现代密码学

Modern Cryptography

张方国

中山大学计算机学院

Office: Room 305, IM School Building

E-mail: isszhfg@mail.sysu.edu.cn

HomePage: https://cse.sysu.edu.cn/content/2460

第23讲数字签名（三）

第7章　签名方案

- 不可否认签名
- Fail-stop签名
- 其他各式各样的签名方案

不可否认签名

不可否认签名是由Chaum和Van Antwerpen在1989年提出的。

特点之一：没有签名者Alice的合作，签名就不能得到验证。该验证签名通过口令-应答协议来实现。

特点之二：签名者Alice不能否认她自己的合法签名。Alice可能声称一个有效的签名是伪造的，并且要么拒绝验证它，要么执行一个协议以便该签名不能得到验证。为了阻止这种情况发生，一个不可否认的签名方案与一个否认协议结合，通过这种方式Alice能够证明一个签名是伪造签名。

一个不可否认签名方案由三部分组成：签名算法、验证算法和否认协议。

不可否认签名

密码体制7.8 Chaum-van Antwerpen签名方案

设$p=2q+1$是一个使得q是素数并且在$\mathbb{Z}_p^*$上的离散对数问题是难处理的素数。设$\alpha \in \mathbb{Z}_p^*$是一个阶为$q$的元素。设$1 \le a \le q-1$，令$\beta = \alpha^a \mod p$。设$G$表示$\mathbb{Z}_p^*$的阶为$q$的乘法子群（$G$由模$p$的二次剩余构成）。设$\mathscr{P}=\mathscr{A}=G$，定义

$$K=\{(p,\alpha,a,\beta): \beta \equiv \alpha^a (\mod p)\}$$

值p,α,β是公钥，a是私钥。

对于$K=(p,\alpha,a,\beta)$和$x \in G$，定义

$$y = sig_K(x) = x^a \mod p$$

对$x,y \in G$，通过执行下面的协议来验证签名：

1. Bob随机选择$e_1,e_2 \in \mathbb{Z}_q$。
2. Bob计算$c = y^{e_1}\beta^{e_2} \mod p$并将它发送给Alice。
3. Alice计算$d = c^{a^{-1} \bmod q} \mod p$并将它发送给Bob。
4. 当且仅当$d \equiv x^{e_1}\alpha^{e_2} (\mod p)$时，Bob将$y$作为合法的签名接收。

不可否认签名

我们将证明Alice只能用很小的概率来欺骗Bob接收一个伪造签名。这个结果不依赖于任何计算假设，即安全性是无条件的。

定理7.3 如果$y \neq x^a \pmod{p}$，那么Bob将至多以$1/q$的概率把y当做x的一个合法签名接收。

不可否认签名

算法7.3 否认协议

1. Bob随机选择$e_1, e_2 \in \mathbb{Z}_q$。
2. Bob计算$c = y^{e_1}\beta^{e_2} \mod p$并将它发送给Alice。
3. Alice计算$d = c^{a^{-1} \mod q} \mod p$并将它发送给Bob。
4. Bob验证$d \neq x^{e_1}\alpha^{e_2} (\mod p)$。
5. Bob随机选择$f_1, f_2 \in \mathbb{Z}_q$。
6. Bob计算$C = y^{f_1}\beta^{f_2} \mod p$并将它发送给Alice。
7. Alice计算$D = c^{a^{-1} \mod q} \mod p$并将它发送给Bob。
8. Bob验证$D \neq x^{f_1}\alpha^{f_2} (\mod p)$。
9. 当且仅当$(d\alpha^{-e_2})^{f_1} \equiv (D\alpha^{-f_2})^{e_1} (\mod p)$时，Bob推断签名$y$是伪造的。

不可否认签名的变型

- 指定确认者签名（DCS）

DCS scheme: **S**, **V**, **C**

- **Setup:** $K^S := (PK_S, SK_S)$ and $K^C := (PK_C, SK_C)$ for **S** and **C**.
- **Sign:** $\sigma = Sign(m, SK_S)$ for a message m.
- **Verify:** Input (m, σ, PK_S) and outputs Accept if σ is an output of $Sign(m, SK_S)$.
- **ConfirmedSign:** $\sigma' = \text{ConfirmedSign}(m, SK_S, PK_C)$ of m.
- **Confirm:** is an interactive protocol between **C** and **V**.
- **Deny:** is an interactive protocol between **C** and **V**.
- **Extract:**Input (m, σ', SK_C, PK_S) and returns a string σ .

