Journal of Computer Applications
计算机应用,2014,34(5):1288 - 1291
ISSN 1001-9081
CODEN JYIIDU
2014-05-10
http://www.joca.cn

文章编号:1001 - 9081(2014)05-1288-04
doi:10.11772/j.issn.1001-9081.2014.05.1288

基于适应性选择密文不可区分性的抗辅助输入泄漏公钥加密方案

王占君[1],马海英[2,3*],王金华[1]

(1.南通大学 理学院,江苏 南通 226007; 2.同济大学 计算机科学与技术系,上海 201804;
3.南通大学 计算机科学与技术学院,江苏 南通 226019)

(*通信作者电子邮箱 m_hying@163.com)

摘 要:现有的抗辅助输入公钥加密方案仅满足选择明文攻击(IND-CPA)安全性,难以满足实际应用的安全需求。基于判定性 Diffie-Hellman (DDH)假设下 CS'98 加密方案和域 $GF(q)$ 上 Goldreich-Levin 定理,构造出一种新型的抗辅助输入泄漏的公钥加密方案。该方案满足适应性选择密文不可区分性(IND-CCA2)安全性,允许攻击者利用辅助输入泄漏信息攻击挑战密文时询问解密预言机。与 BHHO 加密方案相比,尽管加密/解密运算量都增加了近一倍,却实现了更加严格的 IND-CCA2 安全性。

关键词:公钥加密;辅助值输入;适应性选择密文不可区分性;Goldreich-Levin 定理

中图分类号:TP309 **文献标志码**:A

Public key encryption scheme with auxiliary inputs based on indistinguishability under adaptive chosen ciphertext attack

WANG Zhanjun[1], MA Haiying[2,3*], WANG Jinhua[1]

(1. *School of Science, Nantong University, Nantong Jiangsu* 226007, *China*;
2. *Department of Computer Science and Technology, Tongji University, Shanghai* 201804, *China*;
3. *College of Computer Science and Technology, Nantong University, Nantong Jiangsu* 226019, *China*)

Abstract: The existing public key encryption schemes with auxiliary inputs are impractical since they are only of Indistinguishability under Chosen Plaintext Attack (IND-CPA) security. This paper constructed a novel public-key encryption scheme resilient to auxiliary input leakage, which was based on CS'98 encryption scheme and Goldreich-Levin theorem over large field $GF(q)$. The proposed scheme was based on Indistinguishability under Adaptive Chosen Ciphertext Attack (IND-CCA2) security, allowing an attacker to query decryption oracle with auxiliary input leakage when it tried to attack the challenge ciphertext. Compared with the BHHO (Boneh, Halevi, Hamburg, Ostrovsky) encryption scheme, the proposed scheme realizes the more strict IND-CCA2 security in spite of the encryption's and decryption's overhead being nearly doubled.

Key words: public key encryption; auxiliary input; Indistinguishability under Adaptive Chosen Ciphertext Attack (IND-CCA2); Goldreich-Levin theorem

0 引言

现代密码学假定所有攻击者均不能获知用户密钥的任何信息,且要求用户密钥在不同系统中独立选取。然而,在实际应用中,攻击者往往可以利用能量消耗、冷启动等各种边信道攻击获知密钥的部分信息,或者用户在不同密码系统中使用相同的密钥或秘密随机值也会造成部分密钥信息的泄漏。

近年来,学者们针对这些攻击提出了许多不同的泄漏模型[1-9]。2009 年 Akavia 等[1] 在密码学理论会议(Theory of Cryptography Conference, TCC)上首先提出了有界泄漏模型,为了模拟密钥(Secret Key, SK)泄漏,攻击者可以选择任意可计算性函数 $f: SK \rightarrow \{0,1\}^*$,并得到关于 SK 的输出结果(显然,必要的限制是攻击者所选函数 f 不能完全暴露密钥);该模型[1,5] 要求所有可计算泄漏函数 f 的输出长度总和 ℓ 不能超过预定的边界值(该值必须小于密钥长度,且是它的某个分数倍)。Naor[2] 提出了有噪泄漏模型,减少了对泄漏函数 f 限制,允许攻击者获知更多的泄漏信息。为进一步放松对泄漏函数 f 的限制。2009 年 Dodis 等[3] 在计算机理论研讨会(Symposium on Theory of Computing, STOC)上提出了辅助值输入泄漏模型,攻击者能够获知不少于密钥长度的泄漏信息,唯一的限制是任意泄漏函数 f 可逆的概率都是可忽略的,即攻击者利用泄漏信息 $f(SK)$ 仅能以可忽略的优势计算出密钥 SK;同时,Dodis 等[3] 构造出选择明文/密文安全的抗辅助输入泄漏的对称加密方案。2010 年 Dodis 等[4] 在 TCC 会议上将辅助输入泄漏模型扩展到公钥加密体制中,基于误差学习假设和判定性 Diffie-Hellman (Decisional Diffie-Hellman, DDH)假设,构建了 3 个抗辅助输入泄漏的公钥加密方案;然而这些方案仅满足选择明文攻击安全性(Indistinguishability under Chosen Plaintext Attack, IND-CPA),即在利用泄漏信息试图攻破挑战密

