计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2020,29(9):260−265 [doi: 10.15888/j.cnki.csa.007603]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

面向智能产线的 R-ECC 身份认证方法①

杨东升[1,2], 高珊珊[1,2], 尹震宇[1,2], 李明时[1,2], 柴安颖[1,2], 廉梦佳[1,2]

[1](中国科学院大学, 北京 100049)
[2](中国科学院 沈阳计算技术研究所, 沈阳 110168)
通讯作者: 尹震宇, E-mail: 1169747070@qq.com

摘　要: 在智能制造与“工业 4.0”环境下, 智能产线作为智能制造的重要载体, 在其智能运维、状态监控与数据采集方面具有较高研究意义. 本文针对工业物联网智能产线中, 基于 Android 的智能产线移动终端与 OPC UA 服务器通信过程中存在的通信资源受限、数据传输安全性要求高等问题, 在现有 OPC UA 通信模型的基础上, 设计了一种面向智能产线移动终端的身份认证方法 R-ECC (Random-Elliptic Curve Cryptography). 该方法在认证过程中引入了随机数和椭圆密码体制, 在提高 OPC UA 身份认证安全性的同时, 降低了通信资源的消耗量. 实验结果表明, 面向智能产线的 R-ECC 身份认证方法可以有效提高身份认证过程的安全性, 在降低智能产线移动端硬件资源消耗量的同时加快了身份认证速度.

关键词: 智能产线; OPC UA; 身份认证; Android; 椭圆曲线密码学

引用格式: 杨东升,高珊珊,尹震宇,李明时,柴安颖,廉梦佳.面向智能产线的 R-ECC 身份认证方法.计算机系统应用,2020,29(9):260–265. http://www.c-s-a.org.cn/1003-3254/7603.html

R-ECC Identity Authentication Method for Intelligent Manufacturing Line

YANG Dong-Sheng[1,2], GAO Shan-Shan[1,2], YIN Zhen-Yu[1,2], LI Ming-Shi[1,2], CHAI An-Ying[1,2], LIAN Meng-Jia[1,2]

[1](University of Chinese Academy of Sciences, Beijing 100049, China)
[2](Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168, China)

Abstract: In the environment of intelligent manufacturing and “Industry 4.0”, the intelligent manufacturing line as an important carrier of intelligent manufacturing has high research significance in its algorithmic IT operations, condition monitoring, and data acquisition. This article designs an identity authentication method called R-ECC (Random-Elliptic Curve Cryptography) for the mobile terminal of intelligent manufacturing line, which is based on the security model provided by OPC UA. The method addresses the problems of limited communication resources and high security requirement of data transmission in the process of communication between an Android-based mobile terminal and OPC UA server. This method introduces random numbers and elliptic curve cryptography in the authentication process, which improves the security of OPC UA identity authentication and reduces the consumption of communication resources in the same time. The experimental results show that the R-ECC identity authentication method for the mobile terminal of intelligent manufacturing line can effectively improve the security of the authentication process, reduce the hardware resource consumption of the mobile terminal, and accelerate the speed of identity authentication.

Key words: intelligent manufacturing line; OPC UA; identity authentication; Android; elliptic curve cryptography

① 基金项目: 国家重点研发计划 (2017YFE0125300); 辽宁省“兴辽英才计划”(XLYC1802112)
Foundation item: National Key Research and Development Program of China (2017YFE0125300); Talent Program of Revitalizing Liaoning, Liaoning Province, China (XLYC1802112)
收稿时间: 2020-02-18; 修改时间: 2020-03-17; 采用时间: 2020-03-27; csa 在线出版时间: 2020-09-04

随着“工业 4.0”及“中国制造 2025”的推进, 智能制造成为当下工业的发展趋势, 而工业物联网智能化生产线作为智能制造的重要一环, 更是如今的研究热点. 5G 通讯时代的到来, 为工业控制由现场转为远程提供了更好的通信基础, 平板电脑、手机等的高速发展也为工业物联网的许多控制软件在移动端的部署上奠定了基础. 在工业物联网智能生产线的课题研究中, 为实现产线状态的实时可视化与远程操作的便携性, 将智能产线的客户端部署到移动端上. 针对产线的数据采集以及数据集成问题, 本课题采用 OPC UA 架构, 具体的课题环境如图 1 所示. OPC UA 作为由 OPC 基金会提出的最新一代数据集成标准, 在工业物联网中发挥着越来越大的价值. 在国内, 近几年随着工业物联网的不断推进, 关于 OPC UA 的研究也越来越多. 文献 [1] 设计实现了 OPC UA 客户端的搭建, 通过客户端与 OPC UA 服务器进行通信, 实现了 OPC UA 规范中的数据读、写、订阅等服务. 文献 [2] 针对目前制造企业信息系统与物理系统严重分离所产生的信息孤岛问题, 搭建了一套基于 OPC UA 的质量数据监测系统, 完成了 OPC UA 客户端和服务器的设计与开发. 而这些应用软件都是面向资源限制较少的 PC 端进行实现的[1,2].

