第36卷 第14期
Vol.36 No.14
计 算 机 工 程
Computer Engineering
2010年7月
July 2010
·安全技术· 文章编号：1000—3428(2010)14—0122—02 文献标识码：A 中图分类号：TP309

前向安全的代理多重数字签名方案

贺 军[1]，李丽娟[2]，李喜梅[1]，唐春明[3,4]
(1. 怀化职业技术学院计算机与信息工程系，怀化 418000；2. 湖南大学计算机与通信学院，长沙 410082；
3. 广州大学数学与信息科学学院，广州 510006；4. 中国科学院软件研究所信息安全国家重点实验室，北京 100080)

摘 要：将前向安全的思想与代理多重数字签名结合，提出一个前向安全的代理多重签名方案，该方案不仅满足一般代理多重签名方案的性质，而且具有前向安全性。在强 RSA 假定、计算式 Diffie-Hellman 问题及有限域上离散对数问题难解的假设下，该方案具有良好的安全性。

关键词：代理多重签名；前向安全；强 RSA 假定；Diffie-Hellman 问题

Proxy Multi-signature Scheme of Forward Security

HE Jun[1], LI Li-juan[2], LI Xi-mei[1], TANG Chun-ming[3,4]
(1. Computer and Information Engineering Department, Huaihua Vocational and Technical College, Huaihua 418000; 2. School of Computer and Communication, Hunan University, Changsha 410082; 3. School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006; 4. State Key Laboratory of Information Security, Institute of Software Science, Chinese Academy of Sciences, Beijing 100080)

【Abstract】 This paper proposes a forward security proxy multi-signature scheme on the basis of the forward-security idea and proxy multi-signature schemes. The new scheme satisfies security properties of general proxy multi-signature schemes and has forward-security. Under the strong RSA assumption, Diffie-Hellman problem and discrete logarithm problem over finite field, the new scheme has good forward security.

【Key words】 proxy multi-signature; forward security; strong RSA assumption; Diffie-Hellman problem

1 概述

在许多应用环境下，人们需要让一个代理签名者同时代表多个原始签名者进行签名，例如，一个公司要发布一份涉及到财务部、人事部、市场部等多个部门的文件，该文件必须由这些部门联合签名才能生效，这些部门也可以委托他们都信任的一个代理人同时代替他们在文件上签字。这个问题可由代理多重签名来解决。然而，目前提出的代理多重签名方案存在一个共同的问题：当代理签名者的代理密钥泄漏后，所有的代理多重签名都是不安全的。

基于前向安全的思想，研究者提出了前向安全的代理签名方案[1-6]，本文在此基础上提出了一个前向安全的代理多重签名方案，该方案不仅满足一般代理多重数字签名方案的性质，而且具有前向安全性，即使代理签名者在某一时段的私钥泄漏，攻击者也无法伪造该时段之前的代理多重签名。

2 基础知识

2.1 前向安全数字签名的相关知识

数字签名的安全应包括 2 个方面：一方面是签名方案的安全性，即数字签名方案抗密码分析的安全性，这一问题可以通过选用著名的数字签名方案并选用大的安全参数来解决；另一方面是签名密钥的安全性，即密钥保管的安全性，常见的方法是采用多个服务器对密钥分布式共享，例如门限签名方案。但是多个服务器的运行成本较高，而且由于操作系统的安全漏洞，极有可能使攻击者获得每个服务器所持有的密钥，因此多个服务器分布式共享密钥的方法所提供的安全性并没有所期望的那样高。

一旦密钥泄漏，签名者用该密钥所进行的所有签名都将是无效的，要做到完全的安全性是不可能的，但总希望在密钥泄漏后对系统的破坏程度降到最低。1997 年，Anderson 提出了前向安全的数字签名的概念，其本质是数字签名安全的风险控制，基本方法是把整个公钥有效时间划分为若干时段，每个时段采用不同的密钥进行签名，而签名验证公钥在整个公钥有效期内保持不变。即使当前时段的签名密钥被泄漏，也不影响此签名时段以前签名的有效性，从而减少了由于密钥泄漏而造成的损失。

