计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200500002

无双线性对的无证书签名方案及其在配电网中的应用

刘 帅 陈建华
武汉大学数学与统计学院 武汉 430072
(shuai_liu@whu.edu.cn)

摘 要 无证书密码体制解决了传统公钥密码体制存在的公钥证书管理复杂的问题,以及基于身份的密码体制存在的密钥托管问题。因此,文中提出了一种基于椭圆曲线的无双线性对的无证书签名方案,在随机预言机模型以及椭圆曲线离散对数困难问题假设下,利用分叉引理(The Forking Lemma)证明了该方案可以抵抗第一类强敌手和第二类敌手的攻击。然后,将该方案与2016年以来提出的其他4种基于椭圆曲线的无证书签名方案在理论上进行性能比较,并采用C语言实现所有签名方案,对所有方案进行效率比较。实验结果表明,该方案与Jia方案相比平均总耗时相近,与Hassouna方案、Zhang方案和Karati方案相比,平均总耗时分别减少了约51.0%,10.4%和22.1%,说明所提方案的总效率具有一定的优势。最后,将提出的签名方案应用到配电网Modbus TCP(Transmission Control Protocol)模式通信的报文认证中,对提出的认证协议进行了安全性分析,结果表明其可以抵抗重放攻击、伪装攻击和中间人攻击。

关键词:无证书签名;无双线性对;椭圆曲线离散对数问题;分叉引理;配电网;Modbus报文
中图法分类号 TN918

Certificateless Signature Scheme Without Bilinear Pairings and Its Application in Distribution Network

LIU Shuai and CHEN Jian-hua
School of Mathematics and Statistics, Wuhan University, Wuhan 430072, China

Abstract The certificateless cryptosystem solves the complex problem of public key certificate management in the traditional public key cryptosystem and the problem of key escrow in the identity based cryptosystem. This paper proposes a certificateless signature scheme based on the elliptic curve with no bilinear pairings. Under the assumption of random oracle model and the difficulty of elliptic curve discrete logarithm, by using the bifurcation lemma (the Forking lemma), this paper proves that the scheme can resist the attack of the first class of strong adversaries and the second class of adversaries. Then, the performance of the scheme is compared with that of the other four certificateless signature schemes based on elliptic curve proposed since 2016, and all signature schemes are implemented by C language, and the efficiency of all schemes is compared. The results show that the average total time consumption of the proposed scheme is similar to that of Jia scheme, and compared with that of Hassouna scheme, Zhang scheme and Karati scheme, the average total time consumption are decreased by 51.0%, 10.4% and 22.1% respectively, which shows that the total efficiency of this scheme has some advantages. Finally, the signature scheme of this paper is applied to the message authentication of Modbus TCP (Transmission Control Protocol) communication in distribution network. The security analysis of the proposed authentication protocol shows that the proposed scheme can resist replay attack, camouflage attack and man in the middle attack.

Keywords Certificateless signature, No bilinear pairings, Elliptic curve discrete logarithm problem, The Forking Lemma, Distribution network, Modbus message

1 引言

随着通信网络和信息技术越来越广泛地应用于电网之中,电网遭受网络攻击的风险逐渐增大[1]。因此,需要在电网通信过程中对报文采用公钥密码学的数字签名进行认证,以免电网遭受网络攻击而影响系统的安全运行。

在配电网中,当主站和终端的距离较远时,若采用传统公钥密码体制(Public Key Cryptography, PKC)进行数字签名,公钥证书的下载和验证等通信开销较大的过程会影响配电业务的实时性[2]。当采用基于身份的密码体制(Identity-Based Cryptography, IBC)进行数字签名时,虽然PKC体制中复杂的公钥管理问题得到了解决,但IBC体制由于存在密钥托管和密钥分发的问题而在一定程度上受到了限制。无证书公钥密码体制由Al-Riyami等于2003年首次提出[3],无证书签名

到稿日期:2020-05-06 返修日期:2020-07-17 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
通信作者:陈建华(chenjh_ecc@163.com)

方案因为用户公钥通过可靠方式公布和用户私钥只有用户知道，从而解决了 PKC 体制和 IBC 体制存在的问题。

2018 年，Zou 等[4]提出基于 SM2 的数字签名算法的配电网报文认证协议。2019 年，Qiu 等[5]提出采用 SM9 的数字签名算法对配电网报文进行认证。鉴于配电自动化领域处理器的处理能力不高、存储空间有限[6]，使用双线性对会增大计算开销，本文使用基于椭圆曲线上无双线性对的无证书签名方案对配电网报文进行认证。该方案较 Qiu 等提出的方案在减轻处理器的计算负担方面有优势，同时解决了 PKC 体制的公钥管理问题以及 IBC 体制中存在的密钥托管问题。

2　预备知识

2.1　Modbus TCP 报文

Modbus 协议是一种广泛应用于工业领域的通信协议，在当前配电网系统的实际应用中，Modbus 协议因实现简单、协议效率高而被普遍采用[4]。Modbus 协议主要有 Modbus ASCII，Modbus RTU（Remote Terminal Unit）和 Modbus TCP（Transmission Control Protocol）3 种模式。

Modbus ASCII 协议的传输效率远低于 Modbus RTU 协议。Modbus RTU 协议通常被应用于工业现场中不超过百米的短距离通信，遭受网络攻击的风险相对较低。因此，在通信过程中需要重点考虑对 Modbus TCP 报文采用数字签名方法。作为 TCP/IP 的一种具体应用方式，Modbus TCP 模式与经典的 TCP/IP 协议族一样，是一组不同的协议组合构成的四层协议系统，由 14 个字节的以太网首部、20 个字节的 IP 首部以及 20 个字节的 TCP 首部等经典的报文结构组成[5]，如图 1 所示。

