ 生成向量空间的正交空间).对任一输出长度 $2^J\leqslant 4p^{m-3}(p-1)\cdot\upsilon(\cdot)^2$ 的映射 $f:F_p^m\to\{0,1\}^J$, 则

$$SD((\vec{\Delta},f(\vec{\pi}')),(\vec{\Delta},f(\vec{\pi})))\leqslant\upsilon(\cdot) \tag{3}$$

证明:在引理 1 中,置 $d=1$,$l=m-1$,则 X_1 对应于向量 $\vec{\Delta}$ 的正交空间 $V^\perp(\vec{\Delta})$ 的基,X_2 对应于 $\vec{\pi}.T\in Rk_1(F_p^{(m-1)\times 1})$,$\vec{\pi}'$ 与 X_1T 同分布.由于 $\vec{\Delta}$ 是从 F_p^m 上随机选取,X_1 由 $\vec{\Delta}$ 所决定,则 X_1 是 $F_p^{m\times(m-1)}$ 上的均匀分布,有:

$$SD((\vec{\Delta},f(\vec{\pi}')),(\vec{\Delta},f(\vec{\pi})))=SD((X_1,f(X_1T)),(X_1,f(X_2)))\leqslant\upsilon(\cdot). \qquad \square$$

本文采用正交子群 G_1 和 G_2 作为这里的正交空间.后文我们将分析本文方案的泄漏界 $J=(Q-1-2c)\log p_2$.这里,Q 是方案中的泄漏参数,p_2 是子群 G_2 的阶,c 是一常数,满足 $\upsilon(\cdot)=p_2^{-2c}$ 是可以忽略的,其中,$2^\lambda\leqslant p_2\leqslant 2^{\lambda+1}$.

1.2 合数阶双线性群

一个合数阶双线性群描述包括(N,G,G_t,e),阶 N 是多个不相等素数之积.设 $N=p_1p_2p_3$,这里,$p_i(i=1,2,3)$满足对 $i\neq j$,有 $gcd(p_i,p_j)=1$.除了满足传统的素数阶群双线性以外,G 包含阶分别是 p_1,p_2 和 p_3 的子群 G_1,G_2 和 G_3,设其生成元分别是 g_1,g_2 和 g_3,则 G 中的任一元素都可以唯一表示成 $g_1^{n_1}g_2^{n_2}g_3^{n_3}$ 的形式.这里,$n_1,n_2,n_3\in F_N$.合数阶双线性

群除了满足一般双线性群的性质以外,还具有如下特殊性质:

性质 1(子群生成元). 设 g 是 G 的生成元,则 $g^{p_2p_3}$ 是 G_1 的生成元, $g^{p_1p_3}$ 是 G_2 的生成元, $g^{p_1p_2}$ 是 G_3 的生成元.

证明:$g\in G$ 可以唯一表示成 $g=g_1^{n_1}g_2^{n_2}g_3^{n_3}$,这里,$n_1\neq 0 \bmod p_1$,$n_2\neq 0 \bmod p_2$,$n_3\neq 0 \bmod p_3$.

$$g_1^{n_1p_2p_3 \bmod p_1}(g_2^{p_2 \bmod p_2})^{n_2p_3}(g_3^{p_3 \bmod p_3})^{n_3p_2}=g_1^{n_1p_2p_3 \bmod p_1}=g_1, g^{p_2p_3}=(g_1^{n_1}g_2^{n_2}g_3^{n_3})^{p_2p_3}=g_1'.$$

由于 $n_1\neq 0 \bmod p_1$ 且 p_2 和 p_3 与 p_1 互素,根据中国剩余定理,$n_1p_2p_3\neq 0 \bmod p_1$, $g_1'\neq 1_{G_1}$, $g_1'=g^{p_2p_3}$ 是 G_1 的生成元.同理, $g^{p_1p_3}$ 是 G_2 的生成元, $g^{p_2p_3}$ 是 G_3 的生成元. □

性质 2(正交性与非退化性). 对任意 $h_i\in G_i$,$h_j\in G_j$,满足:

$$e(h_i,h_j)\begin{cases}\neq 1, & i=j \text{ (非退化性)}\\ =1, & i\neq j \text{ (正交性)}\end{cases} \tag{4}$$

证明:

(1) 非退化性.非退化是由双线性群的基本性质决定的.合数阶的双线性子群仍满足双线性,因此在任意子群($i=j$)中,对任意 $u,v\in G_i$,满足 $e(u,v)\neq 1$.

(2) 正交性.当 $i\neq j$ 时,h_i,h_j 属于阶分别是 p_i 和 p_j 的子群.设 g 是 G 的生成元,根据子群生成元的性质,h_i 和 h_j 可以分别表示成 $(g^{N/p_i})^{n_i}$ 和 $(g^{N/p_j})^{n_j}$ 的形式:

$$e(h_i,h_j)=e((g^{N/p_i})^{n_i},(g^{N/p_j})^{n_j})=e(g,g)^{\frac{n_in_jN^2}{p_ip_j}}=(e(g,g)^N)^{n_in_j\prod_{k=1,\ldots,3\setminus\{i,j\}}p_k}=1.$$ □

推论 2. 设 G_{ij} 表示 $G_i\times G_j$ 子群($i\neq j$).$h_1\in G_{ij}$,$h_2\in G_{jk}$,则 $e(h_1,h_2)=G_{t,j}$.这里,$G_{t,j}$ 表示由 $e(g_j,g_j)$ 生成的子群.

文中用 G_{ij} 记由(g_i,g_j)生成的阶是 $p_1\times p_2$ 的子群,用 G 表示阶是 $N=p_1p_2p_3$ 的群,即

$$G_{ij}=G_i\times G_j(i,j=1,2,3),\ G=G_1\times G_2\times G_3.$$

2 方案模型

2.1 通配模板及委托

定义 2(HIBE). 层次身份的加密(HIBE)采用树型结构组织用户身份串,即 $I=(I_1,I_2,\ldots,I_\ell)\in\{0,1\}^\ell$.HIBE 由 5 种算法组成:$HIBE=(Setup,KeyExt,KeyDer,Enc,Dec)$,其中,Setup 算法由 PKG 执行,用于生成整个系统的公开参数及主密钥;KeyExt 算法由 PKG 为任意用户(特别是 1 级根用户)生成密钥;KeyDer 算法由用户密钥持有者为其委托身份串生成密钥;Enc 和 Dec 算法分别由加密者和解密者执行消息的加密和解密操作.

说明:事实上,*KeyExt* 算法利用主密钥为任意身份串生成密钥(任意身份串都是树根的子串),而 KeyDer 算法利用用户密钥为其委托身份生成密钥,如果把主密钥看成层次为 0 的身份串(空串)的密钥,则 KeyExt 和 KeyDer 算法功能相同.我们可以把 PKG 看成 0 级身份串的特殊用户,后面的方案中,我们省掉 KeyExt 算法.

定义 3(身份模板). 设*是特殊的通配符,身份模板是定义在集合元素 $(\{0,1\}\cup\{*\})^\ell$ 上的一组有序序列.设身份模板 $P=(a_1,a_2,\ldots,a_\ell)\in\{0,1,*\}^\ell$, $P'=(a_1,a_2,\ldots,a_{\ell'})$,满足:$\ell'\leqslant\ell$,且

$$\begin{cases}a_i=a_i \text{ or } a_i=*, & 1\leqslant i\leqslant\ell'\\ a_i=*, & \ell'+1\leqslant i\leqslant\ell\end{cases} \tag{5}$$

则称身份模板 P'匹配模板 P,记作 $Match(P',P)=1$;若模板不匹配,则记为 $Match(P',P)=0$.

说明:

(1) 若 $P=(*,*,\ldots,*)^\ell$,则该模板为长度为ℓ的任意通配模板,若加密给该模板同任何模板长度不大于ℓ的密钥持有者均可解密其对应密文.

(2) 若身份模板集定义为{0,1}上的有序串,则本方案等同于 HIBE.HIBE 是一类特殊的通配模板加密方案.

定义 4(模板委托). 设 $P=(a_1,a_2,...,a_\ell)\in\{0,1,*\}^\ell$ 是长度为ℓ的模板,我们称满足 $Match(P',P)=1$ 的 P'是 P 的委托模板.

例如,P_1=*@*.*edu.cn*,P_2=*hbut.edu.cn*,则 $Match(P_2,P_1)=1$.这里,P_1=(*cn*,*edu*,*,*),P_2=(*cn*,*edu*,*hbut*).

设系统最大模板长度为 L.在密钥模板方面,功能最强的模板是 $P=(*,*,\ldots,*)^L$(记为Λ),与之对应的密钥 SK_Λ 相当于系统级主密钥,它可以生成任意其他委托模板密钥,在本方案中称为根密钥.功能最弱的模板是 $P=\phi$,任意其他模板都可以为之生成密钥.

与密钥模板相反,在密文模板方面,功能最强的身份模板是 $P=\phi$,意味着没有用户可以解密该密文(只有根密钥才能解密).功能最弱的密文身份模板是 $P=(*,*,\ldots,*)^L$,意味着任何人都可以解密该模板对应的密文.显然,通过对密文模板的设计和控制,可以达到加密消息给不同种类和群用户的接收者.

2.2 弹性泄漏通配模板委托加密模型

定义 5. 弹性泄漏通配模板委托加密方案由 4 种概率多项式时间算法组成:Π=(*Setup*,*KeyDer*,*Enc*,*Dec*).

