ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.11, November 2010, pp.2920−2932
doi: 10.3724/SP.J.1001.2010.03834

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

标准模型下的前向安全多重签名:安全性模型和构造*

于 佳[1+], 郝 蓉[1], 孔凡玉[2,3], 程相国[1], GUO Xiang-Fa[4]

[1](青岛大学 信息工程学院,山东 青岛 266071)

[2](山东大学 网络信息安全研究所,山东 济南 250100)

[3](密码技术与信息安全教育部重点实验室,山东 济南 250100)

[4](Department of Computer Science, National University of Singapore, Singapore 117590, Singapore)

Forward-Secure Multi-Signature in the Standard Model: Security Model and Construction

YU Jia[1+], HAO Rong[1], KONG Fan-Yu[2,3], CHENG Xiang-Guo[1], GUO Xiang-Fa[4]

[1](College of Information Engineering, Qingdao University, Qingdao 266071, China)

[2](Institute of Network Security, Shandong University, Ji'nan 250100, China)

[3](Key Laboratory of Cryptographic Technology and Information Security, Ministry of Education, Ji'nan 250100, China)

[4](Department of Computer Science, National University of Singapore, Singapore 117590, Singapore)

+ Corresponding author: E-mail: qduyujia@gmail.com

Yu J, Hao R, Kong FY, Cheng XG, Guo XF. Forward-Secure multi-signature in the standard model: Security model and construction. *Journal of Software*, 2010,21(11):2920−2932. http://www.jos.org.cn/1000-9825/3834.htm

Abstract: The formal security model of forward-secure multi-signature is examined and a forward-secure multi-signature scheme with provable security is proposed. Even if the current secret keys of all the signers are exposed, all the signatures pertaining to previous periods are still valid in this scheme. The presented scheme has proven to be secure in the standard model.

Key words: forward security; digital signature; multi-signature; provable security; standard model

摘 要: 给出了前向安全多重签名的形式化安全性模型,并提出了一个可证安全的前向安全多重签名方案.在该方案中,即使所有参与多重签名成员的当前密钥泄漏,所有以前时间段的签名也是有效的.证明了方案是标准模型下安全的.

关键词: 前向安全性;数字签名;多重签名;可证安全性;标准模型

中图法分类号: TP309 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant No.60703089 (国家自然科学基金); the Shandong Provincial Natural Science Foundation of China under Grant Nos.ZR2009GQ008, ZR2010FQ019 (山东省自然科学基金); the Science and Technology Project of Provincial Education Department of Shandong Province of China under Grant No.J08LJ02 (山东省教育厅科技计划); the Scientific Research Foundation for the Excellent Middle-Aged and Youth Scientists of Shandong Province of China under Grant No.2008BS01011 (山东省优秀中青年科学家科研奖励基金)

Received 2009-09-11; Accepted 2010-03-11

多重签名是一种重要的面向群体签名.在一个多重签名方案中,用户成员集合中的一个子集联合生成一个有效的多重签名,而验证者确信子集中的每个成员都参与了签名.多重签名的安全性模型最早由 Micali 等人[1]给出,随后出现了一些关于多重签名的其他研究工作,例如文献[2−4].

然而,标准的多重签名存在一个固有的弱点:一旦所有参与者的密钥泄漏,所有的多重签名(包括产生在密钥泄露之前的签名)都不可信任了.因此,如何减小密钥泄漏的危害是一项重要的研究工作.前向安全签名可以减小密钥泄漏的危害,将系统的整个生命周期划分成若干时间段,每个时间段都通过单向的演化函数演化新密钥,并删除以前的旧密钥,而公钥在整个生命周期中保持不变,即便当前的密钥泄漏了,以前时间段的签名仍然是有效的.

前向安全签名的思想由 Anderson[5]提出.Bellare 和 Miner[6]最早提出了实用的前向安全签名方案,并给出了前向安全签名的安全性模型.随后提出了大量关于前向安全签名的构造方案[7−13].密钥隔离签名[14,15]和入侵容忍签名[16−18]作为两种具有更强安全性的签名也已被提出.

前向安全多重签名并不是一个全新的概念,王晓明等人[19]基于文献[6]的思想提出了一个前向安全多重签名方案,文献[20]的研究工作之一是基于文献[10]提出了一个基于双线性映射的前向安全多重签名方案.文献[21]提出了另外一个前向安全多重签名方案,然而该方案被证明并不安全[22].观察目前已经提出的所有前向安全多重签名方案,存在以下两个不足:(1) 没有关于前向安全多重签名的任何形式化的安全性模型定义;(2) 没有任何可证安全的前向安全多重签名.所有存在的方案仅仅是从各自理解的方面进行简单的安全性分析,这导致一些构造的方案并不安全[21].因此,定义前向安全多重签名的安全性模型,并构建可证安全的前向安全多重签名方案,是一项非常有意义的研究工作.由于数字签名在随机预言模型下的安全性证明只是一种启发式证明,因此,构造标准模型下可证安全的高效方案成为近年来密码学家研究的热点.

为了解决目前前向安全多重签名中存在的两个不足,我们给出了前向安全多重签名的形式化安全性模型,并提出了一个可证安全的前向安全多重签名方案.给出的安全性模型融合了数字签名前向安全性[6]和多重签名安全性[1]的模型.方案的所有费用参数,包括密钥产生、密钥更新、签名、验证时间的复杂性和公钥、私钥和签名长度的复杂性都不超过 $O(\log^2 T)$.另外,与已有方案[19,20]不同,在我们提出的方案中,参与成员在形成多重签名时它们之间不需进行任何交互操作.基于 l+1 计算 Diffie-Hellman 问题的难解性,证明了该签名方案在标准模型下是安全的,这相对于随机预言模型下安全的签名方案更有吸引力和优势.

1 前向安全多重签名及其安全性定义

1.1 前向安全多重签名

令 $\Omega=\{\Omega_1,\Omega_2,...,\Omega_n\}$ 表示可能参与多重签名的 n 个成员的集合,L 表示 Ω 的任意成员子集,最终由它们生成多重签名.

定义 1. 前向安全多重签名(forward-secure multi-signature,简称 FSMS)方案是一个由 PPT 算法构成的四元组(*Key*,*Update*,*Sign*,*Ver*).

1. Key,密钥产生算法:

输入:安全参数 k' 和总共时间段数 T.

输出:成员 $\Omega_i(i=1,2,...,n)$ 的初始化份额密钥 $SK_1^{(i)}$,公钥 PK.

2. Update,密钥更新算法:

输入:当前时间段 j,成员 $\Omega_i(i=1,2,...,n)$ 的当前份额密钥 $SK_j^{(i)}$.

输出:下一时间段新的份额密钥 $SK_{j+1}^{(i)}$.

3. Sign,签名算法**:

输入:当前时间段 j,参与多重签名的子群 $L\subseteq\Omega$,每个成员 $\Omega_i(\Omega_i\in L)$的当前份额密钥 $SK_j^{(i)}$,消息 M.

输出:成员集合 L 在第 j 时间段对消息 M 的多重签名$\langle j,L,Sig\rangle$.

4. Ver,验证算法:

输入:参与多重签名的子群 $L\subseteq\Omega$,消息 M,签名$\langle j,L,Sig\rangle$和公钥 $PK^{(i)}|_{\Omega_i\in L}$.

输出:“有效”或“无效”.

1.2 安全性定义

简单来说(非正式的),前向安全多重签名的安全性表现为:即使某一时间段的签名成员集合Ω的所有密钥都泄漏了,敌手也不能成功伪造之前时间段任意成员子集 L 的一个有效多重签名.这里要求 L 中存在一个诚实的成员,它没有被敌手收买,并不参与伪造多重签名,而其他成员均可能被敌手收买.我们用敌手能够伪造 L 的有效多重签名的概率来刻画前向安全多重签名的安全性.敌手为了获取这个目标,它可以收买成员,进行多重签名查询.为了模型化密钥无赖(rogue-key)攻击[1],我们赋予敌手更强的能力,它可以创建收买的任何成员的公私钥.这里只有一个限制,敌手需要在注册公钥时证明私钥是一个有效私钥.为了简化模型,与文献[1]的方法类似,要求敌手在密钥生成阶段输出它收买成员的公私钥信息.允许敌手收买除 1 个成员外的所有成员,它的目标是伪造这个诚实成员.