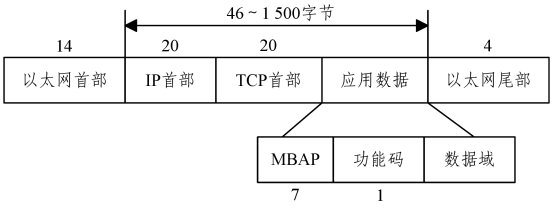

图 1　配电网的 Modbus TCP 报文结构

Fig. 1　Modbus TCP packet structure of distribution network

Modbus TCP 报文中的关键数据主要存储在应用层[5]。Modbus TCP 报文的应用层由 3 个部分组成，分别是 MBAP 报文头、功能码和数据域。在通信过程中，发送端对应用层进行签名；接收端对 Modbus TCP 报文应用层进行认证，并返回应答消息给发送端；发送端验证后确保接收端已经接收到完整报文。

2.2　困难问题

设 F_p 是含 p 个元素的有限域，定义在 F_p（p 是大于 3 的素数）上的椭圆曲线 E 的方程为：

$$y^2=x^3+ax+b \bmod p \tag{1}$$

其中，$a,b\in F_p$ 且 $4a^3+27b^2\neq 0 \bmod p$。满足方程（1）的所有点和一个无穷远点 O 构成的集合 $E(F_p)=\{(x,y)\in F_p^2 \mid (x,y)$ 满足方程（1）$\}\cup\{O\}$ 关于“弦切律”构成一个交换群[7]：$(E(F_p),+)$，其中 O 为该群的单位元，从而可以定义该群上的点乘运算为：$nP=P+\cdots+P$（n 次“+”运算），其中 $n\in Z_q^*$，q 是点 P 的阶。

定义 1（椭圆曲线离散对数问题（Elliptic Curve Discrete Logarithm Problem，ECDLP））　给定椭圆曲线 E 上的点 P，$Q=aP$，其中 $a\in Z_q^*$（q 是点 P 的阶）是未知的随机数，根据 P 和 Q 计算 a。

当点 P 的阶是较大的素数时，普遍认为 ECDLP 在计算上不可行。如果不存在概率多项式时间算法 A 能以不可忽略的优势成功解决 ECDLP，则称 ECDLP 是困难问题。

2.3　无证书签名方案

2.3.1　形式化定义

一个无证书签名方案通常由 7 种算法组成，本文采用简化的定义，即无证书签名方案由系统参数设置算法、部分私钥提取算法、用户密钥生成算法、签名算法和验证算法 5 种算法组成[8]。

（1）系统参数设置算法。输入安全参数 k，KGC 输出系统主密钥 msk 和系统参数 $params$，KGC 公开系统参数 $params$，秘密保存主密钥 msk。

（2）部分私钥提取算法。输入系统参数 $params$、系统主密钥 msk 和用户身份 ID，KGC 输出用户的部分私钥 psk_{ID} 和部分公钥 ppk_{ID}。

（3）用户密钥生成算法。输入系统参数 $params$ 和用户身份 ID，用户产生秘密值 x_{ID}。用户根据部分私钥 psk_{ID} 和秘密值 x_{ID} 产生用户私钥 SK_{ID}，根据部分公钥 ppk_{ID} 和秘密值 x_{ID} 产生用户公钥 PK_{ID}。

（4）签名算法。输入系统参数 $params$、签名者身份 ID、私钥 SK_{ID} 和待签名消息 m，签名者输出对消息 m 的签名 σ。

（5）验证算法。输入系统参数 $params$、消息 m、对消息 m 的签名 σ、签名者身份 ID 和公钥 PK_{ID}，验证者验证用户对消息 m 的签名 σ 是否有效。若签名有效，则输出 1，否则输出 0。

2.3.2　安全模型

对于一个无证书签名方案的安全性，Al-Riyami 等[3]提出其安全模型主要考虑以下两类敌手。

（1）第一类敌手 A_{I}：攻击者不能获得 KGC 的主密钥和目标用户的部分私钥，但是攻击者能替换目标用户的公钥。

（2）第二类敌手 A_{II}：攻击者知道 KGC 的主密钥，但是攻击者不能获得目标用户的秘密值，而且不能替换目标用户的公钥。

Huang 等[9]按敌手的能力从弱到强将敌手（包括 A_{I} 和 A_{II}）分成了 3 类：普通（Normal）敌手、强（Strong）敌手和超级（Super）敌手。如果用户的公钥已经被敌手替换，普通敌手不能得到此用户的有效签名；强敌手必须提供替换后的公钥所对应的秘密值，才能得到使用替换后的公钥进行验证后的有效签名；超级敌手无须提供替换后的公钥所对应的秘密值，就能得到使用替换后的公钥进行验证后的有效签名。方案如果能够抵抗超级敌手的攻击，那么一定能抵抗强敌手的攻击；如果能够抵抗强敌手的攻击，那么一定能抵抗普通敌手的攻击。

Huang 等[9]定义的第一类强敌手 A_{I} 的安全模型通过游戏 1 来定义。

游戏 1　这是一个第一类强敌手 A_{I} 与挑战者 B 进行交互的游戏，过程如下。

(1)系统参数设置:挑战者 B 接受一个安全参数 k 并生成主密钥 msk 和系统参数 $params$,然后将参数 $params$ 发送给 A_I,保密主密钥。

(2)询问阶段:A_I进行以下查询。

1)部分私钥询问:A_I可以请求身份为 ID 的用户的部分私钥。作为响应,B 输出部分私钥 psk_{ID}。

2)秘密值询问:A_I可以请求身份为 ID 的用户的秘密值。作为响应,B 输出秘密值 x_{ID}。

3)公钥询问:A_I可以请求身份为 ID 的用户的公钥。作为响应,B 输出公钥 PK_{ID}。

4)公钥替换:对于身份为 ID 的用户,A_I可以选择新的公钥 PK_{ID}'和对应的秘密值 x_{ID}',将其发送给 B,B 将 PK_{ID}'设置为该用户的新公钥,将 x_{ID}'设置为该用户的新秘密值。

