对G-Paillier加密体制的改进与分析

姜正涛[1]，柳 毅[2]，王育民[2]

(1. 北京航空航天大学计算机学院 北京 100083; 2. 西安电子科技大学综合业务网国家重点实验室 西安 710071)

【摘要】通过适当地选择参数改进了推广的Paillier (G-Paillier)加密体制，减少运算量，提高了加密体制的效率；证明了改进后加密体制的安全性(单向性、语意安全性)与G-Paillier加密体制的安全性是等价的。

关 键 词 概率加密体制; 安全性分析; *n*次剩余问题; 单向性
中图分类号 TP309^{+}.7 文献标识码 A

Improvements and Analysis of G-Paillier Encryption Scheme

JIANG Zheng-tao[1]，LIU Yi[2]，WANG Yu-min[2]

(1. School of Computer Science, Beijing University of Aeronautics and Astronautic Beijing 100083;
2. National Key Lab. of Integrated Service Networks, Xidian Univ. Xi'an 710071)

Abstract The efficiency of the generalized Paillier (G-Paillier) encryption scheme is improved by choosing proper parameters. The efficiency of the improved G-Paillier scheme and the original G-Paillier scheme is compared. The security (one-wayness security, semantic security) equivalence of the improved encryption scheme and the G-Paillier encryption scheme is verified.

Key words probabilistic encryption scheme; security analysis; *n*th residuosity; one-wayness

基于计算和判断 $Z_{n^2}^*$ 上的*n*次剩余问题，文献[1-2]提出了一种抵抗CCA2攻击的概率加密体制，该体制具有语意安全性，可直接用于加密电子投票等有意义的明文消息；文献[3-4]对这一体制的应用与安全性做了有意义的探讨和分析；文献[5]推广了这一体制，并运用它所具有的同态加密的性质给出了在电子投票方面的应用。

加密体制效率的高低直接影响它能否在实际中应用。一种安全的、高效的加密体制会给密码应用领域带来巨大的影响，而且一种安全的加密体制还应是能够抵抗CCA2攻击的概率加密体制。本文在不降低G-Paillier体制(即推广的Paillier体制)的安全性的前提下，选择适当形式的加密参数，明文加密时用乘法运算代替指数运算；同时也改进了解密算法，提高了体制的效率，降低了需要传输公共参数的数据量；并证明了改进的加密体制与G-Paillier体制一样，在相同的困难问题假设下具有单向和语意安全等特性。

1 G-Paillier加密体制

G-Paillier加密体制(设为加密体制1)下，$n = pq$ 为RSA模；$Z_{n^{s+1}}^* \cong G \times H$ ，其中 G 是阶为 n^s ($s \geq 1$)的循环群，$H \cong Z_n^*$ ，且 H 可以看作 $Z_{n^{s+1}}^*$ 中形如 h^{n^s} 元素的集合，$h \in Z_{n^{s+1}}^*$ [5]。

1.1 相关参数

(1) 公开参数 $n = pq$ ， $g \in Z_{n^{s+1}}^*$ ，满足 $g = (1+n)^j x \bmod n^{s+1}$ ，解密用户知道 $j \in Z^+$ ， $(j, n) = 1$ ， $x \in H$ 。

(2) 秘密参数 $\lambda = lcm(p-1, q-1)$ ；整数 d 满足 $d \bmod n \in Z_n^*$ ， $d \equiv 0 \bmod \lambda$ ； $m \in Z_{n^s}$ 是待加密的消息。

1.2 加、解密过程

(1) 加密用户随机选取 $r \in Z_{n^{s+1}}^*$ ，计算 $C = g^m r^{n^s} \bmod n^{s+1}$ 。

(2) 解密用户计算 $C_d \equiv C^d \bmod n^{s+1} = (1+n)^{jdm} \bmod n^{s+1}$ (*)，并恢复明文 $m = (jd)^{-1} jdm \bmod n^s$ 。

收稿日期：2003 – 12 – 02
作者简介：姜正涛(1976 –)，男，博士，主要从事密码等可信计算和抗毁生存等方面的研究.