- $Setup(\lambda,J)$:以系统安全参数λ和密钥泄漏界 J 为输入,本算法生成系统公开参数和根密钥.系统参数 PK 公开给所有用户并应用于其他所有算法.
- $KeyDer(P_1,SK_{P_1},P_2)$:密钥委托算法以通配模板 P_1 及密钥 SK_{P_1} 以及委托模板 P_2 为输入,生成委托钥 SK_{P_2}.
- $Enc(P',M)$:加密算法以接收者模板 P'以及消息 M 为输入,输出密文 $CT_{P'}$.
- $Dec(SK_P,CT_{P'})$:解密算法以系解密密钥 SK_P 和密文 $CT_{P'}$为输入,输出消息 M.

方案一致性. 设 $f_i(\cdot)\in H$ 是满足 $\sum_i f_i(SK_P)\leqslant J$ 的函数族.若 $Match(P',P)=1$,则使用 SK_P 解密 $CT_{P'}$得到 $\hat{M}=M$ 的概率为 1,即

$$\Pr\left[\hat{M}\neq M \;\middle|\; \begin{array}{l}(PK,SK_\Lambda)\leftarrow Setup(\lambda,J)\\ Match(P',P)=1\\ SK_P\leftarrow KeyDer(\Lambda,SK_\Lambda,P)\\ \sum_i f_i(SK_P)\leqslant J\\ CT_{P'}\leftarrow Enc(P',M)\\ \hat{M}\leftarrow Dec(SK_P,CT_{P'})\end{array}\right]\leqslant \upsilon(\lambda) \tag{6}$$

2.3 弹性泄漏语义安全性

定义 6(泄漏寓言机). 泄漏寓言机 O_{Leak} 以密钥 SK_P 和泄漏界 J 为输入,对该寓言机的询问由任一多项式时间可计算的函数 $f:SK_P\rightarrow\{0,1\}^{\leqslant J}$ 发起,该寓言机计算 $f(SK_P)$,返回关于 SK_P 的最多 J 比特的信息.若累计的 $f(SK_P)$ 输出超过 J 比特,寓言机返回ϕ.

我们允许敌手对同一密钥进行多次泄漏寓言机询问,只要其所获得的泄漏总量不超过系统设定的泄漏界 J 即可.为了实现同一密钥的多次泄漏询问,可设计一个队列来记录所询问过的密钥及其泄漏总量.

在实际中应用,攻击者可以对用户的密钥在不同时间周期对同一密钥进行泄漏询问,从而避免泄漏寓言机泄漏界的控制.有效的解决措施是,在密钥的泄漏超出泄漏界之前对密钥进行更新.更新后的密钥与更新前的密钥同分布,在旧密钥被删除或不再使用的情况下,敌手对新密钥的泄漏询无法与旧密钥关联,无法生成一个合法的解密钥.

定义 7(密钥连续泄漏). 在密码方案中,一个公钥对应多个密钥且具有自身密钥更新的能力,产生一个同分布的随机化密钥,称该方案是抗连续泄漏安全的.

事实上,密钥更新只是对内部的随机数进行更新,由于密钥中隐藏的随机数在解密过程中被约掉,其值不影响密钥的解密能力.特别地,若密钥每使用一次就被更新,则称该密钥是完全连续弹性泄漏安全.密钥的完全弹性泄漏在文献[14,18]中有具体描述.

我们给出达到加密方案语义安全性(semantic security)的密文不可区分性的定义,其安全性高于单向安全性.定义 9 中的弹性泄漏语义安全性是在允许敌手进行密钥委托 O_{KeyDer} 和密钥泄漏 O_{Leak} 条件下的密文不可区分性.

定义 8(密文不可区分性). 敌手选择一接收者模板 P^*和两消息(M_0,M_1),$(M_0\neq M_1)$且$|M_0|=|M_1|$,挑战者随机抛币$\mu\in\{0,1\}$并创建密文 $CT_{P^*}=Enc(P^*,M_\mu)$. 攻击者试图猜测密文 CT_{P^*} 中的消息 M_μ.

定义 9(弹性泄漏语义安全性). 对任意多项式时间算法 $A=(A_1,A_2,A_3)$,一个层次身份通配模板加密方案 $\Pi=(Setup,KeyDer,Enc,Dec)$在泄漏函数族 $H(f\in H)$上算法 A 在图 1 中的交互模型中获得的优势 $Adv_{\Pi,A}(\lambda,J)$是可忽略的,则该方案是弹性泄漏语义安全的.

	$Exp_{\Pi,A}(\lambda,J)$
1	$(PK,SK_A)\leftarrow Setup(\lambda,J)$
2	$(M_0,M_1,P^*,state_1)\leftarrow A_1^{O_{KeyDer}(\cdot),O_{Leak}(\cdot)}(PK,P)$ with $\lvert M_0\rvert=\lvert M_1\rvert$
3	$CT^*\leftarrow Enc(P^*,M_\mu)$ with $\mu\leftarrow\{0,1\}$
4	$state_2\leftarrow A_2^{O_{KeyDer}(\cdot)}(PK,state_1,CT^*,P)$ with $Match(P^*,P)=0$
5	$(\mu'=\mu)\leftarrow A_3(state_1,state_2)$
	i) $Adv_{\Pi,A}(\lambda,J)=2\Pr[\mu'=\mu]-1$ ii) 在 A_2 过程中,敌手不允许询问泄漏预言机 O_{Leak},理由是敌手可对挑战密文 CT^* 与消息明文的关系作为泄漏函数 f,从而直接猜测其中加密的消息.

Fig.1 Model of leakage-resilient semantic security

图 1 弹性泄漏语义安全模型

在本安全模型中,敌手可以利用密钥委托寓言机 O_{KeyDer} 对非匹配身份模板获得其完整的密钥,而且可以利用泄漏寓言机 O_{Leak} 对匹配模板获得部分密钥信息.

3 方案设计

设通配模板 $P=(a_1,a_2,...,a_\ell)\in\{0,1,*\}^\ell$ $(\ell\leqslant L)$,则$\ell=|P|$表示模板的长度.把模板中所有通配符对应的元素索引集合记作 $S(P)=\{i|1\leqslant i\leqslant\ell,a_i=*\}$.同样,把模板中所有不含通配符的元素索引集合记作 $\overline{S}(P)=\{i\,|\,1\leqslant i\leqslant\ell,a_i\neq *\}$. 显然, $S(P)\cup\overline{S}(P)=\{1,2,...,\ell\}$.

3.1 设计思路

在该方案中,G_1 用于编码通配模板;G_3 用于隐藏密钥;G_2 子群在具体构造中没有使用,仅用于安全性证明.证明中,通过引入 G_2 元素来构建双系统空间,实现适应性安全性证明.为达到密钥泄漏的容忍,方案中扩展 G_1 空间到 $Q=1+2c+\dfrac{J}{\log p_2}$ 维,Q 是正交空间的维度.根据引理 1,利用 G_1 和 G_2 之间子空间的正交性,用 G_2 空间提供隐藏 G_1 空间上的任意映射,从而容忍 J 比特的密钥泄漏.

设计中,一个通配模板 $P=(a_1,a_2,...,a_\ell)\in\{0,1,*\}^\ell$ 的密钥形式下:

$$SK_P=(d_x,d_y,d_z)=\left((g_1^{\alpha_i}X_i)_{i\in[Q]},g_1^{\rho+\langle\vec{\alpha},\vec{\beta}\rangle}\cdot\prod_{i\in\overline{S}(P)}(u_{i,0}\cdot u_{i,1}^{a_i})^{r_i}\cdot Y,(g_1^{r_i}Z_i)_{i\in\overline{S}(P)}\right)\in G_{13}^{Q+1+|\overline{S}(P)|}\tag{7}$$

其中,d_x 扩展 G_1 空间到 Q 维,用于隐藏含有ρ的 $g_1^{\rho+\langle\vec{\alpha},\vec{\beta}\rangle}$. d_y 关联模板 P 中所有非通配符的元素,并通过 d_z 与模板中每一个非通配元素关联.

设计中的一个发送给身份模板 $P'=(a_1,a_2,...,a_{\ell'})$ 的消息密文结构是:

$$CT_{P'}=(c_0,c_1,c_2,c_3,c_4)=(M\cdot\Omega^s,(g_1^{s\beta_i})_{i\in[Q]},g_1^s,((u_{i,0}u_{i,1}^{a_i})^s)_{i\in\overline{S}(P')},(u_{i,j}^s)_{i\in S(P'),j\in\{0,1\}})\in G_1^{Q+1+|P'|}\times G_t\tag{8}$$

其中,c_0 用于保密消息 M,c_1 隐藏随机数,c_3 和 c_4 分别对应接收者模板 P'中的非通配元素和通配元素.在解密过程中,非通配部分(对应模板索引是 $\overline{S}(P_1)\cap\overline{S}(P_2)$)采用类似 HIBE 的方法,实现密钥组件与密文组件的双线性配对

运算,而密文模板中对应位是通配符(P_i=*).此时,模板索引是 $S(P)\cap\overline{S}(P')$.解密过程中,需要先把通配符委托为与 P_i 相等的非通配符,以实现对应组件配对运算.