5)签名询问:当 A_I查询身份为 ID 的用户对某个消息 m 的签名时,B 使用与 ID 对应的私钥 SK_{ID}来计算签名 σ,并将其发送给 A_I。

(3)伪造阶段:A_I输出目标身份 ID^* 在消息 m^* 上的签名 σ^*。如果满足以下条件,则称 A_I赢得游戏 1。

1)σ^* 是目标身份 ID^* 对消息 m^* 的有效签名。

2)A_I没有询问过目标身份 ID^* 的部分私钥和秘密值。

3)A_I没有询问过目标身份 ID^* 对消息 m^* 的签名。

定义 2 如果在概率多项式时间内,不存在一个第一类强敌手 A_I在自适应选择身份攻击和自适应选择消息攻击下,能以不可忽略的优势赢得游戏 1,那么就称无证书签名方案对第一类强敌手 A_I是存在性不可伪造的。

Al-Riyami 等[3]提出的第二类敌手 A_{II}的安全模型通过游戏 2 来定义。

游戏 2 这是一个第二类敌手 A_{II}和挑战者 B 进行交互的游戏,过程如下。

(1)系统参数设置:挑战者 B 接受一个安全参数 k 并生成主密钥 msk 和系统参数 $params$,然后将主密钥 msk 和参数 $params$ 发送给 A_{II}。

(2)询问阶段:与游戏 1 相同,B 对 A_{II}的部分私钥询问、秘密值询问、公钥询问和签名询问做出响应。

(3)伪造阶段:A_{II}输出目标身份 ID^* 在消息 m^* 上的签名 σ^*。如果满足以下条件,则称 A_{II}赢得游戏 2。

1)σ^* 是目标身份 ID^* 对消息 m^* 的有效签名。

2)A_{II}没有询问过目标身份 ID^* 的秘密值。

3)A_{II}没有询问过目标身份 ID^* 对消息 m^* 的签名。

定义 3 如果在概率多项式时间内,不存在一个第二类敌手 A_{II}在自适应选择身份攻击和自适应选择消息攻击下,能以不可忽略的优势赢得游戏 2,那么就称无证书签名方案对第二类敌手 A_{II}是存在性不可伪造的。

3 无证书签名方案的设计及其安全性证明

3.1 签名方案设计

本文签名方案的部分私钥提取算法的设计基于 Schnorr 签名方案中的签名算法,本文的用户密钥生成算法没有直接使用部分私钥和秘密值作为用户私钥,而是进行了二者的混合计算。在 3.2 节中本文方案的安全性得到证明的情况下,经过 4.1 节的分析和 4.2 节的仿真,经过此次混合计算后设计的签名算法的运算量有一定优势,从而可以减轻配电网处理器的计算负担。

(1)系统参数设置算法:给定安全参数 k,KGC 在椭圆曲线 $E(F_p)$(p 是大于 3 的素数)上选取阶为素数 q 的循环群 G,群 G 的生成元是 G 中任意一个阶为 q 的点 P,KGC 随机选取 $s\in Z_q^*$ 作为系统主密钥 msk,计算 $P_{pub}=sP$ 作为系统公钥。选择 3 个安全 Hash 函数:$H_1:\{0,1\}^*\times G\rightarrow Z_q^*$,$H_2:\{0,1\}^*\times G\times G\rightarrow Z_q^*$ 和 $H_3:\{0,1\}^*\times\{0,1\}^*\times G\times G\rightarrow Z_q^*$。KGC 将系统参数 $params=\{E(F_p),q,G,P,Ppub,H_1,H_2,H_3\}$ 公开,并保密系统主密钥 s。

(2)部分私钥提取算法:输入用户身份 ID,KGC 随机选取 $r_{ID}\in Z_q^*$,KGC 计算 $K=r_{ID}P$,$h_1=H_1(ID,K)$,$d=r_ID+h_1s$,将 K 作为部分公钥 ppk_{ID},d 作为部分私钥 psk_{ID},用安全信道将(K,d)发送给用户。

(3)用户密钥生成算法:用户收到(K,d)后验证等式 $dP=K+H_1(ID,K)P_{pub}$,如果等式不成立,则重新用身份 ID 向 KGC 申请部分私钥,否则继续计算,用户随机选取 $x\in Z_q^*$ 作为秘密值 x_{ID},计算 $Q=xP$,设置用户公钥 $PK_{ID}=(K,Q)$,计算$h_2=H_2(ID,K,Q)$,$y=(d+h_2x)^{-1}$,设置用户私钥 $SK_{ID}=(x,y)$。

(4)签名算法:输入消息 m,签名者使用系统参数 $params$、身份 ID、公钥 $PK_{ID}=(K,Q)$和私钥 $SK_{ID}=(x,y)$,按如下步骤生成对消息 m 的签名$\sigma=(R,t)$。

1)随机选取 $r\in Z_q^*$,计算 $R=rP$。

2)计算$h_3=H_3(m,ID,R,Q)$。

3)计算 $t=y(r+h_3x)$。

(5)验证算法:输入消息签名对(m,σ),验证者使用系统参数 $params$、签名者身份 ID 和公钥 $PK_{ID}=(K,Q)$,按如下步骤验证签名。

1)计算$h_1=H_1(ID,K)$,$h_2=H_2(ID,K,Q)$。

2)计算$h_3=H_3(m,ID,R,Q)$。

3)验证等式 $t(K+h_1P_{pub}+h_2Q)=R+h_3Q$,如果等式成立,则签名有效并输出 1;否则输出 0。

等式的正确性验证过程如下:

$$t(K+h_1P_{pub}+h_2Q)=t(dP+h_2xP)=y(d+h_2x)(r+h_3x)P=R+h_3Q$$

3.2 安全性证明

引理 1(分叉引理,The Forking Lemma[10]) 设 A 是一个概率多项式时间图灵机,其输入仅包含公共数据。分别用 Q 和 R 表示 A 可以向随机预言机请求的查询数和 A 可以向签名者请求的查询数。假设在时间 T 内,A 以概率 $\varepsilon\geqslant 10(R+1)(R+Q)/2^k$ 产生有效签名(m,h,σ_1,σ_2)。如果三重态(h,σ_1,σ_2)可以在不知道密钥的情况下进行模拟,且分布概率不可区分,则有另一台机器通过模拟签名者与 A 交互来获得对 A 的控制,并在预期时间 $T'\leqslant 120\,686QT/\varepsilon$ 内产生两个有效签名(m,h,σ_1,σ_2)和$(m,h',\sigma_1,\sigma_2')$,这里 $h\neq h'$。

