高效弹性泄漏下 CCA2 安全公钥加密体制

张明武[1),3)] 陈泌文[1)] 何德彪[3),4)] 杨 波[2)]

[1)](湖北工业大学计算机学院 武汉 430068)

[2)](陕西师范大学计算机学院 西安 710072)

[3)](中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

[4)](武汉大学软件工程国家重点实验室 武汉 430072)

摘 要 公钥密码体制中要求算法和公钥是公开的而密钥必须是严格保密的,但在实际应用系统中,攻击者可以从保密密钥和加密系统内部通过侧信道攻击等手段获得部分密钥.一旦密钥被泄漏,传统的可证明安全将无法归约.弹性泄漏密码体制用于解决密钥、随机数或内部中间状态等存在泄漏情况下的可证明安全问题.该文提出一种应对密钥弹性泄漏的公钥加密方案,达到抗泄漏条件下的自适应选择密文安全性.在 Naor-Segev 方案的基础上,利用密钥衍射和消息认证码,提高系统计算效率同时有效降低密钥长度,并通过随机提取器达到密钥的弹性泄漏容忍.在保持提取器性能不变的条件下,降低密钥的长度提高了密钥允许的泄漏率.分析显示本方案能容忍 25% 的密钥泄漏率,密钥生成、加密和解密分别相当于 2.4、3.2 和 2.2 个单指数计算量,和其他方案比较,泄漏率、密钥长度和计算量等效率都有一定改善.

关键词 密钥弹性泄漏;公钥加密;选择密文攻击;密钥衍射函数

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2016.00492

An Efficient Leakage-Resilient and CCA2-Secure PKE System

ZHANG Ming-Wu[1),3)] CHEN Mi-Wen[1)] HE De-Biao[3),4)] YANG Bo[2)]

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

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

[3)](*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

[4)](*State Key Laboratory of Software Engineering, Wuhan University, Wuhan* 430072)

Abstract In traditional public-key cryptography, it is required that secret keys must be safely stored, in which the provable security will lose even if a single bit of a secret key is leaked. That is, it is commonly assumed that the secret keys, internal computations and randomness are opaque to external adversaries, and only the cryptographic algorithms and the public keys are public and can be revealed to the possible attackers. However, in practical systems, many attacks from side-channel such as cold-boot attacks, time attacks and power dissipations, can obtain some information from the secret keys or the states of cryptosystem. Leakage-Resilient Cryptosystem (LRC) provides an approach to obtain the provable security in the presence of leakage of secret key, randomness and even internal state. In this paper, we propose a CCA-secure leakage-resilient public-key encryption, in which a key derivation function and a message authentication code are used to improve the efficiency. Besides, a strong randomness extractor is also used to tolerate the leakage. Under the feature of extractor, the size of secret key is reduced and the leakage rate

收稿日期:2014-07-16;最终修改稿收到日期:2015-06-26.本课题得到国家自然科学基金(61370224,61272436)、湖北省自然科学基金(2013CFA046)、信息安全国家重点实验室开放基金(2014-04,2013-3-3)和湖北工业大学高层次人才项目资助.**张明武**,男,1970 年生,博士,教授,中国计算机学会(CCF)高级会员,主要研究领域为密码技术、隐私保护和网络安全协议.E-mail:csmwzhang@gmail.com.**陈泌文**,男,1990 年生,硕士研究生,主要研究方向为网络与信息安全.**何德彪**,男,1981 年生,博士,副教授,主要研究方向为信息与网络安全.**杨 波**,男,1963 年生,博士,教授,主要研究领域为密码学与信息安全.

is enhanced. The computation costs of key generation, encryption and decryption are equivalent to that of 2.4, 3.2 and 2.2 single exponent operations of the finite group, respectively. Compared with related schemes, leakage rate, key size and computation cost are improved.

Keywords key leakage resilience; public-key encryption; chosen-ciphertext attack; key derivation function

1 引　言

传统公钥密码体制要求密钥对所有可能的攻击来说是完全保密的，只有公钥和密码算法是完全公开的[1-3]. 但在实际开放式系统中，攻击者可以通过侧信道攻击获得有关密钥的部分信息，如通过检测关机后的内存获得部分存储于内存的敏感信息[4-6]，通过时间攻击获得密钥或随机数的分布[5,7-8]，通过检测电磁辐射获得通讯信道的数据等[7,9-10]. 传统应对侧信道攻击的方法是通过检测到可能的攻击然后提高硬件抵抗攻击的能力或改进算法强度，但是这些手段不能从根本上容忍敏感信息弹性泄漏的产生从而达到既有方案的可证明安全性.

弹性泄漏密码体制(Leakage-Resilient Cryptography，LRC)允许攻击者在获得密码系统中部分(不可公开的)敏感信息的条件下实现其可证明安全性[4-8,11-15]，该概念最早由 Akavia 等人[4]于 2009 年提出，并设计出公钥密码体制中密钥泄漏及可证明安全的密钥弹性泄漏加密方案. 为了能模拟可能的侧信道攻击，允许攻击者自由选择一个满足可能条件的泄漏函数 f. 为了模拟实际的泄漏，设定攻击者能够访问泄漏预言机(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，前提是所设计的泄漏函数不能获得完整的秘密钥(否则攻击者能力与一个合法用户等价). 在具体的泄漏弹性密码方案中，需要考虑不同类型的泄漏函数以设计抵抗不同攻击的安全方案. 最典型的泄漏函数有 3 种方法表达：(1) 输出有界泄漏函数(Bounded Leakage)，这类泄漏允许攻击者获得密钥中任何部分信息，只要保证对密钥的输出长度不超过系统预先设定的界；(2) 密钥熵泄漏(Entropy Leakage)，它允许攻击者获得比密钥更长的信息，但要保证密钥仍存在一定量的最小熵；(3) 辅助输入泄漏(Auxiliary Input Leakage)，允许获得密钥有关的任何输出，但要保证该泄漏函数在多项式时间上不可逆. 一种简化的泄漏模型是密钥暴露[9-10,16]，该模型中泄漏函数是简单的密钥或密码内存的子集. 与基于密钥暴露的密码相比，弹性泄漏函数可定义为自适应的任意可计算的函数，如攻击者根据公钥或已有的泄漏知识来定义新的密钥泄漏函数，因而具有更强的攻击能力.

Naor 和 Segev[14]在 Cramer-Shoup 提出哈希证明系统(Hash Proof System，HPS)[17]的基础上，提出有界泄漏模型下的公钥加密方案，并容忍 CPA 安全下 25%的泄漏率和 CCA 安全下 16.7%的泄漏率. 后来 Alwen 等人[11]改进文献[4]的工作，构建了边界检索模型的泄漏弹性泄漏公钥加密方案，采用在硬件上不同的存储区域来组织密钥，并要求多个密钥存储模块不能同时被泄漏，可达到 50%的泄漏率. Alwen 等人[8]首次提出在有界提取模型下密钥弹性泄漏模型，并构造在基于格、二次剩余、双线性对等多种安全假设下的加密方案. Halevi 和 Lin[18]提出熵安全的密钥弹性泄漏方案，仅达到 CPA 安全性.

