关于无个人公钥的群认证

蒋绍权

绵阳师范学院信息安全研究所 绵阳 中国 621006

摘要 群认证是一种多方认证机制,研究动态群的成员们如何确认每个成员身份的真实性。这里,群组成员没有个人公钥。 本文首先分析了 Harn 的群认证方案, 证明他的方案在有意义的参数下是不安全的。 我们还研究了群认证和几个多方签名之间的关系。我们证明基于身份的多重签名可以转换为安全群认证协议, 而门限签名方案没有这种特性。我们还证明, 如果去掉签名消息的话, Bellare 和 Neven 的基于 ID 的多重签名方案实际上就是一个安全的群认证协议。

关键词 群认证; 多重签名; 门限签名; 聚合签名
中图法分类号 TP309.2, TP393.08 DOI 号 10.19363/j.cnki.cn10-1380/tn.2017.07.005

On Group Authentication without Personal Public-Keys

JIANG Shaoquan

Institute of Information Security, Mianyang Normal University, Mianyang 621006, China

Abstract We study the group authentication, where a dynamic group of members wish to confirm whether all of them are valid. The restriction is that a member does not have a personal public key. We present an attack to Harn's scheme, which implies that his scheme is insecure as long as the parameters are set to be meaningful. We also study the relation between a group authentication and some multi-party based signatures. We show that an ID-based multi-signature can be converted into a secure group authentication while a threshold signature scheme does not have this property. We also show that an ID-based multi-signature by Bellare and Neven in fact is a secure group authentication when we remove the message to be signed.

Key words group authentication; multi-signature; threshold signature; aggregate signature

1 引言

用户认证(或身份认证)是计算机和通信网络中最重要的安全服务之一。本方向开始于Needham与Schroeder [1]。一个普通的例子是远程登录到服务器或计算机。我们通常用口令来完成认证. 然而, 在许多应用中, 这种方式是行不通的, 因为通信者不一定与对方共享口令。此时, 我们通常用公钥技术来进行认证。基于公钥的认证可以参见Schnorr 认证[2], Okamoto认证[3] 和 Guillou-Quisquater认证[4]。 然而, 这种方式需要将成员身份与其公钥相关联。这种关联通常是利用公钥基础设施(PKI)下的公密钥证书来实现的。

最近, Harn[5] 提出了群认证的概念。这里, 群管理员(GM)为每个成员分配一个成员密钥, 而整个系统只有一个公钥。当一成员群想要认证群中的每个参与者的成员属性时, 他们联合运行认证协议。最后, 每个参与者拒绝或者接受认证的有效性。这种协议可以应用于在线会议系统(例如, Skype, MSN, Wechat), 确保会议中没有假冒者。

群认证的一个简单方式是让任何两个参与者都执一次交互身份认证协议。然而, 如果群大小为 n, 这需要执行 $O(n^2)$ 次这种协议。这显然是低效率的。另一个方式是通过公共服务器来实现, 让每个参与者都向服务器认证自己, 然后服务器向所有群成员发布认证结果。然而, 这种方法引入了一个在线服务器。而且, 这个服务器需要运行 $O(n)$ 次身份认证协议。但是, 如果很多成员同时认证, 则服务器会很拥堵; 如果很多成员依次认证, 则认证过程会很长。因此, 这种认证方式效率也很低。我们还可以要求每个成员用数字签名来认证其身份。然而, 这要求每个成员拥有公共密钥。如前所述, 这是我们不希望看到的, 因为它会引起公钥管理问题。本文的目的是如何找

通讯作者: 蒋绍权, 博士, 教授, Email: shaoquan.jiang@gmail.com。
收稿日期: 2017-02-09; 修改日期: 2017-05-19; 定稿日期: 2017-05-23

到更好的解决方案。

1.1 相关工作

群认证协议首先由 Harn[5]提出并构造了一些方案, 其基本思想是让管理员把主密钥 s 分享给所有成员, 同时公布哈希值 $H(s)$。当需要认证某个群体时, 群体成员一起交互恢复 s。如果某个成员不诚实, 那么恢复出来的主秘密将不同于 s, 因而不可能与哈希值 $H(s)$ 匹配。继 Harn 的工作后, 文献中也出现了一些群认证协议。但是, 这些工作在安全性或者认证效果方面并不令人满意。比如, Li 等[6]基于两个变量的拉格朗日插值构造了群认证方案, 但是这个方案需要管理员参与认证过程, 而且协议只能执行一次。再如, Wang 等[7]完全采用多重签名方案[18]来进行群认证。这种方法甚至都不能抵御重放攻击。

群认证协议在形式上与多种基于群体的签名方案有密切的联系。下面我们就这一点作详细讨论。

成员身份可以通过群签名[8]来认证。如果某用户能生成有效的群签名, 那么签名者必然属于这个群。然而, 这种解决方案是有问题的, 恶意的群成员可以假冒许多诚实用户。在这种情况下, 他可以用自己的密钥假冒一个群成员生成群签名, 而实际上这个成员根本就没有参与群认证。这在电子投票等应用中会成为不安全因素。要避免这个问题, 我们可以让群管理员利用群签名的特性恢复签名者身份。然而, 这意味着认证过程总是需要管理员参与。 这是不合理的。此外, 群签名系统中, 每个用户都有一个公钥。这是我们在群认证中所不希望的。

环签名[9]是与群签名类似的签名方案。然而, 与群签名不同, 环签名的签名者身份是信息论意义下匿名的, 并且群组构成可以是任意的。跟群签名相似, 如果用这种签名来进行群认证的话, 假冒群成员的问题仍然存在, 而且签名者身份还无法确定, 因为它是无条件匿名的。最后, 环签名体制跟群签名一样, 成员都具有公钥。因此, 公钥管理问题也仍然存在。当然, 如果采用基于身份的环签名签名, 这个问题就不存在了。

条件匿名的环签名[10]允许签名者确认他是真正的签名者。然而, 该方案需要签名者交互地执行确认协议。Zeng 等[11-14]和 Wu 等[15]构造了有非交互式确认协议的条件匿名环签名。如果将这种协议应用于群认证, 每个成员可以通过生成环签名和身份确认标签来进行认证。 然而, 这种条件匿名环签名仍然不能得到令人满意的群认证, 因为这跟每个成员用个人签名来进行认证没有任何效率优势。

基于身份的多重签名方案[16]是一种多方签名体制。这里, 用户没有公钥。当一个群需要生成群体签名时, 他们可以运行交互协议来实现, 而群的任何子集都不能代表群生成签名。这种机制与群认证非常相关。如果群组成员共同生成的多重签名是有效的, 则该群组所有成员的身份都是真实的; 反之, 则不然。然而, 它的安全模型与群认证有很大不同。粗略地说, 前者的攻击者只能独立地伪造签名, 而后者的攻击者却可以通过与诚实成员交互运行协议来生成欺骗后者的认证信息。有意思的是, 这种签名体制却可以转换成安全的群认证方案, 因而是与群认证最相关的一类安全机制。第一个可证安全的基于身份的多重签名方案是由 Gentry and Ramzan[17]提出的。他们的方案是基于线性配对的, 因而有效性不能令人满意。方案[16]的构造是基于 RSA 利用 Guillou-Quisquater 签名的积性来实现的。这个工作可以看作是 Guillou 和 Quisquater 体制[18]的安全版本。Wei 等[19]利用相似的特性基于大整数分解构造了一个新的方案, 但其效率不如方案[16]。Wei 等[19]的另一个方案利用了承诺协议。 这个协议需要利用具有同态性质的承诺协议。这种承诺协议可以看作是非交互式 Guillou-Quisquater 零知识证明的一种推广。基于这种同态承诺协议的多重签名方案最早由 Bagherzandi 和 Jarecki[20] 提出。Wei 等[19]的协议可以看作是后者的变种。由于二者都使用了同态承诺协议, 其有效性不如方案[16]。Lin 等[21]基于圆锥曲线构造了一个多重签名方案。但是, 这个方案后来被 Islam 和 Biswas[22]攻破。其实, 构造基于圆锥曲线的密码系统是应当谨慎的, 因为早在 1999 年其内在弱点就已被 Dai, Pei 和 Ye [23]指出。由多重签名衍生出来的还有代理多重签名[24-25]。由于这种签名与本工作的关系没有多重签名来得直接, 我们就不再赘述了。

基于身份的聚合签名[17,26]是另一种多方签名方案, 这里每个成员可以对不同消息上生成自己的签名。此外, 有一个公开的融合算法将群中所有成员的签名融合成一个短签名。我们注意到, 如果所有成员签署相同消息的话, 则基于身份的聚合签名就退化成基于身份的多重签名。如前所述, 这在形式上是适合群认证的。即, 如果聚合签名有效, 则群组成员都是有效的; 反之, 则不然。然而, 由于每个成员生成单独的签名, 所以这种方法产生的群认证不是很有效。此外, 如果所有成员签署相同消息,则聚合签名会退化成多重签名。因此, 在研究到群认证协议的转换时, 我们完全可以只考虑多重签名。鉴于此, 我们对聚合签名的研究现状不再赘述。

