A Forward-Secure Threshold Signature Scheme Based on Multiplicative Secret Sharing

LU Dian-jun[1], Li Xin-yan[2], Wang Yun[3], Zhang Bing-ru[1]

1. Department of Mathematics and Information Science, Qinghai Normal University, Xining, China

2. Department of Mathematics, Changjiang normal college, Chongqing, China

3. Grown-up Education College, Qinghai University, Xining, China;

Email: LDJ@qhnu.edu.cn

Abstract: A new forward-secure threshold digital signature scheme which based on multiplicative secret sharing is put forward in this paper. The scheme has the following property: even if more than the threshold numbers of players are compromised, it is not possible to forge signature relating players to the past. This property is achieved while keeping the public key fixed and updating the secret keys at regular intervals. Having been added a refresh protocol, this scheme can tolerate mobile eavesdropping adversaries.

Key words: digital signature; threshold cryptography; forward security; multiplicative secret sharing

基于乘法共享的前向安全的门限签名方案

芦殿军[1]，李欣妍[2]，王云[3]，张秉儒[1]

1. 青海师范大学数学与信息科学系，青海西宁 中国 810008

2. 长江师范学院数学系，重庆涪陵 中国 408100

3. 青海大学成教学院，青海西宁 中国 810006

Email: LDJ@qhnu.edu.cn

【摘要】提出了一个新的基于乘法共享的前向安全的门限数字签名方案，该方案有如下特点：即使有多于门限数的成员被收买，也不能伪造有关过去的签名；同时，可以保持公钥的固定性和在规则的时间间隔内更新密钥。添加一个再更新算法后，该方案可抵御动态窃听敌手。

【关键词】数字签名；门限密码学；前向安全性；乘法共享

1 引言

一个密钥因“非密码学”的原因而泄露，是对很多密码学方案的最大威胁。通常，大部分补救措施是利用秘密共享[1-2]的方法将密钥分布式地存放在多台服务器上，这种思想的具体体现就是门限签名方案[3-6]。由于签名是在一种分布式的基于秘密共享的环境中进行，敌手为了获得密钥和产生签名必须收买足够多的成员。

尽管分布式的密钥存放使得它更难被敌手获得，但是风险依然存在。作为安全性的第二道防线，文[7]建议提供前向安全性到门限方案中，以减轻由密钥完全暴露所引起的危险。

数字签名的前向安全性由 ANDERSON[8]首次提出，解决问题的方法由 BELLARE[9]等人设计。通过密钥演化运算，他们针对单签名者设计和达到了目的：从一个初始的密钥开始，使用者利用“演化”程序在每一个时间段的最后更新当前的密钥以阻止后来成功进入系统的敌手获得它。

数字签名的前向安全性使得敌手仅能够伪造密钥暴露以后时间段的签名，而不能伪造之前的签名。继 BELLARE[9]之后，文献[10-13]又提出了一些其它改进方案，这些改进旨在使方案更为简单、实用。

将数字签名的前向安全性结合到门限签名中的思想由 ABDALLA[7]等人最先提出。他们认为即使一个敌手控制了所有的成员服务器并且完全掌握了密钥，结合前向安全性和门限密码学，也能够得到一种提高安全性保证的方案。实际上，在他们所构造的方案中，敌手不能用攻破后时间段的密钥来伪造攻破前时间段的签名，所以有关“过去”的签名及密钥的所有知识对于敌手来说是无用的。

本文在 ABDALLA[7]的基础上，采用乘法共享的方法，提出了一种新的前向安全的门限数字签名方案，

基金项目：国家自然科学基金资助项目（60863006）

Foundation Item: The National Natural Science Foundation of China **(60863006)**.