为容忍弹性泄漏，往往会增加密钥或密文的长度，同时也会增加系统的计算复杂度. Naor 和 Yung[19]给出直接利用 CPA 安全的公钥系统构造 CCA 安全的方案，它采用双重加密体制并引入零知识证明用以保证两次加密是针对同一明文，其抗泄漏性在文献[14]中也得到证明，但糟糕的效率影响到在实际中的应用. 改进系统的性能，同时提高系统密钥泄漏容忍的能力，这是研究人员不断研究的热点. Li 等人[20]在文献[14]的基础上，提高了公钥加密系统的泄漏率. Liu 等人[21]改进 HPS 的构建方法来提高明文(消息)空间. Nguyen 等人[22]采用高效的哈希函数提高公钥加密系统的计算效率，文献[23-24]中提出了利用对偶系统加密技术容忍密钥有界泄漏，并支持不同策略函数的表达，所提出的方案在双线性群中构造，密钥和密文及计算代价都比较大. Qin 等人[25]提出结合哈希证明系统和一次性有损过滤器来构造 CCA2 安全的公钥加密方案.

Ananth 等人[26]借助于通用参考串模型设计了基于连续泄露模型下的交互式证明系统.

本文设计一个适应性选择密文安全(CCA2)的密钥弹性泄漏公钥加密方案,在 Naor-Segev[14]方案基础上,引入密钥衍射和消息认证码,提高系统的计算效率同时有效降低密钥和密文的长度,并通过随机提取器达到密钥的弹性泄漏容忍.在保持提取器性能不变的条件下,降低密钥长度同时可以提高密钥允许的泄漏率,在 25% 的密钥被泄漏的情况下,所提出的方案仍是可证明安全的,比文献[14,21]中的方案所容忍泄漏率提高了 8.3%,比文献[27]中基于 DCR 假设的方案泄漏率提高 16.7%.

本文第 2 节介绍基础知识及相关基础理论;第 3 节给出弹性泄漏语义安全性的模型及定义;第 4 节给出方案的设计思想和详细构造,并对方案的性能作分析和比较;第 5 节给出方案抗弹性泄漏安全性的形式化证明;第 6 节给出本文方案的实际应用;第 7 节对本文工作小结并提出今后的研究方向.

2 预备知识

2.1 基本知识

本文中,λ 定义为密码系统的安全参数,J 是密钥泄漏界,$\mu(\lambda)$定义为对参数 λ 在计算上可忽略的函数.有限域 $F_p=\{1,2,\cdots,p-1\}$.设 $S\in\{0,1\}^*$ 表示二进制串,$|S|$ 表示 S 的长度.除特别指明外,本文中所有对数 log 的基为 2.

为对方案的设计、安全性证明和性能分析提供理论分析,给出相关基础概念与定义.

定义 1(最小熵). 设 $X\in\chi$ 是在概率总体 χ 上选取的随机变量,随机变量 X 的最小熵定义为 $H_\infty(X)=-\log(\max_{x\in\chi}\Pr[X=x])$.

最小熵表示在没有附加信息的条件下,可以猜出随机变量 X 的概率:$\forall x\in\chi,\Pr[X=x]\leq 2^{-k}$,这里 $k=H_\infty(X)$.对攻击者来说,最好以最大的概率预测出该随机变量值,X 的可预测性表示为 $\max_x\Pr[X=x]$.

例如,对于二进制上 L 长的随机变量 X,$\Pr[X=0]=\frac{1}{2}$.对 $\forall 1\leq x\leq L$,$\Pr[X=x]=\frac{1}{2L}$,X 的最小熵是 1,但其香农熵是 $1+\frac{1}{2}\log L$.密码系统中对于秘密信息的分布 X,我们要求具有较大的最小熵(随机且均匀分布).

引理 1. 设 X,Y 是两个随机变量,则 $H_\infty(X,Y)\leq H_\infty(X)+\log(|Y|)$.

证明.

$$\begin{aligned}H_\infty(X,Y)&=-\log(\max_{x,y}\Pr[X=x,Y=y])\\&=-\log(\max_{x,y}\Pr[X=x]\Pr[Y=y|X=x])\\&\leq-\log(\max_x\Pr[X=x]/|Y|)\\&=H_\infty(X)+\log(|Y|).\end{aligned}$$

证毕.

根据随机变量 Y 的平均情况下关注随机变量 X 的最坏情况.在给定 Y 的条件下关于 X 的平均条件最小熵 $\widetilde{H}_\infty(X|Y)$定义如下.

定义 2(条件最小熵). 在已知 Y 下的 X 条件最小熵定义为

$$\widetilde{H}_\infty(X\mid Y)=-\log(E_{y\leftarrow\psi}[2^{-H_\infty(X|Y=y)}]).$$

引理 2[28]. 设 X,Y,Z 是随机变量,$Y\in\{0,1\}^J$(不大于 J 长度的二进制串),则

$$\begin{aligned}\widetilde{H}_\infty(X\mid Y,Z)&\geq\widetilde{H}_\infty((X,Y)\mid Z)-J\\&\geq\widetilde{H}_\infty(X\mid Z)-J.\end{aligned}$$

该引理表明,对一随机变量 X,泄漏 J 比特信息量将会减少其最小熵最多是 J.由引理 2 可知,对任意函数 f,有如下引理.

引理 3. 对任意函数 $f:\{0,1\}^*\to\{0,1\}^J$,$\widetilde{H}_\infty(X|f(X))\geq H_\infty(X)-J$.

例如,设密钥 $SK=(x_1,x_2)$,公钥 $PK=g_1^{x_1}g_2^{x_2}$,则公钥 PK 泄漏 SK 的平均条件最小熵 $\widetilde{H}_\infty(SK|PK)\geq H_\infty(SK)-|PK|=H_\infty(SK)-|PK|=\log q$. q 是群的阶.这种密钥格式表明,公钥泄漏密钥的信息量不超过密钥的一半.

定义 3(统计距离). 若随机变量 $X_1,X_2\in\chi$,则 X_1 与 X_2 的统计距离定义为

$$\begin{aligned}SD(X_1;X_2)&=\frac{1}{2}\sum_{x\in\chi}|\Pr[X_1=x]-\Pr[X_2=x]|\\&=\max_A\Pr[X_1\in A]-\Pr[X_2\in A].\end{aligned}$$

若两个变量的统计距离最多是 ε,称两个变量是 ε-接近的,记为 $X_1\approx_\varepsilon X_2$.$U$ 是均匀独立的随机变量,记

$$d(X)=SD(X;U),\ d(X|Y)=SD(X;U|Y).$$

熵的大小代表对应变量的不确定性,统计距离则能界定变量之间的相似性或不可区分性,二者结合有助于构造安全密码协议并进行定量的可证明安全性能分析.

引理 4. 对任何随机变量 X,Y 及任一函数 f,$SD(X;Y)\geq SD(X;f(Y))$.

证明.　显然，对任意函数 f，$f(Y)$ 的信息量不大于全部 Y，即对任意变量 Y 的最大可能性是泄漏全部的 Y.　　证毕.

定义 4(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 X,Y 满足 $|\Pr[A(\lambda,\chi)=1]-\Pr[A(\lambda,\psi)=1]|\leq\mu(\lambda)$，则称 X 和 Y 对算法 1 在安全参数 λ 上是计算不可区分的.

引理 5(区分引理[14]).　设 Z_1,Z_2 和 F 是概率分布上的事件，$Z_1\wedge\neg F=Z_2\wedge\neg F$，则 $|\Pr[Z_2]-\Pr[Z_1]|\leq\Pr[F]$.

证明.

$$\begin{aligned}|\Pr[Z_2]-\Pr[Z_1]|&=|\Pr[Z_2\wedge F]+\Pr[Z_2\wedge\neg F]-\\&\quad\Pr[Z_1\wedge F]-\Pr[Z_1\wedge\neg F]|\\&=|\Pr[Z_2\wedge F]-|\Pr[Z_1\wedge F]|\\&\leq\Pr[F].\end{aligned}$$

证毕.

