并行密钥隔离聚合签名

赵慧艳[1],于 佳[1,2],李 朦[1],寻甜甜[1],赵华伟[2],舒明雷[2]
(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: 为了应对聚合签名中的密钥泄露问题,将并行密钥隔离机制扩展到聚合签名系统中,给出了并行密钥隔离聚合签名的概念.在给出的形式化定义和安全模型的基础上,提出了第一个并行密钥隔离聚合签名方案,并在随机预言模型下证明了方案的安全性.所提出的方案满足密钥隔离性、强密钥隔离性和安全密钥更新等性质,特别在签名验证方面具有较高的效率.引入的两个协助器交替帮助用户进行临时私钥更新,增强了系统防御密钥泄露的能力.

关键词: 密钥隔离;并行性;聚合签名;随机预言模型
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2015)05-1035-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.05.030

Parallel Key-Insulated Aggregate Signature

ZHAO Hui-yan[1], YU Jia[1,2], LI Meng[1], XUN Tian-tian[1], ZHAO Hua-wei[2], SHU Ming-lei[2]
(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: To deal with the key exposure problem in aggregate signature, this paper extends the parallel key-insulated mechanism to aggregate signatures and introduces the primitive of parallel key-insulated aggregate signature. On the basis of formalized definitions and security notions, we propose the first parallel key-insulated aggregate signature scheme and demonstrate that the proposed scheme is provably secure in the random oracle model. The proposed scheme satisfies key-insulated security, strong key-insulated security and secure key-updates. Especially our scheme is high-efficiency in verifications. Two introduced helpers can alternately help users to update the private keys, which strengthen the system's ability to resist the key compromise.

Key words: key-insulation; parallelism; aggregate signature; random oracle model

1 引言

随着数字签名技术越来越多的被应用在便携的、不安全的移动设备中,密钥泄露难以避免.如何处理数字签名中的密钥泄露问题是目前的一个研究热点.密钥演化技术是减小密钥泄露危害的一种方法,包括前向安全技术[1~3]、密钥隔离技术[4,5]和入侵容忍技术[6].第一个有效的密钥隔离签名方案是由 Dodis 等[4]给出的.密钥隔离机制的思想是:将系统的整个生命周期划分为若干时间片段,引入一个安全性较高的外围设备(称作协助器)来帮助用户在每个时间片段进行私钥更新,而公钥保持不变.即使用户一些时间片段的私钥发生泄露,在协助器密钥安全的情况下也不会危害到其他时间片段私钥的安全性.然而,当协助器密钥泄露时,只要用户有一个时间片段的私钥发生泄露,敌手就可以获得该用户的所有时间片段的私钥.为了减小协助器密钥泄露的危害,Hanaoka 等[7]给出了并行密钥隔离概念,使用两个彼此独立的协助器来交替的更新用户私钥.2008 年,Weng 等[8]提出了一个并行密钥隔离签名方案,该方案在随机预言模型下是可证明安全的.之后,密码学家提出了一些密钥隔离签名方案,如文献[9,10].Boneh 等[11]首次提出了聚合签名的概念.在一个聚合签名方案中,不同的用户对不同的消息分别进行签名,这些签名能够合成一个签名,而验证者只需对合成的签名进行验证便可确信签名是否来自指定的用户,从而减小了签名验证的工作量和签名的存储空间.随后,密码学家提出了一些不同的聚合签名方案[12~15].2008 年,Ma 等[16]提出了一个前向安全序列聚合签名方案,但该方案只能保证密钥泄露之前聚合签名的安全性,不能保证之后的安全性,只解决了聚合签名密钥泄露的部分问题.

收稿日期:2014-01-15;修回日期:2014-07-04;责任编辑:蓝红杰
基金项目:国家自然科学基金(No.61272425,No.61202475,No.61402245);青岛市科技计划(No.12-1-4-2(16)-jch,No.13-1-4-151-jch);山东省计算机网络重点实验室开放课题(No.SDKLCN-2013-03);华为科技基金(No.YB2013120027)

为了更好地解决聚合签名中的密钥泄露问题,本文将并行密钥隔离机制引入到聚合签名系统中,提出了并行密钥隔离聚合签名(PKIAS)的概念,不但可以保证密钥泄露之前聚合签名的安全性,还可以保证密钥泄露之后聚合签名的安全性.本文给出了 PKIAS 的形式化定义和安全模型,基于 PKIAS 的定义和安全模型提出了第一个具体的 PKIAS 方案,基于计算 Diffie-Hellman(CDH)假设,证明了方案的安全性.

2 预备知识

2.1 双线性映射

设$\mathbb{G}$是素数 q 阶加法群,$\mathbb{G}_T$ 是 q 阶乘法群,双线性映射 $\hat{e}:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 是满足以下性质的一个映射:

(1)双线性:对于所有的 $P,Q\in\mathbb{G}$, $a,b\in\mathbb{Z}_q^*$,均有 $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$成立.

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

(3)可计算性:对于所有的 $P,Q\in\mathbb{G}$,存在计算 $\hat{e}(P,Q)$的有效算法.

