

基于双线性对的多重数字签名方案

张彩娟¹, 游林^{1,2}

(1. 杭州电子科技大学理学院, 浙江 杭州 310018;

2. 杭州电子科技大学通信学院, 浙江 杭州 310018)

摘要: 基于双线性对及3个困难性问题(IFP、DLP、CDHP)提出了新的多重数字签名方案。新方案将广播多重数字签名中签名快速的优点应用到按序多重数字签名, 改变签名的一般机制, 使签名者同时进行签名; 然后, 由可信第三方验证签名, 验证通过后发送给验证者; 最后, 由验证者将签名转变为按序的。同时, 分析了方案在3个困难问题、防伪攻击和抗部分成员合谋攻击方面的安全性能。新方案具有计算量少、算法简单、获取签名速度快、安全性强等优点。

关键词: 多重数字签名; 按序签名; 广播签名; 安全性

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00061

Digital multi-signature scheme based on bilinear pairing

ZHANG Cai-juan¹, YOU Lin^{1,2}

(1. College of Science, Hangzhou Dianzi University, Hangzhou 310018, China;

2. College of Communication, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: Based on bilinear pairing and three complicated problems, a new digital multi-signature scheme was proposed. In the new scheme, the advantage of fast signature in broadcasting digital multi-signature was applied to sequential digital multi-signature. By changing the general mechanism of signature, signing could be done simultaneously by the signers. Then, the signature was sent to verifier after it was verified by trusted third party. The transformation from concurrent signature to sequential signature was finally realized by the verifier. The security capabilities in three complicated problems, anti-fake attack and anti-conspiracy attack from some members of the new scheme were analyzed. Proposed scheme has many advantages over the old ones, such as fewer calculation, simpler algorithm, faster signing, higher security.

Key words: digital multi-signature, sequential signature, broadcasting signature, security

1 引言

随着互联网的高速发展, 人们希望通过电子设备就能实现远距离的、快速的交易。自1976年Diffie和Hellman^[1]首次提出公钥密码体制的概念后, 数字签名随之产生, 并开始商业通信系

统中得到广泛应用。实际情况中, 有时需要多个用户对同一消息进行签名, 这类需要多个实体对同一份合同进行签名的电子对应物就是多重数字签名。

自引入多重数字签名^[2]的概念后, 不同的多重数字签名方案相继被提出。文献[3~5]提出基于

收稿日期: 2016-05-13; 修回日期: 2016-06-04。通信作者: 张彩娟, 908332087@qq.com

基金项目: 浙江省重点科技创新团队基金资助项目(No.2013TD03)

Foundation Item: Zhejiang Province Science and Technology Innovation Program (No.2013TD03)

离散对数困难性问题的多重数字签名; 文献[5]在离散对数困难性的基础上把整数分解问题也应用到签名里, 使签名方案更安全、可靠; 文献[6~8]给出关于散列函数的发展和其在多重签名中的应用; 文献[9]把盲签名以及代理签名运用到多重签名中形成新的方案; 文献[10,11]中对椭圆曲线密码体制的运用和改进, 使多重签名方案更加多样化; 文献[12]中提出的针对基于离散对数多重签名方案的攻击和文献[13]提出的基于椭圆密码体制的签名方案的攻击, 使多重签名方案更加完善、安全。以上文献各有优缺点, 但其设计思想值得借鉴。

根据多重签名顺序和过程的不同, 可分为按序多重签名和广播多重签名。文献[6,14]给出基于同样问题的按序和广播 2 种多重签名方案, 通过比较可以发现, 按序多重签名方案耗时更久些, 对重大性和紧急性事件有较大影响。例如, 在按序多重数字签名体系中, 当消息发送给签名者时, 若签名者未及时签名, 则后面的签名者也无法对消息进行签名。依此下去, 每个签名者都耽误一点时间, 则最后验证者收到签名的时间就会延长很久。针对按序多重签名方案这一缺点, 本文将按序和广播 2 种多重签名在某种程度上结合起来, 同时又结合离散对数困难性问题、整数分解问题以及 Diffie-Hellman 计算问题来构造新方案。与文献[5]的按序多重数字签名方案相比, 本方案获取签名速度更快、运算量更少、安全性更高。