Fail-stop签名

fail-stop签名方案在防止一个能伪造签名的很强大的攻击者方面提供增强的安全性。

在Oscar对一则消息能伪造Alice签名事件中，Alice将随后能以高概率证明Oscar的签名是伪造的。

我们介绍van Heyst和Pedersen在1992年提出的fail-stop签名方案。它是一次签名方案。方案包括签名算法、验证算法和伪造证明算法。

密码体制7.9 van Heyst和Pedersen签名方案

设$p=2q+1$是一个使得q是素数并且在$\mathbb{Z}_p$上的离散对数是难处理的素数。设$\alpha \in \mathbb{Z}_p^*$是一个阶为$q$的元素。设$1 \le a_0 \le q-1$，令$\beta = \alpha^{a_0} \mod p$。值$p,q,\alpha,\beta$和$a_0$由一个可信中心选择。$p,q,\alpha$和$\beta$是公开的并认为是固定不变的。值$a_0$对包括Alice在内的任何人都是保密的。

设$\mathscr{P}=\mathbb{Z}_q$，$\mathscr{A}=\mathbb{Z}_q \times \mathbb{Z}_q$。密钥具有形式$K=(\gamma_1,\gamma_2,a_1,a_2,b_1,b_2)$，其中$a_1,a_2,b_1,b_2 \in \mathbb{Z}_q$

$$\gamma_1 = \alpha^{a_1}\beta^{a_2} \mod p, \quad \gamma_2 = \alpha^{b_1}\beta^{b_2} \mod p$$

(γ_1,γ_2)是公钥，而(a_1,a_2,b_1,b_2)是私钥。

对于$K=(\gamma_1,\gamma_2,a_1,a_2,b_1,b_2)$和$x \in \mathbb{Z}_q$，定义

$$sig_K(x)=(y_1,y_2)$$

其中

$$y_1 = a_1 + xb_1 \mod q, \quad y_2 = a_2 + xb_2 \mod q$$

对于$y=(y_1,y_2) \in \mathbb{Z}_q \times \mathbb{Z}_q$，我们有

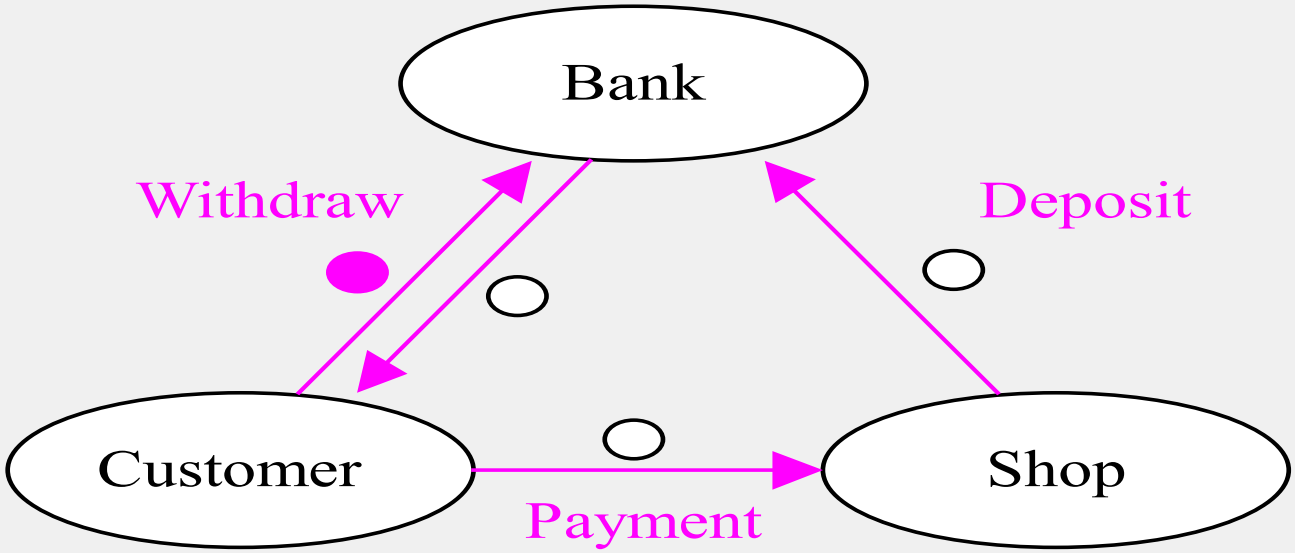
$$ver_K(x,y)=true \Leftrightarrow \gamma_1\gamma_2^x \equiv \alpha^{y_1}\beta^{y_2}(\mod p)$$

