doi:10.3969/j.issn.1003-5060.2015.06.011

一种无证书的顺序聚合签名方案

汤小超, 王 斌, 杨 晴, 李 纯
(扬州大学 信息工程学院,江苏 扬州 225127)

摘 要:已有的聚合签名方案的部分密钥提取过程中存在被敌手伪造的问题。文章基于双线性映射提出了一种新的无证书的顺序聚合签名方案,并将自认证方案与聚合签名方案相结合,从而保证了部分密钥的安全,同时对聚合签名方案过程中的签名算法进行改进以提高性能。结果表明,与聚合签名方案相比,新顺序聚合签名可以改善方案的整体效率。在随机预言模型下证明了该方案可以防止攻击者的伪造。

关键词:无证书签名;聚合签名;顺序聚合签名;双线性映射;随机预言模型
中图分类号:TP309.2 **文献标识码**:A **文章编号**:1003-5060(2015)06-0775-04

A certificateless sequential aggregate signature scheme

TANG Xiao-chao, WANG Bin, YANG Jing, LI Chun
(College of Information Engineering, Yangzhou University, Yangzhou 225127, China)

Abstract: Previous certificateless aggregate signature schemes are subject to adversary's forgery when extracting partial secret key. A new certificateless sequential aggregate signature scheme based on bilinear mapping is presented in this paper. Self-authentication mechanism and aggregate signature are combined to protect the secrecy of partial secret keys. Meanwhile, the algorithm to generate aggregate signatures is improved to enhance efficiency. The result of performance analysis shows that overhead of the proposed sequential aggregate signature scheme is improved in comparison with previous aggregate signature scheme. Finally, the proposed scheme is proven to be secure against forgery under random oracle model.

Key words: certificateless signature; aggregate signature; sequential aggregate signature; bilinear mapping; random oracle model

近年来人们对数字签名的变体进行了多方面的研究[1-2]。聚合签名方案[2]将来自不同的 n 个用户的对 n 个消息的 n 个不同的签名进行聚合,从而生成一个聚合签名。聚合签名可以简化信息验证的过程,从而减少验证签名需要的计算量和数据存储。聚合签名分为无序的聚合签名[2]和顺序的聚合签名[3] 2 种。

由于基于身份的公钥密码系统[4]存在固有的密钥托管问题,文献[5]提出了无证书的公钥密码系统,该系统的私钥由用户和密钥生成中心(key generate center,KGC)共同生成,所以无证书的公钥密码系统解决了密钥托管的问题,以该方案为基础,研究者提出了许多无证书的签名方案。文献[6]提出了基于双线性映射的 2 个无证书聚合签名方案。文献[7]利用双线性映射构造方案,提高了签名以及验证过程中计算效率。文献[8]提出在消息签名阶段不需要双线性映射的计算,而且在验证阶段也只需要 2 步的双线性映射的计算,所以该方案在签名验证时更加高效。

文献[9]的方案是在无证书签名方案的基础上提出的,并给出了正式的安全模型,本文将该方案[9]的部分密钥提取部分与自认证体制[10]相结

收稿日期:2014-06-04;**修回日期**:2014-10-22
基金项目:国家自然科学基金青年基金资助项目(61301111);扬州大学科技创新培育基金资助项目(2013CXJ026)
作者简介:汤小超(1989-),男,江苏泗洪人,扬州大学硕士生;
王 斌(1976-),男,江西萍乡人,博士,扬州大学副教授,硕士生导师.

合,保证了密钥分配中心生成部分密钥在信道传输时的安全性,并对文献[9]方案的签名、聚合签名及聚合验证部分进行了改进,提出了一种无证书的顺序聚合签名方案,并进行了安全性分析。性能分析表明,新提出的顺序聚合签名方案可以改善聚合签名的效率。

