文章编号:1001 - 9081(2010)05 - 1227 - 03

两个指定验证者签名方案的分析与改进

张永洁[1,2], 王彩芬[2], 张玉磊[2]
(1. 甘肃省卫生学校,兰州 730000; 2. 西北师范大学 数学与信息科学学院,兰州 730070)
(zyjie78@163.com)

摘 要:分析了两个基于身份的指定验证者签名方案(Zhang 方案和 Li-Zheng-Zhu 方案),指出了两个签名方案不满足指定验证者签名的安全特性:Zhang 方案不满足不可伪造性,Li-Zheng-Zhu 方案中非指定验证者可以验证签名的有效性,不满足指定验证性。对两个方案进行了改进,改进后的 Zhang 方案满足不可伪造性,并具有与原方案相同的效率;改进后的 Li-Zheng-Zhu 方案不仅满足指定验证性,而且减少了一个双线性对运算,具有较高的效率。

关键词:基于身份签名;指定验证者签名;短签名;双线性对
中图分类号: TP309 **文献标志码**:A

Aanalysis and improvement of two designated verifier signature schemes

ZHANG Yong-jie[1,2], WANG Cai-fen[2], ZHANG Yu-lei[2]
(1. *Gansu Province Health School, Lanzhou Gansu* 730000, *China*;
2. *College of Mathematics and Information Science, Northwest Normal University, Lanzhou Gansu* 730070, *China*)

Abstract: Two identity-based designated verifier signature schemes, which were proposed by Zhang and Li-Zheng-Zhu respectively, were analyzed. It was shown that two schemes did not satisfy the security requirements of designated verifier signature. Zhang's scheme did not meet the unforgeability requirement; Li-Zheng-Zhu's scheme did not have designated verification as although the non-designated-verifier could check the validity of the signatures. Then the schemes were improved. The improved Zhang's scheme owns unforgeability property, and has the same efficiency as the Zhang's. The improved Li-Zheng-Zhu's scheme owns designated verification property; moreover, the improved scheme has reduced one bilinear paring and is more efficient than the Li-Zheng-Zhu's.

Key words: identity-based signature; designated verifier signature; short signature; bilinear pairing

0 引言

在传统数字签名中,任何用户都可以验证签名的有效性,但是,签名者有时仅希望只有指定的用户才可以验证签名。1996 年,文献[1]首次提出了指定验证者签名(Designated Verifier Signature, DVS),签名者指定一个验证者,除了被指定的验证者外其他任何人都不能验证签名,原因在于:被指定的验证者用自己的私钥可以产生一个与原始签名无法区分的签名。DVS 在电子商务、电子政务中有很多重要用途,它可以有效地解决认证和隐私性的冲突。文献[1]同时介绍了强指定验证者签名(Strong Designated Verification Signature, SDVS)的概念,强指定验证者签名是一种特殊的指定验证者签名。在 SDVS 中,由于验证签名时必须使用被指定验证者的私钥,所以只有被指定的验证者才有能力验证签名。文献[2-4]对基于身份的指定验证者签名和强指定验证者签名进行了一定的研究。

最近,文献[5]提出了一个基于身份的指定验证者签名方案(Zhang 方案),声称满足不可伪造性。文献[6]提出了一个基于身份的强指定验证者签名方案(Li-Zheng-Zhu 方案),声称没有第三方可以验证签名的有效性。本文指出,Zhang 方案不满足不可伪造性,敌手可以伪造签名;Li-Zheng-Zhu 方案不满足强指定验证性,不具有验证权限的用户可以验证签名的有效性。本文对两个方案进行了改进,增强了安全性。在 Zhang 方案的基础上,增加了一个哈希函数,提高了方案的安全性,效率与原方案相当。基于短签名[7]设计思路,对 Li-Zheng-Zhu 方案进行了改进,也增加一个哈希函数,但是在验证算法中减少了一个双线性对运算,效率高于原方案。

1 基础知识

1.1 双线性对

设 q 是大素数, G_1 是加法循环群, G_2 乘法循环群,阶均为 q。$P \in G_1$ 为生成元。假设在群 G_1、G_2 中离散对数问题难解,双线性映射 $e: G_1 \times G_1 \to G_2$ 满足下列性质:

双线性性 设 $a,b \in Z_q^*$, $P,Q \in G_1$, $e(aP,bQ) = e(P,Q)^{ab}$。

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

可计算性 对所有的 $P,Q \in G_1$,存在有效算法可以计算 $e(P,Q)$。

1.2 相关困难问题

定义 1 CDH 问题(Computational Diffie-Hellman Problem)。在群 G_1 上,已知 $\langle P, aP, bP\rangle$,输出 abP,其中, $a,b \in Z_q^*$。

收稿日期:2009 - 11 - 19;**修回日期**:2010 - 01 - 21。
基金项目:教育部科学技术研究重点项目(208148);甘肃省教育厅重点项目(0801-01)。
作者简介:张永洁(1978 -),女,甘肃武都人,讲师,硕士,主要研究方向:信息安全; 王彩芬(1963 -),女,河北安国人,教授,博士生导师,博士,主要研究方向:信息安全、电子商务; 张玉磊(1979 -),男,甘肃白银人,讲师,硕士,主要研究方向:信息安全。

定义 2 BDH 问题(Bilinear Diffie-Hellman Problem)。在群 G_1 上,已知$\langle P,aP,bP,cP\rangle$,输出 $e(p,p)^{abc}$,其中,$a,b,c \in Z_q^*$。

1.3 基于身份的指定验证者签名方案(IBDVS)

IBDVS 方案一般包括 5 个算法:系统设置、密钥提取、指定验证者签名、指定验证者签名验证和副本模拟。其中,副本模拟算法主要体现 DVS 的"不可传递性",即除签名者之外,指定验证者也可以产生有效的 DVS。IBDVS 方案的安全特性一般包括:正确性、不可传递性和不可伪造性。基于身份的强指定验证者签名方案(IBSDVS)与 IBDVS 相似,也包括如上所述 5 个算法,其安全性包括以上所述安全特性和强指定性。

2 Zhang 方案的密码学分析

2.1 Zhang 方案简述[5]

Zhang 方案是一个基于身份的指定验证者签名方案,具体算法如下所示。

1)系统设置:PKG 选择阶为素数 q 的循环群 G_1,G_2,选择双线性映射 $e:G_1 \times G_1 \to G_2$,生成元 $P \in G_1$,哈希函数为 $H_1:\{0,1\}^* \to G_1$,$H_2:\{0,1\}^* \times G_1 \to Z_q^*$。PKG 随机选择 $s \in Z_q^*$,计算 $P_{pub} = sP$。主密钥为 s,系统参数为 $Params = \{G_1,G_2,e,q,P,P_{pub},H_1,H_2\}$。

2)密钥提取:给定身份 ID,PKG 计算 $S_{ID} = sH_1(ID)$,将它发送给用户,用户公钥为 $Q_{ID} = H_1(ID)$。

3)指定验证者签名:已知签名者 A 的私钥 S_{IDA}、指定验证者 B 的公钥 Q_{IDB} 和消息 M。A 选择 $r \in Z_q^*$,计算 $U = rQ_{IDB}$,$h = H_2(M,U)$,$V = r^{-1}hS_{IDA}$,则 A 对消息 M 的指定验证者签名为 $\sigma = (U,V)$。

4)指定验证者验证:已知指定验证者 B 的私钥 S_{IDB}、签名者 A 的公钥 Q_{IDA}、消息 M 和签名 $\sigma = (U,V)$。B 首先计算 $h = H_2(M,U)$,然后验证等式 $e(U,V) = e(S_{IDB},hQ_{IDA})$ 是否成立,如果成立,则签名 σ 有效。

5)副本模拟:B 选择 $r' \in Z_q^*$,计算 $U' = r'Q_{IDB}$,$h' = H_2(M,U')$,$V' = r'^{-1}h'S_{IDB}$。显然,对于消息 M 的模拟签名 $\sigma' = (U',V')$ 满足以上验证等式,指定验证者可以产生与签名 σ 不可区分的签名 $\sigma' = (U',V')$。

2.2 Zhang 方案的密码学分析

文献[5]声称方案是安全的、不可伪造的。分析 Zhang 方案,发现该方案是可以伪造的,是不安全的。

假设 $\sigma = (U,V)$ 是签名者 A 指定验证者 B 关于消息 M 的签名,凡是得到签名 $\sigma = (U,V)$ 的任何用户都可以伪造签名。

1)攻击者获得签名:攻击者获得 $\sigma = (U,V)$,其中,$U = rQ_{IDB}$,$V = r^{-1}hS_{IDA}$。计算 $h = H_2(M,U)$,由于 $H_2:\{0,1\}^* \times G_1 \to Z_q^*$,容易计算 h^{-1}。

