

几个无证书签名方案的伪造攻击

王菁¹, 李祖猛²

(1. 广州市信息工程职业学校基础部, 广东 广州 510640;

2. 广东科学技术职业学院计算机工程技术学院(人工智能学院), 广东 珠海 519090)

摘要: 自2003年 Al-Riyami 和 Paterson 首次提出无证书公钥密码体制的概念和第一个无证书签名方案以来, 许多无证书签名方案相继被提出。汤永利等提出了9个无双线性对运算的无证书签名方案, 并声称这些无证书签名方案在椭圆曲线离散对数困难性假设下可证明是安全的。通过对这些无证书签名方案进行安全性分析后, 发现其中的5个可证明安全的无证书签名方案不能抵抗替换公钥攻击, 并且这5个无证书签名方案中的3个签名方案即使在不替换用户公钥的情况下, 攻击者也可以利用用户的原始公钥对任意消息伪造出有效的签名。给出了具体的伪造攻击方法, 证明了这5个无证书签名方案是不安全的。

关键词: 无证书签名; 椭圆曲线; 离散对数; 公钥替换攻击

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020039

Forgery attacks on several certificateless signature schemes

WANG Jing¹, LI Zumeng²

1. Foundation Department, Guangzhou Information Engineering Vocational School, Guangzhou 510640, China

2. Computer Engineering Technical College(Artificial Intelligence College), Guangdong Polytechnic of Science and Technology, Zhuhai 519090, China

Abstract: Since Al-Riyami and Paterson proposed the novel concept of certificateless cryptography and the first certificateless signature scheme in 2003, a lot of certificateless signature schemes were proposed one after another. Recently, Tang et al proposed nine certificateless signature schemes without bilinear pairing. Although they demonstrated that their schemes were unforgeable under the assumption of elliptic curve discrete logarithmic problem, it can be found that five of their schemes could not resist the public key substitution attack, the attacker could use the user's original public key to forge a valid signature for three of these schemes. The attack methods are to demonstrate that prove five certificateless signature schemes are insecure.

Key words: certificateless signature, elliptic curve, discrete logarithm problem, public key replacement attack

1 引言

在2003年亚密会上, Al-Riyami 和 Paterson^[1]首次提出了无证书公钥密码体制的概念, 并且给

出了第一个无证书签名方案。在无证书公钥密码体制中, 密钥生成中心(KGC, key generation center)和用户一起完成用户的部分密钥生成过程, 即用户密钥的一部分数据由KGC产生, 然

收稿日期: 2019-05-09; 修回日期: 2019-07-29

通信作者: 李祖猛, zumengli@126.com

论文引用格式: 王菁, 李祖猛. 几个无证书签名方案的伪造攻击[J]. 网络与信息安全学报, 2020, 6(3): 108-112.

WANG J, LI Z M. Forgery attacks on several certificate lesssignature schemes[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 108-112.

后 KGC 将其安全地传输给用户，用户自己产生密钥的另外一部分数据，这两部分密钥数据组合在一起构成用户的完整密钥。这种产生密钥的方式使 KGC 不能获知用户的完整私钥，进而解决了基于身份的密码体制^[2]中的密钥托管问题，而且在无证书公钥密码体制中，因为不再需要证书中心（CA）对用户的证书进行管理和维护，解决了传统基于 PKI 公钥密码体制^[3]的证书管理问题，使无证书公钥密码体制受到了广泛的关注。

