第五章　签名方案

张磊

华东师范大学 • 软件学院

§5.1　引言

数字世界中的问题

日常生活中遇到的问题:

1. Alice 和 Bob 如何确认签订的合同?
2. Bob 如何确认收到的信件来自 Alice?
3. 信用卡在超市购物时, 如何向银行确认支付订单?

数字世界中的问题

日常生活中遇到的问题:

1. Alice 和 Bob 如何确认签订的合同?
2. Bob 如何确认收到的信件来自 Alice?
3. 信用卡在超市购物时, 如何向银行确认支付订单?

传统方法解决上述问题都是采用手写签名,

数字世界中的问题

日常生活中遇到的问题:

1. Alice 和 Bob 如何确认签订的合同?
2. Bob 如何确认收到的信件来自 Alice?
3. 信用卡在超市购物时, 如何向银行确认支付订单?

传统方法解决上述问题都是采用手写签名, 这有两个缺点:

1. 手写签名无法应用到数字世界中;

数字世界中的问题

日常生活中遇到的问题:

1. Alice 和 Bob 如何确认签订的合同?
2. Bob 如何确认收到的信件来自 Alice?
3. 信用卡在超市购物时, 如何向银行确认支付订单?

传统方法解决上述问题都是采用手写签名, 这有两个缺点:

1. 手写签名无法应用到数字世界中;
2. 手写签名容易被伪造.

数字世界中的问题

日常生活中遇到的问题:

1. Alice 和 Bob 如何确认签订的合同?
2. Bob 如何确认收到的信件来自 Alice?
3. 信用卡在超市购物时, 如何向银行确认支付订单?

传统方法解决上述问题都是采用手写签名, 这有两个缺点:

1. 手写签名无法应用到数字世界中;
2. 手写签名容易被伪造.

签名方案 (Signature Scheme) 是一种给数字消息签名的方法，也称数字签名 (Digital SignatUre), 它至少需要解决以下问题

1. 签名与消息绑定
2. 其他人能够验证签名的有效性
3. 能够防止签名被重复使用, 解决方法: 加入签名时间等信息

签名方案的形式定义

一个签名方案是一个满足下列条件的五元组 $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$:

1. $\mathcal{P}$ 是由所有可能的消息组成的一个有限集合
2. $\mathcal{A}$ 是由所有可能的签名组成的一个有限集合
3. $\mathcal{K}$ 为密钥空间, 是由所有可能的密钥组成的一个有限集合
4. 对每一个 $K \in \mathcal{K}$, 有一个保密签名算法

$$\mathrm{Sig}_K : \mathcal{P} \to \mathcal{A} \in \mathcal{S}$$

和一个相应的公开验证算法

$$\mathrm{Ver}_K : \mathcal{P} \times \mathcal{A} \to \{\mathrm{True}, \mathrm{False}\} \in \mathcal{V},$$

使得对每个消息 $x \in \mathcal{P}$ 和每个签名 $y \in \mathcal{A}$, 都有

$$\mathrm{Ver}_K(x, y) = \begin{cases} \mathrm{True}, & y = \mathrm{Sig}_K(x) \\ \mathrm{False}, & y \neq \mathrm{Sig}_K(x) \end{cases}$$

签名方案相关定义

1. $(x, y) \in \mathcal{P} \times \mathcal{A}$ 称为消息-签名对或者简称签名消息; 使得

$$\mathrm{Ver}_K(x, y) = \mathrm{True}$$

成立的 (x, y) 称为有效消息-签名对 (或简称有效签名消息).

2. 对每个密钥 $K \in \mathcal{K}$, Sig_K 和 Ver_K 应该是多项式时间函数.
3. Sig_K 是保密的, 而 Ver_K 是公开的. 这意味着对给定的消息 x, 除了合法签名者 (比如 Alice) 之外, 任何人 (比如 Oscar) 去产生有效消息-签名对应该计算上不可行.
4. 如果 Oscar 能产生一对 Alice 以前没有签名过的有效 (x, y), 则签名 y 称为伪造签名.