2)攻击者伪造签名:攻击者计算 $U' = h^{-1}U$,$h' = H_2(M,U')$,$V = h'V$,得到关于消息 M 的伪造签名 $\sigma' = (U',V')$ 并发送给指定验证者 B。

3)指定验证者验证:B 收到签名 $\sigma' = (U',V')$,按照验证算法,首先计算 $h' = H_2(M,U')$,然后验证等式 $e(U',V') = e(S_{IDB},h'Q_{IDA})$。

由于 $e(U',V') = e(h^{-1}U,h'V) = e(h^{-1}rQ_{IDB},h'r^{-1}hS_{IDA}) = e(sQ_{IDB},h'Q_{IDA}) = e(S_{IDB},h'Q_{IDA})$,验证等式成立。攻击者可以通过签名 $\sigma = (U,V)$ 伪造新的签名 $\sigma' = (U',V')$,并且 $\sigma' = (U',V')$ 可以通过指定验证者的验证算法。因此,Zhang 方案中的签名是可以伪造的,该方案是不安全的。

2.3 Zhang 方案的改进

为了提高 Zhang 方案的安全性,在原方案的基础上增加一个哈希函数 $H_3:\{0,1\}^* \to G_1$。用户 A 签名时,将 $e(U,V)$ 作为 H_3 的输入。指定验证者 B 验证签名时,将 $e(S_{IDB},hQ_{IDA})$ 作为 H_3 的输入。系统设置算法和密钥提取算法与原方案基本相同,以下仅列出不同之处。

1)指定验证者签名:已知签名者 A 的私钥 S_{IDA}、指定验证者 B 的公钥 Q_{IDB} 和消息 M。A 选择 $r \in Z_q^*$,计算 $U = rQ_{IDB}$,$h = H_2(M,U)$,$V = r^{-1}hS_{IDA}$,$W = H_3(e(U,V))$,则 A 对消息 M 的签名 $\sigma = (U,W)$。

2)指定验证者验证:已知指定验证者 B 的私钥 S_{IDB}、签名者 A 的公钥 Q_{IDA}、消息 M 和签名 $\sigma = (U,W)$。B 首先计算 $h = H_2(M,U)$,然后验证等式 $W = H_3(e(S_{IDB},hQ_{IDA}))$ 是否成立,如果成立,则签名 σ 有效。

3)副本模拟:B 选择 $r' \in Z_q^*$,计算 $U' = r'Q_{IDA}$,$h' = H_2(M,U')$,$V' = r'^{-1}h'S_{IDB}$,$W' = H_3(e(V',U'))$,则有模拟签名 $\sigma' = (U',W')$。

由 $H_3(e(S_{IDB},h'Q_{IDA})) = H_3(e(sQ_{IDB},h'Q_{IDA})) = H_3(e(r'^{-1}h'sQ_{IDB},rQ_{IDA})) = H_3(e(V',U'))$ 可知,签名 $\sigma' = (U',W')$ 满足验证等式,指定验证者可以产生与签名 σ 不可区分的签名 σ'。

2.4 Zhang 改进方案的安全性分析和效率分析

1)正确性:改进方案的正确性可以通过以下等式验证。

$$W' = H_3(e(S_{IDB},hQ_{IDA})) = H_3(e(sQ_{IDB},hQ_{IDA})) = H_3(e(rQ_{IDB},r^{-1}hsQ_{IDA})) = H_3(e(U,V)) = W$$

2)不可传递性:由副本模拟算法可知,指定验证者 B 可以模拟签名副本:B 选择 $r' \in Z_q^*$,计算 $U' = r'Q_{IDA}$,$h' = H_2(M,U')$,$V' = r'^{-1}h'S_{IDB}$,$W' = H_3(e(V',U'))$,则有模拟签名 $\sigma' = (U',W')$。由 $H_3(e(S_{IDB},h'Q_{IDA})) = H_3(e(sQ_{IDB},h'Q_{IDA})) = H_3(e(r'^{-1}h'sQ_{IDB},rQ_{IDA})) = H_3(e(V',U'))$ 可知,签名 $\sigma' = (U',V')$ 是有效的签名。B 能够产生与 A 的签名不可区分的签名副本,所以改进方案满足不可传递性。