与本文提出的签名算法做类比,分叉引理中提到的有效签名(m,h,σ_1,σ_2),对应着本文提出的签名算法中的(m,h_3,R,t)。

定理 1　在基于 ECDLP 是困难问题假设下的随机预言机模型中，本文的无证书签名方案对第一类强敌手 A_{I} 是存在性不可伪造的。

引理 2　假设存在一个计算限制在概率多项式时间内的敌手 A_{I}，进行最多 q_H 次随机预言机询问，最多 q_S 次签名询问，在多项式时间 T 内以不可忽略的优势 $\varepsilon \geqslant 10(q_S+1)(q_S+q_H)/2^k$ 对该签名进行伪造，那么存在一个算法 B 在时间 $T' \leqslant 120\,686 TqH/\varepsilon$ 内解决 ECDLP 困难问题。

证明：算法 B 的目标是 B 作为挑战者与敌手 A_{I} 进行交互，利用 A_{I} 的能力解决 ECDLP 困难问题。一个 ECDLP 困难问题的实例为：给定 P 和 zP，能够输出 ECDLP 困难问题的一个解 z。假设将目标身份 ID^* 的相关参数设置成困难问题的已知条件参数，设 ID^* 的部分私钥 $d=z$ 是未知的随机数，给定 zP。

B 进行系统初始化，随机选取 $r_{ID^*} \in Z_q^*$，计算 $K^* = r_{ID^*} P$ 作为 ID^* 的部分公钥，并计算 $P_{pub} = H_1(ID^*, K^*)^{-1}(zP - K^*)$ 作为系统公钥，此时 ID^* 的部分私钥和部分公钥满足等式 $zP = K^* + H_1(ID^*, K^*)P_{pub}$，因此 ID^* 的部分私钥和部分公钥是有效的。接下来，将系统参数 $params = \{E(F_p), q, G, P, Ppub, H_1, H_2, H_3\}$ 发送给对手 A_{I}。

(1)创建 ID 列表(Create ID)[11]：B 维护一个由六元组 (ID, K, Q, d, x, h_1) 组成的列表 L_{ID}。在列表 L_{ID} 中查询 ID 时，如果 ID 在 L_{ID} 上，则返回对应的 (ID, K, Q, d, x, h_1)；否则，随机选取 $a, b, c \in Z_q^*$，设置 $d=b, x=c$，计算 $K = aP_{pub} + bP$，$Q = cP$，$h_1 = -a$，将新元组 (ID, K, Q, d, x, h_1) 插入列表 L_{ID}，然后返回 (ID, K, Q, d, x, h_1)。以这种方式生成的密钥满足部分密钥生成算法中的等式 $dP = K + H_1(ID, K)P_{pub}$，因此通过上述方式生成的密钥是有效的密钥。

(2)H_1 询问：B 维护一个由三元组 (ID, K, h_1) 组成的列表 L_{H1}，列表初始为空。当 A_{I} 使用身份 ID 向 B 询问 H_1 时，B 检查 ID 是否存在于列表 L_{H1} 中。如果 ID 已经存储在 L_{H1} 中，则 B 将相应的 h_1 返回给 A_{I}；否则，B 查询列表 L_{ID}，将返回值中的元组 (ID, K, h_1) 插入 L_{H1}，并将相应的 h_1 返回给 A_{I}。

(3)H_2 询问：B 维护一个由四元组 (ID, K, Q, h_2) 组成的列表 L_{H2}，列表初始为空。当 A_{I} 使用身份 ID 向 B 询问 H_2 时，B 检查 ID 是否存在于列表 L_{H2} 中。如果 ID 已经存储在 L_{H2} 中，则 B 将相应的 h_2 返回给 A_{I}；否则，B 随机选择一个 h_2，然后将一个新元组 (ID, K, Q, h_2) 插入列表 L_{H2}。接下来，B 将 h_2 返回给 A_{I}。

(4)H_3 询问：B 维护一个由四元组 (m, ID, R, Q, h_3) 组成的列表 L_{H3}。当 A_{I} 使用 (m, ID, R, Q) 向 B 询问 H_3 时，B 检查 (m, ID, R, Q) 是否存在于列表 L_{H3} 中。如果 (m, ID, R, Q) 已经存储在 L_{H3} 中，则 B 将相应的 h_3 返回给 A_{I}；否则，B 随机选择一个 h_3，然后将一个新元组 (m, ID, R, Q, h_3) 插入列表 L_{H3}。接下来，B 将 h_3 返回给 A_{I}。

(5)部分私钥询问：当 A_{I} 使用身份 ID 向 B 询问部分私钥时，如果 $ID = ID^*$，则终止模拟；否则 B 查找列表 L_{ID}，并将返回值中的 d 返回给 A_{I}。

(6)秘密值询问：当 A_{I} 使用身份 ID 向 B 询问秘密值时，如果 $ID = ID^*$，则终止模拟；否则，B 查找列表 L_{ID}，并将返回值中的 x 返回给 A_{I}。

