具有前向安全性质的基于身份的聚合签名方案

韦性佳 张京花 刘增芳 芦殿军
(青海师范大学数学与统计学院 西宁 810008)

摘 要 利用双线性映射、椭圆曲线离散对数、强 RSA 假设,提出了一种具有前向安全性的聚合签名方案。该方案可实现私钥生成中心与签名用户的认证,对签名消息具有前向安全性,进一步保障了系统的安全性。在随机预言模型下证明了该方案在 CDH 问题难解的情况下是安全的。

关键词 聚合签名,前向安全性,计算 Diffie-Hellman 问题,双线性对,强 RSA 假设

中图法分类号 TP309 **文献标识码** A

Identity Based Aggregate Signature Scheme with Forward Security

WEI Xing-jia ZHANG Jing-hua LIU Zeng-fang LU Dian-jun
(College of Mathematics and Statistics, Qinghai Normal University, Xining 810008, China)

Abstract By using the tools of bilinear pairing, discrete logarithm on elliptic curve and strong RSA assumption, this paper proposed a new aggregate signature scheme with forward security. It can realize the authentication between the private key generation center and the signature user, and has the quality of forward security for the signature information, which further guarantees the system's security. The scheme was proved secure in the random oracle paradigm with the assumption that the computational Diffie-hellman (CDH) problem is intractable.

Keywords Aggregate signature, Forward security, Computational Diffie-Hellman problem, Bilinear map, Strong RSA assumption

1 引言

在当今社会,数字签名技术作为保障信息安全的重要手段,已经被广泛应用于日常生产实践中。但随着信息技术的高速发展,传统的一对一的数字签名方案已经无法满足社会的需求,聚合签名(Aggregate Signature, AS)作为一种具有特殊性质的多方参与的数字签名,在效率和安全性方面比传统签名方案更具优势,且已被广泛应用于社会实践中。

2003 年的欧密会上,Boneh 等[1]首次提出了聚合签名的概念,构造了第一个签名方案,并且在随机预言模型(简称 ROM)下证明了方案是抗存在性伪造的。该方案的提出对数字签名的发展具有重要的推动意义。但是,Boneh 的方案存在如下不足[2]:1)计算量较大;2)在安全性方面存在漏洞,可以被模拟敌手攻击;3)在实践中易出错,实用性差。2004 年,Lysyanskaya 等[3]基于陷门置换(trapdoor permutations)提出了第一个有序聚合签名方案(Sequential Aggregate Signature, TP-SAS),但该方案存在一个缺陷,即第 i 个签名者必须用前 $i-1$ 个签名者签署的签名来聚合自己的签名,这就导致签名成本比较高,计算效率相对较低。随后,Cheon 等[4]提出了第一个基于身份的聚合签名方案(简称 IBAS)。Cheng 等[5]和 Xu 等[6]以及 Gentry 等[7]分别提出了几种不同的基于身份的聚合名方案。其中,文献[7]的方案提出了一种非常有效的签名,仅需要 3 个双线性对的运算。近年来,聚合签名的发展极为迅速。2010 年,Shim[8]提出了一种新的 IBAS 方案,该方案极大地降低了聚合签名的计算成本,具有更强的实践价值。2011 年,国内杜红珍等[9]在文献[8]的基础上提出了一种改进的 IBAS 方案。2014 年,Reddy 等[10]提出的一种基于身份的密钥绝缘的聚合签名,使得方案的安全性得到了较大的提升。2016 年,寻甜甜等[11]提出了一种密钥隔离的无证书聚合签名,通过与协助器的交互,实现了对签名者密钥的定时更新。2017 年,许芷岩等[12]构造了一种无线漫游认证中可证安全的无证书聚合签名方案,其不需要双线性对运算,并且具有较高的效率。同年,杜红珍等[13]构造了一种具有固定长度的无证书聚合签名方案,为本文提供了重要的思路。

1997 年,Anderson[14]首次提出了前向安全性理论(forward security)。1999 年,Bellare 等[15-16]提出了一种前向安全的数字签名方案。2001 年,Itkis 等[17]提出一种前向安全签名方案,其有效地实现了签名的验证及存储,但是效率相对较低。2002 年,Kozlov 等[18]利用一种快速的更新算法,提出了一种前向安全的签名方案,该方案周期短,适合移动计算。目前,国内学者针对前向安全性理论也做了大量的研究,比如王彩芬等[19]提出的具有前向安全性的秘密共享方案,其基于有限域上离散对数难解问题和强 RSA 假设,有效地实现了秘密的前向安全性,并且具有很强的实践价值。

本文利用强 RSA 假设[20-21]和椭圆曲线离散对数,在文献[8-10]的基础上提出了一种新的具有前向安全性质的 IBAS

本文受青海省科技创新能力促进计划资助项目(2015-ZJ-724)资助。

韦性佳(1991-),男,硕士生,主要研究方向为代数组合与密码学、数字签名;**张京花**(1990-),女,硕士生,主要研究方向为代数组合与密码学;**刘增芳**(1994-),女,硕士生,主要研究方向为代数组合与密码学;**芦殿军**(1970-),男,教授,主要研究方向为代数组合与密码学、多项式理论、数字签名等,E-mail:ldj@qhnu.edu.cn(通信作者)。