门限签名[27]是另一多方签名方案, 其中只有不

少于门限数量的成员才可以联合生成签名, 而小于门限数量的成员不能生成签名。从形式上说, 这种方案也可以应用于群规模大于门限值的群认证。也就是说, 如果群组能够生成有效的签名, 则每个成员都是有效的; 反之, 则不然。然而, 后面我们将会看到, 这种方法得到的群认证并不一定安全, 而且这种不安全性似乎具有普遍性。具体地说, 我们没有看到能够抵御这种线性攻击的门限签名方案。

1.2 我们的工作

群认证研究动态群成员确认是否每个参与者都具有有效的成员资格。这里, 成员没有公钥, 但是系统有全局公钥。这样的体制可以避免公钥管理问题。特别地, 可以避免使用 PKI 为基础的公钥来实现系统。本文首先对 Harn 的群认证方案[5]进行密码分析, 证明在有意义的参数设置下他的方案是不安全的。我们还研究群认证机制和其他多方签名机制之间的关系。我们证明基于 ID 的多重签名体制可以转换为安全群认证协议。而且, 这种转换还可以应用到基于 ID 的聚合签名。我们还证明, 如果去掉要签名的消息的话, Bellare 和 Neven[16] 基于 ID 的多重签名体制本身就是一个安全的群认证协议。我们注意到, 尽管门限签名方案在形式上可以应用于群认证, 但是得到的协议一般不具有安全性。我们将通过一个实例来佐证。

2 预备知识

下面是本文将要用到的符号。

- 对于正整数 s, 定义 $[s]=\{1, \cdots, s\}$。
- 函数 $\mu(n)$ 是**可忽略的**, 如果对于任何多项式 $f(n)$, 我们有 $\lim_{n\to\infty}\mu(n)f(n)=0$。
- $\{0,1\}^*$ 表示所有有限长比特串组成的集合。
- 对于有限集合 A, $x\leftarrow A$ 表示完全随机地从 A 中选取一个数 x。

2.1 RSA 假设

取大素数 p, q, 令 $N=pq$, $\varphi(N)=(p-1)(q-1)$. 取 e 使得 $\gcd(e, \varphi(N))=1$, 计算 d 使得 $ed=1\bmod(\varphi(N))$。那么, RSA 公钥为 (N, e), 私钥为 d。RSA 假设[28]是说, 给定 $C\leftarrow\mathbb{Z}^*_N$ 和 (N, e), 没有概率多项式时间算法能以不可忽略的概率成功计算 $C^d \pmod N$。

2.2 Diffie-Hellman 假设

设 q 是一个大素数, $\mathbb{G}$ 是一个阶为 q 的循环群。假定 g 是 $\mathbb{G}$ 的随机生成元。那么, **计算 Diffie-Hellman**(CDH) 假设[29]指的是, 给定 g, g^a, g^b (这里 $a, b\leftarrow\mathbb{Z}_q$), 没有概率多项式时间算法能够以不可忽略的概率计算 g^{ab}。**判定 Diffie-Hellman**(DDH)假设[30]指的是, 没有概率多项式时间算法能够以不可忽略的优势区分 (g, g^a, g^b, g^{ab}) 和 (g, g^a, g^b, g^c), 这里 $a, b, c\leftarrow\mathbb{Z}_q$。

2.3 拉格朗日插值

令 $f(x)\in\mathbb{k}[x]$ 是次数为 d 的域 $\mathbb{k}$ 上多项式。对于 $\mathbb{k}$ 中 $L\geqslant d+1$ 个不同值 $x_1, \cdots, x_L$, 令 $y_i=f(x_i)$, $i\in[L]$, 则利用 (x_i, y_i), $i=1, \cdots, L$, 我们可以恢复出 $f(x)$:

$$f(x)=\sum_{i=1}^{L} f(x_i)\prod_{r=1, r\neq i}^{L}\frac{x-x_r}{x_i-x_r} \tag{1}$$

这就是拉格朗日插值公式。给定 $x^*\in\mathbb{k}$, 我们可以看到, $f(x^*)$ 是 $f(x_1), \cdots, f(x_L)$ 的线性组合, 其中组合系数是由 $x_1, \cdots, x_L, x^*$ 完全确定的。

2.4 Shamir 秘密分享

我们现在介绍 Shamir 秘密分享方案[31]。假设某秘密分发中心有一个完全随机取于 $\mathbb{F}_q$ 的秘密 s_0, 打算分享给 n 个参与者, 使得 t 个参与者可以恢复出秘密, 而 $t-1$ 个参与者得不到秘密的任何信息。那么, 他可以完全随机地选取 $s_1, \cdots, s_{t-1}$。令 $f(x)=s_0+s_1x+\cdots+s_{t-1}x^{t-1}$。对于 $i=1, \cdots, n$, 如果参与者 i 的公开标签为 $\mathbb{F}_q$ 中元素 x_i, 则他得到的子密钥可以定义为 $d_i=f(x_i)$。这个方案有如下性质: 任何 t 或更多的子密钥可以通过拉格朗日插值恢复 s_0, 而小于 t 个子密钥则得不到 s_0 的任何信息。

2.5 基本引理

下面, 我们介绍两个引理。一个是 Bellare 等人的分叉引理[32]。这个引理对于估计某种算法提取秘密的概率是非常有用的。

引理 1. (分叉引理)固定 $q\geqslant 1$。设 $\mathbb{S}$ 是一个有 $h\geqslant 2$ 个元素的集合. 令 A 是一个随机算法: 当输入为 $x, \gamma_1, \cdots, \gamma_q$ 时, 返回 (I, σ), 其中 x 由算法 IG 随机选取, $\gamma_i\in\mathbb{S}$, $I\in[0, \cdots, q]$ 及 $\sigma\in\{0, 1\}^*$。acc 表示 A 的接受概率, 定义为 $I\geqslant 1$ 的概率。基于 A 的过程 F_A 是如下随机算法(x 由 IG 选取):

算法 $F_A(x)$

输入: A, x

输出: $(1, \sigma, \sigma')$ 或 $(0, \perp, \perp)$

为 A 提供随机比特流 ρ,

$(\gamma_1, ..., \gamma_q) \leftarrow \mathbb{S}$,

$(I, \sigma) \leftarrow A(x, \gamma_1, ..., \gamma_q; \rho)$,

如果 $I = 0$, 则返回 $(0, \perp, \perp)$。

$(\gamma_1', ..., \gamma_q') \leftarrow \mathbb{S}$,

$(I', \sigma') \leftarrow A(x, \gamma_1, ..., \gamma_{I-1}, \gamma_I', \cdots, \gamma_q'; \rho)$

如果 $(I = I')$且$(\sigma' \neq \sigma)$, 则返回 $(1, \sigma, \sigma')$,

否则返回 $(0, \perp, \perp)$。

令 $frk = \Pr[b = 1: x \leftarrow IG; (b, \sigma, \sigma') \leftarrow F_A(x)]$,

则 $frk \geqslant acc \times (\frac{acc}{q} - \frac{1}{h})$。

下面的引理取自于华罗庚[33]。我们将在证明 Theorem 3 的证明中用到。

引理 2. 若 $N \in \mathbb{N}$, 则 $\prod_{p \leqslant N} \left(1 - \frac{1}{p}\right) = \Theta\left(\frac{1}{\log N}\right)$, 这里 p 是素数变量。

3 模型

本节介绍群认证的模型。这个模型是在 Harn[5] 基础上修改而来的, 包括系统模型和安全模型。

3.1 系统模型

本质上, 群认证是一动态群成员确认群中参与者具有有效成员资格的认证协议。这里要进行认证, 一个群管理员需要向群成员预先分发会员密钥。具体的定义如下。

定义 1. **群认证体制**是包含如下两种算法的安全机制。这里, $\mathbb{U}$ 是成员可能的身份标签集合, 而 $\mathbb{P}$ 是所有可能的群的集合。

1. **密钥生成算法 KG**(1^λ) 群管理器 **GM** 以 λ 为安全参数生成系统公钥 pk。当有人请求加入时, 他会向该用户分配身份标签 $u \in \mathbb{U}$, 生成并提供个人密钥 sk_u 给该用户。

2. **群认证算法 GAuth**(P) 当 $\mathbb{P}$ 中的群 P 希望确认 P 中所有参与者身份的真实性时, 他们使用自己的密钥作为输入共同执行群认证协议。最后, 每个参与者输出 0 或 1, 其中 0 表示拒绝, 1 表示接受。

正确性: 如果 P 中参与者都诚实且没有受到攻击, 那么所有参与者都应该接受认证。

在上述定义中, 成员拥有私钥但没有个人公钥, 而系统有一个全局公钥。这就避免了公钥管理问题。当然, 每个人仍然可以拥有公钥, 而 GM 可以为每个用户颁发公钥证书。以后, 当该成员参与认证时, 他总是把证书跟其他消息一起发给群中其他成员。但是, 这种方案需要群中成员每次都要验证其他成员的公钥。这就大大增加了每个成员的计算开销。