(7)公钥询问：当 A_{I} 使用身份 ID 向 B 询问公钥时，B 查找列表 L_{ID}，并将返回值中的 (K, Q) 返回给 A_{I}。

(8)公钥替换：B 维护一个由五元组 (ID, K, Q, r_{ID}, x) 组成的列表 L_{PK}，列表初始为空。当 A_{I} 向 B 输入 $(ID, K = r_1 P, Q = r_2 P, r_1, r_2)$ 时，B 验证 $K = r_1 P, Q = r_2 P$，设置 $r_{ID} = r_1, x = r_2$，B 将新元组 (ID, K, Q, r_{ID}, x) 加到列表 L_{PK} 上。

(9)签名询问：当 A_{I} 使用 (m, ID) 向 B 询问签名时，如果 $ID = ID^*$，则终止模拟；否则 B 查询列表 L_{PK}，如果 ID 在列表 L_{PK} 中，则提取对应的 (ID, K, Q, r_{ID}, x)，B 随机选取 $r \in Z_q^*$，计算 $t = rx \cdot (r_{ID} + x h_2)^{-1}$，$R = (t \cdot h_1)P_{pub}$，设置 $h_3 = r$，把 (m, ID, R, Q, h_3) 插入列表 L_{H3}，将签名 (R, t) 返回给 A_{I}。我们可以使用构造的公钥验证生成的签名是有效的签名：

$$\begin{aligned} & t(K + h_1 P_{pub} + h_2 Q) \\ &= rx \cdot (r_{ID} + x h_2)^{-1}(K + h_2 Q) + t(h_1 P_{pub}) \\ &= h_3(xP) + (t \cdot h_1)P_{pub} \\ &= R + h_3 Q \end{aligned}$$

否则，B 查询列表 L_{ID}，按照原方案计算签名。因为列表 L_{ID} 中的密钥有效，所以可以生成有效签名。

根据分叉引理，A_{I} 可以在时间 $T' \leqslant 120\,686 QT/\varepsilon$ 内构造两个有效签名 $(m, h_3, R, t = y(r + h_3 x))$ 和 $(m, h_3', R, t' = y(r + h_3' x))$，这里 $h_3 \neq h_3'$，那么 B 可以通过这两个有效签名计算 $(h_3 x - h_3' x)(t - t')^{-1} - h_2 x = z$，得到一个 ECDLP 困难问题的解 z，因此 B 可以在时间 $T' \leqslant 120\,686\, QT/\varepsilon$ 内解决 ECDLP 困难问题。

在基于 ECDLP 困难问题假设下，根据引理 2，本文的无证书签名方案对第一类强敌手 A_I 是存在性不可伪造的。

定理 2　基于 ECDLP 困难问题假设下的随机预言机模型中，本文的无证书签名方案对第二类敌手 A_{II} 是存在性不可伪造的。

引理 3　假设存在一个概率多项式时间第二类敌手 A_{II}，进行最多 q_H 次随机预言机询问，最多 q_S 次签名询问，在多项式时间 T 内以不可忽略的优势 $\varepsilon \geqslant 10(qS+1)(qS+qH)/2^k$ 对该签名进行伪造，那么存在一个算法 B 在时间 $T' \leqslant 120\,686\, TqH/\varepsilon$ 内解决 ECDLP 困难问题。

证明：算法 B 的目标是 B 作为挑战者与敌手 A_{II} 进行交互，利用 A_{II} 的能力解决 ECDLP 困难问题。一个 ECDLP 困难问题的实例为：给定 P 和 zP，能够输出 ECDLP 困难问题的一个解 z。假设将目标身份 ID^* 的相关参数设置成困难问题的已知条件参数，设 ID^* 的秘密值 $x=z$ 是未知的随机数，给定 $Q_{ID^*} = zP$。

B 进行系统初始化，输入安全参数 k，随机选取 $s \in Z_q^*$ 作为系统主密钥，并计算 $P_{pub} = sP$ 作为系统公钥。接下来，将系统参数 $params = \{E(F_p), q, G, P, P_{pub}, H_1, H_2, H_3\}$ 和系统主密钥 s 发送给对手 A_{II}。

(1)创建 ID 列表(Create ID)[12]：B 维护一个由六元组 (ID, K, Q, d, x, h_1) 组成的列表 L_{ID}。在列表 L_{ID} 中查询 ID 时，如果 ID 在 L_{ID} 上，则返回对应的 (ID, K, Q, d, x, h_1)。否则，如果 $ID = ID^*$，则随机选取 $a, b \in Z_q^*$，计算 $K = aP$，$Q = Q_{ID^*}$，$d = a + h_1 s$，设置 $h_1 = b$，x 设置为空，将新元组 $(ID, K,$

$Q,d,\perp,h_1$)插入列表 L_{ID}，其中“$\perp$”表示空，然后返回(ID, $K,Q,d,\perp,h_1$)；如果 $ID\neq ID^*$，则随机选取 $a,b,c\in Z_q^*$，计算 $K=aP,Q=bP$，$d=a+h_1 s$，设置$h_1=c,x=b$，将新元组(ID,K,Q,d,x,h_1)插入列表 L_{ID}，然后返回(ID,K,Q,d,x,h_1)。上述两种方式生成的密钥满足部分密钥生成算法中的等式$dP=K+H_1(ID,K)P_{pub}$，因此其是有效的密钥。

(2)H_1询问：B 维护一个由三元组(ID,K,h_1)组成的列表 L_{H1}，列表初始为空。当 A_{II}使用身份 ID 向 B 询问 H_1时，B 检查 ID 是否存在于列表 L_{H1}中。如果 ID 已经存储在 L_{H1}中，则 B 将相应的h_1返回给 A_{II}；否则，B 查询列表 L_{ID}，将返回值中的元组 (ID,K,h_1)插入 L_{H1}中，并将相应的h_1返回给 A_{II}。

(3)H_2询问：B 维护一个由四元组(ID,K,Q,h_2)组成的列表 L_{H2}，列表初始为空。当 A_{I}使用身份 ID 向 B 询问 H_2时，B 检查 ID 是否存在于列表 L_{H2}中。如果 ID 已经存储在 L_{H2}中，则 B 将相应的h_2返回给 A_{I}，否则，B 随机选择一个h_2，然后将一个新元组(ID,K,Q,h_2)插入列表 L_{H2}。接下来，B 将h_2返回给 A_{I}。