RSA 签名方案

设 $n = pq$, 其中 p, q 是大素数. 设 $\mathcal{P} = \mathcal{A} = \mathbb{Z}_n$, 并定义

$$\mathcal{K} = \{(n, p, q, a, b) \mid ab \equiv 1 \pmod{\phi(x)}\}.$$

其中公钥 $PK = (n, b)$, 私钥 $SK = (p, q, a)$. 对 $K = (n, p, q, a, b)$, 定义签名算法为

$$\mathrm{Sig}_K(x) = x^a \bmod n, \quad x \in \mathbb{Z}_n,$$

验证算法为

$$\mathrm{Ver}_K(x, y) = \mathrm{True} \Leftrightarrow x \equiv y^b \pmod{n}, \quad (x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n.$$

§ 5.2　签名方案的安全性需求

根据攻击者所掌握的信息, 对签名方案的攻击可分为三类:

1. 唯密钥攻击: Oscar 拥有 Alice 的公钥, 也即验证函数 Ver_K

攻击模型

根据攻击者所掌握的信息, 对签名方案的攻击可分为三类:

1. 唯密钥攻击: Oscar 拥有 Alice 的公钥, 也即验证函数 Ver_K
2. 已知消息攻击: Oscar 拥有一系列 Alice 签名的消息-签名对

$$(x_1, y_1), (x_2, y_2), \cdots$$

攻击模型

根据攻击者所掌握的信息, 对签名方案的攻击可分为三类:

1. 唯密钥攻击: Oscar 拥有 Alice 的公钥, 也即验证函数 Ver_K
2. 已知消息攻击: Oscar 拥有一系列 Alice 签名的消息-签名对

$$(x_1, y_1), (x_2, y_2), \cdots$$

3. 选择消息攻击: Oscar 请求 Alice 对一系列由他所选择的消息 $x_1, x_2, \cdots$ 签名, 得到一系列消息-签名对

$$(x_1, y_1), (x_2, y_2), \cdots$$

攻击者目标

攻击者对签名方案的可能攻击目标有三种:

1. 完全破译: Oscar 确定出 Alice 的私钥 (从而获得签名函数 Sig_K), 从而可对任意消息伪造 Alice 的签名

攻击者目标

攻击者对签名方案的可能攻击目标有三种:

1. 完全破译: Oscar 确定出 Alice 的私钥 (从而获得签名函数 Sig_K), 从而可对任意消息伪造 Alice 的签名
2. 选择性伪造: 对 Alice 没有签名过的, 且由他人 (非 Oscar) 选择的消息 x, Oscar 能够以某一不可忽略的概率伪造出 Alice 的有效签名 y

攻击者目标

攻击者对签名方案的可能攻击目标有三种:

1. 完全破译: Oscar 确定出 Alice 的私钥 (从而获得签名函数 Sig_K), 从而可对任意消息伪造 Alice 的签名
2. 选择性伪造: 对 Alice 没有签名过的, 且由他人 (非 Oscar) 选择的消息 x, Oscar 能够以某一不可忽略的概率伪造出 Alice 的有效签名 y
3. 存在性伪造: Oscar 能够伪造 Alice 的一对有效消息-签名对 (x, y), 且 x 不是 Alice 签名过的消息

攻击者目标

攻击者对签名方案的可能攻击目标有三种:

1. 完全破译: Oscar 确定出 Alice 的私钥 (从而获得签名函数 Sig_K), 从而可对任意消息伪造 Alice 的签名
2. 选择性伪造: 对 Alice 没有签名过的, 且由他人 (非 Oscar) 选择的消息 x, Oscar 能够以某一不可忽略的概率伪造出 Alice 的有效签名 y
3. 存在性伪造: Oscar 能够伪造 Alice 的一对有效消息-签名对 (x, y), 且 x 不是 Alice 签名过的消息

对目前的签名方案, 安全性基本上都要求达到选择消息攻击下的存在性不可伪造, 记为 EUF-CMA (Existential UnForgeability under Chosen Message Attacks).

RSA 签名方案的安全性

1. 唯密钥攻击下的存在性伪造:

   对任意的 y, Oscar 可计算 $x \leftarrow y^b \bmod n$, 则 (x, y) 是有效的消息-签名对.

RSA 签名方案的安全性

1. 唯密钥攻击下的存在性伪造:
   对任意的 y, Oscar 可计算 $x \leftarrow y^b \bmod n$, 则 (x, y) 是有效的消息-签名对.

