一种高效的可选择验证完整性和消息源的加密体制

姜正涛 庞辽军 王育民
(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：该文改进了 P. Paillier 等提出的公钥加密体制，提高了体制的效率，并证明了改进后加密体制的安全性与原体制的安全性是等价的。在不增加密文长度的情况下，进一步把此体制改进成高效的“加密+签名”体制，如果消息的接收方认为有必要，可以随时验证明文消息的完整性和消息的确切来源。

关键词：公钥加密体制，安全性分析，n 次剩余问题，加密+签名
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2005)04-0621-04

An Efficient Encryption Scheme with Choosable Process of Verifying Integrity and Source of Messages

Jiang Zheng-tao Pang Liao-jun Wang Yu-min
(*National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an* 710071, *China*)

Abstract The efficiency of a public-key encryption scheme proposed by P. Paillier *et al.* is improved. The equivalence of security of the improved encryption scheme and that of the original encryption scheme is proved. Without increasing the size of the ciphertext, the scheme is further modified into an efficient “signcryption” scheme. If necessary, the receiver can verify the integrity and source of the message at any time.

Key words Public-key encryption scheme, Security analysis, *n*th residuosity problem, Signcryption

1 引言

基于计算和判断 Z_n^2 上的 n 次剩余问题的困难性，P. Paillier 和 Pointcheval (P-P)提出了一种抵抗 CCA2 攻击的密码体制，并给出了一种能够验证消息完整性的加密方案来抵抗适应性攻击[1]，许多密码研究者对这一体制作了有意义的分析和推广[2, 3]。

P-P 加密体制可以看作是对 Okamoto 和 Uchiyama (O-U)提出的加密体制在安全性上的一个改进[4]，避免了选择密文对分解模数的攻击。

本文通过选取适当的参数，提高了 P-P 体制的加、解密效率，并证明了改进后的加密体制的安全性与原体制的安全性等价，分析了改进后（原）加密体制的单向性与几个困难问题的等价关系。在此基础上，在不改变密文长度的情况下，通过加入签名机制或嵌入用户双方共享的秘密身份信息，使此体制成为一种高效的“加密+签名”体制，用户在对密文解密后，如果认为有必要可以随时验证明文消息的完整性和消息的确切来源。最后以表格的形式具体给出了改进的加密体制与原 P-P 加密体制在加、解密的效率以及需要传输的数据量方面的简单对比。

2 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。

加密体制 1

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

3 改进的 P-P 加密体制

加密体制 2——改进的 P-P 加密体制

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 $L(C)=(C^\lambda \bmod n^2-1)/n$。

2003-11-28 收到，2004-07-14 改回
国家自然科学基金重点项目（69931010）资助课题

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一个 $r^n \bmod n^2$ 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。

注 1：以上的结果可以用于改进 Paillier 等给出的其它几种变形的加密体制[1]。

4 对改进的加密体制的安全性分析

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

$$\varepsilon_g:\ Z_n\times Z_n^* \to Z_{n^2}^*$$
$$(x,y) \to g^x y^n \bmod n^2 \tag{1}$$

不难证明此映射是一一映射。

定义 1[1] **n 次剩余** 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。

引理 1 加密体制 1 是单向的，当且仅当 $Z_{n^2}^*$ 中的 n 次剩余问题是困难的。

假设 A 为 $Z_{n^2}^*$ 中所有的阶整除 n 的元素全体，由于 $(1+n)^n \equiv 1 \bmod n^2$，而 $(1+n)^p \neq 1 \bmod n^2$ 和 $(1+n)^q \neq 1 \bmod n^2$，所以 $A=\{(1+n)^i \bmod n^2, i=0,\cdots,1\}$。

由于 Z_n^* 中元素的阶均整除 $\lambda=lcm(p-1,q-1)$，不难证明对任意的 $\alpha_1\neq\alpha_2\in Z_n^*$ 和任意的 $i,j\in[0,\cdots,n-1]$，都有 $(1+n)^i\alpha_1^n \neq (1+n)^j\alpha_2^n$，这样形式的元素共有 $n\lambda$ 个，恰好等于 $Z_{n^2}^*$ 中元素的个数。于是我们得出，对任意的 $g\in Z_{n^2}^*$ 可以写成下面的形式：

$$g=(1+n)^i\beta^n,\quad i\in[0,n-1],\quad \beta\in Z_n^*$$

所以，对于加密体制 1 中的 $g\in Z_{n^2}^*$，存在 $\beta\in Z_n^*$，使得

$$g=(1+n)^i\beta^n \bmod n^2=(1+in)\beta^n \bmod n^2,\quad i\in[0,n-1] \tag{2}$$

这样，加密体制 1 中的密文：

$$C=g^m r^n=(1+n)^{im}(y^m r)^n \bmod n^2$$
$$=(1+n)^{im}R^n \bmod n^2=(1+imn)R^n \bmod n^2 \tag{3}$$

