一种双矩阵组合公钥算法

邵春雨[1,2],苏锦海[2],魏有国[1],周晶晶[1]
(1.武汉军械士官学校,湖北武汉 430075; 2.解放军信息工程大学电子技术学院,河南郑州 450004)

摘 要: 组合公钥算法中存在选择共谋攻击、随机共谋攻击和线性分析共谋攻击.本算法中用户的私钥是基本私钥与辅助私钥的逆元模乘的结果,基本私钥与辅助私钥分别由基本私钥矩阵和辅助私钥矩阵中的元素组合生成,用户的私钥间不存在线性关系.经过分析,本算法可以抵抗组合公钥算法中存在的选择共谋攻击和随机共谋攻击,并且辅助密钥矩阵的大小可以根据需要进行选取,系统的安全性可控.

关键词: 组合公钥; 共谋攻击; 椭圆曲线
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2011) 03-0671-04

A Double Matrix Combined Public Key Algorithm

SHAO Chun-yu[1,2], SU Jin-hai[2], WEI You-guo[1], ZHOU Jing-jing[1]
(1. *Wuhan Ordnance N. C. O Academy of PLA, Wuhan, Hubei* 430075, *China*;
2. *Institute of Electronic Technology, Information Engineering University of PLA, Zhengzhou, Henan* 450004, *China*)

Abstract: There are choice collusion attack, random collusion attack and linear collusion attack in CPK. The user's private key of this algorithm was generated by multiplying the basic private key with the inverse of the assistant private key. The basic private key and the assistant private key was the result of combining the elements of the basic private key matrix and the assistant private key matrix separately. The relationship among user's private keys is nonlinear. By analyzing, this algorithm can defend from the choice collusion attack and random collusion attack that existed in CPK. The size of assistant key matrix can be chose according to need; the security of the system can be controlled.

Key words: CPK; collusion attack; ECC

1 引言

我国学者南湘浩教授于1999年提出组合公钥算法(Combined Public Key – CPK).CPK算法依据离散对数难题的数学原理构建公钥矩阵和私钥矩阵,采用映射算法将用户的标识映射为矩阵的行、列坐标,用以对矩阵元素进行选取与组合,生成数量庞大的由公私钥矩阵元素组成的公私钥对,从而实现基于标识的超大规模密钥生产.

由于CPK具有大规模密钥管理及公钥不需要第三方认证的特点,与PKI、IBE相比具有优势[1~3],得到了广泛的研究,人们已经研究设计了基于CPK算法的安全电子邮件系统、认证系统,将CPK算法应用到网格计算、AD HOC网络、移动IPv6(MIPv6)网络等方面.

由于CPK算法中用户的私钥是私钥矩阵中的某些与用户标识相关的元素模加产生的,私钥间存在线性关系,因此存在下面三种共谋攻击:线性分析共谋攻击[4]、选择共谋攻击[5]、随机共谋攻击[5].

为了解决共谋攻击问题,有人提出采用软硬件相结合的私钥保护法[6],但这种解决方法没有得到业界人士的普遍认同.还有人提出通过扩大密钥矩阵来解决[4],但这种方法只能抵抗线性共谋攻击,不能抵抗选择共谋攻击和随机共谋攻击.2008年,南湘浩教授提出了标识密钥与随机密钥复合的组合公钥2.0版本[7],解决了共谋攻击问题,但如果用户规模较大,存在随机密钥的管理问题.文献[8]设计了一种基于CPK的IBE方案,该方案同样存在共谋攻击问题.文献[9]提出了多域基本模型,试图解决共谋攻击,但该方案中仍然存在选择共谋攻击和随机共谋攻击.

经过研究分析存在的共谋攻击及已有解决方案,发现通过一个私钥矩阵难以消除用户私钥间的线性关系,解决已经存在的共谋攻击问题.本算法利用两个私钥矩阵共同生成用户的私钥,即:在原CPK算法中增加一套辅助密钥矩阵,而原CPK算法中的基本密钥矩阵不变,因此称本算法为双矩阵组合公钥算法.由基本密钥矩阵、辅助密钥矩阵分别产生基本密钥对和辅助密钥对,用户的私钥是基本私钥与辅助私钥逆元模乘的结果,

收稿日期:2009-10-29;修回日期:2010-11-01

因此用户私钥间不存在线性关系.通过分析,本算法可以抵抗已有的选择共谋攻击和随机共谋攻击,并且,辅助密钥矩阵的大小可以根据需要选取,系统的安全性可控.

