REESSE1 加密方案中杠杆函数的充分必要性分析

苏盛辉[1], 杨义先[2], 杨炳儒[1]
(1. 北京科技大学信息工程学院, 北京 100083; 2 北京邮电大学信息工程学院, 北京 100876)

摘 要: 文章介绍了 REESSE1 公钥体制的加密方案, 包括密钥生成、加密和解密 3 个算法. 通过对密钥变换公式中杠杆函数 $\ell(.)$ 为常数或不存在的假设, 讨论了连分式攻击, 因而从逆否命题的角度证明了 $\ell(.)$ 对 REESSE1 体制私钥安全的必要性. 作者通过不确定推理、反例列举和参数归约的方法论述了 $\ell(.)$ 存在时, REESSE1 的私钥安全性等价于多变量排列难题、明文安全性大于离散对数难题, 从而证明了 $\ell(.)$ 对 REESSE1 体制私钥与明文安全的充分性. 最后, 指出了私钥中包含三个独立参数的 REESSE1 体制与私钥中仅包含一个或两个参数的 MH、RSA 和 ElGamal 体制相比, 复杂性得到了显著提高.

关键词: 公钥密码体制; 安全性; 杠杆函数; 连分式; 加密
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2006) 10-1892-04

The Necessity and Sufficiency Analysis of the Lever Function in the REESSE1 Encryption Scheme

SU Sheng-hui[1], YANG Yi-xian[2], YANG Bing-ru[1]
(1. *School of Information Engineering, University of Science & Technology Beijing, Beijing* 100083, *China*;
2. *School of Information Engineering, Beijing University of Post & Telecom, Beijing* 100876, *China*)

Abstract: This paper presents the REESSE1 public key cryptosystem including three algorithms for keys, encryption and decryption, discusses the continued fraction attack by presuming that the lever function $\ell(.)$ in the key transform is one constant or does not exists, and proves that $\ell(.)$ is necessary to the private key security of REESSE1 from the contrapositive assertion. The authors argue that the private key security is equivalent to the multivariate arrangement hardness, and the plaintext security is greater than the discrete logarithm hardness when $\ell(.)$ exists in the transform by expounding the indeterminate reasoning, giving counterexamples and reducing parameters, and so show that $\ell(.)$ is sufficient for the private key and the plaintext securities. At last, point out that the complexity of REESSE1 whose private key contains three independent parameters is far higher than those of MH, RSA and ElGamal whose private keys contain only one or two parameters respectively.

Key words: public key cryptosystem; security; lever function; continued fraction; encryption

1 引言

大家知道, 陷门函数是设计公开密钥密码体制的关键所在, 例如, RSA 体制利用了大数难于分解的问题; ElGamal 体制利用了离散对数难于计算的问题[1]. 为了提高陷门函数的单向性, 通常把简单代数系统上的公钥体制移植到复杂代数系统上, 其实质是对群的运算符进行组合, 形成一种新的更为复杂的运算符. 例如, 椭圆曲线上的 ElGamal 体制与其在简单代数系统上相比安全性得到了较大提高[2].

在一个公钥体制中, 陷门函数一般能阻止从明文恢复密文, 但有时并不能阻止从公钥析取私钥. 例如, 在 MH 体制中, 密文子集和是陷门函数, 但它并不能阻止通过 Shamir 方法从公钥来提取私钥[3]. 在 REESSE1 体制中[4], 明文的安全性是基于子集模乘积这个陷门函数的(见本文第 4.3 节), 同时, 通过杠杆函数 $\ell(.)$ 来保护私钥的安全, 自然, 也就阻止了从私钥来获知明文. 这告诉我们, 在一个公钥体制中, 有时仅有陷门函数并不能保障整个体制的安全. 在本文, 我们将对 $\ell(.)$ 的必要性和充分性进行详细讨论.

2 REESSE1 公钥密码体制简介

在本文中, 我们仅讨论 REESSE1 体制的加密方案, 不考虑其签名方案.

