前向安全的多重数字签名方案

王晓明[1)] 符方伟[2)] 张 震[1)]

[1)](暨南大学计算机系 广州 510632)

[2)](南开大学数学科学学院 天津 300071)

摘 要 首次将前向安全的概念引入到多重数字签名体制,提出了一个前向安全的多重数字签名方案.方案能实现即使所有签名人的签名密钥被泄露,以前所产生的多重数字签名依然有效.另外,方案是基于 Schnorr 签名体制构造的,引入了预计算,对多重数字签名的生成速度有所改进.

关键词 密码学;数字签名;数字签名;前向安全

中图法分类号 TP309

A Forward Secure Multisignature Scheme

WANG Xiao-Ming[1)] FU Fang-Wei[2)] ZHANG Zhen[1)]

[1)](*Department of Computer, Jinan University, Guangzhou* 510632)

[2)](*School of Mathematics Science, Nankai University, Tianjin* 300071)

Abstract A forward secure multisignature scheme is proposed combining the concept of forward security with multisignature. This means that an adversary cannot forge multisignature pertaining to the past even if has gotten the current all signers' keys, that is, previous generated multisignature remains valid. The forward security of the scheme relies on the strong-RSA assumption. Furthermore, the scheme has the shorter time of generating signature since the scheme is constructed based on Schnorr signature.

Keywords cryptography; digital signature; multisignature; forward security

1 引 言

目前,人们已提出了若干多重数字签名方案[1~11],然而,当签名人的签名密钥被泄露后,这些方案都不能提供任何保护,也就是说,一旦签名密钥被泄露,用此签名密钥所产生的多重数字签名将变成无效.因为如果一个攻击者获得签名密钥,他就可以伪造签名,人们无法区分真实的签名和伪造的签名.如何减少由于密钥泄露所带来的对系统安全的影响,一直是人们十分关注的研究课题.1997 年,Anderson 首次提出了前向安全的概念[12].前向安全就是把整个有效时间分成若干个周期,在每个周期内使用不同的签名密钥产生签名,而验证签名的公钥在整个有效时间内都保持不变.即使当前周期的签名密钥被泄露,也并不影响此周期前签名的有效性.从而大大地减少了由于签名密钥泄露而对系统带来的影响.

已提出的多重数字签名方案都不具有前向安全的特性.本文首次将前向安全的概念引入多重数字签名体制,提出了一个前向安全的多重数字签名方案.本方案能实现即使所有签名人的签名密钥被泄露,以前所产生的多重数字签名依然有效.另外,方

收稿日期:2003-03-24;修改稿收到日期:2004-05-10.本课题得到国家自然科学基金(60172060)、广州省自然科学基金(博士启动基金)和暨南大学自然科学基金资助.**王晓明**,女,1960 年生,博士,教授,主要研究方向为信息安全、密码学、计算机网络安全等.E-mail:wxmsq@eyou.com;twxm@jnu.edu.cn.**符方伟**,男,1963 年生,教授,博士生导师,主要研究方向为信息论、密码学、编码理论、数字通信原理等.**张 震**,男,1975 年生,助教,研究方向为信息安全、计算机网络安全等.

案是基于 Schnorr 签名体制[13]构造的,引入了预计算,对多重数字签名的生成速度有所改进.

2 前向安全签名的概念

设签名密钥为 σ_0,公钥为 y.将 y 的有效时间分为若干时间段,如 $1,2,\cdots,T$.在每个时间段内签名人使用不同的签名密钥 $\sigma_i(i=1,2,\cdots,T)$,即第 1 时间段内使用 σ_1,第 2 时间段内使用 σ_2,第 T 时间段内使用 σ_T.而验证签名的公钥 y 在整个有效时间内不变.其中不同的时间段的签名密钥是单向更新的,即由 i 时间段的签名密钥 σ_i 求不出第 $i-1$ 时间段的签名密钥 σ_{i-1},而且签名人在第 i 时间段开始,并获得新的签名密钥 σ_i 后,就从他的机器中删除 σ_{i-1}.这样,即使攻击者在第 i 时间段内入侵用户的机器,他也只能得到 σ_i,而得不到以前的签名密钥 $\sigma_{i-1},\sigma_{i-2},\cdots,\sigma_0$.

