第16卷 第2期
2006年2月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol. 16 No. 2
Feb. 2006

一种基于复合加密的公钥密码系统

王平水[1,2]

(1.合肥工业大学 计算机与信息学院,安徽 合肥 230009)
2.安徽财经大学 网络中心,安徽 蚌埠 233041)

摘 要:公钥密码系统以其算法设计简单、安全性高已经成为密码学领域的一个非常重要的研究课题。为了更加高效地构造公钥密码系统,文中利用方程 $Ax + By = C$ 的解的不定性,提出了将两个加密算法复合成新加密算法的方法,对此做了分析,并给出了具体例子。实践表明,这种基于复合加密的公钥密码系统,算法的时间复杂度和空间复杂度并未受到影响,但其安全性较早期各同类系统更高、更易被用户采纳。

关键词:公钥密码系统;复合加密;背包向量
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1005-3751(2006)02-0206-02

A Public Key Cryptosystem Based on Compound Encryption

WANG Ping-shui[1,2]

(1. School of Computer and Information, Hefei University of Technology, Hefei 230009, China;
2. Network Center of Anhui University of Finance and Economics, Bengbu 233041, China)

Abstract: Public key cryptosystem has become a very important research topic in cryptography field for its simple algorithm design and high security. To build public key cryptosystem more effectively, gave a method to make a new cryptosystem from two given cryptosystems using the Diophantine equation $Ax + By = C$, then analyzed the method and gave some examples. It is proved that this public key cryptosystem based on compound encryption has not been influenced on time complexity and space complexity, but it has more security than the early systems and is much easier to be adopted by users.

Key words: public key cryptosystem; compound encryption; knapsack vector

0 引 言

关于加密算法的复合,早已用于构造加密系统或见于一些文献中[1,2]。例如,迭代MH系统、DES加密算法,以及所谓算法的乘积,都可视为两个或多个加密算法的复合。在文献[3]中,也给出了一种复合加密系统。

用 P 表示明文,F_1 与 F_2 表示两个加密算法,F 表示由 F_1 与 F_2 所产生的复合算法,E_1、E_2 与 E 分别表示用 F_1、F_2 与 F 对 P 加密后所得到的密文。一般地,由 F_1 与 F_2 可以有两种不同的方式产生 F。

其一,是简单的复合,即

$$E = F(P) = F_2(E_1) = F_2(F_1(P))$$

像迭代MH系统就使用这样的复合。

其二,是将 F_1 与 F_2 分别作用于明文 P 的两个不相交的部分,然后以某种方式构成 $F(P)$,例如DES系统。文中的目的在于讨论一种复合加密算法的构成方式,它与已经知道的复合加密算法的构成是不同的,在原则上,属于上述的第二种方式。

以下,在谈到算法函数 $F_1(P)$ 与 $F_2(P)$ 的复合时,当然要涉及它们的定义域等问题,即这些算法的可行性等问题。对于这样一些必要条件,一般来说,在设计加密系统时是容易解决的,所以,总假定这些条件是已经具备的。

1 两个加密算法的复合

以下,主要考虑公钥密码系统的加密算法的复合[4]。

1.1 构 成

设 $F_1(P;k_1)$ 与 $F_2(P;k_2)$ 是两个公开钥加密算法,其中 k_1, k_2 是公开钥。设 D_1 与 D_2 分别是 F_1 与 F_2 的保密钥。

随机地选取 $r, s, r + s = n$,以及满足某些条件的正整数 A, B(以后将给出这些条件)。

设明文 P 的二进制表示是 $p_1 \cdots p_r p_{r+1} \cdots p_n$。记 $P_1 = p_1 \cdots p_r$,$P_2 = p_{r+1} \cdots p_n$,$P = P_1 P_2$。

由复合加密算法 $F = F_1 \oplus F_2$ 将明文 P 加密后的密文是:

$$E = F(P) = AF_1(P_1) + BF_2(P_2) \quad (1)$$

此处加法符号表示普通的算术加法。

收稿日期:2005-05-29
基金项目:安徽省2003自然科学基金项目(03042204)
作者简介:王平水(1972—),男,安徽蚌埠人,讲师,硕士,研究方向为符号计算与网络信息安全;导师:吴国凤,教授,硕士生导师,研究方向为数据库与网络安全。