2.1 互素序列和杠杆函数

定义: 如果 A_1、…、A_n 为 n 个互不相同、两两互素且大于 1 的正整数, 则称 $\{A_1, \cdots, A_n\}$ 为互素序列, 简记为 $\{A_i\}$.

性质: 对任意的正整数 $m \leqslant n$, 从互素序列 $\{A_i\}$ 中任选 m 个项组成子集 $\{Ax_1, \cdots, Ax_m\}$, 则子集的连乘积 $G = Ax_1, \cdots, Ax_m$ 是唯一确定的, 即 G 与 $\{Ax_1, \cdots, Ax_m\}$ 一一对应. G 也称为互素序列乘积.

利用算术基本定理可以证明该性质[4].

在 REESSE1 公钥密码体制中, 密钥变换式为 $C_i \equiv A_i W^{\ell(i)} (\mathrm{mod}\ M)$, 其中, $\ell(i)$ 为幂指数, M 为素模数.

在一个公钥密码体制中, 密钥变换式中的参数 $\ell(i)$ 被称为杠杆函数, 如果它具有下述特点:

(1) $\ell(.)$ 是整数到整数的单射函数, 其定义域为 $[1, n]$, 值域为 $[1, M)$. 令 L_n 代表从定义域到值域的所有单射的集

收稿日期: 2005-05-13; 修回日期: 2006-07-28

合, 则 $\ell(.)\in L_n$, 且$|L_n|\geqslant P_n^n$.

(2) i 与 $\ell(i)$ 之间的映射关系随机确定, 无解析表达式, 故每次公钥生成时, $\ell(.)$ 不一样.

(3) 在密钥变换式中, 不存在从 $\ell(.)$ 到公钥的专门映射.

(4) 从公钥推导私钥时, 不得不考虑 n 个 $\ell(i)$ 的全排列, 故当 n 足够大时, 全排列在有效时间内不可被穷举.

(5) 从私钥解开密文时, 只需要考虑 n 个 $\ell(i)$ 的累加和, 其时间复杂度与 n 多项式相关, 故解密是可行的.

显然, 若把密文当作支点, 则 $\ell(.)$ 是"公开"一端计算量大,"私有"一端计算量小.

2.2 REESSE1 密钥生成算法

(1) 随机产生长度为 n 的互素序列$\{A_1, \cdots, A_n\}$.

(2) 找到一个正素数 $M>\left(\prod_{i=1}^{n}A_i\right)$, 且$(M-1)$含$(n+4)$范围内所有素因子.

(3) 选取一个正整数 $W<M$, 并根据 $WW^{-1}\equiv 1 \pmod M$ 求出 W^{-1}.

(4) 随机产生两两不同的函数值 $\ell(i)\in\Omega=[5, n+4]$, $i=1, \cdots, n$.

(5) 计算非互素序列 $C_i\leftarrow A_i W^{\ell(i)} \bmod M$, $i=1, \cdots, n$.

算法结束后, 以$(\{C_i\}、M)$作为公钥, $(\{A_i\}、W^{-1}、M、\{\ell(i)\})$作为私钥.

注意, 可以选择 $\Omega=\{i\delta\mid i=5, \cdots, n+4\}$ 或$\{i+\delta\mid i=5, \cdots, n+4\}$, 这里 $\delta<[M/n^2]$ 为任意大的正整数. 此时, 仍可保证解密复杂度不超过 $O(n^3)$.

2.3 REESSE1 加密算法

设$(\{C_i\}、M)$为公钥, $b_1\cdots b_n$ 为 n 比特明文分组.

(1) 置 $\overline{G}\leftarrow 1$, $i\leftarrow 1$.

(2) 若 $b_i=1$, 则 $\overline{G}\leftarrow\overline{G}C_i \bmod M$.

(3) 令 $i\leftarrow i+1$, 若 $i\leqslant n$, 则转至(2), 否则, 结束.

最后, $\overline{G}$ 即为所求的密文.