2.2　提取器与剩余哈希

定义 5(提取器(Extractor)).　设 K,ψ 是均匀分布的随机变量总体，对变量 X,Z，其中 X 从 χ 上随机选取且 $H_\infty(X|Z)\geq k$，U 和 R 是分别从 ψ 和 K 上均匀选取的随机变量，若 $\mathrm{SD}((Z,X,\mathrm{Ext}(X;R));(Z,X,U))\leq\varepsilon$，称函数 $\mathrm{Ext}:\chi\times K\to\psi$ 是 (k,ε) 提取器. 若提取器的种子 R 是可以公开的，称该提取器为强提取器.

引理 6.　对任意 $\delta>0$，若 Ext 是一个最坏条件下的 $(k-\log(1/\delta),\varepsilon)$ 的提取器，则 Ext 也是平均条件下的 $(k,\varepsilon+\delta)$ 强提取器.

定义 6(泛函哈希(Universal Hashing)).　一个哈希函数 $H:D\times S\to R$，对任意 $x\neq x'$ 满足 $\Pr\limits_{s\leftarrow S}[H(x;s)=H(x';s)]\leq\dfrac{1}{|R|}$，称该函数是泛函哈希函数.

泛函哈希的构造 1. 设 $D=S=F_q^t$，$R=F_q$，哈希函数 H 定义为 $H(x;s)=\sum\limits_{i=1}^{t}s_ix_i$，则该函数对任意 q 和 t 是一个泛函哈希函数. 易证明该构造满足泛函哈希的性质.

泛函哈希的构造 2. 设 G 是一个阶为 q 的乘法群，$g_0,g_1,\cdots,g_t\in G$. 函数族 $\{H_{k_1,\cdots,k_t}:G^{t+1}\to G\}_{k_i\in F_q}$ 是一个泛函哈希族，即 $D=F_q^t$，$S=G^{t+1}$，$R=G$，$H_{k_1,\cdots,k_t}(g_0,g_1,\cdots,g_t)=g_0\prod\limits_{i=1}^{t}g_i^{k_i}$.

引理 7.　剩余哈希引理(Leftover Hash Lemma，LHL[12]). 设 $\{H_K:\chi\to\psi\}_{K\in K}$ 是泛函哈希族，U 是从 ψ 上随机均匀选取的变量. 对任意 X,Z 及 K，有

$$\mathrm{SD}((H_K(X),K);(U,K))\leq\frac{1}{2}\sqrt{2^{-H_\infty(X)}|Y|},$$

$$\mathrm{SD}((H_K(X),K,Z);(U,K,Z))\leq\frac{1}{2}\sqrt{2^{-H_\infty(X|Z)}|Y|}.$$

该引理表明，任意泛函哈希函数 $\{H_K\}$ 可以构造平均条件下的 (k,ε) 提取器 $\mathrm{Ext}:\chi\times K\to\psi$，其中 K 用于种子，$\log|Y|\leq k-2\log(1/\varepsilon)+2$.

推论 1(基于 LHL 的强提取器).　若 $H:D\times S\to R$ 是一个泛函哈希函数，则该函数也是一个 (k,ε) 的提取器，这里 $k=\log(|R|)+2\log(1/\varepsilon)+1$.

剩余哈希引理表明任何(近似)泛函哈希族可以构造一个强提取器. 设 X 是随机变量，$H_\infty(X)\geq k$，H 是大小为 2^d 输出长度 $m=k-2\log(1/\varepsilon)$. 对任意 $\varepsilon>0$，$h\in H$，定义 $\mathrm{Ext}(x,h)=h(x)$，则 Ext 是一个种子长度是 d 输出长度是 m 的 $(k,\varepsilon/2)$ 强提取器. 该实例中，种子用于选择哈希函数，而提取器的输出是哈希函数输入.

定义 7(消息认证码).　一个消息认证码(MAC)由两个概率多荐式时间算法(Mac，Vfy)组成.

(1) 算法 Mac 以密钥 SK 和消息 N 作为输入，输出一串 tag.

(2) 算法 Vfy 以密钥 SK，消息 N 和串 tag 作为输入，输出 0(拒绝)或 1(接受).

一个消息认证码满足：$\mathrm{Vfy}_{\mathrm{SK}}(N,\mathrm{Mac}_{\mathrm{SK}}(N))=1$.

2.3　泄漏函数

泄漏模型是以泄漏函数的方式体现. 在密码系统中，不同应用场景要求有些函数在多项式时间是可计算的，有些函数是在多项式时间内是不可计算的. 例如，一个函数族 F 是单向的，满足：

(1) 样本化. 从函数族中容易样本化一个函数 f.

(2) 可计算性. 给定 x 容易计算 $f(x)$.

(3) 单向性. 给定 $f(x)$ 以不可忽略的优势在原像样本空间找出原像在计算上是不可行的.

无论何种泄漏模型，我们要求敌手从已知的泄漏密钥中获得完整的密钥是不可行的.

敌手对秘密的泄漏获得是通过泄漏预言机得到. 为保证敌手不能获得整个秘密(如解密密钥、随机数、中间结果等)，必须保证敌手只能从泄漏源获得这些秘密的部分信息. 本文中考虑密钥的泄漏，泄漏模型对泄漏函数的输出不做限定，只保证输出是有界的. 在保证同一密钥输出界的前提下，敌手甚至可以通过多次采用不同的泄漏函数来获得同一密钥的输出.

定义 8(有界泄漏函数). 对任意函数$f:\{0,1\}^*\rightarrow\{0,1\}^L$(其中$L\leq J$),称该函数为有界泄漏函数,也称缩界泄漏函数.

3 弹性泄漏语义安全性

定义 9(泄漏预言机). 泄漏预言机O_{Leak}以密钥 SK 和泄漏界 J 为输入,对该预言机的询问由任一多项式时间可计算的函数 $f:\text{SK}\rightarrow\{0,1\}^L$(其中$L\leq J$)发起,该预言机计算 $f(\text{SK})$,返回关于 SK 的最多 J 比特的信息.若累计密钥 SK 泄漏量$f(\text{SK})$超过 J 比特,预言机返回$\perp$.

为提供敌手自适应性的泄漏预言机询问,允许敌手对同一密钥进行多次泄漏询问,要求所获得的泄漏总量不超过系统设定的泄漏界 J 即可①.为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.

我们给出公钥加密方案的安全性:自适应选择密文不可区分性,其安全性高于单向安全性.在定义 11 中的弹性泄漏 CCA2 安全性是在允许敌手进行密钥泄漏预言机询问 O_{Leak} 和密文解密预言机询问 O_{Dec}条件下的密文不可区分性.

定义 10(自适应选择密文不可区分性). 敌手获得接收者公钥 PK 并具有密文解密询问的能力,选择两消息(M_0,M_1),$M_0\neq M_1$ 且$|M_0|=|M_1|$,挑战者随机抛币 $b\in\{0,1\}$并调用加密算法创建密文$\text{CT}=\text{Enc}_{\text{PK}}(M_b)$.敌手试图猜测密文 CT 中的消息$M_b$.若敌手无法以不可忽略的概率优势猜出 b 的取值,我们称该方案是选择密文不可区分性.

定义 11(自适应弹性泄漏 CCA2 安全性). 对任意多项式时间算法 $A=(A_1,A_2)$,一个公钥加密方案 $\Pi=(\text{Key},\text{Enc},\text{Dec})$在泄漏函数族 H ($f\in H$)上算法 1 在如下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.该抗泄漏交互游戏模型如下.