在概念上, 群认证机制跟基于 ID 的多重签名, 门限签名和基于 ID 的聚合签名有很大关系。在后面的章节, 我们将会详细讨论。

3.2 安全模型

现在, 我们来定义群认证的安全性。 本质上, 我们感兴趣的是攻击者假冒诚实成员参与群认证的情形。为了假冒成功, 我们甚至允许假冒者腐化(corrupt)某些群成员。如果一个成员被腐化, 那么我们就会把他的个人密钥提供给敌手。这代表了成员不诚实、密钥丢失或个人计算机系统被攻破等等情况。在这种情况下, 我们希望群中的所有诚实参与者(参与认证而且没有被腐化)都不会接受认证。这个安全性质很重要。否则, 攻击者可能冒充许多诚实的成员, 使群认证能够成功执行。这样, 敌手就可能对后续的应用产生安全隐患。比如, 如果群认证的后续应用是民主表决的话, 那么攻击者就可能控制表决结果。

此外, 为了体现认证的本质, 我们假设信道是不具认证性的。也就是说, 诚实参与者的每条消息实际上将由攻击者递送。攻击者可以修改甚至删除信道中的消息。他还可以腐化一些成员。被腐化成员的密钥将交由攻击者使用, 而且其后续角色将由攻击者扮演。

在严格的安全定义中, 攻击者的能力是通过腐化请求和认证请求来实现。这些请求是由挑战者 **CH** 维护的。起初, **CH** 执行算法 **Setup** (1^λ) 生成全局公钥 pk。我们假设当敌手产生一个与标签 u 相关的请求, 标签为 u 的成员已经加入了系统并拥有密钥 sk_u。

- **Corrupt**(u) 这表示标签 u 的成员被腐化。结果, **CH** 把 sk_u 提供给攻击者 A。
- **GroupAuth** (P, I_P) 这里 $I_P \subset P$ 包括到目前为止 P 中被腐化的所有成员。当攻击者产生这种请求时, P 中所有成员将交互执行群认证协议, 其中成员集合 I_P 由 A 扮演, 剩余成员由 **CH** 扮演。注意 I_P 可能包含没被腐化的成员。这种情况表示敌手假冒诚实的成员。由于我们假设信道是不具认证性的, 敌手可以延迟, 修改或删除信道中的消息。而且, 任何消息由 A 来递送。

现在我们可以定义群认证协议的安全性了。 这

包含两个属性: 正确性和认证性。

- **正确性** 如果 A 没有攻击群 P 的群认证过程, 则 P 中所有成员将在协议结束后输出 1(即接受认证)。

- **认证性** 如果 A 发出某个 **GroupAuth** (P, I_P) 请求, 使得 I_P 至少包含一个未被腐化的成员, 而且存在诚实的参与者($P-I_P$ 中成员)接受认证, 那么 A 就算攻击成功。我们用 **non-auth** 表示这种事件。我们假设 A 可以自适应地发出多次 **GroupAuth** 请求。如果 **non-auth** 事件在 A 的整个攻击过程没有发生, 那么我们说协议具有**认证性**。

以上的安全模型可以总结成如下定义。

定义 2 群认证协议 $(\Pi, \mathbb{P})$ 是 t **-安全的**, 如果对于任何可以腐化 t 个成员的概率多项式时间敌手 A, 正确性和认证性不成立的概率均不超过某个可忽略函数 $\mu(\lambda)$。当 t 的大小没有限制时, 我们称 $(\Pi, \mathbb{P})$ 是**安全的**。

备注 定义 2 中, 可忽略函数 $\mu(\lambda)$ 只要存在即可。可忽略函数的定义可参见第二节的符号介绍部分。

4 对 Harn 群认证协议的密码分析

Harn[5]提出了几种具有不同安全级别的群认证方案。在本节中, 我们回顾和分析其具有代表性的协议。 我们证明他的协议不能抵御窃听攻击。也就是说, 攻击者只需要通过窃听诚实参与者的消息就可以成功地假冒另一个未被腐化的成员。

4.1 回顾 Harn 群认证协议

令 p 是一个大素数, $\mathbb{U}=\mathbb{F}_p^*$ 是成员所有可能的身份标签集合。为了简单起见, 我们直接称呼标签为 u 的成员为成员 u. 令 H 是一个单向函数。

- **密钥生成** 系统管理员 **GM** 从 $\mathbb{F}_p[x]$ 中随机选取 k 个次数为 $t-1$ 的多项式 $f_1(x), \cdots, f_k(x)$,其中 $tk \geqslant n$. 当成员 u 加入系统时, **GM** 分配私钥 $(f_1(u), \cdots, f_k(u))$ 给他。**GM** 选取自己的私钥为 $s \in \mathbb{F}_p$, 然后从 $\mathbb{F}_p$ 中随机选取 $d_j, w_j, j=1, \cdots, k$ 使得 $s=\sum_{j=1}^{k} d_j f_j(w_j)$ 且 $w_1, \cdots, w_k$ 两两不同。**GM** 最后公布 $d_1, w_1, \cdots, d_k, w_k, H(s)$ 作为系统公共信息。

- **群认证** 当有 $m \geqslant t$ 个成员的群 P 需要认证成员的身份时, 他们运行如下过程。

1. 成员 $u \in P$ 计算并发送信息

$$c_u=\sum_{j=1}^{k} d_j f_j(u) \prod_{u' \in P, u' \neq u} \frac{w_j-u'}{u-u'} \tag{2}$$

到 P 中所有成员。

2. 每个 $u' \in P$ 检查是否 $H(\sum_{u \in P} c_u)=H(s)$。如果成立, 则接受认证; 否则拒绝接受认证。

协议的正确性是这样的: 利用 $f_j(x)$ 的拉格朗日插值, 我们知道 $\sum_{u \in P} f_j(u) \prod_{u' \in P, u' \neq u} \frac{w_j-u'}{u-u'}=f_j(w_j)$ 。于是, $\sum_{u \in P} c_u=\sum_{j=1}^{k} d_j f_j(w_j)=s$。Harn 粗略地分析了该协议的安全性。我们注意到他的安全模式只考虑了一个**温和的**敌手: 攻击者不修改信道上的消息, 但可以腐化 $t-1$ 成员并假冒一个未被腐化的成员。他的协议不要求时间同步。因此, 攻击者可以假冒一个成员时,可以在知道所有来自诚实参与者的消息后, 才送出这个假冒成员的消息。我们称一个群认证协议是**一次性安全的**, 如果该协议只能保证协议执行一次的安全性。 如果一个协议在上述敌手(即腐化 $t-1$ 个成员, 没有修改信道中的消息)下保持一次性安全性, 我们称之为**静态一次性** t **-安全群认证协议**。

4.2 密码分析

下面我们对 Harn 的协议进行安全分析。我们证明这个协议并不是静态一次性 0-安全的。也就是说, 我们的攻击不需要腐化任何成员。 我们的策略是对等式(2)中 c_u 的表达式做仔细分析, 刻划其随机性的自由度。尽管 $f_j(u), u \in P, j=1, \cdots, k$ 一起具有自由度 kt, 等式(2)并不是长度为 tk 的向量, 而只有 m 个元素。我们的想法是分析 c_u 的表达式, 弄清楚其中真正的独立随机变量。这将得到 c_u 的真实自由度。如果 m 大于这个度, 那么敌手就可以利用线性关系从 $m-1$ 成员的消息 c_u 计算出剩下这个成员的消息,从而假冒之。下面的定理就是这个策略的详细实施。

定理 1. 如果 $n \geqslant t+k$, 则 Harn 群认证协议不是静态一次性 0-安全的。

证明: 我们考虑群 $P=\{u_1, \cdots, u_m\}$, 这里 $m=|P| \geqslant t+k$. 这样的群是存在的。比如, P 是所有 n 个成员的集合。令 $c_{u_1}, \cdots, c_{u_m}$ 是 P 中成员忠实地执行协议时的相应消息。在我们考虑任何敌手的攻击策略之前, 我们先来建立 $c_{u_1}, \cdots, c_{u_m}$ 之间的联系。令

$$C_i=c_{u_i} \prod_{u' \in P,\ u' \neq u_i} (u_i-u'), \tag{3}$$

且 $Q_j(x)=d_j f_j(x) \prod_{u' \in P} (w_j-u')$。那么, 由式(2)中 c_u 的

定义, 我们可以直接得到

$$C_i=\sum_{j=1}^{k}\frac{\mathrm{Q}_j(x)}{w_j-x}|_{x=u_i},\ i=1,\ \cdots,\ m \tag{4}$$

不难看出, 得到该等式的过程是无需计算的。令 $h_j=\mathrm{Q}_j(w_j)$。由于 $\mathrm{Q}_j(x)$ 的次数至多为 $t-1$, 那么必存在次数至多为 $t-2$ 多项式 $\mathrm{Q}_j{}^*(x)$ 使得 $\mathrm{Q}_j(x)=h_j+(w_j-x)\mathrm{Q}_j{}^*(x)$。于是, 由等式(4), 我们得到

$$C_i=\sum_{j=1}^{k}\frac{\mathrm{Q}_j(x)}{w_j-x}|_{x=u_i} \tag{5}$$

$$=\sum_{j=1}^{k}\frac{h_j}{w_j-x}|_{x=u_i}+\sum_{j=1}^{k}\mathrm{Q}^*{}_j(x)|_{x=u_i} \tag{6}$$

