抗主密钥泄露和连续泄露的双态仿射函数加密

张明武[1),2),3)] 杨 波[2)] TAKAGI Tsuyoshi[3)]

[1)](华南农业大学信息学院 广州 510642)

[2)](陕西师范大学计算机学院 西安 710072)

[3)](九州大学工业数学研究所 福冈 819-0395 日本)

摘 要 抗密钥泄露安全的加密系统保证在攻击者获得(主)密钥部分信息的情况下仍具有语义安全性.文中设计了一个抗密钥泄露的双态仿射函数加密方案,该方案中加密策略和解密角色定义为仿射空间,并且具有再次委托能力.在双系统加密模型下,实现了自适应安全的抗有界的主密钥泄露和用户密钥连续泄露的加密方案,在标准模型下基于静态子群判定假设证明了该方案的安全性.同时,分析了方案中的主密钥和用户密钥的泄露界和泄露率,通过参数调整可以达到接近73%的泄露率,具有较好的抗泄露性质.

关键词 函数加密;仿射空间;抗泄露;双系统加密;可证安全

中图法分类号 TP309 **DOI号**: 10.3724/SP.J.1016.2012.01856

Master-Key Leakage-Resilient and Continue Leakage-Resilient Functional Encryption in Dual Affine Spaces

ZHANG Ming-Wu[1),2),3)] YANG Bo[2)] TAKAGI Tsuyoshi[3)]

[1)](*College of Information, South China Agricultural University, Guangzhou* 510642)

[2)](*School of Computer Sciences, Shaanxi Normal University, Xi'an* 710072)

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

Abstract A leakage-resilient cryptosystem considers that an attacker is able to learn partial information about some values used throughout the lifetime of the system. Leakage-resilient encryption guarantees that the scheme is semantically secure even though the attacker has the abilities in obtaining bounded private keys and/or master keys. In this paper, we propose a leakage-resilient functional encryption in dual affine spaces that encryption policies and decryption roles are specified as affine (sub)spaces. Also, both encryption policies and decryption roles can perform delegation functionalities, which are flexible and expensive in practical applications. The proposed scheme can tolerant the bounded leakage in masters keys and private keys. We prove the security under the static subgroup decision assumptions in the standard model. Meanwhile, we analyze the tolerant bound and leakage ratio, and benefit the property of fine-grained leakage resilience.

Keywords functional encryption; affine space; leakage resilience; dual system encryption; provable security

收稿日期:2012-05-13;最终修改稿收到日期:2012-07-09.本课题得到国家自然科学基金(60973134,61173164,61272404)、广东省自然科学基金(10151064201000028)和日本JSPS外国特别研究员项目(22-00045)资助.**张明武**,男,1970年生,博士,副教授,中国计算机学会(CCF)高级会员,主要研究方向为密码学与信息安全.E-mail: csmwzhang@gmail.com; mwzhang@imi.kyushu-u.ac.jp. **杨 波**,男,博士,教授,博士生导师,主要研究领域为密码学. **TAKAGI Tsuyoshi**,博士,教授,主要研究领域为密码学.

1 引　言

现代密码学都假定用户密钥对可能的攻击来说是完全隐藏的，但在实际中通过边信道攻击，例如时间攻击、电源耗损、冷启动攻击以及频谱分析等，都能从保密密钥或加密系统内部获得有关密钥的部分信息. Akavia 等人[1]引入密钥泄露概念，攻击者即使从密钥中获得部分信息，而加密方案仍然是语义安全的，则称该加密方案是抗泄露(leakage-resilient)攻击安全的. 为了模拟泄露，设定攻击者能够访问泄露谕言机(leakage oracle)，从而获得关于密钥的任何函数的输出，即 f：$f(SK)\rightarrow\{0,1\}^*$[2-5]. 除了具有以往的语义安全所具有的能力外，攻击者还能够自适应地对泄露谕言机进行询问，唯一的限制是攻击者所获得泄露的输出长度总和不能超过预先设定的边界值，该模型也称有界泄露模型(Bounded Leakage Model，BLM). Alwen 等人[2]首次构建基于边界检索模型(Bounded-Retrieval Model，BRM)的抗密钥泄露的公钥加密方案，它是一种有界泄露模型的方案. Chow 等人[6]在基于 Hash 证明系统[7]的基础上，构建了几种抗泄露的基于身份的加密方案，但不支持主密钥泄露安全，同时把具有委托能力的抗泄露方案作为未解决的公开问题. 文献[6-7]的方案只支持每个身份的单次密钥泄露，Brakershi 等人[8]提出支持密钥连续泄露的加密方案，但不支持主密钥泄露. Lewko 等人[5]提出采用双系统加密技术(Dual System Encryption，DSE)可以构造抗密钥泄露的方案，同时构建了支持有界泄露的 IBE、HIBE 和 ABE 方案.

空间加密(Spatial Encryption，SE)[9-11]采用仿射空间作为解密角色，而仿射空间中的点向量作为加密策略. 根据仿射空间的包含性可实现密钥的再次委托能力. 在标准的 SE 方案的基础上，Vie 和 Abdalla 采用 DSE 技术设计抗密钥泄露的空间加密方案，该方案中可泄露界与空间的维度相关联[12]. 在 SE 方案中，由于加密策略定义为 κ 维的点向量，因此无法实现策略的再次委托能力.

双态仿射函数加密是一般空间加密的一般性扩展. 在双态仿射函数加密方案中，加密策略和解密角色都定义为仿射子空间. 角色委托实现解密能力的再次委托，可以实现类似基于代理的密码系统，而加密策略定义于可委托的仿射空间，扩展的加密策略委托能力可以支持重加密的能力. 因此，双态仿射空间加密具有广泛的模型，它扩展了 PKE[13]、HIBE[14-15]、ABE[16]、HVE[17]、FE[18-19]等方案.

本文设计了一个抗密钥泄露安全的双态仿射函数加密方案，在双系统加密模型下，实现自适应安全抗用户密钥多次泄露和主密钥泄露. 本方案中，加密策略和解密角色都定义为代数仿射向量子空间，并且可以有再次委托的能力. 当解密角色空间与加密策略空间存在一不动点(交集不为空)时，可实现函数的匹配并解密. 本方案中通过引入抗泄露组件，提高密钥的抗泄露能力. 同时通过密钥生成和委托算法的特殊功能，实现主密钥和用户密钥的更新功能，从而提高系统的抗连续泄露性. 本文方案是抗泄露的 IBE、HIBE、SE 和 FE 的一般性扩展：特别地，当加密策略和解密角色缩小为仿射空间中两个点向量时，本方案简化为抗泄露 IBE 方案；当仿射空间定义为树形结构空间而解密角色定义为一个点向量时，本方案为抗泄露 HIBE 方案；当解密角色变成一个点时，本方案为抗泄露 SE 方案.

1.1 基本思路

方案采用多维双系统加密技术实现，可以容忍主密钥的泄露和用户密钥的连续泄露，同时达到自适应安全. 为实现抗主密钥泄露和连续用户密钥泄露，把一维半功能空间扩展为 n 维. 在双系统加密 DSE 技术中，密文和密钥都可以定义两种形态：正常(Normal)和半功能(Semi-Functional，SF). 正常形态密钥可以解密任何一种形式的密文，但 SF 的密钥只能解密正常形态密文，不能解密 SF 密文. 目前实现 DSE 的方法主要有 3 种：基于标签 tag 的构建[15]、基于正交双线性子群的构建[14,16]和基于双对向量空间(Dual Pairing Vector Spaces，DPVS)[18]. 本文采用正交双线性群来设计抗泄露能力. 构建方案的密文和密钥都定义为正常形式，在证明过程中采用混合证明方法，首先密文改变成 SF 形态的，密钥由正常形式逐步改变成 SF 形态，我们要证明敌手不能感知到这些改变，主要基于合数阶群的子群判定假设. 最后模拟器生成 SF 形式的密钥和密文，并作为挑战密文提供给敌手，若敌手能正确解密密文，则可利用它来解决 SF 密钥对 SF 密文的判定性问题.

设计的困难问题是，在密钥由正常形态改变成 SF 形态的过程中，模拟器要为任何仿射向量空间准备密钥并生成相应的 SF 密文. 本文采用有支配能力的 SF 功能密钥来实现：从敌手来看，这些密钥与一般 SF 密钥是同分布的，但从模拟器来看，若解密

一 SF 密文,用支配密钥可以解密成功,因此在敌手询问过程中不会暴露密钥是正常还是 SF 形态的信息.本文扩展 SF 空间到 n 维($n\geq 2$).由于一个密钥的泄露量是有界的,当敌手所获得的泄露量不超过这个量时不能区分正交向量与随机向量.n 越大,抗泄露的容忍性越好.

1.2 本文组织

本文第 2 节介绍所用的一些基础知识;第 3 节给出抗泄露的双态仿射函数加密框架和安全性模型;第 4 节给出详细的构造方案;方案的正确性、一致性和安全性的分析和证明在第 5 节给出;第 6 节讨论本方案的泄露界;第 7 节对本文作出小结.

2 预备知识

2.1 基本概念

设 $\boldsymbol{u}=(u_1,\cdots,u_n),\boldsymbol{v}=(v_1,\cdots,v_n)\in Z_N^n$ 是一组向量,$\langle \boldsymbol{u},\boldsymbol{v}\rangle$ 是向量的内积.设 g 是群 G 的生成元,记 $g^{\boldsymbol{v}}$ 为向量 $g^{\boldsymbol{v}}:=(g^{v_1},\cdots,g^{v_n})\in G^n$.类似,$g^{r\boldsymbol{v}}:=(g^{rv_1},\cdots,g^{rv_n})$,$g^{\langle \boldsymbol{u},\boldsymbol{v}\rangle}:=g^{\boldsymbol{u}^{\top}\boldsymbol{v}}=g^{\sum_i u_i\cdot v_i}$.设 $(N,G,G_t,\hat{e})$ 为双线性群描述,满足对任意 $a,b\in Z_N$,存在有效可计算的双线性映射 $\hat{e}:\hat{e}(g^a,g^b)=\hat{e}(g,g)^{ab}$.$\hat{e}_n(g^{\boldsymbol{u}},g^{\boldsymbol{v}}):=\prod_{i=1}^{n}\hat{e}_n(g^{u_i},g^{v_i})=\hat{e}(g,g)^{\langle \boldsymbol{u},\boldsymbol{v}\rangle}$.设 $\hat{\boldsymbol{g}}^{[n+d]}$ 是长度为 $n+d$ 的一组 G_r 元素的随机向量,$(g^{u_1}\hat{g}_1,g^{u_2}\hat{g}_2,\cdots,g^{u_n}\hat{g}_n,g^{v_1}\hat{g}_{n+1},\cdots,g^{v_d}\hat{g}_{n+d})$ 简记为 $(g^{\boldsymbol{u}},g^{\boldsymbol{v}})*\hat{\boldsymbol{g}}^{[n+d]}$.记 $r\leftarrow S$ 为从集合 S 中随机选取一元素 r.$\mathrm{negl}(\lambda)$ 是对 λ 可忽略的函数,即对任意 $z>0$,一函数 $f(\lambda):N\rightarrow R$ 满足 $f(\lambda)\leq\lambda^{-z}$.

