



现代密码学

第四十九讲 特殊性质的签名算法

信息与软件工程学院



特殊性质的签名算法

A diagram showing four special signature algorithms. On the left, a vertical line connects four white circles. Each circle is partially overlapped by a horizontal blue bar that contains the name of the algorithm in white Chinese characters.

盲签名

不可否认签名

群签名

代理签名

A decorative graphic consisting of several horizontal blue bars of varying lengths, stacked vertically, is positioned to the left of the section header.


盲签名

- 盲签名是在发送者A和签名者B之间的双方协议。其基本思想如下：
A发送给B一段信息，B对它签名并送回A。从这个签名，A能够计算B关于A预先所选消息 m 的签名。
协议完成时，B既不知道消息 m 也不知道消息的签名。
- 盲签名的目的是防止B看到消息和签名，从而使B以后不能将所签消息和发送者A联系起来。

A decorative graphic consisting of several horizontal blue lines of varying lengths, located to the left of the section header.

盲签名的应用

- 发送者A（客户）不希望签名者B（银行）能够将一条先验消息 m 及其签名 $S_B(m)$ 与协议的特定实例相联系。
- 这个特性在电子现金应用中可能很重要，因为那里的消息也许表示A所花的金钱数额。
- 当 m 和 $S_B(m)$ 提交给B进行支付时，B无法推断原先接收签名的是谁。这就是允许A的匿名性，从而A的消费模式不能被监测。

- 
- A decorative blue horizontal bar with a series of parallel lines is positioned on the left side of the slide.
- 盲签名协议需要下列组件：
 - 签名者B的一种数字签名机制。用 $S_B(x)$ 记B对 x 的签名。
 - 函数 f 和 g （只有发送者知道），满足 $g(S_B(f(m))) = S_B(m)$ 。 f 叫做盲化函数， g 叫做去盲函数， $f(m)$ 叫做盲消息。
 - 第2条对 S_B 和 g 的选择加了许多限制。

Chaum盲签名协议

- 发送者A接收B关于盲消息的签名。
- A计算B关于A预先所选消息 m 的签名, $0 \leq m \leq n-1$ 。B既没有消息 m 也没有 m 相关签名的知识。
 - B的RSA公钥和私钥分别是 (n, e) 和 d 。 k 是A随机选择的秘密数, 满足 $0 \leq k \leq n-1$ 且 $\gcd(n, k)=1$ 。
 - 协议步骤。
 - (盲化) A计算 $m^* = mk^e \bmod n$, 将它发送给B。
 - (签名) B计算 $s^* = (m^*)^d \bmod n$, 将它发送给A。
 - (去盲) A计算 $s = k^{-1} s^* \bmod n$, s 就是B关于 m 的签名。

A decorative graphic consisting of several horizontal blue lines of varying lengths, located to the left of the section header.

Chaum盲签名的正确性

- 显然 s 是 m 的签名, 即 $s = m^d \bmod n$ 。
- B既没有消息 m 也没有 m 相关签名 s 的知识。

A decorative graphic consisting of several horizontal blue lines of varying lengths, stacked vertically, is positioned to the left of the title.

特殊性质的签名算法

A diagram showing four special signature algorithms. On the left, there is a vertical line with four white circles connected by it. Each circle is connected to a horizontal blue bar that contains the name of the algorithm.

盲签名

不可否认签名

群签名

代理签名

A decorative graphic consisting of several horizontal blue lines of varying lengths, stacked vertically, is positioned to the left of the title.

不可否认的数字签名

- 不可否认的数字签名由Chaum等在1989年提出。
- 不可否认签名没有签名者的合作，接收者无法验证签名

A decorative graphic consisting of several horizontal blue lines of varying lengths, located to the left of the section header.