方案。该方案将前向安全性融入到签名的生成过程中，使得敌手即使获取了当前时间的签名信息，也无法得到关于之前签名的任何信息。最后，在 ROM 下证明了所提方案是安全的。

2 基础知识

2.1 强 RSA 问题和强 RSA 假设

强 RSA 问题：给定一个 RSA 模数 $N=pq$，选择 $z\in_R Z_N^*$，计算 $r,y\in Z_N^*$，使得 $y^r=z \bmod N$（其中 $r>1,y\in Z_n^*$）。

强 RSA 假设：在不清楚 N 的因子分解的前提下，强 RSA 问题是难求解的。

2.2 计算性 Diffie-Hellman(CDH)问题

对于 $\forall x,y\in Z_q^*$，给定 $P,xP,yP\in G_1$，其中 P 是 G_1 的生成元，称计算 $xyP\in G_1$ 为 G_1 上的计算性 Diffie-Hellman(CDH)问题；并且对于一个多项式敌手 O，定义 O 在时间 T 内针对 G_1 中 CDH 问题的优势为：$adv_{\mathrm{CDH}}(T)=\Pr[O(P,xP,yP)=xyP:P,xP,yP\in G_1]$。

计算性 Diffie-Hellman(CDH)假设：对于任意一个概率多项式时间运算 O，$adv_{O,G_1}^{\mathrm{CDH}}$ 是可忽略的。

2.3 IBAS 方案的定义与安全模型

定义 1(IBAS 方案的定义) 一个 IBAS 方案由一个私钥生成中心(简称 PKG)、n 个签名者$\{P_1,P_2,\cdots,P_n\}$、一个签名聚合者 A 和一个验证者 V 组成，具体由以下 5 个算法组成。

1)Setup 算法：输入系统安全参数 l，PKG 选择系统主密钥 $s\in Z_q^*$，生成系统公钥 Q，然后输出系统参数 $params$；

2)Key-Extract 算法：PKG 利用 P_i 的身份 ID_i 计算 P_i 的私钥 D_i；

3)Signing 算法：P_i 利用自己的身份 ID_i、消息 m_i 以及 $params$，输出 P_i 在 m_i 上的(单一)签名 σ_i；

4)Aggregate 算法：输入 n 个有效的身份-消息-签名对 $(ID_i,m_i,\sigma_i),i=1,2,\cdots,n$，$A$ 输出这 n 个(单一)签名 σ_i 的聚合签名 σ；

5)Verify 算法：输入 $params$，$ID=\{ID_1,ID_2,\cdots,ID_n\}$，$m=\{m_1,m_2,\cdots,m_n\}$，$\sigma$ 和 V 通过验证等式判断聚合签名的有效性。

IBAS 方案的安全模型：

挑战者 C 运行 Setup 算法，生成系统参数 $params$，将其发给敌手 $Oscar$。$Oscar$ 进行以下 $query$(适应性的)。

1)Hash query：对于任意 Hash 函数的输入，C 返回相应的 Hash 值给 $Oscar$。

2)Key-Extract query：查询 P_i 的私钥，C 运行 Key-Extract 算法，生成相应的私钥 D_i，并返回给 $Oscar$。

3)Signing query：对任意一个消息/身份(m_i,ID_i)的签名询问，C 运行 Signing 算法生成相应的(单一)签名 σ_i，并返回给 $Oscar$。

Forgery：$Oscar$ 输出聚合签名 σ，该签名表示 n 个签名用户 $P=\{P_1,P_2,\cdots,P_n\}$ 分别对 n 个不同的消息 m_i 生成的 n 个(单一)签名 $\sigma_i(i=1,2,\cdots,n)$的聚合签名。

我们说敌手 $Oscar$ 获胜，如果：

1)$Oscar$ 输出关于消息 $m=\{m_1,m_2,\cdots,m_n\}$ 的一个有效的聚合签名 σ^*；

2)至少有一个 ID(这里不失一般性设为 ID_1^*)没有经过 Signing 询问。

定义 2 在 ROM 下，若存在一个敌手 $Oscar$ 在时间 t 内以一个不可忽略的优势 ε 赢得了以上过程(最多执行了 q_H 次 Hash query、q_E 次 Key-Extract query 和 q_S 次 Signing query)，则称 $Oscar$ 以$(t,q_H,q_E,q_S,n,\varepsilon)$攻破了一个有 n 个用户的 IBAS 方案。

定义 3 称 IBAS 是$(t,q_H,q_E,q_S,n,\varepsilon)$抗存在性伪造的，如果没有$(t,q_H,q_E,q_S,n,\varepsilon)$敌手能攻破该方案。