2.2 前向安全数字签名中的密钥进化过程

前向安全数字签名的一个重要概念是密钥进化，在系统建立初期，用户首先创建并注册签名验证公钥 PK，获得公钥证书并保存相应的初始私钥 SK_0。假设用户公钥的有效期分为 T 个时段，分别记为 $1,2,\cdots,T$，那么在整个公钥有效期内，公钥是固定的，而签名私钥则随时段不断进化更新，目的在于提供前向安全性。设 SK_i 为第 i $(1\leqslant i\leqslant T)$ 时段的私钥，当系统进入第 i 时段时，首先计算 $SK_i=f(SK_{i-1})$（一般称为密钥进化方程），其中，$f(\cdot)$ 是一个单向函数。得到 SK_i 后，立即删除 SK_{i-1}。这样，攻击者即使在第 i 时段攻入系统时获得 SK_i，仍然无法得到 $SK_{i-1},SK_{i-2},\cdots,SK_0$，因为它们已被删除，并且 SK_i 是由单向函数进化得到的。

密钥的进化过程如图 1 所示。

作者简介：贺 军(1970－)，男，副教授、硕士，主研方向：信息安全；李丽娟，教授、硕士；李喜梅，讲师；唐春明，教授、博士、博士生导师

收稿日期：2010-05-25 **E-mail**：hejunlxmhlq@126.com

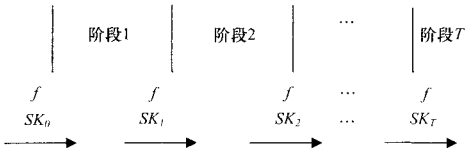

图 1　前向安全数字签名的密钥进化过程

3　前向安全的代理多重数字签名方案

3.1　系统初始化

设 p 和 q 为安全大素数，$N=pq$，整数 $v\in Z_n$ 满足 $gcd(v,(p-1)(q-1))=1$，$A_1,A_2,\cdots,A_n$ 为原始签名者，其私钥为 $x_{A_i}\in Z_N^*(i=1,2,\cdots,n)$，相应的公钥为 $y_{A_i}=x_{A_i}^{-v} \bmod N$ $(i=1,2,\cdots,n)$，B 为代理签名者，私钥为 $x_B\in Z_N^*$，相应的公钥为 $y_B=x_B^{-v^{2^T}} \bmod N$，$h(\cdot)$ 是安全的单向 Hash 函数，系统将公钥有效期划分为 T 个时段，公开 N，$y_{A_i}(i=1,2,\cdots,n)$，y_B，v，T 及 $h(\cdot)$。原始签名者 $A_1,A_2,\cdots,A_n$ 约定并产生代理授权书 m_w，由于代理授权书产生时原始签名者已经确定，因此可以计算原始签名者的公钥乘积 $y=\prod_{i=1}^{n} y_{A_i} \bmod N$，并将 y 写入代理签名授权书 m_w，m_w 中还包括所有原始签名者的身份标识、代理签名者 B 的身份标识、B 的代理权限等。

3.2　代理权产生及验证

代理权产生及验证步骤如下：

(1)每个原始签名者 A_i 随机选取 $k_i\in_R Z_N^*$，并公开 k_i，从而每个原始签名者可以计算 $k=\prod_{i=1}^{n} k_i \bmod N$ 及 $e_1=h(k^v \bmod N\|m_w)\bmod N$，然后 A_i 计算 $\sigma_{A_i}=x_{A_i}^{e_1} \bmod N$，并向 B 秘密发送 (k_i,m_w,σ_{A_i})。