加密算法 F 的公开钥是与 A,B,k_1 及 k_2 有关的数据,它的保密钥则是 A,B,D_1 及 D_2(可能也保密 r 或 s)。

1.2 解　密

由式(1)可知,为了从密文 E 译出明文 P,必须由方程

$$Ax + By = E \tag{2}$$

解出 $F_1(P_1)$ 与 $F_2(P_2)$,然后利用已知的对 F_1 与 F_2 的解密方法分别译出明文 P_1 与 P_2,从而得到明文 P。

方程(2)是一个不定方程。利用Euclid算法,当 $(A,B)=1$ 时,在多项式时间内容易求出(2)的一个特解 (x_0,y_0)。此时,方程(2)的通解具有以下形式:

$$x = x_0 + Bt \quad y = y_0 - At \quad t \in Z \tag{3}$$

如果已知密文 $F_1(P_1)$ 或 $F_2(P_2)$ 满足条件

$$0 \leqslant F_1(P_1) < B \quad 或 \quad 0 \leqslant F_2(P_2) < A \tag{4}$$

则由式(3)可以唯一地确定式(1)的 $F_1(P_1)$ 与 $F_2(P_2)$,从而译出明文 P。

除了条件(4)可以保证唯一地确定所需要的 $F_1(P_1)$ 与 $F_2(P_2)$ 外,下面的定理也提供了这样的条件。

定理[5]　设 $\bar{a}_i=(a_{i1},\cdots,a_{ik})\in Z^k(1\leqslant i\leqslant l)$,$M\in N$,以 λ_k 表示由 $\bar{a}_1,\cdots,\bar{a}_l$ 以及 $\bar{Me}_i=(0,\cdots,0,M,0,\cdots,0)$($M$ 在第 i 个位置)$(l\leqslant i\leqslant k)$ 所构成的整格 $L(\bar{a}_1,\cdots,\bar{a}_l,\bar{Me}_1,\cdots,\bar{Me}_k)$ 的最大相邻极小值,则方程组

$$a_{i1}x_1+\cdots+a_{ik}x_k\equiv c_i \pmod M \quad 1\leqslant i\leqslant l \tag{5}$$

满足

$$x_1^2+\cdots+x_k^2\leqslant M^2\lambda_k^{-2}2^{-k-2} \quad (x_1,\cdots,x_k)\in Z^k$$

的解至多有一个。若诸 a_{ij},c_i 及 M 为已知,则存在多项式时间算法可以求出这个解(或者判定它不存在)。

由上述定理可见,在确定了 λ_k 的数值界限之后,就有多项式时间算法确定满足式(5)的解,或者确定它是不存在的。

上面给出了由方程(2)确定 $F_1(P_1)$ 与 $F_2(P_2)$ 的某些条件和方法,即由密文在多项式时间内译出明文的方法。

另一方面,对于密码分析人员来说,欲由密文 E 破译出明文 P,但又不知保密钥,则将遇到两个方面的困难:第一,在没有关于 A 与 B 的信息的情况下,求解方程(1)在计算上是困难的,其困难程度至少大于特大整数分解因数的困难。这是因为,若取 $B=0$,则方程(2)成为 $Ax=E$,求解 x 即是分解整数为因数 E 之积了。第二,即使得到了 $F_1(P_1)$ 与 $F_2(P_2)$ 的数值,还需要分别破译出明文 P_1 与 P_2,即破译由密码系统 F_1 与 F_2 将明文 P 加密后的密文,显然,其计算时间是破译 $F_1(P_1)$ 与 $F_2(P_2)$ 所需时间之和。

1.3 例　子

例1　设 F_1 是MH加密算法,它的公开加密钥是背包向量 $(b_1,\cdots,b_r)$,保密钥是 k,m 和简单背包向量 $(a_1,\cdots,a_r)$,此处 $(k,m)=1$,并且

$$b_i = ka_i \pmod m \quad l\leqslant i\leqslant r$$

又设 F_2 是RSA加密算法,其公开加密钥是 e 与 m_1,此处 $m_1=pq$,p 与 q 是两个"差不多"相等的大素数,$(e,\varphi(m_1))=1$,其保密钥是 $p,q,\varphi(m_1)$ 以及由 $ee'\equiv 1[\bmod \varphi(m_1)]$ 所确定的 e',$0\leqslant e'<\varphi(m_1)$;又公开正整数 r。

不妨设明文 P 的二进制表示是 $p_1\cdots p_n(n>r)$,记 $P_1=p_1\cdots p_r$,$P_2=p_{r+1}\cdots p_n$。

