密钥隔离的无证书聚合签名

寻甜甜[1],于 佳[1,2],杨光洋[1],江秀秀[1],郝 蓉[1]
(1.青岛大学信息工程学院,山东青岛 266071;2.山东省科学院山东省计算机网络重点实验室,山东济南 250014)

摘 要: 无证书的聚合签名的提出是为了解决密钥托管问题以及复杂的证书管理问题.然而在无证书的聚合签名中,一旦某一签名者的密钥发生泄漏,所有由此签名者参与生成的聚合签名都将不再安全.为了减小无证书的聚合签名中密钥泄漏带来的危害,本文首次将密钥隔离安全机制嵌入到无证书的聚合签名中,提出了密钥隔离的无证书聚合签名的概念和安全模型,并给出了一个实用的方案,通过与协助器的交互,实现了对签名者密钥的定时更新.同时证明了方案在随机预言机模型下是安全的,即,满足密钥隔离安全、强密钥隔离安全和安全密钥更新的性质.

关键词: 聚合签名;密钥隔离;无证书签名;密钥托管;双线性配对
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2016)05-1111-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.05.014

Key-Insulated Certificateless Aggregate Signature

XUN Tian-tian[1], YU Jia[1,2], YANG Guang-yang[1], JIANG Xiu-xiu[1], HAO Rong[1]
(1. *College of Information Engineering, Qingdao University, Qingdao, Shandong* 266071, *China*;
2. *Shandong Provincial Key Laboratory of Computer Network, Shandong Academy of Sciences, Jinan, Shandong* 250014, *China*)

Abstract: Certificateless aggregate signature is proposed to solve the key escrow problem and the complex certificate management problem. If the private key of any signer is exposed, the certificateless aggregate signature generated by the users including this signer will no longer be secure. To mitigate the damages of key-exposure in certificateless aggregate signature, we firstly integrate the key isolation mechanism into certificateless aggregate signature, and proposed the definition of key-insulated certificateless aggregate signature and its security model. We give a practical scheme, which achieves the periodical update of the signer′s secret key by the interaction with the helper. We prove the proposed scheme is secure in the random oracle model, i.e., the scheme has key insulated security, strong key insulated security and secure key updates.

Key words: aggregate signature; key insulation; certificateless signature; key escrow; bilinear pairings

1 引言

2003年,Boneh等人[1]提出了聚合签名的概念,并给出了第一个基于双线性配对的聚合签名方案.在此方案中,n个签名者对n个不同消息的签名可以被压缩成单个签名,而验证方只需对合成的单个签名进行一次验证就能够判断签名是否来自这些签名者.为了解决聚合签名中复杂的证书管理问题,Gentry等[2]提出了基于身份的聚合签名方案,在该方案中,签名者的身份可以替代它的公钥,验证者仅使用签名者的身份就可验证签名是否有效,从而简化了证书管理的过程.由于聚合后的签名和单个签名的长度是相同的,因此该方案验证时所需总的信息量较少,可应用于无线网络等领域.Ah Shim等[3]提出了另外一个基于身份的聚合签名方案,该方案具有更高的效率.

然而,在基于身份的聚合签名方案中,存在密钥托管问题,即私钥生成中心(PKG)知道每个用户的私钥.用户私钥是由PKG跟据用户的身份生成的,也就是说不诚实的PKG可以伪造任何用户的签名,因此密钥托管问题严重威胁到基于身份的密码系统的安全.为了解决这个问题,Al-Riyami和Paterson[4]最先提出了无证书的公钥密码体制,密钥生成中心(KGC)生成用户的部分私钥,用户使用部分私钥和自己选取的秘密值独立生成自己的公私钥,因此,KGC无法伪造用户的签

收稿日期:2014-10-20;修回日期:2015-07-01;责任编辑:马兰英
基金项目:国家自然科学基金(No.61272425,No.61572267);山东省计算机网络重点实验室开放课题(No.SDKLCN-2013-03);青岛市建设事业发展项目(No.JK2015-26)

名,从而解决了基于身份的密码系统中的密钥托管问题.由于既能解决密钥托管问题,又能简化公钥证书的管理,无证书密码体制近些年来受到密码学界的广泛关注.Zheng 等[5]首次提出无证书聚合签名方案,安全性只在一个较弱的模型下得到了证明,随后文献[6]强化了无证书聚合签名的安全性模型,并给出了高效的无证书签名方案.Xiong 等[7]提出了具有常数个配对的无证书聚合签名方案,并称方案在随机预言机模型下是可证安全的.文献[8~15]给出了一些其他的无证书签名方案.