2.4 椭圆曲线离散对数问题(ECDLP)

给定有限域 $GF(q)$ 上的椭圆曲线 E、生成元 $P\in E(GF(q))$、阶 q、$\forall Q\in\langle P\rangle$，寻找 $a\in[0,q-1]$，使得 $Q=aP$。称此问题为椭圆曲线离散对数问题。

2.5 双线性对的基本性质

令$(G_1,+)$和$(G_2,\cdot)$是两个循环群，且$|G_1|=|G_2|=q$(q是大素数)，P 是 G_1 的生成元，存在双线性映射 $e:G_1\times G_1\to G_2$ 满足下列性质：

1)双线性：$\forall P,Q,Q_1,Q_2\in G_1,a,b\in Z_q^*$ 有如下性质：

①$e(aP,bQ)=e(P,Q)^{ab}$；

②$e(P,Q_1+Q_2)=e(P,Q_1)e(P,Q_2)$。

2)非退化性：$\exists P\in G_1$，使得 $e(P,P)\neq 1$。

3)可计算性：$\forall P,Q\in G_1$，存在有效的算法能够计算 $e(P,Q)$。

2.6 前向安全性理论

前向安全性理论(forward security theory)具体如下：1)$P_i(i=1,2\cdots n)$将 S 的有效期分为 T 个时间段；2)在整个有效期内，公钥 PK_U 保持不变，但在第 j 个时间段中私钥 SK_U 随着时间段 j 的改变而变换；3)在第 j 个时段，P_i 计算 $S_j=f(S_{j-1})$，其中 f 是一个单向函数；4)计算出 S_j 后，立即删除 S_{j-1}，这样即使攻击者 A 获得了第 j 个时间段的 S_j 也不能获得关于 $S_0,S_1,\cdots,S_{j-1}$ 的任何信息。如图 1 所示。

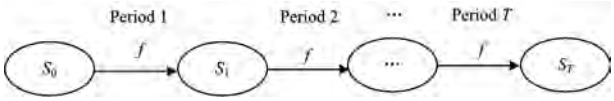

图 1 密钥更新的流程

3 提出的方案

3.1 Setup

给定一个安全参数 l，PKG 的运算如下：

1)生成两个循环群：$(G_1,+),(G_2,\cdot)$，其中，G_1 为椭圆曲线加法群，G_2 为有限域上的乘法群，且$|G_1|=|G_2|=q>2^l$，P 为 G_1 的生成元。

2)双线性映射 $e:G_1\times G_1\to G_2$。

3)T 表示时间周期；$N=p_1p_2$(p_1 和 p_2 是两个大素数)。

4)PKG 计算 $Q=sP$，其中 $s\in_R Z_q^*$。

5)两个 Hash 函数：$H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\to Z_q^*$。

6)系统公开参数：$Params=\{G_1,G_2,e,q,Q,H_1,H_2,N\}$。

3.2 私钥解析算法(PKG 计算)

1)P_i 选择 $ID_i\in\{0,1\}^*$，$r_{i,0}\in_R Z_q^*$，计算 $R_{i,0}=r_{i,0}P$ $(i=1,2,\cdots,n)$，将 $ID_{i,0}$ 和 $R_{i,0}$ 发送给 PKG。

2)PKG 计算：①$Q_i=H_1(ID_i)$；②$D_{i,0}=s(Q_i+R_{i,0})$。

3)PKG 将 $D_{i,0}$ 作为签名初始私钥，并将其通过秘密信道发送给用户 P_i。

3.3 私钥更新算法(P_i 计算)

1)收到签名私钥 $D_{i,0}$ 后，P_i 验证等式 $e(P,D_{i,0})\overset{?}{=}e(Q,$

$Q_i+R_{i,0}$),若等式成立则接受 $D_{i,0}$,反之拒绝;

2)若 $D_{i,0}$有效,则 P_i 计算 $R_{i,j}=r_{i,j}P$,其中 $r_{i,j}=r_{i,j-1}^2 \bmod N$,$j=1,2,\cdots,T$,公开 $R_{i,j}$;

3)P_i 更新第 j 个时间段的签名私钥 $D_{i,j}=D_{i,j-1}+(r_{i,j}-r_{i,j-1})Q$,然后立即删除 $D_{i,j-1}$,$r_{i,j-1}$,$j=1,2,\cdots,T$。

3.4 签名运算(用户 P_i 计算)

1)P_i 计算 $U_{i,j}=r_{i,j}Q$;

2)给定身份、消息 ID_i、$m_i\in\{0,1\}^*$,计算 $h_i=H_2(m_i,ID_i)$;

3)$V_{i,j}=h_iD_{i,j}+U_{i,j}$;

4)$\sigma_{i,j}=\{U_{i,j},V_{i,j}\}$就是第 j 个时间段中 P_i 对消息 m_i 的(单一)签名。

3.5 聚合签名运算

1)聚合签名者 A 计算 $h_i=H_2(m_i,ID_i)$;

