可废除并发签名机制

李保红，牛慧芳，赵银亮
（西安交通大学计算机系科学与技术系，710049，西安）

摘要：针对数字签名的公平交换问题，提出了可废除并发签名机制.在签名阶段，首先由签名者选取一种特殊的keystone信息，再通过单向函数计算出keystone印记，然后使用签名者的私钥对印记进行指数运算，产生出签名者的公钥密文.在进行签名交换之后，利用公布的keystone信息再次计算出keystone印记，并对每个签名者的公钥进行指数运算，然后通过与密文的比较确定签名者身份，从而废除了并发签名的模糊性.与传统并发签名方式相比，所提机制可消除各种攻击的可能性，特别是在产生可废除并发签名时，交换双方只需要产生一个keystone，从而简化了签名交换协议.在一个实现中同时证实，基于随机预言模型在确定性Diffie-Hellman假设和离散对数假设下所提机制是安全的.

关键词：并发签名；签名交换；随机预言模型
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2009)12-0045-05

Revocable Concurrent Signatures

LI Baohong, NIU Huifang, ZHAO Yinliang
(Department of Computer Science and Technology, Xi′an Jiaotong University, Xi′an 710049, China)

Abstract: Aiming at the problem of fair exchange of digital signatures, a scheme of revocable concurrent signatures is proposed. In the step of signing, the signer chooses a piece of special information named keystone. The one-way function is then used to compute the keystone footprint, and then the encryption of the signer's public key is obtained by raising the keystone footprint to the power of his secret key. The keystone footprints are computed once more from the released keystones after the exchange of signatures, and each signer's public key is raised to the power of the keystone footprint. Then the identities of signers are recognized by comparing the results with the encryptions of the public keys produced in the step of signing, and the ambiguity of signatures can be revoked. Compared with traditional concurrent signatures schemes, the proposed scheme can avoid various attacks. Moreover, when a pair of revocable concurrent signatures is produced, only one keystone is required so that exchange protocols are simplified. It has been verified in a concrete construction that the proposed scheme is secure in the random oracle model under the decisional Diffie-Hellman assumption and the discrete logarithms assumption.

Keywords: concurrent signature; signatures exchange; random oracle model

网络环境中的公平交换数字签名是密码学领域广泛研究的问题，主要包括秘密逐步释放(gradual secret releasing)[1]和基于在线、离线的半可信第三方[2]两种解决方案，前者在协议参与者计算能力有较大差异时无法做到严格公平，后者需要第三方的参与，其公平性依赖于半可信性.

Chen等人提出的并发签名方案[3]在许多应用中可避免上述问题，基本思想是：首先由协议一方选

收稿日期：2009-04-11 作者简介：李保红(1968—)，男，博士，讲师. 基金项目：国家高技术研究发展计划资助项目(2008AA01Z136)；西安交通大学校内基金。

择一种特殊信息(称为 keystone),并计算出 keystone 印记;然后协议双方由 keystone 印记产生签名并进行交换;最后公布 keystone,第三方根据 keystone 印记产生的单向性可推断产生模糊签名的签名者身份.由于签名的产生使用了环签名技术,使得签名具有了模糊性,任何第三方只能断定模糊签名由两个签名者之一产生,而无法准确判定签名者身份,因此不会产生不公平的后果.

并发签名方案的新颖性使其受到广泛关注[3-9],尽管它对存在的安全漏洞进行了弥补或者扩展,但仍存在安全漏洞[3-6, 8-11].这些方案之所以存在安全问题,根源在于取消签名模糊性的方法存在缺陷,在 keystone 发布后,双方签名仍然维持模糊性,第三方仅能通过推断来确定签名者身份,即产生模糊签名时需要使用 keystone 印记,而 keystone 印记只能通过 keystone 获得,如果签名者公布了该 keystone,则一个模糊签名必然仅由该签名者产生.这种推断过程中的必然性在上述文献中并未加以证明,因此带来了各种攻击的可能性.

为了解决上述问题,本文提出了可废除并发签名(RCS)的概念,它利用公布的 keystone 可以废除签名的模糊性,任何第三方通过判断算法确定签名者的身份,使得双方交换的签名具备了标准签名的性质,从而消除了针对并发签名模糊性的各种可能的攻击.另外,RCS 只需要一个 keystone,而并发签名采用双方各产生一个 keystone 的方法,因此 RCS 可以使签名交换协议更加简化.