它满足：收买任意少于门限数目个成员的窃听敌手不能伪造签名；收买大于等于门限数目个成员的窃听敌手虽然可以知道当前密钥，却不能伪造当前时间周期之前的签名。方案实现十分简单，使用的密钥也很短，在参与成员 $n=t+1$ 时，可抵御收买 t 个成员的窃听敌手。假设因式分解是困难的，方案在随机预言模型下对于窃听敌手是前向安全的。

2 定义和模型

2.1 通信模式

方案的参与者有 n 个成员，他们被一个广播信道连接，并且能够通过秘密信道进行私人的点到点之间的通信（这样的信道可以由广播信道使用密码学技术得到），假设在设置阶段存在一个可信中心，每个成员均可以进行广播通信和点到点通信。

2.2 敌手的类型

按照敌手所拥有的攻击能力，可分为：(1) 窃听敌手：能获得一个成员的秘密信息，但不能通过任何方式来影响他的行为的敌手；(2) 可中断敌手：不仅能够窃听，而且能够阻止该成员对进程的参与的敌手。(3) 恶意敌手：可以引起一个成员在进程中以不受任何约束的方式违反常规的敌手。

按照敌手的行为模式，可分为：(1) 静态敌手：他在进程开始之前就已经决定了要攻击的成员。(2) 可适应敌手：他可以在进程的运行中随着信息的获得即时地决定被攻击的成员。(3) 动态敌手：他不仅是可适应的，而且能够决定在不同的时间段控制不同的成员。

2.3 前向安全的门限签名

一个 (t,k,n) 门限签名方案是这样的，密钥被分配在 n 个成员中，由 k 个诚实成员合作生成签名，任意掌握了 t 个或少于 t 个密钥份额的敌手不能伪造签名。

本文所讨论的前向安全的门限签名方案 (t,k_s,k_u,n) 使用密钥演化算法，且整个生存期被分成若干个时间段，密钥在不同的时间段内不同，而公钥则是固定的。方案由以下几个阶段组成：

密钥生成阶段：给定一个秘密的参数 k，生成公钥和密钥后分配给所有的成员，该阶段可以由一个可信中心完成，也可以由成员共同完成。

密钥更新阶段：在每一个时间段的开始，k_u 个成员执行更新算法，该算法为签名方案修改密钥，执行完更新算法后，每一个未被攻破的成员将有一个新的时间段中的秘密份额。作为更新算法的一部分，前向安全的方案要求已更新时间段之前的密钥从使用者的机器中删除掉，否则，攻入使用者机器的敌手将获得较早时间段的签名密钥，并进而具有对较早时间段产生签名的能力。

签名生成阶段：k_s 个成员执行签名运算，该算法在当前时间段使用密钥对信息 m 产生一个签名。签名是一个二元组，包括当前时间段及一个标签。假如所有的成员是诚实的，那么签名将被验证算法所接受。

签名验证阶段：与普通的数字签名算法一样，验证算法能被任意拥有公钥的个体执行。对于一个给定的信息，它通过返回“接受”或“拒绝”来指明一个特定的签名是否是有效的。如果对一个消息-签名对执行了验证算法后返回“接受”，我们就说在时间段 j 对消息 m 的签名 $\langle j,tag\rangle$ 是有效的。

2.4 注释：

方案中有 n 个成员，时间段的总数被标记为 T，全部的公钥记为 PK 且由 l 个值构成，记为 $U_1,U_2,\cdots,U_l$。在每一个时间段 j，相应的密钥的 l 个组成部分记为 $S_{1,j},S_{2,j},\cdots,S_{l,j}$，它们被所有的成员共享，成员 ρ 掌握的第 j 个时间段的第 i 个密钥值的份额 $S_{i,j}$ 记为 $S_{i,j}^{(\rho)}$，全部（l 个值）秘密信息记为 $SK_j^{(\rho)}$。一般地，记号 $X^{(\rho)}$ 指的是 ρ 掌握的 X 的份额。