然而,在无证书聚合签名中密钥泄露问题是亟待解决的问题,如果一个签名者密钥发生泄漏,由此签名者参与的所有聚合签名将不再安全.Dodis 等[16]提出的密钥隔离机制,可以定时对私钥进行更新并保证用户公钥不变.某一时间段的私钥泄露不会影响其他时间段系统的安全性,有效地降低了密钥泄露带来的危害.万中美提出的标准模型下的无证书密钥隔离签名[17]方案和无证书的强密钥隔离签名[18]方案,减小了无证书签名中的密钥泄漏问题.

密钥隔离的无证书聚合签名方案目前尚未被提出,一个重要的原因是密钥隔离的无证书聚合签名的构造需要满足:聚合签名的长度应与单个签名的长度相同.这需要构造的无证书签名方案同时具有可聚合性和密钥隔离性.本文的主要贡献是解决了上述问题.首先,给出了密钥隔离的无证书聚合签名的概念;然后,给出了其具体的安全性模型;最后,设计了一个高效的密钥隔离的无证书聚合签名方案,并给出了具体的安全性证明和相关效率分析.在提出的方案中,公钥始终不变,签名者通过与协助器的交互,定时对其私钥进行更新.某一签名者密钥即使发生了泄漏,不会影响到其他未发生密钥泄漏时间段有此签名者参与的聚合签名的安全性,从而减少了密钥泄漏带来的危害.本方案生成的聚合签名的长度和单个签名的长度相同,与签名者人数无关.验证时只需要常数个双线性配对,效率较高.本文提出的方案在给出的安全模型下是可证安全的,满足密钥隔离安全,强密钥隔离安全和安全密钥更新的性质.

2 预备知识

2.1 双线性映射

设 G 是加法循环群,G_T 是乘法循环群,它们的阶均是大素数 q,满足以下性质的映射 $\hat{e}:G\times G\to G_T$ 称为双线性映射:

(1)双线性:对于 $\forall P,Q\in G$, $\forall a,b\in Z_q^*$,$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$.

(2)非退化性:$\exists P,Q\in G$,使得 $\hat{e}(P,Q)\neq 1$.

(3)可计算性:存在有效算法,对 $\forall P,Q\in G$,可计算 $\hat{e}(P,Q)$.

2.2 CDH 困难问题假设

定义 1 (CDH 问题) 设 G 是阶为大素数 q 的加法循环群,将群 G 上的 CDH 问题定义为:给定 $P,aP,bP\in G$,其中 $a,b\in Z_q^*$,计算 $abP\in G$.

定义 2 (CDH 假设) 若对于敌手 A,在多项式时间 t 内,其攻破群 G 上的 CDH 问题的概率均小于 ε,则称群 G 上的(t,ε)-CDH 假设成立.

3 密钥隔离的无证书聚合签名的定义和安全模型

3.1 密钥隔离的无证书聚合签名的定义

定义 3 一个密钥隔离的无证书聚合签名方案包括以下 8 个算法:

(1)Setup(k,N):系统建立算法.输入给定安全参数 k 和总时间段数 N,输出 KGC 的主密钥 s 和公开参数 param.

(2)PartialKey$(s,ID_i,param)$:部分私钥生成算法.输入 KGC 的主密钥 s,签名者身份 $ID_i(1\leqslant i\leqslant n)$和公开参数 $param$,输出签名者 ID_i 的部分私钥 $PSK_{i,j}$.

(3)KeyGen$(PSK_{i,j},ID_i,param)$:密钥生成算法.输入给定签名者身份 ID_i 和公开参数 $param$,输出签名者 ID_i 的初始私钥 $USK_{i,j,0}$,公钥 UPK_i,生成协助器的私钥 HSK,公钥 HPK.

(4)UpdateM$(t,ID_i,HSK,param)$:更新消息生成算法.输入签名者身份 ID_i,时间段 t,协助器私钥 HSK 和公开参数 $param$,输出 t 时间段的更新消息 $UK_{i,j,t}$.

(5)UpdateU$(t,ID_i,USK_{i,j,t-1},UK_{i,j,t},param)$,签名者临时密钥更新算法.输入签名者身份 ID_i,时间段 t 时的更新消息 $UK_{i,j,t}$,$t-1$ 时间段签名者的临时私钥 $USK_{i,j,t-1}$和公开参数 $param$,输出签名者 ID_i 在 t 时间段的临时私钥 $USK_{i,j,t}$.

