可证安全的广播多重盲签名方案*

杨 青 张惠玲 吴成晶
(西安航空学院理学院 西安 710077)

摘 要 对已有多重签名方案进行了安全性分析,提出了可证安全的广播多重盲签名方案。给出了改进的广播多重盲签名算法和验证算法,并证明了改进方案满足盲性和不可伪造性。比较和分析了改进方案的复杂度和安全性,改进方案的运算量减少了 $37.2n+447.8T_{ML}$。改进方案所需运算量少,安全性高且易于实现。

关键词 超椭圆曲线; 约化除子; 盲签名; 双线性对
中图分类号 TP309 **DOI**:10.3969/j.issn.1672-9722.2017.07.026

Provably Secure Broadcast Blind Multisignature Scheme

YANG Qing ZHANG Huiling WU Chengjing
(Faculty of Science, Xi'an Aeronautical University, Xi'an 710077)

Abstract Multisignature algorithm by reference is analyzed. Provably secure broadcast blind multisignature scheme is presented. Specific signature and verification algorithms of Improved broadcast blind multisignature scheme are given. And the Improved scheme meets the propertics of both blindness and non-forgery. The complexity and security of improved scheme are compared and analyzed. Improved scheme reduces computation costs $37.2n+447.8T_{ML}$. Improved scheme has the advantages of low computation complexity, high security and easy to achieve.

Key Words hyperelliptic curve, reduced divisors, blind signature, bilinear pairings
Class Number TP309

1 引言

多个人合作对同一份消息进行签名称为多重数字签名。Harn L 在 1989 年提出了多重签名方案,改进了 RSA 数字签名方案[1]。在 1994 年,Harn L 又提出了基于 Meta-ElGamal 方案的多重签名方案[2]。根据签名过程的不同,多重签名可分为有序多重签名和广播多重签名。有序多重签名是指签名者按照串行的顺序进行签名,广播多重签名对签名顺序没有要求,签名者可以同时进行签名,不必遵循先后次序。2005 年 Harn L 提出了基于 RSA 的有序和广播多重签名方案[3]。近年来,人们在超椭圆曲线上建立密码系统[4],并将双线性对用于多重签名方案[5-7]。

盲签名是指签名人在不知道消息内容的情况下对消息进行签名。它在电子投票和银行电子现金系统方面具有广泛的应用[8]。盲签名应满足以下几条性质:1)不可伪造性,任何第三方都不能伪造盲签名;2)盲性,签名人不知道所签文件或消息的具体内容;3)不可追踪性,签名人无法将有效的签名和被签名的消息联系起来。

本文对文献[7]的多重签名方案进行了改进,提出了高效的基于超椭圆曲线双线性对的广播多重盲签名方案。首先提出改进的广播多重盲签名方案,给出签名算法和验证算法。其次,证明了算法的正确性和安全性。最后,比较和分析了改进方案的安全性和复杂度,并应用于超椭圆曲线密码系统。改进算法克服了原方案不具有盲性的安全隐患,还保留了原方案的优点,并具有快速、高效且易于实现的特点。

* **收稿日期**:2017 年 1 月 10 日,**修回日期**:2017 年 2 月 27 日
基金项目:国家自然科学基金(编号:11302158;11626182);陕西省科技厅项目(编号:2013JM1019;2014K05-43);陕西省教育厅项目(编号:14JK1310);西安航空学院基金项目(编号:2015KY1218;2016GJ1004)资助。
作者简介:杨青,女,硕士,讲师,研究方向:密码学。张惠玲,女,博士,副教授,研究方向:科技评价、信息安全。吴成晶,女,硕士,助教,研究方向:数论和密码学。

2 双线性映射

定义1 设 G_1 为循环加法群，G_2 为循环乘法群，G_1, G_2 的阶均为大素数 q。设双线性映射 $e:G_1\times G_1\to G_2$，它满足以下三个性质：

1）双线性：如果对于任意 $P,Q,R\in G_1$，$a,b\in Z_q^*$，$e(P,Q+R)=e(P,Q)\,e(P,R)$，$e(P+Q,R)=e(P,R)\,e(Q,R)$和$e(aP,bQ)=e(abP,Q)=e(P,abQ)=e(P,Q)^{ab}$。

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

3）可计算性：若 $P,Q\in G_1$，则 $e(P,Q)$ 可在多项式时间内有效计算。

3 改进的广播多重盲签名

该算法由 n 个签名者 $A_1,\cdots,A_n$，消息发送者 I 和签名验证者C组成。n 个广播签名者 $A_1,\cdots,A_n$ 可以同时进行签名，不必遵循先后次序。

3.1 系统参数的设定

设 G_1, G_2 分别是阶为 q（q 为大素数）加法群和乘法群。加法群 G_1 的生成元为 D，双线性映射 $e:G_1\times G_1\to G_2$。H_1 和 H_2 是两个哈希函数：$H_1:\{0,1\}^*\times G_1\to Z_q^*$，$H_2:\{0,1\}^*\to G_1$。系统公开参数 $\Omega=\{G_1,G_2,H_1,H_2,e,q,D\}$。