2.2 CDH 困难问题假设

定义 1(CDH 问题) 给定$(P,aP,bP)\in\mathbb{G}^3$,其中 P 是$\mathbb{G}$的一个生成元,对于未知的 $a,b\in\mathbb{Z}_q^*$,计算 $abP\in\mathbb{G}$.定义多项式时间敌手 $\mathcal{A}$ 解决群$\mathbb{G}$上的 CDH 问题的优势为:

$$Adv_{\mathbb{G},A}^{\mathrm{CDH}}=\Pr[P\in_R\mathbb{G},a,b\in_R\mathbb{Z}_q^*:\mathcal{A}(P,aP,bP)=abP]$$

定义 2(CDH 假设) 若任意多项式 t 时间敌手 $\mathcal{A}$ 解决群$\mathbb{G}$上的 CDH 困难问题的优势均小于 ε,则称群$\mathbb{G}$上的(t,ε)-CDH 假设成立.

3 并行密钥隔离聚合签名及安全性概念

3.1 并行密钥隔离聚合签名

设$\mathbb{P}=\{P_1,\cdots,P_n\}$为参与本次聚合签名的 n 个用户的集合,$\mathbb{M}=\{m_1,\cdots,m_n\}$为 n 个不同的消息的集合.每个用户 $P_i(1\leqslant i\leqslant n)$选择不同的 $m_i(1\leqslant i\leqslant n)$进行签名.不失一般性,假设用户 P_i 签名的消息为 m_i,对应签名为 σ_i.

定义 3 一个并行密钥隔离聚合签名方案 PKIAS=(*Setup*, *HelperUpt*, *UserUpt*, *Sign*, *Aggregate*, *Verify*)由以下 6 个算法构成:

①*Setup*:给定安全参数 k 和时间片段总数目 N,生成所有用户的初始私钥 $TSK_{1,0},\cdots,TSK_{n,0}$和公钥 PK,以及两个协助器密钥(HK_0,HK_1).

②*HelperUpt*:给定时间参数 t 和第 j 个协助器密钥 $HK_j(j=t \bmod 2)$,生成时间片段 t 的更新信息 UK_t.

③*UserUpt*:给定用户 $P_i(i=1,2,\cdots,n)$在时间片段 $t-1$ 的临时私钥 $TSK_{i,t-1}$、下一时间段 t 以及对应的更新信息 UK_t,生成用户 $P_i(i=1,2,\cdots,n)$在时间片段 t 的临时私钥 $TSK_{i,t}$,并将 $TSK_{i,t-1}$和 UK_t 删除.

④*Sign*:给定当前时间参数 t、集合中每个用户 P_i 的当前私钥 $TSK_{i,t}$以及用户所要签名的消息 m_i,生成用户 P_i 在时间片段 t 对消息 m_i 的签名(t,σ_i).

⑤*Aggregate*:给定用户集合中每个用户在时间片段 t 的单个签名(t,σ_i),生成用户集合在 t 时间段的聚合签名(t,σ).

⑥*Verify*:给定参与聚合签名的用户集合、消息、聚合签名(t,σ)以及公钥 PK,当签名(t,σ)有效时,返回 1;否则,返回 0.

3.2 安全性概念

在描述 PKIAS 的安全性质之前,为更好的解释敌手 $\mathcal{A}$ 的攻击能力,我们给出了以下预言:

①协助器密钥预言 $HKO(\cdot)$:输入下标 $j(j=t \bmod 2)$,返回第 j 个协助器密钥 HK_j;

②用户临时私钥预言 $TKO(\cdot,\cdot)$:输入时间参数 t、用户参数 i,返回用户 P_i 的临时私钥 $TSK_{i,t}$;

③签名预言 $SO(\cdot,\cdot)$:输入时间参数 t、消息 m_i,返回签名(t,σ_i).

与文献[8]中选择的密钥聚合安全模型相似,在 PKIAS 的安全模型中,敌手可以收买中的用户,进行聚合签名查询.我们允许敌手收买除 1 个特定用户之外的其他所有用户,它的目标是伪造这个诚实的用户.不失一般性,假定诚实的用户是 P_1.

定义 4 令 $\Pi=(Setup,HelperUpt,UserUpt,Sign,Aggregate,Verify)$是一个并行密钥隔离聚合签名方案.将敌手 $\mathcal{A}$ 成功地伪造一个有效的聚合签名的优势定义为:

$$Adv_{A,\Pi}=\Pr\left[\begin{array}{l}(PK,(TSK_{1,0},\cdots,TSK_{n,0}),(HK_0,HK_1))\leftarrow Setup(k,N)\\((t^*,\sigma^*),\mathbb{M})\leftarrow\mathcal{A}^{TKO(\cdot,\cdot);HKO(\cdot);SO(\cdot,\cdot)}(PK)\\Verify((t^*\sigma^*),\mathbb{M},PK)=1\end{array}\right]$$

其中,要求敌手 $\mathcal{A}$ 必须满足以下条件:

(1)查询消息 $m_1,\cdots,m_n$ 是互不相同的.

(2)不允许敌手 $\mathcal{A}$ 对诚实用户 P_1 进行在时间片段 t^* 的临时私钥查询 $TKO(\cdot,\cdot)$.

(3)不允许敌手 $\mathcal{A}$ 对(t^*,m_1)进行签名查询 $SO(\cdot,\cdot)$.

(4)敌手 $\mathcal{A}$ 不能对两个协助器进行协助器密钥查询 $HKO(\cdot)$.

(5)敌手 $\mathcal{A}$ 不能同时进行临时私钥查询 $TKO(1,t^*-1)$和协助器密钥查询 $HKO(t^* \bmod 2)$.