3 方案描述

用 MFST 表示一个基于乘法共享的 $(t,t+1,t+,t+1)$-门限签名方案，当分享值 X 的时候，每一个成员随机地选取 $X^{(\rho)}$，对于给定的模 N，它们满足 $X\equiv X^{(1)}X^{(2)}\cdots X^{(n)}(\mathrm{mod}\,N)$，该方案的优点是即使存在 $n-1$ 个被收买成员（总数为 n），秘密信息也不会泄露。但在签名和更新进程中均要求有 n 个诚实成员参与。

3.1 方案构造

方案的每一个部分都要求成员进行交互，一个可信中心执行密钥生成运算，它生成和发送初始密钥的份额给每一个成员。每一个成员单独执行密钥演化进程而不需要彼此交互，签名生成要求所有 n 个成员参与，验证可以由任意拥有公钥的个体执行，不需要参与者交互。

本文提出的 MFST 方案描述如下：

3.1.1 MFST.keygen(k,T) 初始化算法

1) 可信中心随机地选取不同的 $k/2$ 比特的素数 p,q，满足 $p\equiv q\equiv 3(\mathrm{mod}\,N)$

2) 可信中心设置 $N=p\cdot q$

3) 对于 $i=1,2,\cdots,l$ 循环

978-1-935068-01-3 © 2009 SciRes.

a) 对于 $\rho=1,2,\cdots,n$ 循环：
可信中心随机地选取 $S_{i,0}^{(\rho)} \in_R Z_N^*$
b) 可信中心计算：
$S_{i,0} \equiv \prod_{\rho=1}^{n} S_{i,0}^{(\rho)} \pmod N$ 和 $U_i \equiv \left(S_{i,0}^{2^{(T+1)}}\right)^{-1} \pmod N$

4) 对于 $\rho=1,2,\cdots,n$ 循环：
a) 可信中心设置：
$SK_0^{(\rho)} = \left(N,T,0,S_{1,0}^{(\rho)},S_{2,0}^{(\rho)},\cdots,S_{l,0}^{(\rho)}\right)$
b) 可信中心对成员 ρ 发送 $SK_0^{(\rho)}$

5) 可信中心设置 $PK=(N,T,U_1,U_2,\cdots,U_l)$ 且公布它

3.1.2 MFST.sign(m,j)签名算法

1) 对于 $\rho=1,2,\cdots,n$ 循环：
a) 成员 ρ 选取一个随机数 $R^{(\rho)} \in_R Z_N^*$
b) 成员 ρ 计算 $Y^{(\rho)} \equiv \left(R^{(\rho)}\right)^{2^{(T+1-j)}} \pmod N$ 并广播它

2) 所有的成员单独地：
a) 计算 $Y \equiv Y^{(1)} \cdot Y^{(2)} \cdots Y^{(n)} \pmod N$
b) 计算 $\delta = H(j,Y,m)$

3) 对于 $\rho=1,2,\cdots,n$ 循环：成员 ρ 计算 $Z^{(\rho)} \equiv R^{(\rho)} \prod_{i=1}^{l} \left(S_{i,j}^{(\rho)}\right)^{\delta} \pmod N$ 并广播它

4) 所有的成员计算：$Z \equiv Z^{(1)}Z^{(2)}\cdots Z^{(n)} \pmod N$

5) 对于消息 m 的签名是 $\langle j,\langle Y,Z\rangle\rangle$ 并且公开它

3.1.3 MFST.verify$_{PK}(m,\gamma)$验证算法

1) 将 γ 当作 $\langle j,\langle Y,Z\rangle\rangle$
2) 如果 $Y \equiv 0 \pmod N$ 则返回 0
3) $\delta = H(j,Y,m)$
4) 如果 $Y \equiv Z^{2^{(T+1-j)}} \cdot \prod_{i=1}^{l} U_i^{\delta} \pmod N$ 则返回 1，否则返回 0

3.1.4 MFST.update(j)密钥更新算法

1) 如果 $j=T$，则返回一个空串，否则继续
2) 对于 $\rho=1,2,\cdots,n$ 循环：
a) 对于 $i=1,2,\cdots,l$ 循环：每一个成员 ρ 计算 $S_{i,j}^{(\rho)} = \left(S_{i,j-1}^{(\rho)}\right)^2 \pmod N$
b) 每一个成员 ρ 从他们的计算机中删除 $SK_{j-1}^{(\rho)}$