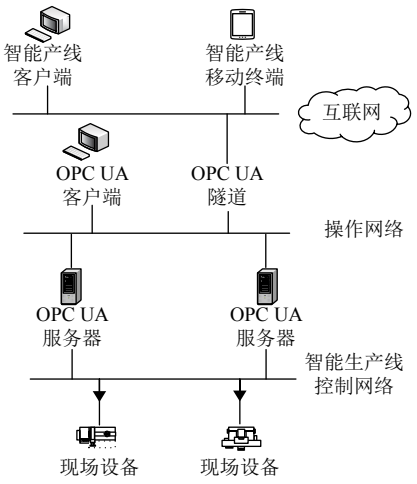

图 1 智能产线系统架构

基于 OPC UA 架构在移动端上设计实现智能产线客户端的过程中, 为保证智能产线的安全性, 必须要保证其通信过程的安全性, 确保其用户的身份可信. 目前也有一些文献对 OPC UA 架构的安全性做了一定的研究. 文献 [3] 阐述了 OPC UA 的安全模型, 针对 OPC UA 应用程序处于不同环境的情况, 在现有安全模型的基础上加入安全策略管理模块, 并在此基础上设计了安全模型中的信息模型. 文献 [4] 分析了在 OPC UA 通信过程中采用不同的编码方式和安全策略对通信实时性的影响, 并对应用程序的应用环境进行安全评估. 然而现有的这些研究, OPC UA 安全架构的实现都运行在资源限制相对较少的“大型”设备上及有线网络中, 在资源受限及安全性要求更高的移动端上的研究较少. 而对于移动端来说, 其处于无线通信网络中, 具有开放性和不稳定性, 更易遭受攻击. 为了保证智能产线安全性, 若继续使用开发 PC 端应用时所使用的身份认证方法, 就要增大密钥的长度, 而这样势必增大了传输过程中带宽的压力[5,6]. 故本文针对移动端的特点, 基于 OPC UA 安全架构, 结合椭圆曲线密码体制以及随机数, 提出了一种面向智能产线移动终端的身份认证方法 R-ECC (Random-Elliptic Curve Cryptography). R-ECC 身份认证方法在实现智能产线移动终端与 OPC UA 服务器的安全通信基础上, 更符合移动端节点轻量级、低功耗的要求.

1 OPC UA 安全模型

OPC UA 架构为保证会话的安全性和可靠性, 定义了一个分层的安全架构. 最上层是应用层, 用来以会话的方式在客户端与服务器之间传递信息. 会话服务中提供了用户认证和授权, 也可以用于对某个产品进行认证和授权; 而 OPC UA 的会话机制需要运行在安全通道上, 通道的安全由通信层来保证, 主要通过数字证书签名和加密传输信息的方式来进行客户端与服务器端的双向认证; 底层的传输层利用 socket 来进行大量信息传输[3,4]. 该安全架构如图 2 所示.

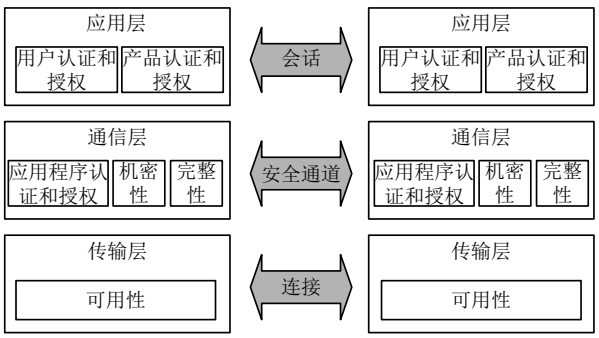

图 2 OPC UA 安全架构

OPC UA 在建立安全通道时, 为保证通信层的安全, 其安全模型是基于公钥基础设施 (PKI) 进行数字证

书的管理, 数字证书中记录了客户端和服务器的公钥信息、签名信息等, 通过权威的第三方机构, 即认证中心进行签发[7]. 而在 OPC UA 中利用数字证书进行加密通信目前普遍是利用了 RSA 公钥密码体制, 在安全通道的创建过程中, 利用 RSA 算法的公钥和私钥进行加密和解密从而实现客户端和服务器端的双向身份认证, 并在身份认证通过即安全通道建立之后派生对称密钥来代替更消耗 CPU 非对称密钥, 用于加密和签名后续信息. 应用层的会话必须建立在通信层安全建立的基础上, 以此来保证所传输的用户口令信息的安全性. 安全通道的创建如图 3 所示.