(6)敌手 $\mathcal{A}$ 不能同时进行临时私钥查询 $TKO(1,t^*+1)$和协助器密钥查询 $HKO((t^*+1) \bmod 2)$.

若对于任意多项式时间敌手 $\mathcal{A}$,其优势 $Adv_{\mathcal{A},\Pi}$均

可以忽略,则称方案Π是密钥隔离安全的.

定义 5　令Π=(*Setup*, *HelperUpt*, *UserUpt*, *Sign*, *Aggregate*, *Verify*)是一个密钥隔离安全的 PKIAS 方案.将敌手 $\mathcal{A}$ 成功地伪造一个有效的聚合签名的优势定义为:

$$Adv_{\mathcal{A},\Pi}=\Pr\left[\begin{array}{l}(PK,(TSK_{1,0},\cdots,TSK_{n,0}),(HK_0,HK_1))\leftarrow Setup(k,N)\\((t^*,\sigma^*),\mathbb{M})\leftarrow\mathcal{A}^{SO(\cdot,\cdot)}(PK,HK_0,HK_1)\\Verify((t^*,\sigma^*),\mathbb{M},PK)=1\end{array}\right]$$

其中,要求敌手 $\mathcal{A}$ 必须满足以下条件:

(1)查询消息 $m_1,\cdots,m_n$ 是互不相同的.

(2)不允许敌手 $\mathcal{A}$ 对 (t^*, m_1) 进行签名查询 $SO(\cdot,\cdot)$.

若对于任意多项式时间敌手 $\mathcal{A}$,其优势 $Adv_{\mathcal{A},\Pi}$ 均可以忽略,则称方案Π是强密钥隔离安全的.

定义 6　当用户 i 在时间片段 t 将临时私钥从 $TSK_{i,t-1}$ 更新到 $TSK_{i,t}$ 时,若敌手对用户设备内存进行攻击,敌手会获得 $TSK_{i,t-1}$、$TSK_{i,t}$ 和 UK_t,如果这与直接将 $TSK_{i,t-1}$ 和 $TSK_{i,t}$ 交给敌手相比,敌手获得的用户私钥信息等同,称 PKIAS 方案满足安全密钥更新的性质.

4　PKIAS 方案设计

4.1　提出的方案

(1) *Setup*:输入安全参数 k,执行如下操作:

①选取两个阶均为素数 q 的加法群$\mathbb{G}$和乘法群$\mathbb{G}_T$,设 P 和 Q 是群$\mathbb{G}$的两个不同的生成元,$\hat{e}:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 为双线性映射.

②$H_1:\{0,1\}^*\to\mathbb{G}$和 $H_2:\{0,1\}^*\times\{0,1\}^*\times\mathbb{G}\to\mathbb{Z}_q^*$ 是两个抗碰撞的 hash 函数.

③随机选取两个协助器密钥 $HK_0, HK_1\in_R\mathbb{Z}_q^*$,计算 $HP_0=HK_0\cdot P$, $HP_1=HK_1\cdot P$.

④$\mathbb{P}$中每个用户 P_i 随机选择私钥 $s_i\in_R\mathbb{Z}_q^*$,计算公钥 $PK_i=s_iP$.

⑤每个用户 P_i 的部分初始化临时私钥设定为 $SK_{i,0}=HK_1\cdot H_1(-1)+(s_i+HK_0)\cdot H_1(0)$.

⑥公钥为 $PK=(PK_1,\cdots,PK_n,HP_0,HP_1)$,用户 P_i $(i=1,2,\cdots,n)$ 的初始化临时私钥为 $TSK_{i,0}=(s_i, SK_{i,0})$,两个协助器密钥为 HK_0, HK_1.

(2) *HelperUpt*:给定时间片段参数 t 以及对应的协助器密钥 $HK_j(j=t \bmod 2)$,第 j 个协助器计算时间片段 t 的更新信息 $UK_t=HK_j(H_1(t)-H_1(t-2))$.

(3) *UserUpt*:给定当前时间段 t、用户 $P_i(i=1,2,\cdots,n)$在 $t-1$ 时间段的临时私钥 $TSK_{i,t-1}$及时间片段 t 内的更新信息 UK_t,每个用户 P_i 计算 $SK_{i,t}=SK_{i,t-1}+UK_t+s_i(H_1(t)-H_1(t-1))$,得到新的用户临时私钥 $TSK_{i,t}=(s_i, SK_{i,t})$.

如果令 $l=t \bmod 2$, $l'=(t-1)\bmod 2$,则用户的部分临时私钥具有如下形式:

$$SK_{i,t}=(s_i+HK_l)H_1(t)+HK_{l'}H_1(t-1).$$

(4) *Sign*:给定时间片段参数 t、每个用户的当前临时私钥 $TSK_{i,t}$以及消息 m_i,每个签名者按如下步骤对所选消息进行签名:

①选择 $r_i\in_R\mathbb{Z}_q^*$,计算 $R_i=r_iP$.

②计算哈希值 $h_i=H_2(t,m_i,R_i)$,并令 $S_i=h_ir_iQ+SK_{i,t}$.

③输出签名(t,R_i,S_i).

(5) *Aggregate*:聚合用户收集中所有用户在时间片段 t 的签名,并计算 $S=\sum_{i=1}^{n}S_i$,则用户集合生成的聚合签名为$(t,\sigma)=(t,R_1,\cdots,R_n,S)$.