1 无证书的顺序聚合签名方案

无证书的顺序聚合签名方案是在文献[9]方案的基础上进行扩展得到的,该方案包含以下算法。

1.1 系统设置

KGC 选取一个安全参数 k。选取一个循环群 G_1,G_1 的生成元为 P,其阶为素数 p。一个循环群 G_2,其阶也为素数 p。双线性映射 $e:G_1\times G_1\rightarrow G_2$。除此之外,KGC 再选取一个随机数 $\lambda\in\mathbf{Z}_p^*$ 作为系统主密钥,计算 $P_T=\lambda\cdot P$。选取 3 个 Hash 函数如下:

$$H_1:\{0,1\}^*\rightarrow G_1,$$
$$H_2:\{0,1\}^*\rightarrow G_1,$$
$$H_3:\{0,1\}^*\rightarrow G_1。$$

所以系统的参数列表为:

$$\text{params}=\langle G_1,G_2,e,P,P_T,H_1,H_2,H_3\rangle。$$

消息空间为:

$$M=\{0,1\}^*。$$

其中,P_T 为系统公钥。

1.2 生成用户密钥

一个用户 U_i,其身份为 $ID_i=\{0,1\}^*$,U_i 随机选取一个数 $x_i\in\mathbf{Z}_p^*$ 作为用户私钥,计算 $X_i=x_i\cdot P$,$Y_i=x_i\cdot P_T$,$P_i=(X_i,Y_i)$作为用户公钥。

1.3 生成部分私钥

用户 U_i 将自己的身份 ID_i 和自己的公钥 P_i 传送给 KGC,接着 KGC 计算出 $D_i=\lambda\cdot Q_i$,其中 $Q_i=H_1(ID_i,P_i)$,并将 D_i 作为部分私钥。KGC 随机选取一个数 $a_i\in\mathbf{Z}_p^*$,计算 $A_i=a_i\cdot P$,$B_i=D_i+a_i\cdot X_i$,最后 KGC 通过公共的通道将(A_i,B_i)发送给相应的用户 U_i。

用户 U_i 收到 KGC 发送的(A_i,B_i)信息后,计算 $D_i=B_i-x_i\cdot A_i$,用户 U_i 就可得到部分私钥 D_i。用户将 D_i 和 x_i 作为签名密钥。

1.4 签名

用户 U_1 的身份为 ID_1,选取消息 $m_1\in M$ 和签名密钥 D_1、x_1,$P_1=(X_1,Y_1)$作为用户公钥。具体签名步骤如下:

(1) 选取一个随机数 $r_1\in\mathbf{Z}_p^*$,并计算 $R_1=r_1\cdot P$。

(2) 计算 $W_1=H_3(m_1\|ID_1\|P_1\|R_1)$。

(3) 计算 $V_1=D_1+x_1\cdot W_1+r_1\cdot x_1\cdot P$。

(4) $\sigma_1=(R_1,V_1)$。用户 U_1 对消息 m_1 的签名即为 σ_1。

1.5 顺序聚合签名

1.5.1 用户 U_2 签名

(1) 用户 U_2 收到用户 U_1 发来的 $\sigma_1=(R_1,V_1)$、m_1、ID_1 时,首先计算 W_1、Q_1,即

$$W_1=H_3(m_1\|ID_1\|P_1\|R_1),$$
$$Q_1=H_1(ID_1,P_1),$$

然后验证 $e(V_1,P)=e(P_T,Q_1)e(W_1,X_1)e(R_1,X_1)$是否成立。如果等式不成立,则停止聚合签名;如果等式成立,则执行以下步骤。

用户 U_2 的身份为 ID_2,选取消息 $m_2\in M$ 和签名密钥 D_2 和 x_2,具体签名步骤如下:

步骤 1 设 $R_1=r_1\cdot P$,选取一个随机数 $r_2\in\mathbf{Z}_p^*$,并计算 R_2,即

$$R_2=R_1+r_2\cdot P=r_1\cdot P+r_2\cdot P=(r_1+r_2)\cdot P。$$

步骤 2 计算 $W_2=H_3(m_2\|ID_2\|P_2\|R_1)$。

步骤 3 $V_1'=V_1+r_2\cdot X_1=D_1+x_1\cdot W_1+(r_1+r_2)\cdot x_1\cdot P$;$V_2'=D_2+x_2\cdot W_2+x_2\cdot R_2$,$V_2=V_1'+V_2'$。

步骤 4 输出聚合签名 $\sigma=(R_1,R_2,V_2)$。用户 U_2 对添加消息 m_2 后的聚合签名即为 σ,并将 σ、$\{m_1,m_2\}$、$\{ID_1,ID_2\}$发送给用户 U_3。