为了更好地刻画敌手的攻击能力,我们给出下面的实验来表示收买 n–1 个成员$(\Omega_2,\ldots,\Omega_n)$的敌手在不同阶段完成的操作.$F$ 表示敌手,k'为安全参数,n 表示总共参与成员个数,T 为总共的时间阶段数,$\xleftarrow{R}$ 表示随机选取.

Experiment *Run-Adversary*(F,k',n,T)

$F\xleftarrow{R}(PK^{(1)})$;

$j\leftarrow 1$;

F 输出有效的公私钥对$(PK^{(i)},SK_1^{(i)})$ for $i=2,\ldots,n$;

Repeat

$d\leftarrow F^{Sign_{SK_j^{(i\in L)}}(L\subseteq\Omega,\Omega_1\in L)(\cdot)}(cma,PK^{(i)}|_{\Omega_i\in\Omega})$;

$SK_{j+1}^{(i)}\leftarrow Update(SK_j^{(i)}|_{\Omega_i\in\Omega})$;

$j\leftarrow j+1$;

Until $(d=breakin)$ or $(j=T)$

$b\leftarrow j$;

$(M^*,\langle j^*,L,sign^*\rangle|_{L\subseteq\Omega})\leftarrow F(forge,SK_b^{(i)}|_{\Omega_i\in\Omega})$;

if $Ver(M^*,\langle j^*,L,sign^*\rangle)=1$ and $1\leqslant j^*<b$

and Ω_1对于M^*在阶段j^*中的$sign_{SK_{j^*}^{(1)}}(\cdot)$没有被查询;

then return (1)

else return (0)

在密钥生成阶段,敌手知道所有的公共参数、总共的时间阶段、一个诚实成员的公钥.不失一般性,假定诚实的成员为Ω_1.敌手生成剩下 n–1 个成员的公私钥对后运行在 3 个阶段:第 1 阶段,选择消息查询阶段(cma),敌手可以查询任何成员子集 $L(L\subseteq\Omega,\Omega_1\in L)$对它选择信息的多重签名(通过对诚实成员$\Omega_1$ 进行签名查询).在这个

** 我们的签名算法定义并没有提及鲁棒性.如果考虑鲁棒性,对于每个成员$\Omega_i(\Omega_i\in L)$生成的签名,其他成员应该能够验证其正确性.如果都正确,则生成最后多重签名.我们提出的前向安全多重签名方案可以提供鲁棒性,然而,为了使定义更具普遍性,这里的签名算法定义并没有涉及到这个问题.

阶段的最后,敌手决定它待在这个阶段还是转入入侵阶段;第 2 阶段,入侵阶段(breakin)(敌手一旦进入这个阶段,就不能返回上一阶段),公开给敌手它决定入侵的时间阶段 b 和所有成员$\Omega_i(\Omega_i\in\Omega)$在此阶段的密钥 $SK_b^{(i)}$;最后一个阶段,伪造阶段(forge),敌手输出伪造的签名信息对,如果敌手成功伪造任何成员子集 $L(L\subseteq\Omega,\Omega_1\in L)$在第 $j^*(j^*<b)$的时间阶段对信息 M^*的多重签名,并且Ω_1在第 1 阶段的第 $j^*(j^*<b)$时间段对 M^*的签名没有被查询,则表示敌手成功了.

定义 2(标准模型下前向安全多重签名的安全性). 令 $FSMS=(Key,Update,Sign,Ver)$是前向安全多重签名方案,$k'$为安全参数,$n$表示总共参与成员个数,$T$为总共的时间段数,$F$表示上述描述的敌手.令 $Succ(FSMS[k',n,T],F)$表示上述实验返回 1 的概率,则方案 FSMS 的不安全性定义为函数:

$$Insec^{FSMS}(FSMS[k',n,T],t,q_{sig})=\max_F\{Succ(FSMS[k',n,T],F)\}.$$

这里,最大值针对满足下列条件的所有敌手:执行上述实验的时间最多为 t,进行的签名预言查询最多为 q_{sig} 次.

2 密码知识

下面给出方案需要的一些常用的密码知识.

令 G_1 和 G_2 分别是阶为素数 p 的两个加法和乘法循环群,$P\in G_1$ 是 G_1 的一个生成元.

双线性映射 $\hat{e}:G_1\times G_1\to G_2$ 满足:

(1) 双线性:对于任意 $P_1,P_2\in G_1,a,b\in Z_p^*$,满足 $\hat{e}(aP_1,bP_2)=\hat{e}(P_1,P_2)^{ab}$.

(2) 非退化性:存在 $P_1,P_2\in G_1$,满足 $\hat{e}(P_1,P_2)\neq 1$.

(3) 可计算性:存在一种有效算法,对任意的 $P_1,P_2\in G_1$,可以计算 $\hat{e}(P_1,P_2)$.

定义 3(计算 l+1 Diffie-Hellman (l+1-DH)问题). 给定 G_1 的一个生成元 P 和 $(P,\alpha P,\alpha^2P,...,\alpha^lP)\in G_1^{l+1}$,计算 $\alpha^{l+1}P\in G_1$.

定义 4(l+1-DH 安全群). 概率算法 A 攻击群 G_1 上的 l+1-DH 问题,如果使用的时间最多为 t,获得的优势概率 $Adv_A\geqslant\varepsilon$,则称算法 $A(t,\varepsilon)$攻击群 G_1 上的 l+1-DH 问题.如果不存在概率算法能够(t,ε)攻击群 G_1 上的 l+1-DH 问题,则称群 G_1 是$(t,\varepsilon)l$+1-DH 安全群.

3 我们提出的标准模型下的前向安全多重签名方案

3.1 符号表示和相关说明

方案采用的是二进制树结构进行密钥的更新操作[10−13,23].采用一个深度为 l 的满二进制树,每个时间阶段对应二进制树的一个节点.每个节点表示一个二进制串 w,根节点表示空二进制串 $w=\varepsilon$,若节点 w 所在的深度小于 l,它的左右儿子节点表示为 $w0$ 和 $w1$.因此,所有节点 w 二进制表示为 $w=w_1w_2\ldots w_j(1\leqslant j\leqslant l)$,$j$ 为节点 w 所在的层数,w^j 的 k 位前缀表示为 $w^j|_k$,即,若 $w^j=w_1\ldots w_t$,则 $w^j|_k=w_1\ldots w_k(k\leqslant t)$.$w^j|_k$ 的兄弟节点表示为 $w^j|_{\bar{k}}$.使用二叉树的前序遍历技术将每个时间段与二进制树的每个节点关联:从根节点 $w^0=\varepsilon$开始,如果 w^j 是中间节点,则 $w^{j+1}=w^j0$,如果 w^j 是叶节点且 $j<T$,则 $w^{j+1}=w^j1$,w'是满足 $w'0$ 是 w^j 前缀的最长比特串.

$Stack^{(i)}$表示成员Ω_i在第 j 时间段持有的份额密钥,它按照密钥更新次序被组织成堆栈的形式,栈顶元素为时间阶段 j 对应的节点私钥 $SK_j^{(i)}$,除了包含 $SK_j^{(i)}$ 外,还包括从根节点到 w^j 路径上所有末位为 0 节点的右兄弟的节点私钥.也就是说,如果 $w'0$ 是 w^j 的前缀,则 $Stack^{(i)}$就包括 $w'1$ 的节点私钥 $SK_{w'1}^{(i)}$.

3.2 方案描述

构造的方案采用了分层的基于身份密码的密钥演化方法[24],该方法可以使方案获得较好的平均性能.为了能够使方案在标准模型下可证安全,我们采用了 Waters 的基于身份加密的方法[25].注意到相似的方法也已被应用于构造一些其他签名方案[12,17],这些方案将二进制树的每个叶节点与每个时间段关联.而我们采用的方法是使用二叉树的前序遍历技术[23],将二进制树的每个节点(包括中间节点)与每个时间段关联,这样的方案可以具

有高效的密钥产生和密钥更新算法.定义总共的时间段个数 $T=2^{l+1}-2$,二进制树的根节点代表第 0 个时间段,按前序遍历的顺序扫描深度为 l 的满二进制树的每个节点,这些节点分别表示第 1,2,…,T 个时间段.