这里的 R 可以看作是 Z_n^* 中的一个随机数。

分析 1 显然，由式(2)恢复 i 同由式(3)恢复 $im \bmod n$ 具有相同的困难性。如果两者都是容易的，则可以由 i 和 $im \bmod n$ 恢复出明文消息 m。这样的话，加密体制 1（由引理 1，即 n 次剩余问题）是容易的；相反，如果 n 次剩余问题是容易的则，由式(2)恢复 $i\in[0,n-1]$ 是容易的。

根据以上的分析，我们得到下面的结论。

定理 1 加密体制 2 是单向的，当且仅当 n 次剩余问题是困难的（当且仅当加密体制 1 是单向的）。

对于 $h\in Z_n^*$[注]，令 $h^n \bmod n^2=[h^n]_0+[h^n]_1 n$，于是

$$(1+n)^x h^n=(1+xn)([h^n]_0+[h^n]_1 n) \bmod n^2$$
$$=[h^n]_0+([h^n]_1+x[h^n]_0)n \tag{4}$$

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(4)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，就是假设在不知道 h 的情况下，由 $h^n \bmod n$ 求 $[h^n]_1$（即 $h^n \bmod n^2$）是困难的。于是我们有下面的结论。

定理 2 加密体制 1 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 3 **$Z_{n^2}^*$ 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。

定义 4 **$Z_{n^2}^*$ 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。

定理 3 加密体制 2（即加密体制 1）是单向的，当且仅当 $Z_{n^2}^*$ 上的部分离散对数问题是困难的。

证明 由式(2)，对于 $g\in Z_{n^2}^*$，存在 $y\in Z_n^*$，使得 $g=(1+n)^i y^n \bmod n^2$，$i\in[0,n-1]$ 于是

$$g^x \bmod n^2=(1+n)^{ix}h^n \bmod n^2 \tag{5}$$

如果 $Z_{n^2}^*$ 上的部分离散对数问题是容易的（即多项式时间内可求解），显然我们可以从 $C=(1+n)^m r^n \bmod n^2$ 和 $C=g^m r^n \bmod n^2$ 中求得 m，于是加密体制 2（即加密体制 1）无单向性。

反之，假设加密体制 2 无单向性。由分析 1，可以由 $g=(1+n)^i\beta^n \bmod n^2$ 和 $C=g^x r^n \bmod n^2$ 恢复出 x，于是部分离散对数问题可解。

因此，加密体制 2（即加密体制 1）的单向性与 $Z_{n^2}^*$ 上的部分离散对数问题是等价的。

根据 Catalano 和 Cramer 等对 Paillier 加密体制的安全性的分析[2,5]，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）。

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

定理 4 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：

[注] $Z_n=\{0,1,\cdots,n-1\}$，$Z_n^*=\{I,(I,n)=1,0<I<n\}$.

$g^{(p-1)/2} \equiv -1 \bmod p$， $g^{(q-1)/2} \equiv 1 \bmod q$）。

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。

以上证明了改进的加密体制（或等价地 P-P 加密体制）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，则改进的体制是安全的。对于这类问题的研究，将另文给出。

5　可选择认证完整性及消息源的加密方案

公钥密码体制最大的贡献就是改变了传统的密钥传输方式，接收者收到某个发送者发送的密钥 K（或消息），他可以直接用 K 来加密或解密需要处理的信息。如果接收者认为有必要，他就需要进一步确认收到的密钥 K（或消息）的确切来源或密文在传输过程中是否已经被更改。Zheng 给出了一种加密+签名的方法，它的效率比传统上加密和签名作为两个独立的步骤运行的效率要高[6]。他的方法把明文消息和密钥区分开来，实际上是公钥与对称密码体制混合使用的一种变形，如果传输的是具体有意义的消息，如表决票和指令等，还需要加密体制另外具有语意安全特性，而 Zheng 的加密方案将泄露一部分的密钥 k_1，由文献[1, 2]关于语意安全性的分析，用改进的 P-P 加密体制可以很好地做到这一点。

参数选择同于第 2 节，其中消息 $m<2^{|n|-t-1}$，随机数 $r<2^t$，$H(\bullet)$是 hash 函数，Sgn(•)是发送者对消息的签名或嵌入与接收者共享的秘密身份信息，||为消息的连接符号。