2 双矩阵 CPK 算法

本算法在原 CPK 算法中增加了辅助密钥矩阵,辅助密钥矩阵负责生成辅助公私钥,由基本公私钥和辅助公私钥共同生成用户公私钥对,辅助密钥矩阵的大小可以根据系统的安全需求而变化,下面是具体算法.

2.1 系统初始化

CPK 算法以有限域 F_p(p 为不等于 2 和 3 的素数)上的椭圆曲线构建,确定椭圆曲线密码的五个参数为 $\{a,b,G,n,p\}$.

2.2 密钥矩阵设置

本算法中的密钥矩阵包括基本密钥矩阵和辅助密钥矩阵:

(1)基本密钥矩阵

在 Z_n(Z_n 是模 n 的有限域)中随机选取 $m\times h$ 个种子私钥 $r_{i,j}$,生成如下 $m\times h$ 基本私钥矩阵 $\boldsymbol{M}_{BSK}$和基本公钥矩阵 $\boldsymbol{M}_{BPK}$:

$$\boldsymbol{M}_{BSK}=\begin{pmatrix} r_{1,1} & \cdots & r_{1,h} \\ \vdots & \ddots & \vdots \\ r_{m,1} & \cdots & r_{m,h} \end{pmatrix} \quad \boldsymbol{M}_{BPK}=\begin{pmatrix} r_{1,1}G & \cdots & r_{1,h}G \\ \vdots & \ddots & \vdots \\ r_{m,1}G & \cdots & r_{m,h}G \end{pmatrix}$$

(2)辅助密钥矩阵

在 Z_n 中随机选取 $l\times t$ 个种子私钥 $s_{i,j}$,生成如下 $l\times t$ 辅助私钥矩阵 $\boldsymbol{M}_{ASK}$和辅助公钥矩阵 $\boldsymbol{M}_{APK}$:

$$\boldsymbol{M}_{ASK}=\begin{pmatrix} s_{1,1} & \cdots & s_{1,t} \\ \vdots & \ddots & \vdots \\ s_{l,1} & \cdots & s_{l,t} \end{pmatrix} \quad \boldsymbol{M}_{APK}=\begin{pmatrix} s_{1,1}G & \cdots & s_{1,t}G \\ \vdots & \ddots & \vdots \\ s_{l,1}G & \cdots & s_{l,t}G \end{pmatrix}$$

管理中心保留 $\boldsymbol{M}_{BSK}$和 $\boldsymbol{M}_{ASK}$,公开 $\boldsymbol{M}_{BPK}$、$\boldsymbol{M}_{APK}$和系统参数:$params=\langle a,b,p,G,n,F_A,F_B\rangle$,其中 F_A,F_B 为映射函数集.

2.3 用户密钥生成

令 PK_{ID}和 sk_{ID}分别表示用户的公钥和私钥,则 PK_{ID}和 sk_{ID}的计算步骤分别如下:

(1)选取函数集 $F_B=\{f_1^B,f_2^B,\cdots,f_h^B\}$,令 $\mathrm{index}_i^B=f_i^B(\mathrm{ID})$,且有 $\forall\, i\in[1,h]$,$\mathrm{index}_i^B\in[1,m]$.给定用户的身份 ID,计算 $\mathrm{index}_1^B=f_1^B(\mathrm{ID}),\cdots,\mathrm{index}_h^B=f_h^B(\mathrm{ID})$,用 (index_i^B,i)表示基本密钥矩阵中行号为 index_i^B 列号为 i 的元素.

(2)对基本公钥矩阵 $\boldsymbol{M}_{BPK}$中的元素进行选取与组合,得到用户的公钥 PK_{ID}:

$$PK_{\mathrm{ID}}=(r_{\mathrm{index}_1^B,1}+\cdots+r_{\mathrm{index}_h^B,h})G$$

(3)对基本私钥矩阵 $\boldsymbol{M}_{BSK}$中的元素进行选取与组合,得到用户的基本私钥 bsk_{ID}:

$$bsk_{\mathrm{ID}}=(r_{\mathrm{index}_1^B,1}+\cdots+r_{\mathrm{index}_h^B,h})\bmod n$$

(4)选取函数集 $F_A=\{f_1^A,f_2^A,\cdots,f_t^A\}$,令 $\mathrm{index}_i^A=f_i^A(\mathrm{ID})$,且有 $\forall\, i\in[1,t]$,$\mathrm{index}_i^A\in[1,l]$.给定用户的身份 ID,计算 $\mathrm{index}_1^A=f_1^A(\mathrm{ID}),\cdots,\mathrm{index}_t^A=f_t^A(\mathrm{ID})$,用 (index_i^A,i)表示辅助密钥矩阵中行号为 index_i^A 列号为 i 的元素.