(6)Sign$(t,ID_i,m_i,USK_{i,j,t},param)$:签名算法.输入时间段 t,签名者身份 ID_i,消息 m_i,签名者 ID_i 在 t 时间段的临时私钥 $USK_{i,j,t}$和公开参数 $param$,输出签名者 ID_i 在 t 时间段对消息 m_i 的签名(t,σ_i).

(7)Aggregate$(\{ID_i\}_{i=1}^n,\{(t,\sigma_i)\}_{i=1}^n,param)$:聚合算法.输入参与签名的 n 个成员的身份$\{ID_i\}_{i=1}^n$,t 时间段 n 个成员的单签名和公开参数 $param$,输出聚合后的签名(t,σ).

(8)Verify$(HPK,\{UPK_i\}_{i=1}^n,\{ID_i\}_{i=1}^n,\{m_i\}_{i=1}^n,(t,\sigma),param)$:聚合签名验证算法.输入 t 时间段的聚合签名(t,σ),协助器公钥 HPK,n 个签名者身份$\{ID_i\}_{i=1}^n$,公钥$\{UPK_i\}_{i=1}^n$和其对应消息$\{m_i\}_{i=1}^n$,公开参数 $param$,验证签名是否有效,当签名有效时,该算法输出 1,否

则,该算法输出 0.

3.2 密钥隔离的无证书聚合签名的安全模型

密钥隔离的无证书聚合签名应该抵御两种类型的攻击者. 第Ⅰ类攻击者可以替换其选择用户的公钥(身份),可以得到任意签名者的部分私钥,某些时间段的临时私钥,但是不能得到 KGC 的主密钥. 第Ⅱ类攻击者可以得到 KGC 的主密钥,因此它可以计算用户的部分私钥,也可以得到用户的某些时间段的临时私钥,但是不能替换用户公钥.

假设敌手 A 已经收买了聚合用户集合 $\{ID_i\}_{i=1}^{k}$ 中的 $k-1$ 个,不失一般性,假定用户 ID_1 是未被收买的. 如果敌手要伪造在时间段 t^*,消息集合 $m^* = \{m_1^*, m_2^*, \cdots, m_k^*\}$ 下的聚合签名 (t^*, σ^*).

在密钥隔离安全模型中的查询阶段,敌手 A_I 可以查询用户 ID_1 在任意时间段 t 时的私钥(其中 $t \neq t^*$),还可以查询用户 ID_1 在任意时间参数 t、任意消息 m 下的签名(其中 $t \neq t^*, m \neq m_1^*$),但是敌手 A_I 不可以查询用户 ID_1 的部分私钥. 敌手 A_{II} 可以查询用户 ID_1 在任意时间段 t 时的私钥(其中 $t \neq t^*$),还可以查询用户 ID_1 在任意时间参数 t、任意消息 m 下的签名(其中 $t - t^*, m = m_1^*$),但是敌手 A_{II} 不可以查询用户 ID_1 的秘密值.

在强密钥隔离安全模型中查询阶段,敌手 A_I 可以查询用户 ID_1 在任意时间参数 t、任意消息 m 下的签名(其中 $t \neq t^*, m \neq m_1^*$),但是不可以查询用户 ID_1 的部分私钥. 敌手 A_{II} 可以查询用户 ID_1 在任意时间参数 t、任意消息 m 下的签名(其中 $t = t^*, m = m_1^*$),但是不可以查询用户 ID_1 的秘密值.

定义 4 如果没有攻击者 A 在多项式时间内以不可忽略的概率赢得以下游戏,我们称方案是密钥隔离安全的.

系统建立阶段 挑战者 C 运行 setup 生成公共参数,并给定用户 $ID_1, ID_2, \cdots, ID_k$,将 $ID_2, \cdots, ID_k$ 的私钥和公共参数发送给攻击者 A. 如果是第 I 类攻击者,C 自己保存主密钥,如果是第Ⅱ类攻击者,C 将主密钥发送给 A.

查询阶段 敌手 A 自适应的向挑战者进行以下查询.

(1)部分私钥提取查询:当 A 查询用户 ID_i 的部分私钥时,C 运行 Setup, PartialKey 算法生成部分私钥 $PSK_{i,j}$ 返回给 A. (只用于第一类攻击者)

(2)公钥提取查询:当 A 查询用户 ID_i 的公钥时,C 运行 KeyGen 算法生成用户公钥 UKP_i 返回给 A.