1 可废除并发签名及交换协议

定义 1 可废除并发签名是包含 SETUP、ASIGN、AVERIFY、JUDGE 等算法的数字签名机制.

SETUP: 是一个概率算法,输入为安全参数 λ;输出为参与者集合 $\mathscr{P}$、信息空间 $\mathscr{M}$、签名空间 $\mathscr{S}$、keystone 的 k 空间 $\mathscr{K}$、keystone 印记空间 $\mathscr{F}$、keystone 印记产生函数 KGEN:$\mathscr{K}\times\mathscr{M}\times\mathscr{M}\rightarrow\mathscr{F}$ 以及系统参数 δ.设参与者集合 $\mathscr{P}=\{P_i\mid 1\leqslant i\leqslant N\}$,$N$ 与 λ 呈多项式关系.该算法还为每个参与者 P_i 输出其公钥 y_i 和私钥 x_i.

ASIGN: 是一个概率算法,输入为$\langle y_i, x_i, y_j, m, f\rangle$,其中 y_i、y_j 为参与者 P_i、P_j 的公钥,x_i 为签名者 P_i 的私钥,$f\in\mathscr{F}$ 是 keystone 印记;输出是由 x_i 产生的关于信息 $m\in\mathscr{M}$ 的模糊签名 $\sigma=\langle L, U, f\rangle$,其中 $L=\{y_i, y_j\}$ 或 $\{y_j, y_i\}$,是参与者 P_i、P_j 的公钥列表,$U\in\mathscr{S}$.

AVERIFY: 是一个确定性算法,输入为$\langle\sigma, m\rangle$,其中 $\sigma=\langle L, U, f\rangle$;输出为 1(签名有效)或 0(签名无效).

JUDGE: 是一个确定性算法,输入为$\langle y_i, \sigma, k, m, m'\rangle$,其中 $k\in\mathscr{K}$,$\sigma=\langle L, U, f\rangle$,$y_i\in L$,并满足 $f=$KGEN(k, m, m')及 AVERIFY$(\sigma, m)=1$;输出为 1 或 0,表示 σ 是否由签名者 P_i(拥有公钥 y_i)产生.

在定义 1 中,m 和 m'是交换双方分别拥有的(公开)信息,交换双方就是交换 m 和 m'的签名.与原有并发签名相比,RCS 要求 keystone 印记 f 由 k、m、m'三者共同产生,而不是仅由 k 产生,其目的是防止攻击者利用 f 再次产生对其他信息的模糊签名,或替换自己原来产生的模糊签名.另一方面,在交换签名时,双方均已经知道 m 和 m',因此上述 keystone 印记的产生方法也是合理的.

假定协议双方 P_a 和 P_b 欲交换信息 m_a,$m_b\in\mathscr{M}$ 签名,并通过 SETUP 算法分别得到公私钥对(y_a, x_a)和(y_b, x_b).根据 RCS 定义,可给出相应的公平交换协议,描述如下.

(1) P_a 选择 $k\in\mathscr{K}$,计算 $f=$KGEN(k, m_a, m_b),然后产生 m_a 的模糊签名 $\sigma_a=\langle L_a, U_a, f\rangle=$ASIGN$(y_a, x_a, y_b, m_a, f)$,并发送给 P_b.

(2)收到 σ_a 后,P_b 验证 AVERIFY$(\sigma_a, m_a)=1$,若不成立则退出协议,否则 P_b 产生 m_b 的模糊签名 $\sigma_b=\langle L_b, U_b, f\rangle=$ASIGN$(y_b, x_b, y_a, m_b, f)$,并发送给 P_a.

(3)P_a 确定 σ_b 是否包含与 σ_a 相同的 f,并验证 AVERIFY$(\sigma_b, m_b)=1$,若不成立则退出协议,否则向 P_b 发送 k.

(4)任意第三方可验证 $f=$KGEN(k, m_a, m_b)、AVERIFY$(\sigma_a, m_a)=1$ 及 AVERIFY$(\sigma_b, m_b)=1$.若成立,则进一步判断 JUDGE$(y_a, \sigma_a, k, m_a, m_b)=1$ 及 JUDGE$(y_b, \sigma_b, k, m_a, m_b)=1$ 是否成立,从而确定签名者身份.