2. 已知消息攻击下的存在性伪造:
   对 Alice 签名过的两个消息-签名对 (x_1, y_1) 和 (x_2, y_2), Oscar 可以得到消息 $x = x_1 x_2 \bmod n$ 的签名 $y = y_1 y_2 \bmod n$.

RSA 签名方案的安全性

1. 唯密钥攻击下的存在性伪造:
   对任意的 y, Oscar 可计算 $x \leftarrow y^b \bmod n$, 则 (x, y) 是有效的消息-签名对.
2. 已知消息攻击下的存在性伪造:
   对 Alice 签名过的两个消息-签名对 (x_1, y_1) 和 (x_2, y_2), Oscar 可以得到消息 $x = x_1 x_2 \bmod n$ 的签名 $y = y_1 y_2 \bmod n$.
3. 选择消息攻击下的选择性伪造:
   对一个由他人选择的 x, Oscar 可以很容易的找到 x_1, x_2 使得 $x = x_1 x_2 \bmod n$, 然后请求 Alice 分别对 x_1, x_2 签名得到 y_1, y_2, 则 $y_1 y_2 \bmod n$ 就是消息 x 的签名.

§ 5.3　ElGamal 签名方案及其安全性

ElGamal 签名方案

设 p 是一个使得在 $\mathbb{Z}_p$ 上离散对数问题是难处理的素数, α 是一个模 p 本原元. 设 $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{A} = \mathbb{Z}_p^* \times \mathbb{Z}_{p-1}$, 定义

$$\mathcal{K} = \{(p, \alpha, a, \beta) \mid \beta = \alpha^a \bmod p\},$$

(p, α, β) 是公钥, a 是私钥.

对 $K = (p, \alpha, a, \beta)$, 以及一个 (秘密) 随机数 $k \in \mathbb{Z}_{p-1}^*$, 定义:

$$\mathrm{Sig}_K(x, k) = (\gamma, \delta), \quad x \in \mathbb{Z}_p^*$$

其中

$$\gamma = \alpha^k \bmod p, \quad \delta = (x - a\gamma)k^{-1} \bmod (p-1).$$

对消息-签名对 $(x, (\gamma, \delta))$, 定义:

$$\mathrm{Ver}_K(x, (\gamma, \delta)) = \mathrm{True} \Leftrightarrow \beta^\gamma \gamma^\delta \equiv \alpha^x \pmod p.$$

ElGamal 签名方案安全性之: 唯密钥攻击下的存在性伪造

Oscar 在只有公钥 (p, α, β) 情形下可生成一个有效的消息-签名对

ElGamal 签名方案安全性之: 唯密钥攻击下的存在性伪造

Oscar 在只有公钥 (p, α, β) 情形下可生成一个有效的消息-签名对

1. 随机选择整数 $0 \le i, j \le p-2$, 使之满足 $\gcd(j, p-1) = 1$;
2. 计算

$$\begin{aligned} \gamma &= \alpha^i \beta^j \bmod p, \\ \delta &= -\gamma j^{-1} \bmod (p-1), \\ x &= -\gamma i j^{-1} \bmod (p-1); \end{aligned}$$

3. 可以验证, 这样构造的 $(x, (\gamma, \delta))$ 是有效的消息-签名对:

$$\beta^\gamma \gamma^\delta \equiv \beta^\gamma (\alpha^i \beta^j)^\delta \equiv \beta^{\gamma + j\delta} \alpha^{i\delta} \equiv \alpha^{i(-\gamma j^{-1})} \equiv \alpha^x \pmod p.$$

ElGamal 签名方案安全性之: 已知消息攻击下的存在性伪造

假设 Oscar 已从 Alice 处获得有效消息-签名对 $(x, (\gamma, \delta))$, 他可按以下方法伪造签名:

假设 Oscar 已从 Alice 处获得有效消息-签名对 $(x,(\gamma,\delta))$, 他可按以下方法伪造签名:

1. 随机选择 $0 \le h, i, j \le p-2$, 使得 $\gcd(h\gamma - j\delta, p-1) = 1$;
2. 计算
$$\begin{aligned}\lambda &= \gamma^h\alpha^i\beta^j \bmod p,\\ \mu &= \delta\lambda(h\gamma - j\delta)^{-1} \bmod (p-1),\\ x' &= \lambda(hx + i\delta)(h\gamma - j\delta)^{-1} \bmod (p-1);\end{aligned}$$
3. 可以验证, 这样构造的 $(x',(\lambda,\mu))$ 是有效的消息-签名对:
$$\beta^\lambda\lambda^\mu \equiv \beta^\lambda(\gamma^h\alpha^i\beta^j)^{\delta\lambda(h\gamma-j\delta)^{-1}} \equiv \alpha^{x'} \pmod p$$

(证明过程中需用到等式 $\gamma^\delta \equiv \alpha^x\beta^{-\gamma} \equiv \pmod p$).

抵抗上述对 RSA 签名方案和 ElGamal 签名方案的伪造攻击最直接的办法就是在签名方案中引入安全 Hash 函数.

Hash 函数与签名方案的巧妙结合

抵抗上述对 RSA 签名方案和 ElGamal 签名方案的伪造攻击最直接的办法就是在签名方案中引入安全 Hash 函数.

假设 $h : \{0,1\}^* \to \mathcal{Z} \subset \mathcal{P}$ 是一个安全 Hash 函数, 则 h 和签名方案的结合使用如下:

消息		消息摘要		签名
x	$\to$	$z = h(x)$	$\to$	$y = \mathrm{Sig}_K(z)$
$x \in \{0,1\}^*$		$z \in \mathcal{Z}$		$y \in \mathcal{A}$

Hash 函数与签名方案的巧妙结合

抵抗上述对 RSA 签名方案和 ElGamal 签名方案的伪造攻击最直接的办法就是在签名方案中引入安全 Hash 函数.

假设 $h : \{0,1\}^* \to \mathcal{Z} \subset \mathcal{P}$ 是一个安全 Hash 函数, 则 h 和签名方案的结合使用如下:

消息		消息摘要		签名
x	$\to$	$z = h(x)$	$\to$	$y = \mathrm{Sig}_K(z)$
$x \in \{0,1\}^*$		$z \in \mathcal{Z}$		$y \in \mathcal{A}$

1. 可以大大加快签名方案运算速度 (当消息 x 较长时可以大大减少签名次数);
2. 当 h 是安全 Hash 函数时, 不仅不会削弱签名方案的安全性, 反而会增加签名方案的安全性.

§ 5.4　ElGamal 签名方案的变形

数字签名算法 (DSA: Digital Signature Algorithm)

设 p 是长为 L 比特的素数, 在 $\mathbb{Z}_p$ 上其离散对数问题是难处理的, 其中 $L \equiv 0 \pmod{64}$ 且 $512 \le L \le 1024$, q 是能被 $p-1$ 整除的 160 比特的素数. 设 $\alpha \in \mathbb{Z}_p^*$ 且 $\mathrm{Ord}_p(\alpha) = q$. 设 $\mathcal{P} = \{0,1\}^*$, $\mathcal{A} = \mathbb{Z}_q^* \times \mathbb{Z}_q^*$, 并定义

$$\mathcal{K} = \{(p, q, \alpha, a, \beta) \mid \beta = \alpha^a \bmod p\},$$

其中 $0 \le a \le q-1$. (p, q, α, β) 是公钥, a 是私钥.
对 $K = (p, q, \alpha, a, \beta)$, 以及一个 (秘密) 随机数 $1 \le k \le q-1$, 定义:

$$\mathrm{Sig}_K(x, k) = (\gamma, \delta), \quad x \in \{0,1\}^*$$

其中

$$\gamma = (\alpha^k \bmod p) \bmod q, \quad \delta = (\text{SHA-1}(x) + a\gamma)k^{-1} \bmod q$$

(如果 $\gamma = 0$ 或者 $\delta = 0$, 应该为 k 另选一个随机数).
对消息-签名对 $(x, (\gamma, \delta))$, 验证通过下面的计算完成:

$$\begin{aligned} e_1 &= \text{SHA-1}(x)\delta^{-1} \bmod q; \\ e_2 &= \gamma\delta^{-1} \bmod q; \\ \mathrm{Ver}_K(x, (\gamma, \delta)) = \text{True} &\Leftrightarrow (\alpha^{e_1}\beta^{e_2} \bmod p) \bmod q = \gamma. \end{aligned}$$