3.2 方案的强化

以上方案对于可适应的窃听敌手是安全的，为了抵御动态窃听敌手，还需要增加一个再更新算法，该算法在每一轮更新阶段的最后执行。这使得一个敌手可能已经获得的可以优先执行更新进程的关于密钥份额的任何知识变得毫无用处。为了完成密钥的再更新，每一个成员分配一个份额，然后用当前份额乘以所有的在更新阶段获得的份额（包括它自己生成的份额）。

再更新算法：每一个成员 i 在再更新进程中的参与方式是，随机地选取 n 个数 $x_1^{(i)},x_2^{(i)},\cdots,x_n^{(i)}$ 使得 $\prod_{j=1}^{n} x_j^{(i)} \equiv 1 \pmod N$，然后对于每一个 $j \in \{1,2,\cdots,n\}$，i 通过一个私人的信道发送 $x_j^{(i)}$ 的值给成员 j。一旦成员 j 接收到所有其他成员的值，他用当前份额的乘积 $\prod_{i=1}^{l} x_j^{(i)} \pmod N$ 来计算他的新的秘密的份额。

4 安全性分析

定理 4.1：在所提出的门限签名方案 MFST$(t,t+1,t+,t+1)$ 中，若 MFST.keygen(k,T) 初始化算法产生的公钥为 $PK=(N,T,U_1,U_2,\cdots,U_l)$，为每个成员 ρ 产生的份额为 $SK_0^{(\rho)} = \left(N,T,0,S_{1,0}^{(\rho)},S_{2,0}^{(\rho)},\cdots,S_{l,0}^{(\rho)}\right)$，MFST.update$(j)$ 算法为密钥份额进行更新，MFST.sign(m,j) 为消息 m 产生的签名是 $\langle j,\langle Y,Z\rangle\rangle$，则 $\langle j,\langle Y,Z\rangle\rangle$ 是 m 的有效签名。

证明：为了验证 $\langle j,\langle Y,Z\rangle\rangle$ 是 m 的有效签名，需要验证 $Y \equiv Z^{2^{(T+1-j)}} \cdot \prod_{i=1}^{l} U_i^{\delta} \pmod N$ 成立，若所得信息均由方案产生，则 $\delta = H(j,Y,m)$，$Y^{(\rho)} \equiv \left(R^{(\rho)}\right)^{2^{(T+1-j)}} \pmod N$，$Y \equiv Y^{(1)} \cdot Y^{(2)} \cdots Y^{(n)} \pmod N$，$U_i \equiv \left(S_{i,0}^{2^{(T+1)}}\right)^{-1} \pmod N$，$S_{i,0} \equiv \prod_{\rho=1}^{n} S_{i,0}^{(\rho)} \pmod N$，$S_{i,j} \equiv \prod_{\rho=1}^{n} S_{i,j}^{(\rho)} \pmod N$，$Z^{(\rho)} \equiv R^{(\rho)} \prod_{i=1}^{l} \left(S_{i,j}^{(\rho)}\right)^{\delta} \pmod N$，$Z \equiv Z^{(1)}Z^{(2)}\cdots Z^{(n)} \pmod N$，

因为：$S_{i,j}^{(\rho)} \equiv \left(S_{i,j-1}^{(\rho)}\right)^1 \equiv \left(S_{i,j-2}^{(\rho)}\right)^2 \equiv \cdots \equiv \left(S_{i,0}^{(\rho)}\right)^{2^j} \pmod N$

所以：$\left(S_{i,0}^{(\rho)}\right) \equiv \left(S_{i,j}^{(\rho)}\right)^{2^{-j}} \pmod N$，

进而 $S_{i,0} \equiv \prod_{\rho=1}^{n} S_{i,0}^{(\rho)} \equiv \left(\prod_{\rho=1}^{n} S_{i,j}^{(\rho)}\right)^{2^{-j}} \pmod N$