2 基础知识

2.1 对称双线性对

设 G_1 是椭圆曲线 $E(F_q)$ 上的一个加法循环群, G_2 是有限域 F_{q^2} 上的乘法循环群, 两者的阶均为 q , 令 g 为 G_1 的生成元。假设 G_1 和 G_2 中的离散对数问题都是难解的, 对称双线性对是一个映射 $e: G_1 \times G_1 \rightarrow G_2$, 它具有如下属性。

- 1) 双线性性。对任意的 $P, Q \in G_1, a, b \in Z_q^*$, 都有 $e(aP, bQ) = e(P, Q)^{ab}$ 成立。
- 2) 非退化性。对任意的 $P, Q \in G_1$, 满足 $e(P, Q) \neq 1$ 。
- 3) 可计算性。存在有效算法, 对任意的 $P, Q \in G_1$, $e(P, Q)$ 都能够有效地计算。

2.2 困难问题假设

定义 1 大整数分解问题 (IFP)。已知 2 个大素数 p, q , 求 $n = pq$ 是容易的, 但若由 n 来求 p 和 q 是困难的, 这就是大整数分解困难问题。

定义 2 离散对数问题 (DLP)。设 G_1 为一个循环群, 对于 $P, Q \in G_1$, 找到一个整数 $a \in Z_q^*$, 使 $Q = aP$ 成立。

定义 3 Diffie-Hellman 计算问题 (CDHP)。对于任意的 $a, b \in Z_q^*$, 给出 $P, aP, bP \in G_1$, 计算出 abP 且满足 $abP \in G_1$ 。

2.3 基于 SDLP 和 IFP 的多重数字签名方案

文献[5]提出基于 SDLP 和 IFP 的按序多重数字签名方案。简述如下。

1) 系统的建立。给出签名的顺序 $G = \{D_1, D_2, \dots, D_l\}$ 。首先, 假设一个安全的散列函数 H' 对原始消息 M' 进行加密得到 $H'(M') = m'$; 其次, 可信任第三方 T 随机选择 2 个大素数 p', q' , 并计算 $n' = p'q'$; 再次, 选取素数 r , 满足 $r|(p'-1)$, $r|(q'-1)$; 然后, 选择元素 $\alpha \in Z_{n'}^*$, 其中, α 对模 n' 的指数为 r ; 最后, 选择 $s \in Z_r^*$, 计算 $\beta = \alpha^s \pmod{n'}$, 并公开系统参数 $(\alpha, \beta, r, n', m')$ 。

2) 签名算法。

Step1 T 随机选取 4 个整数 $a_0, b_0, c_0, d_0 \in Z_r^*$, 其中, 记 $h \equiv (a_0 + sb_0) \pmod{r}$, $k \equiv (c_0 + sd_0) \pmod{r}$, 通过计算 $P = \alpha^{a_0+sb_0} = \alpha^h \pmod{n'}$, $Q = \alpha^{c_0+sd_0} = \alpha^k \pmod{n'}$, 获得公钥 (P, Q) 。

Step2 签名者 D_i 随机选取 2 个整数 $h_i, k_i \in Z_r^*$, 计算 $\alpha^{h_i}, \alpha^{k_i}$ 并通过安全信道将其发送给 T 。 T 接收之后利用已知参数计算 $E_i = \alpha^{h_i}(\alpha^{h_i})^{-s} \pmod{n'}$, $F_i = \alpha^{k_i}(\alpha^{k_i})^{-s} \pmod{n'}$, 随后将 E_i, F_i 秘密地发送给 D_i 。这样, 签名者 D_i 就能利用私钥验证 T 发送给它的 E_i, F_i 是否正确。

Step3 ① 签名者 D_1 利用私钥 (h_1, k_1, E_1, F_1) 以及 m' 计算得到签名 $K_1 = E_1 F_1^{m'} \pmod{n'}$ 和 $g_1 = h_1 + m'k_1 \pmod{r}$, 并把签名 (K_1, g_1) 传给下一个签名者 D_2 。② D_2 接收后验证等式 $K_1 \beta^{g_1} = PQ^{m'} \pmod{n'}$ 是否成立。若成立则计算其签名 $K_2 = K_1 E_2 F_2^{m'} \pmod{n'}$ 和 $g_2 = g_1 + h_2 + m'k_2 \pmod{r}$, 并发送 (K_2, g_2) 给 D_3 。③ 依此进行下去, 直到 D_l 验证 $K_{l-1} \beta^{g_{l-1}} = (PQ^{m'})^{l-1} \pmod{n'}$ 成立, 形成最终签

