

基于门限哈希函数的有效代理签名机制的设计与研究

齐爱琴

(西北民族大学 数学与计算机科学学院 甘肃 兰州 730124)

摘 要: 当今的代理签名技术是在原有签名机制上的改进,无法提供强大的安全保证机制.对比提出了一种基于离散对数的门限哈希函数的方法来构建安全代理签名机制,并提供了详细的安全和性能分析.分析结果显示该机制安全性高、性能稳定.

关键词: 代理签名;哈希函数;离散对数

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2012)04-0131-03

Design and Research of Efficient Proxy Signatures Based on Trapdoor Hash Functions

QI Ai-qin

(School of Mathematics and Computer Science Institute, Northwest University for Nationalities, Lanzhou 730124, China)

Abstract: Unfortunately, most recent constructions of proxy signatures only improve on minor weaknesses of previously built schemes, and can not deliver formal security guarantees. In this study, the paper proposes a technique to construct provably secure proxy signature scheme using trapdoor hash functions and discrete log, then provides the analyses of security and performance. The results show that this proposed scheme achieves superior performance and high security.

Key words: proxy signatures; hash functions; discrete log

1 引言

近些年来,通过加强已有机制的安全性和有效性发展了新的代理签名机制,例如门限代理签名、盲代理签名等^[1-2]. 门限哈希函数是由 Krawczyk 等人^[3]提出的,Mehta 和 Harn 提出了利用门限哈希函数的思想和抗密钥泄漏属性来为每个代理者分配一个代理签名的机制^[4].可是这个方法仅依赖于启发式的安全参数,无法提供强大的安全保证机制.

本文提出了一种基于离散对数和门限哈希函数的方法来构建安全代理签名技术.并提供了相关的安全和性能分析.分析结果显示该机制安全性高、性能稳定.

2 相关假设和说明

假设存在一个公钥证书系统 CA,一个实体可

以关联到 CA 机构的一个证书,这个公钥证书为盲签名实体的身份和它的公钥. CA 负责确保没有两个实体有相同的公钥(公钥是唯一的),CA 也负责区分签名密钥和门限哈希密钥.

假定身份对每个实体是唯一的,不能欺骗和伪造(例如,产生作为公钥哈希的身份).这样用户能唯一地通过公钥来标示,反之亦然.同时,我们也假设存在一个可公开查询使用的公钥目录,实体可以通过这个目录检索到其他实体的公钥作为它们的身份标示.我们也明确定义委任状包含的内容及结构作为我们安全机制的一部分来防止恶意攻击的存在.

3 基于离散对数的门限哈希代理签名方案

当原始签名者因健康、资源限制或其他原因不能履行签名职责时,便将签名权交给代理签名人,由代理签名人代替他履行签名权利.本文设计的基于

离散对数的门限哈希代理签名方案包括初始化阶段、密钥生成阶段、代理签名生成阶段和代理签名验证四个部分。

3.1 系统初始化阶段

可信中心选取系统公共参数 $\text{params} = \langle p, q, \alpha, H, G \rangle$, p, q 为素数且 $q | (p-1)$, α 是 q 的一个本原元, G 和 H 是哈希函数 $\{0, 1\}^* \rightarrow Z_p^*$.

3.2 密钥生成阶段

(1) 原始签名人 D 选取长期私钥 $x \in {}_R Z_p^*$, 计算公钥 $X = \alpha^x$, 代理签名人 P 选取门限密钥 $y \in {}_R Z_p^*$, 计算公共哈希密钥 $Y = \alpha^y \in Z_p^*$.

(2) 原始签名者 D 产生临时(私钥, 公钥)对 $(k \in {}_R Z_p^*, r = \alpha^k \in Z_p^*)$.

(3) 原始签名者 D 产生委任状 w (主要包含原始签名人和代理签名人的身份信息, 代理签名的期限、代签消息种类等), 计算 $\text{TH}_Y(w, r) = \alpha^{hw} Y^r \bmod q$, 而 $hw = H(w \| Y)$, TH 是一个门限哈希函数。

(4) 原始签名者 D 用自己的私钥 k 计算 $t = k + xG(\text{TH}_Y(w, r) \| w \| r) \bmod q$, $\sigma = \langle t, r \rangle$.