(1) 算法 Key:输入安全参数 k',二进制树的深度 l,执行如下:

① 运行 $IG(1^{k'})$产生阶为素数 p 的加法群 G_1 和乘法群 G_2 及双线性映射 $\hat{e}:G_1\times G_1\to G_2$,
随机选择 G_1 的生成元 $P\in_R G_1$.

② Ω中的每个成员Ω_i随机选择 $\alpha^{(i)}\in_R Z_p^*$,令 $P_1^{(i)}=\alpha^{(i)}P$,选择 $P_2,P_3,Q_1,\ldots,Q_l,U',U_1,\ldots,U_n\in G_1$,
并且计算 $Z^{(i)}=\hat{e}(P_1^{(i)},P_2)$.

③ 选择 hash 函数 $H_1:\{0,1\}^*\to\{0,1\}^{n_m}$.

④ 定义函数 $F(w)=P_3+\sum_{j=1}^{k}w_jQ_j, G(m)=U'+\sum_{j=1}^{n_m}m_jU_j$,
这里,$w=w_1\ldots w_k$, $m=m_1\ldots m_{n_m}$ (对于所有的 i,j,有 $w_i,m_j\in\{0,1\}$).
每个成员Ω_i的根密钥为 $sk_\varepsilon^{(i)}=\alpha^{(i)}P_2$,公钥 $PK^{(i)}=(G_1,G_2,\hat{e},P,P_1^{(i)},P_2,P_3,Q_1,\ldots,Q_l,U',U_1,\ldots,U_n,Z^{(i)},k,l,H_1)$.

⑤ 每个成员Ω_i随机选择 $r_0^{(i)},r_1^{(i)}\in Z_p^*$,
令 $sk_0^{(i)}=(\alpha^{(i)}P_2+r_0^{(i)}P_3,r_0^{(i)}P,r_0^{(i)}Q_2,\ldots,r_0^{(i)}Q_l), sk_1^{(i)}=(\alpha^{(i)}P_2+r_1^{(i)}(P_3+Q_1),r_1^{(i)}P,r_1^{(i)}Q_2,\ldots,r_1^{(i)}Q_l)$,
将 $sk_1^{(i)}$ 和 $sk_0^{(i)}$ 依次压入堆栈 $Stack^{(i)}$.

(2) 算法 Update:当前时间段 j,成员$\Omega_i(i=1,2,\ldots,n)$的份额密钥堆栈 $Stack^{(i)}$.
令 $w=w_1w_2\ldots w_k$ 表示对应于第 j 时间段的节点.
每个成员Ω_i从堆栈 $Stack^{(i)}$中将栈顶元素 $SK_j^{(i)}$ 出栈,
解析 $SK_j^{(i)}=(a_0^{(i)},a_1^{(i)},b_{k+1}^{(i)},\ldots,b_l^{(i)})=(\alpha^{(i)}P_2+r'^{(i)}F(w_1\ldots w_k),r'^{(i)}P,r'^{(i)}Q_{k+1},\ldots,r'^{(i)}Q_l)$,按以下方式更新密钥:

① 如果 w 为中间节点,选择 $t_1^{(i)},t_0^{(i)}\in Z_p^*$,计算:

$$\begin{aligned}SK_{w_1\ldots w_k1}^{(i)}&=(a_0^{(i)}+b_{k+1}^{(i)}+t_1^{(i)}\cdot F(w_1\ldots w_k1),a_1^{(i)}+t_1^{(i)}P,b_{k+2}^{(i)}+t_1^{(i)}Q_{k+2},\ldots,b_l^{(i)}+t_1^{(i)}Q_l)\\&=(\alpha^{(i)}P_2+r_1^{(i)}\cdot F(w_1\ldots w_{k-1}1),r_1^{(i)}P,r_1^{(i)}Q_{k+1},\ldots,r_1^{(i)}Q_l),\\SK_{w_1\ldots w_k0}^{(i)}&=(a_0^{(i)}+t_0^{(i)}\cdot F(w_1\ldots w_k0),a_0^{(i)}+t_0^{(i)}P,b_{k+2}^{(i)}+t_0^{(i)}Q_{k+2},\ldots,b_l^{(i)}+t_0^{(i)}Q_l)\\&=(\alpha^{(i)}P_2+r_0^{(i)}\cdot F(w_1\ldots w_{k-1}0),r_0^{(i)}P,r_0^{(i)}Q_{k+1},\ldots,r_0^{(i)}Q_l).\end{aligned}$$

这里, $r_1^{(i)}=r'^{(i)}+t_1^{(i)}$, $r_0^{(i)}=r'^{(i)}+t_0^{(i)}$.
将 $SK_{w_1\ldots w_k1}^{(i)}$ 和 $SK_{w_1\ldots w_k0}^{(i)}$ 依次压栈,并删除 $SK_{w_1\ldots w_k}^{(i)}$.

② 如果 w 为叶节点,则直接删除 $SK_{w_1\ldots w_k}^{(i)}$.

(3) 算法 Sign:当前时间段 j,参与多重签名的子群 $L\subseteq\Omega$,每个成员$\Omega_i(\Omega_i\in L)$的当前份额密钥堆栈 $Stack^{(i)}$,消息 M.令 $w=w_1w_2\ldots w_k$ 表示对应于第 j 时间段的节点.

① 每个成员Ω_i从堆栈 $Stack^{(i)}$中读出栈顶元素 $SK_j^{(i)}$,
解析 $SK_j^{(i)}=(a_0^{(i)},a_1^{(i)},b_{k+1}^{(i)},\ldots,b_l^{(i)})=(\alpha^{(i)}P_2+r^{(i)}F(w_1\ldots w_k),r^{(i)}P,r^{(i)}Q_{k+1},\ldots,r^{(i)}Q_l)$.

② 参与多重签名的子群 $L\subseteq\Omega$中的每个成员Ω_i选择 $s^{(i)}\in Z_p^*$,
计算 $(\sigma_0^{(i)},\sigma_1^{(i)},\sigma_2^{(i)})=(a_0^{(i)}+s^{(i)}G(H_1(M)),a_1^{(i)},s^{(i)}P)$,并返回它的签名$\langle j,(\sigma_0^{(i)},\sigma_1^{(i)},\sigma_2^{(i)})\rangle$.

③ 成员Ω_i的签名$\langle j,(\sigma_0^{(i)},\sigma_1^{(i)},\sigma_2^{(i)})\rangle$正确性可以由下面的等式来验证:

$$\hat{e}(P,\sigma_0^{(i)})\stackrel{?}{=}\hat{e}(F(w_1\ldots w_k),\sigma_1^{(i)})\cdot\hat{e}(G(H_1(M)),\sigma_2^{(i)})\cdot Z^{(i)}.$$

④ 任何人都可以利用通过验证的子群 L 成员的部分签名生成最终子群 L 的多重签名:

$$\langle j,L,(\sigma_0,\sigma_1,\sigma_2)\rangle=\left\langle j,L,\left(\sum_{P_i\in L}\sigma_0^{(i)},\sum_{P_i\in L}\sigma_1^{(i)},\sum_{P_i\in L}\sigma_2^{(i)}\right)\right\rangle.$$

(4) 算法 Ver:参与多重签名的子群 $L\subseteq\Omega$,消息 M,签名$\langle j,L,(\sigma_0,\sigma_1,\sigma_2)\rangle$和公钥 $PK^{(i)}|_{\Omega_i\in L}$.

令 $w=w_1w_2\ldots w_k$ 表示对应于第 j 时间段的节点.验证者计算 $Z=\sum_{Q_i\in L}Z^{(i)}$,验证以下等式是否成立:

$$\hat{e}(P,\sigma_0)\overset{?}{=}\hat{e}(F(w_1\ldots w_k),\sigma_1)\cdot\hat{e}(G(H_1(M)),\sigma_2)\cdot Z,$$

如果成立,则返回“有效”;否则,返回“无效”.