2)验证 n 个单一签名 σ_i 的有效性,并检验 n 个等式:

$$e(P,V_{i,j})=e(Q,h_i(Q_i+R_{i,j}))e(P,U_{i,j}),i=1,2,\cdots,n \tag{1}$$

若都有效,则计算 $U_j=\sum_{i=1}^{n}U_{i,j}$,$V_j=\sum_{i=1}^{n}V_{i,j}$,$j=1,2,\cdots,T$;

3)$\sigma_j=\{U_j,V_j\}$ 就是第 j 个时间段对消息 $m=\{m_1,m_2,\cdots,m_n\}$的聚合签名。

3.6 验证运算

1)给定消息 $m=\{m_1,m_2,\cdots,m_n\}$、身份 $ID=\{ID_1,ID_2,\cdots,ID_n\}$、签名 $\sigma_j=\{U_j,V_j\}$,验证者计算 $h_i=H_2(m_i,ID_i)$;

2)验证者验证等式:

$$e(P,V_j)\stackrel{?}{=}e(Q,\sum_{i=1}^{n}h_i(Q_i+R_{i,j}))e(P,U_j) \tag{2}$$

若等式(2)成立,验证者接受聚合签名,反之拒绝。

4 正确性与安全性分析

4.1 正确性分析

定理 1 若聚合者接受第 j 个时间段的(单一)签名 $\sigma_{i,j}=\{U_{i,j},V_{i,j}\}$,当且仅当等式(1)成立。

证明:(充分性)若聚合者接受签名 $\sigma_{i,j}=\{U_{i,j},V_{i,j}\}$,则一定有 $U_{i,j}=r_{i,j}P$,$V_{i,j}=h_iD_{i,j}+r_{i,j}Q$。

因为 $e(P,V_{i,j})=e(P,h_iD_{i,j}+U_{i,j})$

$=e(P,h_i(D_{i,j-1}+(r_{i,j}-r_{i,j-1})Q)+U_{i,j})$

$=e(P,h_is(Q_i+R_{i,j})+U_{i,j})$

$=e(sP,h_i(Q_i+R_{i,j})e(P,U_{i,j})$

$=e(Q,h_i(Q_i+R_{i,j}))e(P,U_{i,j})$

所以等式(1)成立。

(必要性)若等式(1)成立,即

$e(P,V_{i,j})=e(Q,h_i(Q_i+R_{i,j}))e(P,U_{i,j})$

$=e(P,s(h_i(Q_i+R_{i,j})+U_{i,j})$

$=e(P,(h_is(Q_i+R_{i,j})+U_{i,j})$

$=e(P,h_iD_{i,j}+U_{i,j})$

即有 $V_{i,j}=h_iD_{i,j}+U_{i,j}$,所以$(U_{i,j},V_{i,j})$就是对消息 m_i 的有效签名,因此签名者接受签名信息。

定理 2 若验证者接受第 j 个时间段的签名 $\sigma_j=\{U_j,V_j\}$,当且仅当等式(2)成立。

证明:(充分性)若聚合者接受签名 $\sigma_j=\{U_j,V_j\}$,则一定有 $U_j=\sum_{i=1}^{n}U_{i,j}$,$V_j=\sum_{i=1}^{n}V_{i,j}U_{i,j}=r_{i,j}Q$,$V_{i,j}=h_iD_{i,j}+U_{i,j}$。

因为 $e(P,V_j)=e(P,\sum_{i=1}^{n}V_{i,j})=e(P,\sum_{i=1}^{n}h_iD_{i,j}+U_{i,j})$

$=e(P,\sum_{i=1}^{n}h_i(D_{i,j-1}+(r_{i,j}-r_{i,j-1})Q)+U_{i,j})$

$=e(P,\sum_{i=1}^{n}h_is(Q_i+R_{i,j}))e(P,U_j)$

$=e(Q,\sum_{i=1}^{n}h_i(Q_i+R_{i,j}))e(P,U_j)$

所以等式(2)成立。

(必要性) 若等式(2)成立,即

$$\begin{aligned}e(P,V_j)=e(P,\sum_{i=1}^{n}V_{i,j})&=e(Q,\sum_{i=1}^{n}h_i(Q_i+R_{i,j}))e(P,U_j)\\&=e(P,\sum_{i=1}^{n}(h_is(Q_i+R_{i,j})+U_{i,j}))\\&=e(P,\sum_{i=1}^{n}(h_iD_{i,j}+U_{i,j}))\end{aligned}$$

即有 $V_{i,j}=h_iD_{i,j}+U_{i,j}$,所以$(U_j,V_j)$就是对消息 $m=\{m_1,m_2,\cdots,m_n\}$的有效聚合签名,因此验证者接受聚合签名信息。