无证书签名是无证书公钥密码体制中的研究热点之一。自 Al-Riyami 和 Paterson 在文献[1]中提出第一个无证书签名方案以来，很多无证书签名方案相继被提出^[4-9]。在无证书公钥密码体制中，因为用户的公钥无法认证，所以无证书公钥密码方案的设计必须考虑抵抗替换公钥攻击。另外，在无证书公钥密码体制中，KGC 参与用户私钥的部分数据产生，所以必须考虑恶意不诚实 KGC 的伪造攻击。Huang 等^[10]提出的无证书签名方案的安全模型定义了普通攻击者、强攻击者、超级攻击者。2012 年，王圣宝等^[11]基于离散对数困难问题，提出了一个不使用双线性对的无证书签名方案，并在随机预言模型中给出了安全性证明。但王亚飞等^[12]指出文献[11]是完全不安全的，即攻击者可以获取用户的私钥，并且基于椭圆曲线离散对数问题提出了新的方案，同时在随机预言模型下给出了新方案的安全性证明。但樊爱苑等^[13]对文献[12]中的新方案进行安全性分析后，指出其难以抵抗不诚实 KGC 下的公钥替换攻击，并针对此安全缺陷，改变传统无证书算法顺序，提出了能够抵抗不诚实 KGC 公钥替换攻击的新方案，且新方案避开了双线性运算和逆运算，提升了运算效率，声称其新方案在自适应选择消息攻击下是存在性不可伪造的。2016 年，汤永利等^[14]给出了针对文献[13]中新方案的一个伪造攻击，结论表明第 I 类强攻击者^[10]能成功伪造任意用户对任意消息的有效签名，并基于椭圆曲线离散对数困难性假设提出了 9 个新的改进方案，声称其改进方案中的前两种方案能够抵抗第 I 类超级攻击者^[10]、第 II 类超级攻击者^[10]的攻击，改进方案中的第 3~9 种方案能够抵抗第 I 类强攻击者^[10]、第 II 类超级攻击者的攻击。

本文对汤永利等的 9 个无证书签名方案^[14]进行安全性分析后，发现其中的第 1、2、5、8、9 这 5 个无证书签名方案不能抵抗替换公钥攻击，并且其中第 5、8、9 这 3 个方案即使不替换公钥，攻击者也可以利用用户的原始公钥对任意消息伪造出有效的签名。分析结论表明，文献[14]中的这 5 个签名方案是不安全的。

2 预备知识

2.1 困难问题与安全假设

设 E/F_q 是定义在有限素域 F_q (q 为大素数) 上的椭圆曲线， E/F_q 上的所有点以及无穷远点 O 构成一个循环加法群 G ，点 P 是 G 的一个生成元，其阶为 q 。

定义 1 椭圆曲线离散对数问题 (ECDLP, elliptic curve discrete logarithm problem): 给定 G 上的点 Q ，求 $a \in Z_q^*$ ，使 $Q = aP$ 。

ECDLP 安全假设：不存在概率多项式算法 A ，能够在多项式时间内以不可忽略的优势解决 ECDLP。

2.2 无证书签名方案的形式化定义

在无证书签名方案中，包括 3 个合法参与者：KGC、签名者 ID_s 、验签者 ID_v 。一个无证书签名方案通常包含以下 7 个多项式时间算法。

(1) 系统参数建立算法

由 KGC 运行，输入安全参数 k ，输出系统公开参数 $params$ 和主密钥 s ， s 由 KGC 秘密保管。

(2) 部分私钥生成算法

由 KGC 运行，输入 $params$ 和 s 以及用户的身份 ID ，输出该用户的部分密钥 D_{ID} ，并通过安全信道返回给用户 ID 。

(3) 用户秘密值生成算法

由用户运行，输入 $params$ 和用户的身份 ID ，输出该用户的秘密值 x_{ID} 。

(4) 用户私钥生成算法

由用户运行，输入 $params$ 、用户的身份 ID 、部分密钥 D_{ID} 以及秘密值 x_{ID} ，输出该用户的私钥 SK_{ID} 。

(5) 用户公钥生成算法

由用户运行，输入 $params$ 、用户的身份 ID 、部

分密钥 D_{ID} 以及秘密值 x_{ID} , 输出该用户的公钥 PK_{ID} 。

(6) 签名算法

由签名者 ID_s 运行, 输入 $params$ 、签名者的身份 ID_s 、私钥 SK_{ID_s} 、公钥 PK_{ID_s} 以及待签消息 m , 输出用户 ID_s 对消息 m 的签名值 σ 。