定义 1. 计算不可区分性.对任一 PPT 算法 A,两个概率总体 $\{X_1\},\{Y_2\}$ 满足 $|Pr[A(1^{\lambda},X_1)=1]-Pr[A(1^{\lambda},X_2)=1]|\leq\mathrm{negl}(\lambda)$,则称 X_1 和 X_2 对算法是计算不可区分的.

引理 1[20]. 设 q 是一素数,$m,l,d\in Z_N$ 满足 $m\geq l\geq 2d$,$\boldsymbol{X}_1,\boldsymbol{X}_2$ 分别是 Z_q 上选取的 $m\times l$ 和 $m\times d$ 的随机矩阵.$T\leftarrow Rank_d(\boldsymbol{Z}_q^{l\times d})$ 是秩是 d 的矩阵集.$f:\boldsymbol{Z}_q^{m\times d}\rightarrow\Omega$ 是矩阵 $\boldsymbol{Z}_q^{m\times d}$ 上的任意函数,满足

$$Dist((\boldsymbol{X}_1,f(\boldsymbol{X}_1T)),(\boldsymbol{X}_1,f(\boldsymbol{X}_2)))\leq\mathrm{negl}(\cdot),$$
$$|\Omega|\leq 4q^{l-2d}(q-1)\cdot\mathrm{negl}(\cdot)^2 \quad (1)$$

这里 $Dist(\boldsymbol{X}_1,\boldsymbol{X}_2)$ 表示两个随机变量 $\boldsymbol{X}_1$ 和 $\boldsymbol{X}_2$ 的统计距离.

推论 1. 设 m 是大于 2 的整数,q 是一大素数.设 $\boldsymbol{\delta},\boldsymbol{\tau}\leftarrow Z_q^m,\boldsymbol{\tau}'\leftarrow V_q^{\perp}(\boldsymbol{\delta})$($V^{\perp}(\boldsymbol{\tau})$ 是由基 $\boldsymbol{\tau}$ 生成向量空间的正交空间),对任一函数 $f:Z_q^m\rightarrow\Omega$,

$$Dist((\boldsymbol{\delta},f(\boldsymbol{\tau}')),(\boldsymbol{\delta},f(\boldsymbol{\tau})))\leq\mathrm{negl}(\cdot),$$
$$|\Omega|\leq 4q^{m-3}(q-1)\cdot\mathrm{negl}(\cdot)^2 \quad (2)$$

应用引理 1,置 $d=1,l=m-1$,则 $\boldsymbol{X}_1$ 对应于向量的正交空间 $V^{\perp}(\delta)$ 的基,$\boldsymbol{X}_2$ 对应于 $\bar{\tau}$.本文采用正交子群 G_q 作为这里的正交空间.我们在后面分析和讨论本文方案的泄露界 $\ell_{MSK}=\ell_{SK}=2+(n-1-2c)\log(q)$,此时 $\mathrm{negl}(\cdot)=q^{-c}$ 是可以忽略的.

定义 2. 仿射空间.设 $d\in Z_N,\boldsymbol{x}\in Z_N^{\kappa},M\in Z_N^{d\times\kappa}$,我们定义一仿射空间 $S=Aff(\boldsymbol{M},\boldsymbol{x})\subseteq Z_N^{\kappa}$ 为

$$S=Aff(\boldsymbol{M},\boldsymbol{x}):=\{\boldsymbol{x}+\boldsymbol{M}^{\top}\boldsymbol{z}\,|\,\boldsymbol{z}\in Z_N^d\},$$

称 $d(d\leq\kappa)$ 为仿射空间 S 的维度,记为 $d_2Dim(S)=d$.$T\in Z_N^{d_1\times d_2}$

引理 2. 若两仿射空间 $S_1=Aff(\boldsymbol{M}_1,\boldsymbol{x}_1)$ 维 $\bar{\delta}$ 度为 d_1,$S_2=Aff(\boldsymbol{M}_2,\boldsymbol{x}_2)$ 维度为 d_2,满足 $S_2\subseteq S_1$,则存在一有效可求解的矩阵和向量 $\boldsymbol{z}\in Z_N^{d_1}$,满足 $\boldsymbol{x}_2=\boldsymbol{x}_1+\boldsymbol{M}_1^{\top}\boldsymbol{z}$.

引理 3. 若两仿射空间 $S_1=Aff(\boldsymbol{M}_1,\boldsymbol{x}_1)$ 维度为 d_1,$S_2=Aff(\boldsymbol{M}_2,\boldsymbol{x}_2)$ 维度为 d_2,满足 $S_1\cap S_2\neq\varnothing$,则存在一有效可求解的矩阵 $\boldsymbol{T}_1,\boldsymbol{T}_2$ 和向量 $\boldsymbol{z}_1,\boldsymbol{z}_2$,满足 $\boldsymbol{M}_1\boldsymbol{T}_1=\boldsymbol{M}_2\boldsymbol{T}_2$,$\boldsymbol{x}_1-\boldsymbol{x}_2=\boldsymbol{M}_2^{\top}\boldsymbol{z}_2-\boldsymbol{M}_1^{\top}\boldsymbol{z}_1$.

证明. 设 $S_1\cap S_2=S'$,$S'\subseteq S_1$,$S'\subseteq S_2$,根据引理 2,$\boldsymbol{M}'=\boldsymbol{M}_1\boldsymbol{T}_1$,$\boldsymbol{x}'=\boldsymbol{x}_1+\boldsymbol{M}_1^{\top}\boldsymbol{z}_1$,$\boldsymbol{M}'=\boldsymbol{M}_2\boldsymbol{T}_2$,$\boldsymbol{x}'=\boldsymbol{x}_2+\boldsymbol{M}_2^{\top}\boldsymbol{z}_2$,得证. 证毕.

2.2 合数阶双线性群

一个合数阶的双线性群描述包括 $(N,G,G_t,\hat{e})$,阶 N 是多个不等的素数之积.设 $N=pqr$,这里 p、q、r 是不相等的素数.除满足双线性群的一般性质外,群 G 包含阶分别是 p、q 和 r 的子群 G_p、G_q 和 G_r,设其子群生成元分别是 g、$\bar{g}$ 和 $\hat{g}$,则 G 中的任一元素都可以表示成 $g^{a_1}\bar{g}^{a_2}\hat{g}^{a_3}$ 的形式,这里 $a_1,a_2,a_3\in Z_N$.合数阶双线性群具有如下特殊性质.

性质 1(子群生成元). 设 h 是 G 的生成元,则 h^{qr} 是 G_p 的生成元,h^{pr} 是 G_q 的生成元,h^{pq} 是 $G_rM_2=M_1T$ 的生成元.

性质 2(子群正交性). 设 $h_p\in G_p,h_q\in G_q,h_r\in G_r$,对所有 $a_1,a_2,a_3\in Z_N$,$\hat{e}(h_p^{a_1},h_q^{a_2})=1$,$\hat{e}(h_p^{a_1},h_r^{a_3})=1$,$\hat{e}(h_q^{a_2},h_r^{a_3})=1$.

2.3 数学困难假设

为证明所设计方案的安全性,本文使用如下基于合数阶群的(子)群判定问题,该假设在文献[14,16,18]中已作分析.

假设 1.　设$(N,G=G_p\times G_q\times G_r,G_t,\hat{e})$是阶$N=pqr$的双线性群，$\sigma,\tau\leftarrow Z_N$，$g\in G_p,\bar{g}\in G_q,\hat{g}\in G_r$. 给定元组$\Theta=(N,G,G_t,\hat{e};\ g,\hat{g},T_1=g^{\sigma}\in G_p,T_2=g^{\sigma}\bar{g}^{\tau}\in G_{pq})$，区分$T_1$和$T_2$是个困难问题.

假设 2.　设$(N,G,G_t,\hat{e})$是阶$N=pqr$的双线性群，$\sigma,\varsigma,\tau\leftarrow Z_N,g\in G_p,\bar{g}\in G_q,\hat{g}\in G_r$. 给定元组$\Theta=(N,G,G_t,\hat{e};g,\hat{g},X_1\in G_{pq},X_2\in G_{qr},T_1=g^{\sigma}\hat{g}^{\varsigma}\in G_{pr},T_2=g^{\sigma}\bar{g}^{\tau}\hat{g}^{\varsigma}\in G)$，区分$T_1$和$T_2$是个困难问题.

假设 3.　设$(N,G,G_t,\hat{e})$是阶$N=pqr$的双线性群，$\alpha,s,t,t'\leftarrow Z_N,g\in G_p,\bar{g}\in G_q,\hat{g}\in G_r$. 给定元组$\Theta=(N,G,G_t,\hat{e};\ g,\bar{g},\hat{g},X_1\in g^{\alpha}\bar{g}^{t},X_2\in g^{s}\bar{g}^{t'},T_1=\hat{e}(g^{\alpha},g^{s}),T_2\leftarrow G_t)$，区分$T_1$和$T_2$是个困难问题.

3　方案模型

3.1　双态仿射加密模型

一个双态仿射函数加密(DASE)由 5 个 PPT 算法组成：$\prod=(\mathrm{Init},\mathrm{KeyGen},\mathrm{Dele},\mathrm{Encr},\mathrm{Decr})$. Init 和 KeyGen 算法由可信第三方 PKG 执行，Init 算法生成系统公钥和主密钥，KeyGen 算法为用户持有的仿射空间生成密钥，同时也可以更新主密钥；Dele 算法由一仿射空间钥的持有者为其子空间生成委托密钥，同时也可以更新自己的密钥；Encr 和 Decr 分别由加密者和解密者执行消息的加密和解密操作. 为标记用户密钥和主密钥的泄露和更新，我们定义两个特殊的空间：空仿射空间ϕ和超仿射空间Λ.

(1) $\mathrm{Init}(1^{\lambda},\ell_{MSK},\ell_{SK},\kappa,n)$. 输入系统安全参数$1^{\lambda}$、主密钥泄露界$\ell_{MSK}$、用户密钥泄露界$\ell_{SK}$、抗泄露容忍度$n$和仿射空间的维度$\kappa$，初始化算法生成系统公钥和主密钥.

(2) $\mathrm{KeyGen}(MPK,MSK,S)$. 密钥生成算法输入系统公钥和主密钥，以及一仿射空间S，若$S=\Lambda$则更新主密钥，否则输出S的密钥SK_S.