3.2 签名者密钥的生成

n 个签名者 $A_1,\cdots,A_n$ 的公钥和私钥生成：A_i 随机选取 $x_i\in Z_q^*$，计算公钥 $Y_i=x_iD$，私钥为 x_i，$(i=1,\cdots,n)$，若公钥相同，则重新选取 $x_i\in Z_q^*$。

3.3 签名的生成

对消息 m 产生一个广播多重盲签名，每个签名者 $A_i(1\le i\le n)$ 作如下运算：

1）签名者 A_i 随机选取 $t_i\in Z_q^*$，计算 $T_i=t_iD$，并将 T_i 发送给消息发送者 I。

2）消息发送者 I 随机选取 $\alpha_i,\beta_i\in Z_q^*$，首先计算 $\alpha_i^{-1}\in Z_q^*$，然后计算 $R_i=\alpha_iT_i+\beta_iY_i+\beta_iD$，$R=\sum_{i=1}^{n}R_i$，$h=H_1(m,R)$，$h_i'=\alpha_i^{-1}h-\alpha_i^{-1}\beta_i \bmod q$，$Q=H_2(m/\!/R)$，并将 Q 和 h_i' 分别发送给签名者 A_i，将 Q 和 h 发送给签名验证者 C。

3）签名者 A_i 计算 $\overline{W}_i=(t_i-h_i'x_i)Q$，并发送 $\overline{W}_i$ 给消息发送者 I。

4）消息发送者 I 验证等式：$e(D,\overline{W}_i)=e(T_i-h_i'Y_i,Q)$ 是否成立。若不成立，则消息发送者 I 向签名者 A_i 发出拒绝信息，或要求重新签名。若成立，则 I 计算 $W_i=\alpha_i\overline{W}_i+\beta_iQ$，$W=\sum_{i=1}^{n}W_i$，则 (R,W) 为消息 m 的盲签名，并发送 (R,W) 给签名验证者 C。

3.4 签名的验证

验证者 C 收到 Q,h 和盲签名 (R,W) 后，验证等式 $e(D,W)=e(R-h\sum_{i=1}^{n}Y_i,Q)$ 是否成立。若成立，则宣布盲签名有效，否则无效。

3.5 正确性证明

定理1 若等式 $e(D,W)=e(R-h\sum_{i=1}^{n}Y_i,Q)$ 成立，则消息 m 的盲签名 (R,W) 有效。

证明：

$$\begin{aligned}e(D,W)&=e(D,\sum_{i=1}^{n}W_i)=\prod_{i=1}^{n}e(D,W_i)\\&=\prod_{i=1}^{n}e(D,\alpha_i\overline{W}_i+\beta_iQ)\\&=\prod_{i=1}^{n}e(D,\alpha_i(t_i-h_i'x_i)Q+\beta_iQ)\\&=\prod_{i=1}^{n}e([\alpha_i(t_i-h_i'x_i)+\beta_i]D,Q)\\&=\prod_{i=1}^{n}e(\alpha_iT_i-hY_i+\beta_iY_i+\beta_iD,Q)\\&=\prod_{i=1}^{n}e(R_i-hY_i,Q)\\&=e(\sum_{i=1}^{n}(R_i-hY_i),Q)=e(R-h\sum_{i=1}^{n}Y_i,Q)\end{aligned}$$

4 方案分析

4.1 安全性分析

1）盲性分析。改进方案具有盲性，即签名人不能将消息与签名联系，从而判断出消息和对应的盲签名是否是他所签。改进方案中，给定任意一个有效的广播多重盲签名 (m,R,W)，$R=\sum_{i=1}^{n}R_i$，$W=\sum_{i=1}^{n}W_i$，$W_i=\alpha_i\overline{W}_i+\beta_iQ$，在盲签名过程中产生的任意视图 $(Q,h_i',\overline{W}_i)$，总存在唯一的一对盲因子 $\alpha_i,\beta_i\in Z_n^*$。因为 α_i，β_i 是随机数，任何一个签名者 A_i 都不知道 α_i,β_i，从而无法计算 $\beta_iQ=W_i-\alpha_i\overline{W}_i$。同时，为了防止任何一个签名者 A_i，通过其他步骤计算出 α_i 或 β_i。因为方案中 $h_i'=\alpha_i^{-1}h-\alpha_i^{-1}\beta_i \bmod q$，式中含有两个变量 α_i^{-1}，β_i，所以任何一个签名者 A_i 都无法由此式得出 α_i^{-1}，β_i。总之，任何一个签