定义 1[13]. 如存在一个单向签名密钥更新算法 $KeyUd$,使得签名人可以在第 i 时间段将签名密钥由 σ_{i-1} 更新为 $\sigma_i=KeyUd(\sigma_{i-1})$,并在不同的时间段内使用不同的签名密钥 σ_i 生成签名 $Sign(\sigma_i,m)$(m 是信息),而任何签名验证人都可以用一个不变的公钥 y 及时间段的编号 i 进行验证,即 $Sign(\sigma_i,m)$ 满足等式 $Ver[y,i,Sign(\sigma_i,m),m]=\mathrm{True}$,则这个数字签名为一个前向安全数字签名.

3 前向安全的多重数字签名方案

3.1 初始化阶段

签名中心(SC)首先选择 $n=p_1p_2=(2qp_1'+1)\cdot(2qp_2'+1)$ 和一个阶为 q 的 $g\in QR_n$(即 $g^q=1 \bmod n$),且 $p_1\equiv p_2\equiv 3 \bmod 4$,其中 p_1,p_2,p_1',p_2',q 都为安全的大素数,QR_n 为模 n 的平方剩余集合.SC 选择一对整数 (e,d) 满足 $\gcd(e,\phi(n))=1$,$ed=1 \bmod \phi(n)$,$\phi(n)=(p_1-1)(p_2-1)$.e 为 SC 的公钥,d 为 SC 的私钥.SC 选择一个安全的单向 Hash 函数 h 和时间周期 $1,2,\cdots,T$.然后 SC 为每个签名人 u_i(设签名人的人数为 l)选择一个随机数 $\sigma_{i0}(0<\sigma_{i0}<q,\sigma_{i0}\neq\sigma_{j0},i\neq j)$,并秘密送 σ_{i0} 给签名人 $u_i(i=1,2,\cdots,l)$.最后,SC 计算 $Y_i=(\sigma_{i0}^{-2^{2^{T+1}}})^e \bmod n,i=1,2,\cdots,l$.公布 $PK=\{n,q,g,h,T,Y_i,y_i,i=1,2,\cdots,l\}$,其中 $y_i=g^{k_i} \bmod n$ 为每个签名人的公钥(CA 认证过),k_i 为每个签名人的私钥.

3.2 密钥的更新

在每个周期的开始,每个签名人 u_i 根据前一周期的密钥计算出此周期的密钥 $\sigma_{ij}=\sigma_{ij-1}^2 \bmod n$($\sigma_{ij-1}$ 为第 $j-1$ 周期的密钥,σ_{ij} 为第 j 周期的密钥,$j=1,2,\cdots,T$),然后签名人更新周期序号($j-1$ 被更新为 j),删除前一个周期的密钥(σ_{ij-1}).

3.3 前向安全的多重数字签名的产生

3.3.1 前向安全的有序多重数字签名的产生

在周期 j,设有 l 个签名人 $u_1,u_2,\cdots,u_l$ 签署同一份信息 m,签名顺序为 $u_1,u_2,\cdots,u_l$.设 $\bar{t}$ 为 SC 发送签名的时间标志,要求 u_i 在给定的时间 Δt_i 内签名,这主要用来防止签名重播攻击.SC 广播($\bar{t},m,\Delta t_i,i=1,2,\cdots,l$).