令多项式 $\mathrm{Q}^*(x)=\sum_{j=1}^{k}\mathrm{Q}^*{}_j(x)$, 则 $\mathrm{Q}^*(x)$ 的次数至多为 $t-2$。因此,

$$C_i=\sum\frac{h_j}{w_j-u_i}+\mathrm{Q}^*(x)|_{x=u_i} \tag{7}$$

若 $\mathrm{Q}^*(x)$ 展开为 $\mathrm{Q}^*(x)=\sum_{j=0}^{t-2}\gamma_j x^j$, 则代入 $x=u_i$, 等式(7)就变成了

$$C_i=\sum_{j=1}^{k}\frac{h_j}{w_j-u_i}+\sum_{j=0}^{t-2}\gamma_j{u_i}^j,\ i=1,\cdots,\ m \tag{8}$$

为了清楚起见, 我们将等式(8)写成矩阵形式

$$A\begin{bmatrix}h_1\\ \vdots\\ h_k\\ \gamma_0\\ \vdots\\ \gamma_{t-2}\end{bmatrix}=\begin{bmatrix}C_1\\ \vdots\\ C_m\end{bmatrix}, \tag{9}$$

这里 $A=$

$$\begin{bmatrix}\frac{1}{w_1-u_1} & \cdots & \frac{1}{w_k-u_1} & 1 & u_1 & \cdots & {u_1}^{t-2}\\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ \frac{1}{w_1-u_m} & \cdots & \frac{1}{w_k-u_m} & 1 & u_m & \cdots & {u_m}^{t-2}\end{bmatrix}. \tag{10}$$

记 A 的行为 $A_1,\cdots,A_m$. 根据假设, $m=|P|\geqslant t+k$. 于是, $m>t-1+k\geqslant rank(A)$, 这里第二个不等号是由于 $t-1+k$ 是 A 的列数。这就是说 A 的行数 m 大于 $rank(A)$。因此, 必然存在不全为零的常数 $\lambda_1,\cdots,\lambda_m$ 使得 $\sum_{i=1}^{m}\lambda_i A_i=0$。这里 λ_i, $i=1,\ \cdots,\ m$ 可以由线性代数知识对 A 进行基本的行变换得到。于是, $(\lambda_1,\cdots,\lambda_m)A=\mathbf{0}$。对等式(9)两边左乘行向量 $(\lambda_1,\cdots,\lambda_m)$, 我们得到 $0=\sum_{i=1}^{m}\lambda_i C_i$。假定 $\lambda_\ell\neq 0$。我们得到, $C_\ell=-\lambda_\ell{}^{-1}\sum_{i\neq\ell}\lambda_i C_i$。有了这些分析, 我们就可以给出 A 的攻击策略了。

1. A 计算 $\lambda_1,\ \cdots,\ \lambda_m$, 请求群 P 的认证并假冒成员 ℓ。

2. A 监听来自 $P-\{\ell\}$ 的所有消息。在获得 c_{u_i}, $i\neq\ell$ 后, 他结合 $\{u_j\}_{j\neq i}$ 计算 C_i, $i\neq\ell$ 和 $C_\ell=-\lambda_\ell{}^{-1}\sum_{i\neq\ell}\lambda_i C_i$。

3. 最后, 他利用等式(3)从 C_i 推出 c_{u_i} 并发送给 $P-\{\ell\}$.

根据我们上面的分析, 我们知道 A 的攻击是成功的。这就证明了我们的结果。

备注 注意, Harn[5](他论文中的定理 2)指出, 只要 $kt\geqslant n$, 他的协议是静态一次性 t-安全的。我们的密码分析需要 $n\geqslant t+k$。显然, 存在 n 使得 $t+k\leqslant n\leqslant tk$; 否则, $(t-1)(k-1)<1$, 这意味着 $t=1$ (无意义)或 $k=1$(于是 $n<t+1$, 因为要避免我们的攻击, 这是无意义的)。另一方面, 如果这个方案需要 $n<t+k$ (为了避免我们的攻击), 我们说这也是没有意义的。事实上, 注意到 P 必须满足 $t\leqslant|P|\leqslant n<t+k$。这样, 如果 k 小的话, 则 P 的可选择度很小。如果 k 大的话, 则每个成员必须保持大量的密钥(大概 $k\log p$ 比特)。因此, 只要这个协议的参数设置有意义, 我们的攻击就是有效的。

备注 Harn[5]也构造了一个多次运行下还保持安全的协议。其主要思想是在指数中实现上面的协议。然而, 由于我们的分析只使用 C_i, $i\in P$ 的线性依赖关系, 我们可以在指数上实现类似的密码分析。由于这种扩展分析比较简单, 我们就不再详述了。

5 基于 ID 的多重签名到群认证的转换及其延伸

5.1 基于 ID 的多重签名

基于 ID 的多重签名(ID-Based Multi-Signature, 简记为 IBMS)本质上是一种多方签名方案, 这里动

态的成员群联合签署消息, 但群的任何子集合都不能代表这个群完成签名。 在这种机制中,**GM** 生成全局公钥 pk 和主密钥 sk 。对于每个标识 id, 他使用 pk 和 sk 产生 id 的私钥 sk_{id} 。当群 P 想要联合对消息 M 签名时, 他们彼此通信执行签名协议。最后, 每个成员要么输出一个联合签名 σ, 要么输出 $\perp$(表示拒绝)。要验证群 P 和消息 M 的多重签名 σ, 验证者输入 (σ, pk, P, M), 运行验证算法。最后, 他要么输出 0 (表示拒绝), 要么输出 1(表示接受)。

在安全模型中, 敌手知道公钥 pk, 可以通过腐化攻击得到任何成员 id 的签名密钥 sk_{id} 。他还可以请求得到关于任何群 P 和消息 M 的签名 σ, 其中腐化的成员由攻击者扮演, 而诚实的成员由挑战者扮演。最后, 他输出一个三元组 (σ^*, P^*, M^*)。如果 σ^* 是群 P^* 对消息 M^* 的有效签名且 P^* 至少包含一个没有被腐化的成员, 而且敌手从没有对 (P^*, M^*) 请求签名, 那么我们认为敌手的攻击是成功的。

5.2 基于 ID 的多重签名到群认证的安全转换

在本节中, 我们将提出一个从基于 ID 的多重签名到群认证的安全转换。本质上, 基于 ID 的多重签名可以通过将每个成员的标签设置为其 ID 而应用于群认证, 而签名的消息就是可以确认群中成员身份的信息。这个消息可以通过群中每个成员向其他成员广播一个随机数来实现。具体说来, 如果群 P 希望进行认证, 那么这个转换协议具体步骤如下。

1. P 中的每个 u 广播一个随机数 R_u 到群 P 。

2. P 中每个成员都收到 $\{R_u\}_{u\in P}$ 后, 联合对 $M=\{R_u\}_{u\in P}\,|\,P$ 生成多重签名 σ, 这里 $A\,|\,B$ 表示 A 与 B 的串接(concatenation)。

3. P 中成员接受认证当且仅当 σ 是有效的。

为了方便起见, 我们把上面的协议称为**由基于 ID 的多重签名导出的群认证协议。**

在上面的协议中, 由于 M 包含 P, 可以确定群的成员构成; 由于 M 包含随机数 R_u, 任何诚实成员都可以保证签名不会被重复利用。另外, 签名过程与群认证一样都是交互式的, 而且信道也不具认证性。因此, 多重签名在形式上跟群认证很契合。

然而, IBMS 在安全性方面与群认证并不匹配。上面的安全转换中, 群认证协议输出的是一个多重签名。要使群认证协议是安全的, 我们必须保证在敌手的攻击下成员群不能输出有效的签名。但是, 如果所用的多重签名是安全的, 那么这种签名安全性只能保证攻击者不能获得有效的多重签名 $(\sigma^*, P^*, \{R^*_u\}_{u\in P^*}\,|\,P^*)$, 使得 P^* 存在没有被腐化的成员。此外, 每个没有被腐化的成员应由成员自己(而不是敌手假冒)扮演在协议中的角色。另一方面, 群认证需要的“成员群不能输出有效的签名”是指 P^* 不能生成有效的签名使得 P^* 包含两个未被腐化的成员: 一个由攻击者假冒, 另一个是诚实的参与者。 因此, IBMS 在转换中所能提供的安全保障与群认证的安全需求还是有明显差异的。有意思的是, 这种差异并不影响我们证明这个转换的安全性。

我们的证明思想如下。如果群认证敌手 A 攻破 **GroupAuth** (P^*, I_{P^*}) 的认证性并输出 $(\sigma^*, P^*, \{R^*_u\}_{u\in P^*}\,|\,P^*)$, 那么存在没有被腐化的成员 $u_1\in I_{P^*}$, $u_2\in P^*-I_{P^*}$ 使得 A 假冒 u_1 成功欺骗 u_2 。注意, 这里 u_1 是由 A 扮演的。我们可以将 A 转化成 IBMS 的攻击者 B 。B 模拟 A 的攻击环境, 并回答他的请求。如果 B 腐化除了 u_1 外的所有成员, 那么他就可以扮演 $P^*-I_{P^*}$ 而运行 A 扮演 I_{P^*} 。从而, A 成功假冒 u_1 就使 B 伪造了一个含未被腐化成员 u_1 的多重签名。但是, 我们必须小心: 虽然 u_1 在本认证请求中属于假冒集合 I_{P^*}, 但是在其他认证请求中未必也属于假冒集合 I_P 。此时, B 需要扮演 u_1 的角色却不知道 sk_{u_1} 。幸运的是, 这并不麻烦, 因为多重签名也是交互进行的, B 正好可以向其挑战者请求签名 $\{R_u\}_{u\in P}\,|\,P$ 。这样, 由于 B 并未腐化 u_1, 因此 u_1 将由其挑战者扮演。详细的证明将在下面的定理中给出, 主要细节是要处理 B 事先并不知道 u_1, 却需要保持与 A 交互对话的真实性。