S1. 挑战 C 生成$(\text{PK},\text{SK})\leftarrow\Pi.\text{Key}$并把 PK 发送给 A;

S2. A 选择泄漏函数$f:\{0,1\}^*\rightarrow\{0,1\}^{\leq J}$并发送给 C;

S3. C 根据泄漏预言机O_{Leak}应答自适应性的泄漏 $f(\text{SK})$;

S4. A 选择密文 CT 并发送给挑战者 C;

S5. C 根据解密预言机O_{Dec}应答对 CT 的自适应性解密询问;

S6. A 自适应选择不同 $f\in H$ 重复上面 S2～S3 或不同密文 CT 重复 S4～S5.这种重复次数可以是安全参数 λ 的多项式次数.泄漏询问结束后,A 选择并发送给 C 两个挑战消息(M_0,M_1);

S7. C 随机抛币 $b\in\{0,1\}$,调用加密算法生成$\text{CT}\leftarrow\Pi.\text{Enc}_{\text{PK}}(M_b)$,并将密文发送给 A;

S8. 算法 1 基于已有的知识判定并输出 $b'\in\{0,1\}$作为对 C 随机抛币 b 的猜测.

形式化弹性泄漏安全模型游戏定义如图 1.

	$\text{Exp}_{\Pi,A}(\lambda,J)$
1	$(\text{PK},\text{SK})\leftarrow\text{Key}(\lambda,J)$
2	$(M_0,M_1,state)\leftarrow A_1^{O_{\text{Leak}(f)},O_{\text{Dec}(.)}}(\text{PK})$ with $\lvert M_0\rvert=\lvert M_1\rvert$
3	$\text{CT}\leftarrow\text{Enc}_{\text{PK}}(M_b)$ with $b\leftarrow\{0,1\}$
4	$(b'=b)\leftarrow A_2^{O_{\text{Dec}(.)}}(\text{CT},state)$

$$Adv_{\Pi,A}(\lambda,J)\overset{\text{def}}{=}|2\Pr[b'=b]-1$$

图 1 弹性泄漏 CCA2 安全试验模型

该安全模型中,允许敌手可以执行适应性地进行泄漏预言机询问,即它可以得到公钥后再自适应地选择泄漏函数 f,同时允许敌手进行适应性地进行解密询问.事实上,敌手可以把公钥作为泄漏函数的"硬核",泄漏函数 f 构造与公钥有关,即$f(\text{SK},\text{PK})$.

为避免在 A_2 阶段敌手通过编码挑战密文从而形成特殊的泄漏函数从而区分密文中的消息明文,我们不允许在 A_2 阶段敌手进行泄漏预言机询问.

4 方 案

4.1 方案构造思路

本方案中引入抗碰撞的哈希函数 TCR,密钥衍生函数 KDF(Key Derivation Function)和一个消息认证码 MAC 来实现,同时为达到抗泄漏性,我们引入一强提取器 Ext.TCR 用于实现把部分密文组件(u_1,u_2)映射到 F_q上.密钥衍生函数 KDF 生成两个子密钥:一个用于加密的会话密钥;一个用于内部认证.其中内部认证用于保证密文的不可延展性,认证方式采用消息认证码 MAC 来实现.使用的密钥衍生函数定义为 KDF:$K\rightarrow\{0,1\}^{2\log q}$,满足对任意$v\in K(\lambda)$,算法 B 区分 $\text{KDF}(v)$的输出与一个 $2\log q$ 长

① 泄漏界为整个密码系统生存周期允许泄漏的最大值.

的随机串对系统安全参数 λ 来说在计算上是不可区分的，即下面的概率优势是可忽略的：

$$\left|\Pr_{v\leftarrow K(\lambda)}[B(\mathrm{KDF}(v))=0]-\Pr_{k_1,k_2\leftarrow\{0,1\}^{\log q}}[B(k_1,k_2)=0]\right|\leq\mu(\lambda).$$

密钥衍射函数的输出分为两个子密钥 k_1 和 k_2. 我们实例化以 k_2 为认证密钥的消息认证码 MAC：$G^2\times\{0,1\}^m\rightarrow\{0,1\}^\tau$. 这里 $k_2\in\{0,1\}^{\log q}$ 由密钥衍生函数 KDF 生成. 基于任意满足条件的密钥 k_2，算法 2 在给定若干个关于消息 N 及其认证码 $\mathrm{tag}=\mathrm{MAC}_{k_2}(N)$ 询问输出的情况下，生成一个新的有效认证码在计算上是不可行的，即

$$\Pr[B(N'\neq N\wedge\mathrm{tag}=\mathrm{MAC}_{k_2}(N'),\ \mathrm{tag}\leftarrow\mathrm{MAC}_{k_2}(N),N\leftarrow G^2\times\{0,1\}^m)]\leq\mu(\lambda).$$

根据消息认证码安全标准，MAC 的输出 tag 在 128 bits 时是安全的（即 $\tau=128$），它比一般的群元素长度要小（对因素分解的有限域，80 bits 标准安全时阶 $\log q=512$，椭圆曲线时 $\log q=160$；在 128 位安全下，因式分解困难假设中 $\log q=1536$，椭圆曲线中 $\log q=256$）.

4.2　具体方案

设明文 M 的长度是 m，G 是满足判定性 Diffie-Hellman 假设（DDH 假设）阶为 q 的群. 接下来给出 CCA2 安全的密钥弹性泄漏公钥加密方案构造. 方案中，提取器的种子空间是 Seed.

4.2.1　$\mathrm{Key}(1^\lambda)$.

（1）随机选择 $x_1,x_2,y_1,y_2\in F_q,g_1,g_2\in G$.

（2）计算 $c=g_1^{x_1}g_2^{x_2}$，$d=g_1^{y_1}g_2^{y_2}$.

（3）选择抗碰撞哈希函数 TCR：$G^2\times\mathrm{Seed}\rightarrow F_q$，密钥衍射函数 KDF：$G\rightarrow\{0,1\}^{2\log q}$，及 $(\log q-J,\varepsilon)$ 强提取器 Ext：$\{0,1\}^{\log q}\times\mathrm{Seed}\rightarrow\{0,1\}^m$.

（4）置公钥 $\mathrm{PK}=(g_1,g_2,c,d,\mathrm{TCR},\mathrm{KDF})$.

（5）置密钥 $\mathrm{SK}=(x_1,x_2,y_1,y_2)$.

说明. 事实上，整个系统所有用户可以共用群 (G,q)、TCR、KDF 和提取器 Ext，可以完全预先选定并公开，对每个用户来说不同用户的公钥 (g_1,g_2,c,d) 是不同的. 默认用户的公钥只包括这 4 个元素. 用户的密钥也只包括 4 个 F_q 中的元素.

4.2.2　$\mathrm{Enc}_{\mathrm{PK}}(M)$.

（1）随机选取 $r\in F_q,s\in\mathrm{Seed}$，计算 $u_1=g_1^r,u_2=g_2^r$.

（2）计算 $\alpha=\mathrm{TCR}(u_1,u_2,s)$，$v=c^rd^{r\alpha}$.

（3）计算 $(k_1,k_2)\leftarrow\mathrm{KDF}(v)$，$e=M\oplus\mathrm{Ext}(k_1,s)$.

（4）计算 $\mathrm{tag}\leftarrow\mathrm{MAC}_{k_2}(u_1,u_2,e)$.

（5）输出密文 $\mathrm{CT}=(u_1,u_2,e,\mathrm{tag},s)$.

4.2.3　$\mathrm{Dec}_{\mathrm{SK}}(\mathrm{CT})$

（1）解析 $\mathrm{SK}=(x_1,x_2,y_1,y_2)$ 及 $\mathrm{CT}=(u_1,u_2,e,\mathrm{tag},s)$.

（2）计算 $\alpha=\mathrm{TCR}(u_1,u_2,s)$.