为了完成对信息 m 的签名,签名人 $u_1,u_2,\cdots,u_l$ 执行以下步骤:

①u_1 在 t_1 时间收到信息 m 和 $\bar{t}$ 后,首先验证 $t_1-\bar{t}>\Delta t_1$,如 $t_1-\bar{t}>\Delta t_1$,u_1 将向 SC 发送一个超时信息,表示对 m 的签名失败.否则选择随机数 $0<r_{1j},w_{1j}<q$,计算 $R_{1j}=(g^{r_{1j}})^{2^{2^{T+1-j}}} \bmod n$,$Z_{1j}=\sigma_{1j}g^{w_{1j}} \bmod n$,送 (R_{1j},Z_{1j}) 给下一个签名人 u_2.

②每一位签名人 $u_i(i\geq 2)$ 在 t_i 时间收到 (R_{i-1j},Z_{i-1j}) 后,首先验证 $t_i-\bar{t}>\Delta t_i$,如 $t_i-\bar{t}>\Delta t_i$,请求 u_{i-1} 重发签名消息.否则选择随机数 $0<r_{ij},w_{ij}<q$,计算

$$R_{ij}=R_{i-1j}(g^{r_{ij}})^{2^{2^{T+1-j}}} \bmod n \tag{1}$$

$$Z_{ij}=Z_{i-1j}\sigma_{ij}g^{w_{ij}} \bmod n \tag{2}$$

送 (R_{ij},Z_{ij}) 给下一个签名人 $u_{i+1}(i=2,\cdots,l,u_{l+1}=u_1)$.

③u_1 在 t_1' 时间收到 u_l 送来的 (R_{lj},Z_{lj}) 后,首先验证 $t_1'-(\bar{t}+\Delta t_l)>\Delta t_1$,如 $t_1'-(\bar{t}+\Delta t_l)>\Delta t_1$,请求 u_l 重发签名消息.否则计算

$$u=h(j\|m\|R_{lj}\|Z_{lj}\|\bar{t}) \tag{3}$$

$$s_{1j}=r_{1j}-(w_{1j}e+k_1)u \bmod q \tag{4}$$

送 (R_{lj},Z_{lj},s_{1j}) 给下一个签名人 u_2.

④每一位签名人 $u_i(i\geq 2)$ 在 t_i' 时间收到 (R_{lj},Z_{lj},s_{i-1j}) 后,首先验证 $t_i'-(\bar{t}+\Delta t_l)>\Delta t_i$,如 $t_i'-(\bar{t}+\Delta t_l)>\Delta t_i$,请求 u_{i-1} 重发签名消息.否则计算 $u=h(j\|m\|R_{lj}\|Z_{lj}\|\bar{t})$,验证

$$R_{i-1j}=(g^{2^{2^{T+1-j}}})^{s_{i-1j}}[(Z_{i-1j}^e\prod_{v=1}^{i-1}y_v)^{2^{2^{T+1-j}}}\prod_{v=1}^{i-1}Y_v]^u \bmod n \tag{5}$$

如式(5)成立,计算

$$s_{ij}=s_{i-1j}+r_{ij}-(w_{ij}e+k_i)u \bmod q \tag{6}$$

送 (R_{lj},Z_{lj},s_{ij}) 给下一个签名人 $u_{i+1}(i=2,\cdots,l-1)$,否则要求 u_{i-1} 重发签名消息.

⑤u_l 送 (R_{lj},Z_{lj},s_{lj}) 给 SC,SC 验证 $t'-(\bar{t}+\Delta t_l)>\Delta t_c$,其中 Δt_c 为 u_l 与 SC 之间允许的传输时

间,t'为 SC 收到(R_{lj},Z_{lj},s_{lj})的时间. 如 $t'-(\tilde{t}+\Delta t_l)>\Delta t_c$,请求 u_l 重发签名消息. 否则计算 $u=h(j\|m\|R_{lj}\|Z_{lj}\|\tilde{t})$,验证

$$R_{lj}=(g^{2^{T+1-j}})^{s_{lj}}\left[(Z_{lj}^{e}\prod_{v=1}^{l}y_v)^{2^{T+1-j}}\prod_{v=1}^{l}Y_v\right]^{u} \bmod n \tag{7}$$

如式(7)成立,令 $Z=Z_{lj}$,$s=s_{lj}$,则前向安全的有序多重数字签名为$[j,(m,s,Z,u,\tilde{t})]$. 否则 SC 要求 u_l 重发签名消息.