4.2 安全性分析

定理 3 方案具有前向安全性。

证明:$Oscar$ 如果掌握第 j 个时间段的签名信息:$U_{i,j}=r_{i,j}Q$,$V_{i,j}=h_iD_{i,j}+U_{i,j}$,以及签名者私钥$r_{i,j}$,并且想获取 $U_{i,k}$和 $V_{i,k}$($i=1,2,\cdots,n$;$k=1,2,\cdots,j-1$),则必须获得签名者私钥 $r_{i,k}$和 $D_{i,k}$($k=1,2,\cdots,j-1$),又因为 $D_{i,j}=D_{i,j-1}+(r_{i,j}-r_{i,j-1})Q$,则必须获得 $r_{i,j-1}$。由于 $r_{i,j}=r_{i,j-1}^2 \bmod N$ 必须解决强 RSA 假设,但是强 RSA 假设是难解问题,因此敌手无法获取签名 $V_{i,k}$($k=1,2,\cdots,j-1$)的任何信息,这就保障了签名信息的前向安全性。

定理 4 在 ROM 下,假设敌手 $Oscar$ 以$(t,q_{H_1},q_{H_2},q_E,q_S,n,\varepsilon)$攻破本方案,其中 q_{H_1},q_{H_2},q_E,q_S 分别表示 A 访问 H_1 和 H_2 预言机、私钥解析预言机、签名预言机的次数,则存在一个算法 C 以优势

$$\varepsilon'\geqslant\varepsilon\delta^{q_E+q_S+1}(1-\delta)^{n-1}(n\leqslant q_{H_1},q_{H_2},q_E,q_S;0\leqslant\delta\leqslant1)$$

在时间

$$t'<t+(q_{H_1}+2q_E+3q_S+n+2)t_{\mathrm{sm}}+t_{\mathrm{inv}}$$

内解决群 G_1 中的 CDH 问题。t_{sm}表示计算 G_1 中的标量乘法所用时间,t_{inv}表示计算群 G_2 乘法逆所用的时间。

证明:设 C 为 CDH 攻击算法,给定群 G_1 中一个任意的实例(P,aP,bP),C 的目标为输出 CDH 问题的解 abP。

1)C 运行 setup 算法

定义系统公钥 $Q=aP$,生成系统参数 $Params=\{l,G_1,G_2,e,q,Q,H_1,H_2,N\}$发送给 $Oscar$。$Oscar$ 执行以下询问:

①Hash 询问

C 维护两张列表 L_1 和 L_2,它们分别用于跟踪对 H_1 和 H_2 的询问,且初始都为空。

②H_1 询问

当 $Oscar$ 以 $ID_i\in\{0,1\}^*$ 作为输入,C 调出列表 L_1 时,若 L_1 中已有相应的记录(ID_i,Q_i,t_i,c_i),则返回 Q_i 给 $Oscar$,否则 C 选取 $t_i\in_R Z_q^*$。抛掷一个偏心硬币 $c_i\in\{0,1\}$,$\Pr[c_i=0]=\delta$,$\Pr[c_i=1]=1-\delta$,若 $c_i=0$,则定义 $Q_i=t_iP$,否则 $Q_i=t_i(bP)$,添加(ID_i,Q_i,t_i,c)到列表 L_1 中,返回 Q_i 给 $Oscar$。

③H_2 询问

当 $Oscar$ 以 $ID_i,m_i\in\{0,1\}^*$ 作为输入,C 调出列表 L_2 时,若 L_2 中已有相应的记录,则返回之前定义的 h_i 给 $Oscar$,否则选择 $v_i\in_R Z_q^*$ 给 $Oscar$。

2)私钥解析询问

C 维持列表 L_3,给定 ID_i,C 从列表 L_1 中调出(ID_i,Q_i,t_i,c_i),若 $c_i=1$,则停止模拟,输出 failure;否则选择 $r_{i,j}\in {}_RZ_q^*$,计算 $D_{i,j}=D_{i,j-1}+(r_{i,j}-r_{i,j-1})Q=a(Q_i+R_{i,j})=at_iP+r_{i,j}Q$,将($ID_i$,$D_{i,j}$)添加到 L_3 中,返回 $D_{i,j}$ 给 $Oscar$。

3)签名询问

当 $Oscar$ 对(ID_i,m_i)进行签名询问时,C 从列表 L_1 中调出(ID_i,Q_i,t_i,c_i),计算 $U_{i,j}=r_{i,j}Q$,则 $V_{i,j}=(at_iP+r_{i,j}Q)v_i+U_{i,j}$,输出 $\sigma_{i,j}=\{U_{i,j},V_{i,j}\}$ 就是对消息 m_i 的签名。

上述过程中 $Oscar$ 生成的签名 $\sigma_{i,j}$ 是有效的。原因如下:

$$\begin{aligned}e(P,V_{i,j})&=e(P,(at_iP+r_{i,j}Q)v_i+U_{i,j})\\&=e(P,(at_iP+r_{i,j}aP)v_i)e(P,U_{i,j})\\&=e(aP,(t_iP+r_{i,j}P)v_i)e(P,U_{i,j})\\&=e(Q,(Q_i+R_{i,j})v_i)e(P,U_{i,j})\end{aligned}$$