名 $K_i = K_{i-1} E_i F_i^{m'} \pmod{n'}$ 及 $g_i = g_{i-1} + h_i + m' k_i \pmod{r}$ ，并将签名 (K_i, g_i) 发送给验证者。

3) 签名的验证

验证者接收到 (K_i, g_i) 后，利用公钥进行检验，若 $K_i \beta^{g_i} = (PQ^{m'})^i \pmod{n'}$ 成立，则最终签名 (K_i, g_i) 。

3 新的多重数字签名方案

3.1 系统的建立

首先，可信任第三方 C 选择大素数 q ，并取阶为 q 的循环群 G_1 、 G_2 ，其中， G_1 是加法群， G_2 是乘法群，且 g 为 G_1 的生成元，则有双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 。其次，选取散列函数 $H: \{0,1\}^* \rightarrow Z_q$ ，并对原始消息 M 进行加密得到 $H(M)=m$ 。再次，给出规定的签名顺序 $\Gamma = (U_1, U_2, \dots, U_K)$ 。最后，将签名顺序 Γ 发送给签名验证者并公布系统参数 $(G_1, G_2, q, H, M, e, g)$ 。

3.2 签名算法

Step1 可信任第三方 C 通过随机选取 $t, a, b \in Z_q$ 来产生其私钥 (t, a, b) ，并计算 $e(tg, g) = e^t(g, g)$ ， $e(tg, ag) = e^{at}(g, g)$ ， $e(tg, bg) = e^{bt}(g, g)$ ，令 $T = e^t(g, g)$ ， $A = e^{at}(g, g)$ ， $B = e^{bt}(g, g)$ ，得到公钥 (T, A, B) 。

Step2 ① 签名者 U_i 随机选取大素数 p_i ，令 $n_i = p_i q$ ，同时选择满足条件 $(b_i, p_i, q) = 1$ 的 b_i 。② 计算 n_i 以及满足条件 $b_i c_i \equiv 1 \pmod{n_i}$ 的 c_i ，得到系统公钥 c_i 。③ 记 $A_i = A e^{b_i}(tg, g)$ ， $B_i = B e^{b_i}(tg, g)$ ，通过计算得到签名者 U_i 的私钥 (n_i, b_i, A_i, B_i) 。④ U_i 利用私钥计算 $e(b_i g, g) = e^{b_i}(g, g)$ 和签名 $S_i = A_i B_i^{m'}$ ，并通过安全信道将 $(e^{b_i}(g, g), S_i)$ 秘密地发送给可信任第三方 C 。

Step3 可信任第三方 C 利用它的私钥 t 及 $(A, B, m, e^{b_i}(g, g))$ 来验证

$$S_i = A_i B_i^m = AB^m e^{b_i(1+m)t}(g, g)$$

是否成立。若成立， C 将 (S_i, m, c_i, T) 作为签名发送给验证者；否则，发送空消息。

3.3 签名的验证

当验证者接收到所有签名 (S_i, m, c_i, T) 后，需根据签名顺序 Γ 进行逐一验证。若 $S_j^{c_j} T^{-(1+m)} = A^{c_j} B^{c_j m}$ ($j=1, 2, \dots, i-1$) 成立，而 $S_i^{c_i} T^{-(1+m)} = A^{c_i} B^{c_i m}$

不成立，则判定签名者 $(U_i, U_{i+1}, \dots, U_K)$ 的签名均是无效的。反之，若 $S_j^{c_j} T^{-(1+m)} = A^{c_j} B^{c_j m}$

($j=1, 2, \dots, K$) 都成立，则计算 $S = \prod_{i=1}^K S_i^{c_i}$ ， $C' = \sum_{i=1}^K c_i$ ，并将 (S, m, C', T) 作为最终的签名。因为

$$\begin{aligned} S &= \prod_{i=1}^K S_i^{c_i} \\ &= \prod_{i=1}^K (AB^m e^{b_i(1+m)t}(g, g))^{c_i} \\ &= \prod_{i=1}^K (AB^m)^{c_i} T^{(1+m)} \\ &= (AB^m)^{C'} T^{K(1+m)} \end{aligned}$$