(6) *Verify*:给定参与聚合签名的用户集合、消息集合、时间参数 t 及 t 时刻的聚合签名(t,σ)和钥 PK,验证者验证以下等式是否成立:

$$\hat{e}(P,S)=\hat{e}(n\cdot HP_{l'},H_1(t-1))\hat{e}(n\cdot HP_l+\sum_{i=1}^{n}PK_i,H_1(t))\hat{e}(Q,\sum_{i=1}^{n}h_i\cdot R_i),$$

如果等式成立,则返回"1";否则,返回"0".

4.2　方案的正确性

$$\begin{aligned}\hat{e}(P,S)&=\hat{e}(P,\sum_{i=1}^{n}S_i)\\&=\hat{e}(P,\sum_{i=1}^{n}(h_ir_iQ+SK_{i,t}))\\&=\hat{e}(P,\sum_{i=1}^{n}SK_{i,t})\hat{e}(P,\sum_{i=1}^{n}h_ir_iQ)\\&=\hat{e}(P,\sum_{i=1}^{n}((s_i+HK_l)H_1(t)+HK_{l'}H_1(t-1)))\\&\quad\hat{e}(\sum_{i=1}^{n}h_i\cdot r_iP,Q)\\&=\hat{e}(\sum_{i=1}^{n}s_i\cdot P,H_1(t))\hat{e}(n\cdot HK_l\cdot P,H_1(t))\\&\quad\hat{e}(n\cdot HK_{l'}\cdot P,H_1(t-1))\hat{e}(\sum_{i=1}^{n}h_i\cdot R_i,Q)\\&=\hat{e}(n\cdot HP_{l'},H_1(t-1))\hat{e}(n\cdot HP_l+\sum_{i=1}^{n}PK_i,H_1(t))\\&\quad\hat{e}(Q,\sum_{i=1}^{n}h_i\cdot R_i)\end{aligned}$$

5　安全性分析

定理 1　假设群$\mathbb{G}$上的 CDH 困难问题成立,则提出的 PKIAS 方案是密钥隔离安全的.具体地说,若存在一个(t,ε)敌手 $\mathcal{A}$ 能够攻破方案的密钥隔离安全性($\mathcal{A}$ 最多进行 q_{H_1}次 H_1 查询,q_k 次临时私钥查询,q_s 次签名查询),那么,可以构造一个(t',ε')算法 $\mathcal{B}$ 来解决$\mathbb{G}$上的 CDH 困难问题,其中 t'和ε'分别满足:

$$t'\leqslant t+(q_{H_1}+3q_k+3q_s+2n+2)t_{sm}+t_{me};$$

$$\varepsilon'\leqslant\min\left(\frac{\varepsilon}{2e(q_k+q_s+n-1)},\frac{\varepsilon(q_k+q_s+n)}{2e^2(q_k+q_s+n-1)^2}\right).$$

此处,e 表示自然对数的底,t_{sm}表示在群$\mathbb{G}$上执行一次标量乘运算的时间,t_{me}表示在群$\mathbb{G}$上执行一次模指数运算的时间.

证明 假设存在一个 CDH 挑战($P, X = aP, Y = bP$)$\in \mathbb{G}^3$, $a, b \in_R \mathbb{Z}_q^*$ 未知.算法 $\mathcal{B}$ 通过与敌手 $\mathcal{A}$ 交互求解 abP 的值.$\mathcal{B}$ 抛一个随机币 $\gamma \in \{0,1\}$,来猜测 $\mathcal{A}$ 将查询第 γ 个协助器密钥 HK_γ.不失一般性,假设 $\gamma = 0$.

(1)系统建立阶段 $\mathcal{B}$ 随机选取 $\varphi, s, HK_0 \in \mathbb{Z}_q^*$,并设 $Q = \varphi P$, $PK_1 = sP$, $HP_0 = HK_0 \cdot P$, $HP_1 = X$,然后将 PK_1, HP_0, HP_1 发送给敌手 $\mathcal{A}$.

(2)查询阶段 敌手 $\mathcal{A}$ 进行以下查询,算法 $\mathcal{B}$ 按如下的方式对 $\mathcal{A}$ 的查询进行应答:

H_1 查询:算法 $\mathcal{B}$ 维持一个元组形如($t, c^{(i)}, \lambda^{(i)}, V^{(i)}$)初始为空的列表 H_1 - list,敌手 $\mathcal{A}$ 对 $< t >$ 进行 H_1 查询时,算法 $\mathcal{B}$ 按照以下方式进行应答:

①若 $< t >$ 已经出现在 H_1 - *list* 列表中,则返回以前设定的值给敌手 $\mathcal{A}$.

②否则,$\mathcal{B}$ 先抛一枚偏币 $c \in \{0,1\}$,其中 $c = 1$ 的概率为 δ.

③算法 $\mathcal{B}$ 随机选取 $\lambda \in \mathbb{Z}_q^*$,若 $c = 0$,则将 H_1 的值设定为 $V = \lambda P$,否则设 $V = \lambda Y$.

④最后,将(t, c, λ, V)添加到列表 H_1 - list 中,并将 V 返回给 $\mathcal{A}$.