不可否认签名的应用

- 实体A（客户）希望访问被实体B（银行）控制的某个安全区域。比如该安全区域可能是存放保险箱的房间。在许可访问之前，B要求A签署一份时间和日期的文件。如果A采用了不可否认签名，那么在验证过程中没有A的直接参与，（在以后的日期）B就不能向任何人证明A使用过安全区域中的设施。
- 假定某大公司A制作了一个软件包。A对软件包签名并将它卖给实体B，而B决定将其拷贝再卖给第三方C，那么没有A的合作C就无法验证该软件是否正版。当然，这种措施并不能阻止B用它自己的签名重新签署软件包，但因此B也就无法利用与A名气相关的市场利益。而且追踪B的欺诈行为也将很容易。



- 一个不可否认签名方案有三部分组成：
 - 签名算法
 - 验证协议
 - 否认协议



- 签名者可以声称一个签名是伪造的，在这种情况下，如果签名者拒绝参加验证，就可认为签名者有欺骗行为。如果签名者参加验证，由否认协议就可推断出签名的真伪。
- 否认协议需要做到以下两点
 - B能使A相信一个不合法的签名是伪造的。
 - B以很小的概率使A相信一个合法签名是伪造的。



- 不可否认签名的一个不足之处是签名者有可能不在场或者拒绝合作，而导致签名无法被接收者验证。
 - Chaum提出“指定验证者签名”的概念，其中签名者指定某实体作为签名的验证者。
 - 一旦签名者不在场或者拒绝合作，验证者就有权力与接收者交互来检查签名。
 - 验证者不能产生签名者的签名。



特殊性质的签名算法

A diagram showing four special signature algorithms. On the left, a vertical line of four white circles is connected by a single line. Each circle is connected to a horizontal blue bar that extends to the right. The text for each algorithm is written in white on these bars.

盲签名

不可否认签名

群签名

代理签名

A decorative graphic consisting of several horizontal blue bars of varying lengths, located to the left of the section header.

群签名

- 1991年，Chaum等提出群签名方案。
- 该方案允许群里的某个成员以群的名义匿名地签发消息。满足下述三个条件：
 - 只有群中的成员才能代表群进行签名；
 - 签名的接收者能验证签名是哪一个群的一个合法签名，但不能分辨具体的签名者。
 - 一旦出现争端，可借助群成员或一个可信的机构能识别出签名者。

A decorative graphic consisting of several horizontal blue lines of varying lengths, located to the left of the section header.

群签名的应用

- 一个公司有几台计算机，每台都联在局域网上。公司的每个部门有其自己的打印机（也连在局域网上），并且只有本部门的人员才能允许使用其部门的打印机。因此，打印前必须确认用户在哪个部门工作。同时公司为了保密，不可以暴露用户的身份。然而，如果有人滥用打印机，主管者必须能找出是谁在滥用打印机。



一个群签名方案由以下几个部分组成：

- (1) 建立 (setup) 一个用以产生群公钥和私钥的多项式概率算法。
- (2) 加入 (join) 一个用户和群管理员之间的交互式协议。执行该协议可以使用户成为群成员，群管理员得到群成员的秘密的成员管理密钥，并产生群成员的私钥和成员证书。



- (3) 签名 (sign) 一个概率算法，当输入一个消息、一个群成员的私钥和一个群公钥后，输出对该消息的签名。
- (4) 验证 (verify) 给定一个消息的签名和一个群公钥后，判断该签名相对于该群公钥是否有效。
- (5) 打开 (open) 给定一个签名、群公钥和群私钥的条件下确定签名者的身份。

A decorative graphic consisting of ten horizontal blue lines of varying lengths, stacked vertically, is positioned to the left of the title.

特殊性质的签名算法

A diagram showing four special signature algorithms. On the left, a vertical line connects four white circles. Each circle is connected to a horizontal blue bar that contains the name of the algorithm in white Chinese characters.

盲签名

不可否认签名

群签名

代理签名

A decorative blue horizontal bar with a series of parallel lines is positioned to the left of the section header.

代理签名

一个代理签名方案由以下几个部分组成：

- **系统建立** 选定代理签名方案的系统参数，用户的密钥等。
- **签名权力的委托** 原始签名者将自己的签名权力委托给代理签名者。
- **代理签名的产生** 代理签名者代表原始签名者产生代理签名。
- **代理签名的验证** 验证人验证代理签名的有效性。