(3)秘密值提取查询:当 A 查询用户 ID_i 的秘密值时,C 运行 KeyGen 算法生成秘密值 x_i 返回给 A. 第一类攻击者查询时,当公钥已被替换则返回 $\perp$.

(4)公钥替换查询:假如 A 要替换 ID_i 的公钥为 UPK_i',C 输入新的公钥替换用户公钥. (只用于第一类攻击者)

(5)密钥提取查询:当 A 查询用户 ID_i 的初始密钥和协助器密钥时,C 运行 KeyGen 算法生成 $USK_{i,j,0}$, HPK, HSK 返回给 A.

(6)临时签名密钥提取查询:当 A 查询用户 ID_i 的 t 时间段的临时签名密钥时,C 运行 UpdateU 算法生成 $USK_{i,j,t}$ 返回给 A.

(7)签名查询:当 A 查询 t 时间段用户 ID_i 对消息 m_i 的签名时,C 运行 Sign 算法生成 (t, σ_i) 返回给 A.

伪造阶段 最终 A 输出 k 个消息 $m_1^*, m_2^*, \cdots, m_k^*$ 和生成的聚合签名 (t^*, σ^*).

当且仅当以下条件成立时,我们说算法 A 赢得了这个游戏:

(1) $Verify(PK_H, Q, \{ID_i\}_{i=1}^{k}, \{m_i^*\}_{i=1}^{k}, (t^*, \sigma^*)) = 1$.

(2)如果是第一类攻击者,没有查询 ID_1 的部分私钥.

(3)如果是第二类攻击者,没有查询 ID_1 的秘密值.

(4)没有查询 t^* 时间段 ID_1 临时签名密钥.

(5)没有查询 t^* 时 ID_1 对消息 m_1^* 的签名.

定义 5 如果没有敌手 A 在多项式时间内以不可忽略的概率赢得以下游戏,我们称方案是强密钥隔离安全的.

其中系统建立阶段,部分私钥提取查询,公钥提取查询,秘密值提取查询,公钥替换查询,签名查询同定义 4.

协助器密钥查询:当 A 查询用户 ID_i 的协助器密钥时,C 运行 KeyGen, PartialKey 算法生成 HSK_i, HPK_i, x_i' 返回给 A.

伪造阶段:最终 A 输出 k 个消息 $m_1^*, m_2^*, \cdots, m_k^*$ 和生成的聚合签名 (t^*, σ^*).

当且仅当以下条件成立时,我们说算法 A 赢得了这个游戏:

(1) $Verify(PK_H, Q, \{ID_i\}_{i=1}^{k}, \{m_i^*\}_{i=1}^{k}, (t^*, \sigma^*)) = 1$.

(2)如果是第一类攻击者,没有查询 ID_1 的部分私钥.

(3)如果是第二类攻击者,没有查询 ID_1 的秘密值.

(4)没有查询 t^* 时 ID_1 对消息 m_1^* 的签名.

定义 6 当用户 i 在时间段 t 将临时私钥从 $USK_{i,j,t-1}$ 更新到 $USK_{i,j,t}$ 时,若敌手对用户设备进行攻击,敌手会获得 $USK_{i,j,t-1}$, $USK_{i,j,t}$ 和 $UK_{i,j,t}$,这与直接将 $USK_{i,j,t-1}$ 和 $USK_{i,j,t}$ 交给敌手相比,敌手获得的用户私钥

信息等同,我们称方案满足安全密钥更新.

4 本文提出的方案

本文提出的密钥隔离的无证书聚合签名方案具体算法描述如下:

(1)系统建立算法 Setup(k,N),输入安全参数 k 和总时间段数 N,该算法按如下步骤生成 KGC 的主密钥 s 和公开参数 $param$:

(a)生成阶为大素数 q 的加法循环群 G 和乘法循环群 G_T,生成双线性映射 $\hat{e}:G\times G\rightarrow G_T$.

(b)选择群 G 的任意生成元 $P\in G$.

(c)选择随机数 $s\in Z_q^*$,令 $Q=s\cdot P$,选择随机数 $P_H\in G$,计算 $D_H=s\cdot P_H$.

(d)选择哈希函数 $H_1,H_3:\{0,1\}^*\rightarrow G,H_2,H_4:\{0,1\}^*\rightarrow Z_q^*$.