H_2 查询:算法 $\mathcal{B}$ 维持一个元组形如($t, m^{(i)}, R^{(i)}, W^{(i)}$)初始为空的列表 H_2 - list,当敌手 $\mathcal{A}$ 对 $< t, m, R >$ 进行 H_2 查询时,算法 $\mathcal{B}$ 按照以下方式进行应答:

①若 H_2 - list 列表中已经包含该元组,则返回此前设定的值给 $\mathcal{A}$.

②否则,算法 $\mathcal{B}$ 随机选取 $W \in \mathbb{Z}_q^*$,将元组 $< t, m, R, W >$ 加入到表 H_2 - list 列表中,并将 W 返回给敌手 $\mathcal{A}$.

签名密钥查询:当敌手对 $< i, t >$ 进行临时私钥查询时,算法 $\mathcal{B}$ 首先从列表 H_1 - list 查找出与用户 P_i 相关的元组(t, c_i, λ_i, V_i)和($t-1, c_i', \lambda_i', V_i'$).

①如果 $1 \equiv t \bmod 2$ 且 $c_i = 0$,则设 $SK_{i,t} = \lambda_i \cdot HP_1 + \lambda_i \cdot PK_i + HK_0 \cdot V'_i$.

②如果 $0 \equiv t \bmod 2$ 且 $c_i = 0, c'_i = 0$,则设 $SK_{i,t} = \lambda'_i \cdot HP_1 + \lambda_i \cdot PK_i + HK_0 \cdot V_i$.

③否则,算法 $\mathcal{B}$ 输出失败并中断游戏.

最后,算法 $\mathcal{B}$ 将 $SK_{i,t}$ 发送给敌手 $\mathcal{A}$.

协助器密钥查询:当敌手 $\mathcal{A}$ 进行协助器密钥查询 HK_1 时,算法 $\mathcal{B}$ 输出失败并中断游戏.否则,算法 $\mathcal{B}$ 把 HK_0 发送给敌手 $\mathcal{A}$.

签名查询:当算法 $\mathcal{B}$ 收到签名查询 $< t, m_i >$ 时,算法 $\mathcal{B}$ 首先从列表 H_1 - list 查找出元组(t, c_i, λ_i, V_i)和($t-1, c_i', \lambda_i', V_i'$),然后随机选择 $r_i \in_R \mathbb{Z}_q^*$,计算 $R_i = r_i \cdot P$.查看元组(t, m_i, R_i, W_i)是否在列表 H_2 - list 中,如果在,算法 $\mathcal{B}$ 从中取得 W_i,否则,随机选取 $W \in \mathbb{Z}_q^*$,并把元组 $< t, m_i, R_i, W >$ 加入到表 H_2 - list 列表中.

①如果 $1 \equiv t \bmod 2$ 且 $c_i = 0$,算法 $\mathcal{B}$ 计算

$$S_i = r_i W_i \cdot Q + \lambda_i \cdot HP_1 + \lambda_i \cdot PK_i + HK_0 \cdot V'_i.$$

②如果 $0 \equiv t \bmod 2$ 且 $c_i = 0, c'_i = 0$,算法 $\mathcal{B}$ 计算

$$S_i = r_i W_i \cdot Q + \lambda'_i \cdot HP_1 + \lambda_i \cdot PK_i + HK_0 \cdot V_i.$$

③否则,算法 $\mathcal{B}$ 输出失败并中断游戏.

最后,算法 $\mathcal{B}$ 把(t, R_i, S_i)发送给敌手 $\mathcal{A}$.

(3)伪造阶段 最后,敌手 $\mathcal{A}$ 输出 $n-1$ 个公钥 $PK_2, \cdots, PK_n$,消息 $m_1, m_2, \cdots, m_n$ 以及 t^* 时间段的伪造聚合签名 σ^*.算法 $\mathcal{B}$ 从列表 H_1 - list 查找出元组($t^*, c_i^*, \lambda_i^*, V_i^*$)和($t^*-1, c_i'^*, \lambda_i'^*, V_i'^*$),若 $1 \equiv t^* \bmod 2$ 且 $c_1^* = 1, c_i^* = 0, 2 \leqslant i \leqslant n$,或者 $0 \equiv t^* \bmod 2$ 且 $c_1'^* = 1, c_i'^* = 0, c_i^* = 0, i \geqslant 2$,算法 $\mathcal{B}$ 继续游戏.否则,算法 $\mathcal{B}$ 输出失败并退出游戏.查找出 $n-1$ 个元组对(t^*, m_i^*, R_i^*, W_i^*),算法 $\mathcal{B}$ 分以下两种情况进行处理:

情况 1:当 $1 \equiv t^* \bmod 2, i \geqslant 2$ 时,令 $S_i^* = \lambda_i^* \cdot HP_1 + \lambda_i^* \cdot PK_i + HK_0 \cdot V_i'^* + \varphi W_i^* \cdot R_i^*$,有

$$\begin{aligned}
&\hat{e}(P, S_i^*) \\
&= \hat{e}(P, \lambda_i^* \cdot HP_1 + \lambda_i^* \cdot PK_i + HK_0 \cdot V_i'^* + \varphi W_i^* \cdot R_i^*) \\
&= \hat{e}(P, \lambda_i^* \cdot HP_1)\hat{e}(P, \lambda_i^* \cdot PK_i)\hat{e}(P, HK_0 \cdot V_i'^*)\hat{e}(P, \varphi W_i^* \cdot R_i^*) \\
&= \hat{e}(\lambda_i^* P, HP_1)\hat{e}(\lambda_i^* P, PK_i)\hat{e}(HK_0 \cdot P, V_i'^*)\hat{e}(\varphi P, W_i^* \cdot R_i^*) \\
&= \hat{e}(H_1(t^*), HP_1 + PK_i)\hat{e}(H_1(t^*-1), HP_0)\hat{e}(Q, W_i^* \cdot R_i^*)
\end{aligned}$$