(3) $\mathrm{Dele}(MPK,S_1,SK_1,S_2)$. 密钥委托算法输入系统公钥、仿射空间$S_1$及其密钥$SK_{S_1}$，以及$S_1$的仿射子空间$S_2$，若$S_2=\varnothing$则更新$S_1$的密钥，否则输出$S_2$的密钥$SK_{S_2}$.

(4) $\mathrm{Encr}(MPK,S',m)$. 加密算法输入系统公钥、接收者仿射空间S'以及消息m，输出加密的密文$CT_{S'}$.

(5) $\mathrm{Decr}(MPK,S,SK_S,S',CT_{S'})$. 解密算法输入系统公钥、加密策略空间$S'$及密文$CT_{S'}$、解密角色空间$S$及密钥$SK_S$，输出消息$m$.

正确性与一致性. Q、M和C分别是仿射向量空间、明文空间和密文空间. 对所有正确生成的(MPK,MSK)、S仿射空间密钥SK_S、S'接收者角色的消息m密文$CT_{S'}\in C$. $f(\cdot)$和$f'(\cdot)$是任意的用户密钥和主密钥的泄露函数，满足$\sum_i f_i(SK_S)\le\ell_{SK}$，$\sum_i f_i(MSK)\le\ell_{MSK}$. 若$S\cap S'\neq\varnothing$，使用$SK_S$解密$CT_{S'}$得到$m'=m$. 即

$$Pr\left[\begin{array}{l}(MPK,MSK)\leftarrow\mathrm{Init}(1^{\lambda},\ell_{MSK},\ell_{SK},\kappa,n)\\ S_1,S_2,S'\in Q,\ S_2\cap S'\neq\varnothing,\ m\in M\\ \sum_i f_i(SK_{S_2})\le\ell_{SK},\sum_i f_i(MSK)\le\ell_{MSK}\\ CT_{S'}\leftarrow\mathrm{Encr}(MPK,S',m)\\ m'\leftarrow\mathrm{Decr}(MPK,S_2,\mathrm{Dele}(MPK,S_1,\\ \quad\mathrm{KeyGen}(MPK,MSK,S_1),S_2),S',CT_{S'})\\ m'=m\end{array}\right]\le\mathrm{negl}(\lambda).$$

3.2　安全性模型

抗泄露安全的双态仿射加密的安全模型定义为如下的游戏框架$Exp_{\prod,A}^{\mathrm{LR}}(\lambda)$.

1. 系统参数. 挑战者C运行 Init 算法生成系统参数MPK和主密钥MSK，并把MPK发送给敌手A.

2. 询问 1. 本阶段A自适应地向挑战者进行下列询问：

(1) 创建密钥询问(O_{Crea}). 敌手提供一系列子空间S_j，挑战者生成并存储S_j的密钥SK_{S_j}.

(2) 泄露询问(O_{Leak}). 敌手提供一仿射空间S_j及概率多项式函数$f_i:SK\rightarrow\{0,1\}^*$，挑战者用$f_i(SK_{S_j})$作回答(泄露总长度$\sum_i f_i(SK_{S_j})$不能超过$\ell_{SK}$). 询问中，敌手也可以直接请求一个主密钥泄露的多项式时间函数$f_i(MSK)$询问.

(3) 密钥询问(O_{Revl}). 敌手提供子空间S_j，挑战者以完整的密钥SK_{S_j}作为回答.

(4) 委托钥询问(O_{Dele}). 敌手提供两空间S_1,S_2，挑战者首先查询O_{Crea}的队列是否有SK_{S_1}，如果不存在则调用O_{Crea}为SK_{S_1}生成密钥，然后调用 Dele 算法生成并回答委托钥SK_{S_2}，同时把SK_{S_2}存储于O_{Crea}密钥队列中.

(5) 解密询问(O_{Decr}). 输入一密文CT和一仿射空间S，挑战者生成仿射空间密钥SK_S，输出消息m.

3. 挑战. 敌手随机选择两消息$m_0,m_1\in M$以及挑战子空间S^*，要求S^*不在密钥询问O_{Revl}的队列中，也不是已询问过的空间的仿射子空间，且在泄露询问O_{Leak}获得的比特量小于ℓ_{SK}. 接下来挑战者随机选择$\beta\in\{0,1\}$，计算$CT_{S^*}\leftarrow\mathrm{Encr}(MPK,S^*,m_\beta)$，将密文$CT_{S^*}$发送给敌手$A$.

4. 询问 2. 类似询问 1,但要满足:不能对主密钥 MSK 或挑战 S^* 的密钥作 O_{Crea} 和 O_{Leak} 询问

5. 输出. 敌手输出 β',若 $\beta'=\beta$,敌手赢得该游戏.

对双态仿射加密方案 DASE 的安全游戏中,O_{Crea}、O_{Leak}、O_{Revl}、O_{Dele} 和 O_{Decr} 分别是创建密钥谕言机、泄露谕言机、密钥询问谕言机、委托谕言机和解密谕言机,泄露函数 $f: SK \to \{0,1\}^*$,敌手在 $Exp_{\prod,A}^{\text{LR}}(\lambda)$ 中的优势定义为

$$Adv_{\prod,A}^{\text{LR}}(\lambda) := 2|Pr[\beta'=\beta]-1| \tag{3}$$

定义 3. 抗泄露语义安全性. 对任一个多项式时间内的敌手 A 在 $Exp_{\prod,A}^{\text{LR}}(\lambda)$ 游戏中,同一仿射空间多次用户密钥泄露最多获得 ℓ_{SK} bit 的密钥信息($\sum \ell_j \leq \ell_{SK}$),最多获得 ℓ_{MSK} 的主密钥信息,敌手所获得的优势 $Adv_{\prod,A}^{\text{LR}}(\lambda)$ 是可忽略的,称该抗泄露双态仿射函数加密是(ℓ_{MSK},ℓ_{SK})-LR-CCA 安全的. 若在 $Exp_{\prod,A}^{\text{LR}}(\lambda)$ 游戏中敌手不能询问解密谕言机 O_{Decr},则称该方案是(ℓ_{MSK},ℓ_{SK})-LR-CPA 安全的.

本文重点考虑方案的密钥抗泄露性,对消息的保密性方面所设计的方案达到 CPA 安全. 可以利用转换工具使 CPA 安全的方案达到 CCA 安全. 一般的抗泄露安全只针对用户密钥泄露,本方案在此基础上实现抗主密钥泄露和连续泄露.

定义 4. 抗主密钥泄露. 当系统主密钥在泄露量不超过 ℓ_{MSK} 时,系统仍是安全的,称该方案抗主密钥泄露安全的. ℓ_{MSK} 称为主密钥泄露界.

定义 5. 抗连续泄露. 若一个密码方案具有自身密钥更新的能力,产生一个相同分布的重新随机化的密钥,称该方案是抗连续泄露的.

实际中,攻击者可以对同一用户的密钥进行多次的密钥泄露询问,因此通过多次的泄露询问获得超出泄露界的密钥信息量. 但若密钥可以被更新,则攻击者以前的泄露询问不起作用,需要重新开始对新的密钥进行泄露询问. 特别地,每当密钥被使用(或一定周期)就进行一次密钥更新,这样攻击者无法多次获得同一仿射空间的相同密钥上的泄露信息,此加密方案是完全抗连续泄露的.

4 方案构造

本方案中,一个仿射空间 $S := Aff(\boldsymbol{M},\boldsymbol{x})$ 的密钥形式为

$$\begin{aligned} SK_S &= (k_u, k_a, k_r, k_w) \\ &= (g^{\boldsymbol{u}}, g^{\alpha + r(a+\langle \boldsymbol{x},\boldsymbol{w}\rangle) - \langle \boldsymbol{u},\boldsymbol{v}\rangle}, g^r, g^{r\boldsymbol{M}^{\top}\boldsymbol{w}}) * \hat{g}^{[n+d+2]}, \end{aligned}$$

其中 $k_u \in G^n$,$k_a, k_r \in G$,$k_w \in G^d$,$\hat{g}^{[n+d+2]} \in G_r^{n+d+2}$. 这里 $d = Dim(S)$ 是仿射空间的维度,κ 是最大仿射空间的维度. 系统中 n 是大于等于 2 的整数,它控制密钥泄露的容忍度. n 越大,系统的抗泄露容忍性越好,n 越小,系统的密文和密钥越短. 系统初始化参数中,预先设置主密钥的泄露界 ℓ_{MSK} 和用户密钥的泄露界 ℓ_{SK},并且要求用户在自定义泄露函数 $f(\cdot)$ 的获得密钥的总输出长度不能超过这个界.

(1) $\text{Init}(1^{\lambda}, \ell_{MSK}, \ell_{SK}, \kappa, n)$. PKG 首先调用双线性群生成器生成 $(N = pqr, G = G_p \times G_q \times G_r, G_t, \hat{e})$,然后随机选取 $\alpha \in Z_N$,$\boldsymbol{u},\boldsymbol{v} \in Z_N^n$,$\boldsymbol{w} \in Z_N^{\kappa}$,$g$,$g^a \in G_p$,$\bar{g} \in G_q$,$\hat{g} \in G_r$.

设置并公开系统公钥 $MPK = (N, G, G_t, e; \ell_{MSK}, \ell_{SK}, g, \hat{g}, g^a, g^v, g^{\boldsymbol{w}}, e(g,g)^{\alpha})$,同时保存主密钥 $MSK = (\bar{k}_u, \bar{k}_a, \bar{k}_r, \bar{k}_w) = (g^{\boldsymbol{u}}, g^{\alpha + ra - \langle \boldsymbol{u},\boldsymbol{v}\rangle}, g^r, g^{r\boldsymbol{w}}) * \hat{g}^{[n+\kappa+2]}$.

这里 $\hat{g}^{[n+\kappa+2]}$ 是 G_r 上的一组随机 $n+\kappa+2$ 维向量,可以先随机选择 $\boldsymbol{\eta} \in Z_N^n \times Z_N \times Z_N \times Z_N^{\kappa}$,然后计算 $\hat{g}^{\boldsymbol{\eta}}$ 得到.