4)伪造过程

当 C 承认失败,或者产生第 j 个时间段的签名 σ_j^* 时,$Oscar$ 停止模拟。C 从列表 L_1 中调出(ID_i^*,Q_i^*,t_i^*,c_i^*),若 $c_1^*=1$ 且 $c_i^*=0(i=2,3,\cdots,n)$时继续,否则 C 宣布 failure 并停止。若继续,因 $H_1(ID_1^*)=t_1^*(bP)$,$H_1(ID_i^*)=t_i^*P$,$i=2,3,\cdots,n$,因此伪造的签名必须满足 $e(P,V_j)=e(Q,\sum_{i=1}^{n}h_i(Q_i+R_{i,j}))e(P,U_j)$。

C 检索列表 L_3 中的记录(ID_i^*,$D_{i,j}^*$),然后调出列表 L_1 中的记录(ID_i^*,Q_i^*,t_i^*,c_i^*),计算 $V_{i,j}^*=(at_i^*P+r_{i,j}^*Q)v_i^*+U_{i,j}^*$,$i=2,3,\cdots,n$。则有:

$$\begin{aligned}e(P,V_{i,j}^*)&=e(P,(at_i^*P+r_{i,j}^*Q)v_i^*+U_{i,j}^*)\\&=e(P,(at_i^*P+r_{i,j}^*aP)v_i)e(P,U_{i,j}^*)\\&=e(aP,(t_i^*P+r_{i,j}^*P)v_i^*)e(P,U_{i,j}^*)\\&=e(Q,(Q_i^*+R_{i,j}^*)v_i^*)e(P,U_{i,j}^*)\end{aligned}$$

因此签名 $\sigma_{i,j}^*$ 是有效的。

然后,C 考虑 $V_1^*=V^*-\sum_{i=2}^{n}V_i^*$,则输出

$$\begin{aligned}e(P,V_1^*)&=e(P,V^*-\sum_{i=2}^{n}V_i^*)\\&=e(P,U_{1,j}^*)e(Q,v_1^*(t_1^*bP+r_{1,j}^*P))\\&=e(P,U_{1,j}^*)e(P,v_1^*(t_1^*abP+r_{1,j}^*aP))\\&=e(P,U_{1,j}^*+v_1^*t_1^*abP+v_1^*rU_{1,j}^*))\\&\Rightarrow V_1^*=U_{1,j}^*(1+v_1^*)+v_1^*t_1^*abP\\&\Rightarrow v_1^*t_1^*abP=V_1^*-(1+v_1^*)U_{1,j}^*\\&\Rightarrow abP=(v_1^*)^{-1}(t_1^*)^{-1}(V_1^*-(1+v_1^*)U_{1,j}^*)\end{aligned}$$

C 输出 abP 作为 $Oscar$ 挑战的应答,这样 C 就解决了 CDH 难题的一个实例。

下面分析 C 在该游戏中成功的概率,定义 4 个独立事件 E_1,E_2,E_3,E_4。

E_1:C 回答私钥解析询问没有失败;

E_2:C 回答签名时询问没有失败;

E_3:$Oscar$ 生成一个有效的在 n 个消息/身份(m_i,ID_i)上的聚合签名;

E_4:E_3 中 n 个身份 ID_i 中至少有一个身份在 L_1 中记录 $c=1$。

显然 $\Pr[E_1]\geqslant\delta^{q_E}$,$\Pr[E_2|E_1]\geqslant\delta^{q_S}$,$\Pr[E_3|E_2\wedge E_1]\geqslant\varepsilon$,$\Pr[E_4|E_3\wedge E_2\wedge E_1]\geqslant(1-\delta)^{n-1}\delta$。因此 $\Pr[E_4\wedge E_3\wedge E_2\wedge E_1]=\Pr[E_1]\Pr[E_2|E_1]\Pr[E_3|E_2\wedge E_1]$。$\Pr[E_4|E_3\wedge E_2\wedge E_1]\geqslant\delta^{q_E}\delta^{q_S}\varepsilon(1-\delta)^{n-1}\delta=\varepsilon\delta^{q_E}\delta^{q_S+1}(1-\delta)^{n-1}=f(\delta)$,即 $\varepsilon'\geqslant\varepsilon\delta^{q_E}\delta^{q_S+1}(1-\delta)^{n-1}$。

为了最大化 $f(\delta)$,因为 $f(\delta)$ 为[0,1]上的一个常数,所以对 $\varepsilon\delta^{q_E}\delta^{q_S+1}(1-\delta)^{n-1}=f(\delta)$ 两边同时求导,有:

$$\begin{aligned}&\Rightarrow\varepsilon(q_E+q_S+1)\delta^{q_E+q_S}(1-\delta)^{n-1}+\varepsilon\delta^{q_E+q_S+1}(n-1)(1-\delta)^{n-2}(-1)=0\\&\Rightarrow(q_E+q_S+1)(1-\delta)-\delta(n-1)=0\\&\Rightarrow\delta(q_E+q_S+1+n)=(q_E+q_S+1)\\&\Rightarrow\delta=\frac{(q_E+q_S+1)}{(q_E+q_S+1+n)}\end{aligned}$$