(5)对辅助公钥矩阵 $\boldsymbol{M}_{APK}$中的元素进行选取与组合,得到用户的辅助公钥 APK_{ID}:

$$APK_{\mathrm{ID}}=(s_{\mathrm{index}_1^A,1}+\cdots+s_{\mathrm{index}_t^A,t})G$$

(6)对辅助私钥矩阵 $\boldsymbol{M}_{ASK}$的元素进行选取与组合,得到用户的辅助私钥 ask_{ID}:

$$ask_{\mathrm{ID}}=(s_{\mathrm{index}_1^A,1}+\cdots+s_{\mathrm{index}_t^A,t})\bmod n$$

(7)由步骤(3)、步骤(6)计算用户的私钥 $sk_{\mathrm{ID}}=ask_{\mathrm{ID}}^{-1}\cdot bsk_{\mathrm{ID}}$.

上面的步骤(3)、(6)和(7)只由密钥管理中心计算,而用户和密钥管理中心都可以计算步骤(1)、(2)、(4)和(5).

此算法中公钥和私钥之间的关系如下:

$$\begin{aligned} &sk_{\mathrm{ID}}\bullet APK_{\mathrm{ID}} \\ &=ask_{\mathrm{ID}}^{-1}\cdot bsk_{\mathrm{ID}}\bullet APK_{\mathrm{ID}} \\ &=(s_{\mathrm{index}_1^A,1}+\cdots+s_{\mathrm{index}_t^A,t})^{-1}\cdot(r_{\mathrm{index}_1^B,1}+\cdots \\ &+r_{\mathrm{index}_h^B,h})\bullet(s_{\mathrm{index}_1^A,1}+\cdots+s_{\mathrm{index}_t^A,t})G \\ &=(r_{\mathrm{index}_1^B,1}+\cdots+r_{\mathrm{index}_h^B,h})\bullet G \\ &=PK_{\mathrm{ID}} \end{aligned}$$

即 $PK_{\mathrm{ID}}=sk_{\mathrm{ID}}\bullet APK_{\mathrm{ID}}$.

在原算法中,用户的公私钥是通过基本公私钥矩阵中的密钥因子线性组合生成:$PK_{\mathrm{ID}}=ask_{\mathrm{ID}}\bullet G$;而在本算法中,用户的公私钥是通过基本公私钥矩阵和辅助公私钥矩阵中的密钥因子非线性组合生成:$PK_{\mathrm{ID}}=sk_{\mathrm{ID}}\bullet APK_{\mathrm{ID}}$.由于不同用户的 bsk_{ID}、ask_{ID}不同,因此,用户私钥 sk_{ID}间的关系是非线性的.辅助密钥矩阵的规模 $l\times t$ 不受基本密钥矩阵规模 $m\times h$ 的限制,可以根据系统的安全需求来设置.

2.4 加解密及签名算法

(1)数据加解密

用户 A 把明文 M 编码为 Z_n^* 中一个元素 m,随机选取一个正整数 k,计算:

$(x_1,y_1)=k\bullet APK_B$,$(x_2,y_2)=k\bullet PK_B$,$c=mx_2$

产生密文:$C_m=\{(x_1,y_1),c\}$传送给用户 B.

用户 B 收到密文后,计算:

$sk_B(x_1,y_1)=sk_B\cdot k\bullet APK_B=k\bullet PK_B=(x_2,y_2)$,

恢复明文:$m=cx_2^{-1}$

(2)数字签名

用户 A 把消息 m 的签名(r,l)传送给用户 B,其中:$r=u \bmod n$,$l=k^{-1}(m+r\cdot sk_A) \bmod n$,

$(u,v)=k\cdot APK_A$,$k\in[1,n-1]$

用户 B 收到签名(r,l)后,计算:

$w=l^{-1} \bmod n$,$i=wm \bmod n$,$j=wr \bmod n$,

$(x_1,y_1)=i\cdot APK_A+j\cdot PK_A$

对签名进行验证,如果 $x_1 \bmod n=r$,则签名被验证通过,否则拒绝.