(e)输出 KGC 的主密钥 s,公开参数 param = (G,G_T,q,P,Q,P_H,D_H,H_1,H_2,H_3,H_4,$\hat{e}$).

(2)部分私钥生成算法 PartialKey(s,ID_i,$param$),输入 KGC 的主密钥 s 和签名者身份 $ID_i(1\leqslant i\leqslant n)$,KGC 按如下方式生成部分私钥:

(a)计算 $P_{i,j}=H_1(ID_i,j)\in G$,其中 $j\in\{0,1\}$,$PSK_{i,j}=s\cdot P_{i,j}$.

(b)KGC 将部分私钥 $PSK_{i,j}$ 发送给签名者 ID_i.

(3)密钥生成算法 KeyGen($PSK_{i,j}$,ID_i,$param$),输入给定签名者身份 ID_i,按如下方式生成签名者的初始私钥,签名者公钥和协助器的公私钥:

(a)协助器选择随机数 $x'\in Z_q^*$,计算协助器私钥 $HSK=x'\cdot D_H$,协助器公钥 $HPK=x'\cdot Q$.

(b)计算 $b_{i,0}=H_2(ID_i,0)\in Z_q^*$,其中 0 是时间段.

(c)用户选择随机数 $x_i'\in Z_q^*$,计算 $USK_{i,j,0}=x_i\cdot PSK_{i,j}+b_{i,0}\cdot HSK$.

(d)计算 $UPK_i=x_i\cdot Q$.

(e)算法输出签名者 ID_i 的初始私钥 $USK_{i,j,0}$,签名者公钥 UPK_i,协助器公钥 HPK_i,协助器私钥 HSK_i.

(4)更新消息生成算法 Update$M$(t,ID_i,HSK_i,$param$),协助器根据签名者身份 ID_i 计算并输出 t 时间段的更新消息:

$UK_{i,j,t}=HSK_i\cdot(b_{i,t}-b_{i,t-1})$,发送给签名者 ID_i.

(5)签名者临时私钥更新算法 Update$U$(t,ID_i,$USK_{i,j,t-1}$,$UK_{i,j,t}$,$param$),签名者 ID_i 根据更新消息和 $t-1$ 时间段的临时私钥,计算其在 t 时间段的临时私钥:

$$\begin{aligned}USK_{i,j,t}&=USK_{i,j,t-1}+UK_{i,j,t}\\&=x_i\cdot P_{i,j}+HSK_i\cdot b_{i,t-1}+HSK_i\cdot(b_{i,t}-b_{i,t-1})\\&=x_i\cdot P_{i,j}+HSK_i\cdot b_{i,t}\end{aligned}$$

(6)签名算法 Sign(t,ID_i,m_i,$USK_{i,j,t}$,$param$),在 t 时间段,签名者 ID_i 按如下步骤对其对应消息 m_i 进行签名:

(a)与文献[2]的思想类似,第一个签名者选择一个字符串 w 并广播给其他签名者,保证 w 是唯一的.

(b)计算 $P_w=H_3(w)\in G$.

(c)计算 $c_i=H_4(m_i,ID_i,w)\in Z_q^*$.

(d)生成随机数 $r_i\in Z_q^*$.

(e)计算 $S_{i,t}'=r_iP_w+USK_{i,0,t}+c_i\cdot USK_{i,1,t}$,$T_{i,t}'=r_i\cdot P$.

(f)令 $\sigma_i=(w,S_{i,t}',T_{i,t}')$,输出在 t 时间段,第 i 个签名者 ID_i 对消息 m_i 的签名(t,σ_i).

(7)聚合算法 Aggregate(n,$\{(t,\sigma_i)\}_{i=1}^n$,$param$),任何人都可以按如下方式聚合时间段 t 时的 n 个具有相同 w 的单个签名,输出聚合后的签名为(t,σ),其中 $\sigma=(w,S_{n,t},T_{n,t})$,$S_{n,t}=\sum_{i=1}^n S_{i,t}'$,$T_{n,t}=\sum_{i=1}^n T_{i,t}'$.