因此,C 成功解决 CDH 问题的概率至少为:

$$\varepsilon'\geqslant\varepsilon(\frac{q_E+q_S+1}{q_E+q_S+1+n})^{q_E+q_S+1}(\frac{n}{q_E+q_S+1+n})^{n-1}$$

最后,显然 C 在该游戏中的运行时间为:$t'<t+(q_{H_1}+2q_E+3q_S+n+2)t_{sm}+t_{inv}$。

这说明,若 $Oscar$ 在时间 t 内以 ε 的优势成功伪造了本方案的聚合签名,则 C 可以在时间 t' 内以 ε' 的优势解决 G_1 上的 CDH 问题,然而 CDH 问题是难解的,因此本文的方案在随机预言模型下是抗存在性伪造的。

5 效率分析

用 S 表示标量乘法,E 表示双线性运算,本文方案与其他方案的效率比较结果如表 1 所列。

表 1 各方案的效率比较

IBAS 方案	Sign	Verify	Sign length	Forward security	Security
本文方案	$3S$	$nS+3E$	$2\|G_1\|$	Yes	Provable
文献[8]	$2S$	$nS+2E$	$(n+1)\|G_1\|$	No	Provable
文献[13]	$3S$	$nS+(n+3)E$	$2\|G_1\|$	No	Provable

可以看出,与文献[8]和文献[13]方案相比,本文方案的效率与签名长度都有了改进,其最大特点是实现了前向安全性。

结束语 本文利用强 RSA 假设与椭圆曲线离散对数问题,构造了一种具有前向安全性质的 IBAS 方案。该方案在 Key-Extract 阶段实现了 PKG 与 P_i 的双向验证;在 Signing 阶段,实现了方案的前向安全性,敌手即使掌握当前时间段的签名信息,也仍然无法获取之前时间段的任何信息,从而进一步保障了系统的安全性。然后,我们在 ROM 下对方案的安全性进行了分析,证明了所提方案在 CDH 问题难解的情形下是抗存在性伪造的。最后,将所提方案与文献[8]和文献[13]的方案进行了效率对比,并证明了所提方案实现的签名信息是前向安全的。

参 考 文 献

[1] BONEH D,GENTRY C,LYNN B,et al. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps[J]. Lecture Notes in Computer Science,2002,2656(1):416-432.

[2] KWANGSU L,DONG H,L,MOTI Y. Sequential aggregate signatures with short public keys without random oracles[J]. Theoretical Computer Science 2015,579(C):100-125.

[3] LYSYANSKAYA A,MICALI S,REYZIN L,et al. Sequential Aggregate Signatures from Trapdoor Permutations [M]// Advances in Cryptology-EUROCRYPT 2004. Springer Berlin Heidelberg,2003:74-90.

[4] CHEON J,KIM Y,YOON H. A new ID-based signature with batch verification[J]. Cryptology e-Print Archive,2004.

[5] CHENG X，LIU J，GUO L，et al. Identity-based multi-signature and aggregate signature schemes from m-torsion groups [J]. Journal of Electronics (China)，2006，23(4)：569-573.

[6] XU J，ZHANG Z，FENG D. ID-Based Aggregate Signatures from Bilinear Pairings [M]// Cryptology and Network Security. Springer Berlin Heidelberg，2005：110-119.

[7] GENTRY C，RAMZAN Z. Identity-Based aggregate signatures [C]// International Conference on Theory and Practice of Public-Key Cryptography. Springer-Verlag，2006：257-273.

[8] SHIM K. An ID-based aggregate signature scheme with constant pairing computations[J]. Journal of Systems & Software，2010，83(10)：1873-1880.

[9] 杜红珍，温巧燕. 高效的基于身份的聚合签名方案[J]. 四川大学学报(工程科学版)，2011，43(1)：87-90.

[10] REDDY P，GOPAL P. Identity-based key-insulated aggregate signature scheme[J]. Journal of King Saud University Computer and Information Sciences，2015，29(3)：303-310.

[11] 寻甜甜，于佳，杨光洋，等. 密钥隔离的无证书聚合签名[J]. 电子学报，2016，44(5)：1111-1116.

[12] 许芷岩，吴黎兵，李莉，何德彪. 无线漫游认证中可证安全的无证书聚合签名方案[J]. 通信学报，2017，38(7)：123-130.

[13] 杜红珍，温巧燕. 无证书聚合签名方案的攻击与改进[J]. 中山大学学报(自然科学版)，2017，56(1)：77-84.