这样形成的最终签名长度是固定的，与签名者的个数无关。

上述按序签名方案是在文献[5]的基础上进行改进的，与文献[5]相比，本文引入了双线性对并选取了不同的 n_i ，使方案的安全性更高；同时，又改变了按序签名的体制，使签名经过了可信任第三方和验证者双重的验证，更加真实可靠；且新方案中可信任第三方产生的私钥量较小，节省了密钥存储空间；此外，新方案在整个签名生成的过程中运算量较小、获取签名速度快，签名的长度也是固定的，不随签名者的变化而改变。

4 效率及安全性分析

4.1 效率分析

本文提出的新方案与文献[5]在运算量和签名时间上的比较如表1所示。

记号说明： T_m 表示乘法运算， T_e 表示幂运算， T_a 表示加法运算， Δt_i 表示消息从发送给 U_i 开始到签名结束所消耗的时间， ΔT 表示从消息发出后到所有签名结束需要的总时间。

由表1可知，本文方案在签名所需总时间和签名生成过程中所需运算量上都占有极大优势。显然，新方案获取签名的速度更快、运算量更少、效率更高。

4.2 安全性分析

4.2.1 困难问题

IFP: 由于 (G_1, G_2, e, g, c_i, q) 是公开参数，任何人都能求出 $e(g, g)$ ，但是不能求得 $e^h(g, g)$ 。因为大素数 p_i 是未知的，从而 n_i 也是未知的，所以没有

表 1 2 个方案运算效率对比

方案	签名所需总时间 ΔT	生成签名	签名验证	总运算量
文献[5]方案	$\sum_{i=1}^K \Delta t_i$	$(4n-1)T_m + (3n-2)T_c + (2n-1)T_a$	$T_m + 2T_c$	$4nT_m + 3nT_c + (2n-1)T_a$
本文方案	$\max(\Delta t_1, \Delta t_2, \dots, \Delta t_K)$	$nT_m + nT_c$	$2nT_m + (2n+2)T_c + (n-1)T_a$	$3nT_m + (3n+2)T_c + (n-1)T_a$

人可以通过 c_i 和 q 来求得 b_i ，从而得到 $e^{b_i}(g, g)$ 。求解 b_i 的难度等价于大整数的分解问题。

DLP: 因为 $e(g, g)$ 是可以由公共参数求得的，同时 $e'(g, g) = T$ 是公开的，所以，任何人想要通过 $e(g, g)$ 和 $e'(g, g)$ 来找到 $t' \in Z_q$ ，使 $e^{t'}(g, g) = e'(g, g)$ 成立是不可能的，因为寻找 $t' \in Z_q$ 的过程实际就是解决离散对数问题的过程。

CDHP: 假设攻击者可以通过某种方式截获签名者 U_i 发送给可信任第三方 C 的秘密消息 $e^{b_i}(g, g)$ 。由于 $e(g, g)$ 和 $e'(g, g)$ 是易得或易知的，所以，攻击者根据获得的信息 $e^{b_i}(g, g)$ 来求 $e^{b_{i'}}(g, g)$ 是困难的，求解 $e^{b_{i'}}(g, g)$ 的难度相当于解决 Diffie-Hellman 计算问题。

4.2.2 防伪攻击

假设一个攻击者想要伪装成签名者 U_i 对原始消息 M 进行签名，根据本文所提签名算法可知攻击者可以随机选取大素数 p_i' 和 b_i' ，其中， b_i' 要满足条件 $(b_i', p_i'q) = 1$ 。随后通过计算 $n_i' = p_i'q$ ， $e(b_i'g, g) = e^{b_i'}(g, g)$ 以及满足等式 $b_i'c_i' \equiv 1 \pmod{n_i'}$ 的 c_i' 来伪造 n_i ， $e^{b_i}(g, g)$ 和 c_i ，并将 c_i' 公开。最后，攻击者通过计算 $S_i' = Ae^{b_i'}(tg, g)(Be^{b_i'}(tg, g))^m$ 来伪造签名 (S_i', m, c_i', T) 。显然该签名可以通过验证者的验证，因为 $S_i'^{c_i'} T^{-(1+m)} = A^{c_i'} B^{c_i'm}$ 成立。但是攻击者不知道签名者 U_i 与可信任第三方 C 之间的秘密信道，因此，无法将伪造的 $(e^{b_i'}(g, g), S_i')$ 发送给 C ，也无法通过 C 的验证，从而无法通过 C 将伪造的签名发送给验证者。即该方案有效地防止了攻击者的伪造攻击。