收稿日期:2013-11-18;**修回日期**:2014-01-22。

基金项目:国家自然科学基金资助项目(61272424, 11371207);国家科技支撑计划项目(2012BAH15F03);上海自然科学基金资助项目(13ZR1443100);江苏省高校自然科学研究项目(12KJB520015);南通市科技计划项目(BK2013050, BK2012026, BK2011070)。

作者简介:王占君(1978 -),男,河南鹤壁人,讲师,硕士,主要研究方向:密码学、Hopf 代数; 马海英(1977 -),女,河南卫辉人,讲师,博士研究生,主要研究方向:密码学、网络安全; 王金华(1963 -),男,江苏南通人,教授,博士,主要研究方向:编码密码学、组合设计理论。

文时,不允许攻击者询问解密预言机。尽管 IND-CPA 安全的公钥加密方案具有一定的理论研究价值,但是在实际应用中往往允许攻击者询问解密预言机,且适应性选择密文不可区分性(Indistinguishability under Adaptive Chosen Ciphertext Attack, IND-CCA2)的安全性已成为公钥加密系统的实用性标准。因此,构造 IND-CCA2 抗辅助值输入的公钥加密方案将是一项非常有意义的研究工作。

本文首先给出抗辅助输入公钥加密的 IND-CCA2 安全性定义。通过修改 CS '98 公钥加密方案[10],将辅助值输入泄漏模型扩展到该方案中,基于 DDH 假设和域 $GF(q)$ 上 Goldreich-Levin 定理[4],构造出一种具体的 IND-CCA2 抗辅助值输入泄漏的公钥加密方案,在利用泄漏信息试图攻破挑战密文时,允许攻击者询问解密预言机,实现了更严格安全性定义下的抗辅助值输入的公钥加密机制。

1　预备知识

本章将简要阐述构造本文方案的基础知识,主要包括 DDH 假设和域 $GF(q)$ 上 Goldreich-Levin(GL)定理。

1.1　DDH 假设

令 n 是系统的安全性参数,Γ 是概率多项式时间(Probabilistic Polynomial Time, PPT)群生成器,当输入 n 时,Γ 输出一个具有素数阶 $q = q(n)$ 的群 G。如果对任意 PPT 算法 Alg,元组$\{(g_1, g_2, g_1^r, g_2^r): g_i \in G, r \in \mathbf{Z}_q\}$ 和$\{(g_1, g_2, g_1^{r_1}, g_2^{r_2}): g_i \in G, r_i \in \mathbf{Z}_q\}$ 都是不可区分的。

引理 1[4]　DDH 假设可以扩展为:对任意 PPT 算法 Alg 和任意正整数 m,元组$\{(g_1, g_2, \cdots, g_m, g_1^r, g_2^r, \cdots, g_m^r): g_i \in G, r \in \mathbf{Z}_q\}$ 和$\{(g_1, g_2, \cdots, g_m, g_1^{r_1}, g_2^{r_2}, \cdots, g_m^{r_m}): g_i \in G, r_i \in \mathbf{Z}_q\}$ 都是不可区分的。

1.2　域 $GF(q)$ 上 Goldreich-Levin 定理

令 q 是一个大素数,H 是 $GF(q)$ 的任意子集,n 是一个正整数,$f: H^n \to \{0,1\}^*$ 是任意函数。令向量 $\boldsymbol{s} \leftarrow H^n$,$y \leftarrow f(\boldsymbol{s})$,$\boldsymbol{r} \leftarrow GF(q)^n$,如果存在区分器 D 在 t 时间内使得:

$$\left| \Pr[D(y, \boldsymbol{r}, \langle \boldsymbol{r}, \boldsymbol{s} \rangle) = 1] - \Pr[u \leftarrow GF(q): D(y, \boldsymbol{r}, u) = 1] \right| = \varepsilon$$