因此：$Z^{2^{(T+1-j)}} \cdot \prod_{i=1}^{l} U_i^{\delta} \equiv \left(\prod_{\rho=1}^{n} Z^{(\rho)}\right)^{2^{(T+1-j)}} \cdot \prod_{i=1}^{l} \left(S_{i,j}^{2^{(T+1)}}\right)^{-\delta}$

$$\equiv \left(\prod_{\rho=1}^{n} R^{(\rho)} \prod_{i=1}^{l} \left(S_{i,j}^{(\rho)}\right)^{\delta}\right)^{2^{(T+1-j)}} \cdot \prod_{i=1}^{l} S_{i,0}^{-\delta 2^{(T+1)}}$$

$$\equiv \left(\prod_{\rho=1}^{n} R^{(\rho)}\right)^{2^{(T+1-j)}} \cdot \left(\prod_{i=1}^{l}\prod_{\rho=1}^{n} \left(S_{i,j}^{(\rho)}\right)^{\delta}\right)^{2^{(T+1-j)}} \cdot \prod_{i=1}^{l} \left(\prod_{\rho=1}^{n} \left(S_{i,0}^{(\rho)}\right)\right)^{-\delta \cdot 2^{(T+1)}}$$

$$\equiv \prod_{\rho=1}^{n} Y^{(\rho)} \cdot \left(\prod_{i=1}^{l} S_{i,j}\right)^{\delta \cdot 2^{(T+1-j)}} \cdot \prod_{i=1}^{l} \left(S_{i,0}\right)^{-\delta \cdot 2^{(T+1)}}$$

$$\equiv \prod_{\rho=1}^{n} Y^{(\rho)} \cdot \left(\prod_{i=1}^{l} S_{i,j}\right)^{\delta \cdot 2^{(T+1-j)}} \cdot \prod_{i=1}^{l} \left(S_{i,j}\right)^{-\delta \cdot 2^{(T+1-j)}} \equiv Y \pmod N$$

这样我们证明了 $Y \equiv Z^{2^{(T+1-j)}} \cdot \prod_{i=1}^{l} U_i^{\delta} \pmod N$ 成立，所以 $\langle j, \langle Y, Z \rangle \rangle$ 是 m 的有效签名。

定理 4.2：本文所构造的方案 MFST$(t, t+1, t+, t+1)$ 为前向安全的门限数字签名方案。

证明：本定理的证明建立在单成员 FS 签名方案基础之上，采用文献[9]中的证明思想，并使用模拟敌手在协议中的观察方法。令 F 表示对方案攻击的敌手，希望构造出一种针对前向安全性攻击的算法。F 的攻击分 3 个阶段进行：选择明文攻击阶段；超门限阶段；伪造阶段。对 F 的攻击过程概要描述如下：

在选择明文攻击阶段，敌手将他选择的消息对 *MFST.sign* 算法提出质疑，假设他可以查询随机预言 H（H 是在 *MFST.sign* 算法中使用的公共 Hash 函数），在这个阶段他可以攻入服务器并且掌握秘密的份额，但是对于窃听敌手而言，在任意一个时间段只有不多于 t 个密钥的份额泄露。注意到如果一个成员在更新算法期间被收买，我们就认为该成员在当前期和紧挨的之前期两个时间段中被收买了。在门限方案中，这是一个标准的阶段，因为一个成员在更新阶段所掌握的秘密信息包含这两个时间段的秘密。

在超门限阶段，对于一个特定的时间段 b 来说，敌手可能获得 $t+1$ 或更多的成员的密钥的份额，这使得敌手可以计算出密钥。为了伪造中的简单性，我们给敌手全部的当前系统的情形（例如：实际的密钥和所有的当前阶段的密钥的份额）。如果敌手选择 b 作为恰好下一个时间段，而该段密钥被定义为空串所以敌手不能掌握秘密信息。