(7) 验证算法

由验签者 ID_v 运行, 输入 $params$ 、签名者的身份 ID_s 、公钥 PK_{ID_s} 以及消息 m 和对应的签名值 σ , 若签名验证通过, 输出“1”, 表示接受; 否则输出“0”, 表示拒绝。

3 汤永利等给出的签名方案

针对樊爱宛等方案^[13]存在的安全漏洞, 汤永利等人 2016 年在文献[14]中基于椭圆曲线离散对数困难假设提出了一类改进的可证明安全的无证书签名方案, 具体描述如下。

(1) 系统参数建立算法

输入安全参数 k , 输出 2 个大素数 p 、 q , 满足 $q|p-1$ 。设 P 是循环群 G 的一个阶为 q 的生成元。选择 2 个安全 Hash 函数 $H_1: \{0,1\}^* \rightarrow Z_q^*$, $H_2: \{0,1\}^* \rightarrow Z_q^*$, KGC 选择系统主密钥 $s \in Z_q^*$, 计算系统公钥 $P_0 = sP$, 系统公开参数 $params = \langle p, q, G, P, P_0, H_1, H_2 \rangle$ 。

(2) 部分私钥生成算法

输入 $params$ 和用户的身份 $ID_a \in \{0,1\}^*$, KGC 随机选取 $r_a \in Z_q^*$, 计算 $R_a = r_a P$, $D_a = r_a + sH_1(ID_a, R_a)$, D_a 作为用户 ID_a 的部分私钥, R_a 作为用户的部分公钥, KGC 将 (R_a, D_a) 通过安全信道发送给用户 ID_a 。

用户验证 $D_a P = R_a + H_1(ID_a, R_a) P_0$ 是否成立, 若成立, 则判定 D_a 是有效的部分私钥; 否则, 判定 D_a 无效。

(3) 用户秘密值生成算法

用户随机选取秘密值 $x_a \in Z_q^*$ 。

(4) 用户私钥生成算法

用户 ID_a 的完整私钥 $SK_a = (x_a, D_a)$ 。

(5) 用户公钥生成算法

计算 $X_a = x_a P$, 用户 ID_a 设置其公钥为 $PK_a = (X_a, R_a)$ 。

(6) 签名算法

对消息 $M \in \{0,1\}^*$, 用户 ID_a 按以下方式进行签名:

1) 随机选取 $t \in Z_q^*$, 计算 $T = tP$;

2) 计算 $h_2 = H_2(ID_a, M, R_a, X_a, T)$;

3) 汤永利等的 9 个无证书签名方案如表 1 所示^[14]。根据表 1 的公式计算 v , 消息 M 的签名为 $\sigma = (T, v)$ 。

(7) 验证算法

验签者收到 ID_a 的对消息 M 签名 σ 后, 计算 $h_1 = H_1(ID_a, R_a)$, $h_2 = H_2(ID_a, M, R_a, X_a, T)$, 按表 1 的公式计算 T' , 验证 $T' = T$ 是否成立, 若成立, 则输出“1”, 表示接受; 否则输出“0”, 表示拒绝。

表 1 签名与验证
Table 1 Signature and verification

签名方案	签名阶段计算 v 的值	验证阶段计算 T' 的值
1	$v = x_a + D_a + th_2$	$T' = h_2^{-1}(vP - X_a - R_a - h_1 P_0)$
2	$v = x_a + D_a + th_2^{-1}$	$T' = h_2(vP - X_a - R_a - h_1 P_0)$
3	$v = t^{-1}(h_2 x_a + D_a)$	$T' = v^{-1}(h_2 X_a + R_a + h_1 P_0)$
4	$v = t^{-1}(x_a + h_2 D_a)$	$T' = v^{-1}(X_a + h_2 R_a + h_1 h_2 P_0)$
5	$v = t^{-1}h_2(x_a + D_a)$	$T' = v^{-1}h_2(X_a + R_a + h_1 P_0)$
6	$v = t(h_2 x_a + D_a)^{-1}$	$T' = v(h_2 X_a + R_a + h_1 P_0)$
7	$v = t(x_a + D_a h_2)^{-1}$	$T' = v(X_a + h_2 R_a + h_1 h_2 P_0)$
8	$v = t(h_2 x_a + h_2 D_a)^{-1}$	$T' = v h_2(X_a + R_a + h_1 P_0)$
9	$v = th_2(x_a + D_a)^{-1}$	$T' = h_2^{-1}v(X_a + R_a + h_1 P_0)$