1.3　效率分析

(1) 加密阶段，加密用户需在 $Z_{n^{s+1}}$ 上做两次大指数模乘法运算和一次模乘法运算。

(2) 解密阶段，解密用户首先需要做模指数运算，计算求出 C_d 的值；然后由 C_d 求 $i = jdm \bmod n^s$ (*)；最后根据文献[5]的算法，计算以下参数：

$$\begin{cases} i_1 = L((1+n)^i \bmod n^2) = i \bmod n \\ i_2 = L((1+n)^i \bmod n^3) - \binom{i_1}{2} n \bmod n^2 \\ \vdots \\ i = i_s = L((1+n)^i \bmod n^{s+1}) - (\binom{i_{s-1}}{2} n + \cdots + \binom{i_{s-1}}{s} n^{s-1}) \bmod n^s \end{cases} \tag{1}$$

由于计算 $\binom{i_l}{l+1} n^l$ 至少需要 $2l$ 次模乘法运算 $l = 1, 2, \cdots, s-1$，于是这个过程远远大于 $2s^2$ 次模乘法运算。但本文不区分除法和乘法运算，也没有考虑求 n^l 的幂运算。

2　改进的G-Paillier加密体制

2.1　相关参数

改进的G-Paillier加密体制(设为加密体制2)下，参数选择同于G-Paillier加密体制，其中 $g = 1 + n$ ；解密指数 d 满足 $dn^s \equiv 1 \bmod \lambda$ ； $m \in Z_{n^s}$ 是待加密的消息。

2.2　加、解密过程

(1) 加密用户随机选取 $y \in Z_n^*$，计算 $C = (1+mn) y^{n^s} \bmod n^{s+1}$。

(2) 解密用户计算 $y \equiv C^d \bmod n$ ； $m = \dfrac{y^{-n^s} C \bmod n^{s+1} - 1}{n}$。

2.3　效率分析

(1) 加密过程主要包括求 $y^{n^s} \bmod n^{s+1}$ 的指数模乘法运算和2次模乘法运算。对于经常加密的用户，可以事先随机选取多个 $y \in Z_n^*$，做预计算 $y^{n^s} \bmod n^{s+1}$，并秘密保存。加密时只需随机选择其中一个进行加密运算，这样在加密时只需做两次模乘法运算即可。

(2) 解密过程主要包括1次大指数模乘法运算、1次小指数模乘法运算和2次模乘法运算。本文也不区分乘法与除法运算。

3　两种加密体制的运算效率比较

加密体制2的加密阶段选取的随机数 $r \in Z_n^*$ 与加密体制1的加密阶段选取的随机数 $r \in Z_{n^{s+1}}^*$ 相比，提高了运算的效率，并且没有降低体制的安全性。事实上，若 $y \in Z_{n^{s+1}}^*$，则 $y = y_0 + y_1 n + \cdots + y_s n^s$，其中 $y_k \in Z_n, k = 1, 2, \cdots, s$ ；且有：

$$y^{n^s} \bmod n^{s+1} = (y_0 + y_1 n + \cdots + y_s n^s)^{n^s} \bmod n^{s+1} = y_0^{n^s} \bmod n^{s+1}$$

改进的**G**-Paillier加密体制与**G**-Paillier加密体制的效率比较见表1。图中2–$E(n^{s+1})$表示2个modn^{s+1}指数运算；1–$M(n^{s+1})$表示1个modn^{s+1}乘法运算；>>s^2–M(mod)表示远远多于s^2个modn^k形式的模乘法运算，且k=1，2，…，s+1。

表1　运算效率比较

	加密体制1		加密体制2		
加密	2–$E(n^{s+1})$	1–$M(n^{s+1})$	1–$E(n^{s+1})$	2–$M(n^{s+1})$	
解密	1–$E(n^{s+1})$	>>$2s^2$–M(mod)	1–$E(n^{s+1})$	1–$E(n)$	1–$M(n)$

当$s\geq 1$时，由于$E(n^{s+1})$的计算量远远大于$E(n)$的计算量(分别计算 $g^m \bmod n^{s+1}$， $m\in Z_{n^s}$ 和 $C^d \bmod n$，$d<\lambda$)，显然加密体制2的效率要比加密体制1的效率高，即使在最坏的情况下也至少减少了$(s+1)\mathrm{lb}n-\mathrm{lb}n=s\mathrm{lb}n$次“平方-乘法”运算。$1-E(n)$大约需要$\mathrm{lb}n$次“乘法-平方”运算，当$n$为1 024比特的RSA模时，约需1 024次模$n$的“乘法-平方”运算，当$s\geq 23$时$(2s^2\geq 1\,024)$，改进的加密体制无论加密还是解密均比G-Paillier加密体制的效率高。而当s是比较小的数时(如s=3,4等)，加密体制2的解密效率可能不及加密体制1的解密效率高，但此时(最坏的情况)从加、解密的整个过程来看，仍然比加密体制1少做了$s\log n$次“平方-乘法”运算。