依照文献[3],将协议中 P_a 和 P_b 承担的角色分别称为初始签名者和匹配签名者.

2 安全性定义

定义 2 对于任意 y_i、y_j、x_i、m 和 f,如果满足以下两个条件,则 RCS 是正确的.

(1)AVERIFY(ASIGN$(y_i, x_i, y_j, m, f), m)=1$.

(2)存在 $m'\in\mathscr{M}$,有 $f=$KGEN(k, m, m'),则

JUDGE(y_i, ASIGN(y_i, x_i, y_j, m, f), k, m, m')=1.

定义 3　若任何攻击者 $\mathcal{A}$ 在实验中获胜概率相对于安全参数 λ 可忽略,则 RCS 具有自适应选择消息攻击下的存在性不可伪造性.

由概率多项式时间(PPT)攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 执行的实验如下.

初始化　$\mathcal{C}$ 执行 SETUP(1^λ),产生 $\mathcal{P}$、$\mathcal{M}$、$\mathcal{S}$、$\mathcal{K}$、$\mathcal{F}$、KGEN 和 δ,以及每个 P_i 的 y_i、x_i,公钥输出后传给 $\mathcal{A}$,私钥由 $\mathcal{C}$ 保存.

查询　$\mathcal{A}$ 可执行以下查询操作.

(1)印记查询. $\mathcal{A}$ 向 $\mathcal{C}$ 提交 m, $m'\in\mathcal{M}$,$\mathcal{C}$ 选择一个 $k\in\mathcal{K}$,并返回 f=KGEN(k, m, m'). $\mathcal{C}$ 将元组$\langle f, m, m', k\rangle$存放到印记查询列表中,以便实现 keystone 查询.

(2) keystone 查询. $\mathcal{A}$ 向 $\mathcal{C}$ 提交元组$\langle f, m, m'\rangle$,若 $\mathcal{C}$ 在印记查询列表中找到元组$\langle f, m, m', k\rangle$,则输出 $k\in\mathcal{K}$,否则输出无效.

(3)私钥查询. $\mathcal{A}$ 提交任意 y_i,若 y_i 为 $\mathcal{C}$ 产生的公钥,则 $\mathcal{C}$ 返回相应的 x_i.

(4)签名查询. $\mathcal{A}$ 提交形式为$\langle y_i, y_j, m, f\rangle$的信息,其中 y_i 和 y_j 为任意参与者公钥,并且 $y_i\neq y_j$. $\mathcal{C}$ 返回模糊的 $\sigma=\langle L, U, f\rangle$=ASIGN($y_i$, x_i, y_j, m, f). $\mathcal{A}$ 可用 AVERIFY 算法验证返回结果.

输出　最终 $\mathcal{A}$ 输出 $\sigma=\langle L, U, f\rangle$,其中 $L=\{y_i, y_j\}$,若 AVERIFY(σ, m)=1,并且 $\mathcal{A}$ 未针对$\langle y_i, y_j, m, f\rangle$或$\langle y_j, y_i, m, f\rangle$进行过签名查询,也未针对 y_i 和 y_j 进行过私钥查询,但可以通过印记查询得到 f,甚至通过 keystone 查询得到 $k\in\mathcal{K}$,使得存在 $m'\in\mathcal{M}$,f=KGEN(k, m, m'),则 $\mathcal{A}$ 在本次实验中获胜.

上述定义只包含了外部攻击的情况,即攻击者在不知道双方私钥的情况下,根据已公布或自行产生的 keystone,或者在仅知道 keystone 印记的情况下,伪造任一方的模糊签名,而对于内部攻击的情况则包含在公平性的定义中.

定义 4　攻击者 $\mathcal{A}$ 获胜优势为获胜概率大于猜测概率(1/2)的部分,而且任何攻击者 $\mathcal{A}$ 在实验中的获胜优势相对于安全参数 λ 是可忽略的,则 RCS 具有模糊性.

由 PPT 攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 执行的实验描述如下.

初始化与第一阶段查询　同定义 3.