3.2 方案构造

- *Setup*(λ,J)

给定安全参数λ和系统允许的弹性泄漏界J,算法首先调用双线性群生成算法 G 生成Φ=($N=p_1p_2p_3,G,G_t,e$)←$\varphi(\lambda)$,然后执行下列步骤:

1. 根据双线性群安全参数λ满足 $2^{\lambda}\leqslant p_2\leqslant 2^{\lambda+1}$,找出一个常数 c,使得 p_2^{-2c} 对安全参数λ来说在计算上是可忽略的[**].置 $Q=1+2c+\dfrac{J}{\log p_2}$;
2. 随机选取子群生成元 $g_1\in G_1,g_3\in G_3$;
3. 随机选择$\rho\in F_N$,计算$\Omega=e(g_1,g_1)^{\rho}$;对 $i\in[Q]$,随机选取,$\alpha_i,\beta_i\in F_N$;
4. 对 i=1,…,L(L 是系统允许的身份模板最大长度,即 $L=|\Lambda|$),j=0,1,随机选取 $u_{i,j}\in G_1$;
5. 对 $i\in[Q]$,随机选取 $X_i\in G_3$.同时选取 $Y\in G_3$;
6. 设置根模板密钥:

$$SK_{\Lambda}=(d_x,d_y)=((g_1^{\alpha_i}X_i)_{i\in[Q]},g_1^{\rho+\langle\vec{\alpha},\vec{\beta}\rangle}Y) \tag{9}$$

7. 公开系统参数:

$$PK=(\Phi,g_1,g_3,(g_1^{\beta_i})_{i\in[Q]},(u_{i,j})_{i\in[L],j\in\{0,1\}},\Omega) \tag{10}$$

说明:系统根密钥对应于模板Λ=(*,*,…,*)^L 的密钥,此时,$S(\Lambda)$={1,2,…,L},而 $\overline{S}(\Lambda)=\phi$ .SK_{Λ}写成一般密钥结构形式如下:

$$SK_{\Lambda}=(d_x,d_y,d_z)=\left((g_1^{\alpha_i}X_i)_{i\in[Q]},g_1^{\rho+\langle\vec{\alpha},\vec{\beta}\rangle}\cdot\prod_{i\in\overline{S}(\Lambda)}(u_{i,0}\cdot u_{i,1}^{a_i})^{r_i}\cdot Y,(g_1^{r_i}Z_i)_{i\in\overline{S}(\Lambda)}\right) \tag{11}$$

其中,d_z 组件关联模板 P 中的非通配符,在根密钥中,$d_z=\phi$.

- *KeyDer*(P_1,SK_{P_1},P_2)

设身份模板 $P_1=(a_1,a_2,...,a_{\ell})$ 对应的密钥是:

$$SK_{P_1}=(\hat{d}_x,\hat{d}_y,\hat{d}_z)=((g_1^{\hat{\alpha}_i}\hat{X}_i)_{i\in[Q]},g_1^{\rho+\langle\hat{\vec{\alpha}},\vec{\beta}\rangle}\cdot\prod_{i\in\overline{S}(P_1)}(u_{i,0}u_{i,1}^{a_i})^{\hat{r}_i}\hat{Y},(g_1^{\hat{r}_i}\hat{Z}_i)_{i\in\overline{S}(P_1)}).$$

一个 P_1 的委托模板 $P_2=(a_1,a_2,...,a_{\ell'})$ 满足 *Match*(P_2,P_1)=1.利用 SK_{P_2} 生成 P_2 的委托密钥过程如下:

1. 对 $i\in\overline{S}(P_2)$,随机选取 $r_i\in F_N,Z_i\in G_3$[***];
2. 对 $i\in[Q]$,随机选取 $X_i\in G_3$ 以及 $Y\in G_3$,然后随机选取向量 $\vec{\alpha}\in F_N^Q$;
3. 计算:

$$\begin{aligned}SK_{P_2}&=(d_x,d_y,d_z)\\&=\left((\hat{d}_{x,i}g_1^{\alpha_i}X_i)_{i\in[Q]},\hat{d}_y\cdot g_1^{\langle\vec{\alpha},\vec{\beta}\rangle}\cdot\prod_{i\in\overline{S}(P_2)}(u_{i,0}u_{i,1}^{a_i})^{r_i}Y,(\hat{d}_{z_i}g_1^{r_i}Z_i)_{i\in\overline{S}(P_1)\cap\overline{S}(P_2)}\right)\\&=\left((g_1^{\alpha_i}X_i)_{i\in[Q]},g_1^{\rho+\langle\vec{\alpha}',\vec{\beta}\rangle}\cdot\prod_{i\in\overline{S}(P_2)}(u_{i,0}u_{i,1}^{a_i})^{r_i}Y',(g_1^{r_i}Z_i)_{i\in\overline{S}(P_2)}\right)\end{aligned} \tag{12}$$

[**] 根据 NIST 推荐安全标准,2011 年~2030 年期间,AES-112 比特标准长度是足够安全的,椭圆曲线双线群对应 G_1 长度是 224 比特,G_t 长度是 2 048 比特.在本文方案中,要求 N 不能被因式分解,在对应 AES-112 比特对称密钥安全标准中,N=2048,此时,G_1 长度是 2 048 比特,G_t 长度是 4 096 比特.此时,p_2 长度是 682~683 比特,为达到 p_2^{-2c} 可忽略,此时, $c=-\dfrac{\upsilon(\cdot)}{2|p_2|}$.

[***] 子群 G_3 的生成元 g_3 是公开的,G_3 中的随机元素可以先随机选取 $t\in F_N$,然后计算 $g_3^t \bmod N$ 得到 G_3 中的随机元素.由于 N 是 3 个不同素数 p_1,p_2 和 p_3 之积,根据中国剩余定理, $g_3^t \bmod N$ 后的元素位于 G_3 子群中.

这里, $r_i=\hat{r}_i+r_i, X_i=\hat{X}_iX_i, Y'=\hat{Y}Y, Z_i=\hat{Z}_iZ_i, \vec{\alpha}'=\vec{\hat{\alpha}}+\vec{\alpha}$.由于这些随机数是均匀分布的,因此,委托密钥 SK_{P_2} 与其父密钥 SK_{P_1} 具有相同分布特性.

- $Enc(P',M)$

为加密消息 M 给身份模板 $P'=(a_1,a_2,...,a_\ell)$,加密算法执行:随机选取 $s\in F_N$,计算密文 $CT_{P'}=(c_0,c_1,c_2,c_3,c_4)$.即

$$CT_{P'}=(c_0,c_1,c_2,c_3,c_4)=(M\cdot\Omega^s,(g_1^{s\beta_i})_{i\in[Q]},g_1^s,((u_{i,0}u_{i,1}^{a_i})^s)_{i\in\overline{S}(P')},(u_{i,j}^s)_{i\in S(P'),j\in\{0,1\}}) \tag{13}$$

- $Dec(SK_P,CT_{P'})$

若 $Match(P',P)=0$,返回⊥.密钥模板 P 中非通配符部分与密文模板 P'中非通配符部分相等,根据模板定义,模板索引为 $\overline{S}(P)\cap\overline{S}(P')$ 对应位要相等,类似 HIBE 的解密思路,利用对应组件作配对运算.密钥模板 P_i 位是非通配符($P_i\neq$*),而密文模板对应位是通配符(P_i=*),此时,模板索引是 $S(P)\cap\overline{S}(P')$.要把通配符委托为与 P_i 相等的非通配符,以实现对应组件配对运算.解密过程计算如下:

$$A=\prod_{i\in\overline{S}(P)\cap\overline{S}(P')}e(d_{z_i},c_{3,i})\times\prod_{i\in S(P)\cap\overline{S}(P')}e(d_{z_i},c_{4,i,0}\cdot c_{4,i,1}^{a_i}) \tag{14}$$

$$B=\frac{e(d_y,c_2)}{\prod_{i\in[Q]}e(d_{x,i},c_{1,i})} \tag{15}$$

$$M\leftarrow c_0A/B \tag{16}$$

3.3 解密一致性

$$\begin{aligned}A&=\prod_{i\in\overline{S}(P)\cap\overline{S}(P')}e(d_{z_i},c_{3,i})\times\prod_{i\in S(P)\cap\overline{S}(P')}e(d_{z_i},c_{4,i,0}\cdot c_{4,i,1}^{a_i})\\&=\prod_{i\in\overline{S}(P)\cap\overline{S}(P')}e(g_1^{r_i}Z_i,(u_{i,0}\cdot u_{i,1}^{a_i})^s)\times\prod_{i\in S(P)\cap\overline{S}(P')}e(g_1^{r_i}Z_i,u_{i,0}^s\cdot u_{i,1}^{a_is})\\&=\prod_{i\in\overline{S}(P)\cap\overline{S}(P')}e(g_1^{r_i},(u_{i,0}\cdot u_{i,1}^{a_i})^s)\times\prod_{i\in S(P)\cap\overline{S}(P')}e(g_1^{r_i},u_{i,0}^s\cdot u_{i,1}^{a_is})\\&=\prod_{i\in\overline{S}(P')}e(g_1^{r_i},u_{i,0}u_{i,1}^{a_i})^s\end{aligned} \tag{17}$$

$$\begin{aligned}B&=\frac{e(d_y,c_2)}{\prod_{i\in[Q]}e(d_{x,i},c_{1,i})}\\&=\frac{e(g_1^{\rho+\langle\vec{\alpha},\vec{\beta}\rangle}\cdot\prod_{i\in\overline{S}(P')}(u_{i,0}u_{i,1}^{a_i})^{r_i}Y,g_1^s)}{\prod_{i\in[Q]}e(g_1^{\alpha_i}X_i,g_1^{s\beta_i})}\\&=\frac{e(g_1^{\rho+\langle\vec{\alpha},\vec{\beta}\rangle}\cdot\prod_{i\in\overline{S}(P')}(u_{i,0}u_{i,1}^{a_i})^{r_i},g_1^s)}{\prod_{i\in[Q]}e(g_1^{\alpha_i},g_1^{s\beta_i})}\\&=\frac{e(g_1^{\rho},g_1^s)e(g_1^{\langle\vec{\alpha},\vec{\beta}\rangle},g_1^s)e(\prod_{i\in\overline{S}(P')}(u_{i,0}u_{i,1}^{a_i})^{r_i},g_1^s)}{e(g_1,g_1)^{s\sum_{i\in[Q]}\alpha_i\beta_i}}\\&=\frac{e(g_1,g_1)^{\rho s}e(g_1^{\sum_{i\in[Q]}\alpha_i\beta_i},g_1^s)\prod_{i\in\overline{S}(P')}e((u_{i,0}u_{i,1}^{a_i})^{r_i},g_1^s)}{e(g_1,g_1)^{s\sum_{i\in[Q]}\alpha_i\beta_i}}\\&=A\cdot e(g_1,g_1)^{\rho s}\end{aligned} \tag{18}$$

4 安全性证明

4.1 数学难题假设

为了证明所设计方案的安全性,本文使用如下基于合数阶(子)群判定问题,该假设在文献[8]中已作分析.