2.4 REESSE1 解密算法

设$(\{A_i\}、W^{-1}、M)$为私钥, $\overline{G}$ 为密文.

(1) 计算 $\overline{G}\leftarrow\overline{G}W^{-1} \bmod M$.

(2) 置 $b_1\cdots b_n\leftarrow 0$, $G\leftarrow\overline{G}$, $i\leftarrow 1$.

(3) 若 $A_i\mid G$, 则 $b_i\leftarrow 1$ 且 $G\leftarrow G/A_i$.

(4) 令 $i\leftarrow i+1$, 若$(i\leqslant n$ 且 $G\neq 1)$, 则转至(3).

(5) 若 $G\neq 1$, 则转至(1), 否则, 结束.

最后, $b_1\cdots b_n$ 即为原 n 比特的明文分组.

3 杠杆函数的必要性

杠杆函数的必要性是指: 如果 REESSE1 体制的加密方案是安全的, 则密钥变换式中 $\ell(.)$ 必定存在. 与其等价的逆否命题是: 如果 $\ell(.)$ 为常数或不存在, 则 REESSE1 体制的加密方案是不安全的.

从 2.2 节知, 当杠杆函数 $\ell(.)$ 为整常数 k 时, 密钥变换公式成为 $C_i\equiv A_iW^k \pmod M$. 特别, 当 $k=1$ 时, $C_i\equiv A_iW \pmod M$, 这相当于 $\ell(.)$ 不存在. 由于我们仅改变 $\ell(.)$ 为常数 k, 所以, 体制的加密算法和解密算法仍然适用, 只是解密的时间复杂度由 $O(n^3)$ 降为 $O(n^2)$.

下面, 我们来分析在 $\ell(.)$ 为常数 k 的假设条件下, 如何从 REESSE1 体制的公钥推出私钥.

此时, $C_i\equiv A_iW^k \pmod M$, 加之$(Z_M^*, \cdot)$是交换群[5], 故有 $C_i^{-1}\equiv A_i^{-1}W^{-k} \pmod M$.

令 $G_x(C_xC_{n-1} \pmod M)$, 其中 $x\in[1, n-1]$.

则 $G_x\equiv A_xW^kA_{n-1}W^{-k}\equiv A_xA_n^{-1} \pmod M$, 即$A_nG_x-LM=A_x$.

两边同除以(A_nM)得

$$G_x/M-L/A_n=A_x/(A_nM) \tag{1}$$

由于 $M>\left(\prod_{i=1}^{n}A_i\right)$ 和 $A_i\geqslant 2$, 故有

$$G_x/M-L/A_n=A_x/(A_nM)<A_x/\left(A_n\prod_{i=1}^{n}A_i\right)=1/\left(A_n^2\prod_{i=1(i\neq x)}^{n}A_i\right)$$

$$\leqslant 1/(2^{n-2}A_n^2), \text{即} G_x/M-L/A_n<1/(2^{n-2}A_n^2) \tag{2}$$

不难看出, 式(1)右边是一个非常小的数, 根据连分式理论[6], L/A_n 应该为 G_x/M 连分式的一个收敛. 如果不是, 则 x 取别的下标, 直到 L/A_n 是一个收敛为止. 由于 G_x/M 的连分式长度不超过$(\log_2M+1)$, 因此, 依据不等式(2), L/A_n 可以被简单确定, 即 A_n 可以被确定. 进而 $W^k\equiv C_nA_n^{-1} \pmod M$ 可以被确定, 从而原互素序列$\{A_i\equiv C_iW^{-k} \pmod M\}$能够被恢复.

注意, 式(2)只是在我们所讨论的问题中成立, 离开我们所讨论的问题, 它不一定成立. 由于任何两个 C_x 与 C_y 中 W 的幂次相等, $C_xC_y^{-1}$ 中 W 的幂次总为零, 所以, $\ell(.)$ 为常数 k 时, 不存在不确定推理问题. 另外, 当 G_x/M 的一个收敛满足式(2)时, 其后的收敛也很可能满足式(2), 但如果 A_n 相当大, 则可以排除.