4 安全性分析

定理 1. 假定$\langle j,L,(\sigma_0,\sigma_1,\sigma_2)\rangle$是 Sign 算法第 j 时间段对消息 M 产生的签名,则

$$Ver(M,PK^{(i)}|_{Q_i\in L},\langle j,L,(\sigma_0,\sigma_1,\sigma_2)\rangle)=\text{“有效”}.$$

证明:令 $w=w_1w_2\ldots w_k$ 表示对应于第 j 时间段的节点,所以,

$$\begin{aligned}\hat{e}(P,\sigma_0)&=\hat{e}\left(P,\sum_{Q_i\in L}\sigma_0^{(i)}\right)\\&=\hat{e}\left(P,\sum_{Q_i\in L}(a_0^{(i)}+s^{(i)}G(H_1(M)))\right)\\&=\hat{e}\left(P,\sum_{Q_i\in L}(\alpha^{(i)}P_2+r^{(i)}F(w_1\ldots w_k)+s^{(i)}G(H_1(M)))\right)\\&=\prod_{Q_i\in L}\hat{e}(P,\alpha^{(i)}P_2)\cdot\prod_{Q_i\in L}\hat{e}(P,r^{(i)}F(w_1\ldots w_k))\cdot\prod_{Q_i\in L}\hat{e}(P,s^{(i)}G(H_1(M)))\\&=\prod_{Q_i\in L}\hat{e}(\alpha^{(i)}P,P_2)\cdot\hat{e}\left(\sum_{Q_i\in L}r^{(i)}P,F(w_1\ldots w_k)\right)\cdot\hat{e}\left(\sum_{Q_i\in L}s^{(i)}P,G(H_1(M))\right)\\&=\prod_{Q_i\in L}\hat{e}(P_1^{(i)},P_2)\cdot\hat{e}\left(\sum_{Q_i\in L}a_1^{(i)},F(w_1\ldots w_k)\right)\cdot\hat{e}\left(\sum_{Q_i\in L}\sigma_2^{(i)},G(H_1(M))\right)\\&=\hat{e}\left(\sum_{Q_i\in L}\sigma_1^{(i)},F(w_1\ldots w_k)\right)\cdot\hat{e}\left(\sum_{Q_i\in L}\sigma_2^{(i)},G(H_1(M))\right)\cdot\prod_{Q_i\in L}Z^{(i)}\\&=\hat{e}(F(w_1\ldots w_k),\sigma_1)\cdot\hat{e}(G(H_1(M)),\sigma_2)\cdot Z.\end{aligned}$$

□

定理 2. 如果存在一个伪造者 F 运行时间最多为 t,进行的签名预言查询最多为 q_s 次,并且满足 $Succ(FSMS[k',n,T],F)=\varepsilon$,则存在一个算法 I 能够(t',ε')-攻击群 G_1 上的 l+1-DH 问题.这里,

$$t'=t+O((q_s+\log T)\log T\cdot t_{G_1}),$$

$$\varepsilon'=\frac{1}{8q_s(n_m+1)}\cdot\frac{1}{T+2\log(T+2)-2}\cdot\varepsilon,$$

其中,t_{G_1} 表示 G_1 中的运算最多所需要的时间.

证明:如果存在一个伪造者 F 运行时间最多为 t,进行的签名预言查询最多为 q_s 次,以ε的概率攻击所提出的方案,我们构造一个算法 $I(t',\varepsilon')$解决 G_1 中的 l+1-DH 问题.

首先,算法 I 输入 $(g,z_1=\alpha P,z_2=\alpha^2P,\ldots,z_l=\alpha^lP)\in G_1^{l+1}$,目标是通过运行 F 输出 $z_l=\alpha^{l+1}P$.I 选取总共的阶段数 T,并随机猜测 F 产生伪造签名的时间段 $j^*(0<j^*\leqslant T)$,她猜对正确的概率是 $1/T$,若 $j^*<T/2$ 则退出.第 j^*时间段对应的二进制树节点表示为 $w^*=w_0^*w_1^*\ldots w_k^*$,其中,$w_0^*=\varepsilon$.

(1) 密钥产生阶段.算法 I 的任务是计算公共参数.首先选择 $\gamma\in_R Z_p^*$, 令

$$P_1^{(1)}=\alpha P=z_1 \tag{1}$$

$$P_2=(\gamma+\alpha^l)P=\gamma P+z_l \tag{2}$$

因此,

$$\alpha P_2=(\alpha\gamma+\alpha^{l+1})P=\gamma z_1+z_{l+1} \tag{3}$$

算法 I 不知道它的值.I 选择 $\gamma_1,\gamma_2,\ldots,\gamma_l,\delta\in Z_p^*$,令

$$P_3=\delta P+\sum_{j=1}^{k}w_j^*z_{l-j+1} \tag{4}$$

$$Q_j=\gamma_jP-z_{l-j+1}(j=1,\ldots,l) \tag{5}$$

I 然后令 $\tau_m=2q_s$,选择$\lambda_m\in_R\{0,1,\ldots,n_m\}$,假定 $\tau_m(n_m+1)<p$.算法 I 选择$\eta'\in_R Z_p$ 和向量 $(\eta_1,\ldots,\eta_{n_m})$,其中,$\eta_j\in_R Z_p$.算法 I 再选择$\mu'\in_R Z_p$ 和向量 $(\eta_1,\ldots,\eta_{n_m})$,其中,$\mu_j\in_R Z_p$.

为了方便表示,为消息 $M(m=H_1(M))$定义以下函数:

$$J(m)=\eta'+\sum_{j=1}^{n_m}m_j\eta_j-\tau_m\lambda_m,\ K(m)=\mu'+\sum_{j=1}^{n_m}m_j\mu_j.$$

I 构造公共参数如下:

$$U'=(\eta'-\tau_m\lambda_m)P_2+\mu'P,\ U_i=\eta_iP_2+\mu_iP \text{ for } 1\leqslant i\leqslant n_m.$$

因此,对于任意消息 $M(m=H_1(M))$,下面的等式成立:

$$G(m)=U'+\sum_{j=1}^{n_m}m_jU_j=J(m)P_2+K(m)P \tag{6}$$

计算:

$$Z^{(1)}=\hat{e}(P_1^{(1)},P_2) \tag{7}$$

提供给 F 公共参数 $PK^{(1)}=(G_1,G_2,\hat{e},P,P_1^{(1)},P_2,P_3,Q_1,...,Q_l,U',U_1,...,U_n,Z^{(1)},k,l,H_1)$ 和总共阶段数 T.

F 输出其他 n–1 个成员有效的初始化公私钥对.显然,初始化的私钥可以生成任何时间段的私钥.

(2) 选择消息查询阶段的模拟.当 F 要求Ω_1参与第 j 时间段对消息 $M(m=H_1(M))$的多重签名时,I 执行如下操作:

(a) 如果 $J(m)=0(\mathrm{mod}\ p)$,则 I 退出;

(b) 否则,随机选择$r_j^{(1)}\in Z_p^*,s^{(1)}\in Z_p^*$,计算并回答对 I 的签名查询:

如果我们定义$\overline{s}^{(1)}=s^{(1)}-\alpha/J(m)$,由等式(1)、等式(6)可得:

$$\alpha P_2+r_j^{(1)}F(w_1...w_k)+\overline{s}^{(1)}G(H_1(M))=-\frac{K(m)}{J(m)}P_1^{(1)}+r_j^{(1)}F(w_1...w_k)+\overline{s}^{(1)}G(H_1(M))+\left(\alpha P_2+\frac{K(m)}{J(m)}P_1^{(1)}\right)$$

$$=-\frac{K(m)}{J(m)}P_1+r_j^{(1)}F(w_1...w_k)+s^{(1)}G(H_1(M)),$$

$$\overline{s}^{(1)}P=s^{(1)}P-\frac{\alpha}{J(m)}P=s^{(1)}P-\frac{1}{J(m)}P_1^{(1)},$$

$$(\sigma_0^{(1)},\sigma_1^{(1)},\sigma_2^{(1)})=\left(-\frac{K(m)}{J(m)}P_1+r_j^{(1)}F(w_1...w_k)+s^{(1)}G(H_1(M)),r_j^{(1)}P,s^{(1)}P-\frac{1}{J(m)}P_1^{(1)}\right).$$

返回 $(\sigma_0^{(1)},\sigma_1^{(1)},\sigma_2^{(1)})$ 给 F.

