第 34 卷 第 3 期 计 算 机 工 程 2008 年 2 月
Vol.34 No.3 Computer Engineering February 2008
·博士论文· 文章编号：1000—3428(2008)03—0038—02 文献标识码：A 中图分类号：TP309+.7

Paillier-Pointcheval 公钥概率加密体制的改进

姜正涛[1]，刘建伟[2]，王育民[3]
（1. 北京航空航天大学计算机学院，北京 100083；2. 北京航空航天大学电子信息工程学院，北京 100083；
3. 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：分析 P. Paillier 等提出的公钥概率加密体制的安全性，证明它的单向性与几类问题的等价关系，进一步证明了在不降低安全性的前提下，可以通过选取适当的参数，提高体制的效率，减少通信量，在此基础上给出改进的加密体制，加密和解密的效率比以往的体制有了很大的提高。

关键词：安全性分析；公钥概率加密体制；参数选择

Improvement on Paillier-Pointcheval Probabilistic Public-key Encryption Scheme

JIANG Zheng-tao[1], LIU Jian-wei[2], WANG Yu-min[3]
(1. School of Computer and Technology, Beihang University, Beijing 100083; 2. School of Electronic and Information Engineering, Beihang University, Beijing 100083; 3. National Key Lab of Integrated Service Networks, Xidian Univ., Xi'an 710071)

【Abstract】 Security analysis of P. Paillier(etc)'s public-key encryption scheme(P-P) is proposed. Equivalent relations of one-wayness of P-P encryption scheme with other problems are verified. So without lowering the security, this paper improves the efficiency and reduces the data to be transferred by using proper parameters. The improved encryption scheme is specified, with the process of encryption/decryption being more efficient than that of P-P encryption scheme.

【Key words】 security analysis; probabilistic public-key encryption scheme; parameter selection

基于计算和判断Z_n^2上的n次剩余问题的困难性假设， P. Paillier和D. Pointcheval (P-P) 在1999年亚洲密码会议上提出了一种抵抗CCA2 攻击的密码体制[1]。P-P加密体制可以看作是对T. Okamoto和 S.Uchiyama(O-U)提出的加密体制在安全性上的一个改进[2]，避免了选择密文对分解模数的攻击。

1 P-P 加密体制

$n=pq$ 是RSA 模数，$g\in Z_{n^2}^*$， $\lambda=lcm(p-1,q-1)$， $m\in Z_n$ 是待加密的消息。

P-P 加密体制如下：

公开参数：n, g

秘密参数：λ

加密：随机选取 $r\in Z_n^*$

$$C=g^m r^n \bmod n^2$$

解密：$m=\dfrac{L(C^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$

其中，$L(x)=\dfrac{x-1}{n}$；$x\in Z_{n^2}$，且 $x\equiv 1 \bmod n$。

2 P-P 加密体制的分析

假设 $n=pq$ 是 RSA 模， $g\in Z_{n^2}^*$，定义函数 ε_g 如下：

$$\varepsilon_g: Z_n\times Z_n^* \to Z_{n^2}^*$$

$$(x,y) \to g^x y^n \bmod n^2 \quad (1)$$

不难证明此映射是一一映射。

定义 1 n次剩余[1]：对于式(1)定义的函数 ε_g 和某个 $y\in Z_n^*$，满足的 $\varepsilon_g(x,y)=w$ 的唯一的x，称为 $Z_{n^2}^*$ 中w的n次剩余。

定义 2 n 次剩余问题：由 w 求 x 的问题，称为 n 次剩余问题。

定义 3 判断 n 次剩余问题：假设给定 $w\in Z_{n^2}^*$，判断是否存在某个 $y\in Z_n^*$，满足 $w=y^n \bmod n^2$ 的问题称为判断 n 次剩余问题。

引理 1 加密体制是安全的，当且仅当 $Z_{n^2}^*$ 中的 n 次剩余问题是困难的。

引理 2 加密体制是语意安全的，当且仅当 $Z_{n^2}^*$ 中的判断 n 次剩余问题是困难的。

由于 $n=pq$，因此

$$Z_{n^2}^* \cong A\times B \quad (2)$$

其中，A 为 $Z_{n^2}^*$ 中所有的阶整除 n 的元素全体；B 为 $Z_{n^2}^*$ 中所有的阶整除 $\lambda=lcm(p-1,q-1)$ 的元素全体。