因此,(t^*, σ_i^*) = (t^*, R_i^*, S_i^*)是一个有效的签名.令 $S_1^* = S^* - \sum_{i=2}^n S_i^*$,可以得到

$$\begin{aligned}
\hat{e}(P, S_1^*) &= \hat{e}(P, S^* - \textstyle\sum_{i=2}^n S_i^*) \\
&= \hat{e}(P, S^*)\hat{e}(P, \textstyle\sum_{i=2}^n S_i^*)^{-1} \\
&= \hat{e}(H_1(t^*), n \cdot HP_1 + \textstyle\sum_{i=1}^n PK_i) \\
&\quad \hat{e}(H_1(t^*-1), n \cdot HP_0)\hat{e}(P, \textstyle\sum_{i=1}^n \varphi W_i^* \cdot R_i^*) \cdot \\
&\quad \hat{e}(H_1(t^*), (n-1) \cdot HP_1 + \textstyle\sum_{i=2}^n PK_i)^{-1} \\
&\quad \hat{e}(H_1(t^*-1), (n-1) \cdot HP_0)^{-1} \\
&\quad \hat{e}(P, \textstyle\sum_{i=2}^n \varphi W_i^* \cdot R_i^*)^{-1} \\
&= \hat{e}(H_1(t^*), HP_1 + PK_1)\hat{e}(H_1(t^*-1), HP_0) \\
&\quad \hat{e}(Q, W_1^* \cdot R_1^*)
\end{aligned}$$

其中,$H_1(t^*) = \lambda_1^* \cdot Y$, $H_1(t^*-1) = V_1'^*$,则

$$\hat{e}(P, S_1^*) = \hat{e}(\lambda_1^* \cdot Y, X)\,\hat{e}(V_1^*, sP)\,\hat{e}(V_1'^*, HK_0 \cdot P)\,\hat{e}(Q, W_1^* \cdot R_1^*).$$

从而算法 $\mathcal{B}$ 按照如下方法计算 abP 的值,从而解决群$\mathbb{G}$上 CDH 问题:

$$abP = (\lambda_1^*)^{-1} \cdot (S_1^* - sV_1^* - HK_0 \cdot V_1'^* - \varphi W_1^* \cdot R_1^*).$$

情况 2:当 $0 \equiv t^* \bmod 2$ 时,令 $S_i^* = \lambda_i^* HP_0 + \lambda_i^* PK_i + \lambda_i'^* \cdot X + \varphi W_i^* \cdot R_i^*$,算法 $\mathcal{B}$ 按照情况 1 的分析方法,计算 abP 的值,从而解决群$\mathbb{G}$上 CDH 问题:

$abP = (\lambda_1'^{*})^{-1} \cdot (S_1^* - sV_1^* - HK_0 \cdot V_1^* - \varphi W_1^* \cdot R_1^*)$.

通过分析容易知道算法 $\mathcal{B}$ 的时间复杂度为

$$t' \leqslant t + (q_{H_1} + 3q_k + 3q_s + 2n + 2)t_{sm} + t_{me}.$$

通过分析算法 $\mathcal{B}$ 在情况 1 和情况 2 中的优势可得,算法 $\mathcal{B}$ 解决群$\mathbb{G}$上 CDH 问题的概率

$$\varepsilon' \leqslant \min(\varepsilon'_1, \varepsilon'_2) =$$

$$\min\left(\frac{\varepsilon}{2e(q_k + q_s + n - 1)}, \frac{\varepsilon(q_k + q_s + n)}{2e^2(q_k + q_s + n - 1)^2}\right).$$

定理 2　假设群$\mathbb{G}$上的 CDH 困难问题成立,则提出的 PKIAS 方案是强密钥隔离安全的.具体地说,若存在一个(t,ε)敌手 $\mathcal{A}$ 能够攻破方案的密钥隔离安全性($\mathcal{A}$ 最多进行 q_{H_1}次 H_1 查询,q_s 次签名查询),那么,可以构造一个(t',ε')算法 $\mathcal{B}$ 来解决$\mathbb{G}$上的 CDH 困难问题,其中 t'和ε'分别满足:

$$t' \leqslant t + (q_{H_1} + 5q_s + 2n + 2)t_{sm} + t_{me};$$

$$\varepsilon' \leqslant \frac{\varepsilon}{e(q_s + n - 1)}.$$

证明　假设存在一个 CDH 挑战$(P, X = aP, Y = bP) \in \mathbb{Z}^3$, $a, b \in_R \mathbb{Z}_q^*$ 未知.算法 $\mathcal{B}$ 通过与敌手 $\mathcal{A}$ 交互求解 abP 的值.

(1)系统建立阶段　$\mathcal{B}$ 随机选取 $\varphi, HK_0, HK_1 \in \mathbb{Z}_q^*$,并设 $Q = \varphi P$, $PK_1 = X$, $HP_0 = HK_0 \cdot P$, $HP_1 = HK_1 \cdot P$.然后将 PK_1, HP_0, HP_1 发送给敌手 $\mathcal{A}$.