(3) 入侵阶段的模拟.F 进行入侵阶段 b,I 需要提供给 F 成员Ω_1第 $b(b>j^*)$时间段的密钥(其他 n–1 个成员的密钥,F 可以直接从它们的初始阶段密钥计算获得).

令第 b 时间段对应的节点为 $w^b=w_0w_1\ldots w_s(s\leqslant l)$,其中,$w_0=\varepsilon$.因为 $b>j^*$,所以按前序扫描顺序,节点 w^*必定在 w^b 之前.换句话说,必定是下面两种情况之一:(1) 存在某个 $c(0\leqslant c\leqslant\min\{s,k\})$,满足 $w_i=w_i^*$(对于所有 $0\leqslant i\leqslant c$),但 $w_{c+1}=1, w_{c+1}^*=0$;(2) 对于所有 $1\leqslant i\leqslant k$,有 $w_i^*=w_i$.当情况(2)发生时,I 退出.

当情况(1)发生时,执行以下操作:

(a) I 首先计算从根节点到节点 $w^b=w_1\ldots w_k$ 路径上所有满足 $w_j=0$ 的节点 $w^b|_j=w_1\ldots w_j(1\leqslant j\leqslant k)$的右兄弟节点 $w^b|_{\overline{j}}=w_1...w_{j-1}1$的私钥.对于每一个 $w^b|_{\overline{j}}=w_1...w_{j-1}1(1\leqslant j\leqslant k)$ 节点对应的时间段 j',I 选择 $r^{(1)}\in_R Z_p$,可以计算出

$$SK_{j'}^{(1)}=(\alpha P_2+r^{(1)}(P_3+w_1Q_1+...+w_{j-1}Q_{j-1}+Q_j),r^{(1)}P,r^{(1)}Q_{j+1},...,r^{(1)}Q_l).$$

这是因为:

- 当 $j>c+1$ 时,I 定义 $r^{(1)}=\overline{r}^{(1)}+\alpha^{c+1}\in Z_p$,由等式(3)~等式(5)可知下面的关系成立:

$$\alpha P_2 + r^{(1)}(P_3 + w_1Q_1 + ... + w_{j-1}Q_{j-1} + Q_j) =$$

$$\gamma z_1 + z_{l+1} + r^{(1)}\left(\delta P + \sum_{m=1}^{k} w_m^* z_{l-m+1} + w_1\gamma_1 P - w_1 z_l + ... + w_{j-1}\gamma_{j-1}P - w_{j-1}z_{l-j+2} + \gamma_j P - z_{l-j+1}\right) =$$

$$\gamma z_1 + z_{l+1} + r^{(1)}\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{j-1} w_m\gamma_m P + \sum_{m=c+2}^{j-1} w_m z_{l-m+1} + \gamma_j P - z_{l-j+1}\right) =$$

$$\gamma z_1 + z_{l+1} + (\bar{r}^{(1)} + \alpha^{c+1})\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{j-1} w_m\gamma_m P + \sum_{m=c+2}^{j-1} w_m z_{l-m+1} + \gamma_j P - z_{l-j+1}\right) =$$

$$\gamma z_1 + z_{l+1} + \bar{r}^{(1)}\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{j-1} w_m\gamma_m P + \sum_{m=c+2}^{j-1} w_m z_{l-m+1} + \gamma_j P - z_{l-j+1}\right) +$$

$$\alpha^{c+1}\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{j-1} w_m\gamma_m P + \sum_{m=c+2}^{j-1} w_m z_{l-m+1} + \gamma_j P - z_{l-j+1}\right) =$$

$$\gamma z_1 + z_{l+1} + \bar{r}^{(1)}\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{j-1} w_m\gamma_m P + \sum_{m=c+2}^{j-1} w_m z_{l-m+1} + \gamma_j P - z_{l-j+1}\right) +$$

$$\left(\delta z^{c+1} + \sum_{m=c+2}^{k} w_m^* z_{l-m+c+2} - z_{l+1} + \sum_{m=1}^{j-1} w_m\gamma_m z^{c+1} + \sum_{m=c+2}^{j-1} w_m z_{l-m+c+2} + \gamma_j z^{c+1} - z_{l-j+c+2}\right) =$$

$$\gamma z_1 + \bar{r}^{(1)}\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{j-1} w_m\gamma_m P + \sum_{m=c+2}^{j-1} w_m z_{l-m+1} + \gamma_j P - z_{l-j+1}\right) +$$

$$\left(\delta z^{c+1} + \sum_{m=c+2}^{k} w_m^* z_{l-m+c+2} + \sum_{m=1}^{j-1} w_m\gamma_m z^{c+1} + \sum_{m=c+2}^{j-1} w_m z_{l-m+c+2} + \gamma_j z^{c+1} - z_{l-j+c+2}\right),$$

并且 $r^{(1)}P = (\bar{r}^{(1)} + \alpha^{c+1})P = \bar{r}^{(1)}P + z^{c+1}$,这里有 $c \leqslant l-1$.

当 $c+2<j+1 \leqslant m \leqslant l$ 时,由等式(5)可得:

$$r^{(1)}Q_m = (\bar{r}^{(1)} + \alpha^{c+1})(\gamma_m P - z_{l-m+1}) = \bar{r}^{(1)}(\gamma_m P - z_{l-m+1}) + (\gamma_m z^{c+1} - z_{l-m+c+2}).$$

- 当 $j<c+1$ 时,I 定义 $r^{(1)} = \bar{r}^{(1)} + \alpha^j \in Z_p$,由等式(3)~等式(5)可知下面的关系成立:

$$\alpha P_2 + r^{(1)}(P_3 + w_1Q_1 + ... + w_{j-1}Q_{j-1} + Q_j) =$$

$$\gamma z_1 + z_{l+1} + r^{(1)}\left(\delta P + \sum_{m=1}^{k} w_m^* z_{l-m+1} + w_1\gamma_1 P - w_1 z_l + ... + w_{j-1}\gamma_{j-1}P - w_{j-1}z_{l-j+2} + \gamma_j P - z_{l-j+1}\right) =$$

$$\gamma z_1 + z_{l+1} + r^{(1)}\left(\delta P + \sum_{m=j+1}^{k} w_m^* z_{l-m+1} + \sum_{m=1}^{j-1} w_m\gamma_m P + \gamma_j P - z_{l-j+1}\right) =$$

$$\gamma z_1 + z_{l+1} + (\bar{r}^{(1)} + \alpha^j)\left(\delta P + \sum_{m=j+1}^{k} w_m^* z_{l-m+1} + \sum_{m=1}^{j-1} w_m\gamma_m P + \gamma_j P - z_{l-j+1}\right) =$$

$$\gamma z_1 + z_{l+1} + \bar{r}^{(1)}\left(\delta P + \sum_{m=j+1}^{k} w_m^* z_{l-m+1} + \sum_{m=1}^{j-1} w_m\gamma_m P + \gamma_j P - z_{l-j+1}\right) +$$

$$\alpha^j\left(\delta P + \sum_{m=j+1}^{k} w_m^* z_{l-m+1} + \sum_{m=1}^{j-1} w_m\gamma_m P + \gamma_j P - z_{l-j+1}\right) =$$

$$\gamma z_1 + z_{l+1} + \bar{r}^{(1)}\left(\delta P + \sum_{m=j+1}^{k} w_m^* z_{l-m+1} + \sum_{m=1}^{j-1} w_m\gamma_m P + \gamma_j P - z_{l-j+1}\right) +$$

$$\left(\delta z^j + \sum_{m=j+1}^{k} w_m^* z_{l-m+j+1} + \sum_{m=1}^{j-1} w_m\gamma_m z^j + \gamma_j z^j - z_{l+1}\right) =$$

$$\gamma z_1 + \bar{r}^{(1)}\left(\delta P + \sum_{m=j+1}^{k} w_m^* z_{l-m+1} + \sum_{m=1}^{j-1} w_m\gamma_m P + \gamma_j P - z_{l-j+1}\right) +$$

$$\left(\delta z^j + \sum_{m=j+1}^{k} w_m^* z_{l-m+j+1} + \sum_{m=1}^{j-1} w_m\gamma_m z^j + \gamma_j z^j\right),$$

并且 $r^{(1)}P = (\bar{r}^{(1)} + \alpha^j)P = \bar{r}^{(1)}P + z^j$,这里有 $j \leqslant l-1$.