(8)聚合签名验证算法 Verify(HPK,$\{UPK_i\}_{i=1}^n$,$\{ID_i\}_{i=1}^n$,$\{m_i\}_{i=1}^n$,(t,σ),$param$),验证者输入 t 时间段时聚合签名(t,σ),协助器公钥 HPK,n 个签名者身份 $\{ID_i\}_{i=1}^n$,公钥 $\{UPK_i\}_{i=1}^n$ 和其对应消息 $\{m_i\}_{i=1}^n$,验证以下等式:

$$\begin{aligned}\hat{e}(S_{n,t},P)=\hat{e}(T_{n,t},P_w)\hat{e}\Big(\sum_{i=1}^n(P_{i,0}+c_i\cdot P_{i,1}),\\\sum_{i=1}^n UPK_i\Big)\hat{e}\Big(\sum_{i=1}^n((1+c_i)\cdot b_{i,t}\cdot Q_H),\\HPK\Big)\end{aligned}$$

当等式成立时,该算法输出 1,等式不成立时,该算法输出 0.

5 方案的正确性和安全性分析

5.1 方案的正确性

方案的正确性由以下推导可知:

$$\begin{aligned}&\hat{e}(S_{n,t},P)\\&=\hat{e}\Big(\sum_{i=1}^n(r_i\cdot P_w+US_{i,0,t}+c_i\cdot US_{i,1,t}),P\Big)\\&=\hat{e}\Big(\sum_{i=1}^n r_i\cdot P_w,P\Big)\hat{e}\Big(\sum_{i=1}^n(US_{i,0,t}+c_i\cdot US_{i,1,t}),P\Big)\\&=\hat{e}\Big(\sum_{i=1}^n r_i\cdot P_w,P\Big)\hat{e}\Big(\sum_{i=1}^n((x_i\cdot s\cdot P_{i,0}+x'\cdot s\cdot b_{i,t}\cdot Q_H)\\&\quad+c_i\cdot(x_i\cdot s\cdot P_{i,1}+x'\cdot s\cdot b_{i,t}\cdot Q_H)),P\Big)\\&=\hat{e}\Big(\sum_{i=1}^n r_i\cdot P_w,P\Big)\hat{e}\Big(s\cdot\sum_{i=1}^n x_i\cdot(P_{i,0}+c_i\cdot P_{i,1}),P\Big)\\&\quad\cdot\hat{e}\Big(s\cdot x'\cdot\sum_{i=1}^n((1+c_i)\cdot b_{i,t}\cdot Q_H),P\Big)\\&=\hat{e}\Big(\sum_{i=1}^n r_i\cdot P,P_w\Big)\hat{e}\Big(\sum_{i=1}^n(P_{i,0}+c_i\cdot P_{i,1}),\sum_{i=1}^n(x_i\cdot s\cdot P)\Big)\\&\quad\cdot\hat{e}\Big(\sum_{i=1}^n((1+c_i)\cdot b_{i,t}\cdot Q_H),x'\cdot s\cdot P\Big)\end{aligned}$$

$$=\hat{e}(T_{n,t},P_w)\hat{e}(\sum_{i=1}^{n}(P_{i,0}+c_i\cdot P_{i,1}),\sum_{i=1}^{n}UPK_i)$$
$$\cdot\hat{e}(\sum_{i=1}^{n}((1+c_i)\cdot b_{i,t}\cdot Q_H),HPK).$$

5.2 方案的安全性

下面介绍方案的 5 个安全性定理,考虑篇幅的原因,安全性定理的详细证明见文献[19].

定理 1 假设群 G 中的 CDH 问题成立,则我们所提出的方案在随机预言模型下是密钥隔离安全的. 若敌手 A_I 可以在时间 t 内通过 $q_{H_i}(i=1,2,3,4)$ 次 H_i 预言查询,q_P 次部分私钥提取查询,q_{PK} 次公钥提取查询,q_K 次密钥提取查询,q_T 次临时签名密钥提取查询,q_S 次签名查询,以至少概率 ε 攻破所示方案的密钥隔离安全,则就存在(t',ε')算法 B 可以攻破 CDH 假设,其中

$$\varepsilon\geq\varepsilon'\cdot e\cdot q_S^2\cdot(2q_P+q_T+N),$$
$$t\leq t'-c_G(2q_{H_1}+q_{H_3}+2q_{H_4}+2q_P+q_{PK}+6q_{SK}+4q_T+12q_S+2N+3).$$