挑战　$\mathcal{A}$ 选择元组$\langle y_i, y_j, m\rangle$作为向 $\mathcal{C}$ 发出的挑战,但要求 $\mathcal{A}$ 未针对 y_i 和 y_j 进行过私钥查询. $\mathcal{C}$ 随机选择 $k\in\mathcal{K}$,$m'\in\mathcal{M}$,计算 f=KGEN(k, m, m'),并随机选择 $b\in\{0, 1\}$,若 b=0,则 $\mathcal{C}$ 输出 $\sigma_0=\langle L_0, U_0, f\rangle$=ASIGN($y_i$, x_i, y_j, m, f),否则输出 $\sigma_1=\langle L_1, U_1, f\rangle$=ASIGN($y_j$, x_j, y_i, m, f),并将 σ_b 交给 $\mathcal{A}$.

第二阶段查询　同定义 3,同时要求 $\mathcal{A}$ 不能针对 y_i 和 y_j 进行过私钥查询,并且 $\mathcal{A}$ 不能针对 f 进行 keystone 查询.

输出　$\mathcal{A}$ 输出对 b 的猜测 b',若 $b=b'$,则 $\mathcal{A}$ 在本次实验中获胜.

模糊性的含义是指,任意一个外部攻击者(不知道双方私钥)无法分辨产生模糊签名的签名者身份. 该定义与文献[3]的不同之处是要求攻击者不能获得产生模糊签名的 keystone,否则可通过 JUDGE 算法废除模糊性. 由于签名只需要在 keystone 公布前具有模糊性,因此该要求是合理的.

定义 5　如果任何攻击者 $\mathcal{A}$ 在实验中获胜的概率相对于安全参数 λ 是可忽略的,则 RCS 具有公平性.

由 PPT 攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 执行的实验描述如下.

初始化与查询　同定义 3.

输出　$\mathcal{A}$ 选择元组$\langle y_j, y_i, m, f\rangle$,输出 $\sigma=\langle L, U, f\rangle$及 m',使得 AVERIFY (σ, m)=1,但要求 $\mathcal{A}$ 未针对 y_i 进行过私钥查询,并且需满足以下两个条件之一,则 $\mathcal{A}$ 在本次实验中获胜.

(1)f 是以前印记查询的输出,即 $\mathcal{C}$ 的印记查询列表中存在元组$\langle f, m, m', k\rangle$,但 $\mathcal{A}$ 未针对 f 进行过 keystone 查询,并有 JUDGE(y_j, σ, k, m, m')=0.

(2)$\mathcal{A}$ 针对 f 进行过 keystone 查询,已获得 k. 在 $\mathcal{A}$ 输出 σ 后,$\mathcal{C}$ 使用相同的 f 产生 m' 的 $\sigma'=\langle L', U', f\rangle$=ASIGN($y_i$, x_i, y_j, m', f),其中 L' 与 L 包含相同公钥(但次序可不同). $\mathcal{A}$ 得到 σ',在验证 AVERIFY (σ', m')=1 的情况下输出 $k\in\mathcal{K}$,使得 f=KGEN(k, m, m'),并且有 JUDGE(y_j, σ, k, m, m')=0,JUDGE(y_i, σ', k, m, m')=1.

上述定义中的条件(1)要求作为匹配签名者的攻击者不能产生一个有效的模糊签名,使得 keystone 发布后,JUDGE 算法无法判定攻击者就是签名者,由此维护了初始签名者的公平性. 条件(2) 要求在双方使用相同印记产生模糊签名后,作为初始签名者的攻击者,不能只将一个模糊签名与匹配签名者进行绑定,由此维护匹配签名者的公平性. 公平

性也排除了内部伪造的情况，即一方无法伪造一个模糊签名，并使之与对方的身份绑定.

定义 6 若可废除并发签名具有正确性、不可伪造性、模糊性和公平性，则称其为安全的.

3 可废除并发签名的实现

基于 Herranz 等人的环签名[12]，给出一个 RCS 的具体实现方案，其算法如下.

SETUP 算法选择两个大质数 p 和 q，满足 $q|(p-1)$，$q\geqslant 2^{\lambda}$. 设 G_q 是 $\boldsymbol{Z}_p^*$ 上阶为 q 的子群，生成元为 g. 算法选择 hash 函数 H_1，H_2：$\{0,1\}^*\rightarrow\boldsymbol{Z}_q$，将 $\mathcal{M}$、$\mathcal{S}$、$\mathcal{K}$ 和 $\mathcal{F}$ 分别定义为：$\mathcal{M}=\{0,1\}^*$，$\mathcal{S}=\mathcal{K}=\boldsymbol{Z}_q$，$\mathcal{F}=G_q$，而函数 KGEN 定义为 KGEN$(k, m, m')=g^{H_1(k\|m\|m')} \bmod p$，其中“‖”表示拼接. 此外，算法为每个参与者 P_i 随机选择 $x_i\in\boldsymbol{Z}_q$，计算 $y_i=g^{x_i} \bmod p$，并通过秘密信道将 x_i 发送给 P_i. 算法公布 $\delta=\langle p, q, g\rangle$.