(2) $\text{KeyGen}(MPK, MSK, S)$. 第 1 步,PKG 为仿射空间 $S := Aff(\boldsymbol{M},\boldsymbol{x})$ 生成导入密钥 $\widehat{SK}_S$:设 $d = Dim(S)$,

$$\begin{aligned} \widehat{SK}_S &= (\hat{k}_u, \hat{k}_a, \hat{k}_r, \hat{k}_w) \\ &= (\bar{k}_u, \bar{k}_a \cdot \prod_{i=1}^{d} (\bar{k}_{w_i})^{x_i}, \bar{k}_r, \phi(g^{\boldsymbol{M}^{\top}}, \bar{k}_w)) \\ &= (g^{\boldsymbol{u}}, g^{\alpha + r(a+\langle \boldsymbol{x},\boldsymbol{w}\rangle) - \langle \boldsymbol{u},\boldsymbol{v}\rangle}, g^r, g^{r\boldsymbol{M}^{\top}\boldsymbol{w}}) * \hat{g}^{[n+d+2]} \end{aligned} \tag{4}$$

这里,设仿射矩阵 $\boldsymbol{M} = (\boldsymbol{X}_1, \cdots, \boldsymbol{X}_d)^{\top} \in Z_N^{d \times \kappa}$,定义 $\phi(g^{\boldsymbol{M}^{\top}}, \bar{k}_w) := (g^{\langle \boldsymbol{X}_1, r\boldsymbol{w}\rangle}, \cdots, g^{\langle \boldsymbol{X}_d, r\boldsymbol{w}\rangle})$.

第 2 步,对 $\widehat{SK}_S$ 进行随机化处理:随机选择 $r' \in Z_N$,$\boldsymbol{u}' \in Z_N^n$,$\hat{g}^{\boldsymbol{\eta}} \in G_r^{n+d+2}$,计算

$$\begin{aligned} SK_S &= \widehat{SK}_S * \langle g^{\boldsymbol{u}'}, g^{r'(a+\langle \boldsymbol{x},\boldsymbol{w}\rangle)} \cdot g^{\langle -\boldsymbol{u}', \boldsymbol{v}\rangle}, g^{r'}, g^{r'\boldsymbol{M}^{\top}\boldsymbol{w}} \rangle * \hat{g}^{\boldsymbol{\eta}} \\ &= \langle g^{\boldsymbol{u}+\boldsymbol{u}'}, g^{\alpha + (r+r')(a+\langle \boldsymbol{x},\boldsymbol{w}\rangle) - \langle \boldsymbol{u}+\boldsymbol{u}', \boldsymbol{v}\rangle}, g^{r+r'}, g^{(r+r')\boldsymbol{M}^{\top}\boldsymbol{w}} \rangle * \\ &\quad \hat{g}^{\boldsymbol{\eta} + [n+d+2]} \end{aligned} \tag{5}$$

由于 $r, r', \boldsymbol{u}, \boldsymbol{u}'$ 是 Z_N 上随机选取的,因此随机化前后的密钥是同分布的.

值得注意的是,当为一个特殊的 κ 维的仿射空间 Λ:$S_{\Lambda} = Aff(\boldsymbol{E}, \boldsymbol{0})$ 生成密钥时($\boldsymbol{E}$ 是单位阵,$\boldsymbol{0}$ 是零向量),本质上是在更新主密钥 MSK. 此时,$\langle \boldsymbol{0}, \boldsymbol{w}\rangle = 0$,$g^{r\boldsymbol{E}^{\top}\boldsymbol{w}} = g^{r\boldsymbol{w}}$,即经过密钥导入和随机化之后,密钥结构没有变化,只是用新随机数代替原来的 r 和 $\boldsymbol{u}$.

(3) Dele(MPK, S_1, SK_1, S_2). $S_2 = Aff(\boldsymbol{M}_2, \boldsymbol{x}_2)$ 是 $S_1 = Aff(\boldsymbol{M}_1, \boldsymbol{x}_1)$ 的仿射子空间，即 $S_2 \subseteq S_1$，设 $d_1 = Dim(S_1), d_2 = Dim(S_2)$，根据引理 2，存在一有效的计算求出 T 和 $\boldsymbol{z}$ 满足 $\boldsymbol{M}_2 = \boldsymbol{M}_1 T$, $\boldsymbol{x}_2 = \boldsymbol{x}_1 + \boldsymbol{M}_1^{\top}\boldsymbol{z}$.

① 若 $S_2 = S_1$，则系统更新委托者自身密钥 SK_{S_1}：采用 KeyGen 中的更新算法(5)，可以获得与原有密钥同分布的新密钥.

② 若 $S_2 \subset S_1$，S_1 为 S_2 生成委托密钥(设 S_1 的密钥是 $SK_{S_1} = (\boldsymbol{k}_u, \boldsymbol{k}_a, \boldsymbol{k}_r, \boldsymbol{k}_w)$)：首先生成导入密钥

$$\begin{aligned}\widehat{SK}_{S_2} &= (\hat{\boldsymbol{k}}_u, \hat{\boldsymbol{k}}_a, \hat{\boldsymbol{k}}_r, \hat{\boldsymbol{k}}_w)\\ &= (\boldsymbol{k}_u, \boldsymbol{k}_a g^{r\boldsymbol{M}_1^{\top}\boldsymbol{z}\boldsymbol{w}}, \boldsymbol{k}_r, \psi(g^{\boldsymbol{M}_1^{\top}}, \bar{\boldsymbol{k}}_w))\\ &= (g^{\boldsymbol{u}}, g^{\alpha + r(a + \langle \boldsymbol{x}_2, \boldsymbol{w}\rangle) - \langle \boldsymbol{u}, \boldsymbol{v}\rangle}, g^{r}, g^{r\boldsymbol{M}_2^{\top}\boldsymbol{w}}) * \hat{g}^{[n+d_2+2]}.\end{aligned}$$

第 2 步，对 $\widehat{SK}_{S_2}$ 再随机化，获得与 $\widehat{SK}_{S_2}$ 同分布的密钥 SK_{S_2}：随机选择 $r' \in Z_N$, $\boldsymbol{u}' \in Z_N^n$, $\hat{g}^{\boldsymbol{\eta}} \in G_r^{n+d_2+2}$，计算

$$\begin{aligned}SK_{S_2} &= \widehat{SK}_{S_2} * \langle g^{\boldsymbol{u}'}, g^{r'(a+\langle \boldsymbol{x}_2, \boldsymbol{w}\rangle)} \cdot g^{\langle -\boldsymbol{u}', \boldsymbol{v}\rangle}, g^{r'}, g^{r'\boldsymbol{M}_2^{\top}\boldsymbol{w}}\rangle * \hat{g}^{\boldsymbol{\eta}}\\ &= \langle g^{\boldsymbol{u}+\boldsymbol{u}'}, g^{\alpha + (r+r')(a+\langle \boldsymbol{x}_2, \boldsymbol{w}\rangle) - \langle \boldsymbol{u}+\boldsymbol{u}', \boldsymbol{v}\rangle}, g^{r+r'}, g^{(r+r')\boldsymbol{M}_2^{\top}\boldsymbol{w}}\rangle *\\ &\quad \hat{g}^{\boldsymbol{\eta}+[n+d_2+2]}\end{aligned} \tag{6}$$

(4) Encr(MPK, S', m) 给定一消息 $m \in G_t$ 和一接收者仿射空间角色 $S' = Aff(\boldsymbol{M}', \boldsymbol{x}')$，本算法随机选取 $s \in Z_N$，生成密文 $CT_{S'}$.

$$\begin{aligned}CT_{S'} &= (c_m, \boldsymbol{c}_v, c_s, c_a, \boldsymbol{c}_w)\\ &= (m \cdot \hat{e}(g,g)^{s\alpha}, g^{s\boldsymbol{v}}, g^{s}, g^{-s(a+\langle \boldsymbol{x}', \boldsymbol{w}\rangle)}, g^{s\boldsymbol{M}'^{\top}\boldsymbol{w}})\end{aligned} \tag{7}$$

特别地，当接收角色空间 S' 缩小为仿射空间的一个点向量 $\boldsymbol{x}'$ 时，$\boldsymbol{M}' = \varnothing, \boldsymbol{c}_w = \boldsymbol{1}_G$. 此时加密方案简化为一般的空间加密方案[9-10].

(5) Decr($MPK, S, SK_S, S', CT_{S'}$). 若解密者的角色空间 $S = Aff(\boldsymbol{M}, \boldsymbol{x})$ 与加密策略空间 $S' = Aff(\boldsymbol{M}', \boldsymbol{x}')$ 的交不为空($S \cap S' \neq \varnothing$)，则存在一仿射空间点向量 $\boldsymbol{x}^* \in S \cap S'$. 根据线性代数性质及引理 3，可以有效地找出向量 $\boldsymbol{z}, \boldsymbol{z}'$ 满足：$\boldsymbol{x}^* = \boldsymbol{x} + \boldsymbol{M}^{\top}\boldsymbol{z} = \boldsymbol{x}' + (\boldsymbol{M}')^{\top}\boldsymbol{z}'$.

解析 $SK_S = (\boldsymbol{k}_u, \boldsymbol{k}_a, \boldsymbol{k}_r, \boldsymbol{k}_w)$, $CT_{S'} = (c_m, \boldsymbol{c}_v, c_s, c_a, \boldsymbol{c}_w)$，计算

$$k_\delta = k_a \cdot \prod_{i=1}^{d} (\boldsymbol{k}_{w_i})^{z_i}, \quad c_\delta = c_a \cdot \prod_{i=1}^{d} (\boldsymbol{c}_{w_i})^{z_i} \tag{8}$$

这里 $d = Dim(S \cap S')$. 输出消息 m.

$$m = \frac{c_m}{\hat{e}(\boldsymbol{k}_u, \boldsymbol{c}_v)\hat{e}(k_\delta, c_r)\hat{e}(k_s, c_\delta)} \tag{9}$$

5　方案正性与安全性

5.1　正确性

5.1.1　解密一致性

密文 $CT_{S'}$ 中，$c_m \in G_t, \boldsymbol{c}_v, c_a, c_s, \boldsymbol{c}_w \in G_p$，而密钥 $SK_S \in G_{pr}$，根据子群的正交性、密钥与密文的双线性运算(c_m 除外)，密钥的 G_r 子群元素 $\hat{g}^{[n+d+2]}$ 将被约除. 因此解密一致性只需考虑子群 G_p 中元素的计算. 根据引理 3，$\boldsymbol{x}^* = \boldsymbol{x} + \boldsymbol{M}^{\top}\boldsymbol{z} = \boldsymbol{x}' + (\boldsymbol{M}')^{\top}\boldsymbol{z}'$.

$$\begin{aligned}k_\delta &= k_a \cdot \prod_{i=1}^{d} (\boldsymbol{k}_{w_i})^{z_i} = g^{\alpha + r(a+\langle \boldsymbol{x}, \boldsymbol{w}\rangle) - \langle \boldsymbol{u}, \boldsymbol{v}\rangle} g^{r\boldsymbol{M}^{\top}\boldsymbol{z}\boldsymbol{w}}\\ &= g^{\alpha + r(a+\langle \boldsymbol{x}, \boldsymbol{w}\rangle) - \langle \boldsymbol{u}, \boldsymbol{v}\rangle} g^{r\langle \boldsymbol{x}^* - \boldsymbol{x}\rangle \boldsymbol{w}}\\ &= g^{\alpha + r(a+\langle \boldsymbol{x}^*, \boldsymbol{w}\rangle) - \langle \boldsymbol{u}, \boldsymbol{v}\rangle},\end{aligned}$$