表2是当RSA模数为1 024比特的合数时，需要传输公共参数的数据量比较。

表2 传输数据比较

	加密体制1	加密体制2
传输数据量/(bit)	n,g (1 024+(s+1)×1 024)	n (1 024)

可以证明加密体制2的加密阶段选取的随机数 $r\in Z_n^*$ 与加密体制1的加密阶段选取的随机数 $r\in Z_{n^{s+1}}^*$ 相比，提高了运算的效率，并且没有降低体制的安全性。事实上，若 $y\in Z_{n^{s+1}}^*$，则 $y=y_0+y_1n+\cdots+y_sn^s$，其中 $y_k\in Z_n$，且 $k=1,2,\cdots,s$。

另外，可以对加密体制2做进一步改进，在加密时，密文 $C=(1+mn)y^e \bmod n^{s+1}$；$e$为公开参数，同于RSA中的公开密钥；解密指数$d$满足 $de\equiv 1 \bmod \varphi(n)$；$\varphi(\cdot)$是欧拉函数。解密时计算

$$y\equiv C^d \bmod n \text{ 和 } m=\frac{y^{-e}C \bmod n^{s+1}-1}{n}$$

4 安全性分析

定理 **1** 当且仅当加密体制1是单向的，加密体制2是单向的。

证明 体制1的密文是 $C_1=(1+n)^{jm}(x^mr^{n^s}) \bmod n^{s+1}$；体制2的密文是 $C_2=(1+mn)y^{n^s} \bmod n^{s+1}$。根据文献[5]的算法，知道 $m=m_1+m_2n+\cdots+m_sn^{s-1}$后，可以求得整数$M$满足：

$$(1+mn)y^{n^s} \bmod n^{s+1}=(1+m_1n+\cdots+m_sn^s)y^{n^s} \bmod n^{s+1}=(1+n)^M y^{n^s} \bmod n^{s+1} \tag{2}$$

同样，知道 M 后也可通过计算求得式(2)中相应的 m。因此，攻击者恢复 M 与恢复 $m=m_1+m_2n+\cdots+m_sn^{s-1}$在计算上是等价的，可以通过分析由密文$C_2$恢复 M 的困难性，来讨论由密文C_2恢复明文m的困难性。

假设加密体制2不是单向的，即攻击者能够由C_2计算 M，由于 y 和 r 都是加密者随机选取的，所以由C_2计算 M，当且仅当可以由 $C_1=(1+n)^{jm}(x^mr^{n^s}) \bmod n^{s+1}$ 计算 $jm \bmod n^s$，由文献[5]对 H 的定义可知，x 是 $Z_{n^{s+1}}^*$ 中的 n 次剩余；当且仅当可以由 $g=(1+n)^j x \bmod n^{s+1}$ 求得 j，求得 j 后计算 $m=j^{-1}(jm) \bmod n^s$。于是，加密体制1无单向性；反之，假设加密体制1无单向性，可以用类似的方法证明加密体制2也无单向性。因此，加密体制2与加密体制1的单向性是等价的。

定义 1 如果在仅知道两条明文 m'、m'' 以及其中一条明文对应的密文 C 的情况下，攻击者不能判断C是哪条明文对应的密文，就说此加密体制具有语意安全特性。

文献[1]给出了判断 n 次剩余的定义，为了便于讨论，本文给出推广判断高次剩余的定义。

定义 2 判断 n^s 次剩余已知 $w\in Z_{n^{s+1}}$，判断是否存在一个元素 $g\in Z_{n^{s+1}}$，满足 $w\equiv g^{n^s} \bmod n^{s+1}$ 的问题，称为判断 n^k 次剩余问题，记为 CS_s。

定理 **2** 加密体制2与加密体制1的语意安全性是等价的，且均等价于 CS_s。

证明 由定理1，给定明文 m' 和 m''，攻击者可以求得具有式(2)形式的 M_1 和 M_2。当且仅当能够判断加密体制1的密文对应的明文消息，于是能够判断加密体制2的密文对应的明文消息。

因此，加密体制2与加密体制1的语意安全性是等价的，并且显然等价于 CS_s 问题的困难性。

定理 **3** 当且仅当由 $y^{n^s} \bmod n$ 求 $y^{n^s} \bmod n^{s+1}$ 是困难的，加密体制2(即加密体制1)是单向的。