由 F_1 与 F_2 复合而成的加密算法 $F=F_1\oplus F_2$ 对明文 P 加密后的结果是密文

$$E = E(P) = \sum_{i=1}^{r} b_ip_i + E_2$$

其中

$$E_2 = P_2^e \pmod{m_1} \quad 0\leqslant E_2\leqslant m_1$$

由加密过程可见,若记 k' 满足

$$E_0\equiv k'E \pmod m \quad 0\leqslant E_0<m$$

其中 $kk'\equiv 1 \pmod m$ $0\leqslant R'<m$,则

$$E_0\equiv k'E = \sum_{i=1}^{r} a_ip_i + k'E_2 \tag{6}$$

设

$$k' > \sum_{i=1}^{r} a_i \quad k'(m_1+1)<mL \quad L=O(\log^{\lambda}m) \tag{7}$$

其中 $\lambda>0$ 是某个常数,则存在某个确定的数 A_0,$0\leqslant A_0<L$,使得

$$\sum_{i=1}^{r} a_ip_i + k'E_2 = E_0 + A_0\,m \tag{8}$$

因此,对于每个 A,$0\leqslant A<L$,解方程

$$x + k'y = E_0 + Am \tag{9}$$

就得 L 个解。其中必有一组解 $(x_0,y_0)=(\sum_{i=1}^{r} a_ip_i,E_2)$。在确定这一组解之后,就可以利用简单背包向量 $(a_1,\cdots,a_r)$ 及RSA系统的解密算法恢复明文 P_1 与 P_2,从而得到明文 P。

应该指出,如果 $L=1$,则式(9)即 $x+k'y=E_0$。一般地,对于 L 个不同的 A 值可得到 L 个方程(9)的解,为了从这 L 个解中确定 $(\sum_{i=1}^{r} a_ip_i,E_2)$,可以像Rabin公钥系统那样,在加密前附加一定数量的随机位在明文末尾(随机位的数量当然要限制在不影响系统安全的范围内)。然后将它们与密文同时发送出去作为校正码。

对于每个 A 值,解方程(9)只需要使用Euclid算法和算术运算,因此,在多项式时间内可以从密文恢复出明文。

例2[6]　设 F_1 与 F_2 都是MH加密算法,它们的公开加密钥分别是 $(A_1,\cdots,A_r)$ 与 $(B_1,\cdots,B_s)$,保密钥分别为 $k_1,(a_1,\cdots,a_r)$ 与 $k_2,(b_1,\cdots,b_s)$ 以及大整数 m,此处 $(a_1,\cdots,a_r)$ 与 $(b_1,\cdots,b_s)$ 都是简单背包向量,$(k_1,m)=(k_2,m)=1$。

由 F_1 与 F_2 复合而成的加密算法 $F=F_1\oplus F_2$ 是一个背包型加密算法,它的公开加密钥是背包向量 $(A_1,\cdots,$

(下转第211页)

第二种攻击方法是对证书库的攻击,它使证书库不能提供服务。基于分簇的分布式 CA 策略,可以处理从(1,0,r)到(1,s,r)形式的攻击(r 是簇中受到攻击的证书库的数量),设 t 是簇中证书库节点的数量($t > r$)。令 $b = t - r$,则簇中至少有 b 个证书库可以提供服务。这样只要簇中有一个证书库可以提供服务,就不会影响簇中的正常操作。这种增加证书库的冗余策略,提高了证书库的抗攻击能力,能有效地保证网络的正常运行。

第三种攻击方法是用户身份伪造,通过这种方法非法用户可以获得网络中的重要资源。系统中 RA 主要负责对用户身份的审查。用户只有通过 RA 才能获得入网证书。而 RA 是由控制中心指定,它具有较高的安全性。

3 结　论

文中提出的分布式有线 PKI 和无线分布式 PKI 相结合的安全体系结构,解决了移动 Ad Hoc 网络中存在的一些安全问题,具有较高的安全性。基于门限算法的分布式 CA 签名的应用,解决了单点 CA 易受攻击的问题。有线分布式 CA 签名算法的应用为移动 Ad Hoc 网络的物理层、数据链路层以及路由层的安全提供了保证。无线分布式 PKI 保证了网络资源访问的安全性。分簇算法的应用减少了节点要存放证书所需的容量和网络中的通信流量。椭圆曲线算法的应用减少了节点计算的复杂度。

参考文献:

[1] Asokan N, Ginzboorg P. Key Agreement in Ad - hoc Networks[EB/OL]. http://citeseer.ist.psu.edu/cache/papers/cs/14830/. http:zSzzSzwww.semper.orgz Szsirenez Szpeoplez Szasokanz Szresearchz Szccr.pdf/asokan99key.pdf, 2005.