3)不可伪造性:在签名算法中,V 是通过签名者 A 的私钥 S_{IDA} 计算得到的,同时,$e(U,V)$ 内嵌在 H_3 哈希函数中。由哈希函数和双线性对的不可逆性可知,攻击者无法通过 H_3 的值计算得到签名者的私钥,攻击者无法获得有效、正确的签名,因此改进方案是不可伪造的。

4)效率分析:与原方案相比,改进方案将原验证算法中的一个对运算转移到签名算法中,对运算的总数不变。因此,改进方案的效率与原方案的效率相同。

3 Li-Zheng-Zhu 方案的密码学分析

3.1 Li-Zheng-Zhu 方案简述[6]

Li-Zheng-Zhu 方案是一个基于身份的强指定验证者签名方案,方案中的哈希函数为 H_1、$H_2:\{0,1\}^* \to G_1$,系统设置算法和密钥提取算法与 Zhang 方案基本相同,故略去。

1)指定验证者签名:已知签名者 A 的私钥 sk_{IDA}、指定验

证者 B 的公钥 Q_{IDB} 和消息 M。A 随机选择 $r \in Z_q^*$,计算 $U = rQ_{IDB}$, $V = e(rH_2(M) + sk_{IDA}, Q_{IDB})$。则 A 对消息 M 的签名 $\sigma = (U,V)$。

2) 指定验证者验证:已知指定验证者 B 的私钥 sk_{IDB}、签名者 A 的公钥 Q_{IDA}、消息 M 和签名 $\sigma = (U,V)$,B 验证等式 $V = e(H_2(M),U)e(Q_{IDA},sk_{IDB})$ 是否成立,如果成立,则签名 σ 有效。

3) 副本模拟:B 随机选择 $r' \in Z_q^*$,并计算 $U' = r'sk_{IDB}$, $V' = e(r'H_2(M) + Q_{IDA}, sk_{IDB})$,则有模拟签名 $\sigma' = (U',V')$。显然 $\sigma' = (U',V')$ 有效。

3.2 Li-Zheng-Zhu 方案的密码学分析

文献[6]声称,验证等式中需要验证者的私钥,所以没有第三方可以验证签名的有效性,该方案是强指定验证签名。分析 Li-Zheng-Zhu 方案,发现非指定验证者也可以验证签名的有效性。

假设 $\sigma = (U,V)$ 是消息 M 的指定验证签名,凡是得到 σ 签名的任何用户都可以计算出 $e(Q_{IDA},sk_{IDB})$,并可以验证下一个新签名 $\sigma^* = (U^*,V^*)$。

1) 首先计算 $H_2(M)$ 和 $e(H_2(M),U)$,然后根据验证等式 $V = e(H_2(M),U)e(Q_{IDA},sk_{IDB})$ 计算 $e(Q_{IDA},sk_{IDB}) = V/e(H_2(M),U)$。$e(Q_{IDA},sk_{IDB})$ 是固定值,因此利用 $e(Q_{IDA},sk_{IDB})$ 可以验证其他签名。

2) 如果攻击者得到新消息 M^* 的签名 $\sigma^* = (U^*,V^*)$,可以验证签名 $\sigma^* = (U^*,V^*)$ 的有效性。攻击者首先计算 $H_2(M^*)$,然后可以验证 $V^* = e(H_2(M^*),U^*)e(Q_{IDA},sk_{IDB})$ 等式成立。

攻击者之前已经得到了固定值 $e(Q_{IDA},sk_{IDB})$,所以攻击者在不知道指定验证者 B 私钥的情况下,很容易验证下一个新的指定验证签名的有效性。

3.3 Li-Zheng-Zhu 方案的改进

为了克服 Li-Zheng-Zhu 方案的不足,使用短签名[7]对方案改进。首先在系统设置算法中增加一个哈希函数 $H_3:\{0,1\}^* \rightarrow Z_q^*$,并修改 H_2 哈希函数的输入,然后执行以下过程。

1) 指定验证者签名:已知签名者 A 的私钥 sk_{IDA}、指定验证者 B 的公钥 Q_{IDB} 和消息 M。A 随机选择 $r \in Z_q^*$,计算 $U = rQ_{IDA}$, $h = H_3(e(sk_{IDA},rQ_{IDB}))$, $V = hH_2(M,U)$。A 对消息 M 的指定验证签名为 $\sigma = (U,V)$。