4 替换公钥攻击

假设攻击者 Eve 希望假冒用户 ID_a 对消息 M 进行签名, 用户 ID_a 的公钥 $PK_a = (X_a, R_a)$ 。

4.1 签名方案 1 的攻击

通过分析该方案的签名验证等式 $T' = h_2^{-1}(vP - X_a - R_a - h_1 P_0)$ 可知, 对于不知道系统主密钥 s 的攻击者 Eve 而言, 若想成功伪造签名 $\sigma = (T, v)$ 值, 只需借助替换后的公钥 X^* 将隐藏有系统主密钥 s 的系统公钥 $P_0 = sP$ 在运算中消除。从而可以在不知道系统主密钥 s 的情况下, 通过验证等式再计算出签名值中的 v , 最终可以假冒用户 ID_a 构造出对任意消息 M 的有效签名值。

攻击者 Eve 执行以下步骤即可成功伪造签名：

- 1) 随机选取 $r^* \in Z_q^*$ ，计算 $R^* = r^*P$ ；
- 2) 计算 $h_1^* = H_1(\text{ID}_a, R^*)$ ；
- 3) 随机选取 $x^* \in Z_q^*$ ，计算 $X^* = x^*P - h_1^*P_0$ ；
- 4) 利用 $\text{PK}_a^* = (X^*, R^*)$ 替换用户 ID_a 的原有公钥 $\text{PK}_a = (X_a, R_a)$ ；
- 5) 随机选取 $t \in Z_q^*$ ，计算 $T = tP$ ；
- 6) 计算 $h_2^* = H_2(\text{ID}_a, M, R^*, X^*, T)$ ；
- 7) 计算 $v = h_2^*t + x^* + r^*$ ；
- 8) 得到伪造的签名 $\sigma = (T, v)$ 。

该签名 $\sigma = (T, v)$ 可以通过第三方的验证，

因为

$$\begin{aligned} T' &= (h_2^*)^{-1}(vP - X^* - R^* - h_1^*P_0) = \\ &= (h_2^*)^{-1}((h_2^*t + x^* + r^*)P - (x^*P - h_1^*P_0) - R^* - h_1^*P_0) = \\ &= (h_2^*)^{-1}((h_2^*t + x^* + r^*)P - x^*P + h_1^*P_0 - R^* - h_1^*P_0) = \\ &= (h_2^*)^{-1}((h_2^*t + x^* + r^*)P - x^*P - r^*P) = \\ &= (h_2^*)^{-1}((h_2^*t + x^* + r^*) - x^* - r^*)P = \\ &= (h_2^*)^{-1}(h_2^*t)P = tP = T \end{aligned}$$

4.2 其他签名方案的攻击

根据以上对签名方案 1 的替换公钥攻击与分析可知，文献[14]给出的签名方案 2、5、8、9 都可以利用类似签名方案 1 中的攻击方法进行替换公钥攻击，具体的替换公钥攻击过程在此不再赘述。

4.3 替换公钥攻击原因分析

文献[14]中的 1、2、5、8、9 方案易受替换公钥攻击的原因是这些方案不满足 Rafael-Ricardo 关于无证书的一般模式的要求^[15]。Rafael-Ricardo 无证书方案的一般模式要求：对于消息 M 的无证书签名方案，若该方案对应签名元组为 (σ_1, h, σ_2) ，该元组 (σ_1, h, σ_2) 需满足以下 3 个条件：