定理 2 假设群 G 中的 CDH 问题成立,则我们所提出的方案在预言模型下是强密钥隔离安全的. 若敌手 A_I 可以在时间 t 内通过 $q_{H_i}(i=1,2,3,4)$ 次 H_i 预言查询,q_P 次部分私钥提取查询,q_{PK} 次公钥提取查询,q_H 次协助器密钥提取查询,q_S 次签名查询,以至少概率 ε 攻破所示方案的强密钥隔离安全,则就存在(t',ε')算法 B 可以攻破 CDH 假设,其中,

$$\varepsilon\geq\varepsilon'\cdot e\cdot q_S^2\cdot(q_P+N),$$
$$t\leq t'-c_G(2q_{H_1}+q_{H_3}+2q_{H_4}+2q_P+q_{PK}+6q_{SK}+3q_H+10q_S+2N+3).$$

定理 3 本文提出的方案在两类攻击者的攻击下是满足安全密钥更新的.

定理 4 假设群 G 中的 CDH 问题成立,则我们所提出的方案在预言机模型下是强密钥隔离安全的. 若敌手 A_H 可以在时间 t 内通过 $q_{H_i}(i=1,2,3,4)$ 次 H_i 预言查询,q_P 次部分私钥提取查询,q_{PK} 次公钥提取查询,q_H 次协助器密钥提取查询,q_S 次签名查询,以至少概率 ε 攻破所示方案的强密钥隔离安全,则就存在(t',ε')算法 B 可以攻破 CDH 假设,其中,

$$\varepsilon\geq\varepsilon'\cdot e^2\cdot q_S^2\cdot(q_T+N),$$
$$t\leq t'-c_G(2q_{H_1}+q_{H_3}+2q_{H_4}+q_{PK}+5q_{SK}+4q_T+12q_S+2N+3).$$

定理 5 假设群 G 中的 CDH 问题成立,则我们所提出的方案在预言机模型下是强密钥隔离安全的. 若敌手 A_I 可以在时间 t 内通过 $q_{H_i}(i=1,2,3,4)$ 次 H_i 预言查询,q_P 次秘密值提取查询,q_{PK} 次公钥提取查询,q_H 次协助器密钥提取查询,q_S 次签名查询,以至少概率 ε 攻破所示方案的强密钥隔离安全,则就存在(t',ε')算法 B 可以攻破 CDH 假设,其中

$$\varepsilon\geq\varepsilon'\cdot e^2\cdot q_S^4\cdot N^2,$$
$$t\leq t'-c_G(2q_{H_1}+q_{H_3}+2q_{H_4}+q_{PK}+3q_H+10q_S+2N+3).$$

6 方案性能分析与比较

本节将提出的无证书密钥隔离聚合签名同另外几个签名方案在性能方面的比较见表 1.

表 1 本方案与其他方案的比较

方案	性质	是否聚合签名	安全性	
			是否保证前向安全	是否保证后向安全
Gentry 的方案[2]	基于身份	是	否	否
Zheng 的方案[5]	无证书	是	否	否
万中美的方案[18]	无证书	否	是	是
本文方案	无证书	是	是	是

从表 1 中可以看出,本方案同时满足无证书,聚合和密钥隔离等性质,这是其他方案所没有的. 文献[2,18]是基于身份的签名方法,具有密钥托管问题,本方案和文献[5]不存在这个问题. 在安全性方面,本方案和文献[18]可以提供前向安全性和后向安全性,而文献[2,5]的方案均没有提供这些安全性质,它们不能抵御密钥泄露问题.

表 2 中,n 表示聚合签名中签名者的个数,Pairing 表示一次群 G 中的配对运算,MUL 表示一次群 G 中的乘法运算,忽略群 G 中的加法运算. 一般来说,群中的加法运算耗时可以忽略,配对运算耗时最多. 本方案在生成聚合签名的整个过程中,只需要群 G 中的乘法运算;而验证阶段只需要 4 次配对运算和乘法运算,因此,本方案具有较高的效率.

表 2 本方案的效率分析

算法	Setup	PartialKey	KeyGen	UpdateM	UpdateU	Sign	Aggregate	Verify
运算次数	1MUL	3nMUL	9nMUL	2nMUL		3nMUL		4Pairing +2nMUL

7 结论

为了解决无证书的聚合签名中密钥泄漏的问题,将密钥隔离安全机制嵌入到无证书的聚合签名中,首次提出了密钥隔离的无证书聚合签名的概念和安全模型,并给出第一个具体的方案. 本文提出的无证书密钥隔离聚合签名不需要私用公钥证书,并且不存在密钥托管的问题;同时,运用密钥隔离机制,减少了密钥泄漏带来的危害;方案满足密钥隔离安全,强密钥隔离安全和安全密钥更新等性质,具有很高的安全性;聚合后的签名长度与单个签名长度相同,与签名者人数无关.