当 $j+1 \leqslant m \leqslant l$ 时,由等式(5)可得:

$$r^{(1)}Q_m = (\bar{r}^{(1)} + \alpha^j)(\gamma_m P - z_{l-m+1}) = \bar{r}^{(1)}(\gamma_m P - z_{l-m+1}) + (\gamma_m z^{c+1} - z_{l-m+j+1}).$$

(b) I 为了生成 $SK_b^{(1)}$,选择 $r^{(1)} \in_R Z_p$,定义 $r^{(1)} = \bar{r}^{(1)} + a^s \in Z_p$,$I$ 可以计算:

$$SK_b^{(1)} = (\alpha^{(1)}P_2 + r^{(1)}(P_3 + w_1Q_1 + ... + w_sQ_s), r^{(1)}P, r^{(1)}Q_{s+1}, ..., r^{(1)}Q_l).$$

这是因为,由等式(3)~等式(5)可知下面的关系成立:

$$\alpha P_2 + r^{(1)}(P_3 + w_1Q_1 + ... + w_sQ_s) =$$
$$\gamma z_1 + z_{l+1} + r^{(1)}\left(\delta P + \sum_{m=1}^{k} w_m^* z_{l-m+1} + w_1\gamma_1 P - w_1 z_l + ... + w_s\gamma_s P - w_s z_{l-s+1}\right) =$$
$$\gamma z_1 + z_{l+1} + r^{(1)}\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{s} w_m\gamma_m P + \sum_{m=c+2}^{s} w_m z_{l-m+1}\right) =$$
$$\gamma z_1 + z_{l+1} + (\bar{r}^{(1)} + \alpha^{c+1})\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{s} w_m\gamma_m P + \sum_{m=c+2}^{s} w_m z_{l-m+1}\right) =$$
$$\gamma z_1 + z_{l+1} + \bar{r}^{(1)}\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{s} w_m\gamma_m P + \sum_{m=c+2}^{s} w_m z_{l-m+1}\right) +$$
$$\alpha^{c+1}\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{s} w_m\gamma_m P + \sum_{m=c+2}^{s} w_m z_{l-m+1}\right) =$$
$$\gamma z_1 + z_{l+1} + \bar{r}^{(1)}\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{s} w_m\gamma_m P + \sum_{m=c+2}^{s} w_m z_{l-m+1}\right) +$$
$$\left(\delta z^{c+1} + \sum_{m=c+2}^{k} w_m^* z_{l-m+c+2} - z_{l+1} + \sum_{m=1}^{s} w_m\gamma_m z^{c+1} + \sum_{m=c+2}^{s} w_m z_{l-m+c+2}\right) =$$
$$\gamma z_1 + \bar{r}^{(1)}\left(\delta P + \sum_{m=c+2}^{k} w_m^* z_{l-m+1} - z_{l-c} + \sum_{m=1}^{s} w_m\gamma_m P + \sum_{m=c+2}^{s} w_m z_{l-m+1}\right) +$$
$$\left(\delta z^{c+1} + \sum_{m=c+2}^{k} w_m^* z_{l-m+c+2} + \sum_{m=1}^{s} w_m\gamma_m z^{c+1} + \sum_{m=c+2}^{s} w_m z_{l-m+c+2}\right),$$

并且$r^{(1)}P = (\bar{r}^{(1)} + \alpha^{c+1})P = \bar{r}^{(1)}P + z^{c+1}$,这里有 $c \leqslant l-1$.

当 $c+2 \leqslant s+1 \leqslant m \leqslant l$ 时,由等式(5)可得:

$$r^{(1)}Q_m = (\bar{r}^{(1)} + \alpha^{c+1})(\gamma_m P - z_{l-m+1}) = \bar{r}^{(1)}(\gamma_m P - z_{l-m+1}) + (\gamma_m z^{c+1} - z_{l-m+c+2}).$$

因此,由步骤(a)、步骤(b)可得,当情况(1)发生时,I 可以提供给 F 成员 Ω_1 第 b 时间段的 $Stack^{(1)}$所有密钥.

(4) 伪造阶段.如果回答完敌手 F 的签名查询后,I 没有退出,I 恰好猜对了 j^*,敌手 F 会以至少 ε 的概率输出集合 $L(L\subseteq\Omega,\Omega_1\in L)$在第 j^*时间段对消息 $M^*(m^*=H_1(M^*))$伪造的有效多重签名 $\langle j^*, L, \sigma^* = (\sigma_0^*, \sigma_1^*, \sigma_2^*)\rangle$.如果 $J(m^*)\neq 0(\text{mod } p)$,则退出;否则$(J(m^*)=0(\text{mod } p))$,意味着 $G(m^*)=K(m^*)P$,根据成员 $\Omega_i(\Omega_i\in L/\{\Omega_1\})$的密钥,计算它们各自的部分签名 $\langle j^*, (\sigma_0^{(i)*}, \sigma_1^{(i)*}, \sigma_2^{(i)*})\rangle$.因此,可以计算 Ω_1 在此时间段上的有效签名:

$$\left\langle j^*, \left(\sigma_0^{(1)*} = \sigma_0^* - \sum_{P_i\in L/\{P_1\}} \sigma_0^{(i)*}, \sigma_1^{(1)*} = \sigma_1^* - \sum_{P_i\in L/\{P_1\}} \sigma_1^{(i)*}, \sigma_2^{(1)*} = \sigma_2^* - \sum_{P_i\in L/\{P_1\}} \sigma_2^{(i)*}\right)\right\rangle.$$

所以,存在某个 $r,s\in Z_p$ 有下面的关系:

$$\sigma_0^{(1)*} = \alpha P_2 + rF(w_1^*...w_k^*) + sK(m^*)P \tag{8}$$
$$\sigma_1^{(1)*} = rP \tag{9}$$
$$\sigma_2^{(1)*} = sP \tag{10}$$

又因为 $F(w_1^*...w_k^*) = \left(\delta + \sum_{j=1}^{k}\gamma_j w_j^*\right)P$,所以算法 I 可以根据等式(3)、等式(8)~等式(10)成功计算并输出

$$\alpha^{(l+1)}P = z_{l+1} = \sigma_0^{(1)*} - \gamma z_1 - \left(\delta + \sum_{j=1}^{k}\gamma_j w_j^*\right)\sigma_1^{(1)*} - K(m^*)\sigma_2^{(1)*}.$$

概率分析.下面分析 I 不退出的概率.考虑以下事件:.

事件 A_i:在第 i 次签名查询时,有 $J(m)\neq 0(\text{mod } p)$.

事件 A^*:$J(m^*)=0(\text{mod } p)$.

事件 B:I 猜的 j^*满足 $j^*\geqslant T/2$.

事件 C:在入侵阶段时,情况(1)发生.

事件 $\bigwedge_{i=1}^{q_s} A_i \wedge A^*$ 和事件 $B\wedge C$ 是独立的.

显然,I 不退出的概率为 $\Pr\left(\bigwedge_{i=1}^{q_s} A_i \wedge A^* \wedge B \wedge C\right)$.

为了使分析更加容易,我们将界定 A_i 子事件的概率,考虑 A_i 的子事件 A_i'.

事件 A_i': 在第 i 次签名查询时,有 $J(m)\neq 0(\text{mod } \tau_m)$.