注. 在每个周期开始时,签名人可以预先计算 $g^{2^{T+1-j}}$,在每次签名前,签名人可以预先计算 $R_{ij}=(g^{2^{T+1-j}})^{r_{ij}} \bmod n$,$Z_{ij}=\sigma_{ij}g^{w_{ij}} \bmod n$.

3.3.2　前向安全的广播多重数字签名的产生

在周期 j,设有 l 个签名人 $u_1,u_2,\cdots,u_l$ 签署同一份信息 m. 设 $\tilde{t}$ 为 SC 发送签名的时间标志,要求签名人 u_i 在给定的时间 Δt 内签名. SC 广播$(\tilde{t},m,\Delta t)$.

为了完成对信息 m 的签名,签名人 $u_1,u_2,\cdots,u_l$ 执行以下步骤:

①每一位签名人 u_i 选择随机数 $0<r_{ij},w_{ij}<q$,计算 $R_{ij}=(g^{r_{ij}})^{2^{T+1-j}} \bmod n$,$Z_{ij}=\sigma_{ij}g^{w_{ij}} \bmod n$,广播$(R_{ij},Z_{ij})$.

②每一位签名人 u_i 收到$(R_{ij},Z_{ij},i=1,2,\cdots,i-1,i+1,\cdots,l))$后,计算

$$R_j=\prod_{i=1}^{l}R_{ij} \bmod n,\ Z_j=\prod_{i=1}^{l}Z_{ij} \bmod n,$$

$u=h(j\|m\|R_j\|Z_j\|\tilde{t})$,$s_{ij}=r_{ij}-(w_{ij}e+k_i)u \bmod q$ 送 s_{ij} 给 SC.

③SC 首先验证签名消息是否在 $t=\tilde{t}+\Delta t$ 时间之前,如有的消息在 t 时间之后到达,SC 要求签名人重发签名消息;如所有签名消息都在 t 时间之前到达,SC 计算

$$R_j=\prod_{i=1}^{l}R_{ij} \bmod n,\ Z_j=\prod_{i=1}^{l}Z_{ij} \bmod n,$$
$$u=h(j\|m\|R_j\|Z_j\|\tilde{t}),$$

验证

$$R_{ij}=(g^{2^{T+1-j}})^{s_{ij}}\left[(Z_{ij}^{e}y_i)^{2^{T+1-j}}Y_i\right]^{u} \bmod n,\quad i=1,2,\cdots,l \tag{8}$$

如式(8)成立,计算 $s_j=\sum_{i=1}^{l}s_{ij} \bmod q$. 令 $Z=Z_j$,$s=s_j$,则前向安全的广播多重数字签名为$[j,(m,s,Z,u,\tilde{t})]$. 如式(8)不成立,u_i 签名无效,要求 u_i 重发签名消息.

3.4　前向安全的多重数字签名的验证

签名验证人收到$[j,(m,s,Z,u,\tilde{t})]$后,计算

$$y=\prod_{i=1}^{l}y_i \bmod n,\ Y=\prod_{i=1}^{l}Y_i \bmod n,$$
$$R'=(g^{2^{T+1-j}})^{s}\left[(Z^{e}y)^{2^{T+1-j}}Y\right]^{u} \bmod n \tag{9}$$

验证

$$u=h(j\|m\|R'\|Z\|\tilde{t}) \tag{10}$$

如式(10)成立,则多重数字签名有效,否则多重数字签名无效.