例如, 当 $n=6$, $k=3$ 时, 设互素序列为$\{11, 10, 3, 7, 17, 13\}$, 选取 $M=510931$, $W=17797$. 因此, $W^3=504387 \bmod 510931$.

由 $C_i\equiv A_iW^3 \pmod M$ 知非互素序列为: $\{438947, 445491, 491299, 465123, 399683, 425859\}$. 其逆序列$\{C_i^{-1}\}$为: $\{189051, 156863, 182256, 224090, 392820, 238571\}$.

令 $G_2\equiv C_2C_6^{-1} \pmod M$, 则

$G_2\equiv 445491\times 238571\equiv 432327 \pmod{510931}$.

从式(1)得: $432327/510931-L/A_6=A_2/(510931A_6)$.

依据连分式表示法, $432327/510931=1/(a_1+1/(a_2+1/(a_3+\cdots)))$.

由欧几里德算法求出 $a_1, a_2, a_3, \cdots$, 得

$432327/510931=1/(1+1/(5+1/(1+1/(1+1/(3929+1/(1+1/(2+1/3))))))))$.

试探取: $L/A_6=1/(1+1/(5+1/(1+1/1)))=11/13$, 则可能 $A_6=13$. 这时

$432327/510931-11/13=0.000001506<1/(2^4A_6^2)=1/(16\times 13^2)=0.000369822$,

满足式(2), 因此, 可以确定 $A_6=13$. 进而从 $A_6、C_6$ 可求出 $W^3=504387$ 以及原互素序列$\{A_i\}$.

上述讨论说明, 当杠杆函数为常数 k 或不存在时, 可以从公钥推出私钥并进一步从密文恢复明文. 我们将上述方法称为连分式攻击. 因此, $\ell(.)$ 对 REESSE1 体制的安全性来说

是必要的.

4 杠杆函数的充分性讨论

杠杆函数的充分性是指: 如果密钥变换式中 $\ell(.)$ 存在, 则 REESSE1 体制的私钥与明文是安全的. 这里的安全是指相对于某个难题的安全.

4.1 连分式攻击失败

当杠杆函数 $\ell(.)$ 存在时, 知密钥变换公式为 $C_i \equiv A_i W^{\ell(i)} (\mathrm{mod}\ M)$. 此时, $\ell(.)$ 给攻击者带来了至少两个困难: (1) 无法直接判断一些 C_i 中的参数 W 是否被逆元 W^{-1} 抵消. (2) 不存在用于验证不确定推理假设的多项式时间内的准则.

不确定推理是指先假设 W 和 W^{-1} 相互抵消, 然后根据逻辑结果来判断这种假设是否成立.

按照 3 节的思路, 先从 $\{C_i\}$ 中选 $h \leqslant n/2$ 个元素, 再另选 $m \leqslant n/2$ 个不同的元素. 令

$$G_Y \equiv Cy_1 \cdot \cdots \cdot Cy_h (\mathrm{mod}\ M),$$

$$G_X \equiv Cx_1 \cdot \cdots \cdot Cx_m (\mathrm{mod}\ M),$$

$$G_Z \equiv G_X G_Y^{-1} (\mathrm{mod}\ M),$$

并且规定 $Cy_i \neq Cx_j$, $i \in \{1, \cdots, h\}$, $j \in \{1, \cdots, m\}$.