其他形式的签名

- 盲签名
- 部分盲签名
- 群签名
- 环签名
- 可验证的加密的签名(VES)
- 代理签名
- …

盲签名

一般数字签字中，总是要先知道文件内容而后才签署，这正是通常所需要的。但有时需要某人对一个文件签字，但又不让他知道文件内容，称此为**盲签字**(Blind Signature)，它是由Chaum1983年最先提出的



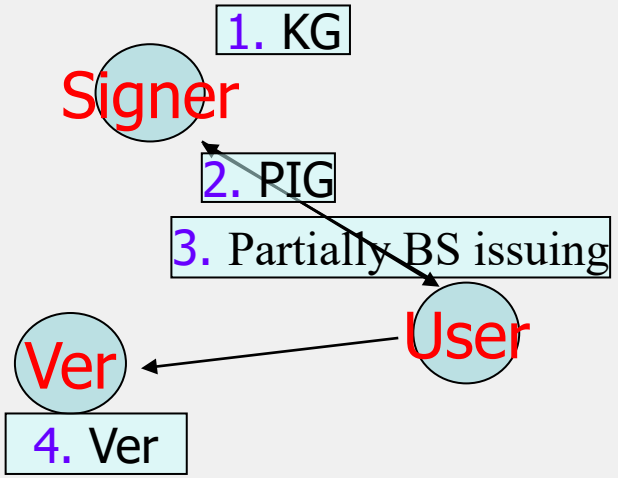
Eletronic payment Model

盲RSA签名

部分盲签名

- Partially Blind Signature:
  signer, user and verifier

  Key Generation:
  Public information generation:
  Partially blind signature issuing:
  Verification:



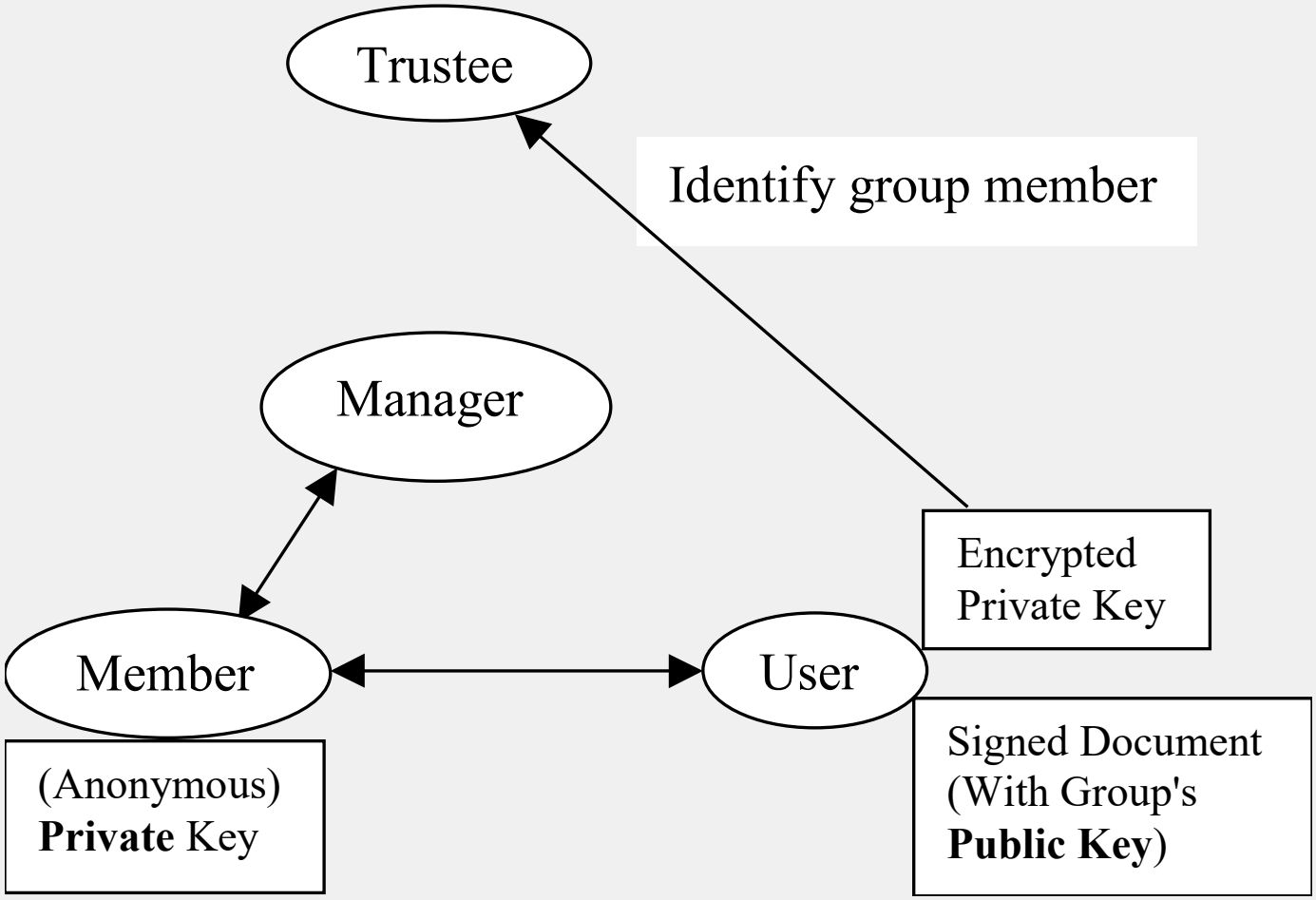
- Security:
  the completeness the partial blindness and the non-forgeability (one-more forgery)