3　算法分析

3.1　算法原理分析

在双矩阵组合公钥算法中,加解密和签名验证算法与原 CPK 算法不同,本算法中加解密和签名验证用到的都是辅助公钥 APK_{ID},而不是基点 G,因此,本算法中辅助公钥 APK_{ID}的作用类似于椭圆曲线密码体制中基点 G.可见,本算法类似于根据每个用户的标识,通过辅助公钥矩阵中元素组合的方式为每个用户选取了一个基点.

ECC 密码体制中用户的公私钥间的关系为:$sk \xrightarrow{G} sk\cdot G$.本算法中用户的公私钥间的关系为:$sk \xrightarrow{P} sk\cdot P$,其中 $P=a\cdot G$.

由于基点 G 的阶 n 为一个大素数,由近世代数知识可知,APK_{ID}仍为基点 G 所生成的子群的一个生成元,且以 APK_{ID}为生成元的子群的阶仍然为 n,因此,其安全性与椭圆曲线密码体制的安全性相同.

3.2　抗选择共谋攻击分析

原 CPK 算法中的选择共谋攻击[5]如下:设用户 A 与用户 B 和用户 C 分别是$(j_1,j_2,\cdots,j_{t1})$层不同和$(s_1,s_2,\cdots,s_{t_2})$层不同的,且用户 B 和用户 C 与用户 A 是层互斥不同的,则 3 个用户 A,B,C 共谋,可以得到与用户 A 是$(j_1,j_2,\cdots,j_{t1},s_1,s_2,\cdots,s_{t_2})$层不同的用户的私钥.

双矩阵组合公钥算法中,虽然在 $\boldsymbol{M}_{BSK}$中选取的基本私钥间存在"层不同"和"层互斥不同"的关系,在 $\boldsymbol{M}_{ASK}$中选取的辅助私钥间也存在"层不同"和"层互斥不同"这两种关系,但用户私钥间的关系却是非线性的,因此,用户相互间不能线性表示,本算法可以抵抗选择共谋攻击.

设基本密钥矩阵与辅助密钥矩阵的大小相同,使用相同的映射算法,用户 A、B 和 C 的组合私钥分别为:

$$sk_0=(s_{i_{01},1}+s_{i_{02},2}+\cdots+s_{i_{0n},n})^{-1}(r_{i_{01},1}+r_{i_{02},2}+\cdots+r_{i_{0n},n})$$

$$sk_1=(s_{i_{11},1}+s_{i_{12},2}+\cdots+s_{i_{1n},n})^{-1}(r_{i_{11},1}+r_{i_{12},2}+\cdots+r_{i_{1n},n})$$

$$sk_2=(s_{i_{21},1}+s_{i_{22},2}+\cdots+s_{i_{2n},n})^{-1}(r_{i_{21},1}+r_{i_{22},2}+\cdots+r_{i_{2n},n})$$

其中,用户 A 与用户 B 和用户 C 的基本密钥分别是$(j_1,j_2,\cdots,j_{t1})$层不同和$(s_1,s_2,\cdots,s_{t_2})$层不同的,且用户 B 和用户 C 与用户 A 是层互斥不同的;用户 A 与用户 B 和用户 C 的辅助密钥也分别是$(j_1,j_2,\cdots,j_{t1})$层不同和$(s_1,s_2,\cdots,s_{t_2})$层不同的,且用户 B 和用户 C 与用户 A 是层互斥不同的.

将用户 A、B、C 的私钥变成如下形式:

$$(s_{i_{01},1}+s_{i_{02},2}+\cdots+s_{i_{0n},n})sk_0=r_{i_{01},1}+r_{i_{02},2}+\cdots+r_{i_{0n},n} \quad (1)$$

$$(s_{i_{11},1}+s_{i_{12},2}+\cdots+s_{i_{1n},n})sk_1=r_{i_{11},1}+r_{i_{12},2}+\cdots+r_{i_{1n},n} \quad (2)$$

$$(s_{i_{21},1}+s_{i_{22},2}+\cdots+s_{i_{2n},n})sk_2=r_{i_{21},1}+r_{i_{22},2}+\cdots+r_{i_{2n},n} \quad (3)$$

于是由式(2)－式(1)得到:

$$(s_{i_{11},1}+s_{i_{12},2}+\cdots+s_{i_{1n},n})sk_1-(s_{i_{01},1}+s_{i_{02},2}+\cdots+s_{i_{0n},n})sk_0$$
$$=(r_{i_{1j_1},j_1}-r_{i_{0j_1},j_1})+(r_{i_{1j_2},j_2}-r_{i_{0j_2},j_2})+\cdots+(r_{i_{1j_{t_1}},j_{t_1}}-r_{i_{0j_{t_1}},j_{t_1}})$$