名者 A_i 都不能得出 α_i, β_i。改进方案中任何一个签名者 A_i 都不能将所签消息和对应的盲签名联系起来，从而改进方案具有盲签名的盲性。

2）方案具有不可伪造性。若攻击者企图冒充签名者 A_i 的签名 $\overline{W}_i=(t_i-h_i'x_i)Q$，需求解 x_i。这必需求解超椭圆曲线离散对数问题，在计算上是不可行的。若攻击者企图伪造消息 m 的盲签名 (R,W)，由于攻击者无法得到 α_i,β_i（见盲性分析），就不能计算出 $W=\sum_{i=1}^{n}W_i$，$W_i=\alpha_i\overline{W}_i+\beta_iQ$。所以，方案具有不可伪造性。

3）防止签名集体内部人员伪造盲签名。若签名集体内部的某个签名者想伪造 A_i 的签名，那他必须通过消息发送者 I 的验证。假设他可以获得 α_i,β_i，但需要计算 $\overline{W}_i=(t_i-h_i'x_i)Q$，这需要求解 x_i，等同于求解超椭圆曲线离散对数问题，这在计算上是不可行的。所以改进方案能够防止签名集体内部人员伪造盲签名。

4.2 效率分析

本文的方案与文献[9]进行了效率比较，不同密码体制下的运算量转换关系（表1），选取亏格为2的超椭圆曲线，且特征为2。高效的超椭圆曲线除子加法和倍点运算的计算公式，参见文献[10~11]。除子加法运算的运算量为1I+3S+22M，并且除子倍点运算的运算量为1I+5S+22M，其中I，S，M分别表示有限域上的求逆、平方和乘法，并有1I=30M，1S=0.8M。假定签名者人数均为 n，改进方案总的计算量为 $(n+1)T_{BP}+(8n+1)T_{HEM}+(7n-2)T_{HEA}$，由表1中可得，转换后运算量为 $(922.8n+32.2)T_{ML}$。文献[9]方案的总计算量为 $(4n+2)T_{EX}$，即转换后运算量为 $(960n+480)T_{ML}$。因此，本文的运算时间量减少了 $(37.2n+447.8)T_{ML}$，改进方案具有运算量少，效率高等优点。

表1　不同密码体制下的操作运算转换关系

T_{HEM}：超椭圆曲线上执行除子标量乘运算的运算量，$1T_{HEX}=56T_{ML}$
T_{EX}：执行模幂运算的运算量，$1T_{EX}=240T_{ML}$
T_{BP}：执行双线性对运算的运算量，$1T_{BP}=87T_{ML}$
T_{ML}：执行模乘运算的运算量
T_{HEA}：超椭圆曲线上执行除子加法运算的运算量，$1T_{HEA}=55.4T_{ML}$

5 结语

本文提出了基于超椭圆曲线双线性对的广播多重盲签名方案，广泛应用于匿名电子投票系统，电子现金交易、网络职称评审及电子银行系统等。比较和分析了改进方案的安全性和效率，与文献[9]的计算效率相比较，改进方案的运算量减少了 $(37.2n+447.8)T_{ML}$。改进方案具有运算量低，高安全性能以及易于实现等优点。

参考文献

[1] Harn L, Kiesler T. New schem for digital multisignatures [J]. Electronics letters, 1989, 25(15): 1002-1003.

[2] Harn L. New digital signature scheme based on discrete logarithm[J]. Electronics letters, 1994, 30(5): 396-398.

[3] Harn L, Lin CY, Wu C T. Structured multisignature algorithms [J]. IEE computers and digital techniques, 2004, 151(3): 231-234.

[4] Yang Siman, Wu Hongfeng, LI Jiyou. Access structures of hyperelliptic secret sharing schemes[J]. Finite Fields and Their Applications, 2016, 37(1): 46-53.

[5] Islam S.H., Biswas G.P. A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings[J]. Journal of King Saud University--Computer and Information Sciences, 2014, 26(1): 55-67.

[6] Islam S.H., Biswas G.P. Provably secure certificateless strong designated verifier signature scheme based on elliptic curve bilinearpairings[J]. Journal of King Saud University--Computer and Information Sciences, 2013, 25(1): 51-61.

[7] Islam S.H., Biswas G.P. Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings [J]. Journal of King Saud University--Computer and Information Sciences, 2014, 26(1): 89-97.

[8] Li Fagen, Zhang Mingwu, Takagi Tsuyoshi. Identity-based partially blind signature in the standard model for electronic cash [J]. Mathematical and computer modeling, 2013, 58(1): 196-203.

[9] Debasis Giri, Srivastava P. D.. An improved efficient multisignature scheme in group communication systems [C]// Proceedings of the 2007 International Conference on Advanced Computing and Communications (ICACC '07), 2007: 447-435.

[10] 李明，孔凡玉，朱大铭. 超椭圆曲线上Montgomery标量乘的快速计算公式[J]. 软件学报，2013，24(10)：2275-2288.
LI Ming, KONG Fanyu, ZHU Daming. Fast addition formulae for Montgomery Ladder scalar multiplication on hyperelliptic curves [J]. Journal of Software, 2013, 24(10): 2275-2288.

[11] Lange T. Formulae for arithmetic on genus 2 hyperelliptic curves [J]. Applicable algebra in engineering, communication and computing, 2005, 15(5): 295-328.