（3）计算 $v=u_1^{x_1+y_1\alpha}u_2^{x_2+y_2\alpha}$.

（4）计算 $(k_1,k_2)\leftarrow\mathrm{KDF}(v)$.

（5）若 $\mathrm{tag}\neq\mathrm{MAC}_{k_2}(u_1,u_2,e)$，直接返回解密失败 $\perp$.

（6）输出 $M\leftarrow e\oplus\mathrm{Ext}(k_1,s)$.

4.3　性能分析

本节比较几种弹性泄漏的公钥加密方案. 所比较的方案皆基于 DDH 语言上的安全假设，并可以此来构造哈希证明系统，从而扩展并应用于其他的安全假设中，如二次剩余、双线性群假设等. 采用 DDH 假设的有限域实际中可以基于因式分解的困难假设构造，也可以在椭圆曲线上的离散对数问题构造. 对于因式分解的假设中，置 G 为 $p=2q+1$ 的阶是 q 的子群.

泄漏率定义为密钥允许的泄漏与整个密钥长度的比值，即 $\rho=\dfrac{J}{|\mathrm{SK}|}$. 显然，敌手从该密码系统中所获得的有关密钥 $\mathrm{SK}=(x_1,x_2,y_1,y_2)$ 的信息源有：

（1）公钥 $\mathrm{PK}=(g_1,g_2,c,d,\mathrm{TCR},\mathrm{KDF})$；

（2）挑战密文 $\mathrm{CT}^*=(u_1^*,u_2^*,e^*,\mathrm{tag}^*,s^*)$；

（3）密钥泄漏询问输出 $f(\mathrm{SK})$；

（4）解密询问的输出；

（5）挑战明文 (M_b^*,M_{1-b}^*)；

（6）提取器 Ext 的输出.

上述信息中，根据语义安全性的性质，解密询问无法获得有关密钥的任何信息（只能获得明文）. 本文中消息与密钥和提取器种子是独立分布的[①]，根据 KDF 和 TCR 的性质（定义 7），无法从其输出中获得有关输入的有用信息.

设敌手获得密钥的泄漏长度是 $J=|f(\mathrm{SK})|$，给定 $(c=g_1^{x_1}g_2^{x_2},d=g_1^{y_1}g_2^{y_2},f(\mathrm{SK}))$ 的情况下，v 的最小熵 $H_\infty(v|c,d,f(\mathrm{SK}))\geq\log q-J$. 根据密钥衍射函数的性质，$k_1$ 和 k_2 仍具有 $\log q-J$ 的最小熵，KDF 无法获得密钥的信息，即 $Adv_A^{\mathrm{KDF}}=\Pr[K_1=k_1,K_2=k_2]\leq 2^J/q$. 同样，消息认证码 tag^* 也不泄漏密钥的信息.

① 消息相关加密（Message Dependent Encryption）中，加密的消息和密钥之间存在一定关系. 该方案中密文中除公钥相关信息对密钥存在泄漏熵之外，加密消息本身也存在对密钥的泄漏. 本文不考虑此类情况.

密钥中 x_1,x_2,y_2 和 y_2 是独立选取的，它们之间相互独立. 因此在敌手获得相关信息的条件下的密钥仍具有的条件最小熵：

$$\begin{aligned}&\widetilde{H}_\infty(\mathrm{SK}|\mathrm{PK},\mathrm{CT}^*,f(\mathrm{SK}),(M_b,M_{1-b}),J\text{-bit leakage})\\&=\widetilde{H}_\infty(\mathrm{SK}|c,d,\mathrm{CT}^*,f(\mathrm{SK}),M_b,J\text{-bit leakage})\\&=\widetilde{H}_\infty(\mathrm{SK}|c,d,u_1^*,u_2^*,M_b\oplus\mathrm{Ext}(k_1,s^*),\mathrm{tag}^*,s^*,\\&\quad f(\mathrm{SK}),M_b,J\text{-bit leakage})\\&=\widetilde{H}_\infty(\mathrm{SK}|c,d,M_b\oplus\mathrm{Ext}(k_1,s^*),s^*,f(\mathrm{SK}),M_b,\\&\quad J\text{-bit leakage})\\&\geqslant\widetilde{H}_\infty(\mathrm{SK}|c,d,M_b\oplus\mathrm{Ext}(k_1,s^*),s^*,M_b)-J\\&=\log q-J,\end{aligned}$$

式中，u_1^*,u_2^*,M_{1-b} 与 SK 无关. 提取器 Ext 是 $(\log q-J,\varepsilon)$ 强提取器，用以增强密钥的随机性. 在敌手获得公钥、泄漏预言机询问、解密预言机询问、挑战密文及选择挑战明文的前提下，最后系统中密钥仍具有不大于的 $\log q-J$ 信息熵. 为达到系统中密钥仍具有一定量有最小熵，要求系统泄漏界 $J\leqslant\log q$，即 $J=\log q-\omega(1)$. 同时，系统中密钥 $\mathrm{SK}=(x_1,x_2,y_1,y_2)\in F_q^4$，$|\mathrm{SK}|=4\log q$，因此方案所达到的最大泄漏率 $\rho=J/|\mathrm{SK}|=25\%$.

在 AES-80 标准安全下，基于因式分解构造中，$|p|=1024$，$|q|=512$，对于椭圆曲线则要求 $|q|=160$. 对于安全性更高的 AES-128 安全标准，因式分解构造中 $|p|=3076$，$|q|=1538$，对于椭圆曲线则要求 $|q|=256$. 对于方案中的消息认证码，目前对 128 位的认证码的输出是安全的，它比一个群元素的长度要短，且消息认证码 MAC 是对称密钥的计算，效率比群指数运算要快. 同时，密钥衍射函数 KDF 计算量与哈希函数的运算量相当，实际计算中可以忽略其复杂度.

基于 DDH 假设的方案构造中，密文与密钥长度主要取决于群元素的个数，而计算量主要取决于多指数(me)、单指数(se)、以及群元素判定(gmc)等计算量.

在计算量方面，1me=1.2se[①]，1gmc=1se. 表 1 列出和分析几种方案的密文与密钥长度、泄漏率和安全级别的比较，表 2 列出方案的计算性能，为能有数量上的比较，把对多指数运算和群元素比较运算统一转换为单指数运算的运算量. 由于文献[19]方案中用到了零知识证明，其效率与一般群的指数运算完全不在一个数量级，因此对其加密和解密计算量不作比较. 文献[14]中设计两个方案，分别达到 CCA1 安全和 CCA2 安全，我们分别记为 NS09a 和 NS09b.

表 1 密文、密钥、泄漏率及安全性比较

方案	公钥长度	密钥长度	密文长度	泄漏率 ρ/%	安全级别
BHHO08[14,29]	$(t+1)\|q\|$	$t\|q\|$	$(t+1)\|q\|$	$1-\frac{2}{t}$	LR-CPA
NS09a[14]	$4\|q\|$	$4\|q\|$	$3\|q\|+\|M\|+\|\mathrm{Seed}\|$	25	LR-CCA1
LZSS13[20]	$4\|q\|$	$4\|q\|$	$3\|q\|+\|M\|+\|\mathrm{Seed}\|$	25	LR-CCA1
NY90[19]	$10\|q\|$	$4\|q\|$	$2\|\mathrm{CT}\|+\|\Pi\|$	50	LR-CCA2
NS09b[14]	$5\|q\|$	$6\|q\|$	$2\|q\|+\|M\|+\|\mathrm{tag}\|+\|\mathrm{Seed}\|$	16.7	LR-CCA2
LWZ13[21]	$5\|q\|$	$6\|q\|$	$4\|q\|+\|\mathrm{Seed}\|$	16.7	LR-CCA2
KNP13[29]	$4\|q\|$	$4\|q\|$	$\frac{7}{3}\|q\|+\|\mathrm{Seed}\|+\|M\|$	8.3	LR-CCA2
本文方案	$4\|q\|$	$4\|q\|$	$2\|q\|+\|M\|+\|\mathrm{tag}\|+\|\mathrm{Seed}\|$	25	LR-CCA2

注：该方案用到可认证的加密；$|\mathrm{AuthEnc}|$：可认证的加密密文长度. $|q|=\log q$；$|M|$：明文长度；$|\mathrm{tag}|$：认证标签长度；$|\mathrm{Seed}|$：提取器种子长度.