同理，$c_\delta = g^{-s(a+\langle \boldsymbol{x}^*, \boldsymbol{w}\rangle)}$，

$$\hat{e}(\boldsymbol{k}_u, \boldsymbol{c}_v) = \hat{e}(g^{\boldsymbol{u}}, g^{s\boldsymbol{v}}) = \hat{e}(g,g)^{s\langle \boldsymbol{u}, \boldsymbol{v}\rangle} \tag{10}$$

$$\begin{aligned}\hat{e}(k_\delta, c_r) &= \hat{e}(g^{\alpha + r(a+\langle \boldsymbol{x}^*, \boldsymbol{w}\rangle) - \langle \boldsymbol{u}, \boldsymbol{v}\rangle}, g^{s})\\ &= \hat{e}(g,g)^{s\alpha}\hat{e}(g,g)^{rs(a+\langle \boldsymbol{x}^*, \boldsymbol{w}\rangle)}\hat{e}(g,g)^{-s\langle \boldsymbol{u}, \boldsymbol{v}\rangle}\end{aligned} \tag{11}$$

$$\hat{e}(k_s, c_\delta) = \hat{e}(g^{r}, g^{-s(a+\langle \boldsymbol{x}^*, \boldsymbol{w}\rangle)}) = \hat{e}(g,g)^{-rs(a+\langle \boldsymbol{x}^*, \boldsymbol{w}\rangle)} \tag{12}$$

$$\hat{e}(\boldsymbol{k}_u, \boldsymbol{c}_v)\hat{e}(k_\delta, c_r)\hat{e}(k_s, c_\delta) = \hat{e}(g,g)^{s\alpha} \tag{13}$$

使用上述盲化因子 $\hat{e}(g,g)^{s\alpha}$ 可以从 c_m 中正确提取消息 m.

5.1.2　密钥生成正确性

在 KeyGen 中，PKG 利用主密钥 MSK 对任一仿射空间 $S = Aff(\boldsymbol{M}, \boldsymbol{x})$ 生成密钥 $SK_S = (\boldsymbol{k}_u, k_a, k_r, \boldsymbol{k}_w) \in G_{pr}^{n+d+2}$. 这里 $\boldsymbol{k}_u, k_r$ 用于隐藏随机数 $\boldsymbol{u}$ 和 r，我们主要验证 k_a 和 $\boldsymbol{k}_w$ 的正确性.

$$\begin{aligned}\hat{k}_a &= \bar{k}_a \cdot \prod_{i=1}^{d} (\bar{k}_{w_i})^{x_i} = g^{\alpha + ra - \langle \boldsymbol{u}, \boldsymbol{v}\rangle} \cdot g^{r\langle \boldsymbol{x}, \boldsymbol{w}\rangle} * \hat{g}'\\ &= g^{\alpha + r(a+\langle \boldsymbol{x}, \boldsymbol{w}\rangle) - \langle \boldsymbol{u}, \boldsymbol{v}\rangle} * \hat{g}' \in G_{pr}\end{aligned} \tag{14}$$

$$\begin{aligned}\hat{\boldsymbol{k}}_w &= \psi(g^{M^{\top}}, \bar{k}_w) = (g^{\langle \boldsymbol{X}_1, r\boldsymbol{w}\rangle}, \cdots, g^{\langle \boldsymbol{X}_d, r\boldsymbol{w}\rangle}) * \hat{g}^{[d]}\\ &= g^{r\boldsymbol{M}^{\top}\boldsymbol{w}} * \hat{g}^{[d]} \in G_{pr}^{d}\end{aligned} \tag{15}$$

在随机化过程中，密钥的结构和长度没有发生变化，只是用新的随机数 $\boldsymbol{u} + \boldsymbol{u}'$ 和 $r + r'$ 代替原密钥中的 $\boldsymbol{u}$ 和 r，因此不影响密钥的一致性.

5.1.3　委托钥正确性

S_2 是 S_1 的仿射子空间，根据引理 2，存在一有效可求解的矩阵 $\boldsymbol{M}$ 和向量 $\boldsymbol{z}$，满足 $\boldsymbol{x}_2 = \boldsymbol{x}_1 + \boldsymbol{M}^{\top}\boldsymbol{z}$，故 $\boldsymbol{M}^{\top}\boldsymbol{z} = -\boldsymbol{x}_1 + \boldsymbol{x}_2$. 对生成的 S_2 的委托密钥中，$\hat{\boldsymbol{k}}_w$ 的求解过程与式(6)相同.

$$\hat{k}_a = r\boldsymbol{M}_1^{\top}\boldsymbol{z}\boldsymbol{w} = g^{\alpha + r(a+\langle \boldsymbol{x}_1, \boldsymbol{w}\rangle) - \langle \boldsymbol{u}, \boldsymbol{v}\rangle} g^{r\langle -\boldsymbol{x}_1 + \boldsymbol{x}_2, \boldsymbol{w}\rangle} = g^{\alpha + r(a+\langle \boldsymbol{x}_2, \boldsymbol{w}\rangle) - \langle \boldsymbol{u}, \boldsymbol{v}\rangle} \tag{16}$$

5.2 密钥更新

5.2.1 主密钥更新

PKG 可以通过对特殊仿射空间 $S_\Delta = (\boldsymbol{E}, \boldsymbol{0})$ 的密钥提取来更新主密钥 MSK：$Dim(S_\Delta) = \kappa$，$\boldsymbol{E}$ 是单位阵，$\boldsymbol{0}$ 是零向量. 主密钥更新是对密钥中的随机数进行再随机化处理，由于主密钥中每个组件都与随机数关联，因此进行主密钥更新可以容忍系统的泄露，我们很容易得到下面的定理.

定理 1. 在 DASE 方案中，主密钥更新不影响系统以前和以后产生的密钥，但可以提高系统的抗主密钥泄露安全性.

通过周期性更新主密钥，可以抗主密钥的连续泄露.

5.2.2 用户密钥更新

在 Dele 算法中，任何密钥持有者除了可以为仿射子空间生成子密钥外，还可以更新自身密钥. 在密钥结构和长度不变的情况下，通过再随机化随机数的功能实现密钥更新.

定理 2. 在 DASE 方案中，密钥更新不影响该密钥生成的子密钥，但可以提高系统的抗主密钥泄露安全性.

关于密钥可泄露的大小与安全强度，我们在后面讨论.

5.3 委托路径独立性

本方案具有委托路径独立性：一个委托的密钥与路径无关. 设有 3 个仿射空间 S_1, S_2, S_3 满足 $S_3 \subseteq S_2 \subseteq S_1$，则为 $S3$ 生成的两个密钥 Dele$(MPK, S_1, SK_{S_1}, S_3)$ 与 Dele$(MPK, S_2, Dele(MPK, S_1, SK_{S_1}, S_2), S_3)$ 是计算不可区分的.

5.4 安全性

与一般加密方案的证明不同之处在于，一般的语义安全性只需要回答敌手的密钥询问，而本方案允许敌手进行额外的主密钥 MSK 和仿射空间角色密钥 SK_S 的泄露询问. 特别地，敌手可以对挑战的仿射子空间作有界长度的密钥泄露询问. 可泄露的界 ℓ_{MSK}, ℓ_{SK} 是安全参数的多项式表达式，即 $\ell_{MSK} = \ell_{MSK}(\lambda)$，$\ell_{SK} = \ell_{SK}(\lambda)$.

首先，挑战者 C 运行 Init 算法生成系统参数和主密钥，并把系统公钥发送给敌手 A. 同时，C 提供给敌手一个记录主密钥 MSK 及关联的用户密钥 SK 及泄露量的句柄 $H := (Handle, Space, (MSK \cup SK), Leaked\text{-}bit))$，以利敌手进行询问并保持相应的状态.

在询问阶段，由于 $O_{\text{KeyGen}}, O_{\text{Dele}}$ 都可以由 O_{Crea} 生成，在询问阶段敌手可以自适应地进行三种询问：$O_{\text{Crea}}, O_{\text{Leak}}$ 和 O_{Revl}. 在 O_{Crea} 中，敌手提供一个主密钥的句柄给挑战者，并请求挑战者生成一个密钥，并存储在相应队列中. 每次询问后，挑战者要返回一个与相应句柄相应的用户密钥给 A，使得 A 在后面的 O_{Leak} 和 O_{Revl} 询问中能够对应它所使用的句柄.

在 O_{Leak} 询问中，A 使用句柄可以有选择性地进行泄露询问，所有的泄露函数 f_i 和泄露量由敌手自适应地选择（只要泄露总量不超过 ℓ_{MSK} 和 ℓ_{SK}）. 在此询问过程中，挑战者记录敌手每次所泄露过的密钥及泄露量. 当敌手请求一个 O_{Crea} 询问时，挑战者创建一条上述记录并置初值为 0.

O_{Revl} 询问允许敌手获得某一仿射空间的 S 生成的密钥 SK_S. 为了保持一致性，敌手只需提供一个 S 的句柄. 显然，敌手不能获得主密钥的询问，也不能对挑战的仿射空间作密钥提取询问. 为此，挑战者用集合 R 记录已询问过的仿射空间.

方案中 KeyGen 或 Dele 产生的密钥和 Encr 生成的密文都是正常形式的，为了帮助证明，我们设计半功能化的密钥形式. 基本方法是对原来密钥和密文组件乘以 G_q 中的随机元素（G_q 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）. 随机选取 $\bar{g}^{\theta_1}, \bar{g}^{\gamma_1} \in G_q^{n+2}$，$\bar{g}^{\theta_2}, \bar{g}^{\gamma_2} \in G_q^{d}$，计算半功能密钥：

$$\widetilde{SK}_S := ((\boldsymbol{k}_u, k_a, k_r) * \bar{g}^{\theta_1}, \boldsymbol{k}_w * \bar{g}^{\theta_2}) \in G_{pqr}^{n+d+2}.$$

半功能密文：

$$\widetilde{CT}_{S'} := (c_m, (\boldsymbol{c}_v, c_s, c_a) * \bar{g}^{\gamma_1}, \boldsymbol{c}_w * \bar{g}^{\gamma_2}) \in G_t \times G_{pq}^{n+d+2}.$$

显然一个半功能密钥要成功解密一个半功能密文，除了加密策略 S' 与解密角色 S 满足 $S \cap S' \neq \varnothing$，根据式(8)还要满足 $\langle \boldsymbol{\theta}_1, \boldsymbol{\gamma}_1 \rangle + \langle \boldsymbol{M}^{\top}\boldsymbol{z}\boldsymbol{\theta}_2, \boldsymbol{M}'^{\top}\boldsymbol{z}'\boldsymbol{\gamma}_2 \rangle = 0 \bmod q$.