- 1) 从一个大集合中随机选择 σ_1 ；
- 2) h 至少是 M 、 σ_1 和用户公钥的哈希值；
- 3) σ_2 只依赖于 M 、 σ_1 和 h 。

以文献[14]中的 1 方案为例分析，该方案中的签名元组为 $\sigma = (T, v)$ ，其中， T 通过随机选取 $t \in Z_q^*$ 计算得到，符合 Rafael-Ricardo 无证书方案的一般模式的第 1 条要求，其中，摘要值 $h_2 = H_2(\text{ID}_a, M, R_a, X_a, T)$ ，满足 Rafael-Ricardo

无证书方案的一般模式的第 2 条要求，但 $v = x_a + D_a + th_2$ ，其中， h_2 可以通过 t 选取使 v 不依赖于 h_2 ，由此可知，该方案不符合 Rafael-Ricardo 无证书方案的一般模式的第 3 条要求。而文献[14]中给出的 3、4、6、7 方案满足 Rafael-Ricardo 关于无证书的一般模式。以其中的方案 4 为例进行说明：该方案的签名元组为 $\sigma = (T, v)$ ，显然满足 Rafael-Ricardo 无证书方案的一般模式的前两条要求，并且 $v = t^{-1}(x_a + h_2D_a)$ ，无法通过 t 选取使 v 不依赖于 h_2 。由此可知，该方案满足 Rafael-Ricardo 无证书方案的一般模式的第 3 条要求。

具有 Rafael-Ricardo 无证书一般模式特征的签名方案，可以抵抗一般用户的公钥替换攻击^[15]。所以文献[14]中给出的 3、4、6、7 方案可以抵抗前述的替换公钥攻击，具体证明过程可以参考文献[15]。

5 其他类型的伪造攻击

5.1 签名方案 5 的攻击

文献[14]中给出的签名方案 5 的验证等式为 $T' = v^{-1}h_2(X_a + R_a + h_1P_0)$ ，其中，随机数 T 的完整性检验值 $h_2 = H_2(\text{ID}_a, M, R_a, X_a, T)$ 可以与被特殊选择的签名值 v 运算构造出初始参与签名的随机数 T 。攻击者 Eve 可以在不替换用户 ID_a 的原始公钥 $\text{PK}_a = (X_a, R_a)$ 的情况下，伪造用户 ID_a 对任意消息 M 的签名，具体伪造攻击步骤如下。

- 1) 计算 $h_1 = H_1(\text{ID}_a, R_a)$ 。
- 2) 随机选取 $t \in Z_q^*$ ，计算 $T = t(X_a + R_a + h_1P_0)$ 。
- 3) 计算 $h_2 = H_2(\text{ID}_a, M, R_a, X_a, T)$ 。
- 4) 计算 $v = h_2t^{-1}$ 。
- 5) 得到伪造的签名 $\sigma = (T, v)$ 。

该签名 $\sigma = (T, v)$ 可以通过第三方的验证，

因为

$$\begin{aligned} T' &= v^{-1}h_2(X_a + R_a + h_1P_0) = \\ &= (h_2t^{-1})^{-1}h_2(X_a + R_a + h_1P_0) = \\ &= t(X_a + R_a + h_1P_0) = T \end{aligned}$$

5.2 其他签名方案的攻击

根据以上对签名方案 5 的伪造攻击与分析可知，文献[14]中给出的签名方案 8、9 的验证等式

分别为

$$T' = v h_2(X_a + R_a + h_1 P_0)$$

$$T' = v h_2^{-1}(X_a + R_a + h_1 P_0)$$

显然这两个签名方案与文献[14]中签名方案5存在相同的安全漏洞,可以利用与4.1节中类似的伪造攻击方法在不替换用户公钥的情况下,对任意选择的消息进行伪造签名,具体攻击过程在此不再赘述。

5.3 攻击原因分析

文献[14]中的5、8、9方案可以在不替换用户公钥的情况下,对任意消息伪造签名的原因是计算 T' 的等式中摘要值 h_2 可以通过特定选择的 v 值抵消,从而导致 T' 可以通过已有公开参数用户公钥 X_a 、 R_a 、系统公钥 P_0 等计算得到。显然,文献[14]中的其他方案,无法通过 v 值的选取,将验证等式中的摘要值 h_2 消除,所以文献[14]中的其他方案可以抵抗本节中提出的不替换公钥的伪造攻击。