3.5　安全性的分析

(1)$[j,(m,s,Z,u,\tilde{t})]$是有效前向安全的多重数字签名.

为了证明$[j,(m,s,Z,u,\tilde{t})]$是有效前向安全的多重数字签名,则需要证明式(10)成立.

根据式(1),(2),(4),(6)和式(7)得

$$R'=(g^{2^{T+1-j}})^{\sum_{i=1}^{l}r_{ij}-(w_{ij}e+k_i)u}\left\{\left[\prod_{i=1}^{l}(\sigma_{ij}g^{w_{ij}})^{e}\prod_{i=1}^{l}y_i\right]^{2^{T+1-j}}\prod_{i=1}^{l}Y_i\right\}^{u}$$
$$=\prod_{i=1}^{l}\left[(g^{r_{ij}}g^{-w_{ij}eu}y_i^{-u})^{2^{T+1-j}}(\sigma_{ij}^{eu}g^{w_{ij}eu}y_i^{u})^{2^{T+1-j}}(\sigma_{i0}^{-2^{T+1}})^{eu}\right]$$
$$=\prod_{i=1}^{l}(g^{r_{ij}})^{2^{T+1-j}}=R_{lj} \bmod n$$

根据式(3)和上式得

$$u=h(j\|m\|R_{lj}\|Z_{lj}\|\tilde{t})=h(j\|m\|R'\|Z\|\tilde{t}).$$

则$[j,(m,s,Z,u,\tilde{t})]$是有效的前向安全的多重数字签名.

(2)方案具有前向安全的特性

本方案的前向安全是基于强 RSA 假定[14].

强 RSA 假定[14]. 已知 n 和 $\alpha\in Z_n^*$,n 为两个大素数的乘积,则找出一个 $\beta\in Z_n^*$,且满足 $\beta^r=\alpha \bmod n$ $(r>1)$是一个非常困难的问题.

如果攻击者已获得所有签名人的第 j 周期的密钥 $\sigma_{ij}(i=1,2,\cdots,l)$,企图通过 $\sigma_{ij}=\sigma_{i-1j}^{2} \bmod n$ 求 σ_{i-1j},这是一个强 RSA 假定的问题,所以攻击者无法通过 σ_{ij} 获得 $k<j$ 周期的密钥 $\sigma_{ik}(k<l)$.

设伪造者对同一个 R_{lj} 给出了两个签名(j,s,Z,u)和(j,s',Z,u'). 如这两个签名是有效的,则

$$(g^{2^{T+1-j}})^{s}\left[(Z^{e}y)^{2^{T+1-j}}Y\right]^{u}=(g^{2^{T+1-j}})^{s'}\left[(Z^{e}y)^{2^{T+1-j}}Y\right]^{u'} \bmod n.$$

令 $\tilde{s}=s-s'$,$\tilde{u}=u'-u$,上式可以写为

$$(g^{\tilde{s}})^{2^{T+1-j}}=\left[(Z^{e}y)^{2^{T+1-j}}Y\right]^{\tilde{u}} \bmod n \tag{11}$$

如 $\tilde{u}$ 除尽 $\tilde{s}$,那么式(11)就可以写为

$$(g^{\tilde{s}/\tilde{u}}/(Z^{e}y))^{2^{T+1-j}}=Y \bmod n,$$

选择一个随机数 $\alpha\in Z_n^*$,令 $Y=\alpha^{2^{T+1-j}} \bmod n$,则有 $(g^{\tilde{s}/\tilde{u}}/(Z^{e}y))^{2^{T+1-j}}=\alpha^{2^{T+1-j}} \bmod n$. 因为 n 是 Blum 整数,所以

$$(g^{\tilde{s}/\tilde{u}}/(Z^{e}y))^{2}=\alpha^{2} \bmod n.$$

根据上式可以计算出 α^2 的一个平方根，而 α 是一个随机元素 $\in Z_n^*$，这与强 RSA 假定矛盾，所以假设错误.