参考文献

[1] Boneh D,Gentry C,Lynn B,et al. Aggregate and verifiably

encrypted signatures from bilinear maps[A]. Proceedings of Cryptology-EUROCRYPT 2003[C]. Berlin: Springer-Verlag, 2003. 416 – 432.
[2] Craig G, Zulfikar R. Identity-based aggregate signatures [A]. Proceedings of Public Key Cryptography 2006[C]. Berlin: Springer-Verlag, 2006. 257 – 273.
[3] Kyung A S. An ID-based aggregate signature scheme with constant pairing computations[J]. Journal of Systems and Software, 2010, 83(10): 1873 – 1880.
[4] Al-Riyami S S, Paterson K. Certificateless public key cryptography [A]. Proceedings of Cryptology-ASIACRYPT 2003[C]. Berlin: Springer – Verlag, 2003. 452 – 473.
[5] Zheng G, Yu L, Xuan H, Chen K. Practical Certificateless aggregate signatures from bilinear maps[J]. Journal of Information Science and Engineering, 2008, 26(6): 2093 – 2106.
[6] Zhang L, Zhang F T. Security model for certificateless aggregate signature schemes[A]. Proceedings of Computational Intelligence and Security 2008[C]. Suzhou: IEEE, 2008. 2. 364 – 368.
[7] Xiong H, Guang Z, Chen Z, Li F G. An Efficient certificateless aggregate signature with constant pairing computations [J]. Information Science, 2013, 219(10): 225 – 235.
[8] Chen Y, Horng G, Liu C, et al. Efficient certificateless aggregate signature scheme[J]. J. Electronic Science and Technology, 2012, 10(3): 209 – 214.
[9] Zhou M, Zhang M, Wang C, et al. CCLAS: A practical and compact certificateless aggregate signature with share extraction[J]. International Journal of Network Security, 2014, 16(2): 157 – 164.
[10] Zhang F, Shen L, Wu G. Notes on the security of certificateless aggregate signature schemes[J]. Information Sciences, 2014, 287(10): 32 – 37.
[11] Zhang L, Qin B, Wu Q H, Zhang F T. Novel efficient certificateless aggregate signatures[A]. Proceedings of Applied Algebra, Algebraic Algorithms and Error-Correcting Codes[C]. Berlin: Springer-Verlag, 2009. 235 – 238.
[12] Zhang L, Zhang F T. A new certificateless aggregate signature scheme[J]. Computer Communications, 2009, 32 (6): 1079 – 1085.
[13] Zhang J, Mao J. An efficient RSA-based certificateless signature scheme[J]. Journal of Systems and Software, 2012, 85(3): 638 – 642.
[14] Chen H, Song W G, Zhao B. Certificateless aggregate signature scheme[A]. Proceedings of International Conference on E-Business and E-Government[C]. Guangzhou: IEEE, 2010. 3790 – 3793.
[15] Gong Z, Long Y, Hong X, Chen K F. Practical certificateless aggregate signatures from bilinear maps[J]. Journal of Information Science and Engineering, 2010, 26(6): 2093 – 2106.
[16] Dodis Y, Katz J, et al. Key-insulated public-key cryptosystems [A]. Proceedings of Cryptology-Eyrocrypt 2002 [C]. Berlin: Springer-Verlag, 2002. 65 – 82.
[17] Wan Z, Lai X, Weng J, et al. Certificateless key-insulated signature without random oracles[J]. Journal of Zhejiang University Science A, 2009, 10(2): 1790 – 1800.
[18] Wan Z M, Lai X J, Weng J, Li J G. Certificateless strong key-insulated signature[A]. Proceedings of Information Science and Technology [C]. Nanjing: IEEE, 2011. 270 – 276.
[19] 寻甜甜. 密钥隔离的聚合签名的研究[D]. 青岛: 青岛大学硕士论文, 2015. 34 – 51.

作者简介

寻甜甜 女, 1988 年出生于山东济宁. 青岛大学硕士, 现为山东外事翻译职业学院助教, 主要研究方向信息安全.

于 佳(通信作者) 男, 1976 年生于山东青岛. 青岛大学教授, 信息安全系主任, 研究生导师. 主要研究方向为密码学与信息安全.
E-mail: qduyujia@ gmail. com