设 $\Phi=(N=p_1p_2p_3,G=G_1\times G_2\times G_3,G_t,e)$是阶为 N的双线性群,其中,p_1,p_2 和 p_3 是互素的大素数,满足 $2^\lambda\leqslant p_2\leqslant 2^{\lambda+1}$.

下列假设在给定部分已知信息的情况下,猜出μ的概率优势对于安全参数λ是可忽略的,即$\upsilon(\lambda)\approx 0$.

数学假设 1. 给定双线性群Φ以及 g_1,g_3,区分子群 G_1 和 G_{12} 中的元素是困难的,即

$$\Pr\left[\mu=0\left|\begin{array}{l} g_1\in G_1, g_3\in G_3 \\ \mu\leftarrow\{0,1\} \\ T_0\leftarrow G_1, T_1\leftarrow G_{12} \\ T_\mu=\mu(T_0-T_1)+T_1 \end{array}\right.\right]=\frac{1}{2}+\upsilon(\cdot).$$

数学假设 2. 给定双线性群Φ,g_1,g_3,X_1X_2 和 Y_2Y_3,区分子群 G_{12} 中随机元素和 G 中的元素是困难的,即

$$\Pr\left[\mu=0\left|\begin{array}{l} g_1\in G_1, g_3\in G_3 \\ X_1X_2\in G_{12}, Y_2Y_3\in G_{13} \\ \mu\leftarrow\{0,1\} \\ T_0\leftarrow G_{13}, T_1\leftarrow G \\ T_\mu=\mu(T_0-T_1)+T_1 \end{array}\right.\right]=\frac{1}{2}+\upsilon(\cdot).$$

数学假设 3. 给定双线性群Φ,g_1,g_2,g_3 以及 $g_1^\rho X_2$ 和 $g_1^s Y_2$,区分判断 $e(g_1,g_1)^{\rho s}$ 与 G_t 中的随机元素是困难的,即

$$\Pr\left[\mu=0\left|\begin{array}{l} g_1\in G_1, g_2\in G_2 \\ g_3\in G_3, g_1^\rho X_2, g_1^s Y_2\in G_{12} \\ \mu\leftarrow\{0,1\} \\ T_0=e(g_1,g_1)^{\rho s}, T_1\leftarrow G_t \\ T_\mu=\mu(T_0-T_1)+T_1 \end{array}\right.\right]=\frac{1}{2}+\upsilon(\cdot).$$

4.2 抗泄漏安全性证明

4.2.1 半功能密钥与密文

采用双系统技术,我们设计半功能化的密钥和密文形式.基本方法是,对原来密钥和密文组件乘以 G_2 中的随机元素(G_2 在实际方案中没有涉及,仅用于安全性证明中设计半功能化密文或密钥).

- **半功能密钥**

设 $SK_P=(d_x,d_y,d_z)$是 *KeyDer* 算法生成的正常形态密钥.随机选取 $k\in F_N$.对 $i\in[Q]$,随机选择$\delta_i\in F_N$;对 $i\in\overline{S}(P)$,随机选择 $z_i\in F_N$,计算:

$$SK_P=(\hat{d}_x,\hat{d}_y,\hat{d}_z)=((d_{x_i}\cdot g_2^{\delta_i})_{i\in[Q]},d_y g_2^k,(d_{z_i}\cdot g_2^{z_i})_{i\in\overline{S}(P)}).$$

- **半功能密文**

设 $CT_P=(c_0,c_1,c_2,c_3,c_4)$是调用 *Enc* 算法生成的正常形态密文.随机选取 $x\in F_N$.对 $i\in[Q]$,随机选择$\theta_i\in F_N$;对 $i\in\overline{S}(P)$,选取 $t_i\in F_N$;对 $i\in S(P),j\in\{0,1\}$,随机选择 $\hat{z}_{i,j}\in F_N$:

$$CT_P=(\hat{c}_0,\hat{c}_1,\hat{c}_2,\hat{c}_3,\hat{c}_4)=(c_0,(c_{1,i}\cdot g_2^{\theta_i})_{i\in[Q]},c_2\cdot g_2^x,(c_{3,i}\cdot g_2^{t_i})_{i\in\overline{S}(P)},(c_{4,i,j}\cdot g_2^{\hat{z}_{i,j}})_{i\in S(P),j\in\{0,1\}}).$$

一个半功能密钥要成功地解密一个半功能密文,除了密文模板 P'与密钥模板 P 满足 $Match(P',P)=1$ 外,还要求 G_2 部分可以约去,即,利用半功能密钥 SK_P 和半功能密文 $CT_{P'}$代入公式(14)~公式(16)时,使得:

$$e(g_2,g_2)^{\langle\vec{\delta},\vec{\theta}\rangle}e(g_2,g_2)^{x-k}e(g_2,g_2)^{\prod_{i\in S(P)\cap\overline{S}(P')}z_i-t_i}e(g_2,g_2)^{\prod_{i\in\overline{S}(P)\cap\overline{S}(P')}z_i-\hat{z}_{i,0}\hat{z}_{i,1}^{a_i}}=1 \tag{19}$$

即

$$\langle\vec{\delta},\vec{\theta}\rangle+x-k+\prod_{i\in S(P)\cap\overline{S}(P')}(z_i-t_i)+\prod_{i\in\overline{S}(P)\cap\overline{S}(P')}(z_i-\hat{z}_{i,0}\hat{z}_{i,1}^{a_i})=0 \bmod p_2 \tag{20}$$

根据双系统加密的性质,攻击者在未知解密密钥的情况下,敌手能够成功地解密挑战密文的优势等价于一个半功能密钥成功解密一个半功能密文的概率优势.在等式(20)中,除 a_i 外,其他变量都是从 F_N 中均匀选取的,使得该等式成立的概率是 $1/p_2$.

接下来我们考虑更特殊的情况,即,在敌手获得部分解密密钥(密钥弹性泄漏)的情况下,是否敌手存在解密挑战密文的优势.若一个半功能密钥可以成功地解密一个半功能密文,则称该密钥是支配型半功能的;否则,称该密钥是真半功能的.为此,我们要证明的是:在敌手获得部分泄漏的情况下,构造一个支配型半功能密钥的概率优势是可忽略的.

4.2.2 不可区分性游戏

为了给出形式化的安全性证明,我们使用一系列游戏,用于实现把正常形式的询问密钥和挑战密文转换为半功能形式的密钥和密文:

1. Γ_{Real}:本游戏中密文和密钥均为正常形式,即,密文和密钥由Π算法生成,敌手执行安全性的弹性泄漏语义安全模型.
2. Γ_{CSF}:本游戏与Γ_{Real}游戏的区别在于,在挑战阶段的输出用半功能密文 CT_P.
3. Γ_{KSF_j}:设 q 是敌手在安全游戏中对密钥的最大询问次数.在本游戏中,密文仍是半功能化的;同时,对$\leqslant j$ 的密钥是半功能密钥,而$>j$ 的密钥是正常形式的密钥,对第 j 个密钥是加入安全假设的实例.显然,当 j=0 时,$\Gamma_{KSF_0}=\Gamma_{CSF}$;$j$=$q$ 时,Γ_{KSF_j} 中生成的密文和密钥都是半功能的.当 $1\leqslant j\leqslant q$ 时,本游戏中密钥中前 $j-1$ 个是半功能的,后面的都是正常密钥.我们证明,对所有 j,Γ_{KSF_j} 与 $\Gamma_{KSF_{j+1}}$ 在计算上是不可区分的.
4. Γ_{LR_j}:本游戏与 Γ_{KSF_j} 的区别在于,允许敌手对满足匹配密文的模板作泄漏询问 O_{Leak},其泄漏量最大是 J 比特.我们证明:敌手在该游戏中,在已获得部分匹配密钥泄漏的条件下,不能成功构造成支配型密钥.
5. Γ_{CM}:本游戏在 Γ_{LR_q} 的基础上,将密文中的 c_0 组件用 G_t 的随机元素替换.