(5) 原始签名者 D 形成委托证书 $\text{cert} = \langle \sigma, w \rangle$ 发送给代理签名者 P .

3.3 代理签名生成阶段

代理签名者 P 收到证书 $\text{cert} = \langle \sigma, w \rangle$ 后, 执行以下计算:

(1) 检查 w 和原始签名者的是否一致, 如果检查失败, 忽略此信息。

(2) 计算 $\text{TH}_Y(w, r) = \alpha^{hw+y} \bmod q$ 和 $h = G(\text{TH}_Y(w, r) \| w \| r)$. 如果 $r = \alpha^t X^{-h} \bmod q$, 那么在原始签名者的公钥 X 下的 h 上的签名 $\sigma = \langle t, r \rangle$ 是有效的, 给出接受证书信息, 代理签名人 P 按以下步骤计算代理签名 σp .

(3) 产生(门限密钥、哈希密钥)对 $(z \in {}_R Z_p^*, Z = \alpha^z \in Z_p^*)$.

(4) 计算 $c = z^{-1}(hw - hm + yr) \bmod q$, 而 $hm = H(m \| Z)$.

(5) 代理签名 σp 是 4 元组 $\langle \text{cert}, m, c, hm \rangle$, 将 σp 发送给验证者 V .

3.4 代理签名验证阶段

给定代理签名 σp , 验证者 V 能按以下步骤验证签名的有效性。

(1) 检查消息 m 和委任状 w 的关系是否一致, 如果不一致, 给出代理签名错误的信息。

(2) 从公共目录中查找代理者的公共哈希密钥 Y 和原始签名者的公共密钥 r , 计算 $\text{TH}_Y(w, r) =$

$\alpha^{hw} Y^r \bmod q$ 和 $h = G(\text{TH}_Y(w, r) \| w \| r)$.

(3) 计算 $r' = \alpha^t X^{-h} \bmod q$, 检查是否 $r' \neq r$, 若不相等则输出代理签名 σp 无效的信息。

(4) 计算 $Z' = \alpha^{(hw-hm)c^{-1}} Y^{rc^{-1}} \bmod p$, 检查是否 $hm = H(m \| Z')$, 如果不相等, 输出无效信息, 否则输出代理签名正确有效的信息。

为了使用私钥 $x (x \in {}_R Z_p^*)$ 签名一个消息 m , 原始签名者产生临时密钥对 $(k \in {}_R Z_p^*, r = \alpha^k \in Z_p^*)$, $t = k + xH(m \| r) \bmod q$, 并形成 m 上的签名 $\sigma = \langle t, r \rangle$. 为了验证 σ 关于 m 在公钥 $X = \alpha^x \bmod q$ 上的正确性, 验证者计算 $r' = \alpha^t X^{-h} \bmod q$, 并检查是否 $r' = r \bmod q$, 如果等式成立, 签名 σ 关于 m 在公钥 X 上是有效的, 反之则无效. 为验证代理者 P 的代理签名在消息 m 上的有效性, 验证者只需计算 $Z' = \alpha^{(hw-hm)c^{-1}} Y^{rc^{-1}} \bmod p$, 检查 hm 是否等于 $H(m \| Z')$, 如哈希值相等, 代理签名有效。

4 安全及性能分析

4.1 抗原始签名者关于新委任状的签名伪造

让原始签名者 D 作为委托者, 想去授权签名权利给一个代理签名者 P . TH 是一个门限哈希函数并能计算密钥泄漏碰撞. 在授权期间, 委托者使用代理的哈希密钥产生签名, 即委任状门限哈希值 $\text{TH}_Y(w, r)$ 的签名 σ , 代理使用它的门限密钥 y 来找到 $\langle w', c, Y' \rangle$ 以便 $\text{TH}_Y(w, r) = \text{TH}_{Y'}(w', r)$. 这种行为实际上是伪造一个委托者关于新委任状的签名. 为了阻止这种简单的伪造, 在我们的实现中委托者在授权期间产生一个签名 $\text{TH}_Y(w, r) \| w$ 来代替原有的 $\text{TH}_Y(w, r)$, 现在即使代理能找到在委任状 w 和 w' 之间的一个碰撞使 $\text{TH}_Y(w, r) = \text{TH}_{Y'}(w', r)$, 由于 $\text{TH}_Y(w, r) \| w \neq \text{TH}_{Y'}(w', r) \| w'$, 从而阻止伪造。