如 $\tilde{u}$ 除不尽 $\tilde{s}$，那么选随机数 σ_0，$\alpha \in Z_n^*$，令 $g=\alpha^2$，$Y=1/\sigma_0^{2^{T+1}}$，则式(11)可以写为

$$(g^{\tilde{s}})^{2^{T+1-j}} = [(Z^e y)^{2^{T+1-j}}/\sigma_0^{2^{T+1}}]^{\tilde{u}} \bmod n,$$

即 $(g^{\tilde{s}})^{2^{T+1-j}} = (Z^e y/\sigma_j)^{\tilde{u}2^{T+1-j}} \bmod n$，因为 n 是 Blum 整数，所以 $g^{\tilde{s}} = (Z^e y/\sigma_j)^{\tilde{u}} \bmod n$. 又因为存在 $a,b \in Z_n^*$，使得 $\gcd(\tilde{s},\tilde{u}) = a\tilde{u} + b\tilde{s}$. 令 $c = g^a (Z^e y/\sigma_j)^b$，$r = \tilde{u}/\gcd(\tilde{u},\tilde{s})$，所以有

$$g^{a\tilde{u}} (Z^e y/\sigma_j)^{\tilde{u}b} = g^{b\tilde{s}} g^{a\tilde{u}} = g^{\gcd(\tilde{s},\tilde{u})} \bmod n,$$

$$c^{\tilde{u}} = g^{\gcd(\tilde{s},\tilde{u})} \bmod n.$$

所以 $g = c^r \bmod n$，$r>1$，即

$$\alpha^2 = c^r \bmod n,$$

当 r 为偶数时，从上式可以获得 α^2 的一个平方根；当 r 为奇数时，从上式可以获得 α 的一个根，阶为 r. 这与强 RSA 假定矛盾，所以假设错误.

综上所述，本方案具有前向安全的特性.

(3)方案能抵抗伪造攻击

假定知道 $(j,m,R_{lj},Z,\tilde{t},y_i,Y_i,i=1,2,\cdots,l)$，攻击者企图通过验证式(见式(9)，(10))

$$R_{lj} = R' = (g^{2^{T+1-j}})^s [(Z^e \prod_{i=1}^{l} y_i)^{2^{T+1-j}} \prod_{i=1}^{l} Y_i]^{h(j\|m\|R_{lj}\|Z\|\tilde{t})} \bmod n$$

求 s，这相当于求解离散对数的问题. 若假定 $(j,m,s,Z,\tilde{t},y_i,Y_i,i=1,2,\cdots,l)$，通过上式求 R_{lj}，这相当于求解离散对数的问题和单向 Hash 函数求反的问题. 若假定 $(j,m,R_{lj},s,\tilde{t},y_i,i=1,2,\cdots,l)$，通过上式求 Z，这相当于大数分解和单向 Hash 函数求反的问题.

如果攻击者企图伪造部分多重数字签名，使得全体多重数字签名满足验证式，那么本方案要对部分签名验证，所以伪造的部分签名无法通过验证式(5). 如攻击者企图在假定某些参数的情况下，通过式(5)求解某些参数，以达到伪造出有效的部分签名的目的，那么用与上面一样的方法可以分析，这是不可行的. 所以攻击者无法伪造出有效的部分签名.

综上所述，本方案能抵抗伪造攻击.

(4)方案能抵抗内部攻击

在本方案中，若有不诚实的签名人 u_{i-1} 给接受者 u_i 或 SC 提供伪造的签名，u_i 或 SC 可以通过验证式(5)或验证式(8)发现 u_{i-1} 的欺诈行为，并要求 u_{i-1} 重新发送真实的签名. 如果不诚实的签名人 u_{i-1} 用提供伪签名的方式延误时间，阻止对消息 m 的签名. SC 可以根据签名接受人 u_i 提供的失败信息查找原因及时处理.