由式(3)－式(1)得到:

$$(s_{i_{21},1}+s_{i_{22},2}+\cdots+s_{i_{2n},n})sk_2-(s_{i_{01},1}+s_{i_{02},2}+\cdots+s_{i_{0n},n})sk_0$$
$$=(r_{i_{2s_1},s_1}-r_{i_{0s_1},s_1})+(r_{i_{2s_2},s_2}-r_{i_{0s_2},s_2})+\cdots+(r_{i_{1s_{t_2}},s_{t2}}-r_{i_{0s_{t_2}},s_{t2}})$$

由互斥性得到:

式(1)+[式(2)－式(1)]+[式(3)－式(1)]:

$$(s_{i_{11},1}+s_{i_{12},2}+\cdots+s_{i_{1n},n})sk_1+(s_{i_{21},1}+s_{i_{22},2}+\cdots+s_{i_{2n},n})sk_2$$
$$-(s_{i_{01},1}+s_{i_{02},2}+\cdots+s_{i_{0n},n})sk_0$$
$$=\sum_{p\notin\Omega}r_{i_{0p},p}+r_{i_{1j_1},j_1}+\cdots+r_{i_{1j_{t_1}},j_{t_1}}+r_{i_{2s_1},s_1}+\cdots+r_{i_{2s_{t_2}},s_{t2}}$$

上式等号右侧为受到共谋用户的基本私钥,但是显然等号左侧:

$$(s_{i_{11},1}+s_{i_{12},2}+\cdots+s_{i_{1n},n})sk_1+(s_{i_{21},1}+s_{i_{22},2}+\cdots+s_{i_{2n},n})sk_2$$
$$-(s_{i_{01},1}+s_{i_{02},2}+\cdots+s_{i_{0n},n})sk_0$$
$$\neq(\sum_{p\notin\Omega}s_{i_{0p},p}+s_{i_{1j_1},j_1}+\cdots+s_{i_{1j_{t_1}},j_{t_1}}+s_{i_{2s_1},s_1}+\cdots+s_{i_{2s_{t_2}},s_{t2}})(sk_1+sk_2-sk_0)$$

其中:$\sum_{p\notin\Omega}s_{i_{0p},p}+s_{i_{1j_1},j_1}+\cdots+s_{i_{1j_{t_1}},j_{t_1}}+s_{i_{2s_1},s_1}+\cdots+s_{i_{2s_{t_2}},s_{t2}}$为受到共谋用户的辅助私钥.

可见,3 个用户 A,B,C 共谋,得不到与用户 A 是$(j_1,j_2,\cdots,j_{t1},s_1,s_2,\cdots,s_{t_2})$层不同的用户的私钥.用户相互间不能线性表示,本算法可以抵抗选择共谋攻击.

3.3　抗随机共谋攻击分析

双矩阵组合公钥算法中,用户的公钥通过下式计算:　$PK_{\mathrm{ID}}=(r_{\mathrm{index}_1^B,1}+\cdots+r_{\mathrm{index}_h^B,h})$

虽然用户的公钥间仍然存在线性关系,但公钥和私钥间的关系却发生了变化:$PK_{\mathrm{ID}}=sk_{\mathrm{ID}}\cdot APK_{\mathrm{ID}}$.

由 3.2 可知用户相互间不能线性表示,因此,即使存在 $PK_3-PK_2=\Delta PK_{21}$的情况下,私钥间不存在 $sk_3=2sk_2-sk_1$ 或 $sk_3=2sk_1-sk_2$ 的关系,可见,本算法可以抵抗随机共谋攻击.

3.4　抗线性分析共谋攻击分析

在双矩阵组合公钥算法中用户的私钥 $sk_{\mathrm{ID}}=$

$(ask_{ID}^{-1} \cdot bsk_{ID}) \bmod n$,可以变化成如下形式:

$$ask_{ID} \cdot sk_{ID} - bsk_{ID} = 0$$

即

$$(s_{index_1^A,1} + \cdots + s_{index_t^A,t}) \cdot sk_{ID} - (r_{index_1^B,1} + \cdots + r_{index_h^B,h}) = 0$$

可见,非线性方程可以转化为线性方程,也就是说求解非线性方程组可以转化为求解线性方程组,因此,本算法仍然存在线性分析共谋攻击.

如果基本密钥矩阵和辅助密钥矩阵的规模都为 $m \times h$,攻击者需要构造出 $2[(m-1)h+1]$个线性无关的方程,才能解出与基本私钥矩阵和辅助私钥矩阵等价的密钥因子矩阵,因此本算法可以抵抗 $2(m-1)h+1$ 个用户的线性分析共谋攻击.