(下转第566页)

ϕ-hemicontractive mappings[J]. Math.Comput Model, 2000, 32: 791-801.
[2] Huang N J, Gao C J, Huang X P. New iteration procedures with errors for multivalued ϕ-strongly pseudocontractive and ϕ-strongly accretive mappings[J].Comput and Math with Appl, 2002, 43: 1 381-1 390.
[3] Ghosh M K, Debnath L. Convergence of ishikawa iterates of quasi-nonexpansive mappings[J]. J Math Anal Appl, 1997, 207: 96-103.
[4] Goebel K,Kirk W A. A fixed point theorem for asymptotically nonexpansive mappings[J]. Proc.Amer.Math.Soc, 1972, 35: 171-174.
[5] Ishikawa S. Fixed points by a new iteration method[J].Proc.Amer.Math.Soc, 1974, 44: 147-150.
[6] Chang S S, Cho Y J, Kim J K. The equivalence between the convergence of modified picard, modified Mann, and modified ishikawa iterations[J]. Mathematical and Computer Modelling, 2003, 37: 987-991.
[7] Liu Qihou. Ierative sequences for asymptotically quasi-nonexpansive mappings with error member[J]. J Math Anal Appl, 2001, 259: 18-24.
[8] 王 缨. 渐近拟非扩张映象的带误差的迭代序列[J]. 西南师范大学学报(自然科学版), 2003, 28(1): 52-54.

编 辑 孙晓丹

(上接第530页)

证明 令 $y^{n^s} \bmod n^{s+1} = y_0 + y_1 n + \cdots + y_s n^s$，其中 $y_i \in Z_n \quad i = 1, 2, \cdots, s$。加密体制2的密文如下，即：

$$C = (1 + m_1 n + m_2 n^2 + \cdots + m_s n^s) y^{n^s} \bmod n^{s+1} =$$

$$y_0 + (y_0 m_1 + y_1) n + (y_0 m_2 + y_1 m_1 + y_2) n^2 + \cdots + (y_0 m_s + \cdots + y_s) n^s \bmod n^{s+1} \quad (3)$$

显然，$y_0 = y^{n^s} \bmod n = C \bmod n$ 是已知的。如果由 $y^{n^s} \bmod n$ 求 $y^{n^s} \bmod n^{s+1}$ 是容易的，则攻击者能够从密文 C 恢复出式(3)中的 $m_0, m_1, \cdots, m_s$，于是可以恢复明文 $m = m_0 + m_1 n + \cdots + m_s n^{s-1}$。反之，如果攻击者能够从密文 C 恢复出明文消息 m，攻击者可以用同样的方法恢复 $y_1, y_2, \cdots, y_s$，于是求得 $y^{n^s} \bmod n^{s+1}$。因此，加密体制2的单向性与由 $y^{n^s} \bmod n$ 求 $y^{n^s} \bmod n^{s+1}$ 的困难性是等价的。于是，由定理1可以得到，加密体制1的单向性也与由 $y^{n^s} \bmod n$ 求 $y^{n^s} \bmod n^{s+1}$ 的困难性等价。

5 结 论

加、解密效率的高低直接影响加密体制的性能。本文的主要结论是在不降低安全性的前提下，通过选择特殊的公共参数改进加、解密的方式，提高加密体制的效率，降低需要传输的数据量。本文还证明了改进的G-Paillier体制的安全性与G-Paillier体制一样，具有单向性和语意安全性。

参 考 文 献

[1] Paillier P. Public-key based on composite degree residuosity classes[C]//Advances in Cryptology-EUROCRYPT'99, LNCS 1233, Prague, 1999.
[2] Paillier P, Pointcheval D. Efficient public-key cryptosystem provably secure against active adversaries[C] //Advances in Cryptology-ASIACRYPT'99, LNCS 1716, Singapore, 1999.
[3] Catalano D, Gennaro R, Graham N H. The bit security of Paillier' encryption scheme and its applications [C]//Advances in Cryptology-EUROCRYPTO'01, LNCS 2045, Aarhus, 2001.
[4] Sakurai K, Takagi T. New semantically secure public-key cryptosystems from the RSA-primitive[C]// Advances in Cryptology-PKC'02, LNCS 2274, Paris, 2002
[5] Damgard I, Jurik M. A generalization, a simplification and some application of Paillier's probabilistic public-key system[C]// Advances in Cryptology-PKC'99, LNCS 1992, KamaKura, 2001.

编 辑 熊思亮