表 2 计算性能比较

方案	公钥长度	密钥长度	密文长度	消息空间
BHHO08[29]	$(t-2)$me$=1.2(t-2)$se	1me$+t$se$=(1.2+t)$se	$(t-1)$me$=1.2(t-1)$se	$M\in G$
NS09a[14]	2me$=2.4$se	32e$=3$se	2me$+$1gmc$=3.4$se	$\|q\|-J$
LZSS13[20]	2me$=2.4$se	1me$+$2se$=3.2$se	2me$+$1gmc$=3.4$se	$\|q\|-J$
NY90[19]	2me$=2.4$se	1me$+$1se$+$NIZK	1me$+$1gmc$+$NIZK	$M\in G$
NS09b[14]	3me$=3.6$se	1me$+$3se$=4.2$se	1me$+$1gmc$=2.2$se	$\|q\|-J$
LWZ13[21]	3me$=3.6$se	2me$+$2se$=4.4$se	2me$+$1gmc$=3.4$se	$M\in G$
本文方案	2me$=2.4$se	1me$+$2se$=3.2$se	1me$+$1gmc$=2.2$se	$\|q\|-J$

注：me：多指数运算；se：单指数运算；gmc：群元素比较；NIZK：零知识证明(计算量大). 1me$=1.2$se，1gmc$=$1se.

在 CCA2 安全级别的方案中，本文方案密钥只有 4 个群元素，比 NSb[14,21] 缩短了 33%，和方案[19,29]中密钥长度相当，但文献[19]中需要零知识证明，效

① 根据 Bernstein 的工作，一个多指数的运算量是 $\left(1+\frac{2}{\log\log q}\right)\log q$，近似 1.2 个单指数运算时间.
Bernstein D J. Pippenger's exponentiation algorithm. http://cr.yp.to/papers/pippenger.pdf, 2002

率很低.在泄漏率方面,本文方案和 CCA1 安全的 NS09a[14,20]都达到 25%,比同安全级别的 NS09b 和文献[21]提高了 8.3%,比文献[29]中提高了 16.7%.在计算量方面,由表 2 可以看出,本文的方案具有较好的计算效率.

5　安全性

本方案的安全性基于判定性 Diffie-Hellman 假设,即对 $r_1 \neq r_2$,任意多项时间的算法 1 区分 $T_1=(g_1,g_2,g_1^{r_1},g_2^{r_1})$与 $T_2=(g_1,g_2,g_1^{r_1},g_2^{r_2})$是计算上不可行的.$T_1$称为有效的 Deffie-Hellman 元组,$T_2$称为无效的 Diffie-Hellman 元组.

根据第 3 节的安全游戏,抗泄漏安全性要求由随机抛币选择明文 M_b产生的加密密文 CT 中无法猜出抛币 b.密文结构中,若(g_1,g_2,u_1,u_2)是一个有效的 Diffie-Hellman 元组,即 $u_1=g_1^{r_1}$,$u_2=g_2^{r_2}$且 $r_1=r_2$,称密文CT称为有效密文(Valid ciphertext),否则称为无效密文(Invalid ciphertext).若密文解密中满足验证等式,即 $\text{tag}\neq\text{MAC}_{k_2}(u_1,u_2,e)$,则称该密文满足一致性(Consistent ciphertext),否则是不一致的密文(Inconsistent ciphertext).显然,使用一合法密钥解密密文时,此密文对密钥来说应当是有效且满足一致性的.

安全性证明过程中,我们采用一系列计算上不可区分游戏来证明.第 1 个游戏 Θ_0就是第 3 节所定义的安全游戏,设挑战密文是$\text{CT}^*=(u_1^*,u_2^*,e^*,\text{tag}^*,s^*)$,显然在这个游戏中 $r=r_1=r_2$.第 2 个游戏 Θ_1中,将 u_1^* 和 u_2^* 改变为非合法 Diffie-Hellman 元组,即 $r_1\neq r_2$,根据 DDH 假设,这种变化是计算上不可区分的.显然,Θ_1是一个无效密文.第 3 个游戏 Θ_2中,$\alpha^*=\text{TCR}(u_1^*,u_2^*,s^*)$仍是挑战密文中的元组计算而来,此时 v 的计算也按照挑战密文中的 u_1^* 和 u_2^* 来计算,显然此时生成的(k_1,k_2)可以通过验证等,是个一致性密文.第 4 个游戏 Θ_3中,置 $\alpha=\text{TCR}(u_1,u_2,s^*)$,其中$(u_1,u_2)$是安全假设实例中的元组.显然 $\alpha=\alpha^*$ 的概率是一个哈希函数可能碰撞的概率.此时经过前面的变化询问的密文是无效密文.第 5 个游戏 Θ_4中,挑战者拒绝所有无效密文的解密询问.我们证明,敌手根据公开信息和询问的泄漏密钥,无法把一个无效密文转换为有效密文.最后一个游戏中,将密文中的明文组件 e^* 用一个$\{0,1\}^*$中的随机数代替.显然,此时密文是一个无效的不一致密文.根据哈希证明系统的性质[17],若一个有效密文与一个无效密文是不可区分的,我们可以证明该方案是语义安全的.

接下来分析敌手允许从游戏中所能获得有关密钥的信息界.从安全游戏中可知,敌手获得有效密钥的信息来源主要有:一是公钥 PK 可能泄漏密钥熵;二是泄漏预言机的询问 $f(\text{SK})$;三是挑战密文中隐藏关密钥的信息.

定理 1.　设 λ 是系统安全参数,TCR 是抗碰撞的哈希函数,KDF 是密钥衍射函数,Ext 是$(\log q-J,\varepsilon)$强提取器.Q 是系统中敌手的解密询问的次数,则方案 Π 是 (J,ε')的 CCA 安全的公钥加密方案,其中

$$\begin{cases}\varepsilon' \leq \varepsilon + Adv_A^{\text{DDH}}(\lambda)+Q\,Adv_A^{\text{TCR}}(\lambda)+Adv_A^{\text{KDF}}(\lambda)+\\ \qquad Adv_A^{\text{MAC}}(\lambda)+\dfrac{2^J}{q/Q-1}+\dfrac{1}{q^2}+\dfrac{2^{J/2-1}}{\sqrt{q}}\\ J=\log q-m-\omega(\log\lambda)\end{cases}.$$

证明.　设 Z_i是系列游戏 Θ_i对应的事件.在 Θ_0中生成挑战密文$\text{CT}^*=\text{Enc}(M_b)=(u_1^*,u_2^*,e^*,\text{tag}^*,s^*)$,加密过程中所用的随机数和中间结果分别是$(r^*,\alpha^*,\text{tag}^*,v^*,k_1^*,k_2^*)$.其中 r^*,k_1^* 和 k_2^* 对敌手来说在加密过程中是完全隐藏的.对于敌手 A 的泄漏询问或解密询问,挑战者分别调用 O_{Dec}和 O_{Leak}进行应答.事件 Z_0表示敌手 A 能成功猜出 b.