由于 $\{\ell(i)\}$ 取值的任意性($\{5, \cdots, n+4\}$ 的一个排列), 我们无法断定 G_Z 中不含 W 或 W^{-1} 因子. 为了进一步推导, 我们不得不假设 G_X 中的 W 与 G_Y^{-1} 中的 W^{-1} 相互抵消. 于是

$$G_Z \equiv Ax_1 \cdot \cdots \cdot Ax_m \cdot A_{y_1}^{-1} \cdot \cdots \cdot A_{y_h}^{-1} (\mathrm{mod}\ M),$$

$$G_Z A y_1 \cdot \cdots \cdot A y_h - LM = Ax_1 \cdot \cdots \cdot Ax_m.$$

记 $A_Y = Ay_1 \cdot \cdots \cdot Ay_h$, 得到

$$G_Z/M - L/A_Y = Ax_1 \cdot \cdots \cdot Ax_m/(MA_Y) \tag{3}$$

由于 $M > \prod_{i=1}^{n} A_i$ 和 $A_i \geqslant 2$, 故有

$$G_Z/M - L/A_Y < 1/(2^{n-m-h} A_Y^2) \tag{4}$$

与 3 节类似, 式(3)的右边是一个很小的数, 故 L/A_Y 可以被看作是 G_Z/M 连分式的一个收敛. 由于符合条件(4)的收敛可能有多个, 从而有多个而不是一个 A_Y 的值将被确定.

根据 A_Y 的组成, 可分两种情况来讨论.

(i) $h = 1$ 的情况

假设 $n = 96$, $\ell(.)$ 值域为 $\{5, \cdots, 100\}$. 并且取 $m = 2$. 此时, $\ell(y_1) = \ell(x_1) + \ell(x_2)$ 的概率, 即攻击成功率为 $P_{1,2} = (45 \times 46)/(C_{96}^2 C_{94}^1) \approx 0.004829$. 显然, 如果 m 越大, 则 $P_{1,2}$ 越小, 因为分母中 C_{96}^m 将变大. 例如, 当 $m = 48$ 时, $C_{96}^{48} > 2^{92}$.

$h = 1$ 时, $A_Y = Ay_1$, 如果 A_Y 确定, 则意味着某个 A_i 很有可能直接暴露出来. 但对于单个 A_i 来讲, 它既可以是素数, 也可以是合数, 因此, "A_y 是否为素数" 不能作为 W 和 W^{-1} 相互抵消的判断准则. 同样, 式(4)也不能作为 W 和 W^{-1} 相互抵消的充分条件, 而只是必要条件, 这是由于 $\ell(.)$ 的不确定性造成的[4]. 即在 C_i 和 W 确定的情况下, A_i 与 $\ell(i)$ 不能被确定, 甚至没有一对一关系(如果 W 是非生成元); 在 C_i 和 A_i 确定时, W 与 $\ell(i)$ 不能被确定, 并且, 没有一对一关系(因为 $gcd(\ell(i), M^{-1}) > 1$). 因此, 非线性同余式 $C_i \equiv A_i W^{\ell(i)} (\mathrm{mod}\ M)$ 中包含内在随机性.

例如, 当 $n = 6$ 时, 设互素序列为 $\{11, 10, 3, 7, 17, 13\}$, 选择 $M = 510931$, 任取 $W = 17797$, $\ell(1) = 9$, $\ell(2) = 6$, $\ell(3) = 10$, $\ell(4) = 5$, $\ell(5) = 7$, $\ell(6) = 8$. 注意, 此时, $\ell(y_1) = \ell(x_1) + \ell(x_2)$ 不成立.

因此, $W^5 = 353831$, $W^6 = 416663$, $W^7 = 209808$, $W^8 = 69228$, $W^9 = 196075$, $W^{10} = 398976$.

由 $C_i \equiv A_i W^{\ell(i)} (\mathrm{mod}\ M)$ 得非互素序列为: $\{113101, 79182, 175066, 433093, 501150, 389033\}$. 其逆序列 $\{C_i^{-1}\}$ 为: $\{266775, 236469, 435654, 149312, 434038, 425203\}$.

任取 $y_1 = 5$, $x_1 = 2$, $x_2 = 6$, 令 $G_Z \equiv C_2 C_6 C_5^{-1}$, 则 $G_Z \equiv 79182 \times 389033 \times 434038 \equiv 342114 (\mathrm{mod}\ 510931)$.