定理 2. 设 Π 是一个安全的基于 ID 的多重签名体制。那么, 由 Π 导出的群认证协议是安全的。

证明. 假设导出的群认证协议被敌手 A 以不可忽略的概率 ε 攻破。那么, 我们构造一个敌手 B 以不可忽略的概率 ε' (待定)攻破多重签名 Π 。令 pk 是多重签名体制的公钥。那么, B 以 pk 为输入运行 A, 并准备回答来自 A 的签名及腐化请求。对于任何 **GroupAuth** (P, I_P) 请求, 我们称 $P-\mathbb{C}$ 中没有出现在以前的 **GroupAuth** $(P', I_{P'})$ (准确地说, P')中的成员为**新成员**, 其中 $\mathbb{C}$ 是在 **GroupAuth** (P, I_P) 请求之前被腐化的所有成员的集合。假设整个安全游戏中新成员累积数量的上界为 ν 。所有的新成员可以按照其出现的顺序进行排序(注意: **GroupAuth** (P, I_P) 中 P 的成员可以按字母顺序排列)。那么, B 随机选

取 $I \leftarrow \{1, \cdots, \nu\}$(猜测 A 将假冒第 I 个新成员, 而猜对的概率为 $1/\nu$; B 将利用 A 来伪造含有第 I 个新成员的多重签名; 这样, B 可以腐化除了这个新成员外的所有成员)。令 Φ_0 表示目前为止被 A 腐化的所有成员的集合, Φ_1 是积累到目前为止所有的新成员集合。安全游戏开始时, $\Phi_0 = \Phi_1 = \phi$ (空集)。令 Ψ 为 B 记录的 (u, sk_u) 列表(初始为空)。 B 按如下策略回应 A 的腐化和认证请求。

■ **Corrupt**(u) 如果 A 腐化成员 u, 则 B 首先将 u 添加到 Φ_0 中, 然后检查 Ψ 中是否有记录 (u, sk_u)。如果有, 则他返回 sk_u; 否则, 他向自己的 IBMS 挑战者发出腐化 u 的请求并得到 sk_u。收到 sk_u 后, 他将 (u, sk_u) 添加到 Ψ 中, 并将 sk_u 转发给 A。

■ **GroupAuth**(P, I_P) 在这种情况下, 设认证协议附加步骤的消息列表为 $\{R_u\}_{u\in P}$。值得注意的是, 由于信道不具备认证性, 不同的成员看到的 $\{R_u\}_{u\in P}$ 可能不一样。这个情况对普通的消息也是一样。因此, B 扮演的某个成员总是根据自己见到的消息(如 $\{R_u\}_{u\in P}$)来采取相应的行动。我们分如下情况来讨论 B 的行为。为了明确起见, 设 Φ_1 还没针对 **GroupAuth** (P, I_P) 进行更新。因此, $\Phi_1 \cup (P - \Phi_1 \cup \Phi_0)$才是涵盖了 **GroupAuth**$(P, I_P)$ 的累积至今的所有新成员的集合。

1. 情形 $|\Phi_1| + |P - \Phi_1 \cup \Phi_0| < I$: 这表示第 I 个新成员还没有出现。 这种情况下, B 腐化新成员集合 $P - \Phi_1 \cup \Phi_0$ 并获得他们的私钥。接着, 他把该集合每个新成员 u 相应的信息 (u, sk_u) 添加到 Ψ 中。同时, 他把新成员 $P - \Phi_1 \cup \Phi_0$ 添加到 Φ_1 中。最后, B 与 A 交互执行 **GroupAuth**(P, I_P) , 其中 A 扮演 I_P 而 B 扮演其余的成员。 B 可做到这一点, 因为他知道 P 中所有成员的私钥。

2. 情形 $|\Phi_1| < I$ 但 $|\Phi_1| + |P - \Phi_1 \cup \Phi_0| \geq I$: 这表示第 I 个新成员第一次出现正好是在目前的 P 中。这种情况下, 令 u_I 是 $\Phi_1 \cup (P - \Phi_1 \cup \Phi_0)$ 中第 I 个新成员(必有 $u_I \in (P - \Phi_1 \cup \Phi_0)$)。那么, B 腐化 $P - \Phi_1 \cup \Phi_0 - \{u_I\}$ 中所有成员, 并获得他们的私钥。然后, 他把这些腐化了的 u 的相应信息 (u, sk_u) 添加到 Ψ 中。 同时, 他把 $P - \Phi_1 \cup \Phi_0$ 添加到 Φ_1 中。最后, 如果 $u_I \in I_P$, 则 B 扮演 $P - I_P$ 与 A 实施 **GroupAuth**(P, I_P) 的运行。 B 可以做到这一点, 因为他拥有除 sk_{u_I} 外的所有成员私钥。如果 $u_I \notin I_P$, 则 B 向自己的 IBMS 挑战者请求群 P 对消息 $M = \{R_u\}_{u\in P} \mid P$ 的多重签名。在这种情况下, 由于 ID u_I 是没有被 B 腐化, 其角色将由 B 的挑战者扮演, 而 $P - \{u_I\}$ 由 B 扮演。 B 可以做到这一点, 因为他知道 $P - I_P - \{u_I\}$ 的私钥因而可以扮演这些角色, 同时他可以运行 A 扮演 I_P 中的会员的角色。这样, 他可以把 $P - I_P$ 的消息转发给 A, 而把 I_P 的消息转发给 $P - I_P$ (u_I 由 B 的挑战者扮演, 而 B 扮演余下的角色)。于是, 在 A 看来, 他在与 B 共同执行 **GroupAuth**(P, I_P) ,而在 B 的挑战者看来, 他与 B 共同签署消息 M (其中 $P - \{u_I\}$ 已被腐化)。

3. 情形 $|\Phi_1| \geq I$: 这表示第 I 个新成员在此前某个 **GroupAuth** 中已经出现过。在这种情形下, B 可以执行如下策略。他腐化 $P - \{u_I\}$ (无论 $u_I \in P$ 与否)。然后, 他像以前一样更新 Φ_1, Ψ。接下来, 如果 $u_I \notin P$ 或者 $u_I \in I_P$, 那么他可以与 A 交互通信完成 **GroupAuth**(P, I_P) 的运行。他能做到这一点, 原因如下: 当 $u_I \notin P - I_P$ 时, 而他知道所有成员 $P - I_P$ 的密钥; 当 $u_I \in P - I_P$ 时, 他的策略与情况 2 类似。

4. **异常** 如果 **Corrupt**(u_I) 的请求出现(按照新成员的定义, 这位第 I 个新成员第一次出现是在 **GroupAuth** 中且没有被腐化。), 那么 B 宣布失败。在这情况下, A 不可能假冒 u_I, 因为他只能假冒没有被腐化的成员。因此, B 猜测 A 将假冒第 I 个新成员是不对的(因为这个成员是 u_I, 正在被 A 腐化)。

最后, 当 A 与 B 的对话结束后, B 检查 A 是否在某个 **GroupAuth**(P, I_P) 的运行中成功假冒 u_I。如果是, 令 $(\{R_u\}_{u\in P} \mid P, \sigma, P)$ 是 P 中某个诚实参与者接受认证时的验证信息。这样一个成员的存在是由我们关于 A 成功假冒 u_1 的假设所保证的。那么, B 就输出 $(\{R_u\}_{u\in P} \mid P, \sigma, P)$ 作为他的 IBMS 伪造。另一方面, 如果 A 失败, 那么 B 也宣告失败。

现在我们来分析 B 的成功概率。我们注意到, 在**异常**事件发生后(即 u_I 被腐化), B 宣告失败而中止。此时, 如果我们修改 B: 给他提供 sk_{u_I} 让他正常地与 A 对话直至结束, 那么 A 成功冒充 u_I 的事件也不会发生(因为 u_I 已被腐化, 不符合假冒的条件)。另一方面, 如果**异常**事件不发生, 则 A 与 B 的对话与实际的群认证安全模型中的描述是完全一致的, 而且 B 作为 IBMS 的攻击者也是合法的。最后, 在异常事件发生之前, I 是独立于 A 的所见信息(view)的。因