[14] ANDERSON R. Two remarks on public-key cryptology[C]// ACM Conference on Computer and Communications Security. 1997.

[15] BELLARE M，MINER S. A Forward-Secure Digital Signature Scheme[C] // International Cryptology Conference. Springer Berlin Heidelberg，1999：431-448.

[16] BELLARE M，YEE B. Forward security in private key cryptography[J]. Lecture Notes in Computer Science，Springer-Verlag，Berlin，2003：1-18.

[17] ITKIS G，REYZIN L. Forward-Secure Signatures with Optimal Signing and Verifying [M]// Advances in Cryptology - CRYPTO 2001. Springer Berlin Heidelberg，2001：332-354.

[18] KOZLOV A，REYZIN L. Forward-Secure Signatures with Fast Key Update [M] // Security in Communication Networks. Springer Berlin Heidelberg，2003：241-256.

[19] 王彩芬，刘国军，贾爱库，等. 具有前向安全性质的秘密共享方案. [J]电子与信息学报，2006，28(9)：1974-1976.

[20] 汪保友，胡运发. 基于强 RSA 假设的签名方案[J]. 软件学报，2002，13(8)：1729-1734.

[21] 徐文华，贺前华，李韬. 基于强 RSA 假设的数字签名方案[J]. 华中科技大学学报(自然科学版)，2008，36(12)：24-26.

(上接第 363 页)

综上，ASQN 中的量子信道恢复机制所需时间短，占用的网络资源也更少，因此 ASQN 中量子信道故障恢复机制是有效的。

结束语　本文分析了现有量子密钥分发网络存在的问题，提出了一种基于光开关切换的 QKD 网络模型 ASQN，同时提出了一种基于多路径策略和源路由技术的先导信号协议。同时，量子密钥分发通信过程需要进行大量信息的交互，而这些 QKD 交互信息是通过经典网络信道传输的，经典网络信道的能力有限，很容易造成网络局部的负载压力过大，因此下一步将研究对经典信息传输的优化。

参 考 文 献

[1] 王剑，王振国. 量子密码协议理论研究[M]. 长沙：国防科技大学出版社，2011：79-100.

[2] ID-Quantique (Geneva，Switzerland) [OL]. http://www.idquantique.com.

[3] 万骏. 浅谈量子通信理论及其应用[J]. 科技传播，2018(6)：1674-6708.

[4] BENNET C H，BRASSARD G. Quantum cryptography：Public key distribution andcointossing[C]// IEEE International Conference on Computers Systems and Signal Processing Bangalore. 1984：175-179.

[5] BECHMANN-PASQUINUCCI H，PERES A. Quantum cryptography with 3-state systems[J]. Physical Review Letters，2000，85(15)：3313-3316.

[6] BRUSS D. Optimal eavesdropping in quantum cryptography with six states[J]. Physical Review Letters，1998，81(14)：3018-3021.

[7] BIHAM E，HUNTTER B，MOR T. Quantum cryptographic network based on quantum memories[J]. Physical Review A，1996，54(4)：2651.

[8] TOWNSEND P. Quantum cryptography on optical fibernetworks in European 98 Parallel Processing[J]. Springer，1998，1470：35-46.

[9] TOWNSEND P. Quantum cryptography on multiuser optical fiber network[J]. Nature，1997，385(6611)：47-49.

[10] LONGDELL，FRAVEL J J，SELLARS E，et al. Stopped light with storage times Greater than one second using electrom agentically induced transparency in a solid[J]. Physical Review Letters，2005，95：63-601.

[11] CHEN Z，BCHE N，ZHAO B. Experimental demonstration of a BDCZ quantum repeater node[J]. Nature，2008，454(28)：1098-1101.

[12] YUAN Z S，CHEN Y A. Fault-tolerent quantum repeater with atomic ensembles and linear optical[J]. Physical Review A，2007，76(2)：22-29.

[13] CLAUSEN C，USMANI I，BUSSIERES F. Quatum storage of photonic entanglement in a crystal[J]. Nature，2011，469：508-511.

[14] TOLIVER P，CHAPURAN T E，RUNSEP R J，et al. Experimental investigation of quantum key distribution through transparent optical switch elements[J]. IEEE Photonics Technology Letters，2003，15(11)：1669-1671.

[15] BEIGE A，ENGLERT B G，KURTSIEFER C，et al. Secure communication with single-photon two-qubit states[J]. Physical Review A，2002，35(28)：407-413.

[16] CAI Q Y. The "Ping-Pong" protocol can be attacked without eavesdropping[J]. Physical Review Letters，2003，91(10)：109801.

[17] CAI Q Y，LI B W. Deterministic secure communication without using entanglement[J]. China Physical Letters，2004，21(4)：601-603.

[18] MAN Z X，ZHANG Z J，LI Y. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations[J]. China Physical Letters，2005，22(1)：18-21.

[19] WANG J，ZHANG Q，TANG C J. Multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state[J]. Optics Communications，2006，266(2)：732-737.