(4)H_3询问：B 维护一个由四元组(m,ID,R,Q,h_3)组成的列表 L_{H3}。当 A_{I}使用(m,ID,R,Q)向 B 询问 H_3时，B 检查(m,ID,R,Q)是否存在于列表 L_{H3}中。如果(m,ID,R,Q)已经存储在 L_{H3}中，则 B 将相应的h_3返回给 A_{I}；否则，B 随机选择一个h_3，然后将一个新元组(m,ID,R,Q,h_3)插入列表 L_{H3}。接下来，B 将h_3返回给 A_{I}。

(5)部分私钥询问：当 A_{II}使用身份 ID 向 B 询问部分私钥时，B 查找列表 L_{ID}，将返回值中的 d 返回给 A_{II}。

(6)秘密值询问：当 A_{II}使用身份 ID 向 B 询问秘密值时，如果 $ID=ID^*$，则终止模拟；否则 B 查找列表 L_{ID}，并将返回值中的 x 返回给 A_{II}。

(7)公钥询问：当 A_{II}使用身份 ID 向 B 询问公钥时，B 查找列表 L_{ID}，并将返回值中的(K,Q)返回给 A_{II}。

(8)签名询问：当 A_{II}使用(m,ID)向 B 询问签名时，如果 $ID=ID^*$，则终止模拟；否则，B 查询列表 L_{ID}，根据返回值按照原方案计算签名。因为列表 L_{ID}中的密钥有效，所以可以生成有效签名。

根据分叉引理，A_{II}可以在时间 $T'\leqslant 120\,686QT/\varepsilon$ 内构造两个有效签名($m,h_3^{(1)},R,t^{(1)}=y(r+h_3^{(1)}z)$)和($m,h_3^{(2)},R,t^{(2)}=y(r+h_3^{(2)}z)$)，这里$h_3^{(1)}\neq h_3^{(2)}$，那么根据签名方案 B 得到一个方程组：

$$t^{(i)}(d+h_2 z)=(r+h_3^{(i)}z),i=1,2 \tag{2}$$

在方程组(2)中，r,z 对 B 是未知的变量，那么 B 可以通过解这个方程组得到z，然后输出 z 作为 ECDLP 困难问题的一个实例解答。因此，B 可以在时间 $T'\leqslant 120\,686QT/\varepsilon$ 内解决 ECDLP 困难问题。

在基于 ECDLP 困难问题假设下，根据引理 3，本文的无证书签名方案对第二类敌手 A_{II}是存在性不可伪造的。

4 签名方案的性能分析及效率比较

将本文方案与 2016 年以来提出的 4 种基于椭圆曲线的无证书签名方案进行性能分析与效率比较，因为其中 Hassouna 等[12]的方案和 Zhang 等[13]的方案使用了双线性对，所以在进行效率比较时，在同一运行环境(CPU 为 Intel Core i7-5500U@ 2.4 GHz，内存为 4 GB(DDR3 1 600 MHz)，及操作系统为 64 位 Windows 10)下，在 Microsoft Visual Studio 2010 开发平台上，统一使用斯坦福 BONEH 等开发的 PBC 库并采用 C 语言来实现所有签名方案，对签名方案中包含的双线性对统一用 PBC 中运算最快的 A 型双线性对来实现。

4.1 性能分析

表 1 列出了本文提出的无证书签名方案与 2016 年以来提出的其他 4 种无证书签名方案分别在签名阶段和验证阶段的性能比较结果，其中 B 表示一次双线性对运算，C 表示一次椭圆曲线点乘运算，D 表示一次椭圆曲线点加运算，E 表示一次模幂运算，M 表示一次模乘运算，A 表示一次模加运算，I 表示一次模逆运算，H 表示使用一次 Hash 函数。

表 1 各方案的性能比较

Table 1 Performance comparison of different schemes

方案	签名阶段	验证阶段
Hassouna 等[12]的方案	B+C+E+M+H	4B+H
Zhang 等[13]的方案	C+M+2A+I+H	B+3C+3D+2H
Karati 等[15]的方案	C+2M+2A+I+H	3C+3D+2H
Jia 等[16]的方案	C+3M+2A+I+2H	4C+2D+2H
本文方案	C+2M+A+H	4C+3D+3H

从表 1 可以看出，本文方案在签名阶段的性能较其他 4 种方案具有一定优势，验证阶段较 Hassouna 等[12]的方案和 Zhang 等[13]的方案具有一定优势，与 Karati 等[15]的方案和 Jia 等[16]的方案性能相近。

4.2 效率比较

统一使用随机生成的只含有英文字母和数字的 60 个字符(对应大小为 480 bit)作为待签名的消息 m，分别测量这 5 种签名方案运行 60 次的签名平均耗时、验证平均耗时以及从系统参数设置算法到验证算法结束的方案平均总耗时，各平均耗时如表 2 和图 2 所示。由表 2 可知，本文方案的签名平均总耗时约为 0.095s，其中签名阶段平均耗时约为 0.015 s，验证阶段约为 0.019 s。与 Hassouna 等[12]的方案相比，本文方案的签名平均耗时和验证平均耗时分别减少了约 63.4% 和 55.8%，平均总耗时减少了约 51.0%。与 Zhang 等[13]和 Karati 等[15]的方案相比，本文方案的签名平均耗时和验证平均耗时相近，平均总耗时分别减少了约 10.4% 和 22.1%。与 Jia 等[16]的方案相比，本文方案的签名平均耗时、验证平均耗时与平均总耗时相近。由此可见，本文方案平均总耗时较短，运行效率更高。

表 2 各方案运行 60 次的平均耗时比较

Table 2 Average time-consuming comparison of all schemes running 60 times

(单位：s)