(2)代理签名者 B 收到所有的 (k_i,m_w,σ_{A_i}) 后计算 $k=\prod_{i=1}^{n} k_i \bmod N$ 以及 $e_1=h(k^v \bmod N\|m_w)\bmod N$，验证 $\sigma_{A_i}^v y_{A_i}^{e_1}\stackrel{?}{\equiv}1 \bmod N$，如果对所有原始签名者等式都成立，并且 B 同意 m_w 中的约定，则接受 A_i 的委托，否则拒绝代理。如果 B 接受代理，则计算 $\sigma=\prod_{i=1}^{n}\sigma_{A_i} \bmod N$。

3.3　代理签名者私钥进化及代理密钥生成

令 $x_{B_0}=x_B$ 为代理签名者 B 的初始密钥，系统一旦进入第 $i(1\leqslant i\leqslant T)$ 时段，代理签名者 B 使用 $i-1$ 时段的私钥 $x_{B_{i-1}}$ 生成 i 时段的私钥 $x_{B_i}=x_{B_{i-1}}^2 \bmod N$，得到 x_{B_i} 后立即删除 $x_{B_{i-1}}$，显然有 $x_{B_i}=x_{B_0}^{2^i} \bmod N$。此时，代理签名者 B 计算 $\delta_i=\sigma x_{B_i}^{e_1} \bmod N$ 作为第 i 时段的代理签名密钥。

3.4　代理多重签名生成

设系统进入第 i 时段，待签名的消息为 M，代理签名者 B 随机选取 $r\in_R Z_N^*$，计算 $e=h(r^{v^{2^{T-i}}} \bmod N\|i\|M)$ 以及 $s=r\delta_i^e \bmod N$，消息 M 的代理多重签名为 (M,i,k,m_w,e,s)。

3.5　代理多重签名的验证

代理签名验证者 V 收到签名 (M,i,k,m_w,e,s) 后，计算 $e_1=h(k^v \bmod N\|m_w)\bmod N$，然后计算 $R=s^{v^{2^{T-i}}}(y^{2^{T+1-i}}y_B)^{e_1e} \bmod N$ 以及 $e'=h(R\|i\|M)$，若 $e=e'$，则把签名 (M,i,k,m_w,e,s) 作为合法签名。

4　新方案的性能分析

本文提出的前向安全的代理多重签名方案，在强 RSA 假定、计算式 Diffie-Hellman 问题及有限域上离散对数问题难解的假设下具有良好的安全性。

4.1　可验证性

完整的代理多重签名中包含代理授权书 m_w，描述了原始签名者和代理签名者的身份，代理多重签名的有效性验证实质是验证 $r^{v^{2^{T-i-1}}}\stackrel{?}{\equiv}s^{v^{2^{T+1-i}}}(y^{2^{T+1-i}}y_B)^{e_1e} \bmod N$，其中，$y$ 与 y_B 表明原始签名者同意代理签名，验证式的正确性可由下式证明：

$$s^{v^{2^{T+1-i}}}(y^{2^{T+1-i}}y_B)^{e_1e}\equiv(r\delta_i^e)^{v^{2^{T+1-i}}}((\prod_{i=1}^{n}x_{A_i}^{-v})^{2^{T+1-i}}x_{B_0}^{-v^{2^{T+1}}})^{e_1e}\equiv$$

$$r^{v^{2^{T+1-i}}}(\sigma x_{B_i}^{e_1})^{ev^{2^{T+1-i}}}((\prod_{i=1}^{n}x_{A_i}^{-v})^{2^{T+1-i}}x_{B_0}^{-v^{2^{T+1}}})^{e_1e}\equiv$$

$$r^{v^{2^{T+1-i}}}(x_{B_i}^{e_1}\prod_{i=1}^{n}\sigma_{A_i})^{ev^{2^{T+1-i}}}((\prod_{i=1}^{n}x_{A_i}^{-v})^{2^{T+1-i}}x_{B_0}^{-v^{2^{T+1}}})^{e_1e}\equiv$$

$$r^{v^{2^{T+1-i}}}(x_{B_i}^{e_1}\prod_{i=1}^{n}x_{A_i}^{e_1})^{ev^{2^{T+1-i}}}((\prod_{i=1}^{n}x_{A_i}^{-v})^{2^{T+1-i}}x_{B_0}^{-v^{2^{T+1}}})^{e_1e}\equiv$$