则存在一个可逆器 Inv 在 $t' = t \cdot poly(n, |H|, 1/\varepsilon)$ 时间内求得 $\boldsymbol{s}$ 的概率:

$$\Pr[\boldsymbol{s} \leftarrow H^n, y \leftarrow f(\boldsymbol{s}): Inv(y) = \boldsymbol{s}] \geqslant \varepsilon^3/(512 \cdot n \cdot q^2)。$$

2　IND-CCA2 安全性定义和辅助输入函数族

2.1　IND-CCA2 安全性定义

定义 1　给定公钥加密方案 $\Pi = (Gen, Enc, Dec)$ 和辅助输入函数族 Φ,Π 在 Φ 下的 IND-CCA2 安全性由攻击者 A 和仿真器 S 之间的游戏定义如下:

1) KeyGen。S 运行密钥生成算法 KeyGen(n, ε),得到公/私钥对 (PK, SK),并将 PK 发送给 A。

2) 询问阶段 1。A 可以询问如下的预言机和辅助输入函数:

① 解密预言机 ODec$(\cdot)$。A 提交密文 CT 给 ODec$(\cdot)$,S 运行 ODec$(\cdot)$ 解密 CT,返回相应的信息;

② 泄漏预言机 $OL(\cdot)$。对任意辅助输入函数 $f \in \Phi$,A 提交 f 给 S,S 将 $f(PK, SK)$ 返回给 A。

3) 挑战阶段。A 提交两个等长的消息 M_0, M_1 给 S,S 随机选择 $b \in \{0,1\}$,计算挑战密文 $CT^* = \text{Enc}(PK, M_b)$,并将 CT^* 发送给 A。

4) 询问阶段 2。与询问阶段 1 相同,除了 A 不能将挑战密文 CT^* 提交给解密预言机 ODec$(\cdot)$,且不能进行泄漏询问。

5) 猜测。A 输出 b 的猜测值 b'。

当 $b = b'$ 时,称敌手 A 赢得上述游戏;否则,A 失败。下面定义 A 赢得上述游戏的优势为 $Adv_{A,f}(n) = |\Pr[b = b'] - 1/2|$。如果对任意 PPT 攻击者 A 和任意辅助助输入函数 $f \in \Phi$,A 的优势 $Adv_{A,f}(n)$ 都是可以忽略的,则称公钥加密方案 Π 在辅助输入函数族 Φ 下是 IND-CCA2 安全的。

2.2　辅助输入函数族

由于本文借鉴 Dodis 等[4]提出的辅助输入泄漏模型,我们将简述与该模型相关的两类辅助输入函数族。令密钥 SK 是长度为 k 的随机串,PK 是与其对应的公钥。Φ_{OW} 和 $\Phi_{\text{PK-OW}}$ 是两类辅助输入函数族,唯一的限制是根据泄漏信息很难计算出密钥 SK。依据文献[4]的引理 3.1,可推理出如下结论:

1) $\Phi_{\text{OW}}(h(k))$ 是一个多项式时间(PPT)可计算的函数族 $f: \{0,1\}^{|SK|+|PK|} \to \{0,1\}^*$,使得给定 $f(PK, SK)$,任意 PPT 算法求得 SK 的概率都不超过 $h(k) \geqslant 2^{-k}$。如果公钥加密方案 Π 在函数族 $\Phi_{\text{OW}}(h(k))$ 下是 IND-CCA2 安全的,则称该方案 Π 是 $h(k)$-AI-CCA2 安全的(又称强辅助输入的 CCA2 安全性)。

2) $\Phi_{\text{PK-OW}}(h(k))$ 是一个 PPT 可计算的函数族 $f: \{0,1\}^{|SK|+|PK|} \to \{0,1\}^*$,使得给定 PK 和 $f(PK, SK)$,任意 PPT 算法求得 SK 的概率都不超过 $h(k) \geqslant 2^{-k}$。如果公钥加密方案 Π 在函数族 $\Phi_{\text{PK-OW}}(h(k))$ 下是 IND-CCA2 安全的,则称该方案 Π 是 $h(k)$-wAI-CCA2 安全的(又称弱辅助输入的 CCA2 安全性)。

引理 2[4]　给定公钥加密方案 Π,令其公钥长度为 $t(k)$,满足以下 2 个结论:

1) 若 Π 是 $h(k)$-AI-CCA2 安全的,则 Π 是 $h(k)$-wAI-CCA2 安全的;

2) 若 Π 是 $h(k)$-wAI-CCA2 安全的,则 Π 是 $(2^{-t(k)} \cdot h(k))$-AI-CCA2 安全的。

3　IND-CCA2 抗辅助值输入的公钥加密方案

令 n 是安全性参数,Γ 是概率多项式时间的群生成器,当输入 n 时,Γ 输出一个具有素数阶 $q = q(n)$ 的群 G。

KeyGen(n, ε)　令 $0 < \varepsilon < 1$,$m = (6 \text{ lb } q)^{1/\varepsilon}$,$G \leftarrow \Gamma(n)$。对 $i = 1, 2, \cdots, m$,该密钥生成算法随机选择生成元 g_i,$\bar{g}_i \in G$ 和 $x_i, \bar{x}_i, y_i, \bar{y}_i \in \mathbf{Z}_q$,$z_i \in \{0,1\}$,计算:$c = \prod_{i=1}^{m} g_i^{x_i} \bar{g}_i^{\bar{x}_i}$,$d = \prod_{i=1}^{m} g_i^{y_i} \bar{g}_i^{\bar{y}_i}$,$h = \prod_{i=1}^{m} g_i^{z_i}$;然后,取哈希函数 H。用户公钥 $PK = (\boldsymbol{g}, c, d, h, H)$,其中 $\boldsymbol{g} = (g_1, \bar{g}_1, g_2, \bar{g}_2, \cdots, g_m, \bar{g}_m)$,用户私钥 $SK = (\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$,其中:$\boldsymbol{x} = (x_1, \bar{x}_1, x_2, \bar{x}_2, \cdots, x_m, \bar{x}_m)$,$\boldsymbol{y} = (y_1, \bar{y}_1, y_2, \bar{y}_2, \cdots, y_m, \bar{y}_m)$,$\boldsymbol{z} = (z_1, z_2, \cdots, z_m)$。

Enc(M, PK)　给定消息 $M \in G$,该加密算法首先选择随机数 $r \in \mathbf{Z}_q$,对 $i = 1, 2, \cdots, m$,计算:$u_i = g_i^r$,$\bar{u}_i = \bar{g}_i^r$,$e = M \cdot h^r$,$\alpha = H(u_1, \bar{u}_1, \cdots, u_m, \bar{u}_m, e)$,$v = c^r d^{r\alpha}$,密文 $CT = ((u_i, \bar{u}_i)_{i=1,2,\cdots,m}, e, v)$。

Dec(CT, SK)　给定密文 CT,对 $i = 1, 2, \cdots, m$,该解密算法首先计算 $\alpha = H(u_1, \bar{u}_1, \cdots, u_m, \bar{u}_m, e)$,验证 $\prod_{i=1}^{m} u_i^{x_i + y_i \cdot \alpha} \bar{u}_i^{\bar{x}_i + \bar{y}_i \cdot \alpha} = v$

是否成立:如等式成立,则输出消息 $M = e \cdot \left(\prod_{i=1}^{m} u_i^{z_i}\right)^{-1}$;否则,拒绝解密。

正确性 按照该加密方案生成的密文都能被正确解密。

证明 由于 $u_i = g_i^r, \bar{u}_i = \bar{g}_i^r$,所以:

$$\prod_{i=1}^{m} u_i^{x_i+y_i\cdot\alpha}\bar{u}_i^{\bar{x}_i+\bar{y}_i\cdot\alpha} = \prod_{i=1}^{m}(g_i^{x_i+y_i\cdot\alpha}\bar{g}_i^{\bar{x}_i+\bar{y}_i\cdot\alpha})^r = \prod_{i=1}^{m}(g_i^{x_i}\bar{g}_i^{\bar{x}_i})^r\prod_{i=1}^{m}(g_i^{y_i}\bar{g}_i^{\bar{y}_i})^{r\alpha} = c^r d^{r\alpha}$$

所以密文通过验证,然后:

$$e \cdot \left(\prod_{i=1}^{m} u_i^{z_i}\right)^{-1} = M \cdot h^r \cdot \left(\prod_{i=1}^{m} u_i^{z_i}\right)^{-1} = M \cdot \left(\prod_{i=1}^{m} g_i^{z_i}\right)^r \cdot \left(\prod_{i=1}^{m} u_i^{z_i}\right)^{-1} = M$$