(2)查询阶段　在本阶段,敌手 $\mathcal{A}$ 发出以下一系列查询,算法 $\mathcal{B}$ 按如下的方式对 $\mathcal{A}$ 的查询进行应答:

H_1 查询:算法 $\mathcal{B}$ 按照定理 1 的方法应答敌手的查询,不同的是 $c = 1$ 的概率为$\frac{1}{q_s + n}$.

H_2 查询:算法 $\mathcal{B}$ 按照定理 1 的方法应答敌手的查询.

签名查询:当算法 $\mathcal{B}$ 收到一个签名查询 $< t, m_i >$ 时,算法 $\mathcal{B}$ 首先从列表 H_1 - list 查找出元组(t, c_i, λ_i, V_i)和$(t-1, c_i', \lambda_i', V_i')$,然后随机选择 $r_i \in_R \mathbb{Z}_q^*$,计算 $R_i = r_i \cdot P$.查看元组(t, m_i, R_i, W_i)是否在列表 H_2 - list 中,如果在,算法 $\mathcal{B}$ 从中取得 W_i,否则,随机选取 $W \in \mathbb{Z}_q^*$,并把元组 $< t, m_i, R_i, W >$ 加入到表 H_2 - list 列表中.

①如果 $1 \equiv t \bmod 2$ 且 $c_i = 0$,算法 $\mathcal{B}$ 计算

$S_i = r_i W_i \cdot Q + HK_1 \cdot V_i + \lambda_i \cdot PK_i + HK_0 \cdot V'_i$;

②如果 $0 \equiv t \bmod 2$ 且 $c_i = 0$,算法 $\mathcal{B}$ 计算

$S_i = r_i W_i \cdot Q + HK_1 \cdot V'_i + \lambda_i \cdot PK_i + \lambda_i \cdot HP_0$;

③否则,算法 $\mathcal{B}$ 输出失败并中断游戏.

最后,算法 $\mathcal{B}$ 把(t, R_i, S_i)发送给敌手 $\mathcal{A}$.

(3)伪造阶段　最后,敌手 $\mathcal{A}$ 输出 $n-1$ 个公钥 $PK_2, \cdots, PK_n$,消息 $m_1, m_2, \cdots, m_n$ 以及 t^*时间段的伪造聚合签名 σ^*.算法 $\mathcal{B}$ 从列表 H_1 - list 查找出元组$(t^*, c_i^*, \lambda_i^*, V_i^*)$和$(t^*-1, c_i'^*, \lambda_i'^*, V_i'^*)$,若 $c_1^* = 0, c_i^* = 1, 2 \leqslant i \leqslant n$,算法 $\mathcal{B}$ 失败退出.否则,算法 $\mathcal{B}$ 从列表 H_2 - list 查找出 $n-1$ 个元组对$(t^*, m_i^*, R_i^*, W_i^*)$,算法 $\mathcal{B}$ 分以下两种情况进行处理:

情况 1:当 $1 \equiv t^* \bmod 2, i \geqslant 2$ 时,令 $S_i^* = HK_1 \cdot V_i^* + \lambda_i^* \cdot PK_i + HK_0 \cdot V_i'^* + \varphi W_i^* \cdot R_i^*$,算法 $\mathcal{B}$ 可计算 abP 的值:

$abP = (\lambda_1^*)^{-1} \cdot (S_1^* - HK_1 \cdot V_1^* - HK_0 \cdot V_1'^* - \varphi W_1^* \cdot R_1^*)$.

情况 2:当 $0 \equiv t^* \bmod 2, i \geqslant 2$ 时,令 $S_i^* = HK_1 \cdot V_i'^* + HK_0 \cdot V_i^* + \lambda_i^* \cdot PK_i + \varphi W_i^* \cdot R_i^*$,算法 $\mathcal{B}$ 可以成功的计算出 abP 的值:

$abP = (\lambda_1^*)^{-1} \cdot (S_1^* - HK_1 \cdot V_1'^* - HK_0 \cdot V_1^* - \varphi W_1^* \cdot R_1^*)$.

类似于定理 1 的分析,可知算法 $\mathcal{B}$ 的时间复杂度 t'及其攻破群$\mathbb{G}$上的 CDH 困难问题的优势 ε'分别满足

$$t' \leqslant t + (q_{H_1} + 5q_s + 2n + 2)t_{sm} + t_{me};$$

$$\varepsilon' \leqslant \frac{\varepsilon}{e(q_s + n - 1)}.$$

定理 3　提出的 PKIAS 方案是满足安全密钥更新的.

证明　由方案的描述可知,对于任意的时间片段 t,更新信息 UK_t 均可由 $TSK_{i,t-1}$和 $TSK_{i,t}$推出.所以,该方案是满足安全密钥更新要求的.

6　方案分析

表 1 给出了提出方案的主要算法需要的计算量和满足的安全性.提出的 PKIAS 签名方案具有以下优势:

(1)聚合签名的长度更短.聚合签名$(t, R_1, \cdots, R_n, S)$与不聚合签名相比节约了比特空间(表示中群元素的位长度).

(2)验证需要的计算量较小.提出的方案验证算法只要 4 个双线性配对运算,与参与聚合的签名数无关.因此,验证效率较高.