于是，对于任意 $g\in Z_{n^2}^*$, g 可以写成下列的乘积形式：

$$g=\alpha\beta$$

其中，$\alpha\in A, \beta\in B$。

基金项目：国家自然科学基金资助项目(60672102)；中国博士后科学基金资助项目(20060400035)

作者简介：姜正涛(1976－)，男，博士后，主研方向：密码学，信息安全，可信计算，信任管理；刘建伟，副教授、博士；王育民，教授、博士生导师

收稿日期：2007-02-20 **E-mail：**z.t.jiang@163.com

不难看出 $B \cong Z_n^*$；又因为 $(1+n)^n \equiv 1 \bmod n^2$，而

$(1+n)^p \neq 1 \bmod n^2$，$(1+n)^q \neq 1 \bmod n^2$

所以，A 为 $Z_{n^2}^*$ 中的阶为 n 的循环群，且 1+n 是 A 的生成元。

这样，g 可进一步写成下列的乘积形式：

$g = (1+n)^i \beta$，$i \in [0.n-1]$，$\beta \in B$

对于任意的 $g \in Z_{n^2}^*$，容易验证 $g^{n\lambda} \equiv 1 \bmod n^2$，所以，$g^n \in B$。

对于每个 $\beta \in B$，在 $Z_{n^2}^*$ 中的 n 次根的个数至多为 n。于是，B 中的每个元素 β，存在 $Z_{n^2}^*$ 中的某个元素 h 满足：$\beta = h^n \bmod n^2$。

于是，加密体制 1 中的密文

$$C = g^x r^n \bmod n^2 = ((1+n)^i h^n)^x r^n \bmod n^2 = (1+n)^{ix} (h^x r)^n \bmod n^2$$

其中，$g = (1+n)^i h^n$；$i \in [0, n-1]$；$h \in Z_n^*$，且 h 的阶为 nT，$T \approx \lambda$。

如果不能保证几乎对所有的 $i \in (0,n)$ 和 $h \in Z_n^*$，攻击者从 $g = (1+n)^i h^n$ 恢复 $i \in (0,n)$ 的困难性，就不能保证攻击者由 $C = (1+n)^{ix} (h^x r)^n \bmod n^2$ 恢复 $ix \bmod n$ 的困难性，反之亦然。

所以，在假设 P-P 体制是安全的条件下，由 $g = (1+n)^i h^n$ 恢复 $i \in (0,n)$ 与由 $C = (1+n)^{ix} (h^x r)^n \bmod n^2$ 恢复 $ix \bmod n$ 都是困难的。

由以上的分析可以得到下面的结果。

定理 1 P-P 体制是安全，当且仅当对几乎所有的 $h \in Z_n^*$，由 $(1+n)^i h^n$ 恢复 $i \in (0,n)$ 是困难的。

推论 1 $Z_{n^2}^*$ 中的 n 次剩余问题是困难的，当且仅当由 $(1+n)^x h^n$ 恢复 $x \bmod n$ 是困难的。

证明 由定理 1 和引理 1 可得

令 $h^n \bmod n^2 = [h^n]_0 + [h^n]_1 n$，于是

$$(1+n)^x h^n = (1+xn)([h^n]_0 + [h^n]_1 n) \bmod n^2 = [h^n]_0 + ([h^n]_1 + x[h^n]_0)n \quad (3)$$

一个显然的结果就是 $[h^n]_0 = h^n \bmod n = C \bmod n$ 是知道的。于是，式(3)中对 x 起到加密作用的只有 $[h^n]_1$。所以，假设 $Z_{n^2}^*$ 中的 n 次剩余问题是困难的，即假设在不知道 h 的情况下，由 $h^n \bmod n$ 求 $[h^n]_1$ (即，$h^n \bmod n^2$)是困难的。于是有以下的结果：

推论 2 加密体制 是单向的，当且仅当在不知道 h 的情况下，由 $h^n \bmod n$ 求 $h^n \bmod n^2$ 是困难的。

定义 4 $Z_{n^2}^*$ 上的离散对数问题：对于 $g \in Z_{n^2}^*$，由 $g^x \bmod n^2$ 求 $x \bmod n\lambda$ 的问题称为 $Z_{n^2}^*$ 上的离散对数问题，记为 DL。