$$r^{v^{2^{T+1-i}}}((\prod_{i=1}^{n}x_{A_i}^{v})^{2^{T+1-i}}x_{B_i}^{v^{2^{T+1}}}(\prod_{i=1}^{n}x_{A_i}^{-v})^{2^{T+1-i}}x_{B_0}^{-v^{2^{T+1}}})^{e_1e}\equiv$$

$$r^{v^{2^{T+1-i}}}((\prod_{i=1}^{n}x_{A_i}^{v})^{2^{T+1-i}}x_{B_0}^{v^{2^i}2^{T+1-i}}(\prod_{i=1}^{n}x_{A_i}^{-v})^{2^{T+1-i}}x_{B_0}^{-v^{2^{T+1}}})^{e_1e}\equiv$$

$$r^{v^{2^{T+1-i}}} \bmod N$$

4.2　安全性

该方案具有一般代理多重签名方案所具有的安全性。

(1)强不可伪造性

任何攻击者都不能伪造代理签名者在 i 时段的代理签名。假如攻击者能够伪造代理签名，那么他必能伪造一组数 (M,i,k,m_w,e',s') 满足以下式子：

$$e_1=h(k^v \bmod N\|m_w)\bmod N$$

$$R'=s'^{v^{2^{T+1-i}}}(y^{2^{T+1-i}}y_B)^{e_1e'} \bmod N$$

$$e'=h(R'\|i\|M)$$

事实上，如果取定 s' 则无法确定 e'；如果取定 e' 求 s'，那么必须由 $e'=h(R'\|i\|M)$ 得到 R'，然后由 R' 及 $R'=s'^{v^{2^{T+1-i}}}(y^{2^{T+1-i}}y_B)^{e_1e'} \bmod N$ 得到 s'，这与 $h(\cdot)$ 是安全的 Hash 函数及强 RSA 假定矛盾。另一方面，攻击者也无法直接伪造代理签名密钥 $\delta_i=\sigma x_{B_i}^{e_1} \bmod N$，因为攻击者无法得到 σ 和 x_{B_i}。即使所有原始签名者联合也不能伪造代理密钥，因为他们只知道 σ，不能得到代理签名者在 i 时段的私钥 x_{B_i}。

(2)代理授权书 m_w 不可伪造

A_i 如果可以伪造 (k_i,m_w,σ_{A_i}) 使其通过验证式 $\sigma_{A_i}^v y_{A_i}^{e_1}\stackrel{?}{\equiv}1 \bmod N$，那么有 2 种方法：如果取定 k_i 及 m_w，由于 $e_1=h(k^v \bmod N\|m_w)\bmod N$，$e_1$ 确定，必须由 $\sigma_{A_i}^v y_{A_i}^{e_1}\stackrel{?}{\equiv}1 \bmod N$ 求出 σ_{A_i}，由强 RSA 假定，这是困难的。如果取定 k_i 及 σ_{A_i}，必须由 $\sigma_{A_i}^v y_{A_i}^{e_1}\stackrel{?}{\equiv}1 \bmod N$ 求出 e_1，然后由 $e_1=h(k^v \bmod N\|m_w)\bmod N$ 得到 m_w，这与 $h(\cdot)$ 是安全的 Hash 函数矛盾。如果取定 σ_{A_i} 及 m_w，则需由 $\sigma_{A_i}^v y_{A_i}^{e_1}\stackrel{?}{\equiv}1 \bmod N$ 求出 e_1，然后由 $e_1=h(k^v \bmod N\|m_w)\bmod N$ 得到 k_i，这也与 $h(\cdot)$ 是安全的 Hash 函数矛盾。所以，A_i 不能伪造 m_w。同时代理签名者 B 也不能伪造代理授权书 m_w，否则 B 能找到 m_w' 满足 $h(k^v \bmod N\|m_w')\equiv h(k^v \bmod N\|m_w)\bmod N$，这也与 $h(\cdot)$ 是安全的 Hash 函数矛盾，因此，m_w 不可伪造。由于 m_w 中包括所有