在第 1 个游戏中,密钥和密文均是正常形式(由第 3 节的算法生成);而最后,游戏Γ_{CM}中,密钥和密文均是半功能化的,且消息组件 c_0 是 G_t 中的随机元素.对于最后一个游戏,密钥和密文全是半功能化,利用双系统性质,半功能密钥不能解密一半功能密文.而对于半功能化生成算法中未变化的组件 c_0,与一个随机元素不可区分.如果我们所设计的一系列游戏在计算上是不可区分的,这样反推第 1 个游戏中的密文获得对询问密钥情况来说则无法解密.

4.2.3 形式化证明

为了形式化证明本文方案的安全性,本节证明游戏之间在安全参数上是概率不可区分的.而根据双系统加密系统的定理,对于半功能密钥解密,真半功能挑战密文是不可行的.我们得出如下定理:

定理 1(抗泄漏语义安全性). 一个层次通配模板加密方案Π=(*Setup*,*KeyDer*,*Enc*,*Dec*),敌手可以询问对任意密钥(匹配和非匹配密钥)上的关于泄漏函数 $f\in H$ 上的最多 J 比特泄漏,以及非匹配挑战密钥的密钥提取询问,在安全数学假设 1~假设 3 下,若敌手在游戏Γ_{Real},Γ_{CSF},Γ_{KSF_j},Γ_{LR_j} 和Γ_{CM}之间是安全参数λ上计算不可区分的,则该方案是(λ,J)-弹性泄漏安全语义的.

证明:我们采用不可区分证明的引理(2)~引理(5)来证明方案的安全性.Γ_{Real}是本文提出构造方案(密文在 G_1 子群,而密钥在 G_{13} 子群).Γ_{CSF} 表明,敌手无法区分半功能挑战密文和正常形态密文.Γ_{KSF_j} 用于描述半功能密钥不能解密半功能密文.Γ_{LR_j} 用于描述敌手在获得匹配模板泄漏询问 O_{Leak} 的基础上,不能将一半功能化密钥转换成支配型半功能密钥.Γ_{CM} 描述消息隐藏组件与随机元素不可区分.从敌手的角度来看,Γ_{CM} 中的元素是随机化的,因此无法解密挑战密文. □

接下来给出引理(2)~引理(5)的详细证明.

引理 2. 若安全假设 1 存在,则任何多项式时间内的算法 A=(A_1,A_2,A_3)对Γ_{Real}和Γ_{CSF}是计算上不可区分的.

证明:假设一种多项式时间算法 A 以不可忽略的优势区分Γ_{Real}和Γ_{CSF},我们可以构建一种算法 B 作为模拟器,以相同的优势解决假设 1 难题.当 B 收到假设 1 的实例后,其目标是猜测元素 $T\in G_1$ 还是 $T\in G_{12}$.为此,B 扮演模拟器并回答 A 的询问及挑战.

在系统初始化阶段,B 选择使得 p_2^{-2c} 可忽略的 c,计算 $Q=1+2c+\frac{J}{\log p_2}$. 然后随机选取生成元 $g_1\in G_1, g_3\in G_3$. 对 $i\in[J], j\in\{0,1\}$,随机选取 $u_{i,j}\in G_1$.随机选取 $X_1,\ldots,X_Q,Y\in G_3$.在有限域 F_N 上随机选取 $\rho,\alpha_1,\beta_1,\ldots,\alpha_Q,\beta_Q\in F_N$.置系统参数 $PK=(\Phi,g_1,g_3,(g_1^{\beta_i})_{i\in[Q]},(u_{i,j})_{i\in[L],j\in\{0,1\}},\Omega=e(g_1,g_1)^{\rho})$,并发送给 A.由于 B 知道 $\vec{\alpha}$ 和 ρ,可以生成系统根密钥 SK_A,并为任何子模板生成委托密钥;同时,可以回答敌手 A 的密钥委托和密钥泄漏询问.

当 A 请求挑战,并提交给 B 两个挑战消息 (M_0,M_1) 及一个挑战通配模板 P^* 时,B 随机选择 $\mu\leftarrow\{0,1\}$,计算并返回挑战密文 $CT_{P^*}=(M_\mu e(T,g^{\rho}),(T^{\beta_i})_{i\in[Q]},T,(u_{i,j}^{a_i^*})_{i\in\bar{S}(P^*)},(u_{i,j})_{i\in S(P^*),jin\{0,1\}})$.

B 知道根密钥,在询问 2 阶段仍然可以回答 A 的密钥提取询问.在输出阶段,A 输出对密文中消息挑战消息 M_μ 的猜测 μ'.B 以相同的输出 μ' 作为对假设 1 的猜测:若 $\mu'=0$,则 $T\in G_1$;若 $\mu'=1$,则 $T\in G_{12}$.显然,若 $T\in G_1$,则密文 CT_{P^*} 是正常形态的(密文中没有 G_2 部分),此时,B 可以正确模拟 Γ_{Real}.若 $T=g_1^{n_1}g_2^{n_2}\in G_{12}$,则 CT_{P^*} 是半功能化的.对敌手来说,密文组件中 G_2 部分不为 1,此时可以正确模拟 Γ_{CSF}.若算法 A 可以成功输出 $\mu'=\mu$,则 B 以 μ' 作为安全假设的应答.因此,当安全假设 1 存在时,Γ_{Real} 和 Γ_{CSF} 在计算上是不可区分的. □

引理 3. 若假设 2 存在,则在任意多项式时间内,算法 $A=(A_1,A_2,A_3)$ 对 $1\leqslant j\leqslant q-1$, Γ_{KSF_j} 和 $\Gamma_{KSF_{j+1}}$ 是计算上不可区分的.

证明:显然,当 $j=0$ 时, $\Gamma_{KSF_0}=\Gamma_{CSF}$.若存在一种多项式时间的算法 A 以不可忽略的优势区分 Γ_{KSF_j} 和 $\Gamma_{KSF_{j+1}}$,则可以构建一种算法 B,以相同的优势解决安全假设 2.B 的目标是:收到假设 2 的实例 $(\Phi,g_1,g_3,X_1X_2,Y_2Y_3,T)$ 后,推断 $T\in G_{13}$ 还是 $T\in G$.B 所要做的工作是:当 $T\in G_{13}$ 时,成功模拟 Γ_{KSF_j};当 $T\in G$ 时,成功模拟 $\Gamma_{KSF_{j+1}}$.

初始化阶段,B 选择使得 p_2^{-2c} 可忽略的 c,计算 $Q=1+2c+\frac{J}{\log p_2}$. 随机选取 $g_1,u_{1,0},u_{1,1},\ldots,u_{L,0},u_{L,1}\in G_1, g_3\in G_3$. 在有限域 F_N 上随机选取 $\rho,\alpha_1,\beta_1,\ldots,\alpha_Q,\beta_Q\in F_N$.置系统参数 $PK=(\Phi,g_1,g_3,(g_1^{\beta_i})_{i\in[Q]},(u_{i,j})_{i\in[L],j\in\{0,1\}},\Omega=e(g_1,g_1)^{\rho})$.

对于 A 的密钥询问,B 的回答分为以下 3 种情况:

1. 对前面 $j-1$ 个密钥,B 以半功能化密钥形式作应答:

$$SK_P=\left((g_1^{\alpha_i}X_iX_i)_{i\in[Q]},g_1^{\rho+\langle\vec{\alpha},\vec{\beta}\rangle}\cdot\prod_{i\in\bar{S}(P)}(u_{i,0}u_{i,1}^{a_i})^{r_i}YY',(g_1^{r_i}Z_iZ_i)_{i\in\bar{S}(P)}\right),$$

其中, $X_i,Y,Z_i\in G_3, X_i',Y',Z_i'\in G_2$;

2. 对第 j 个密钥,B 以挑战 T 来生成密钥:

$$SK_P=\left((T^{\alpha_i})_{i\in[Q]},T^{\rho+\langle\vec{\alpha},\vec{\beta}\rangle}\cdot\prod_{i\in\bar{S}(P)}(u_{i,0}u_{i,1}^{a_i})^{r_i},(T^{r_i})_{i\in\bar{S}(P)}\right);$$

3. 从 $j+1$ 密钥开始,B 输出正常形态密钥:

$$SK_P=\left((g_1^{\alpha_i}X_i)_{i\in[Q]},g_1^{\rho+\langle\vec{\alpha},\vec{\beta}\rangle}\cdot\prod_{i\in\bar{S}(P)}(u_{i,0}u_{i,1}^{a_i})^{r_i}Y,(g_1^{r_i}Z_i)_{i\in\bar{S}(P)}\right).$$

在挑战阶段,对挑战的通配模板 $P^*=(a_1^*,a_2^*,...,a_\ell^*)$,输出半功能挑战密文:

$$CT_{P^*}=(M_\mu\cdot e(X_1X_2,g_1^{\rho}),((X_1X_2)^{\beta_i})_{i\in[Q]},(X_1X_2),(u_{i,0}u_{i,1}^{a_i^*})_{i\in\bar{S}(P^*)},(u_{i,j})_{i\in S(P^*),j\in\{0,1\}}).$$