群签名

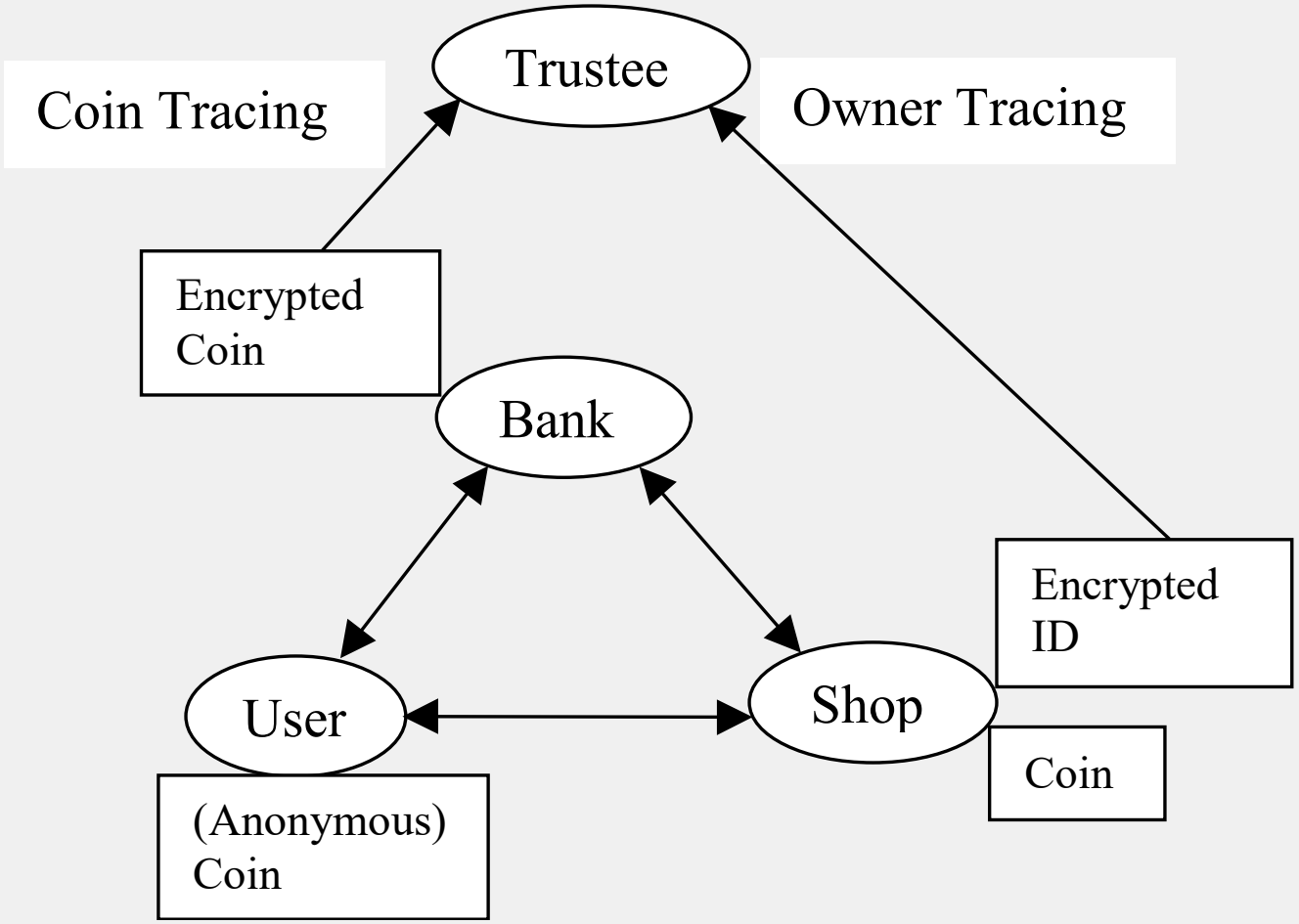
群体密码学(Group-Oriented Cryptography)1987年由Desmedt提出。它是研究面向社团或群体中所有成员需要的密码体制。在群体密码中，有一个公用的公钥，群体外面的人可以用它向群体发送加密消息，密文收到后要由群体内部成员的子集共同进行解密。