1.5.2 用户 U_i 签名

用户 U_i $(i\geqslant 3)$收到用户 U_{i-1} 发来 $\sigma_{i-1}=(R_1,R_{i-1},V_{i-1})$,$\{m_1,m_2,\cdots,m_{i-1}\}$,$\{ID_1,ID_2,\cdots,ID_{i-1}\}$时,首先计算 W_j、Q_j,即

$$W_j=H_3(m_j\|ID_j\|P_j\|R_1),\ 1\leqslant j\leqslant i-1;$$
$$Q_j=H_1(ID_j,P_j),\ 1\leqslant j\leqslant i-1。$$

然后验证 $e(V_{i-1},P)=e(P_T,\sum_{j=1}^{i-1}Q_j)\prod_{j=1}^{i-1}e(W_j,X_j)e(R_{i-1},\sum_{j=1}^{i-1}X_j)$ 是否成立。如果等式不成立,则说明前面的签名存在错误;如果等式成立,则说明前面的聚合签名都正确,则用户 U_i 对消息 m_i 执行以下步骤:

步骤 1 设 $R_{i-1}=r_{i-1}\cdot P$,选取一个随机数 $r_i\in\mathbf{Z}_p^*$,并计算:

$$R_i=R_{i-1}+r_i\cdot P=r_{i-1}\cdot P+r_i\cdot P=(r_{i-1}+r_i)\cdot P。$$

步骤 2 计算 $W_i=H_3(m_i\|ID_i\|P_i\|R_1)$。

步骤 3　$V_{i-1}'=V_{i-1}+r_i\cdot\sum_{j=1}^{i-1}X_i$,

$V_i'=D_i+x_i\cdot W_i+x_i\cdot R_i$,

$V_i=V_{i-1}'+V_i'$。

步骤 4　输出聚合签名 $\sigma=(R_1,R_i,V_i)$。

2　方案的安全和效率

为了验证安全性分析结果,本文给出了数论假设,即可计算 Diffie-Hellman(CDH)问题为:

$$\forall\ P,aP,bP\in G_1,$$

其中 $a,b\in\mathbf{Z}_p^*$,根据(P,aP,bP,G_1)计算 abP 的结果是不可行的。

2.1　安全性分析

首先在 CDH 安全假设的条件下对单个签名的安全性进行分析。

定理 1　如果攻击者 A 能以概率 ε 对单个签名进行伪造,则可以构造一个求解器以相同的概率解决 CDH 问题。

证明　设攻击者 A 的一次运行能以概率 ε 输出对消息 m_1 的伪造签名 $\sigma=(R_1,V_1)$,满足验证方程为:

$$e(V_1,P)=e(P_T,Q_1)e(W_1,X_1)e(R_1,X_1)\tag{1}$$

设 $W_1=H_3(m_1\|\mathrm{ID}_1\|P_1\|R_1)$,将 $H_3(\cdot)$ 视为 random oracle,即攻击者必须提交 x,才能获取 $y=H_3(x)$的值,而不能自行求值,且 y 的值在 $H_3(\cdot)$的值域上随机分布。

因此一次成功的伪造签名必须把 $m_1\|\mathrm{ID}_1\|P_1\|R_1$ 作为输入查询 $H_3(\cdot)$,否则 $H_3(\cdot)$在 $m_1\|\mathrm{ID}_1\|P_1\|R_1$ 上得到的输出是随机、不可预测的。设 $m_1\|\mathrm{ID}_1\|P_1\|R_1$ 出现在攻击者对 $H_3(\cdot)$的第 i 次查询。

现在回卷攻击者状态,在攻击者的第 2 次运行中保持攻击者对 $H_3(\cdot)$的前 $i-1$ 次查询的回答不变,但重新选取对 $H_3(\cdot)$的第 i 次查询 $m_1\|\mathrm{ID}_1\|P_1\|R_1$及之后查询的回答。