使用一个正常密钥解密半功能挑战密文,若 $Match(P^*,P)=1$ 且 $T\in G_{13}$,则能正常解密,此时成功模拟 Γ_{KSF_j}.使用一个半功能密钥来解密半功能挑战密文,当 $Match(P^*,P)=1$ 且 $T=g_1^{n_1}g_2^{n_2}g_3^{n_3}\in G(=G_{123})$ 时,采用 Dec 算法进行配对运算时,由于密文和密钥都有 g_2 部分,配对计算产生额外的 g_2 相关的部分.设 $X_1X_2=g_1^{m_1}g_2^{m_2}$,则解密配对运算后 G_2 部分是 $e(g_2,g_2)^{m_2-n_2+m_2n_2\sum_{i\in[Q]}\alpha_i\beta_i}$.若敌手成功解密 CT_{P^*},则 $m_2-n_2+m_2n_2\sum_{i\in[Q]}\alpha_i\beta_i=0 \bmod p_2$,而 m_2 和 n_2 是 F_{p_2} 上均匀分布的,此时成功模拟 $\Gamma_{KSF_{j+1}}$.若算法 A 可以成功地区分 Γ_{KSF_j} 和 $\Gamma_{KSF_{j+1}}$,则 B 可以以 A 的区分输出优势解决安全假设 2 的判定. □

引理 3 证明了算法 A 在非匹配密钥泄漏条件下无法区分 Γ_{KSF_j} 和 $\Gamma_{KSF_{j+1}}$. 接下来我们证明:对于匹配密钥 SK_P 满足 $Match(P^*,P)=1$,算法 A 获得部分密钥泄漏的条件下,仍不能将一个半功能密钥 SK_P 转换为可以解密挑战密文 CT_{P^*} 的支配型半功能密钥.该引理如下:

引理 4. 设系统泄漏界 $J=(Q-1-2c)\log p_2,c$ 是一个正整数，使得 $p_2^{-2c}\leqslant\upsilon(\lambda)$. 对任意一种多项式时间算法 A,在 Γ_{KSF_j} 游戏中把第 j 个密钥 SK_P 关联到匹配挑战密文通配模板 CT_{P^*}, 即 $Match(P^*,P)=1$,此时,A 将这个半功能密钥转换成支配型半功能化密钥的概率优势是可忽略的.

证明:假设一种多项式时间算法 A 以不可忽略的概率优势实现支配型半功能密钥转换,我们可以构造一种算法 B,以相同的优势区分两个分布 $(\vec{\Delta},f(\vec{\pi}))$ 和 $(\vec{\Delta},f(\vec{\pi}'))$, 而这两个分布在引理 1 中已证明是不可区分的,并在推论 1 中给予进一步的细化.在推论 1 中,B 首先置 $m=Q+1,d=1,p=p_2$(其中,p_2 是 N 的一个素数因子).算法 B 的目标是,借助 A 的不可忽略的转换能力来区分 $(\vec{\Delta},f(\vec{\pi}))$ 和 $(\vec{\Delta},f(\vec{\pi}'))$.

B 模拟游戏 Γ_{KSF_j} 过程如下:首先运行 Setup 算法生成根密钥 MSK_A和公开参数 PK.显然,由于知道系统根密钥,B 可以回答敌手的任何询问,包括密钥提取和泄漏询问,但不能获得对挑战模板 P^*相匹配的模板密钥提取询问,即,所询问的委托密钥 $SK_P=KeyDer(\Lambda,SK_\Lambda,P)$满足 $Match(P^*,P)\neq1$(否则,A 获得了完整的解密钥).我们允许 A 对任何满足 $Match(P^*,P)=1$ 的模板 P 请求泄漏询问.

对于匹配挑战模板 P^*(即 $Match(P^*,P)=1$)的密钥泄漏询问,B 应答如下:设 $f\in H$ 是个概率多项式时间的泄漏函数,输入域是 $F_{p_2}^{Q+1}$, 输出域大小是 $\{0,1\}^J$.B 收到推论 1 的输出 $(\vec{\Delta},f(\vec{\pi}))$, 这里, $\vec{\pi}$ 是 $\vec{x}$ 或 $\vec{x}'$. B 使用分布 $f(\vec{\pi})$ 回答 A 的第 j 个密钥泄漏询问:

首先根据KeyDer算法生成一个正常形态的密钥 SK_P,然后随机选取 $r\in F_{p_2},\vec{\theta}\in F_{p_2}^{|\overline{S}(P)|}$, 置半功能化密钥中的 G_2 子群部分是:

$$(\underbrace{b_1,...,b_Q}_{d_x},\underbrace{b_{Q+1}+r}_{d_y},\underbrace{\theta_1,...,\theta_{|\overline{S}(P)|}}_{d_z}).$$

A 请求询问挑战模板 P^*,若第 j 模板不匹配 P^*,即 $Match(P^*,P)\neq1$,B 模拟失败,并随机输出 $\vec{\pi}$ 作为对 $\vec{\Delta}$ 是否正交的猜测;否则,第 j 模板满足 $Match(P^*,P)=1$.设 $k=|\overline{S}(P^*)|$,B 选择 $t_1,...,t_k,z_{1,0},z_{1,1},...,z_{k,0},z_{k,1}\in F_{p_2}$,满足:

$$r\Delta_{Q+1}-\prod_{i\in S(P)\cap\overline{S}(P^*)}(\theta_i-t_i)-\prod_{i\in\overline{S}(P)\cap\overline{S}(P^*)}(\theta_i-z_{i,0}z_{i,1}^{a_i^*})=0 \bmod p_2 \tag{21}$$

接着调用 Enc 算法创建模板 P^*的密文,然后以 $((\Delta)_{i\in[Q]},\Delta_{Q+1},\vec{t},\vec{z})$ 作为挑战密文的半功能因子,即, CT_{P^*} 的 G_2 部分是:

$$(0,\underbrace{\Delta_1,...,\Delta_Q}_{c_1},\underbrace{\Delta_{Q+1}}_{c_2},\underbrace{t_1,...,t_k}_{c_3},\underbrace{z_{1,0},z_{1,1},...,z_{k,0},z_{k,1}}_{c_4}).$$

若向量 $\vec{\Delta}$ 与 $\vec{b}$ 正交,即 $\langle\vec{\Delta},\vec{b}\rangle=0$,则第 j 个密钥是支配型半功能的;若 $\vec{\Delta}$ 与 $\vec{b}$ 不正交,则挑战密钥是真半功能的.半功能密钥和半功能密文配对运算后,并根据公式(21)结果,$e(g_2,g_2)$部分的指数是:

$$\begin{aligned}
&\sum_{i\in[Q]}\Delta_i b_i+\Delta_{Q+1}(b_{Q+1}+r)-\prod_{i\in S(P)\cap\overline{S}(P^*)}(\theta_i-t_i)-\prod_{i\in\overline{S}(P)\cap\overline{S}(P^*)}(\theta_i-z_{i,0}z_{i,1}^{a_i^*})\\
&=\prod_{i\in[Q]}\Delta_i b_i+\Delta_{Q+1}b_{Q+1}+\Delta_{Q+1}r-\prod_{i\in S(P)\cap\overline{S}(P^*)}(\theta_i-t_i)-\prod_{i\in\overline{S}(P)\cap\overline{S}(P^*)}(\theta_i-z_{i,0}z_{i,1}^{a_i^*})\\
&=\prod_{i\in[Q]}\Delta_i b_i+\Delta_{Q+1}b_{Q+1}=\sum_{i\in[Q+1]}\Delta_i b_i\\
&=\langle\vec{\Delta},\vec{b}\rangle \bmod p_2
\end{aligned} \tag{22}$$

显然,若公式(22)为 0,即向量 $\vec{\Delta}$ 与 $\vec{b}$ 正交,则解密配对运算后 $e(g_2,g_2)^0=1$,该密钥是支配型半功能的;否则, $\langle\vec{\Delta},\vec{b}\rangle\neq0$,该密钥是真半功能的.若 A 可以将一半功能密钥转换为支配型半功能的,则 B 以算法 A 的输出区分两个分布 $(\vec{\Delta},f(\vec{\pi}))$ 和 $(\vec{\Delta},f(\vec{\pi}))$. 这与引理 1 及其推论 1 矛盾.因此,不存在多项式时间算法构建支配型半功能密钥. □

引理 5. 若安全假设 3 存在,任何多项式时间内的算法 $A=(A_1,A_2,A_3)$区分 Γ_{LR_q} 和Γ_{CM}是计算上不可区分的.

证明:设一种多项式时间的算法 A 以不可忽略的优势区分 Γ_{LR_q} 和Γ_{CM},我们构建算法 B,以相同的优势解决安全假设 3 的判定.当收到假设 3 的实例 $(\Phi,g_1,g_2,g_3,g_1^{\rho}X_2,g_1^2Y_2,T)$ 时,B 的目标是输出 $T=e(g^{\alpha},g^{s})$还是 T 只能为 G_t 中的随机元素的猜测.