4 安全性证明和性能比较

4.1 安全性证明

定理 1 如果 DDH 假设在群 G 上是成立的,则本文的加密方案是(2^{-m^e})-AI-CCA2 安全的(当$\boldsymbol{g}$ 被作为公共参数时)。

证明 根据引理2(第2部分)和用户公钥长度为3 lb q,要证明定理 1 成立,仅需证明本文的加密方案是$(q^3 \cdot 2^{-m^e})$-wAI-CCA2 安全的。因此,对于任意辅助值输入函数 f,在给定$(\boldsymbol{g},c,d,h,f(\boldsymbol{g},\boldsymbol{x},\boldsymbol{y},z))$的前提下,求向量 $\boldsymbol{z}$ 的概率不超过 $q^3 \cdot 2^{-m^e}$。此外,定义任意 PPT 攻击者 A 攻破该加密方案的优势为 $\delta = \delta(n) = Adv_{A,f}(n)$。

为了计算 $Adv_{A,f}(n)$,需考虑一系列实验,用 $Adv_{A,f}^{(i)}(n)$ 表示 A 在第 i 个实验中的优势。

实验 1 该实验就是定义 1 中的实验。攻击者 A 获得 $PK = (\boldsymbol{g},c,d,h,H)$、辅助输入值 $f(\boldsymbol{g},\boldsymbol{x},\boldsymbol{y},z)$ 和解密预言机。当 A 进行解密询问时,解密预言机类似解密算法,首先验证等式 $\prod_{i=1}^{m} u_i^{x_i+y_i\cdot\alpha}\bar{u}_i^{\bar{x}_i+\bar{y}_i\cdot\alpha} = v$,输出 $M = e \cdot \left(\prod_{i=1}^{m} u_i^{z_i}\right)^{-1}$。$A$ 选择两个等长消息 M_0 和 M_1,然后,得到挑战密文 $CT^* = \mathrm{Enc}(M_b, PK)$,其中:随机值 $b \in \{0,1\}$。最后,A 输出 b 的猜测值 b'。如果 $b = b'$,则 A 赢得该实验;否则,失败。由定义可知 $Adv_{A,f}^{(0)}(n) = Adv_{A,f}(n) = \delta$。

实验 2 与实验 1 类似,除了挑战密文 CT^* 是用私钥生成的,而不是 $\mathrm{Enc}(M_b, PK)$。特别地,定义 $\mathrm{Enc}'(M_b,\boldsymbol{g},\boldsymbol{x},\boldsymbol{y},z)$ 如下:选择随机值 $r \in \mathbf{Z}_q$,对 $i = 1,2,\cdots,m$,计算:$u_i = g_i^r$, $\bar{u}_i = \bar{g}_i^r, e = M_b \cdot \prod_{i=1}^{m} u_i^{z_i}, \alpha = H(u_1,\bar{u}_1,\cdots,u_m,\bar{u}_m,e), v = \prod_{i=1}^{m} u_i^{x_i+y_i\cdot\alpha}\bar{u}_i^{\bar{x}_i+\bar{y}_i\cdot\alpha}$,密文 $CT^* = ((u_i,\bar{u}_i)_{i=1,2,\cdots,m}, e, v)$。

断言 1 $\mathrm{Enc}'(M_b,\boldsymbol{g},\boldsymbol{x},\boldsymbol{y},z)$ 和 $\mathrm{Enc}(M_b, PK)$ 生成的挑战密文是不可区分的,即 $Adv_{A,f}^{(0)}(n) = Adv_{A,f}^{(1)}(n)$。

证明 给定$\boldsymbol{g},\boldsymbol{x},\boldsymbol{y},z$,则 c,d,h 将被确定。选择随机值 $r \in \mathbf{Z}_q$,对 $i = 1,2,\cdots,m$,加密算法 $\mathrm{Enc}'()$ 计算:$u_i = g_i^r, \bar{u}_i = \bar{g}_i^r$, $e = M_b \cdot \prod_{i=1}^{m} u_i^{z_i} = M_b \cdot \left(\prod_{i=1}^{m} g_i^{z_i}\right)^r = M_b \cdot h^r, \alpha = H(u_1,\bar{u}_1,\cdots,u_m,\bar{u}_m,e)$, $v = \prod_{i=1}^{m} u_i^{x_i+y_i\cdot\alpha}\bar{u}_i^{\bar{x}_i+\bar{y}_i\cdot\alpha} = \prod_{i=1}^{m}(g_i^{x_i+y_i\cdot\alpha}\bar{g}_i^{\bar{x}_i+\bar{y}_i\cdot\alpha})^r = \prod_{i=1}^{m}(g_i^{x_i}\bar{g}_i^{\bar{x}_i})^r\prod_{i=1}^{m}(g_i^{y_i}\bar{g}_i^{\bar{y}_i})^{r\alpha} = c^r d^{r\alpha}$。