在伪造阶段，敌手对信息 m 和时间段 k 输出一个消息-签名对 $(m, \langle k, tag \rangle)$。假如 m 在时间段 k，在选择明文攻击阶段没有被提出质疑并且同时满足以下两条则认为敌手成功了：(1)他的输出被 *MFST.verify* 接受，并且 k 比敌手进入超门限阶段的时间段 b 更早。(2)他能够输出一个被 *MFST.verify* 接受的消息-签名对，而且没有收买多于 t 个成员。由于 *MFST* 算法的特点是即使存在 $n-1$ 个被收买的成员，秘密信息也不会泄露，故以上两条均不能满足，所以该方案对于动态窃听敌手来说，具有前向安全性。

5 结束语

本文在 Abdalla [7]等人的基础上，采用乘法秘密共享的方法，提出了一种新的前向安全的门限数字签名方案。该方案具备如下优势：收买任意少于门限数目个成员的敌手不能伪造签名；收买大于或等于门限数目个成员的敌手虽然可以知道当前密钥，却不能伪造当前时间周期之前的签名；可抵御动态窃听敌手。

References (参考文献)

[1] ITO M, SAITO A, MATSUMOTO T. Secret sharing scheme realizing general access structure[A]. LOBECOM Tokyo'87 [C]. Tokyo: IEEE, 1987. 99-102

[2] SIMMONS G. An introduction to shared secret and/or shared control schemes and their application in Contemporary Cryptology [J]. The Science of Information Integrity, 1992, 441-497

[3] DESMEDT Y, FRANKEL Y. Shared generation of authenticators and signatures [A]. In: Feigenbaum J, editor. Advances in Cryptology - CRYPTO '91 [C]. Berlin: Springer-Verlag, 1991. 457-469

[4] DESMEDT Y. Threshold cryptosystems [A]. In: Seberry J, Zheng Y, editors. Advances in Cryptology-AUSCRYPT'92[C]. Berlin: Springer –Verlag, 1993. 3-14

[5] PEDERSEN T. A threshold cryptosystem without a trusted party [A]. In: Davies D W, editor. Advances in Cryptology-EUROCRYPT'91[C]. Berlin: Springer-Verlag, 1991. 522-526

[6] SHOUP V. Practical threshold signatures [A]. In: Preneel B, editor. Advances in Cryptology-EUROCRYPT 2000[C]. Berlin: Springer –Verlag, 2000. 207-220

[7] ABDALLA M, MINER S, NAMPREMPRE C. Forward-secure threshold signature schemes [A]. In: Naccache D, editor. Cryptology-CT-RSA 2001[C]. Berlin: Springer-Verlag, 2001. 441-456

[8] Anderson R. Two remarks on public-key cryptology[R]. Relevant material presented by the author in an invited lecture at the ACM CCS' 97, 1997

[9] BELLARE M, MINER S. A forward-secure digital signature scheme [A]. In: Wiener M, editor. Advances in Cryptology-CRYPTO' 99 [C]. Berlin: Springer-Verlag, 1999. 431-448

[10] ABDALLA M, REYZIN L. A new forward-secure digital signature scheme [A]. In: Okamoto T, editor. Asiacrypt 2000[C]. Berlin: Springer –Verlag, 2000.116-129

[11] ITKIS G, REYZIN L. Forward-secure signatures with optimal signing and verifying [A]. In: Kilian J, editor. CRYPTO 2001[C]. Berlin: Springer-Verlag, 2001. 499-514

[12] KOZLOV A, REYZIN L. Forward-secure signatures with fast key update [A]. In: Cimato S, editor. Security in communication networks[C]. Berlin: Springer-Verlag, 2002. 247-262

[13] Lu Dianjun, Zhang Bingru, zhao Haixing. A forward-secure threshold signature scheme based on polynomial secret sharing [J]. Journal on Communications, 2009, 30(1): 45-49(in Chinese)

978-1-935068-01-3 © 2009 SciRes.