设攻击者第 2 次运行输出的伪造签名为 $\sigma=(R_1,\overline{V_1})$,$m_1$,验证方程为:

$$e(\overline{V_1},P)=e(P_T,Q_1)e(\overline{W_1},X_1)e(R_1,X_1)\tag{2}$$

$\overline{W_1}=H_3(m_1\|\mathrm{ID}_1\|P_1\|R_1)$为在第 2 次运行中对 $m_1\|\mathrm{ID}_1\|P_1\|R_1$ 所选取的回答。

2 个验证方程(1)、(2)相除,可得:

$$e(V_1-\overline{V_1},P)=e(W_1-\overline{W_1},X_1)\tag{3}$$

设有一个算法 B 给定输入为 $P,aP,bP\in G_1$,其中 $a,b\in\mathbf{Z}_p^*$,试图求解 CDH 问题,即计算 abP。

算法 B 模拟攻击者 A 的安全试验环境,并回答 A 发出的 random oracle 查询,B 设置第 1 个用户的公钥为 $X_1=bP$,对 $H_3(\cdot)$采取的模拟方法如下:

攻击者提交 x,B 选取 $w\in\mathbf{Z}_p$,返回 $w\cdot(aP)$作为 $H_3(x)$的值。

第 1 次运行攻击者时,对 $m_1\|\mathrm{ID}_1\|P_1\|R_1$,B 选取 $w_i\in\mathbf{Z}_p$,设置 $W_1=H_3(m_1\|\mathrm{ID}_1\|P_1\|R_1)=w_i\cdot(aP)$。

第 2 次运行攻击者时,B 选取$\overline{w_i}\in\mathbf{Z}_p$,设置$\overline{W_1}=H_3(m_1\|\mathrm{ID}_1\|P_1\|R_1)=\overline{w_i}\cdot(aP)$,将 W_1、$\overline{W_1}$代入方程(3),则有:

$$e(V_1-\overline{V_1},P)=e((w_i-\overline{w_i})\cdot aP,bP)。$$

故 $e((w_i-\overline{w_i})^{-1}\cdot(V_1-\overline{V_1}),P)=e(abP,P)$,则 abP 为$(w_i-\overline{w_i})^{-1}\cdot(V_1-\overline{V_1})$。

由 CDH 假设可知,根据(P,aP,bP,G_1)计算 abP 的结果是不可行的,以上结果与数论假设矛盾,定理得证。

根据顺序聚合的签名过程,每次聚合本质上是将当前签名人生成的独立签名和已有的部分聚合签名进行线性叠加。若一个攻击者 A′可以针对某个用户伪造其参与顺序聚合签名,则在顺序聚合签名的某个位置,必然存在一个对该用户的签名伪造,且能通过验证。由上述关于单个签名的安全分析可知,本文构造的顺序聚合签名方案也是安全的。

2.2　效率分析

本文通过计算量和通信量比较 2 种方案的效率(假设有 n 个用户参与),结果见表 1 所列,对于计算代价较小的运算忽略不计。表 1 中,M 为点乘运算;H 为 Hash 函数运算;E 为双线性运算。从表 1 可看出,文献[9]提出的方案和本文方案的计算量是基本相同的。因为本方案对文献[7]中方案的随机数 $R_i(1\leqslant i\leqslant n)$也进行了聚合,在文献[9]方案中需要传输数据$\{R_1,R_2,\cdots,R_n\}$,而在本方案中只需要传输 R_1、R_n 即可,所以在通信开销方面本方案是优于文献[9]的。

表 1　效率比较

方案	个体签名	聚合验证
文献[9]	$3nM+(n+1)H$	$(n+1)M+(2n+1)H+(3+n)E$
本文	$3nM+nH$	$(n+1)M+2nH+(3+n)E$

(下转第 850 页)

学科的相关知识,研究成果不仅可以解决矿山开采沉陷监测过程中数据采集的瓶颈问题,节约人力资源,还可应用于高层建筑物变形监测,港口、码头、堤防变形监测,山体滑坡变形监测,城市地表沉降和桥梁等的变形监测;同时为研究我国"北斗二代"在矿山沉陷监测领域的应用提供了先期的研究基础。

[参 考 文 献]

[1] 何国清,杨 伦,凌赓娣,等.矿山开采沉陷学[M].徐州:中国矿业大学出版社,1991:53-56.