我们的假定$\tau_m(n_m+1)<p$意味着$0\leqslant\tau_m\lambda_m<p, 0\leqslant\eta'+\sum_{j=1}^{n_m}m_j\eta_j<p$. 易知,$J(m)=0(\mathrm{mod}\ p)$暗示着$J(m)=0(\mathrm{mod}\ \tau_m)$,所以,$J(m)\neq 0(\mathrm{mod}\ \tau_m)$暗示着$J(m)\neq 0(\mathrm{mod}\ p)$.

因此$\Pr\left(\bigwedge_{i=1}^{q_s}A_i\wedge A^*\wedge B\wedge C\right)\geqslant\Pr\left(\bigwedge_{i=1}^{q_s}A_i'\wedge A^*\wedge B\wedge C\right)$.

计算:

$$\Pr[A^*]=\Pr[J(m^*)=0(\mathrm{mod}\ p)]=\Pr[J(m^*)=0(\mathrm{mod}\ p)\wedge J(m^*)=0(\mathrm{mod}\ \tau_m)]$$

$$=\Pr[J(m^*)=0(\mathrm{mod}\ \tau_m)]\cdot\Pr[J(m^*)=0(\mathrm{mod}\ p)\mid J(m^*)=0(\mathrm{mod}\ \tau_m)]=\frac{1}{\tau_m}\cdot\frac{1}{n_m+1}.$$

观察到

$$\Pr\left(\bigwedge_{i=1}^{q_s}A_i'\wedge A^*\right)=\Pr(A^*)\cdot\Pr\left(\bigwedge_{i=1}^{q_s}A_i'\mid A^*\right)=\Pr(A^*)\cdot\left(1-\Pr\left(\bigvee_{i=1}^{q_s}\neg A_i'\mid A^*\right)\right)$$

$$\geqslant\frac{1}{\tau_m}\cdot\frac{1}{n_m+1}\cdot\left(1-\frac{q_s}{\tau_m}\right)=\frac{1}{\tau_m}\cdot\frac{1}{n_m+1}\cdot\frac{\tau_m-q_s}{\tau_m}.$$

由于$\tau_m=2q_s$,因此,$\Pr(\bigwedge_{i=1}^{q_s}A_i'\wedge A^*)\geqslant\frac{1}{4q_s(n_m+1)}$.

显然,$\Pr(B)\geqslant 1/2$.

因为二进制树的层数为l层,所以根节点的左子树上有2^l-1个节点,从根节点到节点$w^b=w_1\ldots w_k(k\leqslant l)$的路径上最多有$l-1$个节点(根和$w^b$除外).这意味着,如果事件$B$发生,$w^b$之前(按前序扫描)至少有$2^l+l-2$个节点,对应于$2^l+l-2$个时间段.而这些时间段中,最多有$l-1$对应于情况(2),其他都对应于情况(1).

因此,$\Pr(C\mid B)\geqslant\frac{2^l-1}{2^l+l-2}$.

由第3.2节的定义可知,$T=2^{l+1}-2$,因此$l=\log(T+2)-1$.

因为事件$\bigwedge_{i=1}^{q_s}A_i'\wedge A^*$和$B\wedge C$相互独立,所以有

$$\Pr[\neg abort]=\Pr\left(\bigwedge_{i=1}^{q_s}A_i\wedge A^*\wedge B\wedge C\right)\geqslant\Pr\left(\bigwedge_{i=1}^{q_s}A_i'\wedge A^*\wedge B\wedge C\right)=\Pr\left(\bigwedge_{i=1}^{q_s}A_i'\wedge A^*\right)\cdot\Pr(B\wedge C)$$

$$=\Pr\left(\bigwedge_{i=1}^{q_s}A_i'\wedge A^*\right)\cdot\Pr(B)\cdot\Pr(C\mid B)\geqslant\frac{1}{4q_s(n_m+1)}\cdot\frac{1}{2}\cdot\frac{2^l-1}{2^l+l-2}$$

$$=\frac{1}{8q_s(n_m+1)}\cdot\frac{(T+2)/2-1}{(T+2)/2+\log(T+2)-2}=\frac{1}{8q_s(n_m+1)}\cdot\frac{T}{T+2\log(T+2)-2}.$$

因为I猜对伪造阶段j^*的概率为$1/T$,并且如果I不退出,F至少以ε的概率产成一个有效签名,所以I能够以不小于$\frac{1}{8q_s(n_m+1)}\cdot\frac{1}{T+2\log(T+2)-2}\cdot\varepsilon$的概率计算$\alpha^{(l+1)}P$.

时间分析.从上面的分析可以看出,I执行的时间主要由选择消息查询和入侵模拟中的一些G_1中的运算构成.在所有的选择消息查询中最多需要$O(q_s\log T\cdot t_{G_1})$时间,入侵模拟最多需要$O(\log^2 T\cdot t_{G_1})$时间.因为$F$完成伪造的时间为$t$,所以$I$总共运行时间最多为$t+O((q_s+\log T)\log T\cdot t_{G_1})$.

因此,定理2成立. □

定理3. 令FSMS[k',n,T]表示上述提出的前向安全多重签名方案,k'为安全参数,n表示总共参与成员个数,T为总共的时间段数,对于任意t和q_s,以下关系成立:

$$Insec^{FSMS}(FSMS[k',n,T],t,q_s)\leqslant 8q_s(n_m+1)(T+2\log(T+2)-2)\cdot Insec^{l+1\text{-DH}}(k',t'),$$

其中,$t'=t+O((q_s+\log T)\log T\cdot t_{G_1})$.

证明:设 $Insec^{l+1\text{-DH}}(k',t')=\varepsilon'$,即不存在算法 $I(t',\varepsilon')$攻击群 G_1 上的 l+1-DH 问题,由定理 2 得,对于任何敌手 F 都满足以下关系:

$$Succ(FSMS[k',n,T],F) \leqslant \varepsilon = 8q_s(n_m+1)(T+2\log(T+2)-2)\cdot\varepsilon'$$
$$= 8q_s(n_m+1)(T+2\log(T+2)-2)\cdot Insec^{l+1\text{-DH}}(k',t'),$$

又由定义 2 得:

$$Insec^{FSMS}(FSMS[k',n,T],t,q_s) \leqslant 8q_s(n_m+1)(T+2\log(T+2)-2)\cdot Insec^{l+1\text{-DH}}(k',t'),$$

其中, $t'=t+O((q_s+\log T)\log T\cdot t_{G_1})$. □

5 讨 论

我们提出的前向安全多重签名方案还有一个重要的优点:可以在每个成员的份额签名产生之后再确定形成多重签名的子集 L,这样的方案具有更好的灵活性.

表 1 给出了提出方案的各性能参数关于总共时间阶段数 T 的复杂性.方案 Key 算法、Update 算法、Sign 算法、Ver 算法时间的复杂性以及公钥、私钥、签名长度的复杂性分别为 $O(\log T)$,$O(\log T)$,$O(1)$,$O(1)$,$O(\log T)$,$O(\log^2 T)$和 $O(1)$.分析方法比较容易,这里不再赘述.

Table 1 Performance complexities (in terms of T)

表 1 性能复杂性(关于 T 项)

	Algorithm *Key*	Algorithm *Update*	Algorithm *Sign*	Algorithm *Ver*
Complexities	$O(\log T)$	$O(\log T)$	$O(1)$	$O(1)$
	Publice key	Secret key		Signature
Size (bit)	$O(\log T)$	$O(\log^2 T)$		$O(1)$

表 2 给出了所提出的方案与已有的前向安全多重签名方案[19,20]的对比.

(1) 算法 Sign 有无交互.文献[19,20]方案的 Sign 算法都需要参与成员交互完成,而本文提出的方案的 Sign 算法不需参与成员的任何交互.因此,我们的方案更能适合 Ad Hoc 网络这种自组织的环境.

(2) 安全性基于的难解问题.文献[19]的方案的安全性是基于强 RSA 假设,文献[20]的方案的安全性依赖于文献[10]是基于 CDH 假设的,本文提出的方案的安全性基于的是 l+1-DH 假设.