(5)方案能抵抗重播攻击

因在本方案中引入了时间标志，每次都要对时间进行验证，所以能抵抗重播攻击.

4 结束语

本文构造了两种不同类型的前向安全的多重数字签名方案：一种是有序，另一种是广播. 两种方案均基于 Schnorr 体制构造. 与已往的多重数字签名方案相比，增加了前向安全特性，引入了预计算，在签名的生成速度和长度上有了一些改进. 同时，也对方案安全性进行了分析，得到本方案能抵抗内部等一切攻击，是一个安全、简单、实用、具有前向安全的多重数字签名方案的结论.

参 考 文 献

1 Kamoto T.. A digital multisignature scheme using bijective public-key cryptosystem. ACM Transactions on Computer Systems, 1988, 6(8): 432～441

2 Boldyreva A.. Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme. In: Proceedings of the Public Key Cryptography'03, Florida, USA, 2003, 31～46

3 Ohta K., Okamoto T.. Multi-signature scheme secure against active insider attacks. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 1999, E82-A(1): 21～31

4 Lin C. Y., Wu T. C., Hwang J. J.. ID-based structured multi-signature schemes. In: de Decker B ed.. Advances in Network and Distributed Systems Security. Boston: Kluwer Academic Publishers, 2001, 45～59

5 He W. H. Weaknesses in some multisignature schemes for specified group of verifiers. Information Processing Letters, 2002, 83(2): 95～99

6 Micali S., Ohta K., Reyzin L.. Accountable-subgroup multi-signature: Extended abstract. In: Proceedings of the ACM Conference on Computer and Communication Security 2001 (CCS 2001). Philadelphia, PA, USA, 2001, 245～254

7 Harn L.. Group—oriented (t,n) threshold digital signature scheme and digital multisignature. IEEE Proceedings of Computer Digital Technology, 1994, 141(5): 307～313

8 Hwang S. J., Chen C. Y., Chang C. C.. An encryption /multisignature scheme with specified receiving groups. Computer Systems Science and Engineering, 1998, 13(2): 109～112

9 Doi H., Mambo M., Okamoto E.. On the security of the RSA-based multisignature scheme for various group structures. In: Proceedings of the 5th Australasian Conference-ACISP2000, Canberra, Australasian, 2000, 352～367

10 Popescu C.. Blind signature and blind multisignature schemes using elliptic curves. Studia Universitatis, "Babes-Bolyai", Informatica, 1999, XLIII(2): 43～49

11 Li Zi-Chen, Yang Yi-Xian. ElGamal's multisignature scheme. Journal of Beijing University of Posts and Telecommunications, 1999, 22(2): 30～34(in Chinese)
(李子臣,扬义先. ElGamal多重数字签名方案. 北京邮电大学学报,1999, 22(2): 30～34)

12 Anderson R.. Invited lecture. In: Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, 1997, 1～7

13 Schneier B.. Applied Cryptography—Protocols, Algorithms, and Source Code in C. New York: John Wiley & Sons, 1996

14 Kozlov A., Reyzin L.. Forward-secure signature with fast key update. In: Proceedings of Security in Communication Networks, Amalf, Italy, 2002, 241～256

WANG Xiao-Ming, born in 1960, Ph. D., professor. Her research interests include information security, cryptography, security protocols in Internet etc.

FU Fang-Wei, born in 1963, professor, Ph. D. supervisor. His research interests include information theory, cryptography, coding theory, discrete mathematics, and digital communication theory etc.

ZHANG Zhen, born in 1975, assistant. His research interests include information security, security protocols in Internet etc.

Background

This project "Research on Special Digital Signatures" aims to put forward new special digital signature algorithms and schemes, and find out new applications of the special digital signatures in actuality. Our research group has published many papers in international and internal Journals and Conference about this project. This work designs a forward secure multisignature scheme combining the concept of forward security with multisignature.