假设 $(C_2\ C_6)$ 中的 W 与 C_5^{-1} 中的 W^{-1} 恰好相互抵消, 于是 $342114 \equiv A_2 A_6 A_5^{-1} (\mathrm{mod}\ 510931)$.

从式(3)得: $342114/510931 - L/A_5 = A_2 A_6/(510931\ A_5)$.

由欧几里德算法求出 $a_1, a_2, a_3, \cdots$, 得

$342114/510931 = 1/(1 + 1/(2 + 1/(37 + 1/(1 + 1/(2 + \cdots + 1/4))))))$.

试探取: $L/A_5 = 1/(1 + 1/2) = 2/3$, 则可能 $A_5 = 3$. 这时

$342114/510931 - 2/3 = 0.002922769 < 1/(2^{6-2-1} A_5^2) = 1/(8 \times 3^2) = 0.013888889$, 满足式(4), 因此, 推导出 $A_5 = 3$. 这与实际 $A_5 = 17$ 矛盾, 所以, 式(4)不能作为充分条件.

进一步, 由于 W 和 $\ell(i)$ 的任意性, 根据式(3)和(4), A_i 将被推导为每个可能的值. 因此, 依据式(3)和(4)所做攻击的时间复杂度至少将达到 $O(n!)$.

(ii) $h \neq 1$ 的情况

这时, $A_Y = Ay_1 \cdot \cdots \cdot Ay_h$ 是一个因式分解问题. 大家知道, 任何一个合数 $A_Y \neq p^k$ (p 为素数) 可分解为若干个素数的乘积, 且从该合数的因式可得到多个不同长度和不同排列的互素序列.

例如, 令 $A_Y = 210$, 则可以得到互素序列 $\{6, 35\}$、$\{10, 21\}$、$\{5, 6, 7\}$、$\{3, 7, 10\}$、$\{2, 3, 5, 7\}$、$\{3, 2, 5, 7\}$ 等等.

事实表明, 无论 W 与 W^{-1} 抵消与否, 大多数情况下都能从 A_Z/M 连分式的满足条件(4)的收敛中找到至少一个 A_Y, 它能表达成 h 个互素整数的乘积. 因此, "A_Y 能否表达成 h 个互素整数的乘积" 不可以作为验证 W 与 W^{-1} 抵消假设的准则.

如果试图穷举 $\{\ell(i)\}$ 的排列, 则有可能根据式(3)和(4)求出序列 $\{A_i\}$. 但穷举 $\{\ell(i)\}$ 的排列是 $O(n!)$ 时间复杂度, 这里 $n!$ 表示阶乘.

故杠杆函数 $\ell(.)$ 存在时, 不确定推理失败, 即连分式攻击失效.

4.2 从公钥推导私钥等价于多变量排列难题

在 REESSE1 公钥体制中, 密钥变换公式为 $C_i \equiv A_i W^{\ell(i)} (\mathrm{mod}\ M)$. 在 2.1 节我们提过, 在密钥生成算法中, 可以规定 $\ell(i) \in \{i \delta \mid i = 5, \cdots, n+4\}$.

对于一个具体的 C_i 而言, 假设在某种极端情况下, 相应的 A_i 和 W 被泄露, 则有 $W^{\ell(i)} \equiv C_i A_i^{-1} (\mathrm{mod}\ M)$, 由于 $\ell(i) \in (1, M)$, 求 $\ell(i)$ 是离散对数难题. 因此, 在正常情况下, 从公钥

推导私钥是比离散对数更困难的.

在下面, 我们讨论 n 个 C_i 联立的情况.

设 $p_g > n$ 为体制中最大素常数, 则每个 $A_i \in \Lambda = \{2, \cdots, p_g\}$, 这里 Λ 至少含有 n 个素数. 令 $\tilde{N}$ 为 $[2, p_g]$ 区间内可能的互素序列个数, 则显然 $\tilde{N} > A_n^n = n!$.