6 结束语

由于无证书签名体制不存在密钥托管问题,同时在验证签名过程中无须验证签名者公钥的合法性,所以无证书公钥密码体制的研究受到了较高的关注。本文对文献[14]中的9个无证书签名方案进行安全性分析后,发现其中的5个方案不能抵抗替换公钥攻击,并且其中的3个签名方案即使在不替换用户公钥的情况下,攻击者也可以对任意选择的消息伪造出有效的签名,并给出了具体的攻击方案。分析结论表明这5个无证书签名方案是不安全的。

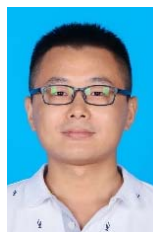
参考文献:

- [1] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptology-ASIACRYPT 2003. 2013: 452-473.
- [2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology-CRYPTO'84. 1985: 47-58.
- [3] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 664-654.
- [4] ISLAM S H, BISWAS G P. Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography[J]. International Journal of Computer Mathematics, 2013, 90(11): 2244-2258.
- [5] FENG S R, MO J, FENG S R, et al. An efficient and provably secure certificateless short signature scheme[C]//International Conference on Computer Science & Electronics Engineering. 2013.
- [6] GONG P, LI P. Further improvement of a certificateless signature scheme without pairing[J]. International Journal of Communication Systems, 2014, 27(10): 2083-2091.
- [7] ISLAM S H, OBAIDAT M S. Design of provably secure and efficient certificateless blind signature scheme using bilinear pairing[J]. Security and Communication Networks, 2015, 8(18): 4319-4332.
- [8] ALLAM A M, ALI I A, MAHGOUB S M. A provably secure certificateless organizational signature schemes[J]. International Journal of Communication Systems, 2017, 30(5): 1760-1768.
- [9] KYUNG-AH S. A new certificateless signature scheme provably secure in the standard model[J]. IEEE Systems Journal, 2018:1-10.
- [10] HUANG X, MU Y, SUSILO W, et al. Certificateless signature revisited[J]. Lecture Notes in Computer Science, 2007, 4586: 308-322.
- [11] 王圣宝, 刘文浩, 谢琪. 无双线性配对的无证书签名方案[J]. 通信学报, 2012, 33(4): 93-98.
WANG S B, LIU W H, XIE Q. Certificateless signature scheme without bilinear pairings[J]. Journal on Communications, 2012, 33(4): 93-98.
- [12] 王亚飞, 张睿哲. 强安全无对的无证书签名方案[J]. 通信学报, 2013, 34(2): 94-99, 108.
WANG Y F, ZHANG R Z. Strongly secure certificateless signature scheme without pairings[J]. Journal on Communications, 2013, 34(2): 94-99, 108.
- [13] 樊爱宛, 杨照锋, 谢丽明. 强安全无证书签名方案的安全性分析与改进[J]. 通信学报, 2014, 35(5): 118-123.
FAN A W, YANG Z F, XIE L M. Security analysis and improvement of strongly secure certificate less signature scheme[J]. Journal on Communications, 2014, 35(5): 118-123.
- [14] 汤永利, 王菲菲, 叶青, 等. 改进的可证明安全无证书签名方案[J]. 北京邮电大学学报, 2016, 39(1): 112-116.
TANG Y L, WANG F F, YE Q, et al. Improved provably secure certificateless signature scheme[J]. Journal of Beijing University of Posts and Telecommunications, 2016, 39(1): 112-116.
- [15] RAFAEL C, RICARDO D. Two notes on the security of certificateless signatures[C]//International Conference on Provable Security. Springer-verlag, 2007. 2007: 85-102.

[作者简介]



王菁(1983—),女,山西运城人,硕士,主要研究方向为最优化理论与方法、网络算法及其在通信网中的应用。



李祖猛(1984—),男,山东临清人,硕士,主要研究方向为密码学与信息安全。