[2] 能源煤总[1989]25 号,煤矿测量规程[S].

[3] 余学祥,秦永洋,孙兴平,等.相邻工作面综合地表移动观测站的设计与连接测量[J].大连大学学报,2008,29(6):74-79.

[4] 余学祥,秦永洋,孙兴平,等.顾桥煤矿 11-2 煤综采面地表移动变形基本特征分析[J].矿山测量,2009(12):8-12.

[5] 余学祥,邓蓉蓉,张美微,等.基于似单差法的井筒沉降监测试验与结果分析[J].合肥工业大学学报:自然科学版,2012,35(6):804-808.

[6] 张敬霞,刘 超,龙仁波,等.矿区高精度 GPS 地表变形监测体系[J].合肥工业大学学报:自然科学版,2013,36(7):855-860.

[7] 安徽理工大学导航定位技术应用研究所,淮南矿业(集团)有限责任公司.地表移动自动化监测系统研究技术设计[R].淮南:安徽理工大学,2013.

[8] 柯福阳.GNSS 网络综合服务关键算法研究与系统开发[D].南京:东南大学,2010.

[9] 吕伟才,秦永洋,孙兴平.基于 GIS 的矿山开采沉陷综合数据处理软件包的设计[J].矿山测量,2008(4):24-28.

[10] Yu Xuexiang, Lü Weicai. Development of the coal mine exploiting subsidence integrative softwares for data processing and analyzing[C]//Proc of 2011 Conference on Mine Geological Environment Protection, Land Reclamation and Ecological Rehabilitation Technology Exchange Seminar. Scientific Research Publishing, USA, 2011: 105-109.

[11] 吕伟才,秦永洋,孙兴平,等.矿山开采沉陷预计及制图软件的研制[J].矿山测量,2010(5):58-60.

[12] 安徽理工大学导航定位技术应用研究所,淮南矿业(集团)有限责任公司.地表移动自动化监测系统研究中期研究报告[R].淮南:安徽理工大学,2014.

(责任编辑 张淑艳)

(上接第 777 页)

3 结束语

本文提出了一种无证书的顺序聚合签名方案,该方案不同于现有的聚合签名方案,因为现有的签名方案大多是无序的,而该方案的签名是有顺序的。本方案的部分密钥生成过程中引入了自认证签名方案,解决了部分密钥的安全问题,同时相对聚合签名,方案的效率也较高。在随机预言模型下证明了该方案可以防止攻击者的伪造攻击。

[参 考 文 献]

[1] 薛益民,米军利.可撤销匿名性的盲代理群签名方案[J].合肥工业大学学报:自然科学版,2013,36(12):1465-1467.

[2] Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]//Advance in Cryptology-EUROCRYPT 2003, Warsaw, Poland. Berlin: Springer, 2003: 416-432.

[3] Lysyanskaya A, Micali S, Reyzin L, et al. Sequential aggregate signatures from trapdoor permutations[C]//Advances in Cryptology-EUROCRYPT 2004, Interlaken, Switzerland. Berlin: Springer, 2004: 74-90.

[4] Shamir A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology: Proceedings of CRYPTO 84. Berlin: Springer, 1985: 47-53.

[5] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]//Advances in Cryptology-ASIACRYPT 2003, Taipei, Taiwan. Berlin: Springer, 2003: 452-473.

[6] Gong Zheng, Long Yu, Hong Xuan, et al. Two certificateless aggregate signature from bilinear maps[C]//Eighth ACIS International Conference, 2007: 188-193.

[7] 曹素珍,王彩芬,程文华,等.一种高效的无证书聚合签名方案[J].计算机工程,2011,37(18):157-159,166.

[8] Li Fengyin, Liu Peiyu. An efficient certificateless signature scheme from bilinear parings[C]//Network Computing and Information Security (NCIS), 2011: 35-37.

[9] Zhang Lei, Zhang Futai. A new certificateless aggregate signature scheme[J]. Computer Communications, 2009, 32(6): 1079-1085.

[10] Shao Zuhua. Self-certified signature scheme from pairings[J]. The Journal of Systems and Software, 2006, 80(3): 388-395.

(责任编辑 闫杏丽)