此, A 在与 B 对话中成功假冒 u_1 的概率为 ε/ν。最后, 当 A 成功时, $(\{R_u\}_{u\in P}\,|\,P,\ \sigma,\ P)$ 是一个有效的签名。另一方面, 由于 P 包含某个诚实的参与者 $u*$, 随机数 R_{u*} 重复以前某个相应数据(群 P 的其他 **GroupAuth** 中的 R_{u*})的概率是可以忽略不计。因此, $\{R_u\}_{u\in P}\,|\,P$ 在以前的签名请求中是没有出现过的。这样, B 的输出 $(\{R_u\}_{u\in P}\,|\,P,\ \sigma,\ P)$ 是一个有效签名伪造。由于 ε/ν 是不可忽略的, 这就与 Π 是安全的 IBMS 签名相矛盾。

5.3 转换应用于基于 ID 的聚合签名

本小节将说明上面的安全转换也可以把基于 ID 的聚合签名转换为一个安全群认证。为此, 我们先介绍基于 ID 的聚合签名。

基于 ID 的聚合签名是一个多方签名方案, 可以让任意的用户子集共同生成签名, 而不需要交互通信。具体说来, 当群 P 希望共同生成一个签名时, P 中每个身份为 id 使用自己的秘密私钥 sk_{id} 独立地生成一个自己对消息 M_{id} 的签名 σ_{id}。然后, 任何人可以用一个聚合算法把所有成员的签名 σ_{id} 融合成一个紧凑的签名 σ。验证算法是输入 $(\sigma,\ P,\ \{M_{id}\}_{id\in P})$, 输出为 1(接受)或 0(拒绝)。

基于 ID 的聚合签名的安全模型跟基于身份的多重签名类似。敌手可以腐化任何成员, 得到其密钥, 也可以请求得到任何成员 id 关于任何消息 M_{id} 的签名 σ_{id}。最后, 这个聚合签名是安全的, 如果没有对手可以伪造某个群 P 的聚合签名 $(\sigma,\ P,\ \{M_{id}\}_{id\in P})$, 这里 P 包含至少一个没被腐化的成员 id 使得 $(id,\ M_{id})$ 从没有被用于签名请求。

我们注意到聚合签名跟多重签名很相似。不同的是, 多重签名需要群中所有成员参与签名交互协议, 而聚合签名中, 每个用户独立地签署自己的消息。当然, 如果每个成员签署同样的消息, 聚合签名就变成了一个特殊的多重签名方案。因此, 如果我们把 5.1 节的安全转换应用于基于 ID 的聚合签名, 那么我们就可以从定理 2 得到如下的推论。

推论 基于 ID 的安全聚合签名意味着一个安全的基于 ID 的多重签名和安全群认证。

6 Bellare-Neven IBMS 用于群认证

在上一节中, 我们通过一个简单的安全转换把 IBMS 转换成群认证协议。这种方法得到的群认证协议的缺点是轮数复杂性增加了。对于具体多重签名方案, 我们或许可以通过其他方式得到安全的群认证协议。下面, 我们证明 Bellare 与 Neven[16]基于 ID 的多重签名方案忽略要签名的消息后实际上就是一个安全的群认证协议。因为这个协议很高效, 我们有必要特别介绍和分析一下。

系统初始化 GM 生成 RSA 公钥 $(N,\ e)$ 和私钥 d。设 $H:\ \{0,1\}^*\to\mathbb{Z}_N^*$ 是一个哈希函数。假定所有可能的成员集合为 $\mathbb{U}$。对于成员 $u\in\mathbb{U}$, 定义其私钥为 $w_u=H(u)^d \bmod N$。系统公钥是 $(N,\ e)$。

GAuth (P) 群 P 打算进行群认证以确认其成员的有效性时, 他们共同执行如下交互协议。

1. 每个 $u\in P$ 选取 $r_u\leftarrow\mathbb{Z}_N^*$, 计算 $R_u=r_u^{\,e} \bmod N$。然后, 他把 $\tau_u=H(R_u)$ 广播到 P 中所有成员。

2. 当每个 u' 收到所有 $u\in P$ 发来的 τ_u, 他把 $R_{u'}$ 广播至 P 中所有成员。

3. 当 $u\in P$ 收到全部 $R_{u'}$ 后, 他验证是否 $\tau_{u'}=H(R_{u'})$。如果不成立, 则他拒绝; 否则, 他计算 $R=\prod_{u'\in P}R_{u'}$, $c=H(P\,|\,R)$ 和 $s_u=r_u w_u^{\,c}$, 并把 s_u 广播至所有 P 中成员。

4. 从每个 $u\in P$ 收到 s_u, u' 检查是否

$$R\Big(\prod_{u\in P}H(u)\Big)^c=\Big(\prod_{u\in P}s_u\Big)^e \bmod N。\tag{11}$$

他接受认证当且仅当等式(11)成立。

协议效率 协议中每个成员仅需要 4 次指数运算和计算 $3|P|+2$ 次乘法, 包括 $\prod_{u\in P}R_u,\prod_{u\in P}H(u),\prod_{u\in P}s_u$, 式(11)左边乘 R 以及 s_u 中乘以 r_u。另外, 每个成员还需要 $|P|+1$ 次计算 H 函数。

安全性 虽然该协议仅仅是 Bellare 和 Neven[16]删除要签名的消息 M 得来的, 但是由于群认证与 IBMS 的安全模型不同, 我们需要重新给出它作为群认证协议的安全证明。不过, 由于这个证明的策略与 Bellare 和 Neven 的 IBMS 证明有相似之处, 我们把它放在附录中。

定理 3. 上面的群认证协议在 RSA 假设下是安全的。

7 群认证与门限签名的关系

在本节中, 我们讨论门限签名与群认证的关系。我们将看到, 虽然前者概念上可以应用到后者, 所得到的群认证方案却没有安全保障。

7.1 门限签名

门限签名本质上是指超过门限数量的成员可以联合生成签名, 而小于或等于门限数量的成员却不能。严格地说, **GM** 生成一个验证密钥 vk 和签名主密钥 sk 。然后, 他把 sk 通过一个 (t, n) 门限秘密分享方案分享给 n 个成员。成员 i 收到的子密钥为 sk_i 。当成员群 P 希望生成消息 M 的签名时, 每个 $i\in P$ 用他的子密钥 sk_i 生成 M 的部分签名 sig_i, 并广播到群 P 的所有成员。最后, 群 P 用公开算法把 sig_i, $i\in P$ 整合成完整的签名 sig 。

在安全模型中, 敌手可以腐化 $t-1$ 个成员, 可以自适应地请求任何消息的签名。安全性要求敌手不能产生新的消息的签名。

7.2 从门限签名到群认证的可能性

门限签名从形式上可以应用于群认证。与多重签名一样, 我们可以附加一个步骤来生成随机消息。即, 对群 P 的认证, 每个成员 i 可以广播一个随机数 R_i 至群 P 的所有成员。然后, P 共同生成 $M=\{R_i\}_{i\in P}\,|\,P$ 的门限签名。

但是, 门限签名的安全性并不能保证得到的群认证协议的安全性。门限签名安全性只能保证敌手在腐化 $t-1$ 个成员后仍然不能独立伪造签名。然而, 群 P 的认证则要求敌手在冒充某诚实成员参与协议运行后不能使任何一个参与协议的诚实成员接受认证。可以看出二者的安全需求是有显著差异的。由于这种差异, 使用上述方法得到的群认证协议没有任何安全保障。

另外, 我们注意到, 门限签名的构造通常是将部分签名使用拉格朗日插值的方式线性组合成完整签名。这种线性性质使得门限构造很方便, 但是应用于群认证也给敌手带来了方便。下面, 我们用一个例子来说明这一点。

7.3 导出群认证协议的不安全性: 一个例子

我们考虑 Boldyreva[27]的门限签名方案。该方案是基于一个差距 Diffie-Hellman(GapDH)假设的。也就是说, DDH 问题很容易(即 DDH 假设不成立), 而 CDH 问题是很难的(即 CDH 假设成立)。

系统初始化 设 $\mathbb{G}$ 是一个满足 GapDH 假设的素数 q 阶群。假定 g 是 $\mathbb{G}$ 的生成元。**GM** 随机选取 $a_0\leftarrow\mathbb{Z}_q$, 计算 $A_0=g^{a_0}$ 。然后, 他随机选取 $a_1, \cdots, a_{t-1}$,定义 $f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}$ 。设 x_i 是成员 i 的标签。**GM** 计算 $y_i=f(x_i)$ 和 $A_i=g^{a_i}$ 。最后, 他设置群公钥为 $(q, g, A_0, \cdots, A_{t-1})$, 成员 i 的私钥为 y_i 。注意, 如果我们定义 $Y_i=g^{y_i}$, 则 Y_i 是可以公开计算的: $Y_i=\prod_{j=0}^{t-1}A_j^{x_i^j}$ 。 由于 y_i 对应于 Y_i , 成员 i 实际上有公钥 Y_i 。只不过这个公钥可由群公钥计算出来而已。

签名 令 H: $\{0,1\}^*\rightarrow\mathbb{G}$ 是一个哈希函数。假设群 P 要共同签署的消息为 M 。那么, 成员 $i\in P$ 可以产生部分签名 $\sigma_i=H(M)^{y_i}$ 并广播给 P 中所有成员。