ASIGN 对于输入$\langle y_i, x_i, y_j, m, f\rangle$，签名者 P_i 选择对于$\{i, j\}$的随机排列 π，即 $\pi(i)=i$、$\pi(j)=j$ 或$\pi(i)=j$、$\pi(j)=i$ 的概率均为 1/2，并由此得到公钥列表 $L=\{y_{\pi(i)}, y_{\pi(j)}\}$. P_i 选取随机数 a_j，$a_i\in\boldsymbol{Z}_q$ 做如下计算

$$\left.\begin{aligned}
&F=f^{x_i} \bmod p\\
&R_j=g^{a_j} \bmod p;\quad S_j=f^{a_j} \bmod p\\
&h_j=H_2(L\|\ m\|f\|F\|R_j\|S_j)\\
&R_i=g^{a_i}y^{-h_j} \bmod p;\quad S_i=f^{a_i}F^{-h_j} \bmod p\\
&h_i=H_2(L\|m\|f\|F\|R_i\|S_i)\\
&t=a_i+a_j+x_ih_i \bmod q
\end{aligned}\right\}\quad(1)$$

最后得到 $\sigma=\langle L, R_{\pi(i)}, S_{\pi(i)}, R_{\pi(j)}, S_{\pi(j)}, h_{\pi(i)}, h_{\pi(j)}, t, F, f\rangle$.

算法中使用随机排列 π 的目的是隐藏签名者的身份，使得攻击者无法根据公钥排列次序判定签名者身份. 另外，签名中的 $h_{\pi(i)}$、$h_{\pi(j)}$ 可以省略，以减少签名长度.

AVERIFY 输入 $\sigma=\langle L, R_i, S_i, R_j, S_j, h_i, h_j, t, F, f\rangle$ 及 m，其中 $L=\{y_i, y_j\}$，验证者验证 h_i、h_j 的正确性后判断以下两式是否成立

$$g^t=R_iR_jy_i^{h_i}y_j^{h_j} \bmod p \qquad (2)$$

$$f^t=S_iS_jF^{h_i}F^{h_j} \bmod p \qquad (3)$$

若成立，算法输出 1，否则输出 0.

JUDGE 输入 k、m 的 $\sigma=\langle L, R_i, S_i, R_j, S_j, h_i, h_j, t, F, f\rangle$ 及 m'，其中 $L=\{y_i, y_j\}$，在满足 $f=g^{H_1(k\|m\|m')} \bmod p$ 及 AVERIFY$(\sigma, m)=1$ 的情况下，算法验证等式 $F=y_i^{H_1(k\|m\|m')} \bmod p$ 是否成立，若成立输出 1，否则输出 0.

容易验证上述签名算法的正确性，即

$$g^t=g^{a_i}g^{a_j}(g^{x_i})^{h_i}=g^{a_i}g^{a_j}y_i^{h_i}$$

$$R_iR_jy_i^{h_i}y_j^{h_j}=g^{a_i}y_j^{-h_j}g^{a_j}y_i^{h_i}y_j^{h_j}$$

因此式(2)成立，同样可验证式(3)成立. 另外，$y_i^{H_1(k\|m\|m')}=(g^{x_i})^{H_1(k\|m\|m')}=f^{x_i}$，故 JUDGE 算法也是正确的.

4 可废除并发签名的安全性

RCS 签名的模糊性、不可伪造性和公平性分别由定理 1～定理 3 保证，限于篇幅，这些定理仅给出证明梗概. 证明过程采用随机预言模型，将 H_1、H_2 对应的随机 Oracle 分别称为 H_1-Oracle、H_2-Oracle.