初始化阶段,B 选择使得 p_2^{-2c} 可忽略的 c,计算 $Q=1+2c+\dfrac{J}{\log p_2}$.然后随机选取 $g_1,u_{1,0},u_{1,1},\ldots,u_{L,0},u_{L,1}\in G_1$, $g_2\in G_2,g_3\in G_3$.在有限域 F_N 上,随机选取$\alpha_1,\beta_1,\ldots,\alpha_Q,\beta_Q\in F_N$.置

$$PK=(\Phi,g_1,g_3,(g_1^{\beta_i})_{i\in[Q]},(u_{i,j})_{i\in[L],j\in\{0,1\}},\Omega=e(g_1,g_1)^{\rho}).$$

值得注意的是,虽然 B 不知道ρ,但可以利用 $g_1^{\rho}X_2$ 来计算,即

$$\Omega=(g_1,g_1^{\rho}X_2)=e(g_1,g_1)^{\rho}.$$

在密钥询问阶段,B 生成并回答半功能密钥:

$$SK_P=\left((g_1^{\alpha_i}X_i)_{i\in[Q]},(g_1^{\rho}X_2)g_1^{\langle\vec{\alpha},\vec{\beta}\rangle}\cdot\prod_{i\in\bar{S}(P)}(u_{i,0}u_{i,1}^{a_i})^{r_i}Y,(g_1^{r_i})_{i\in\bar{S}(P)}\right).$$

在挑战阶段,算法 A 提交两个挑战的消息(M_0,M_1)及一挑战模板 $P^*=(a_1^*,a_2^*,\ldots,a_{\ell}^*)$, B 随机选择$\mu\leftarrow\{0,1\}$,生成半功能挑战密文:

$$CT_{P^*}=(M_{\mu}T,(g_1^{\beta_i})_{i\in[Q]},(g_1^{s}Y_2),(u_{i,0}u_{i,1}^{a_i^*})_{i\in\bar{S}(P^*)},(u_{i,j})_{i\in S(P^*),j\in\{0,1\}}).$$

若 $T=e(g^{\rho},g^{s})$, CT_{P^*} 是半功能化的,而 SK_P 是支配型半功能密钥,可以成功解密 CT_{P^*}, B 成功地模拟游戏 Γ_{LR_q}. 当 T 是 G_t 中的随机元素时,$c_0=M_{\mu}T$ 是 G_t 中完全随机的元素,此时,密文是随机消息的半功能密文,B 成功模拟游戏Γ_{CM}.若算法 A 以不可忽略的优势猜测 $T=e(g_1^{\rho},g_1^{s})$ 还是 T 为随机的 G_t 元素,则 B 以算法 A 的输出解决安全假设 3 的判定. □

5 泄漏容忍性能与应用实例

5.1 应用实例

在生物特征数据(如指纹、眼膜、声音等)作为用户身份时,可为产生具有高熵的秘密信息提供一个广泛的来源,但由于其存在一定的不可精确再生性[26],因此采用通配身份模板可有效解决.例如,对于一个指纹信息,我们重点关注关键点的数据,其他部分可以以通配符代替.只要包括关键点的信息的模板匹配,我们可以认为两个指纹数据是匹配的.在多次验证用户生物特征数据时,只需测试是否与生物特征模板匹配即可.

实际应用中,在不同安全需求中有不同的模板处理.例如,在出入境管理中,指纹模板需要双手的指纹数据;而应用于一般的公务处理时,如门禁认证和计算机登录认证等,只需要一只手的指纹数据.为了实现密钥的可重用性和管理的方便性,我们可以生成双手(左手 L 和右手 R)的指纹模板,并以关键点数据作为模板中非通配项,而其他点数据作为通配项.一个数据 M 加密时,指定需要双手的指纹密钥才能解密时,$CT_{P'}$中加密模板 $P'=L||R$. 这样,只有解密者用双手指纹模板密钥才能解密消息(见图 2 右上解密部分).在一些需要委托解密功能中,可以通过 KeyDer 算法生成一委托密钥 SK_R 或 SK_L,受委托者只能实现对 $P'=R$(或 $P'=L$)的指纹模板密文的解密功能(图 2 右下解密部分).

显然,在密钥委托过程中,要保证委托密钥 SK_P 不能被泄漏,这也是传统方案必须在密钥分发过程中存在安全的秘密信道的原因.同时,加密算法和密钥在执行时都必须在调入内存,攻击者通过冷启动攻击也可能获得有关密钥的部分信息.在传统的非抗弹性泄漏的方案中,若解密钥有任何泄漏,则可证明安全将失效.而本文方案允许密钥在最多存在 J 比特泄漏的情况下,方案仍是安全的.

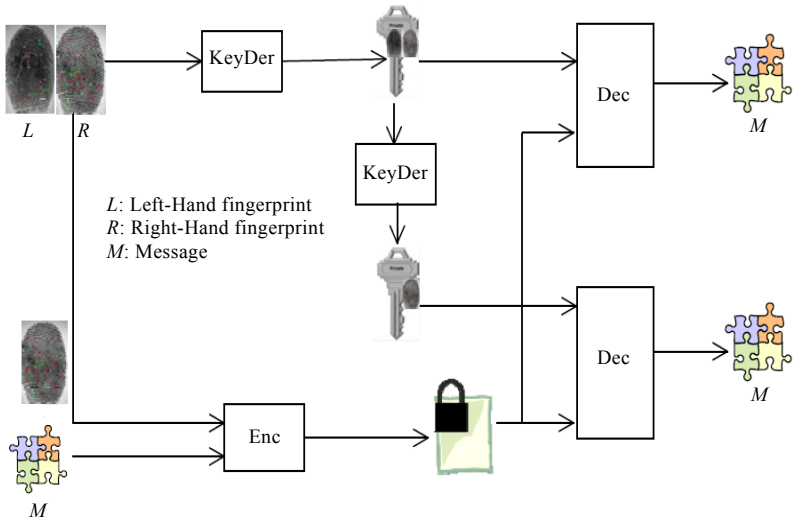


Fig.2 Application scenario

图 2 应用实例

5.2 性能分析

我们以目前足够安全的 AES-112 安全标准来分析和讨论所提出方案的弹性泄漏安全性能.

G 群是椭圆曲线上的群,对应在 AES-112 安全标准下 N=2048 比特,同时,$|G|$=2048 比特,$|G_t|$=4096 比特.P_1,p_2 和 p_3 长度近似为 2048/3,置$|p_1|=|p_3|=683$,$|p_2|=682$.定义 $LP=p_2^{-2c}$ 为弹性泄漏的概率,为保证抗泄漏性要求,LP 是可忽略的:

$$LP=p_2^{-2c}=(2^{862})^{-2c}=2^{-1363c}\approx 2.48\times 10^{-411c}.$$

事实上,当 c=0.05 时,弹性泄漏概率 LP=2.48×10^{-20},此时可以看作是可忽略的概率优势.因此,参数 c 在泄漏界 $Q=1+2c+\dfrac{J}{\log p_2}$ 上是可忽略的,即

$$Q=\left\lceil 1+\frac{J}{|p_2|}\right\rceil.$$

接下来分析系统允许的泄漏界 $LB=J$.

在系统初始化过程中,$Q=1+2c+\dfrac{J}{\log p_2}$,可求得:

$$J=(Q-1-2c)\log p_2\approx(Q-1)|p_2|=682(Q-1)\text{比特}.$$

显然,Q 越大,系统能够容忍的密钥泄漏就越大.同时也必须指出,Q 越大,系统的公开参数、密钥和密文等长度也随之变大.

系统泄漏界 LR、公开参数 PK、密文 CT_P 与模板密钥 SK_P 与泄漏参数 Q 之间的关系如图 3~图 6 所示,其中,图 5 和图 6 显示密文和密钥大小随泄漏参数 Q 和模板委托模板深度$|P|$之间的关系.

在该方案中,密钥大小与模板中非通配符元素个数有关.设模板长度 L=100,泄漏参数 Q=100,密钥大小随托模板深度而变化如图 5 所示,密钥大小在 152K~280K 比特之间,本方案的密钥大小可以容忍 68K 比特的密钥泄漏(如图 3 所示).在实际应用中,可以根据实际需要确定合适的泄漏界.特别地,当 Q=1 时,c=0,J=0,本方案简化为传统的非弹性泄漏的通配模板加密方案.

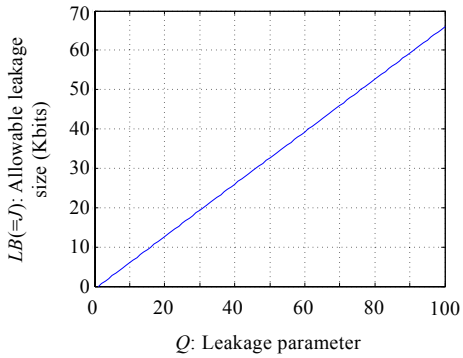


Fig.3 Leakage bound $LB(J)$ (Kbits)

图 3 泄漏界 $LB(J)$(Kbits)

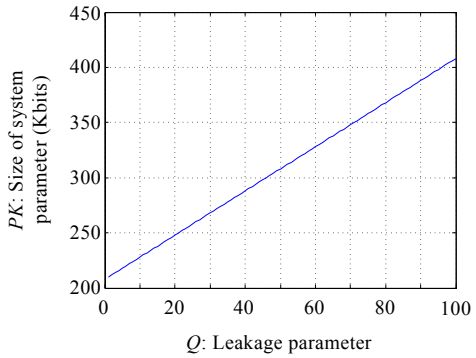


Fig.4 Size of system parameter (Kbits)

图 4 系统参数大小(Kbits)

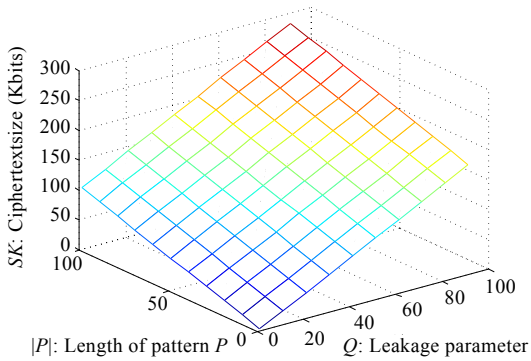


Fig.5 Size of pattern key (Kbits)

图 5 模板密钥大小(Kbits)

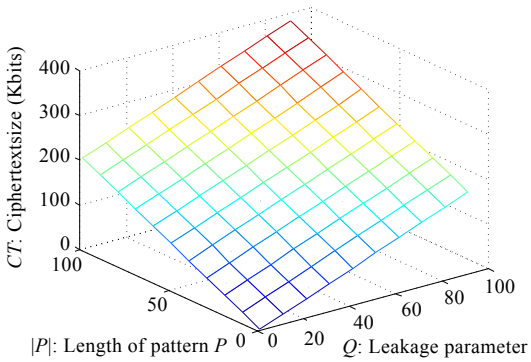


Fig.6 Size of ciphertext (Kbits)

图 6 密文大小(Kbits)

6 结束语

本文设计了一个密钥弹性泄漏安全的可委托通配模板加密方案,支持匹配挑战模板的密钥在部分泄漏条件下仍然具有语义安全性.通配模板定义为字母表{0,1,*}上的串,可以有效地在噪信道上敏感信息传输和对应内存攻击等环境中实现通配搜索和模板匹配的应用,如批量邮件保密传输、生物特征数据密钥管理、密文关键字搜索、数据库外包访问等.