由 Enc() 定义可知,这两个加密算法生成的挑战密文是完全相同的。

实验 3 与实验 2 类似,除了挑战密文中的向量$(u_i, \bar{u}_i)_{i=1,2,\cdots,m}$ 是取值于 G^{2m} 的均匀分布,即 $u_i = g^{r_i}, \bar{u}_i = \bar{g}^{\bar{r}_i}$,其中 $\boldsymbol{g}$ 是 G 的某个生成元,随机数 $r_i, \bar{r}_i \in \mathbf{Z}_q$,且相互独立。

$$e = M_b \cdot \prod_{i=1}^{m} u_i^{z_i}$$

$$\alpha = H(u_1,\bar{u}_1,\cdots,u_m,\bar{u}_m,e)$$

$$v = \prod_{i=1}^{m} u_i^{x_i+y_i\cdot\alpha}\bar{u}_i^{\bar{x}_i+\bar{y}_i\cdot\alpha}$$

与实验 2 相同。由 DDH 假设和引理 1,A 至多以可以忽略的优势区分实验 2 和实验 3。

断言 2 如果 DDH 假设成立,对任意 PPT 敌手 A 和辅助输入函数 f,则 $\left|Adv_{A,f}^{(1)}(n) - Adv_{A,f}^{(2)}(n)\right| \leqslant negl(n)$,其中:$negl(n)$ 表示一个可忽略的函数,即对任意多项式函数 $P(n)$,当 $n \to \infty$ 时,$negl(n)$ 比 $1/P(n)$ 趋于 0 的速度更快。

证明 在实验 2 中,挑战密文 $CT = \left(u_1 = g_1^r, \bar{u}_1 = \bar{g}_1^r, \cdots, u_m = g_m^r, \bar{u}_m = \bar{g}_m^r, e = M_b \cdot \prod_{i=1}^{m} u_i^{z_i}, \alpha = H(u_1,\bar{u}_1,\cdots,u_m,\bar{u}_m,e), v = \prod_{i=1}^{m} u_i^{x_i+y_i\cdot\alpha}\bar{u}_i^{\bar{x}_i+\bar{y}_i\cdot\alpha}\right)$。在实验 3 中,挑战密文 $CT = \left(u_1 = g^{r_1}, \bar{u}_1 = \bar{g}^{\bar{r}_1}, \cdots, u_m = g^{r_m}, \bar{u}_m = \bar{g}^{\bar{r}_m}, e = M_b \cdot \prod_{i=1}^{m} u_i^{z_i}, \alpha = H(u_1,\bar{u}_1,\cdots,u_m,\bar{u}_m,e), v = \prod_{i=1}^{m} u_i^{x_i+y_i\cdot\alpha}\bar{u}_i^{\bar{x}_i+\bar{y}_i\cdot\alpha}\right)$。由 DDH 假设可知,这两个挑战密文是不可区分的。

实验 4 与实验 3 类似,除了挑战密文中的 e 被 G 中的一个随机元素所替代,即挑战密文为$((u_i = g^{r_i}, \bar{u}_i = \bar{g}^{\bar{r}_i})_{i=1,2,\cdots,m}, \alpha = H(u_1,\bar{u}_1,\cdots,u_m,\bar{u}_m,e), e = g^u, v = u_i^{x_i+y_i\cdot\alpha}\bar{u}_i^{\bar{x}_i+\bar{y}_i\cdot\alpha})$,其中:随机数 $u, r_i, \bar{r}_i \in \mathbf{Z}_q$,且相互独立。

断言 3 对任意 PPT 攻击者 A 和辅助输入函数 f,$\left|Adv_{A,f}^{(2)}(n) - Adv_{A,f}^{(3)}(n)\right| \leqslant negl(n)$。