验证 当 $j\in P$ 收到来至每个成员 $i\in P$ 的部分签名 σ_i 后, 他计算 $\sigma=\prod_{i\in P}\sigma_i^{\lambda_i}$, 其中 $\lambda_i=\prod_{j\in P, i\neq j}\frac{-x_j}{x_i-x_j}$ 是 $\{y_i\}_{i\in P}$ 用等式(1)的拉格朗日插值公式恢复 $a_0=f(0)$ 时 y_i 的系数。签名验证是要检查是否 $(g, A, H(M), \sigma)$ 是一个 Diffie-Hellman 数组(即形如 (g, g^x, g^y, g^{xy}) 的数组), 这里我们用了 DDH 假设很容易攻破这一条件。如果是, 则接受签名; 否则拒绝。

应用于群认证 把上述体制按本节开始的方式应用于群认证。假设 $i\in P$ 在附加步骤中发送的随机数为 R_i , 则 P 将使用上述方案共同生成 $M=\{R_i\}_{i\in P}\,|\,P$ 的签名 σ 。

密码分析 现在我们证明上述所得的群认证是不安全的。令 $P=\{1, \cdots, t+1\}$ 且敌手打算假冒成员 $t+1$ 。由于 $f(x)$ 次数为 $t-1$, 成员 $\{1, \cdots, t\}$ 可以恢复 $f(x)$ 。于是, 可以用拉格朗日插值计算常数 $v_1, \cdots, v_t$ 使得 $y_{t+1}=y_1v_1+\cdots+y_tv_t$ 。 敌手可以用这个关系攻破群认证如下。他先窃听部分签名 $\sigma_i=H(M)^{y_i}$, $i=1, \cdots, t$ 。然后, 他计算部分签名 $\sigma_{t+1}=\prod_{i=1}^{t}\sigma_i^{v_i}=H(M)^{\sum_{i=1}^{t}v_iy_i}=H(M)^{y_{t+1}}$, 正确! 这就成功地冒充了成员 $t+1$ 。

8 结束语

本文研究了群认证协议。这是一种可以认证群成员身份有效性的协议。这里的群可以是不固定的, 而任何群成员都没有个人公钥。另外, 敌手可以进行主动攻击。这种协议非常适合在线会议系统判定是否所有会议成员的身份都是真实的。本文对 Harn 群认证协议提出了一种攻击方案, 证明基于 ID 的多重签名可以安全转换成群认证协议。我们还通过一个

反例表明, 门限签名方案虽然可以形式上应用于群认证, 却不能保证得到的协议的安全性。群认证协议还有些问题可以研究。一个可能的问题是讨论信息论安全的群认证协议的存在性。另一个可能是研究基于对称密码系统的群认证协议的存在性及构造。

致谢 两位审稿专家对本文提出了很多深刻有益的修改意见。作者对此非常感谢。

参考文献

[1] R. M. Needham and M. D. Schroeder, using encryption for authentication in large networks of computers, *Communications of the ACM*, vol 21, pp. 993-999, 1978.

[2] C. P. Schnorr, efficient signature generation by smart cards, *Journal of Cryptology*, no 4, pp. 161-174, 1991.

[3] T. Okamoto, provably secure and practical identification schemes and corresponding signature schemes, in *Proc. Advances in Cryptology-CRYPTO 1992*, E. F. Brickell (Ed.), LNCS 740, Springer, pp. 31-53, 1993.

[4] L. C. Guillou and J. J. Quisquater, a practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory, in Proc. *Advances in Cryptology-EUROCRYPT'88*, C. G. Gunther (Ed.), LNCS 330, Springer, pp. 123-128, 1988.

[5] L. Harn, Group Authentication, *IEEE Transaction on Computers*, Vol. 62, No. 9, pp. 1893-1898, Sept. 2013.

[6] Shi Li, Inshil Doh, Kijoon Chae, A Group Authentication Scheme based on Lagrange Interpolation Polynomial, in *proc 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (IMIS'16), pp. 386-391, IEEE, 2016.

[7] Feng Wang, Chin-Chen Chang and Yeh-Chieh Chou, Group Authentication and Group Key Distribution for Ad Hoc Networks, *International Journal of Network Security*, vol.17, no.2, pp. 199-207, Mar. 2015.

[8] M. Bellare, D. Micciancio and B. Warinschi, Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions, in *Proc. Advances in Cryptology-EUROCRYPT*'03, E. Biham (Ed.), LNCS 2656, Springer-Verlag, pp. 614-629, 2003.

[9] R. L. Rivest, A. Shamir and Y. Tauman, How to Leak a Secret, in *Proc. Advances in Cryptology-ASIACRYPT 2001*, pp. 552-565, 2001.

[10] Y. Komano, K. Ohta, A. Shimbo and S. Kawamura, Toward the fair anonymous signatures: Deniable ring signatures, in *Proc. CT-RSA 2006*, San Jose, CA, USA, 13-17 Feb, pp. 174-191, Springer, 2006.

[11] S. Zeng, S. Jiang and Z. Qin, A new conditionally anonymous ring signature, in *Proc. COCOON* 2011, Dallas, Texas, USA, 14-16 August, pp. 479-491, 2011.

[12] S. Zeng, S. Jiang and Z. Qin, An efficient conditionally anonymous ring signature in the random oracle model. *Theoretical Computer Science*, vol. 461, pp. 106-114, Elsevier , 2012.

[13] S. Zeng, Z. Qin, Q. Lu and Q. Li, Efficient and random oracle-free conditionally anonymous ring signature, in *Proc. ProvSec 2012*, Chengdu, China, 26-28 September, pp. 21-34, 2012.

[14] S Zeng, Q. Li, Z. Qin and Q. Lu, Non-interactive deniable ring signature without random oracles, *Security and Communication Networks*, vol 9, no 12, pp. 1810-1819, 2016.

[15] Q. Wu, W. Susilo, Y. Mu and F. Zhang, Ad hoc group signatures, in *Proc. IWSEC* 2006, Kyoto, Japan, 23-24 October, pp. 120-135, 2006.

[16] M. Bellare and G. Neven, Identity-based multi-signatures from RSA, in *Proc. CT-RSA 2007*, pp. 145-162, Springer, 2007.

[17] C. Gentry and Z. Ramzan, Identity-based aggregate signature. In *Proc. 9th International Conference on Theory and Practice of Public-Key Cryptography* (PKC 2006), LNCS 3958, Springer, pp. 257-273, 2006.

[18] L. C. Guillou and J. J. Quisquater, A "paradoxical" indentity-based signature scheme resulting from zero-knowledge, in *proc Advances in cryptology-CRYPTO'88*, S. Goldwasser (Ed.), LNCS 403, Springer-Verlag, pp. 216–231, 1990.

[19] Lifei Wei, Zhenfu Cao and Xiaolei Dong, Secure identity-based multisignature schemes under quadratic residue assumptions, *Security Comm. Networks*, vol 6, no 6, pp. 689-701, 2013.

[20] Ali Bagherzandi and Stanis_law Jarecki, Identity-Based Aggregate and Multi-Signature Schemes Based on RSA, *Proc 13th International Conference on Practice and Theory in Public Key Cryptography* (PKC 2010), P.Q. Nguyen and D. Pointcheval (Eds.), LNCS 6056, Spinger-verlag, pp. 480–498, 2010.

[21] Song Lin, Biao Wang, Zhoujun Li, Digital multisignature on the generalized conic curve over Zn, *computers & security,* vol28, pp. 100-104, 2009.

[22] SK Hafizul Islam and G. P. Biswas, Cryptanalysis of Lin et al.'s Digital Multi-Signature Scheme on the Generalized Conic Curve Over Zn, *Inf. Sci. Lett.* , vol **3**, no. 2, pp. 63-68, 2014.

[23] Z. Dai, D. Pei and D. Ye, Cryptanalysis of a public key cryptosystem based on conic curves, in *Proc the international workshop on cryptographic techniques and e-commerce* (CrypTec'99), M. Blum (Ed.), HongKong, 1999.

[24] Feng Wang, Chin-Chen Chang, Changlu Lin and Shih-Chang Chang, Secure and Efficient Identity-based Proxy Multi-signature Using Cubic Residues, *International Journal of Network Security,* vol.18, no.1, pp.90-98, 2016.

[25] M. R. Asaar, M. Salmasizadeh and W. Susilo, An identity-based multi-proxy multi-signature scheme without bilinear pairings and its

variants. *The Computer Journal*, vol 58, no 4, pp. 1021-1039, 2015.

[26] Jae Hyun Ahn, Matthew Green, Susan Hohenberger, Synchronized Aggregate Signatures: New Definitions, Constructions and Applications, *Proc. 17th ACM Conference on Computer and Communications Security* (CCS 2010), pp. 473-484, ACM, 2010.

[27] A. Boldyreva. Threshold signatures, multi-signatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme, in *Proc. PKC 2003*, LNCS 2567, Springer-Verlag, 2003.

[28] R. L. Rivest, A. Shamir and L. M. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communication of ACM*, vol 21, no. 2, pp. 120-126, 1978.

[29] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory,* vol. 22, no. 6, pp. 644-654, Nov 1976.

[30] D. Boneh, The Decision Diffie–Hellman Problem, in *Proceedings of the Third Algorithmic Number Theory Symposium* (ANTS'98), LNCS 1423, pp. 48–63, 1998.