为了证明方案的安全性，我们使用一系列不可区分的游戏，最初游戏 Leak 中密钥和密文均是正常形式，而最后的 LeakCK 中密钥和密文均是半功能化的，LeakCKM 中的消息组件 c_m 是随机化的. 定义如下：

(1) Leak. 本游戏中密文和密钥均为正常形式，即密文和密钥由 DASE 中算法生成，敌手执行 $Exp_{\Pi,A}^{\text{LR}}(\lambda)$ 定义的游戏模型.

(2) LeakD. 与 Leak 的区别在于，对敌手的 Dele 和 KeyGen 询问，用 O_{Crea} 代替. 由于这两个谕言

机所生成的密钥是不可区分的，因此 LeakD 与 Leak 是不可区分的.

(3) LeakC. 本游戏与 LeakD 的区别在于，在挑战阶段，挑战者用半功能密文 $\widetilde{CT}_{S'}$ 作为挑战的输出.

(4) LeakCK$_j$. 与 LeakC 相同的是，本游戏中密文仍是半功能化的. 同时，本游戏产生半功能化的密钥存储于 H 中，O_{Crea} 生成正常的密钥而 O_{Leak} 和 O_{Revl} 生成半功能化的密钥. 与密钥询问一样，本游戏也生成半功能的主密钥. 显然，$j=0$ 时，LeakCK$_0$ = LeakC；$j=q_e$（q_e 是询问的最大次数）时，LeakCK 中生成的密文和密钥都是半功能化的. 当 $1\leq j\leq q_e$ 时，所生成的密钥中前 $j-1$ 个是半功能化的，后面的都是正常密钥. 我们证明对所有 j，LeakCK$_j$ 与 LeakCK$_{j+1}$ 是不可区分的. 同时，我们证明敌手在 Leak$_{j+1}$ 中不能构造可解密挑战密文的支配型密钥.

(5) LeakCKM. 与 LeakCK 不同的是，本游戏中密文中的 c_m 改变成 G_t 中的随机元素. 通过 LeakCK 与 LeakCKM 的不可区分性，我们可以证明 c_m 对消息是保密的.

定理 3.　在一个抗泄露的双态仿射函数加密方案中，若 Leak，LeakD，LeakC，LeakCK，LeakCKM 之间是计算性不可区分的，则该方案是抗泄露安全的.

证明.　我们采用一系列不可区分的证明引理 4～8 来证明本抗泄露方案的安全性. Leak 是本文提出方案的正常密钥和密文，而 LeakCK 表明敌手无法区分的半功能化密文和密钥，LeakCKM 是对消息隐藏组件与随机元素不可区分. 引理 7 在引理 1 的分布不可区分性的基础上证明在泄露界中，敌手无法构造一个支配型的密钥去解密挑战密文. 因此从敌手来看，这些游戏不可区分，而 LeakCK 和 LeakCKM 是完全随机化的密文组件，敌手无法从这些组件中获得密文的有用信息. 因此，本方案是 (ℓ_{MSK},ℓ_{SK})-LR-CPA 安全的.

引理 4.　任何多项式时间内的敌手 A 无法区分 Leak 和 LeakD.

证明.　O_{Crea} 执行 O_{KeyGen} 的输出. 通过 KeyGen 和 Dele 的算法可知，两者的输出是同一分布的，同时 O_{Dele} 的委托密钥也应当在 O_{Crea} 生成的密钥队列中，因此 O_{KeyGen} 和 O_{Dele} 都可以由 O_{Crea} 生成，敌手无法区别一个密钥是哪个谕言机生成.

引理 5.　若安全假设 1 存在，则任何多项式时间内的敌手 A 无法区分 LeakC 和 LeakD.

证明.　假设一多项式时间的敌手 A 可以以不可忽略的优势区分 LeakD 和 LeakC，则我们可以构建一算法 D 作为模拟器以相同的优势解决安全假设 1.

当 D 收到假设 1 的实例 $(N,G,G_t,\hat{e};g,\hat{g})$，$D$ 的目标是猜测一元素 $T\in G_p$ 还是 $T\in G_{pq}$. 为此，D 扮演模拟器并回答敌手 A 的询问及挑战如下

(1) 初始化. D 随机选择 $\alpha,a,\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}\in Z_N^{2n+\kappa+2}$，置系统公钥 $MPK=(N,g,\hat{g},g^a,g^v,g^w)$ 并发送给 A.

(2) 询问 1. 由于 D 知道系统主密钥 α 和 $\boldsymbol{v}$，因此可以为任何仿射空间生成密钥，并且可以回答敌手 A 的 O_{Crea}、O_{Leak}、O_{Revl}、O_{KeyGen} 及 O_{Dele} 等询问.

(3) 挑战. 当 A 提交给 D 两个挑战的消息 Gm_0,m_1 及挑战子空间 $S^*=Aff(\boldsymbol{M}^*,\boldsymbol{x}^*)$，模拟器 D 随机选择 $\beta\in\{0,1\}$，输出密文 $CT_{S^*}=(c_m,\boldsymbol{c}_v,c_s,c_a,\boldsymbol{c}_w)=(m_\beta\hat{e}(T,g^\alpha),T^v,T,T^{-(a+\langle\boldsymbol{x}^*,\boldsymbol{w}\rangle)},T^{(\boldsymbol{M}^*)^\top\boldsymbol{w}})$.

(4) 询问 2. 与询问 1 相同，同时要求 A 不能对 S^* 及其超空间作 O_{Revl} 询问.

(5) 输出. A 输出对密文中消息 m_β 的猜测 β'. D 以相同的输出 β' 作为对假设 1 的猜测：$\beta'=0$ 则 $T\in G_p$，$\beta'=1$ 则 $T\in G_{pq}$. 若 $T\in G_p$，则密文 CT_{S^*} 是正常形态的（没有 G_q 元素），此时 B 可以正确模拟 Leak. 若 $T=g^\sigma\bar{g}^\tau\in G_{pq}$，则密文是半功能化的，此时 $c_m=m_\beta\hat{e}(T,g^\alpha)=m\,\hat{e}(g,g)^\alpha$，$\boldsymbol{\theta}=\tau(\boldsymbol{v},1,-a+\langle-\boldsymbol{x}^*,\boldsymbol{w}\rangle,(\boldsymbol{M}^*)^\top\boldsymbol{w})$. 事实上，虽然 $a,\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}$ 是从 Z_N 中选取. 但在公开参数 MPK 中时都是作为 $g\in G_p$ 的指数，因此这些值模 q 是不为 0 的（p,q,r 是互素的阶）. 对敌手来说密文组件中 G_q 部分不为 1_{G_q}. 因此可以正确模拟 LeakC.

引理 6.　若安全假设 2 存在，则任何多项式时间内的敌手 A 无法区分 LeakCK$_j$ 和 LeakCK$_{j+1}$.

证明.　若一多项式时间的敌手 A 以不可忽略的优势区分 LeakCK$_j$ 和 LeakCK$_{j+1}$，我们可以构建一算法 D 以相同的优势解决安全假设 2. D 的目标是判断假设 2 的实例 $(g,\hat{g},\boldsymbol{X}_1,\boldsymbol{X}_2,T)$ 中 T 为 G_{pq} 还是 G 中的元素. 我们证明当 $T\in G_{pq}$ 时，D 能成功模拟 LeakCK$_j$，当 $T\in G$ 时，D 能成功模拟 Leak$_{j+1}$.

(1) 初始化. D 随机选择 $\alpha,a,\boldsymbol{v},\boldsymbol{w}\in Z_N^{n+\kappa+2}$，设置系统公钥 $MPK=(g,\hat{g},g^a,g^{\boldsymbol{w}},g^{\boldsymbol{w}},\hat{e}(g,g)^\alpha)$.

(2) 询问 1. 本阶段对密钥回答分为 3 种情况

① 对前面的 $j-1$ 个密钥，D 设置成半功能密钥，即 $SK_S=(g^{\boldsymbol{u}},g^{\alpha+r(a+\langle\boldsymbol{x},\boldsymbol{w}\rangle)-\langle\boldsymbol{u},\boldsymbol{v}\rangle},g^r,g^{r\boldsymbol{M}^\top\boldsymbol{w}})*$

$\hat{g}^{[n+d+2]} * X_2^{[n+d+2]} \in G^{n+d+2}$.

② 对第 j 个密钥，D 将生成挑战项的密钥，$SK_S=(T^{\boldsymbol{u}}, g^{\alpha}T^{a+\langle \boldsymbol{x},\boldsymbol{w}\rangle-\langle \boldsymbol{u},\boldsymbol{v}\rangle}, T, T^{\boldsymbol{M}^{\top}\boldsymbol{w}}) * \hat{g}^{[n+d+2]}$.

显然，当 $T\in G_{pr}$ 时，SK_S 是正常形态的. 当 $T=g^{\sigma}\bar{g}^{\tau}\hat{g}^{\varsigma}\in G$（注：$G=G_{pqr}$）时，半功能密钥因子 $\boldsymbol{\theta}=\tau(\boldsymbol{u}, a+\langle \boldsymbol{x},\boldsymbol{w}\rangle-\langle \boldsymbol{u},\boldsymbol{v}\rangle, 1, \boldsymbol{M}^{\top}\boldsymbol{w})$. $\boldsymbol{\theta}$ 作为 $g\in G_p$ 的指数（计算时 mod$p$）而 p 与 q 互素，因此 $\boldsymbol{\theta}\neq\boldsymbol{0}$，从敌手来看 SK_S 是半功能的.

③ 从 $j+1$ 密钥开始，D 输出正常形式的密钥，即 $SK_S=(g^{\boldsymbol{u}}, g^{\alpha+r(a+\langle \boldsymbol{x},\boldsymbol{w}\rangle-\langle \boldsymbol{u},\boldsymbol{v}\rangle)}, g^{r}, g^{r\boldsymbol{M}^{\top}\boldsymbol{w}}) * \hat{g}^{[n+d+2]}\in G_{pr}^{n+d+2}$.

(3) 挑战. D 生成一个半功能化的密文：

$\widetilde{CT}_{S^*}=(m_{\beta}\hat{e}(X_1, g^{\alpha}), X_1^{\boldsymbol{v}}, X_1, X_1^{-a-\langle \boldsymbol{x}^*,\boldsymbol{w}\rangle}, X_1^{(\boldsymbol{M}^*)^{\top}\boldsymbol{w}})$.

(4) 设 $X_1=g^{k_1}\bar{g}^{k_2}\in G_{pq}$，挑战密文中半功能化因子 $\boldsymbol{\gamma}=k_2(\boldsymbol{v}, 1, -a-\langle \boldsymbol{x}^*,\boldsymbol{w}\rangle, (\boldsymbol{M}^*)^{\top}\boldsymbol{w})$.