椭圆曲线 DSA (ECDSA: Elliptic Curve Digital Signature Algorithm)

设 p 是大素数, E 是定义在 $\mathbb{Z}_p$ 上椭圆曲线. 设 α 是 E 上阶为 q (q 是素数) 的点 (即 $q\alpha = \mathcal{O}$), 使得在 $\langle\alpha\rangle = \{i\alpha \mid 0 \le i \le q-1\}$ 上的离散对数问题是难处理的.

设 $\mathcal{P} = \{0,1\}^*$, $\mathcal{A} = \mathbb{Z}_q^* \times \mathbb{Z}_q^*$, 并定义

$$\mathcal{K} = \{(p, q, E, \alpha, a, \beta) \mid \beta = a\alpha\},$$

其中 $0 \le a \le q-1$. (p, q, E, α, β) 是公钥, a 是私钥.

对 $K = (p, q, E, \alpha, a, \beta)$, 以及一个 (秘密) 随机数 $1 \le k \le q-1$, 定义:

$$\mathrm{Sig}_K(x, k) = (r, s), \quad x \in \{0,1\}^*$$

其中

$$\begin{aligned} k\alpha &= (u, v) \\ r &= u \bmod q \\ s &= (\text{SHA-1}(x) + ar)k^{-1} \bmod q \end{aligned}$$

(如果 $r = 0$ 或者 $s = 0$, 应该为 k 另选一个随机数).

对消息-签名对 $(x, (r, s))$, 验证通过下面的计算完成:

$$\begin{aligned} w &= s^{-1} \bmod q; \\ i &= w \cdot \text{SHA-1}(x) \bmod q; \\ j &= wr \bmod q; \\ (u, v) &= i\alpha + j\beta; \\ \mathrm{Ver}_K(x, (r, s)) = \text{True} &\Leftrightarrow u \bmod q = r. \end{aligned}$$

§5.5　可证安全的签名方案

一次签名

此方案给出一种由单向双射函数构造可证明安全签名方案的方法

一次签名

此方案给出一种由单向双射函数构造可证明安全签名方案的方法

Lamport 签名方案

设 k 是一个正整数且 $\mathcal{P} = \{0,1\}^k$. 假定 $f : Y \to Z$ 是一个单向双射函数, 并且 $\mathcal{A} = Y^k$. 随机选择 $2k$ 个数 $y_{i,j} \in Y$, 并计算

$$z_{i,j} = f(y_{i,j}),\ 1 \le i \le k,\ j = 0, 1.$$

密钥 K 由 $2k$ 个 $y_{i,j}$ 和 $2k$ 个 $z_{i,j}$ 组成, 其中 $y_{i,j}$ 是私钥, $z_{i,j}$ 是公钥. 对于 $K = (y_{i,j}, z_{i,j} \mid 1 \le i \le k,\ j = 0, 1)$, 定义

$$\mathrm{Sig}_K(x_1, \cdots, x_k) = (y_{1,x_1}, \cdots, y_{k,x_k}),\ x_i \in \{0, 1\}.$$

对于消息-签名对$((x_1, \cdots, x_k), (a_1, \cdots, a_k))$, 定义

$$\mathrm{Ver}_K((x_1, \cdots, x_k), (a_1, \cdots, a_k)) = \mathrm{True} \Leftrightarrow f(a_i) = z_{i,x_i},\ 1 \le i \le k.$$

Lamport 签名方案特点

1. 可证明上述 Lamport 签名方案是唯密钥攻击下存在性不可伪造的;

Lamport 签名方案特点

1. 可证明上述 Lamport 签名方案是唯密钥攻击下存在性不可伪造的;
2. 消息扩展太严重, 限制了它的使用: 比如当 f 为模指数函数

$$f(x) = \alpha^x \bmod p$$

时, 为了保证 f 的单向性, p 应该要 1024 比特长度, 这意味着每签名 1 比特消息, 均产生 1024 比特签名.