4.2.3 抗部分成员合谋攻击

本文方案在一定程度上将按序多重签名与广播多重签名结合起来，先由每个签名者 U_i 独立地进行签名 (S_i, m, c_i, T) ，然后，将 (S_i, m, c_i, T) 交给可信任第三方 C 进行验证，验证通过后由 C 将签名直接发送给验证者。验证者接收到所有签名

$(S_i, m, c_i, T), i = 1 \dots K$ 后，按照预定的顺序对签名进行逐一验证，验证成功后再统一形成总的签名 (S, m, C', T) 。正是由于该算法中签名者 U_i 进行签名时是各自独立的，且每个签名 (S_i, m, c_i, T) 要经过 C 的验证才能发送给验证者，所以，整个方案中没有通过签名者相互合作而形成的公私钥，即部分成员之间是无法通过合谋来伪造任何东西的。

从上面安全性的分析可以看出，双线性对的引入、不同 n_i 的选取以及新结构的构造使新方案更安全，防攻击能力更强。

5 结束语

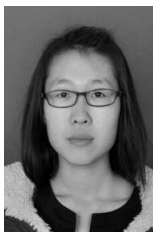
针对按序多重数字签名方案获取签名速度慢的特点，本文改变了传统按序签名的体制，将按序和广播签名在一定程度上结合起来，形成新的按序多重签名体制。新方案具有运算量少、算法简单、获取签名速度快、安全性强等优点，同时，方案中新的构造方法为签名节省了大量时间，极具推广性，是具有发展潜力的多重数字签名方案。

参考文献:

- [1] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
- [2] ITAKURA K. A public-key cryptosystem suitable for digital multi-signatures[J]. Nec Research & Development, 1983, 71(1): 474-480.
- [3] LU L R, ZENG J J, KUANG Y H, et al. A new multi-signature scheme based on discrete logarithm problem and its distributed computation[J]. Chinese Journal of Computers, 2002, 25(12): 1417-1420.
- [4] BURMESTER M, DESMEDT Y, DOI H, et al. A structured elgamal-type multi-signature scheme[C]//The 3rd International Workshop on Practice and Theory in Public Key Cryptography. c2000: 466-483.
- [5] DÍAZ R D, ENCINAS L H, MASQUÉ J M. A multi-signature scheme based on the SDLP and on the IFP[C]// International Conference on Computational Intelligence in Security for Information Systems. c2011:135-142.

- [6] ZHANG J H, WEI Y Z, WANG Y M. Digital multi-signatures scheme based on RSA[J]. Journal of China Institute of Communications, 2003, 24(8): 150-154.
- [7] U.S. Department of Commerce. Secure Hash standard-SHS: federal information processing standards publication 180-4[M]. Create Space Independent Publishing Platform, 2012.
- [8] NOROOZI E, DAND S M, SABOUHI A, et al. A new dynamic hash algorithm in digital signature[J]. Advanced Machine Learning Technologies and Applications, 2012, 322(12): 583-589.
- [9] GUO W, ZHANG J Z, LI Y P, et al. Multi-proxy strong blind quantum signature scheme[J]. International Journal of Theoretical Physics, 2016, 55(3): 1-13.
- [10] LI F, XUE Q. Two improved proxy multi-signature schemes based on the elliptic curve cryptosystem[M]//Computing and Intelligent Systems. Berlin Heidelberg: Springer, 2011: 101-109.
- [11] CHOUKSEY R, SIVASHANKARI R, SINGHAI P. ECDLP based proxy multi-signature scheme[M]//Advances in Computing and Information Technology. Berlin Heidelberg: Springer, 2012: 71-79.
- [12] HAN X X, WANG G P, BAO F, et al. An attack to multi-signature schemes based on discrete logarithm[J]. Chinese Journal of Computers, 2004, 27(8): 1147-1152.
- [13] LIU Y, LUO P, DAI Y Q. Attack on digital multi-signature scheme based on elliptic curve cryptosystem[J]. Journal of Computer Science & Technology, 2007, 22(1): 92-94.
- [14] WANG X F, ZHANG J, WANG S P. Digital multi-signature scheme and its security proof[J]. Chinese Journal of Computer, 2008, 31(1): 176-183.

作者简介:



张彩娟(1993-), 女, 山西大同人, 杭州电子科技大学硕士生, 主要研究方向为信息安全与密码学。



游林(1966-), 男, 江西临川人, 杭州电子科技大学教授, 主要研究方向为信息安全与密码学。