如果令 $\ell(1) = \cdots = \ell(n) = 5$, 并且每个 A_i 遍历 Λ, 则可以得到含 W 真实值的约 $5^n p_g$ 个值. 因此, W 的可能值个数能降低到 $5^n p_g$. 虽然这对 REESSE1 的安全性没有影响, 但用户可以选择 $\Omega = \{i + \delta \mid i = 5, \cdots, n+4\}$ 来避免它.

假设攻击者猜测序列 $\{A_i\}$ 和 $\{\ell(i)\}$, 并在 $O(T_W)$ 时间内求出 n 个 W, 如果这些值两两相等, 则认为猜测正确. 注意, 对于第 i 个方程, A_i 被允许取 Λ 中任何值只要它与 $\{A_1, \cdots, A_{i-1}\}$ 两两互素, $\{\ell(i)\}$ 被允许取 $\{5, \cdots, n+4\}$ 中任何值只要它与 $\{\ell(1), \cdots, \ell(i-1)\}$ 两两不同, 这意味着猜测 $\{A_i\}$ 和 $\{\ell(i)\}$ 是排列问题. 因此, 这种攻击所需的时间复杂度为 $O(\tilde{N}(n!)T_W) > O(2^n)$.

类似地, 如果攻击者猜测 W 和序列 $\{\ell(i)\}$, 则攻击复杂度为 $O(5^n p_g (n!) T_A) > O(2^n)$. 如果攻击者猜测 W 和序列 $\{A_i\}$, 则攻击复杂度为 $O(5^n p_g \tilde{N} T_\ell) > O(5^n p_g (n!) T_\ell) > O(2^n)$. 这里, $O(T_A)$、$O(T_\ell)$ 分别为计算序列 $\{A_i\}$ 和 $\{\ell(i)\}$ 的时间.

4.1 和 4.2 讨论了两种最有效的攻击私钥的方法, 它们皆是多变量排列问题, 时间复杂度至少为 $O(n!)$. 这些表明: 当 $\ell(.)$ 存在时, 从公钥推导私钥是比阶乘问题 $O(n!)$ 更困难的, 在多项式时间内无解. 从这个意义上说, 杠杆函数 $\ell(.)$ 是 REESSE1 私钥安全的充分条件.

4.3　从密文破译明文是比离散对数更困难的

根据 2.3 节加密算法, 密文 $\overline{G} \equiv \prod_{i=1}^{n} C_i^{b_i} \pmod M$. 这里, $b_1 \cdots b_n$ 为明文, $\{C_i\}$ 为公钥.

考虑一种极端情况. 假设 $C_1 = \cdots = C_n = C$, 则

$\overline{G} \equiv \prod_{i=1}^{n} C^{b_i} \pmod M$, 其可以表示为 $\overline{G} \equiv C^{\sum b_i} \pmod M$.

因为我们不仅要求出 $\sum_{i=1}^{n} b_i$ 的值, 而且也要求出 $b_i = 1$ 的位置, 故我们把 $\sum_{i=1}^{n} b_i$ 等价地表示为 $(\sum_{i=1}^{n} b_i 2^{i-1})$, 并令 $x = (\sum_{i=1}^{n} b_i 2^{i-1})$, 则相应地

$\overline{G} \equiv C^x \pmod M$.

显然, 求 x 是一个离散对数问题. 这说明如果 REESSE1 的明文破译问题能解决, 则离散对数问题能解决. 所以, 当 $C_1 \neq \cdots \neq C_n$ 时, 已知密文和公钥企图恢复明文是比离散对数更困难的问题.

注意, 当把 $\overline{G}$ 转化为互素序列乘积 G 时, 则求明文 $b_1 \cdots b_n$ 是容易的. 所以说, REESSE1 的明文安全性是建立在从子集元素求子集模乘积易、但从子集模乘积求子集元素难的陷门问题上的.