证明 如果存在一个攻击者 A 以 δ 优势区分实验 3 和实验 4,则可以构造一个仿真器 B 可以相同的优势区分$(PK, f(\boldsymbol{g},\boldsymbol{x},\boldsymbol{y},z), \boldsymbol{r} \in \mathbf{Z}_q^m, \langle \boldsymbol{r},z\rangle)$和$(PK, f(\boldsymbol{g},\boldsymbol{x},\boldsymbol{y},z), \boldsymbol{r} = (r_1,\cdots,r_m) \in \mathbf{Z}_q^m, u)$。$B$ 生成 $PK = (\boldsymbol{g},c,d,h,H)$、辅助输入值 $f(\boldsymbol{g},\boldsymbol{x},\boldsymbol{y},z)$、$u$ 和解密预言机,解密预言机类似解密算法。A 选择两个等长消息 M_0 和 M_1;然后,得到挑战密文 $CT^* = \left((u_i = g^{r_i}, \bar{u}_i = g^{\bar{r}_i})_{i=1,2,\cdots,m}, e = M_b \cdot g^u, \alpha = H(u_1,\bar{u}_1,\cdots,u_m,\bar{u}_m,e), v = \prod_{i=1}^{m} u_i^{x_i+y_i\cdot\alpha}\bar{u}_i^{\bar{x}_i+\bar{y}_i\cdot\alpha}\right)$,其中:随机值 $b \in \{0,1\}$;最后,A 输出 b 的猜测值 b'。如果 $b = b'$,则 B 输出 1;否则,输出 0。由上述构造可知,当 $u = \langle \boldsymbol{r},z\rangle$ 时,B 完美仿真实验 3;当 u 为随机值时,B 完美仿真实验 4。因此,B 也以 δ 的优势区分实验 3 和实验 4,即 B 以 δ 的优势区分$(PK, f(\boldsymbol{g},\boldsymbol{x},\boldsymbol{y},z), \boldsymbol{r} \in \mathbf{Z}_q^m, \langle \boldsymbol{r},z\rangle)$和$(PK, f(\boldsymbol{g},\boldsymbol{x},\boldsymbol{y},z), \boldsymbol{r} \in \mathbf{Z}_q^m, u)$。根据扩展的 GL 定理,可以构造一个算法以 $\frac{\delta^3}{512mq^2} = q^3\frac{\delta^3}{512mq^5} = q^3\frac{\delta^3 q}{512mq^6} = q^3\frac{\delta^3 q}{512m}\frac{1}{q^6} > q^3 2^{-m^e}$ 的概率求得 f 的原象 $\boldsymbol{z}$,其中当 n 充分大时,$\frac{\delta^3 q}{512m} > 1$。这与关于 f 的假设矛盾,因此 $\left|Adv_{A,f}^{(2)}(n) -\right.$

$Adv^{(3)}_{A,f}(n)\mid \leqslant negl(n)$。

在实验4中,挑战密文与b无关,因此在在实验4中A的优势为零,即$Adv^{(3)}_{A,f}(n)=0$,又由于实验系列相互不可区分,因此$Adv_{A,f}(n)\leqslant negl(n)$。

4.2　与其他方案的性能比较

本节将 BHHO 的抗辅助输入公钥加密方案和本文方案的各项性能指标进行比较,并在表 1 中具体列出,其中:q 表示群G的阶,$m=(6\ \mathrm{lb}\ q)^{1/\varepsilon}$,M、E 和 ME 分别为群$G$中的乘法、指数和多指数运算。从表 1 的各项数据可以看出:本方案与 BHHO 方案相比,虽然密钥长度、密文长度、加/解密运算量有所增加,但本方案却实现了更为严格的 IND-CCA2 安全性,更能满足现实生活中对密码学算法的安全需求。与文献[11－12]相比,本文实现了公钥加密环境下的无界泄露,而文献[11]仅实现了公钥加密环境中的有界泄露;文献[12]实现了身份基加密系统中的连续有界泄露。随着计算机性能的逐步提高,本文方案中增加的计算开销是可以容忍的,因此,该方案仍具有很强的实用性。

表 1　抗辅助输入公钥加密方案性能比较

方案	密钥长度	密文长度	加密运算量	泄露程度	安全性
BHHO[4]	m	$(m+1)\mathrm{lb}\,q$	$(m+1)$E+1M	1ME+M	CPA
本文方案	$(4\mathrm{lb}\,q+1)m$	$2(m+1)\mathrm{lb}\,q$	$(2m+1)$ E+2M	2ME+M	IND-CCA2

5　结语

本文首先给出抗辅助输入公钥加密的 IND-CCA2 安全性定义。基于 DDH 假设和域$GF(q)$上 Goldreich-Levin 定理,对 CS '98 加密方案进行改造,提出一个新的 IND-CCA2 抗辅助值输入的公钥加密方案。与 BHHO 方案相比,虽然密钥/密文长度和计算开销有所增加,但是,却实现了更严格的 IND-CCA2 安全性。

参考文献:

[1] AKAVIA A, GOLDWASSER S, VAIKUNTANATHAN V. Simultaneous hardcore bits and cryptography against memory attacks [C]// Proceedings of the 6th Theory of Cryptography Conference. Berlin: Springer-Verlag, 2009: 474－495.