(3) 安全性依赖的模型.文献[19,20]的方案是基于文献[6,10]构造的,其安全性最多在随机预言模型下安全,而本文提出的方案是标准模型下安全.因此,我们的方案具有更高的安全层次.

(4) 安全性分析的强度.文献[19]仅仅从作者理解的方面进行简单的安全性分析,文献[20]没有进行安全性分析,这两个方案都不具有可证安全性.而本文提出的方案是可证安全的.

Table 2 Related comparisons

表 2 相关比较

	Need interactions in algorithm Sign or not	The based hard problem	The based security model	The strength of security analysis
Scheme in Ref.[19]	Yes	Strong RSA Assumption	RO model	Simple analysis
Scheme in Ref.[20]	Yes	CDH Assumption	RO model	No security analysis
Our scheme	No	l+1-DH Assumption	Standard model	Provable security

6 结 论

给出了前向安全多重签名的安全性模型,并提出了一个可证安全的前向安全多重签名方案.方案满足:即使所有参与多重签名成员的当前密钥泄漏,所有以前时间段的多重签名也有效.基于 l+1-DH 假设,证明了提出的方案是标准模型下安全的.

References:

[1] Micali S, Ohta K, Reyzin L. Accountable-Subgroup multisignatures. In: Proc. of the 8th ACM Conf. on Computer and Communications Security. 2001. 245−254.

[2] Ohta K, Okamoto T. A digital multisignature scheme based on the Fiat-Shamir scheme. In: Imai H, Rivest R, Matsumoto T, eds. Proc. of the Asiacrypt 1991. LNCS 739, Berlin: Springer-Verlag, 1991. 139−148.

[3] Boldyreva A. Threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-Group signature scheme. In: Desmedt Y, ed. Proc. of the PKC 2003. LNCS 2567, Berlin: Springer-Verlag, 2002. 31−46.

[4] Komano Y, Ohta K, Shimbo A, Kawamura S. Formal security model of multisignatures. In: Katsikas S, Lopez J, Backes M, Gritzalis S, Preneel B, eds. Proc. of the ISC 2006. LNCS 4176, Berlin: Springer-Verlag, 2006. 146−160.

[5] Anderson R. Two remarks on public key cryptology. In: Proc. of the Invited Lecture, ACM-CCS'97. 1997. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-549.pdf

[6] Bellare M, Miner S. A forward-secure digital signature scheme. In: Wiener M, ed. Proc. of the CRYPTO'99. LNCS 1666, Berlin: Springer-Verlag, 1999. 431−448.

[7] Abdalla M, Reyzin L. A new forward-secure digital signature scheme. In: Okamoto T, ed. Proc. of the Asiacrypt 2000. LNCS 1976, Berlin: Springer-Verlag, 2000. 116−129.

[8] Itkis G, Reyzin L. Forward-Secure signatures with optimal signing and verifying. In: Kilian J, ed. Proc. of the Crypto 2001. LNCS 2139, Berlin: Springer-Verlag, 2001. 499−514.

[9] Kozlov A, Reyzin L. Forward-Secure signatures with fast key update. In: Cimato S, Galdi C, Persiano G, eds. Proc. of the Security in Communication Networks 2002. LNCS 2576, Berlin: Springer-Verlag, 2002. 247−262.

[10] Hu F, Wu C, Irwin J. A new forward secure signature scheme using bilinear maps. Cryptology ePrint Archive, 2003. http://eprint.iacr.org/2003/188.pdf

[11] Kang B, Park J, Halm S. A new forward secure signature scheme. Cryptology ePrint Archive, 2004. http://eprint.iacr.org/2004/183

[12] Boyen X, Shacham H, Shen E, Waters B. Forward secure signatures with untrusted update. In: Proc. of the 13th ACM Conf. on Computer and Communications Security. 2006. 191−200.

[13] Yu J, Kong F, Cheng X, Hao R, Li G. Construction of yet another forward secure signature scheme using bilinear maps. In: Baek J, Bao F, Chen K, Lai X, eds. Proc. of the ProvSec 2008. LNCS 5324, Berlin: Springer-Verlag, 2008. 83−97.

[14] Dodis Y, Katz J, Xu S, Yung M. Strong key-insulated signature scheme. In: Desmedt Y, ed. Proc. of the PKC 2003. LNCS 2567, Berlin: Springer-Verlag, 2003. 130−144.

[15] Weng J, Chen KF, Liu SL, Li XX. Identity-Based strong key-insulated signature without random oracles. Journal of Software, 2008, 19(6):1555−1564 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/1555.htm [doi: 10.3724/SP.J.1001.2008. 01555]

[16] Itkis G, Reyzin L. SiBIR: Signer-Base intrusion-resilient signatures. In: Yung M, ed. Proc. of the Crypto 2002. LNCS 2442, Berlin: Springer-Verlag, 2002. 499−514.

[17] Libert B, Quisquater J, Yung M. Efficient intrusion-resilient signatures without random oracles. In: Lipmaa H, Yung M, Lin D, eds. Proc. of the Inscrypt 2006. LNCS 4318, Berlin: Springer-Verlag, 2006. 27−41.

[18] Yu J, Kong F, Cheng X, Hao R, Guo XF. Intrusion-Resilient signature scheme with provable security. Journal of Software, 2010, 21(9):2352−2366 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3772.htm [doi: 10.3724/SP.J.1001.2010. 03772]

[19] Wang X, Fu F, Zhang Z. A forward secure multisignature scheme. Chinese Journal of Computers, 2004,27(9):1177−1181 (in Chinese with English abstract).

[20] Sherman S, Lucas C, Yiu S, Chow K. Forward-Secure multisignature and blind signature schemes. Applied Mathematics and Computation, 2005,168(2):895−908. [doi: 10.1016/j.amc.2004.09.015]

[21] Sunitha N, Amberker B. Forward-Secure multi-signatures. In: Parashar M, Aggarwal S, eds. Proc. of the ICDCIT 2008. LNCS 5375, Berlin: Springer-Verlag, 2008. 89−99.

[22] Yu J, Hao R, Kong F, Cheng X, Zhao H, Chen Y. Cryptanalysis of a type of forward secure signatures and multi-signatures. Int'l Journal of Computers and Applications, 2010,32(4):1−6.

[23] Canetti R, Halevi S, Katz J. A forward-secure public-key encryption scheme. In: Biham E, ed. Proc. of the Eurocrypt 2003. LNCS 2656, Berlin: Springer-Verlag, 2003. 255−271.

[24] Boneh D, Boyen X, Goh E. Hierarchical identity based encryption with constant size ciphertext. In: Cramer R, ed. Proc. of the Eurocrypt 2005. LNCS 3493, Berlin: Springer-Verlag, 2005. 440−456.

[25] Waters B. Efficient identity-based encryption without random oracles. In: Cramer R, ed. Proc. of the Eurocrypt 2005. LNCS 3494, Berlin: Springer-Verlag, 2005. 114−127.

附中文参考文献:

[15] 翁健,陈克非,刘胜利,李祥学.标准模型下基于身份的强密钥隔离签名.软件学报,2008,19(6):1555−1564. http://www.jos.org.cn/1000-9825/19/1555.htm [doi: 10.3724/SP.J.1001.2008.01555]

[18] 于佳,孔凡玉,程相国,郝蓉,Guo Xiangfa.可证安全的入侵容忍签名方案.软件学报,2010,21(9):2352−2366 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3772.htm [doi: 10.3724/SP.J.1001.2010.03772]

[19] 王晓明,符方伟,张震.前向安全的多重数字签名方案.计算机学报,2004,27(9):1177−1181.

于佳(1976－),男,山东青岛人,博士,副教授,CCF 会员,主要研究领域为密码学,网络信息安全.

郝蓉(1976－),女,讲师,主要研究领域为密码学,网络信息安全.

孔凡玉(1978－),男,博士,副教授,主要研究领域为密码学.

程相国(1969－),男,博士,副教授,主要研究领域为密码学.

GUO Xiang-Fa(1979－),男,博士生,主要研究领域为网络信息安全.