4.2 抗委托者的签名伪造

当一个代理者获得了委托者关于消息 $m = \text{TH}_Y(w, r) \| w$ 的签名 σ 后, 依然能伪造一个在 $m' = \text{TH}_{Y'}(w', r) \| w'$ 上的委托者的签名 σ , 其中 $w \neq w'$ 和 $\text{TH}_Y(w, r) = \text{TH}_{Y'}(w', r)$. 为了避免这种伪造情形的出现, 我们可设计签名产生在 $1/m$ 上来代替 m , 并用这种方法区分委托者的标准签名和代理后创建的伪造签名。

4.3 抗碰撞伪造性和基本抗碰撞伪造性

设 TH 是一个关联哈希密钥 Y 的门限哈希函数. 给定系统参数 params 和哈希密钥 Y, Y' 的一个碰撞伪造被定义用于找到一个 $\langle m, r, m', c \rangle$ 以便

$[m \neq m'] \wedge [\text{TH}_Y(m, r) = \text{TH}_{Y'}(m', C)]$. 当 $Y = Y'$ 时, 碰撞叫做一个简单的碰撞, 当 $Y \neq Y'$ 时, 碰撞叫做一个基本碰撞.

让 F 是一个概率上的多项式时间算法, 采用哈希密钥 Y, Y' 和系统参数 params 作为输入, 输出是一个 $\langle m, r, m', c \rangle$. 我们定义概率上的多项式时间算法碰撞伪造 F 的可能性如下:

$$\text{Adv}_F^{\text{CFG}}(\lambda) = \Pr[\text{Col}(F(\text{params}, Y, Y'), Y, Y')].$$

抗碰撞伪造: 门限哈希方案是抗碰撞伪造的. 如所有概率上的多项式时间算法 F 在参数 λ 的情况下输出 $\langle m, r, m', c \rangle$ 满足 $\text{Col}(F(\text{params}, Y, Y'), Y, Y') \wedge [Y = Y']$, $\text{Adv}_F^{\text{CFG}}(\lambda)$ 是可以忽略的.

基本的抗碰撞伪造: 门限哈希方案是基本抗碰撞伪造的. 如果所有概率上的多项式时间算法 F 在参数 λ 的情况下输出 $\langle m, r, m', c \rangle$ 满足 $\text{Col}(F(\text{params}, Y, Y'), Y, Y') \wedge [Y \neq Y']$, $\text{Adv}_F^{\text{CFG}}(\lambda)$ 可忽略.

在基本定义基础上, 我们需要考虑两个情况: (1) 当 $Y = Y'$ 时抗碰撞伪造; (2) 当 $Y \neq Y'$ 时基本的抗碰撞伪造. 由于篇幅限制, 本文只给出 $Y \neq Y'$ 时的基本抗碰撞伪造的证明.

对于 $Y \neq Y'$ 的情况, 假定存在一个概率上的多项式时间算法 F , 给定哈希密钥 Y, Y' 和参数 p, q, α , F 运行一个多项式时间算法输出一个 $\langle m, r, m', c \rangle$ 使得 $m \neq m', r \neq c$ 和不可忽略的 $\text{TH}_Y(m, r) = \text{TH}_{Y'}(m', c)$. 给定 F 我们能构建一个多项式时间算法 g 可以违背离散对数问题: 给定一个离散对数实例 $\langle p, q, \alpha, X \rangle$, g 需要找到 x 使得 $X = \alpha^x \bmod p$, 找到 v 使得 $V = \alpha^v \bmod p$. g 独立地运行伪造 F 的两个实例, F 中的每一个实例用独立的随机数执行 $\langle p, q, \alpha, X, V \rangle$ 作为输入, F 的每个实例产生碰撞伪造 $\langle m_1, r_1, m'_1, c_1 \rangle$ 和 $\langle m_2, r_2, m'_2, c_2 \rangle$, 如果 $m_1 = m_2$ 或者 $r_1 = r_2$ 或者 $m'_1 = m'_2$ 或者 $c_1 = c_2$. 重复 F 的执行, 给定 $\text{TH}_Y(m_1, r_1) = \text{TH}_{Y'}(m'_1, c_1)$ 和 $\text{TH}_Y(m_2, r_2) = \text{TH}_{Y'}(m'_2, c_2)$, 获得两个线性公式:

$$H(m_1 \parallel X) + xr_1 = H(m'_1 \parallel V) + vc_1 \bmod q$$

$$H(m_2 \parallel X) + xr_2 = H(m'_2 \parallel V) + vc_2 \bmod q$$

从而能求解出 x 和 v , 与离散对数问题矛盾, 从而证明结论.

4.4 抗密钥泄露性.

让 TH 是一个关联哈希密钥 Y 的门限哈希函数. 密钥泄露问题能描述如下: 给定系统参数 params 、哈希密钥 Y 和 $\langle m, r, m', r', Y' \rangle$, 使得 $\text{TH}_Y(m, r) = \text{TH}_{Y'}(m', r')$, 密钥泄露问题是找到门

限密钥相应的哈希密钥 Y .

让 K 是一个概率上的多项式时间算法, 采用哈希密钥 $Y, \langle m, r, m', r', Y' \rangle$ 和 params 作为参数输入, 以便 $\text{TH}_Y(m, r) = \text{TH}_{Y'}(m', r')$, 输出相应的哈希密钥 Y 的门限密钥 y , 我们定义概率上的多项式时间算法碰撞伪造 K 的可能性如下:

$$\text{Adv}_K^{\text{Key}}(\lambda) = \Pr[\text{Col}(K(\text{params}, Y, m, r, m', r', Y'), Y) = \text{true}].$$

抗密钥泄露: 门限哈希方案是抗密钥泄露的, 如果如果所有概率上的多项式时间算法 K 在参数 λ 的情况下 $\text{Adv}_K^{\text{Key}}(\lambda)$ 是可以忽略的. 即给定两个元组 $\langle m, r, Y \rangle, \langle m', r', Y' \rangle, m \neq m', r \neq r', Y \neq Y'$ 和 $\text{TH}_Y(m, r) = \text{TH}_{Y'}(m', r')$, 一个多项式时间算法的可能性输出是可忽略的.

证明: 假定这里存在一个多项式的时间算法输出 y' 在一个多项式的时间具有不可忽略性. 哈希函数 Y' 的离散对数能被如下计算:

$$y' = (r')^{-1} (H(m \parallel Y) + y * r - H(m' \parallel Y')) \bmod q.$$

这与已知的离散对数假设相矛盾. 因此门限哈希机制是抗密钥泄露的.

上述方案保证强壮的不可伪造性, 可验证性, 强烈的身份性, 强壮的不可否认性和误用的阻止、抗碰撞伪造、抗密钥泄露等. 安全性高, 性能稳定.

5 结束语

本文描述了一种基于离散对数的哈希门限函数的代理签名方案, 同时提供了包括正确性、安全性和性能的理论分析. 未来, 我们计划用基于密码的线性反馈移位寄存器去提高我们机制的效率.

参考文献:

- [1] 左黎明, 刘二根, 汤鹏志. 一种基于椭圆曲线的代理多重盲签名方案 [J]. 微电子学与计算机, 2010, 27(9): 69-72.
- [2] 秦艳琳, 吴晓平. 对一种代理盲多重签名的分析与改进 [J]. 微电子学与计算机, 2010, 27(10): 37-40.
- [3] Krawczyk H, Rabin T. Chameleon signatures [C] // Proc Network and Distributed System Security Symp NDSS, [s. l.]: the Internet Society, 2000.
- [4] Mehta M, Harn L. Efficient one-time proxy signatures [J]. IEE Proc Commun, 2005, 152(2): 129-133.

作者简介:

齐爱琴 女, (1979—), 硕士, 讲师. 研究方向为网络信息安全.