在原 CPK 算法中,如果基本密钥矩阵的规模为 $m \times 2h$,可以抵抗 $2(m-1)h$ 个用户的线性分析共谋攻击;如果基本密钥矩阵的规模为 $2m \times h$,可以抵抗$(2m-1) \times h$ 个用户的线性分析共谋攻击.

可见,在存储量相同时,二者抵抗线性分析共谋攻击的能力基本相同.但本算法中不存在选择共谋攻击和随机共谋攻击,因此,在存储量相同的情况下,本算法的安全性比原算法的安全性好.

3.5 矩阵规模分析

设系统中实际用户数为 N,m、h 的选取与系统中实际用户数 N 有关,要求 $m^h \geqslant N$,如果 $m^h < N$ 就会出现不同用户的基本私钥相同,公钥 PK_{ID}相同的情况;在用户规模一定时选取的 m、h 应使存储量 mh 最小.

l、t 的选取与系统中实际用户数 N 有关,要求 $l^t \geqslant N$,如果 $l^t < N$ 就会出现不同用户的辅助密钥相同的情况;l 和 t 的选取还与系统安全性有关,在双矩阵 CPK 算法中,用户要进行共谋攻击,需要求解包含$(m-1)h+(l-1)t+2$ 个未知数的线性方程组,mh 一定,lt 越大抗线性共谋攻击能力越强,在存储量允许的情况下 lt 应尽可能的大.

密钥辅助矩阵的引入使得双矩阵 CPK 算法具有了抵抗选择共谋攻击和随机共谋攻击的能力.m 和 h 的选取和用户规模有关,l 和 t 的选取不仅和用户规模有关,还和系统的安全性有关,l 和 t 的大小可变,系统的安全性可控.

4 总结

本算法通过引入辅助私钥消除了用户私钥间的线性关系,解决了已有的选择共谋攻击和随机共谋攻击问题,但本算法中求解非线性方程组可以转化为求解线性方程组,因此仍然存在线性分析共谋攻击问题,如何提高抵抗线性共谋攻击的能力,设计完全无共谋攻击的组合公钥算法,值得进一步研究.

参考文献

[1] 汪宇光.CPK 认证体制的技术特点及应用[J].电子科学技术评论,2005,(2):5-10.

[2] 管海明.CPK 与 PKI 的性能分析[J].计算机安全,2003,(8):17-8.

[3] 周加法,马涛,等. PKI、CPK、IBC 性能浅析[J].信息工程大学学报,2005,6(3):26-31.
Zhou Jafa, Ma Tao, et al. Comparison and Analysis of PKI、CPK and IBC[J]. Journal of Information Engineering University,2005,6(3):26-31.(in Chinese)

[4] 陈华平,关志.关于 CPK 若干问题的说明[J].信息安全与通信保密,2007,(9):47-49.

[5] 赵美玲,张少武.基于 ECC 的组合公钥技术的安全性分析[J].计算机工程,2008,34(1):156-157.

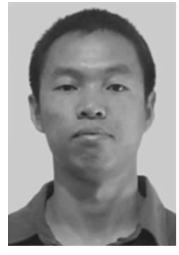
[6] 南湘浩.CPK 标识认证[M].北京:国防工业出版社,2006.

[7] 南湘浩,陈华平.组合公钥(CPK)体制标准[J].国家信息安全测评认证,2008,(4):12-14.

[8] 陈文华,肖亦伟.基于 CPK 的 IBE 方案[J].软件导刊,2008,7(2):88-89.
Chen Wenhua, Xiao Yiwei. A provably secure identity-based encryption scheme based on CPK[J]. Software Guide,2008,7(2):88-89.(in Chinese)

[9] 徐鹏,崔国华,等.非双线性映射下一种实用的和可证明安全的 IBE 方案[J].计算机研究与发展,2008,45(10):1687-1695.

作者简介



邵春雨 男,1984 年生于吉林.武汉军械士官学校教员.主要研究方向为密钥管理.
E-mail:saocunu@163.com.

苏锦海 男,1963 年生于河北.信息工程大学教授,硕士生导师.主要研究方向为信息安全.

魏有国 男,1968 年出生于湖北.武汉军械士官学校教员.研究方向 O 装备保障.

周晶晶 女,1977 年出生于江西.武汉军械士官学校教员.研究方向为系统仿真.