设 $\widetilde{SK}_S=((\boldsymbol{k}_u, k_a, k_r) * \bar{g}^{\theta_1}, \boldsymbol{k}_w * \bar{g}^{\theta_2})$，在半功能化密钥生成或委托时，根据式(8)，若 S 使用半功能密钥 $\widetilde{SK}_S$ 去生成一子空间密钥 $\boldsymbol{x}_2=\boldsymbol{x}_1+\boldsymbol{M}^{\top}\boldsymbol{z}$，则半功能化参数 $\boldsymbol{\theta}'=\boldsymbol{\theta}_1+(0,\cdots,0,\langle \boldsymbol{z},\boldsymbol{\theta}_2\rangle)$. 同样，半功能化密钥参数 $\boldsymbol{\gamma}'=\boldsymbol{\gamma}_1+(0,\cdots,0,\langle \boldsymbol{z}',\boldsymbol{\gamma}_2\rangle)$.

$$\langle \boldsymbol{\theta}',\boldsymbol{\gamma}'\rangle=\tau k_2(\langle \boldsymbol{u},\boldsymbol{v}\rangle-a-\langle \boldsymbol{x}^*,\boldsymbol{w}\rangle-\langle (\boldsymbol{M}^*)^{\top}\boldsymbol{z}',\boldsymbol{w}\rangle+a+\langle \boldsymbol{x},\boldsymbol{w}\rangle-\langle \boldsymbol{u},\boldsymbol{v}\rangle+\langle \boldsymbol{M}^{\top}\boldsymbol{z},\boldsymbol{w}\rangle)\bmod q$$

$$=\tau k_2(\langle \boldsymbol{x}-\boldsymbol{x}^*,\boldsymbol{w}\rangle+\langle (\boldsymbol{M}^*)^{\top}\boldsymbol{z}'-\boldsymbol{M}^{\top}\boldsymbol{z},\boldsymbol{w}\rangle)\bmod q.$$

若敌手解密 $CT_{S'}$，则 $\langle \boldsymbol{\theta}',\boldsymbol{\gamma}'\rangle=0\bmod q$. 若敌手可以区分 Leak_j 和 Leak_{j+1}，我们可以不可忽略的优势找出 N 的因式 q，并成功解决安全假设 2.

引理 7. 设泄露界 $\ell_{SK}=(n-1-2c)\log q$，c 是一正整数. 对任一 PPT 敌手 A 在 Leak_{j+1} 中把第 j 个密钥关联到挑战密文向量空间，把第 j 个半功能密钥替换成支配型密钥去解密挑战密文的优势是可忽略的.

证明. 假设一个 PPT 敌手 A 以不可忽略的优势达到上述的转换，我们可以构造一算法 B 以相同的优势区分 $(\boldsymbol{\delta}, f(\boldsymbol{\tau}))$ 和 $(\boldsymbol{\delta}, f(\boldsymbol{\tau}'))$ 从而攻击引理 1 和推论 1 的结论. 在本证明中主要考虑密钥结构，我们把主密钥当成超仿射空间的密钥，这样所有的泄露都由密钥泄露谕言机 O_{Leak} 生成. B 收到推论 1 的实例后，置 $m=n+1$，q 是 N 的因子. B 的目标是借助 A 证明上述两个分布有不可忽略的优势.

B 模拟 Leak_{j+1} 如下：首先运行 Init 算法生成主密钥 MSK 和系统公钥 MPK，把公钥 MPK 发送给敌手 A. 由于 B 知道系统主密钥，因此可以回答敌手的任何询问.

假定在第 j 个密钥询问中，敌手以不可忽略的优势选择与挑战空间有不动点的空间 S^*（如不能达到不可区分的优势，则敌手无法构造支配密钥去解密密文，同时不能区分两个分布）.

B 接下来回答 A 的请求生成泄露串. f 是一个 PPT 时间的函数，输入域是 Z_q^{n+1}，值域大小是 $2^{\ell_{SK}}$. B 收到 $(\boldsymbol{\delta}, f(\boldsymbol{\tau}))$，这里 $\boldsymbol{\tau}$ 是 $\boldsymbol{x}$ 或 $\boldsymbol{x}'$，B 使用 $f(\boldsymbol{\tau})$ 回答敌手的第 i 个密钥泄露询问如下：选择 $r_1, r_2, \boldsymbol{\theta}\in Z_q^{d+2}$，置 G_q 子群部分密钥 $\bar{g}^{\upsilon}$，这里 $\boldsymbol{\upsilon}=(\upsilon_1,\cdots,\upsilon_n, r_1, \upsilon_{n+1}+r_2, \boldsymbol{\theta})$.

A 询问挑战空间 S^*，若第 j 空间钥队列中不包含 S^*，B 失败并随机输出 $\boldsymbol{\tau}$ 是 $\boldsymbol{\delta}$ 正交的猜测. 否则，若第 j 个仿射空间是 $S=Aff(\boldsymbol{M},\boldsymbol{x})$，则存在一算法求解 $\boldsymbol{x}^*=\boldsymbol{x}+\boldsymbol{M}\boldsymbol{z}$. B 随机选择 $k_2\in Z_q$ 满足 $\upsilon_{n+1}+r_2$，$(r_1+\langle \boldsymbol{z},\boldsymbol{\theta}\rangle)k_2=0\bmod q$，然后使用 $(\boldsymbol{\delta}, k_2)\in Z_q^{n+2}$ 作为参数构造挑战密文. 若 $\boldsymbol{\delta}$ 与 $\boldsymbol{\upsilon}$ 正交，则第 j 个密钥是支配型半功能的，即 $(\upsilon_1,\cdots,\upsilon_n, r_1, \upsilon_{n+1}+r_2)+(0,\cdots,0,\langle \boldsymbol{x},\boldsymbol{\theta}\rangle) * \boldsymbol{\delta}=\langle \boldsymbol{\upsilon},\boldsymbol{\delta}\rangle+\delta_{n+1}r_2+(r_1+\langle \boldsymbol{x},\boldsymbol{\theta}\rangle)k_2=0\bmod q$. 若 $\boldsymbol{\delta}$ 与 $\boldsymbol{\upsilon}$ 不正交，则挑战密钥是真半功能的，即上式恒不为 0.

B 使用 A 的挑战输出以不可忽略的优势区分 $(\boldsymbol{\delta}, f(\boldsymbol{\tau}))$ 和 $(\boldsymbol{\delta}, f(\boldsymbol{\tau}))$. 这与引理 1 的推论 1 矛盾. 因此敌手在 Leak_{j+1} 中把一个半功能密钥替换成支配型半功能密钥的优势是可忽略的.

引理 8. 若安全假设 3 存在，则任何多项式时间内的敌手 A 无法区分 LeakCK 和 LeakCKM.

证明. 假设一多项式时间的敌手 A 以不可忽略的优势区分 LeakCK 和 LeakCKM，我们可以构建一算法 D 以相同的优势解决安全假设 3.

当 D 收到假设 3 的实例，D 的目标是猜测 $T=\hat{e}(g^{\alpha}, g^{s})$ 还是 $T(g,\bar{g},\hat{g}, X_1=g^{\alpha}\bar{g}^{t}, X_2=g^{s}\bar{g}^{t'}, T)$ 只能为 G_t 中的随机猜测. 为此，D 扮演模拟器并回答敌手 A 的询问及挑战如下：

(1) 初始化. D 随机选择 $a, \boldsymbol{v}, \boldsymbol{w}\in Z_N^{1+n+\kappa}$（此时 D 并不知道 α），公钥组件 $\hat{e}(g,g)^{\alpha}$ 可由 $\hat{e}(X_1, g)=\hat{e}(g,g)^{\alpha}$ 计算. 置系统公钥 $MPK=(N, g, \hat{g}, g^{a}, g^{\boldsymbol{v}}, g^{\boldsymbol{w}}, \hat{e}(g,g)^{\alpha})$ 并发送给 A.

(2) 询问 1. 为回答 A 的密钥询问，模拟器随机选择 $\boldsymbol{u}, r\in Z_N^n\times Z_N$，生成半功能密钥 $SK_S=(g^{\boldsymbol{u}}, X_1 g^{r(a+\langle \boldsymbol{x},\boldsymbol{w}\rangle-\langle \boldsymbol{u},\boldsymbol{v}\rangle)}, g^{r}, g^{r\boldsymbol{M}^{\top}\boldsymbol{w}}) * \hat{g}^{[n+d+2]} * \bar{g}^{[n+d+2]}$. 显然 D，SK_S 是半功能的.

(3) 挑战. A 提交给 D 两个挑战的消息 m_0, m_1

及挑战子空间 $S^*=Aff(\boldsymbol{M}^*,\boldsymbol{x}^*)$，模拟器 D 随机选择 $\beta\in\{0,1\}$，输出密文 $CT_{S^*}=(m_\beta\cdot T, X_2^{\nu}, X_2, X_2^{-a-\langle \boldsymbol{x}^*,\boldsymbol{w}\rangle}, X_2^{(\boldsymbol{M}^*)^{\top}\boldsymbol{w}})$.

(4) 询问 2. 与询问 1 相同，同时要求 A 不能对 S^* 及其超空间作 O_{Revl} 询问.

(5) 输出 $X_2=g^s\bar{g}^{t'}$. 当 $T=\hat{e}(g^{\alpha},g^s)$ 时，CT_{S^*} 是半功能化的，其半功能参数 $\boldsymbol{\gamma}=t'(\boldsymbol{u},1,-a-\langle \boldsymbol{x}^*,\boldsymbol{w}\rangle,(\boldsymbol{M}^*)^{\top}\boldsymbol{w})$，成功模拟 LeakCK.

当 T 是 G_t 中的随机元素时，c_m 是 G_t 中完全随机的元素，此时密文是一随机消息的半功能密文，β 在密文中是信息论隐藏的，成功模拟 LeakCKM. 若敌手 A 以不可忽略的优势猜测 β，D 使用 A 的输出成功解决安全假设 3.

定理 3 得证.　　证毕.

6　泄露性能分析

为分析密钥抗泄露性能，我们给出如下两个定义.

定义 6.　主密钥泄露率(Master-key Leakage Ratio). 可泄露的主密钥 MSK 大小与主密钥长度的比值称为主密钥泄露率 MLR. $MLR=\frac{\ell_{MSK}}{|MSK|}$.

定义 7.　密钥泄露率(Secret-key Leakage Ratio). 可泄露的用户密钥 SK_S 大小与密钥长度的比值称为密钥泄露率 SLR. $SLR=\frac{\ell_{SK}}{|SK_S|}$.

方案中主密钥长度是固定的，在参数确定的情况下泄露界也是确定的，因此 MLR 一般是确定的. 本方案具有密钥委托的功能，密钥长度在委托中随仿射子空间的维度变化. SLR 除与系统的参数有关外，还与仿射空间有关.