定理 1 在随机预言模型下，假定存在 PPT 攻击者 $\mathcal{A}$，在定义 4 的实验限定时间 τ 内获得了不可忽略的优势 ε，则存在另一个攻击者 $\mathcal{B}$，在时间 $\tau'\leqslant\tau+(Q_f+Q_h+Q_s)\tau_h+Q_s\tau_s$ 之内，以不可忽略优势 $\varepsilon'\geqslant\frac{2}{N(N-1)}\left(1-\frac{(2Q_s+Q_h+2)(Q_s+1)}{2^{\lambda}}\right)\left(1-\frac{(Q_f+1)Q_f}{2^{\lambda}}\right)\frac{\varepsilon}{2}$ 解决确定性 Diffie-Hellman(DDH)问题，其中 Q_f、Q_h 和 Q_s 分别表示印记查询(H_1-Oracle 查询)、H_2-Oracle 查询和签名查询次数，τ_h、τ_s 表示 H_2-Oracle 查询和签名查询的时间.

证明 $\mathcal{B}$ 模拟挑战者 $\mathcal{C}$ 与 $\mathcal{A}$ 交互，利用 $\mathcal{A}$ 解决 DDH 问题. 给定 DDH 问题实例$\langle g, g^{\alpha}, g^{\beta}, g^{\gamma}\rangle$及随机数 g^{φ}，$\mathcal{B}$ 随机选择 $b\in\{0,1\}$及参与者 P_{u_0}、P_{u_1}，将其公钥设置为 $y_{u_b}=g^{\alpha}$、$y_{u_{\bar{b}}}=g^{\varphi}$. 当 $\mathcal{A}$ 给出挑战元组$\langle y_i, y_j, m\rangle$时，若 $i, j\in\{u_0, u_1\}$(概率为 $\frac{2}{N(N-1)}$)，$\mathcal{B}$ 将 f 和 F 的值设置为 g^{β}、g^{γ}，并且当 $\mathcal{A}$ 的输出 $b'=b$ 时 $\mathcal{B}$ 输出 1，否则输出 0，分别表示 $\mathcal{B}$ 判断 $g^{\gamma}=g^{\alpha\beta}$ 成立和不成立. 由此可计算出 $\mathcal{B}$ 正确解决 DDH 问题的优势大于 $\varepsilon/2$，考虑 $\mathcal{B}$ 在模拟 $\mathcal{C}$ 的过程中可能停机的概率，因而定理 1 得证.

定理 2 在随机预言模型下，假定存在 PPT 攻击者 $\mathcal{A}$，在定义 3 的实验限定时间 τ 之内以不可忽略概率 $\varepsilon\geqslant(12Q_h(Q_h-1)+6(Q_h+2Q_s)^2)/2^{\lambda}$ 伪造了一个有效的 RCS 签名，则可在期望时间 $\tau'\leqslant 144\ 823Q_h(Q_h-1)(\tau+\tau_sQ_s)/2^{\lambda+1}$ 之内解决离散对数(DL)问题.

证明 本文提出的 RCS 签名在形式上完全符合文

献[12]中一般环签名的要求，因此 Forking 引理[12]对其适用. 运用 Forking 引理，即重放攻击者 $\mathcal{A}$，使 $\mathcal{A}$ 输出针对某个 m 的两个有效的 RCS 签名$\langle L, R_i, S_i, R_j, S_j, h_i, h_j, t, F, f\rangle$、$\langle L, R_i, S_i, R_j, S_j, h'_i, h'_j, t', F, f\rangle$（为了简单起见，将 π 设为恒等映射）. 若 $h_i = h'_i$，$h_j \neq h'_j$，根据式（2）有 $g^t = R_i R_j y_i^{h_i} y_j^{h_j}$，$g^{t'} = R_i R_j y_i^{h'_i} y_j^{h'_j}$，则 $g^{t-t'} = y_j^{h_j - h'_j} = g^{x_j(h_j - h'_j)}$，故可计算出 $x_j = (t-t')/(h_j - h'_j) \bmod q$. 当 $h_j = h'_j$，$h_i \neq h'_i$ 时，同样可计算出 x_i. 这意味着，攻击者由参与者公钥可计算出对应私钥，故解决了 DL 问题.

定理 3　不存在 PPT 攻击者能够在定义 5 的实验中以不可忽略的概率胜出.