在 Θ_1中,挑战者 C 知道密钥,直接用密钥生成挑战密文:随机选取 $r^*,s^*\in F_q$,计算

$$\begin{aligned}&u_1=g_1^{r^*},\\ &u_2=g_2^{r^*},\\ &\alpha=\text{TCR}(u_1^*,u_2^*,s^*),\\ &v^*=u_1^{x_1+y_1\alpha}u_2^{x_2+y_2\alpha},\\ &(k_1,k_2)\leftarrow\text{KDF}(v^*),\\ &e^*=M_b\oplus\text{Ext}(k_1,s^*),\\ &\text{tag}^*=\text{MAC}(u_1,u_2,s^*).\end{aligned}$$

置密文 $\text{CT}=(u_1^*=u_1,u_2^*=u_2,e^*,\text{tag}^*,s^*)$.在密文生成过程中,只是把 v 的计算用密钥来计算,因此本变化与 Θ_0是不可区分的,且(g_1,g_2,u_1^*,u_2^*)仍是有效 Diffie-Hellman 元组,即 $\Pr[Z_1]=\Pr[Z_0]$.

在Θ_2中,(g_1,g_2,u_1^*,u_2^*)用非法的 Diffie-Hellman 元组代替:随机选取 $r_1^*,r_2^*\in F_q(r_1^*\neq r_2^*)$,$u_1^*=g_1^{r_1^*}$,$u_2^*=g_2^{r_2^*}$,而其他的密文元组保持不变(事实上在 Θ_1中其他元组的计算与 r_1^* 和 r_2^* 无关).根据 DDH 假设,区分有效的和无效的 Diffie-Hellman 元组在计算上是不可行的,因此本游戏的变化对敌手来说是在计算上不可区分的,其优势等价于解决 DDH 问题,

即$|\Pr[Z_2]-\Pr[Z_1]|\leq Adv_A^{\mathrm{DDH}}(\lambda)$.

在Θ_3中,事件F_1是挑战者拒绝对所有密文$(u_1, u_2, e, \mathrm{tag}, s)\neq(u_1^*, u_2^*, e^*, \mathrm{tag}^*, s^*)$,但$\mathrm{TCR}(u_1,u_2,s)=\mathrm{TCR}(u_1^*,u_2^*,s^*)$的解密询问.显然此游戏中满足拒绝的条件是哈希函数的碰撞概率.容易得到$\Pr[Z_3\wedge\neg F_1]=\Pr[Z_2\wedge\neg F_1]$,设敌手最多进行$Q$次解密询问,根据引理5,$|\Pr[Z_3]-\Pr[Z_2]|\leq\Pr[F_1]\leq QAdv_A^{\mathrm{TCR}}(\lambda)$.

根据上面的变化,挑战密文是无效密文(无效Diffie-Hellman元组).在Θ_4中,挑战者拒绝敌手提供的所有无效密文的解密询问,即公开的(g_1,g_2)与密文中的(u_1,u_2)不构成有效Diffie-Hellman元组.设F_2是挑战者由于无效密文而拒绝应答解密询问的事件,则有

$$\Pr[Z_4|\neg F_2]=\Pr[Z_3|\neg F_2],$$
$$|\Pr[Z_4]-\Pr[Z_3]|\leq\Pr[F_2].$$

由4.3节抗泄漏性能的分析可知,事件F_2发生的概率:CT是一个无效密文,设$r_1=\log_{g_1}u_1$,$r_2=\log_{g_2}u_2$.显然$r_1\neq r_2$.对$\mathrm{CT}\neq\mathrm{CT}^*$,$\alpha\neq\alpha^*$,则有

$$\begin{bmatrix}\log_{g_1}c\\ \log_{g_1}d\\ \log_{g_1}v^*\\ \log_{g_1}v\end{bmatrix}=\begin{bmatrix}1&0&\gamma&0\\ 0&1&0&\gamma\\ r_1^*&r_1^*\alpha&r_2^*\gamma&r_2^*\gamma\alpha\\ r_1&r_1\alpha&r_2\gamma&r_2\gamma\alpha\end{bmatrix}\times\begin{bmatrix}x_1\\ y_1\\ x_2\\ y_2\end{bmatrix}.$$

上式中$\det(M)=\gamma^2(r_2^*-r_1^*)(r_2-r_1)(\alpha^*-\alpha)\neq0$,意味着$v^*$与密文CT无关.对于$Q\geq1$,无效密文被解密预言机接受的概率是$2^J/(q/Q-1)$.因此有

$$|\Pr[Z_4]-\Pr[Z_3]|\leq Adv_A^{\mathrm{KDF}}+\frac{2^J}{q/Q-1}.$$

接下来我们考虑Θ_5,该游戏中消息组件e^*由一m长的随机串代替.经过Θ_4的变换,所有无效密文都被解密预言机拒绝,解密预言机无法获得有关密钥的信息.事实上,在Θ_4中,当(u_1,u_2)被替换后,已证明该转换是不可区分的.本游戏重点考虑密文中的(e,tag,s).假定若$e^*=e$,$\mathrm{tag}^*=\mathrm{tag}$,$s^*=s$则$\mathrm{CT}^*=\mathrm{CT}$(Ext是一个强提取器,种子$s$是公开的,证明中我们默认使用相同的种子$s$).对密钥信息获取有帮助的主要有公钥PK,挑战密文中的(e^*,tag^*),以及泄漏预言机的输出$f(\mathrm{SK})$.

显然若$v^*=v$则$(k_1^*,k_2^*)=(k_1,k_2)$.若CT被解密预言机接受,则有$\mathrm{tag}=\mathrm{MAC}_{k_1^*}(u_1,u_2,e)$.若$e^*=e$则$\mathrm{tag}^*=\mathrm{tag}$,这样$\mathrm{CT}^*=\mathrm{CT}$.我们考虑$\mathrm{CT}^*\neq\mathrm{CT}$,根据MAC的性质要求$e^*\neq e$.此时CT被解密预言机接受的概率是$Adv_A^{\mathrm{MAC}}(\lambda)$.

本游戏中$e^*\in\{0,1\}^m$为随机选取,$H_\infty(e^*)=m$.若要求$M_b\oplus\mathrm{Ext}(k_1^*,s^*)$与$e^*$统计不可区分,Ext是$(\log q-J,\varepsilon)$的强提取器,则

$$H_\infty(k_1|\mathrm{PK},f(\mathrm{SK}),\mathrm{tag}^*)=\log q-J+\omega(\log\lambda).$$

根据剩余哈希引理7,有

$$\mathrm{SD}(e^*;e)\leq\frac{1}{2}\sqrt{q\frac{2^J}{q^2}}=\frac{2^{\frac{J}{2}-1}}{\sqrt{q}}.$$

同时$\Pr[u_1=u_1^*,u_2=u_2^*]=\frac{1}{q^2}$,因此

$$|\Pr[Z_5]-\Pr[Z_4]|\leq\frac{1}{q^2}+\frac{2^{J/2-1}}{\sqrt{q}}+Adv_A^{\mathrm{MAC}}(\lambda).$$

敌手猜测随机串e^*和加密消息密文组件$M_b\oplus\mathrm{Ext}(k_1^*,s^*)$的概率是$\Pr[Z_5]=1/2+\varepsilon$.由于$\varepsilon$是在安全参数下多项式时间是可忽略的,因此敌手攻击本方案的概率与一个随机抛币在计算上是不可区分的. 证毕.