“加密+签名”体制 3

公开参数：n，秘密参数：$b=\lambda^{-1} \bmod n$；

加密：$z=\mathrm{Sgn}(H(m\|r))+r \bmod n$，$C=(1+(m\|r)n)z^n \bmod n^2$；

解密：$m'\|r'=bL(C) \bmod n$，其中 $L(C)=(C^\lambda \bmod n^2-1)/n$；

*验证：$H(m'\|r')$?=Very(Sgn$H(m\|r)$)。

在“加密+签名”体制 3 中，用户可以用与加密体制 2 同样的步骤恢复出明文 m，如果认为有必要他可以随时运行“加密+签名”体制 3 的验证步骤，来验证 m 的完整性以及确切来源，如果验证等式成立则密文在传输中没有被改动，同时也验证了消息的正确来源，起到了非否认的作用，否则丢弃消息。对于经常发送消息的用户双方来说，如果他们拥有事前共享的秘密身份信息 I_{AB}，可以直接与明文消息“异或”来代替签名，即 $\mathrm{Sgn}(H(m\|r))=m\|r \oplus I_{AB}$，可进一步提高“签名+加密”的效率。

6　效率分析

各种体制的运算效率比较如表 1。

“加密+签名”体制 3 是对文献[1]抵抗适应性攻击的改进，加、解密的效率有了很大程度的提高。用户双方事前如果有共享的秘密身份信息，则体制 3 将拥有几乎与改进的加密体制 2 同样高的效率。

表 2 列出了当取 RSA 模数为 1024 bit 时的传输公共参数的数据量比较：

表 2　传输效率比较

	加密体制 1	加密体制 2
传输数据（量）	n,g (3072bit)	n (1024bit)

7　结论

本文的主要结果是在不降低安全性的前提下提高 P-P 体制的加、解密效率，并同时改进了抵抗适应性攻击的加密方案，分析了改进后（原）加密体制的单向性与几个困难问题的等价关系。文献[1]的抵抗适应性攻击加密方案只验证的数据完整性，本文在改进的 P-P 体制的基础上和在不增加密文长度的前提下，通过加入签名机制，使此体制成为一种高效的“加密+签名”体制。如果认为有必要接收方可以随时验证消息的完整性和消息的确切来源。如果事前用户双方有共享的秘密身份信息，则“加密+签名”体制将与改进的 P-P 加密体制几乎具有相同的效率。本文的结果同样可用于提高文献[1]中其它几种加密方案的效率

表 1　运算效率比较

	加密体制 1	加密体制 2	加密体制 2 (含预计算)	抵抗适应性攻击加密体制 1	“加密+签名”体制 3
加密	2-$E(n^2)$　1-$M(n^2)$	1-$E(n^2)$　2-$M(n^2)$	2-$M(n^2)$	2-$E(n^2)$　1-$M(n^2)$	1-$E(n^2)$　2-$M(n^2)$　1-Sgn
解密	2-L　1-$D(n)$	1-L　1-$M(n)$	1-L　1-$M(n)$	2-L　1-$D(n)$　2-$E(n)$　1-$M(n)$	1-L　1-$M(n)$　*1-Very

符号表示：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，$L(x)=(x^\lambda \bmod n^2-1)/n$；1-Sgn：一个签名运算；1-Very：一个验证运算。

参 考 文 献

[1] Paillier P, Pointcheval D. Efficient public-key cryptosystem provably secure against active adversaries. Advances in Cryptology-ASIACRYPT'99, 1999, LNCS Vol. 1716: 163 – 179.

[2] Catalano D, Gennaro R, Graham N H. The bit security of Paillier' encryption scheme and its applications. Advances in Cryptology-EUROCRYPTO'01, 2001, LNCS Vol. 2045: 229 – 243.

[3] Damgard I, Jurik M. A generalization, a simplification and some applications of Paillier's probabilistic public-key system. Advances in Cryptology-PKC'99, 2001, LNCS Vol. 1992: 119 – 136.

[4] Okamoto T, Uchiyama S. A new public key cryptosystem as secure as factoring. Advances in Cryptology EUROCRYPTO'98, 1998, LNCS Vol. 1043: 309 – 318.

[5] Cramer R, Shoup V. Universal hash proofs and a Paradigm for adaptive chosen ciphertext secure public-key encryption. Advances in Cryptology EUROCRYPTO'02, 2002, LNCS Vol. 2332: 45 – 94.

[6] Zheng Y L. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature)+cost (encryption). Advances in Cryptology CRYPTO'97, 1997, LNCS Vol. 1294: 165 – 179.

姜正涛： 男，1977年生，博士生，主要研究方向为密码算法理论的研究与分析、数论及其应用、通信网的安全、电子现金及相关技术等.

庞辽军： 男，1978年生，博士生，主要研究方向为电子商务中的安全理论与技术.

王育民： 男，1936年生，博士生导师，主要从事编码理论、密码学、信息安全等领域的科研与教学工作.