(下转第 126 页)

因此，有如下结论：

$$\left|(E_b(E_a(S_x^1))\cap(E_a(E_b(S_y^0))\right|=\left|S_x^1\cap S_y^0\right|=k$$

令 $S_1(x,f_1(x,y))=\{x,r_1',E_a(S_x^1),E_b(S_y^0),E_a(E_b(S_y^0))\}$，则有

$$S_1(x,f_1(x,y),f_2(x,y))=\{x,r_1',E_a(S_x^1),E_b(S_y^0),E_a(E_b(S_y^0)),k\}$$

$$\{VIEW_1^{\pi}(x,y),OUTPUT_2^{\pi}(x,y)\}=\{x,r_1,E_a(S_x^1),E_b(S_y^0),E_a(E_b(S_y^0)),k\}$$

由此可以推出

$$\{S_1(x,f_1(x,y)),f_2(x,y)\}_{x,y}\overset{c}{\equiv}\{(VIEW_1^{\pi}(x,y),OUTPUT_2^{\pi}(x,y)\}_{x,y}$$

用类似的方法还可以构造一个模拟器 S_2，使得

$$\{(f_1(x,y)),S_2(y,f_2(x,y))\}_{x,y}\overset{c}{\equiv}\{(OUTPUT_1^{\pi}(x,y),VIEW_2^{\pi}(x,y)\}_{x,y}$$

这样就完成了定理的证明。

4.2 效率分析

作为安全多方计算协议的一个重要组成模块，百万富翁问题解决方案的效率直接影响整个安全多方计算协议的效率。下面针对本文提出的协议分析其计算及通信复杂度，并与其他相关的百万富翁问题解决方案进行比较。

(1)计算复杂度：假设 $0<\max(|x|,|y|)=n$，其中，$|x|$（$|y|$）表示输入 x（y）的长度(二进制形式)。本文方案需要 $O(n)$ 次加解密运算。需要注意的是，与其他解决方案中公钥密码系统的加解密运算不同，本文方案采用的是对称的可交换加密函数，其加解密效率高于其他方案。另外，虽然模指数运算是隐藏信息的一种常用技术手段，但该运算需要消耗大量的计算资源，而本文方案不需要复杂的模指数运算(加解密算法中除外)，在这一点上，计算复杂度大大降低，其他简单运算需要 $O(n^2)$。相关方案计算复杂度比较结果见表 1。

表 1 各方案计算及通信复杂度比较

解决方案	计算复杂度			通信复杂度
	加解密	模指数运算	其他运算	
文献[1]方案	$O(2^n)$	$O(2^n)$	$O(2^{2^n})$	3
文献[3]方案	无	$O(n)$	$O(2^n)$	$O(n)$
文献[5]方案	无	$O(1)$	$O(2^n)$	3
本文方案	$O(n)$	无	$O(n^2)$	4

(2)通信复杂度：衡量一个计算方案效率的首要指标是其计算复杂度，但是对于安全多方计算来说，仅计算复杂度无法全面地描述一个解决方案的优劣。在安全多方计算中，参与方相互之间要进行通信，而在通信过程中，所有参与方都需要等待自己所需的数据，因此，通信复杂度也是衡量安全多方计算效率的一个重要指标。本文用通信的轮数表示通信复杂度，提出的解决方案包括 3 轮用以传输加密结果的通信，1 轮传输最终比较结果的通信，总的通信复杂度为 4 轮。由表 1 可以看出，本文的解决方案整体性能优于其他方案。

5 结束语

本文利用 0 编码与 1 编码构造了一种新的百万富翁问题解决方案。该方案避免了复杂的模指数运算，有效地减小了计算与通信复杂度，同时利用安全多方计算中理想模型与现实协议相比较的方法，证明了方案的安全性。因此，本文方案是一个安全的解决方案，高效地解决了无信息泄漏的数值比较问题。

参考文献

[1] Yao A C. Protocols for Secure Computation[C]//Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science. Los Alamitos, CA, USA: IEEE Computer Society Press, 1982: 160-164.