群签名(Group Signature)是面向群体密码学中的一个课题，1991年由Chaum和van Heyst提出。它有下述几个特点：① 只有群中成员能代表群体签字；② 接收到签字的人可以用公钥验证群签字，但不可能知道由群体中那个成员所签；③ 发生争议时可由群体中的成员或可信赖机构识别群签字的签字者。

Group signatures



群签名构造公平电子现金

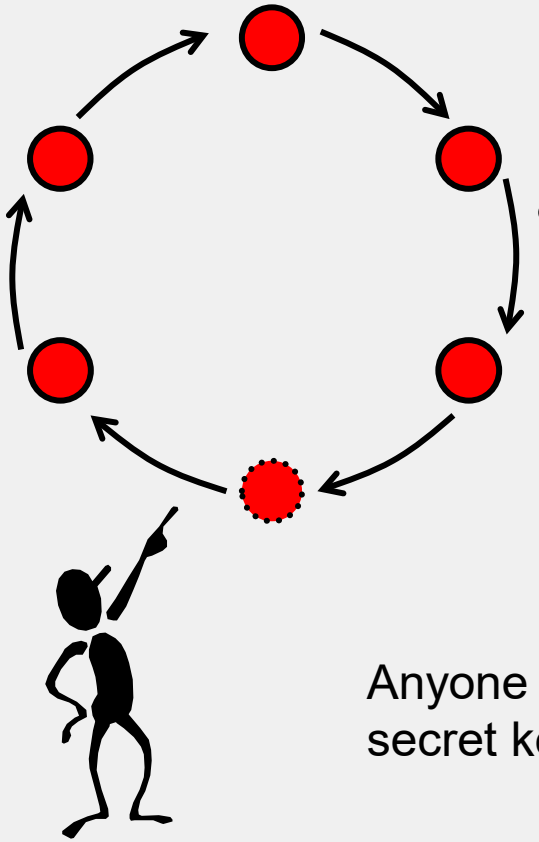


Ring signature

- In 2001, a ring signature scheme was proposed by Rivest, Shamir, Tauman.
- The signature scheme convinces a verifier that a document has been signed by one of n independent signers.

Ring Signature

- A signer can connect the head and tail of the series of values by using own secret key.
- A verifier computes series of values from the message and members' public keys, and checks that a signature has a ring structure.



Anyone cannot distinguish a part of the signature which is used secret key.

Anyone cannot distinguish the actual signer.

环签名的应用

- 2人环签名（DVS）
- 环签名与门罗币
- 门限环签名

随堂测试

1，在 Lamport 签名方案中，假设有两个 k 元组 x 和 x' 被 Alice 使用相同的密钥签名。设 l 表示 x 和 x' 不同的坐标数，即

$$l = |\{i : x_i \neq x'_i\}|$$

证明 Oscar 能对 $2^l - 2$ 个新的消息签名。

2，

考虑椭圆曲线 $E: y^2 \equiv x^3 + ax + b \pmod p$，其中 $4a^3 + 27b^2 \not\equiv 0 \pmod p$，$p > 3$ 是一个素数。

(a) 很显然点 $P = (y_1, y_2) \in E$ 具有阶数 3，当且仅当 $2P = -P$。利用这个事实，证明，如果 $P = (y_1, y_2) \in E$ 具有阶数 3，则有：

$$3x_1^4 + 6ax_1^2 + 12x_1 b - a^2 \equiv 0 \pmod p \qquad (6.7)$$

(b) 从式(6.7)推出结论：E 上至多有 8 个阶数为 3 的点。

3，

在 ElGamal 签名方案或 DSA 中不允许 $\delta = 0$。证明如果对消息签名时 $\delta = 0$，那么攻击者很容易计算出密钥 a。