本方案支持有限界的密钥 SK_S 和主密钥 MSK 的抗泄露安全. 根据引理 1、推论 1 及引理 7，对于大素数 q，任意泄露函数的输出 $|\Omega|\leq 4q^{m-3}(q-1)\cdot \mathrm{negl}(\cdot)^2=4\left(1-\frac{1}{q}\right)q^{m-2}\cdot\mathrm{negl}(\cdot)^2\leq 4q^{m-2}\cdot\mathrm{negl}(\cdot)^2$. 为达到 $\mathrm{negl}(\cdot)$ 的可忽略性，设 $\mathrm{negl}(\cdot)=q^{-c}$，$n+1=m$，则可泄露的长度 $\ell_k=\log_2|\Omega|=2+(m-2-2c)\log_2 q=2+(n-1-2c)\log_2 q$ bit. 这里 n 是大于等于 2 的任意正整数，c 是可选择的常数. 显然，$N=pqr$，方案中泄露的界由子群 G_q 的阶 q 决定，与 p,r 无关，我们可以通过调整 G 子群的大小来实现优化的密钥长度和泄露界.

我们考虑 AES-80 标准的安全性，由于 N 要不能被因式分解，$N=1024$ bit，G 是椭圆曲线上的双线性群，$|G|=\log_2\lambda=1024$. 设 $|p|=a_1\lambda$，$|q|=a_2\lambda$，$|r|=a_3\lambda$，$(a_1,a_2,a_3>0)$. $MSK\in G_{pr}^{n+\kappa+2}$，$|MSK|=1024(n+\kappa+2)$ bit. 主密钥泄露率 $MLR=\frac{a_2(n-1-2c)}{(n+\kappa+2)(1+a_1+a_3)}$，而每个仿射子空间的密钥泄露率 $SLR=\frac{a_2(n-1-2c)}{(n+d+2)(1+a_1+a_3)}$，这里 $d=Dim(S)$. 可见，随着委托的深入，d 减小，密钥泄露率会变大，主要原因是仿射子空间越小，其密钥越短. 我们可以通过调整参数 n,c,a_1,a_2,a_3 可以得到不同的泄露率. 在图 1 中，在空间的最大维度设定为 50，子空间阶的大小分别是 160 bit、704 bit 和 160 bit 的情况下，我们分析密钥的泄露率随泄露参数 n 的变化. 结果显示，当 $n=100$ 时，密钥的可泄露率达到 73% 仍是安全的. 图 2 显示在 $n=100,\kappa=50,c=1$ 的情况下，系统性能随委托深度 d 的变化情况. 可知，随着委托的深入，用户的仿射角色空间变小($d=Dim(S)$递减)，但用户密钥的抗泄露能力提高.

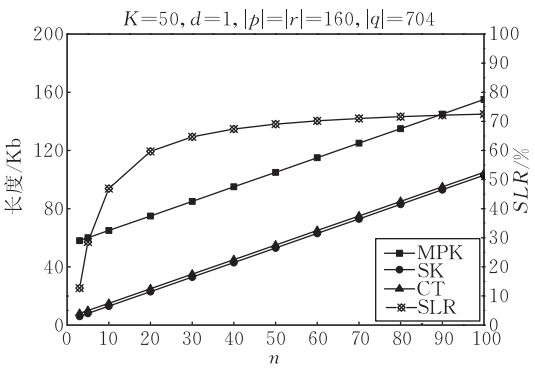

图 1　公钥 MPK/密钥 SK/密文 CT/泄露率 SLR 随泄露参数 n 的变化

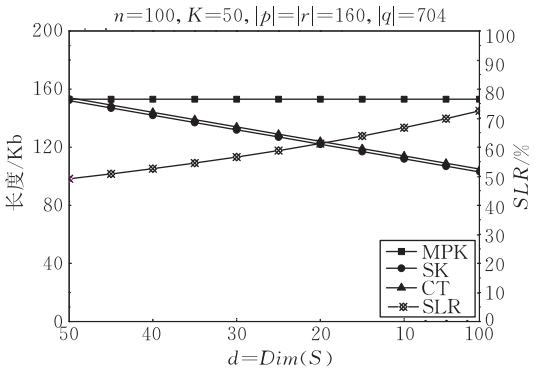

图 2　公钥 MPK/密钥 SK/密文 CT/泄露率 SLR 随仿射委托深度 d 的变化($d=Dim(S)$)

7　小　结

本文提出了一种抗主密钥泄露和连续用户密钥

泄露的双态仿射函数加密方案,在标准模型下证明了该方案的安全性,分析了方案中的主密钥和用户密钥的泄露界,通过优化参数可达到 73% 的泄露率,具有较好的抗泄露性能.改进本文方案达到通过设计高熵不可逆的函数达到支持无界密钥泄露的加密方案是接下来研究的目标.

参 考 文 献

[1] Akavia A, Goldwasser S, Vaikuntanathan V. Simultaneous hardcore bits and cryptography against memory attacks.//Proceedings of the TCC'09. LNCS 5444. San Francisco, CA, USA, 2009: 474-495

[2] Alwen J, Dodis Y, Wichs D. Leakage-resilient public-key in the bounded-retrieval model//Proceedings of the CRYPTO'09. Santa Barbara, CA, USA. LNCS 5677, 2009: 36-54

[3] Boyle E, Segev G, Wichs D. Fully leakage-resilient signatures//Proceedings of the EUROCRYPT'11. Tallinn, Estonia. LNCS 6632, 2011: 89-108

[4] Lewko A B, Lewko M, Waters B. How to leak on key updates//Proceedings of the STOC'11. San Jose, CA, USA, 2011: 725-734

[5] Lewko A B, Rouselakis Y, Waters B. Achieving leakage resilience through dual system encryption//Proceedings of the TCC'11. Rhode Island, USA. LNCS 6597, 2011: 70-88

[6] Chow S, Dodis D, Rouselakis, Waters B. Practical leakage-resilient identity-based encryption from simple assumptions//Proceedings of the ACM-CCS'10. Chicago, IL, USA, 2010: 152-161

[7] Alwen J, Dodis Y, Naor M. Public-key encryption in the bounded-retrieval model//Proceedings of the EUROCRYPT'10. Monaco and Nice, French Riviera. LNCS 6110, 2010: 113-134

[8] Brakershi Z, Kalai Y T, Katz J, Vaikuntanathan V. Overcoming the hole in the bucket: Public-key cryptogaphy resilient to continual memory leakage//Proceedings of the FOCS'10. Las Vegas, Nevada, USA, 2010: 501-510

[9] Boneh D, Hamburg M. Generalized identity based and broadcast encryption schemes//Proceedings of the ASIACRYPT'08. Melbourne, Australia. LNCS 5350, 2008: 455-470

[10] Zhou M, Cao Z. Spatial encryption under simple assumptions//Proceedings of the Provsec'09. Guangzhou, China. LNCS 5848, 2009: 19-31

[11] Moriyama D, Doi H. A fully secure spatial encryption scheme. IEICE Transactions, 2011, 94-A(1): 28-35

[12] Vie J J, Abdalla M. A leakage-resilient spatial encryption scheme//www. jill-jenn. net/works/a-leakage-resilient-spatial-encryption-scheme. pdf, 2011

[13] Kang Li, Wang Zhi-Yi. The efficient CCA secure public-key encryption scheme. Chinese Journal of Computers, 2011, 34(2): 236-242(in Chinese)
(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)

[14] Lewko A B, Waters B. New techniques for dual system encryption and fully secure hibe with short ciphertexts//Proceedings of the TCC'10. Zurich, Switzerland. LNCS 5978, 2010: 455-479

[15] Waters B. Dual system encryption: Realizing fully secure Ibe and Hibe under simple assumptions//Proceedings of the CRYPTO'09. Santa Barbara, CA, USA. LNCS 5677, 2009: 619-636

[16] Lewko A B, Waters B. Decentralizing attribute-based encryption//Proceedings of the EUROCRYPT'11. Tallinn, Estonia. LNCS 6632, 2011: 568-588

[17] Lee K, Lee D H. Improved hidden vector encryption with short ciphertexts and tokens. Designs, Codes and Cryptography, 2011, 58(3): 297-319

[18] Zhang M, Takagi T. GeoEnc: Geometric area based keys and policies in functional encryption systems//Proceedings of the ACISP'11. Melbourne, Australia. LNCS 6812, 2011: 241-258

[19] Okamoto T, Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption//Proceedings of the CRYPTO'10. Santa Barbara, CA, USA. LNCS 6223, 2010: 191-208

[20] Boldyreva A, Fehr S, O'Neill A. On notions of security for deterministic encryption, and efficient constructions without random oracles//Proceedings of the CRYPTO'08. Santa Barbara, CA, USA. LNCS 5157, 2008: 335-359

ZHANG Ming-Wu, born in 1970, Ph. D., associate professor. His research interests include cryptography technology, privacy preservation and network security.

YANG Bo, born in 1963, Ph.D., professor. His research interests include cryptography and information security.

TAKAGI Tsuyoshi, born in 1969, Ph. D., professor. His main research interests focus on the cryptography analysis and protocol.

Background

Traditionally, most security definitions assume that no information about the secret key is leaked. Otherwise, the security is broken. However, this is not practical due to unexpected attacks. Taking side-channel attacks as example, an adversary may attain the information about the internal state or the key from a hardware device (such as memory, communication cable, wireless channel etc), and then uses this information to break the security of a cryptographic primitive. In order to tolerant the possible key leakage, leakage-resilient cryptography models a class of leakage output by allowing the adversary is able to specify a computable leakage function and obtaining the partial keys or other possibly internal states from the output of function. An encryption scheme is semantically leakage-resilient secure if the adversary is able to gain the partial information about private keys or master keys.

In a delegatable encryption scheme, the delegation has the partial order relation such as reflexivity, antisymmetry and transitivity. We use a special algebra structure of partial order relation—affine space—as encryption policy and decryption role to construct a delegatable encryption scheme. In particular, the encryption policies and decryption roles are specified as the affine subspace and the delegations are defined as affine transformations over the affine spaces. Our scheme is leakage-resilient that supports the private key leakage resilience and the master key leakage resilience. Especially, the scheme is simplified as an IBE or HIBE when the affine subspace is reduced as a point vector in affine space. We prove the security from the technique of dual system encryption and statistical indistinguishability of orthogonal subspaces. We also give the leakage performance and show it gains approximate 73% leakage ratio.

This paper is supported by the National Natural Science Foundation of China under Grant Nos. 60973134, 61173164 and 61272404, Guangdong Natural Science Foundation under Grant No. 10151064201000028, and Grant-in-Aid for JSPS Fellows of Japan under Grant No. 22-00045.