性, R4: 不可追踪性, R5: 前向保密, R6: 已知会话密钥攻击的抵抗性, R7: 中间人攻击的抵抗性, R8: 抗重放攻击, R9: 抗公钥替换攻击, R10: 解决密钥托管问题, R11: 不建立安全信道. 不同方法的安全属性比较如表 1.

(2) 计算代价比较

选择一个带生成器p的群$\mathbb{G}$, 其中是一个 160 位素数q, p是从超奇异椭圆曲线$E(F_p)$: $y^2 = x^3 + ax + b \bmod p$中选取的一个点 ($p$是一个 512 位素数).

本文使用 MIRACL Crypto SDK 测试了上述操作, 并在 2.53 GHz、i7 CPU 和 4 GB 内存的 64 位 Windows 10 操作系统上运行实验. 表 2 列出了这些操作的平均运行时间. 对于计算成本分析, 表 2 给出了一些基本操作的执行时间. 表 3 给出了文献 [9–12] 和本文提出的方案计算代价比较.

表 1 安全属性比较

属性	文献[9]	文献[10]	文献[11]	文献[12]	本文方案
R1	√	√	√	√	√
R2	√	√	√	√	√
R3	×	×	×	×	√
R4	×	×	×	×	√
R5	√	√	√	√	√
R6	√	√	√	√	√
R7	×	×	×	√	√
R8	×	×	×	×	√
R9	×	×	×	√	√
R10	√	√	√	√	√
R11	√	√	√	√	√

表 2 基本操作的执行时间

符号	表述	执行时间(ms)
T_M	$\mathbb{G}$模乘操作	1.4202
T_P	双线性对操作	10.3092

表 3 该方案与其他方案用户计算代价比较

方案	用户计算代价 (ms)
文献[9]	$T_M + 2T_p \approx 13.1496$
文献[10]	$T_M + 2T_p \approx 13.1496$
文献[11]	$7T_M \approx 9.9414$
文献[12]	$8T_M + T_p \approx 21.6708$
本文方案	$4T_M \approx 5.6808$

对于认证密钥协商过程中的计算代价, 文献 [9] 需要运行 1 个模乘运算和 2 个双线性对运算, 所以总的运行时间为 13.1496 ms. 文献 [10] 需要运行 1 个模乘运算和 2 个双线性对运算, 总的运行时间为 13.1496 ms. 文献 [11] 需要运行 7 个模乘运算, 总的运行时间为 9.9414 ms. 文献 [12] 需要运行 8 个模乘运算和 1 个双线性对运算, 所以总的运行时间为 21.6708 ms. 本文提出的方案需要运行 4 个模乘运算, 总的运行时间为 5.6808 ms.

图 5 清楚的展示出计算代价的比较结果, 从图中直观得到本文方案计算代价明显优于其他方案.

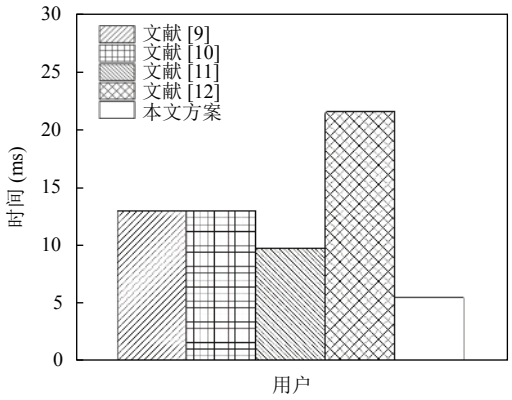

图 5 用户计算代价比较

4 总结

为了克服注册时密钥托管, 安全信道建立代价高等问题, 几个基于证书认证密钥协商方案已经被提出. 但是, 这些方案大多采用昂贵的双线性对运算, 在计算和通信开销方面性能不理想. 本文提出了一个采用椭圆曲线的基于证书的认证密钥协商协议. 安全性分析表明, 该协议在随机预言机模型下是安全的, 能够满足基于证书的认证密钥协商协议下的安全需求. 性能分析结果表明, 该协议具有较低的计算代价. 本文提出的协议对各种类型的攻击具有强大的弹性, 这也使它适合广泛的应用程序使用, 以在不同级别上维护安全性. 在本文的基础上, 可进一步研究用户、雾节点、云服务器三方认证密钥协商方案.