2) 指定验证者验证:已知指定验证者 B 的私钥 sk_{IDB}、签名者 A 的公钥 Q_{IDA}、消息 M 和签名 $\sigma = (U,V)$,B 计算 $h' = H_3(e(U,sk_{IDB}))$,并验证等式 $V = h'H_2(M,U)$ 是否成立,如果成立,则签名 σ 有效。

3) 副本模拟:B 选择 $r' \in Z_q^*$,计算 $U' = r'Q_{IDA}$, $h' = H_3(e(r'Q_{IDA},sk_{IDB}))$, $V' = h'H_2(M,U')$,则有模拟签名 $\sigma' = (U',V')$。显然,验证等式成立,即模拟签名 $\sigma' = (U',V')$ 有效。

3.4 Li-Zheng-Zhu 改进方案的安全性分析和效率分析

1) 正确性:改进方案的正确性可以通过以下等式验证。

$$h' = H_3(e(U,sk_{IDB})) = H_3(e(rQ_{IDA},sQ_{IDB})) = H_3(e(sQ_{IDA},rQ_{IDB})) = H_3(e(sk_{IDA},rQ_{IDB})) = h$$

2) 不可传递性:由改进方案的副本模拟过程可知,模拟签名是有效的签名。指定验证者 B 能够产生与签名者 A 的签名不可区分的签名副本,所以改进方案满足不可传递性。

3) 不可伪造性:在改进方案中,一方面,签名时,如果没有签名者 A 的私钥 sk_{IDA},就无法计算 H_3 哈希函数。同时,包含签名者 A 私钥的 $e(sk_{IDA},rQ_{IDB})$ 内嵌在 H_3 哈希函数中,由哈希函数和双线性对的不可逆性可知,即使攻击者知道 H_3 的值,也无法计算出签名者的私钥。另一方面,签名的安全性是由短签名的安全性来保证的,短签名被证明是安全的[7],因此该进方案也是安全的。

4) 强指定性:在验证过程中,计算 H_3 哈希函数必须使用指定验证者 B 的私钥,否则验证等式不成立。同时,攻击者从已经获得的签名中得不到有用的信息,因此,改进方案是一个强指定验证签名方案。

5) 效率分析:由表 1 数据可知(P 表示对运算,M 表示 G_1 群上的数乘运算),Li-Zheng-Zhu 方案需要 3 个对运算,改进方案只需要 2 个对运算。因此,改进方案的效率比原方案的效率高。

表 1　方案的效率比较

方案	签名过程	验证过程
Li-Zheng-Zhu 原方案	1P + 2M	2P
改进方案	1P + 3M	1P

4　结语

指定验证者签名要求设计方案不仅满足不可伪造性,同时必须满足指定验证性。本文分析了两个指定验证者签名方案 Zhang 方案和 Li-Zheng-Zhu 方案,指出前者不满足不可伪造性、后者不满足指定验证性。对两个方案进行了改进,改进后的 Zhang 方案具有与原方案相同的效率,改进后的 Li-Zheng-Zhu 方案比原方案少一个双线性对运算,与原方案相比,具有较高的效率。

参考文献:

[1] JAKOBSSON M, SAKO K, IMPAGLIAZZO R. Designated verifier proofs and their applications [C]// Cryptology-EUROCRYPT 1996, LNCS 1070. Berlin: Springer-Verlag, 1996: 142 - 154.

[2] SUSILO W, ZHANG FANGGUO, MU YI. Identity based strong designated verifier signature schemes [C]// ACISP'2004: Proceedings of the 9th Australasian Conference on Information Security and Privacy, LNCS 3108. Berlin: Springer-Verlag, 2004: 313 - 324.

[3] KUMAR K P, SHAILAJA G, SAXENA A. Identity based strong designated verifier signature scheme [EB/OL]. [2009 - 09 - 22]. http://eprint.iacr.org/2006/134.pdf.

[4] ZHANG J, MAO J. A novel id-based designated verifier signature scheme [J]. Information Sciences, 2008, 178(3): 766 - 773.

[5] 张学军. 高效的基于身份的指定验证者签名[J]. 计算机工程, 2009, 35(5): 131 - 132, 135.

[6] 李明祥, 郑雪峰, 朱建勇, 等. 一种高效的基于身份的强指定验证者签名方案[J]. 四川大学学报: 工程科学版, 2009, 41(7): 176 - 180.

[7] BONEH D, LYNN B, SHACHAM H. Short signature from the Weil pairing [C]// Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, LNCS 2248. Berlin: Springer-Verlag, 2001: 514 - 532.