Lamport 签名方案举例

已知 7879 是一个素数, 3 是 $\mathbb{Z}_{7879}^{*}$ 的一个本原元, 定义

$$f(x) = 3^{x} \bmod 7879.$$

假设 $k = 3$, Alice 选择 $2k = 6$ 个随机数

$$\begin{array}{lll} y_{1,0} = 5831, & y_{2,0} = 803, & y_{3,0} = 4285, \\ y_{1,1} = 735, & y_{2,1} = 2467, & y_{3,1} = 6449. \end{array}$$

然后 Alice 计算在函数 f 作用下 6 个 $y_{i,j}$ 的像

$$\begin{array}{lll} z_{1,0} = 2009, & z_{2,0} = 4672, & z_{3,0} = 268, \\ z_{1,1} = 3810, & z_{2,1} = 4721, & z_{3,1} = 5731. \end{array}$$

这些 $z_{i,j}$ 是公开的. 现在假设 Alice 要对消息 $x = (1, 1, 0)$ 签名, 其签名结果为

$$y \triangleq (y_{1,1}, y_{2,1}, y_{3,0}) = (735, 2467, 4285).$$

Lamport 签名方案举例

已知 7879 是一个素数, 3 是 $\mathbb{Z}_{7879}^*$ 的一个本原元, 定义

$$f(x) = 3^x \bmod 7879.$$

假设 $k = 3$, Alice 选择 $2k = 6$ 个随机数

$$\begin{aligned} y_{1,0} &= 5831, & y_{2,0} &= 803, & y_{3,0} &= 4285, \\ y_{1,1} &= 735, & y_{2,1} &= 2467, & y_{3,1} &= 6449. \end{aligned}$$

然后 Alice 计算在函数 f 作用下 6 个 $y_{i,j}$ 的像

$$\begin{aligned} z_{1,0} &= 2009, & z_{2,0} &= 4672, & z_{3,0} &= 268, \\ z_{1,1} &= 3810, & z_{2,1} &= 4721, & z_{3,1} &= 5731. \end{aligned}$$

这些 $z_{i,j}$ 是公开的. 现在假设 Alice 要对消息 $x = (1, 1, 0)$ 签名, 其签名结果为

$$y \triangleq (y_{1,1}, y_{2,1}, y_{3,0}) = (735, 2467, 4285).$$

为了验证消息-签名对 $(x = (1, 1, 0),\ y = (735, 2467, 4285))$, 只需验证下列等式是否成立

$$3^{735} \bmod 7879 = z_{1,1},$$

$$3^{2467} \bmod 7879 = z_{2,1},$$

$$3^{4285} \bmod 7879 = z_{3,0}.$$

全域 Hash 签名方案

此方案给出一种由陷门单向置换构造可证明安全签名方案的方法

此方案给出一种由陷门单向置换构造可证明安全签名方案的方法

全域 Hash 签名方案

设 k 是一个正整数, $f:\{0,1\}^k \to \{0,1\}^k$ 是一个陷门单向置换, $G:\{0,1\}^* \to \{0,1\}^k$ 是一个“随机”函数. 设 $\mathcal{P}=\{0,1\}^*$, 且 $\mathcal{A}=\{0,1\}^k$. 定义密钥 $K=(f,f^{-1},G)$, 其中 f^{-1} 是私钥, (f,G) 是公钥.

对于密钥 $K=(f,f^{-1},G)$, 定义:

$$\mathrm{Sig}_K(x)=f^{-1}(G(x)),\quad x\in\{0,1\}^*,$$

对于消息-签名对 (x,y), 定义

$$\mathrm{Ver}_K(x,y)=\mathrm{True} \Leftrightarrow f(y)=G(x).$$

全域 Hash 签名方案特点

1. 全域 Hash 签名方案名字来源于该签名方案要求随机函数 G (实现时为安全 Hash 函数) 的值域与陷门单向置换 f 的定义域相同;

全域 Hash 签名方案特点

1. 全域 Hash 签名方案名字来源于该签名方案要求随机函数 G (实现时为安全 Hash 函数) 的值域与陷门单向置换 f 的定义域相同;
2. 可证明上述全域 Hash 签名方案是选择消息攻击下存在性不可伪造 (即 EUF-CMA) 的.