[2] Goldreich O, Micali S, Wigerson A. How to Play Any Mental Game[C]//Proceedings of the 19th Annual ACM Conference on Theory of Computing. New York, USA: ACM Press, 1987: 218-229.

[3] Ioannidis I, Grama A. An Efficient Protocol for Yao's Millionaires' Problem[C]//Proceedings of the 36th Hawaii International Conference on System Sciences. Hawaii, USA: [s. n.], 2003.

[4] Schoenmakers B, Tuyls P. Practical Two-party Computation Based on the Conditional Gate[C]//Proceedings of Asiacrypt'04. Jeju, Korea: [s. n.], 2004.

[5] Li Shundong, Dai Yiqi, You Qiyou. An Efficient Solution to Yao's Millionaires' Problem[J]. ACTA Electronica Sinica, 2005, 33(5): 769-773.

编辑 张正兴

(上接第 123 页)

原始签名者的身份标识、代理签名者 B 的身份标识及 B 的代理权限，使得本文提出的方案还具有强可识别性、强不可否认性及抗滥用性。

(3)安全性的其他方面

该方案中规定了代理终止时间 $\tilde{t}$，从而具有限制代理权期限的功能；代理授权过程无需安全信道，便于实现；签名验证同时使用原始签名者和代理签名者的公钥，有效地分离了签名权和代理权。

4.3 前向安全性

在特殊的情况下，代理签名者第 i 时段的代理签名密钥泄漏，由于 $\delta_i=\sigma x_{B_i}^{e_i} \bmod N$ 攻击者无法得到 x_{B_i}，即使是原始签名人联合也只能得到 $x_{B_i}^{e_i} \bmod N$，由强 RSA 假定还是不能求出 x_{B_i}。即使是更不幸的情况，代理签名者第 i 时段的私钥 x_{B_i} 泄漏，攻击者仍无法伪造代理签名者在第 $j(j<i)$ 时段的代理签名，因为由强RSA 假定攻击者无法从 $x_{B_j}=x_{B_{j+1}}^2 \bmod N=x_{B_{j+2}}^{2^2} \bmod N=\cdots=x_{B_i}^{2^{i-j}} \bmod N$ 得到 x_{B_j}。因而本文提出的方案具有前向安全性。

5 结束语

在传统的代理多重签名方案中，仍没有有效的方法解决如何减少由于代理者私钥或是代理密钥泄漏所带来的损失。本文基于前向安全的思想提出了一个前向安全的代理多重签名方案，在 Hash 函数的安全性假设及强 RSA 假定下分析了方案的安全性，证明该方案不仅满足一般代理多重签名方案的安全性，而且具有前向安全性。

参考文献

[1] 牛江品，张建中. 基于双线性对的前向安全代理签名方案[J]. 计算机工程, 2009, 35(6): 164-165.

[2] 陈海滨，杨晓元，梁中银，等. 一种无证书的前向安全代理签名方案[J]. 计算机工程, 2010, 36(2):156-157.

[3] 王玲玲，张国印，马春光. 基于环 Zn 上圆锥曲线的前向安全环签名方案[J]. 计算机工程, 2008, 34(6): 33-34.

[4] Abdalla M, Reyzin L. A New Forward-secure Digital Signature Scheme[C]//Proc. of Asiacrypt'76. Berlin, Germany: Springer, 1976: 116-129.

[5] 王玲玲，张国印，马春光. 前向安全的多重数字签名方案[J]. 计算机学报, 2004, 27(9): 1177-1181.

[6] Itkins G, Reyzin L. Forward-secure Signatures with Optimal Signing and Verifying[C]//Proc. of Crypto'01. Berlin, Germany: Springer, 2001: 332-354.

编辑 索书志