6 方案应用

本节给出本文方案在实际中的典型应用.在物联网系统中,为保证开放节点中的数据安全,一般要引入加密体制来保证物联网节点存储数据的私密性.与此对应的是,实现加密系统的密钥也是一同保存在该节点中以供相应节点实现对数据的解密(密钥对攻击者来说是黑盒).显然,攻击者对密钥系统的攻击期望更大于对加密系统算法本身的关注.特别是物联网一般采用离散网络结构,大部分节点架设于室外,并通过无线通讯来实现数据的传输,这极易让攻击者通过侧信道攻击的手段获得敏感机密信息(包括密钥)提供便利.采用本文方案,从算法上设计可证明安全的密码系统,在给定攻击者一定量密钥的情形下(灰盒密钥),仍能保证系统仍具有黑盒密码系统的安全强度.

本文方案的另一个典型的应用场景是银行ATM系统.我们假定用户的银行卡号为公钥,对应的交易取款密码为密钥.事实上,在取款或交易过程中,交易密码可能被意者由视频监控、POS机监听、甚至在输入密码的过程中观测按键的手势、频率或速度等方式来获得部分的交易密码.传统采用公钥加密方式来保护敏感信息的方案在交易密码被泄漏的情况下是不能证明为完全安全的(虽然攻击者未得到全部的交易密码,但通过字典攻击或穷举搜索可以极大概率实现猜测攻击).采用本文的方案,在即便1/4的交易密码被窃取的情形下,仍保证系统

是安全的，在一定程度上实现了密钥增强能力.

7 结束语

本文提出一种有效 CCA 安全的公钥加密方案，在 25% 密钥被泄漏的情况下仍保证该方案是可证明安全的. 文中给出系统的安全模型、实际构造以及安全性证明，并给出详细的性能分析和比较，结果显示本方案在 CCA2 安全级别的方案中具有较短密钥和较高计算效率. 接下来的工作是在保证系统计算效率的情形下设计容忍更高泄漏率的方案，同时考虑到很多实际攻击方案（如病毒）可以控制伪随机发生器从而控制密码系统随机数的安全性，构造抗伪随机数泄漏的方案，也是接下来的研究内容.

参 考 文 献

[1] Bitansky N, Dachman-Soled D, Lin H. Leakage-tolerant computation with input-independent preprocessing//Proceedings of the CRYPTO'14. Santa Barbara, USA, 2014: 146-167

[2] 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)

[3] Dodis Y, Pietrzak K. Leakage-resilient pseudorandom functions and side-channel attacks on Feistel networks//Proceedings of the CRYPTO'10. Santa Barbara, USA, 2010: 21-40

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

[5] 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, USA, 2010: 501-510

[6] Zhang Ming-Wu, Yang Bo, 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)
(张明武，杨波，Takagi T. 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)

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

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

[9] Yu J, Kong F Y, Cheng X G, et al. Intrusion-resilient identity-based signature: Security definition and construction. Journal of Systems and Software, 2012, 85(2): 382-391

[10] Yu Jia, Cheng Xiang-Guo, Li Fa-Geng, et al. Provably secure intrusion-resilient public-key encryption scheme in the standard model. Journal of Software, 2013, 24(2): 266-278 (in Chinese)
(于佳，程相国，李发根等. 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)

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

[12] Barak B, Dodis Y, Krawczyk H, et al. Leftover hash lemma, revisited//Proceedings of the CRYPTO'11. Santa Barbara, USA, 2011: 1-20

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

[14] Naor M, Segev G. Public-key cryptosystems resilient to key leakage//Proceedings of the CRYPTO'09. Santa Barbara, USA, 2009: 18-35

[15] Kiltz E, Pietrzak K. Leakage resilient ElGamal encryption//Proceedings of the ASIACRYPT'10. Singapore, 2010: 595-612

[16] Canetti R, Dodis Y, Halevi S, et al. Exposure-resilient function and all-or-nothing transforms//Proceedings of the EUROCRYPT'00. Bruges, Belgium, 2000: 453-469

[17] Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption//Proceedings of the EUROCRYPT'02. Amsterdam, Netherlands, 2002: 45-64

[18] Halevi S, Lin H. After-the-fact leakage in public-key encryption//Proceedings of the TCC'11. Providence, USA, 2011: 107-124

[19] Naor M, Yung M. Public-key cryptosystems provably secure against chosen ciphertext attacks//Proceedings of the STOC'90. New York, USA, 1990: 427-437

[20] Li S J, Zhang F, Sun X, Shen L. Efficient leakage-resilient public key encryption from DDH assumption. Cluster Computing, 2013, 16(4): 797-806

[21] Liu S, Weng J, Zhao Y. Efficient public key cryptosystem resilient to key leakage chosen ciphertext attacks//Proceedings of the CT-RSA'13. San Francisco, USA, 2013: 84-100

[22] Nguyen M H, Yasunage K, Tanaka K. Leakage-resilient CCA2 public-key encryption form 4-wise independent hash functions//Proceedings of the ATC'11. Da Nang, Vietnam, 2011: 14-17

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

[24] Zhang M, Yang B, Takagi T. Bounded leakage-resilient functional encryption with hidden vector predicate. The Computer Journal, 2013, 56(4): 464-477

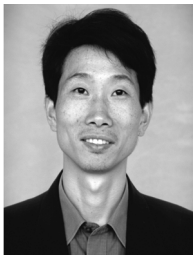
[25] Qin B, Liu S. Leakage-resilient chosen-ciphertext secure public-key encryption from hash proof system and one-time lossy filter//Proceedings of the ASIACRYPT'13. Bengaluru, India, 2013: 381-400

[26] Ananth P, Goyal V, Pandey O. Interactive proofs under continual memory leakage//Proceedings of the CRYPTO'14. Santa Barbara, USA, 2014: 164-182

[27] Kurosawa K, Nojima R, Phong L T. New leakage-resilient CCA-secure public key encryption. Journal of Mathematical Cryptology, 2013, 7(4): 297-312

[28] 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

[29] Boneh D, Halevi S, Hamburg M, Ostrovsky R. Circular-secure encryption from decision Diffie-Hellman//Proceedings of the CRYPTO'08. LNCS 5175. Santa Barbara, USA, 2008: 108-125



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

CHEN Mi-Wen, born in 1990, M. S. candidate. His main research focuses on information security and network security.

HE De-Biao, born in 1981, Ph. D., associate professor. His main research interests include information and network security.

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

Background

Security primitives of modern cryptography technology has modelled attackers as having only black-box access to the primitives, and ensure that secret keys must be safely stored and internal states are not leaked to the attackers. However, these security models fail to capture many real scenarios in which the attackers can gain traditional information about secret states through side-channel. In order to against this type of attacks, there are two complementary approaches to improve the security construction. One approach is to diminish the damage of this specific attacks by designing reinforced hardware (hardware- based level). And the other approach is to modify the traditional black＝box model and construct the scheme to against the attack (algorithm-based level).

In this paper, we address the problem of CCA2-secure leakage-resilient public-key encryption in the algorithm-based level, and give the security model and construction. We introduce a key derivation function and a message authentication code to enhance the efficiency and employ a strong randomness extractor to tolerate the leakage. Under the feature of extractor, the size of secret key is reduced and the leakage rate is enhanced. Compared with related schemes, our scheme enjoys a shorter secret key size and higher relative key leakage rate. Concretely, the computation costs of key generation, encryption and decryption are equivalent to 2.4, 3.2 and 2.2 single exponents of the finite group, respectively.

This study is partially supported by the National Natural Science Foundation of China under Grant Nos. 61370224 and 61272436, and the Key Program of Natural Science Foundation of Hubei Province under Grant No. 2013CFA046, and the Open Fund Program for State Key Laboratory of Information Security of China under grants 2014-04 and 2013-03.