[2] Capkun S, Buttyan L, Hubaux J P. Self - Organized Public - Key Management for Mobile Ad Hoc Networks[R]. Technical Report EPFL/IC/200234, Lausanne: Swiss Federal Institute of Technology, 2002.

[3] Zhou L, Haas Z J. Securing Ad Hoc Networks[J]. IEEE Network, 1999, 13:24 - 30.

[4] 戴元军, 杨　成. 基于椭圆曲线密码体制的(t,n)门限签名方案[J]. 计算机应用研究, 2004(9):142 - 143.

[5] 徐海霞, 李　宝. 分布式密钥分发方案的安全性证明[J]. 软件学报, 2005, 16(4):570 - 576.

[6] 伍忠东, 谢维信, 喻建平. 一种安全增强的基于椭圆曲线可验证门限签名方案[J]. 计算机发展和研究, 2005, 42(4):705 - 710.

[7] Zouridaki C, Mark B L, Gaj K, et al. Distributed CA - based PKI for Mobile Ad Hoc Networks Using Elliptic Curve Cryptography[Z]. Lecture Notes in Computer Science[s. l.]: Springer - Verlag GmbH, 2004. 232 - 245.

(上接第 207 页)

$A_r, B_1, \cdots, B_s)$, r 与 s 都是保密的。

2 注　记

1)第一部分中的原则可以用于多个加密算法的复合。此时,需要解形如:

$$\lambda_1 x_1 + \cdots + \lambda_k x_k = E$$

的方程。由前面的定理可以得到确定上述方程解的条件,即对诸 λ 所需附加的条件。

2) 第一部分中的两个例子都用到简单背包向量,这并不是必要的。事实上,若有背包向量$(a_1, \cdots, a_n)$使得方程

$$a_1 x_1 + \cdots + a_n x_n = b$$

的求解总是容易计算的(当已知某些陷门信息时),就可用它代替例子中的简单背包向量,称这样的向量为易解背包向量。在文献[7] 中所设计的背包向量就是易解背包向量。

3) 前面的两个例子中均取 F_1 与 F_2 为公钥密码系统的算法函数,这当然不是必要的。它们也可以是传统的加密算法函数。例如[8],在例 1 中,若取 F_2 是用伪随机数列$(\lambda_1, \cdots \lambda_s)$对 $P_2 = p_{r+1} \cdots p_n (n = r + s)$ 加密的算法,即用二进制数 $a_1 \cdots a_s$ 作为 $E_2 = F_2(P_2)$,其中 $a_i \equiv p_{i+r} + \lambda_i \pmod 2$, $\lambda_i = 0$ 或 1, $1 \leqslant i \leqslant s$,那么,容易看出,在例 1 中对 $F(P), F_1(P_1), F_2(P_2)$ 所做的分析都仍是有效的,只不过要将式(7) 中的 $k'(m_1 + 1) < mL$ 改为 $k'(2^{s+1} + 1) < mL$。

参考文献:

[1] Salomaa A. Public - Key Cryptography[M]. New York: Springer - Verlag, 1990.

[2] van Tilborg H C A. An Introduction to Cryptography[M]. Boston: Kluwer Academic Publishers, 1988.

[3] 曹珍富. 公钥密码学[M]. 哈尔滨: 黑龙江教育出版社, 1993.

[4] Koblitz N. A Course in Number Theory and Cryptography [M]. New York: Springer - Verlag, 1987.

[5] Frieszetal A M. Reconstructing Truncated Integer Variables Satisfying Linear Congruences[J]. SIAM J. Comput, 1988, 17:262 - 280.

[6] Diffie W, Hellman M E. New Directions in Cryptography[J]. IEEE Trans. Informat. Theory, 1976, 22:644 - 654.

[7] Ben - Zion C. Two Issues in Public Key Cryptography[M]. ACM Distin guished Dissertations, MIT campus, USA: The MIT Press, 1985.

[8] ElGamal T. A Public - Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm[J]. IEEE Trans. Informat. Theory, 1995, 31:469 - 472.