方案	签名平均耗时	验证平均耗时	方案平均总耗时
Hassouna 等[12]的方案	0.041	0.043	0.194
Zhang 等[13]的方案	0.016	0.020	0.106
Karati 等[15]的方案	0.016	0.017	0.122
Jia 等[16]的方案	0.017	0.018	0.097
本文方案	0.015	0.019	0.095

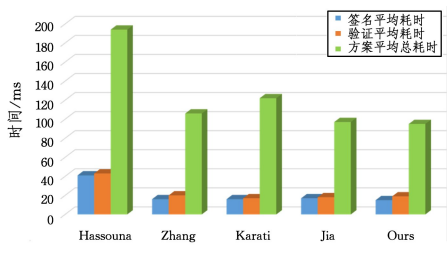

图 2　本文方案和其他方案运行 60 次的平均计算开销

Fig. 2　Average computation cost of proposed scheme and other schemes running 60 times

4.3　仿真过程的核心代码

基于斯坦福 BONEH 等开发的 PBC 库，实现本文签名方案的 C 语言核心代码如下：

```
//签名
element_init_Zr(r,pairing);//初始化 r 为Z_q^* 中的变量
element_init_G1(R,pairing);//初始化 R 为 G 中的变量
(下面出现的Z_q^* 和 G 中的变量在使用前都要在 PBC 库中初始化，这里不再赘述)
element_random(r);//随机选取 r
element_mul_zn(R,P,r);//计算 R=rP
element_to_bytes(R_bit,R);//将 R 转化为字符串，下同
element_to_bytes(Q_bit,Q);//字符串转化
strcat(m_ID_R_Q,ID);//将消息 m 与 ID 拼接，下同
strcat(m_ID_R_Q,(const char*)R_bit);//拼接
strcat(m_ID_R_Q,(const char*)Q _bit);//拼接
element_from_hash(h3,m_ID_R_Q,strlen(m_ID_R_Q));//计算h3
element_mul(t,h3,x);//计算h3 x
element_add(t,t,r);//计算 r+h3 x
element_mul(t,t,y);//计算 t=y(r+h3 x)
//验证签名
element_set(R_v,R);
element_set(t_v,t);//验证者收到签名(R,t)
element_to_bytes(K_bit_v,K);//字符串转化
strcat(ID_K_v,(const char*)K_bit_v);//拼接
element_from_hash(h1_v,ID_K_v,strlen(ID_K_v));//计算h1
element_to_bytes(Q_bit_v,Q);//字符串转化
strcat(ID_K_Q_v,(const char*)K_bit_v);//拼接
strcat(ID_K_Q_v,(const char*)Q_bit_v);//拼接
element_from_hash(h2_v,ID_K_Q_v,strlen(ID_K_Q_v));//计算h2
element_mul_zn(P_left,Ppub,h1_v);计算h1 Ppub
element_add(P_left,P_left,K);//计算 K+h1 Ppub
element_mul_zn(P_temp,Q,h2_v);//计算h2 Q
element_add(P_left,P_left,P_temp);
//计算 K+h1 Ppub+h2 Q
element_mul_zn(P_left,P_left,t_v);
//计算 t(K+h1 Ppub+h2 Q)
element_to_bytes(R_bit_v,R_v);//字符串转化
strcat(m_ID_R_Q_v,ID_v);//拼接
strcat(m_ID_R_Q_v,(const char*)R_bit_v);//拼接
strcat(m_ID_R_Q_v,(const char*)Q_bit_v);//拼接
element_from_hash(h3_v,m_ID_R_Q_v,strlen(m_ID_R_Q_v));
//计算h3
element_mul_zn(P_rignt,Q,h3_v);//计算h3 Q
element_add(P_rignt,R_v,P_rignt);//计算 R+h3 Q
boolisVerify=! element_cmp(P_left,P_rignt);//验证等式 t(K+h1 Ppub+h2 Q)=R+h3 Q，如果成立则布尔变量为 1，否则为 0。
```

5　配电网 Modbus TCP 报文认证过程中的应用

5.1　认证协议

本文提出一种基于上述无证书签名方案的配电网 Modbus TCP 报文认证协议，过程如下。

(1)密钥注册：新加入的电子设备向密钥生成中心提交分配给设备的身份标识 ID，申请部分私钥，并根据自己的秘密值和部分密钥设置自己的私钥和公钥，再以安全方式将私钥输入电子设备。

(2)发送端签名：电子设备发送端采用上述无证书签名算法对配电网 Modbus TCP 报文的应用层数据进行数字签名，主要步骤如下。

1)压缩数据：将发送端身份 ID_1 和时间戳 T_1 加入原始数据 $data$ 后端，得到的中间数据为 $data \| ID_1 \| T_1$。发送端对中间数据使用安全 Hash 算法即 SHA-256 算法得到中间数据的信息摘要 $hash(data \| ID_1 \| T_1)$。

2)生成签名：发送端采用本文的无证书签名方案签名算法进行签名，得到发送端对中间数据信息摘要的签名(R_1, t_1)。

3)组合报文：将签名(R_1, t_1)添加到中间数据后端，得到的最终数据为 $data \| ID_1 \| T_1 \| R_1 \| t_1$，将其与报文的其他部分组合成完整配电网 TCP 报文，并发送给接收端。

(3)接收端验证：电子设备接收端对接收的 TCP 报文进行验证，验证发送端身份以及接收数据的完整性和及时性。设接收 TCP 报文的应用层数据为 $data' \| ID_1' \| T_1' \| R_1' \| t_1'$。

1)验证时间戳 T_1'：根据 T_1'是否在给定时间范围内来判断 T_1'是否新鲜。如果 T_1'不在时间范围内，则该报文无效，终止验证；否则进行下一步验证。

2)验证签名：输入身份标识 ID_1'、发送端公钥、系统公钥、数据 $data' \| ID_1' \| T_1'$和签名(R_1', t_1')，用本文的无证书签名方案验证算法对签名(R_1', t_1')进行验证。如果验证成功，则报文为有效报文；如果验证失败，则报文为无效报文。