本文给出了系统模型、方案构造、安全性证明以及抗泄漏性能分析,同时给出了方案在指纹模板作为身份的数据加密中的应用.接下来的工作将在提高系统泄漏界与改进系统性能方面做更多的研究.

致谢 感谢以色列本古里安大学(Ben Gurion University of Negev)的李西明博士在生物特征数据和性能分析的讨论和帮助.

References:

[1] Boneh D, Hamburg M. Generalized identity based and broadcast encryption schemes. In: Proc. of the Advances in Cryptology—ASIACRYPT 2008. LNCS 5350, 2008. 455−470. [doi: 10.1007/978-3-540-89255-7_28]

[2] Shi E, Waters B. Delegating capabilities in predicate encryption systems. In: Proc. of the ICALP 2008. LNCS 5126, Springer-Verlag, 2008. 560−578. [doi: 10.1007/978-3-540-70583-3_46]

[3] Abdalla M, Kiltz E, Neven G. Generalized key delegation for hierarchical identity-based encryption. In: Proc. of the ESORICS 2007. LNCS 4734, 2007. 139−154. [doi: 10.1007/978-3-540-74835-9_10]

[4] Abdalla M, Caro AD, Phan DH. Generalized key delegation for wildcarded identity-based and inner-product encryption. IEEE Trans. on Information Forensics and Security, 2012,7(6):1695−1706. [doi: 10.1109/TIFS.2012.2213594]

[5] Zhang M, Takagi T. GeoEnc: Geometric area based keys and policies in functional encryption systems. In: Proc. of the ACISP 2011. LNCS 6812, 2011. 241−258. [doi: 10.1007/978-3-642-22497-3_16]

[6] Kang L, Wang ZY. The efficient CCA secure public-key encryption scheme. The Chinese Journal of Computers, 2011,34(2): 236−242 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.00236]

[7] Boldyreva A, Fehr S, O'Neill A. On notions of security for deterministic encryption, and efficient constructions without random oracles. In: Proc. of the Advances in Cryptology—CRYPTO 2008. LNCS 5157, 2008. 335−359. [doi: 10.1007/978-3-540-85174-5_19]

[8] Lewko AB, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Proc. of the TCC 2010. LNCS 5978, 2010. 455−479. [doi: 10.1007/978-3-642-11799-2_27]

[9] Abdalla M, Birkett J, Catalano D, Dent AW, Malone-Lee J, Neven G, Schuldt JCN, Smart NP. Wildcarded identity-based encryption. Journal of Cryptography, 2011,24(1):42−82. [doi: 10.1007/s00145-010-9060-3]

[10] Alwen J, Dodis Y, Naor M. Public-Key encryption in the bounded-retrieval model. In: Proc. of the Advances in Cryptology—EUROCRYPT 2010. LNCS 6110, 2010. 113−134. [doi: 10.1007/978-3-642-13190-5_6]

[11] Alwen J, Dodis Y, Wichs D. Leakage-Resilient public-key in the bounded-retrieval model. In: Proc. of the Advances in Cryptology—CRYPTO 2009. LNCS 5677, 2009. 36−54. [doi: 10.1007/978-3-642-03356-8_3]

[12] Brakershi Z, Kalai YT, Katz J, Vaikuntanathan V. Overcoming the hole in the bucket: public-key cryptogaphy resilient to continual memory leakage. In: Proc. of the FOCS 2010. 2010. 501−510. [doi: 10.1109/FOCS.2010.55]

[13] Chow S, Dodis D, Rouselakis Y, Waters B. Practical leakage-resilient identity-based encryption from simple assumptions. In: Proc. of the ACM-CCS 2010. 2010. 152−161. [doi: 10.1145/1866307.1866325]

[14] Kiltz E, Pietrzak K. Leakage resilient ElGamal encryption. In: Proc. of the Advances in Cryptology—ASIACRYPT 2010. LNCS 6377, 2010. 595−612. [doi: 10.1007/978-3-642-17373-8_34]

[15] Liu S,Weng J, Zhao Y. Efficient public key cryptosystem resilient to key leakage chosen ciphertext attacks. In: Proc. of the CT-RSA 2013. LNCS 7779, 2013. 84−100. [doi: 10.1007/978-3-642-36095-4_6]

[16] Lewko AB, Rouselakis Y, Waters B. Achieving leakage resilience through dual system encryption. In: Proc. of the TCC 2011. LNCS 6597, 2011. 70−88. [doi: 10.1007/978-3-642-19571-6_6]

[17] Waters B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Proc. of the Advances in Cryptology—CRYPTO 2009. LNCS 5677, 2009. 619−636. [doi: 10.1007/978-3-642-03356-8_36]

[18] Zhang M, Yang B, Takagi T. Master-Key leakage-resilient and continue leakage-resilient functional encryption in dual affine spaces. Chinese Journal of Computers, 2012,35(9):1856−1867 (in Chinese with English abstract).

[19] Akavia A, Goldwasser S, Vaikuntanathan V. Simultaneous hardcore bits and cryptography against memory attacks. In: Proc. of the TCC 2009. LNCS 5444, 2009. 474−495. [doi: 10.1007/978-3-642-00457-5_28]

[20] Dodis V, Haralambier K, Lopez-Alt A, Wichs D. Efficient public-key cryptography in the presence of key leakage. In: Proc. of the Advances in Cryptology—ASIACRYPT 2010. LNCS 6377, 2010. 613−631. [doi: 10.1007/978-3-642-17373-8_35]

[21] Dodis V, Ostrovsky R, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM Journal of Computers, 2008,38(1):97−119. [doi: 10.1137/060651380]

[22] Sahai A, Water B. Fuzzy identity-based encryption. In: Proc. of the Advances in Cryptology—EUROCRYPT 2005. LNCS 3494, 2005. 457−473. [doi: 10.1007/11426639_27]

[23] Zhang M, Yang B, Takagi T. Bounded leakage-resilient functional encryption with hidden vector predicate. The Computer Journal, 2013,56(4):464−477. [doi: 10.1093/comjnl/bxs133]

[24] Yu J, Cheng XG, Li FG, Pan ZK, Kong FY, Hao R. Provably secure intrusion-resilient public-key encryption scheme in the standard model. Ruan Jian Xue Bao/Journal of Software, 2013,24(2):266−278 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4324.htm [doi: 10.3724/SP.J.1001.2013.04324]

[25] Yu J, Kong FY, Cheng XG, Hao R, Guo XF. A provably secure intrusion-resilient signature scheme. Ruan Jian Xue Bao/Journal of Software, 2010,21(9):2352−2366 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3772.htm [doi: 10.3724/SP.J.1001.2010.03772]

[26] Li X, Yang B, Guo Y, Yao J. A new key hiding scheme based on fingerprint. Journal of Computer Research and Development, 2013,50(3):532−539 (in Chinese with English abstract).

附中文参考文献:

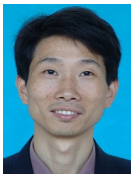
[6] 康立,王之怡.高效的适应性选择密文安全公钥加密算法.计算机学报,2011,34(2):236−242. [doi: 10.3724/SP.J.1016.2011.00236]

[18] 张明武,杨波,Tsuyoshi Takagi.抗主密钥泄漏和连续泄漏的双态仿射函数加密.计算机学报,2012,35(9):1856−1867.

[24] 于佳,程相国,李发根,潘振宽,孔凡玉,郝蓉.标准模型下可证明安全的入侵容忍公钥加密方案.软件学报,2013,24(2):266−278. http://www.jos.org.cn/1000-9825/4324.htm [doi: 10.3724/SP.J.1001.2013.04324]

[25] 于佳,孔凡玉,程相国,郝蓉.可证安全的入侵容忍签名方案.软件学报,2010,21(9):2352−2366. http://www.jos.org.cn/1000-9825/3772.htm [doi: 10.3724/SP.J.1001.2010.03772]

[26] 李西明,杨波,郭玉彬,姚金涛.一种新的基于指纹的密钥隐藏方案.计算机研究与发展,2012,50(3):532−539.



张明武(1970－),男,湖北仙桃人,博士,教授,CCF 高级会员,主要研究领域为密码学,信息安全与隐私保护.

杨波(1963－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.

王春枝(1963－),女,博士,教授,CCF 高级会员,主要研究领域为网络安全.

高木刚(1969－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.