定义 5 $Z_{n^2}^*$ 上的部分离散对数问题：对于 $g \in Z_{n^2}^*$，由 $g^x \bmod n^2$ 求 $x \bmod n$ 的问题称为 $Z_{n^2}^*$ 上的部分离散对数问题。

由定理 1 和推论 2，不难得到下面的结果：

定理 2 P-P 体制是安全的，当且仅当 $Z_{n^2}^*$ 上的部分离散对数问题是困难的。

根据D. Catalano等对Paillier加密体制的比特安全性的分析[3]，本文在假设 $Z_{n^2}^*$ 上的离散对数为n-困难的($DL_g(.)$ is n hard)的条件下，P-P体制的所有n个比特将同时具有核心安全性(simultaneously hard-core)[4]。

对于 $Z_{n^2}^*$ 上一般的离散对数问题，本文不加证明地给出下列结果：

定理 3 对于任意的 $g \in Z_{n^2}^*$，求 $g \bmod n$(或n^2) 的阶（或阶的倍数）等价于分解 n，(这里的 g 满足：$g^{\frac{p-1}{2}} \equiv -1 \bmod p$，$g^{\frac{q-1}{2}} \equiv 1 \bmod q$)。

定理 4 如果存在算法求解 $Z_{n^2}^*$ 上的离散对数问题，当且仅当存在算法分解 n 和求解 $GF(p)$, $GF(q)$上的离散对数问题。

以上证明了 P-P 体制的单向性与几类相关问题的简单等价关系，如果在绝大多数情况下 $Z_{n^2}^*$ 上的离散对数问题是困难的，则 P-P 体制是安全的。

3 P-P 加密体制的改进

由第 1 节对加密体制的安全性分析，在不降低原有体制安全性的条件下，可以通过选择适当的参数，提高体制的加、解密的效率。

改进的 P-P 加密体制如下：

公开参数：n

秘密参数：$b = \lambda^{-1} \bmod n$

加密：$C = (1+mn) r^n \bmod n^2$

解密：$m = bL(C) \bmod n$

其中，$L(C) = \dfrac{C^\lambda \bmod n^2 - 1}{n}$。

由于r是在加密之前由加密用户随机选取的，加密用户可以在加密之前随机选择多个 $r \in Z_n^*$，并作预计算 $r^n \bmod n^2$，在加密时用户随机选取某个 $r^n \bmod n^2$ 对明文m加密即可。这样，加密只需在 Z_{n^2} 上做两个简单的乘法运算，进一步提高了加密的效率。以上的结果适应于Paillier等给出的其他几种变形的加密体制[1,5]，事先选取大量的随机数r适合实时要求高的应用场景，再权衡存储空间与传输的实时性，需要保证r的随机性和保密性，否则将降低语义甚至安全性。

4 P-P 加密体制的效率比较

运算效率比较如表 1 所示。

表 1 运算效率比较

	加密体制	改进的加密体制	改进的加密体制(含预计算)
加密	2-$E(n^2)$；1-$M(n^2)$	1-$E(n^2)$；2-$M(n^2)$	2-$M(n^2)$
解密	2-L； 1-$D(n)$	1-L；1-$M(n)$	1-L；1-$M(n)$

表 1 中符号表示如下：

2-$E(n^2)$：2 个modn^2幂运算；1-$M(n^2)$：1 个modn^2乘法运算；1-$D(n)$：1 个mod$n$除法运算；2-L：2 个L函数的计算，$L(x)=(x^\lambda \bmod n^2-1)/n$。

表 2 是取 RSA 模数为 1 024 bit 时传输的数据量比较。

表 2 传输效率比较

	加密体制	改进的加密体制
传输数据	n, g (3 072)	n (1 024)

5 结束语

本文证明了 P-P 体制的单向性与几个相关困难问题的等价关系的结果。并证明了可以在不降低原体制安全性的前提下，通过选择适当的参数提高体制的加、解密效率。通过对某些数据的预计算，可以在加密时只做两个乘法运算，进一步提高了体制的效率，但需要保证预计算随机数的随机和安全性。同时本文的方案也减少了需要传输的数据量。本文的结果同样可用于提高文献[1]中其他几种加密方案的效率。

（下转第 42 页）