(4)接收端回应：从接收的数据中提取 $data' \| ID_1' \| T_1'$，将接收端身份 ID_2 和时间戳 T_2 加入后端组成回应数据，并对其使用安全 Hash 算法即 SHA-256 算法得到其信息摘要 $hash(data' \| ID_1' \| T_1' \| ID_2 \| T_2)$，然后采用本文中的无证书签名方案签名算法进行签名，将得到的签名(R_2, t_2)添加在回应数据后端，将其与报文其他部分组合成完整配电网报文，并发送给发送端。

(5)发送端验证：发送端对收到的接收端回应的报文进行验证，依次验证时间戳 T_2 的新鲜性和签名(R_2, t_2)的有效性，确保接收端及时收到报文，并且确认接收端接收的报文的完整性。

5.2　安全性分析

5.2.1　抗重放攻击

时间戳不仅出现在传送的报文中，还需要出现在认证的

中间数据 $data \| ID \| T$ 中。因此，如果攻击者让接收端对先前发送端发送过的报文进行身份认证，则该报文无法通过接收端的验证，此通信协议可以抵抗重放攻击。

5.2.2 抗伪装攻击

攻击者如果想伪装成发送端 A 进行通信，那么需要有能力生成发送端 A 发出的有效报文，即必须有能力伪造出发送端 A 对中间数据的有效签名。通过对本文签名方案的安全性分析可知，只有用户 A 能够生成 A 对中间数据的有效签名，其他不知道 A 完整私钥的用户不能生成 A 对中间数据的有效签名，因此此通信协议可以抵抗伪装攻击。

5.2.3 抗中间人攻击

根据 5.2.2 节的分析，不知道发送端 A 完整私钥的攻击者无法伪装成 A 进行通信，攻击者无法伪造出 A 的有效认证信息，因此此通信协议可以抵抗中间人攻击。

结束语 为了解决配电网通信使用传统公钥密码体制和基于身份密码体制时存在的问题，结合配电网终端的计算和存储能力，本文提出了一种基于椭圆曲线的无双线性对的无证书签名方案，在随机预言机模型以及 ECDLP 困难问题假设下，证明了该方案的安全性；C 语言实现的结果表明了该方案总体运行效率较高；最后将该签名方案应用到配电网 Modbus TCP 报文认证中并分析了其安全性。本文提出的认证协议适用于配电网报文内容安全级别不高的情况，在本文无证书签名方案的密码体制下，下一步将研究可以对报文内容进行加密和解密的方案。

参 考 文 献

[1] PIATKOWSKA E, BAJRAKTARI A, CHHAJED D, et al. Tool support for data protection impact assessment in the smart grid [J]. Elektrotechnik und Information stechnik, 2017, 134(1): 26-29.

[2] DENG W, WEN K, ZHANG H, et al. Design and analysis of data encryption and authentication scheme for distribution grid [J]. Computer Engineering & Software, 2017, 38(6): 17-23.

[3] AL-RIYAMI S, PATERSON K G. Certificateless public key cryptography[C]// Advances in Cryptology—ASIACRYPT'03. Berlin: Springer-Verlag, 2003.

[4] ZOU X F, XIAO Y X. Modbus telegram security of distribution network based on SM2[J]. Power System Protection and Control, 2018, 46(12): 151-157.

[5] QIU F, CHEN LL, LIN N, et al. Security analysis and improvement of Modbus message in distribution network based on SM9 [J]. China Power, 2019, 52 (10): 18-25.

[6] ZHANG Z H, ZHOU J, DING K, et al. The Applications of Asymmetric Encryption of Digital Signature Technology in Distribution Automation System [J]. Electrical Automation, 2012(3): 43-45.

[7] ENGE A. Elliptic Curves and Their Applications to Cryptography-An Introduction[M]. Kluwer Academic Publishers, 1999: 39-40.

[8] WU T, JING X J. Cryptanalysis and Improvement of a Certificateless Signature Scheme with Strong Unforgeability[J]. Acta Electronica Sinica, 2018, 46(3): 602-606.

[9] HUANG X, Mu Y, SUSILO W, et al. Certificateless Signature Revisited[C]// Australasian Conference on Information Security & Privacy. Washington D. C., USA: IEEE Press, 2007: 308-322.

[10] POINTCHEVAL D, STERN J. Security Arguments for Digital Signatures and Blind Signatures [J]. Journal of Cryptology, 2000, 13(3): 361-396.

[11] HE D B, CHEN J H, ZHANG R. An efficient and provably-secure certificateless signature scheme without bilinear pairings [J]. International Journal of Communication Systems, 2011, 25(11): 1432-1442.

[12] HASSOUNA M, BASHIER E, BARRY B. A Strongly Secure Certificateless Digital Signature Scheme in The Random Oracle Model [J]. International Journal of Network Security, 2016, 18(5): 938-945.

[13] ZHANG Y, DENG R, ZHENG D, et al. Efficient and Robust Certificateless Signature for Data Crowdsensing in Cloud-assisted Industrial IoT[J]. IEEE Transactions on Industrial Informatics, 2019, 15(9): 5099-5108.

[14] KRISHNAMOORTHY M, PERUMAL V. Secure and efficient hand-over authentication in WLAN using elliptic curve RSA [J]. Computers & Electrical Engineering, 2017, 64: 552-566.

[15] KARATI A, ISLAM S H, BISWAS G P. A Pairing-free and Provably Secure Certificateless Signature Scheme[J]. Information Sciences, 2018, 450: 378-391.

[16] JIA X Y, HE D B, LIU Q, et al. An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment[J]. Ad Hoc Networks, 2018, 71(15): 78-87.

LIU Shuai, born in 1995, postgraduate. His main research interests include elliptic curve cryptography and information security.

CHEN Jian-hua, born in 1964, Ph. D, professor, Ph. D supervisor. His main research interests include cryptography and information security.