(3)具有更好的灵活性.本文提出的方案中,生成聚合签名的用户群并不是固定的,不同的用户群产生不同的聚合签名,增强了整个系统的灵活性.

(4)安全性更高.方案引入了并行密钥隔离机制,比一般的聚合签名方案安全强度更高.

其中,$M_{\mathbb{G}}$表示$\mathbb{G}$中的点乘运算,$M_{\mathbb{G}_T}$表示$\mathbb{G}_T$ 中的点乘运算,$H_{\mathbb{G}}$表示映射到$\mathbb{G}$哈希函数运算,$H_{\mathbb{Z}_q^*}$表示映射到$\mathbb{Z}_q^*$ 的哈希函数运算,E 表示双线性配对运算.

表 1 方案的性能参数

主要算法需要的计算量	密钥生成	$(2+3n)M_{G}$
	私钥更新	$2nM_{G}+2H_{G}$
	签名生成	$3nM_{G}+nH_{Z_q^*}$
	验证	$4E+(n+2)M_{G}+2M_{G_T}$
聚合签名的长度	$n+1$	
安全性	密钥隔离安全、强密钥隔离安全、安全密钥更新	

7 总结

本文给出了并行密钥隔离聚合签名的概念,增强了聚合签名系统抵御密钥泄露的能力.给出了 PKIAS 的安全模型,并提出了一个可证安全的并行密钥隔离聚合签名方案,不但满足并行密钥隔离机制的所有安全属性,而且签名验证效率较高,只需要 4 个双线性配对运算.在 CDH 困难问题的假设下,证明了提出的方案在随机预言模型下满足密钥隔离安全性、强密钥隔离安全性和安全密钥更新的性质.

参考文献

[1] Bellare M, Miner S. A forward-secure digital signature scheme [A]. Proceedings of the CRYPTO 1999[C]. 1999. 431 – 448.

[2] Yu J, Kong F Y, Cheng X G, et al. One forward-secure signature scheme using bilinear maps and its applications[J]. Information Sciences, 2014, 279: 60 – 76.

[3] Yu J, Hao R, Kong F Y, Cheng X G, et al. Forward-secure identity-based signature: security notions and construction[J]. Information Sciences, 2011, 181(3): 648 – 660.

[4] Dodis Y, Katz J, Xu S, et al. Strong key-insulated signature schemes[A]. Proceedings of the 6th Int Workshop on Practice and Theory in Public Key Cryptography[C]. Berlin: Springer, 2003, 130 – 144.

[5] 葛立荣,于佳,程相国,等.标准模型下支持多协助器的强密钥隔离签名方案[J].计算机研究与发展.2014,51(5):1081 – 1088.
Ge L R, Yu J, Cheng X G, et al. Strong key-insulated signature scheme supporting multi-helpers in the standard model[J]. Journal of Computer Research and Development, 2014, 51(5): 1081 – 1088. (in Chinese)

[6] Yu J, Kong F Y, Cheng X G, Hao R, et al. Intrusion-resilient identity-based signature: security definition and construction[J]. Journal of Systems and Software, 2012, 85(2): 382 – 391.

[7] Hanaoka G, Hanaoka Y, Imai H. Parallel key-insulated public key encryption[A]. Proceedings of Public Key Cryptography-PKC 2006[C]. Berlin: Springer, 2006. 105 – 122.

[8] Weng J, Chen K F, et al. Parallel key-insulated signature framework and construction[J]. Journal of Shanghai Jiaotong University, 2008, 13(1): 6 – 11.

[9] Wan Z M, Lai X J, et al. Strong key-insulated signature in the standard model[J]. Journal of Shanghai Jiaotong University, 2010, 15(6): 657 – 661.

[10] Chen J H, Chen K F, Yu L. Identity-based threshold key-insulated signature[J]. High Technology Letters, 2012, 18(3): 275 – 280.

[11] Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps[A]. Proceedings of Cryptology-Eurocrypt'03[C]. Berlin: Springer, 2003. 416 – 432.

[12] Lu S, Ostrovsky R, Sahai A, Shacham H, et al. Sequential aggregate signatures and multi signatures without random oracles [A]. Proceedings of Cryptology-Eurocrypt'06[C]. Berlin: Springer, 2006. 456 – 485.

[13] Brogle K, Goldberg Sh, Reyzin L. Sequential aggregate signatures with lazy verification from trapdoor permutations[A]. Proceedings of the 18th international conference on The Theory and Application of Cryptology and Information Security [C]. Berlin: Springer, 2012. 644 – 662.

[14] 杜红珍,黄梅娟,温巧燕.高效的可证明安全的无证书聚合签名方案[J].电子学报,2013,41(1):72 – 76.
Du H Z, Huang M J, Wen Q Y. Efficient and provably-secure certificateless aggregate signature scheme[J]. Acta Electronica Sinica, 2013, 41(1): 72 – 76. (in Chinese)

[15] Lu S, Ostrovsky R, Sahai A, Shacham H, et al. Sequential aggregate signatures, multisignatures, and verifiably encrypted signatures without random oracles[J]. Journal of Cryptology, 2013, 26(2): 340 – 373.

[16] Ma D. Practical forward secure sequential aggregate signatures [A]. Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security[C]. New York: ACM, 2008. 341 – 352.

作者简介

赵慧艳 女,1986 年生于山东潍坊.青岛大学硕士.研究方向为信息安全.

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