[2] NAOR M, SEGEV G. Public-key cryptosystems resilient to key leakage [C]// Proceeding of the 29th Annual International Cryptology Conference. Berlin: Springer-Verlag, 2009: 18－35.

[3] DODIS Y, KALAI Y T, LOVETT S. On cryptography with auxiliary input [C]// Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009: 621－630.

[4] DODIS Y, GOLDWASSER S, KALAI Y T, *et al*. Public-key encryption schemes with auxiliary inputs [C]// TCC '10: Proceedings of the 7th International Conference on Theory of Cryptography. Berlin: Springer-Verlag, 2010: 361－381.

[5] ALWEN J, DODIS Y, WICHS D. Leakage-resilient public-key cryptography in the bounded-retrieval model [C]// Proceeding of the 29th Annual International Cryptology Conference. Berlin: Springer-Verlag, 2009: 36－54.

[6] DZIEMBOWSKI S, PIETRZAK K. Leakage-resilient cryptography [C]// Proceeding of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 2008: 293－302.

[7] PIETRAK K. A leakage-resilient mode of operation [C]// Proceeding of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2009: 462－482.

[8] PETIT C, STANDAERT F X, PEREIRA O, *et al*. A block cipher based pseudo random number generator secure against side-channel key recovery[C]// Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2008: 56－65.

[9] MICALI S, REYZIN L. Physically observable cryptography (extended abstract) [C]// Proceedings of the 2004 1st Theory of Cryptography Conference. Berlin: Springer-Verlag, 2004: 278－296.

[10] CRAMER R, SHOUP V. A practical public key encryption system provably secure against adaptive chosen ciphertext attack [C]// CS '98: Proceeding of the 18th Annual International Cryptology Conference. Berlin: Springer-Verlag, 1998: 13－25.

[11] ALWEN J, DODIS Y, NAOR M, *et al*. Public-key encryption in the bounded-retrieval model [C]// Proceeding of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2010: 113－134.

[12] LEWKO A, ROUSELAKIS Y, WATERS B. Achieving leakage resilience through dual system encryption [C]// TCC '11: Proceedings of the 8th Conference on Theory of Cryptography. Berlin: Springer-Verlag, 2011: 70－88.

(上接第 1258 页)

[4] HWANG K, DONGARRA J, FOX G C, *et al*. Distributed and cloud computing: from parallel processing to the Internet of things [M]. San Francisco: Morgan Kaufmann, 2011.

[5] DARLINGTON J, COHEN J, LEE W. An architecture for a next-generation Internet based on Web services and utility computing [C]// WETICE '06: Proceedings of the 15th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. Piscataway: IEEE Press, 2006: 169－174.

[6] XU W, CHA J. A manufacturing grid architecture based on Jini and SORCER [C]// Proceedings of the 16th ISPE International Conference on Concurrent Engineering. Berlin: Springer, 2009: 855－864.

[7] The Apache Software Foundation. Apache river news [EB/OL]. [2013-05-18]. http://river.apache.org/.

[8] School of Mechatronic Systems Engineering. Product design and optimization laboratory [EB/OL]. [2013-02-12]. http://www.sfu.ca/~gwa5/index.html.

[9] SRIKANTH G U, MAHESWARI V U, SHANTHI A P, *et al*. A survey on real time task scheduling [J]. European Journal of Scientific Research, 2012, 69(1): 33－41.

[10] MAO J. Task scheduling of parallel programming systems using ant colony optimization [EB/OL]. [2013-03-11]. http://www.academypublisher.com/proc/iscsct10/papers/iscsct10p179.pdf.

[11] BLUM C. Ant colony optimization: introduction and recent trends [J]. Physics of Life Reviews, 2005, 2(4): 353－373.

[12] CHEN H, CHENG A M K, KUO Y W. Assigning real-time tasks to heterogeneous processors by applying ant colony optimization [J]. Journal of Parallel and Distributed Computing, 2011, 71(1): 132－142.