证明　对于定义 5 的情况（1），由于 m 的 $\sigma = \langle L, R_i, S_i, R_j, S_j, h_i, h_j, t, F, f\rangle$（其中 $L = \{y_i, y_j\}$）经过算法 AVERIFY 验证，而且 $\mathcal{A}$ 不知道 x_i，则 $\mathcal{A}$ 只能用 x_j 产生签名，否则违背定理 2. 又由于 JUDGE$(y_j, \sigma, k, m, m') = 0$，则存在 $x_s \neq x_j$，使得 $F = f^{x_s} \bmod p$. 根据 Forking 引理，$\mathcal{A}$ 可产生 m 的两个有效的签名$\langle L, R_i, S_i, R_j, S_j, h_i, h_j, t, F, f\rangle$和$\langle L, R_i, S_i, R_j, S_j, h'_i, h'_j, t', F, f\rangle$，并且 $h_i = h'_i$，$h_j \neq h'_j$，否则 $\mathcal{A}$ 可计算出 x_i. 由于 $h_j \neq h'_j$，因此可得到 $x_j (t-t')/(h_j - h'_j) \bmod q$. 根据式（3）有 $f^t = S_i S_j F^{h_i} F^{h_j}$，$f^{t'} = S_i S_j F^{h'_i} F^{h'_j}$，则可计算出 $x_s = (t-t')/(h_j - h'_j) \bmod q$，因此有 $x_s = x_j$，与假设矛盾. 情况（2）可类似证明.

5　结　论

本文提出了可废除并发签名的概念，其主要优点是 keystone 的公布可以显式地废除并发签名的模糊性，任意第三方可以通过确定性算法，而不是采用缺乏严谨性的推断方式来确定签名者身份，由此消除了各种攻击的可能性. 可废除并发签名的另一个优点是交换双方只需产生一个 keystone，简化了签名交换协议. 本文也给出了一个可废除并发签名的具体实现，并证明了其安全性.

在一些应用中，协议双方需要交换的是信息而非签名，因此下一步的工作是扩展可废除并发签名技术，以用于解决信息的公平交换问题.

参考文献：

[1] Garay G, Pomerance C. Timed fair exchange of standard signatures[C]// Proceedings of Financial Cryptography. Berlin, Germany: Springer, 2003: 190-207.

[2] ATENIESE G. Verifiable encryption of digital signatures and applications [J]. ACM Transactions on Information and System Security, 2004, 7(1): 1-20.

[3] CHEN Liqun, KUDLA C, PATERSON K G. Concurrent signatures [C]// Advances in Cryptology: Eurocrypt 2004. Berlin, Germany: Springer, 2004: 287-305.

[4] SUSILO W, MU Yi, ZHANG Fangguo. Perfect concurrent signature schemes [C]// Proceedings of 6th International Conference on Information and Communications Security. Berlin, Germany: Springer, 2004: 14-27.

[5] WANG Guilin, BAO Feng, ZHOU Jianying. The Fairness of perfect concurrent signature [C]// Proceedings of 8th International Conference on Information and Communications Security. Berlin, Germany: Springer, 2006: 435-451.

[6] CHOW S S M, SUSILO W. Generic construction of (identity-based) perfect concurrent signatures [C]// Proceedings of 7th International Conference on Information and Communications Security. Berlin, Germany: Springer, 2005: 194-206.

[7] NGUYEN K. Asymmetric concurrent signatures[C]// Proceedings of 7th International Conference on Information and Communications Security. Berlin, Germany: Springer, 2005: 181-193.

[8] SUSILO W, Mu Yi. Tripartite concurrent signatures [C]// Proceedings of 20th IFIP International Information Security Conference on Information Security. Berlin, Germany: Springer, 2005: 425-441.

[9] TONIEN D, SUSILO W, SAFAVI-NAINI R. Multiparty concurrent signatures[C]// Proceedings of 9th International Conference on Information Security. Berlin, Germany: Springer, 2006: 131-145.

[10] LI Yunfeng, HE Dake, LU Xianhui. Accountability of perfect concurrent signature [C]// Proceedings of 2008 International Conference on Computer and Electrical Engineering. Los Alamitos, CA, USA: IEEE Computer Society, 2008: 773-777.

[11] SHIEH C T. Fair multi-party concurrent signatures [D]. Taibei: National Central University, 2008.

[12] HERRANZ J, SAEZ G. Forking lemmas for ring signature schemes [C]// Proceedings of Progress in Cryptology: Indocrypt'03. Berlin, Germany: Springer, 2003: 266-279.

（编辑　苗凌）