[31] A. Shamir, How to share a secret, *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[32] M. Bellare, G. Neven, Multi-Signatures in the Plain Public-Key Model and a General Forking Lemma, in *Proc. 13th ACM Conference on Computer and Communications Security* (CCS 2006), A. Juels et al. (Eds.), pp. 390-399, ACM, 2006.

[33] L. Hua, *Introduction to Number Theory*, Science Press China, 1965. (华罗庚, *数论导引*, 科学出版社, 1965 年)

附录　定理 3 的证明

证明　如果存在敌手 A 以不可忽略的概率 ε 攻破群认证, 则我们构造一个对手 B 以不可忽略的概率 ε' 攻破 RSA 假设。不失一般性, 假设 A 通过假冒某固定成员(记作 u_1)攻破群认证(这个假设只把 A 的成功概率降低了一个多项式分式因子, 因而不影响结果)。另外, 如果认证请求 $\mathbf{GroupAuth}(P, I_P)$ 中, $u_1 \in P$ 且 $P - I_P$ 非空(即 P 至少包含一个诚实的参与者), 那么我们称该认证为**一个特殊的群认证请求**(简记为 **SGA** 请求)。设 A 的 **SGA** 请求总数有上界 υ。为了方便使用分叉引理, B 构造一个算法 A'来实施攻击。A'随机选取 $I \leftarrow \{1, \cdots, \upsilon\}$ (猜测 A 在第 I 次 **SGA** 请求中成功假冒 u_1)。给定公钥 (N, e) 和挑战密文 C, A'运行 A, 提供公钥 (N, e) 并与他进行如下对话。

■ *H -oracle.*　A'为 *H -oracle* 维护一个列表 $\mathbb{L}$ (初始为空)。他首先把 $(u_1, C, \square)$ 添加到 $\mathbb{L}$ 中。以后每当有哈希查询 x, 他检查是否 $\mathbb{L}$ 存在一个纪录 (x, y, z)。如果是, 他返回 y; 否则, 他运行如下策略。

◆ 如果 $x \in \mathbb{U}$, 他随机选取 $m_x \leftarrow \mathbb{Z}_N^*$, 定义 $H(x) = m_x^e \bmod N$, 并把 (x, m_x^e, m_x) 添加到 $\mathbb{L}$ 中。

◆ 如果 $x \notin \mathbb{U}$, 他随机选取 $y \leftarrow \mathbb{Z}_N^*$, 定义 $H(x) = y$, 并把 $(x, y, \square)$ 添加到 $\mathbb{L}$ 中。

从上面的描述, 我们可以看到, H -oracle 是完全定义好的。

■ **成员密钥**　对 $u \neq u_1$, A'从 $\mathbb{L}$ 提取 (u, m_u^e, m_u),并定义私钥 $w_u = H(u)^d = m_u^{ed} \bmod N = m_u$。此外, 定义 $w_{u_1} = H(u_1)^d = C^d$ (对 A'是未知的)。

■ $\mathbf{Corrupt}(u)$　由于 A 不会腐化 u_1(否则, 他不可能假冒 u_1), $u \neq u_1$。于是, A'可以把 m_u 给 A。

■ $\mathbf{GroupAuth}(P, I_P)$　如果 $u_1 \in I_P$ 或者 $u_1 \notin P$, 则 $P - I_P$ 不包含成员 u_1。因为 A'知道所有 $u \neq u_1$ 的密钥 w_u, 他可以扮演 $P - I_P$ 与 A (扮演 I_P)对话运行认证协议。否则, $u_i \in P$ 但 $u_1 \notin I_P$。这种情况下, 对于成员 $u \neq u_1$, A' 拥有 w_u, 因而可以扮演 u。于是, 我们只需要考虑会员 $u = u_1$ 的情形。此时, 他的策略如下。 他首先随机选取 $s_{u_1} \leftarrow \mathbb{Z}_N^*$ 和 $c \leftarrow \mathbb{Z}_N^*$, 计算 $R_{u_1} = s_{u_1}^e C^{-c} \bmod N$ 和 $\tau_{u_1} = H(R_{u_1})$, 并把 τ_{u_1} 广播到 P 中所有成员。当收到其他成员 $u \in P - \{u_1\}$ 的消息 τ_u 后, 他从 $\mathbb{L}$ 查找记录 $(R_u, \tau_u, *)$。我们忽略没有找到该记录的情形(否则后来通过验证 $H(R_u) = \tau_u$ 的概率仅为 $\frac{1}{\varphi(N)}$, 可忽略的!)。然后, A'计算 $R = \prod_{u \in P} R_u$ 并检查是否 $(P \mid R, y, *) \in \mathbb{L}$。我们假定这样的纪录并不存在, 因为 R_{u_1} 独立于 A 在此之前的所见(view)因而他能计算 R 的概率仅为 $\frac{1}{\varphi(N)}$ (可忽略)。这样, A'可以定义 $H(P \mid R) = c$ 并相应地更新 $\mathbb{L}$。本次协议运行剩下的步骤就很容易了, 不再赘述。可以看到群认证请求得到了完美地模拟。

在模拟的最后, A'察看整个历史纪录, 看看是否 A 在第 I 次 **SGA** 请求中成功假冒 u_1。如果是, 则 A'输出 $(I, (s_{u_i}, c))$, 其中 s_{u_1} 是会员 u_1 在第 I 次 **SGA** 请求中步骤 2 的消息而 $c=H(P|R)$。然后, B 把 A'和 A 回朔到第 I 次 **SGA** 请求开始处, 保持 A'和 A 的随机源不变, 除了对于任何 $l \geqslant I$, 第 l 次 **SGA** 请求中 $H(P|R)$ 随机数 c_l 改用新的随机数 c'_l。然后, B 运行 A'和 A 直至结束。假设 A'这次的输出为 $(I', (s'_{u_1}, c'))$, 这里 $c'=c'_I$. 如果 $I \neq I'$, 则 B 宣告失败; 否则, 他检查是否 $\gcd(c'-c, e)=1$。如果不成立, 则 B 同样宣告失败; 否则, 他用扩展欧几里德算法计算 a,b 使得 $a(c'-c)+be=1$。然后, 他输出 $m_{u_1}=(s'_{u_1}/s_{u_1})^a C^b$ 作为他对密文 $m_{u_1}{}^e = C \bmod N$ 的解密结果。这个答案是正确的, 因为 $s_{u_1}{}^e = C^c R_{u_1}$, $s'_{u_1}{}^e = C^{c'} R_{u_1}$ (注意 C 和 R_{u_1} 是保持不变的, 因为整个系统的随机比特只有从第 I 个 SGA 请求中计算 $H(P|R)$ 时才会开始发生变化)。于是, $s_{u_1}=m_{u_1}{}^c r_{u_1}$, $s'_{u_1}=m_{u_1}{}^{c'} r_{u_1}$, 这里 $r_{u_1}{}^e = R_{u_1}$。因此, $(s'_{u_1}/s_{u_1})^a C^b = m_{u_1}{}^{(c'-c)a} m_{u_1}{}^{eb} = m_{u_1}$。

我们现在来分析 B 的成功概率。注意到, 如果 A 在真实的群认证系统中成功假冒 u_1 的概率为 ε, 那么他与 A'的模拟对话在第 I 次 **SGA** 请求中成功假冒 u_1 的概率为 $\frac{\varepsilon}{\upsilon}$。这是因为 I 是完全随机地从 $\{1, \cdots, \upsilon\}$ 中选取, 且独立于 A'与 A 的对话。因此, 利用分叉引理, 以 A'作为引理中的 A, c_i 作为引理中的 γ_i, 我们知道 $I=I'$ 及 $c' \neq c$ 的概率为 $\frac{\varepsilon}{\upsilon}\left(\frac{\varepsilon}{\upsilon^2}-\frac{1}{\varphi(N)}\right)$, 不可忽略! 进一步地, 给定 c, 由于 $c'-c$ 均匀分布于 $\{-c, -c+1, \cdots, N-c-1\}$, 而 $(c'-c) \bmod e$ 在此区间取值 $\lfloor N/e \rfloor$ 或 $\lfloor N/e \rfloor+1$ 次。因此, $\gcd(c'-c, e)=1$ 的概率至少为 $\frac{1}{2}\varphi(e)/e = \frac{1}{2}\prod_{p|e}(1-1/p)$。从引理 2, 我们知道这个概率下界为 $\Omega\left(\frac{1}{\log e}\right) \geqslant \Omega\left(\frac{1}{\log N}\right)$。结合前面的分析, 我们知道 B 成功的概率至少为 $\frac{\varepsilon}{\upsilon}\left(\frac{\varepsilon}{\upsilon^2}-\frac{1}{\varphi(N)}\right) \times \Omega\left(\frac{1}{\log N}\right) = \Omega\left(\frac{\varepsilon^2}{\upsilon^3 \log N}\right)$, 仍然是不可忽略的。这就违背了 RSA 假设。

蒋绍权 于 2005 年在加拿大滑铁卢大学电子信息系统专业获得博士学位。现任绵阳师范学院教授。研究领域为密码学与信息安全。研究兴趣包括: 密码协议、信息论安全、公钥密码系统、通信系统安全和网络安全。
Email: shaoquan.jiang@gmail.com