参考文献

1 Mumtaz S, Huq KMS, Rodriguez J. Direct mobile-to-mobile communication: Paradigm for 5G. IEEE Wireless Communications, 2014, 21(5): 14–23. [doi: 10.1109/MWC.2014.6940429]

2 周晓斌, 许勇, 张凌. 一种开放式 PKI 身份认证模型的研究. 国防科技大学学报, 2013, 35(1): 169–174. [doi: 10.3969/j.issn.1001-2486.2013.01.030]

3 Shamir A. Identity-based cryptosystems and signature schemes. Blakley GR, Chaum D. Advances in Cryptology. Berlin, Heidelberg: Springer, 1985. 47–53.
4 Al-Riyami SS, Paterson KG. Certificateless public key cryptography. Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security. Taipei, China. 2003. 452–473.
5 Xie Y, Wu LB, Shen J, *et al*. Efficient two-party certificateless authenticated key agreement protocol under GDH assumption. International Journal of Ad Hoc and Ubiquitous Computing, 2019, 30(1): 11–25. [doi: 10.1504/IJAHUC.2019.097093]
6 Shi YJ, Li JH. Two-party authenticated key agreement in certificateless public key cryptography. Wuhan University Journal of Natural Sciences, 2007, 12(1): 71–74. [doi: 10.1007/s11859-006-0194-y]
7 Zhang L, Zhang FT, Wu QH, *et al*. Simulatable certificateless two-party authenticated key agreement protocol. Information Sciences, 2010, 180(6): 1020–1030. [doi: 10.1016/j.ins.2009.11.036]
8 Gentry C. Certificate-based encryption and the certificate revocation problem. Biham E. Advances in Cryptology—Eurocrypt 2003. Berlin, Heidelberg: Springer, 2003. 272–293.
9 Wang SB, Cao ZF. Escrow-free certificate-based authenticated key agreement protocol from pairings. Wuhan University Journal of Natural Sciences, 2007, 12(1): 63–66. [doi: 10.1007/s11859-006-0189-8]
10 Luo M, Wen YY, Zhao H. A certificate-based authenticated key agreement protocol for SIP-based VoIP networks. Proceedings of 2008 IFIP International Conference on Network and Parallel Computing. Shanghai, China. 2008. 3–10.
11 Lu Y, Zhang QL, Li JG, *et al*. An efficient certificate-based authenticated key agreement protocol without bilinear pairing. Journal of Information Technology and Control, 2017, 46(3): 345–359.
12 Lu Y, Zhang QL, Li JG. A certificate-based AKA protocol secure against public key replacement attacks. The International Arab Journal of Information Technology, 2019, 16(4): 754–765.
13 Ma MM, He DB, Wang HQ, *et al*. An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks. IEEE Internet of Things Journal, 2019, 6(5): 8065–8075. [doi: 10.1109/JIOT.2019.2902840]
14 Liu XX, Ma WP, Cao H. NPMA: A novel privacy-preserving mutual authentication in TMIS for mobile edge-cloud architecture. Journal of Medical Systems, 2019, 43(10): 318. [doi: 10.1007/s10916-019-1444-9]
15 Mahmood K, Chaudhry SA, Naqvi H, *et al*. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Future Generation Computer Systems, 2018, 81: 557–565. [doi: 10.1016/j.future.2017.05.002]
16 Xue KP, Hong PL, Ma CS. A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. Journal of Computer and System Sciences, 2014, 80(1): 195–206. [doi: 10.1016/j.jcss.2013.07.004]
17 Wu F, Xu LL, Li X, *et al*. A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography. IEEE Systems Journal, 2019, 13(3): 2830–2838. [doi: 10.1109/JSYST.2018.2876226]
18 Miller VS. Use of elliptic curves in cryptography. In: Williams HC, ed. Advances in Cryptology—CRYPTO '85. Berlin, Heidelberg: Springer, 1986. 417–426.