从第 3 节知, 如果 $\ell(.)$ 不存在, 则可以从公钥译出私钥, 进而在私钥的基础上从密文恢复明文, 即 $\ell(.)$ 对明文的安全性来说也是必要的. 从这一节知, 当 $\ell(.)$ 存在时, 则求取明文是比离散对数更困难的, 所以, $\ell(.)$ 对 REESSE1 明文的安全性来说也是充分的.

5　跋

综合上述, 杠杆函数 $\ell(i)$ 对 REESSE1 体制的私钥与明文安全性来说既是必要的, 也是充分的. 所以, 杠杆函数和陷门函数的共同作用保障了 REESSE1 体制加密方案的安全性.

杠杆函数 $\ell(i)$ 的存在使 REESSE1 体制的安全性发生了质的变化. 为什么会这样呢? 首先, 从密钥变换公式 $C_i \equiv A_i W^{\ell(i)} \pmod M$ 可以看出, REESSE1 体制的私钥部分隐藏了三个未知参数, 即 A_i、W 和 $\ell(i)$. 这与 MH 背包、RSA 或 ElGamal 体制有着显著不同, 后三者的私钥部分只隐藏了一个或两个未知参数. 其次, 是由于“三体问题”的存在, 即两个天体的运动能够很好地被 Newton 传统力学所解释, 但三个天体的运动根本不能为 Newton 定律所解释. Poincaré H 认为这是确定性非线性系统中的内在随机性问题, 即混沌. “三体问题”提示我们, 在非线性系统中, 参数个数从 2 增加到 3, 不仅仅是量的变化, 而且是质的飞跃, 带来了系统复杂性的显著提高. 鉴于上述原因, 我们把 REESSE1 体制归属于多变量公钥密码体制.

注意, 在本文中, 我们仅讨论杠杆函数 $\ell(.)$ 对 REESSE1 加密方案的充分必要性. 对 REESSE1 签名方案的讨论与改进将在另外一篇文章中叙述.

在公开文献中, 我们只是给出了 REESSE1 加密方案的理论算法. 当 $n = 128$ 时, 该理论算法的密钥空间是较大的, 解密时间复杂度也是较高的, 为 $O(n^3)$. 因此, 在实际应用中, 我们已经对理论算法进行了降模优化. 优化后, $n = 128$ 时, 复杂度降为为 $O(n^2)$, $\log_2 M = 640$, 公钥长度为 122880 比特 = 15360 字节 < 16K 字节, 远在普通 IC 卡 64K 字节的存储容量之内, 因此, 符合实用要求.

致谢　REESSE1 体制在研究过程中, 得到了中科院下属院所、国防科技大学、北京大学、武汉大学等单位有关专家和学者的热忱指导与帮助, 在此, 作者表示衷心的感谢.

参考文献:

[1] Menezes A J. Oorschot P. van and Vanstone S. Handbook of Applied Cryptography[M]. London: CRC Press, 1997. 285- 289, 294- 297.

[2] Stallings Willian. Cryptography and Network Security: Principles and Practice (2nd Ed.)[M]. New Jersey: Prentice-Hall, Inc., 1999. 193- 198.

[3] Shamire A. On the cryptocomplexity of knapsack system[A]. Proceedings of the 11th ACM STOC'79[C]. 1979. 118- 129.

[4] 苏盛辉. REESSE1 公开密钥密码体制[J]. 计算机工程与科学, 2003, (5): 13- 16.

[5] Snaith Victor P. Groups, Rings and Galois Theory[M]. Singapore: World Scientific Publishing Co Pte Ltd., 1998. 42- 46.

[6] Yan Song Y. Number Theory for Computing (2nd Ed.)[M]. Berlin: Springer-Verlag, 2002. 44- 51.

作者简介:

苏盛辉　男, 教授级高工, 候选博士. 本、硕分别毕业于国防科大和北京大学, 自 2000 年以来主导提出 REESSE 系列密码体制, 获国家发明专利权 3 项. 研究兴趣: 密码算法、信息安全和决策支持系统.

E-mail: sheenway@126.com