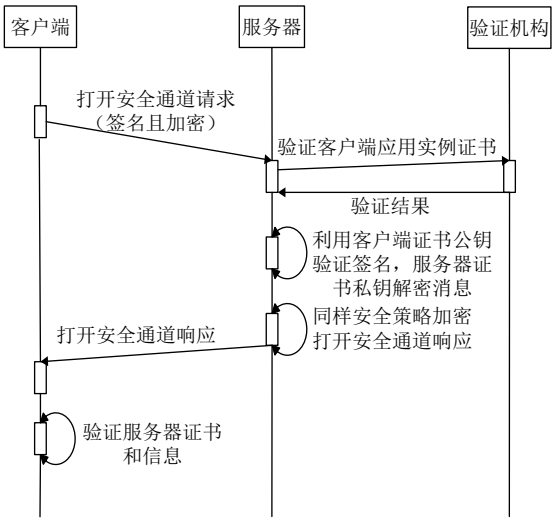

图 3 OPC UA 安全通道创建过程

2 面向智能产线移动终端的 R-ECC 身份认证方法

本文所提出的面向智能产线移动终端的 R-ECC 身份认证方法, 是在符合 OPC UA 安全架构的基础上, 基于椭圆曲线密码体制进行密钥协商创建安全通道, 并在安全通道的基础上创建会话, 实现一次一密, 保证客户端和服务器的安全通信. 面向智能产线移动终端的 R-ECC 身份认证方法的逻辑图见图 4.

智能产线移动终端与 OPC UA 服务器建立连接过程如下:

先做出一系列假设: E 为系统选定的椭圆曲线, G 为基点, n 为椭圆曲线的阶; h 为具有单向性和可碰撞性的哈希函数, f 是椭圆曲线上的点到定长二进制的映射函数; 移动端标识ID_c, 私钥d_c, 公钥$Q_c = d_cG$; OPC UA 服务器端标识ID_s, 私钥d_s, 公钥$Q_s = d_sG$. 移动端和服务器都拥有由认证中心颁发的证书, 但都还没有获得对方的证书. 移动端输入的用户凭证设为用户名 *id*, 密码 *pwd*. R-ECC 身份认证方法的认证过程见图 5.

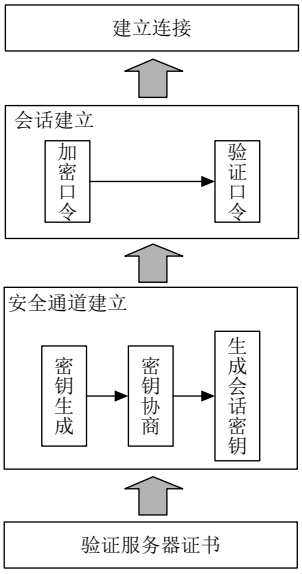

图 4 面向智能产线移动终端的 R-ECC 身份认证方法

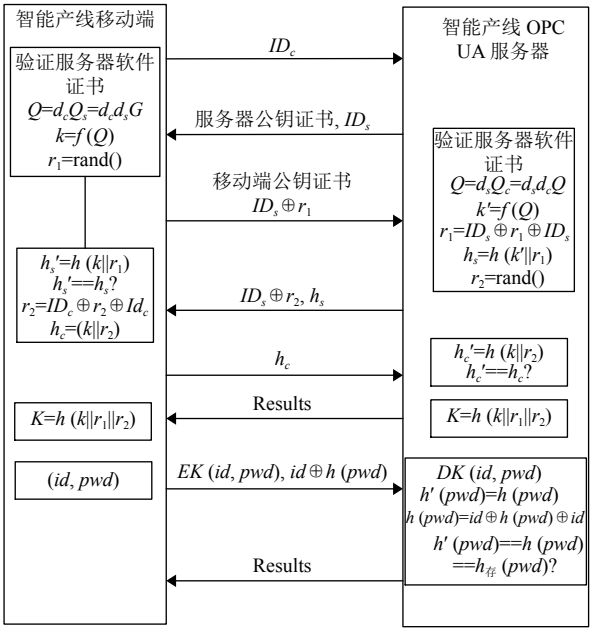

图 5 R-ECC 身份认证方法的执行过程

(1) 验证 OPC UA 服务器应用实例证书. 移动端将其客户端标识ID_c发送给 OPC UA 服务器, 获得服务器的响应, 该响应中包含了服务器标识ID_s以及公钥证书, 移动端验证该证书, 包括检查证书是否在有效期、验

证 CA 签名等.

(2) 密钥生成. 若服务器证书值得信赖, 移动端使用其私钥d_c, 并从服务器证书中提取服务器公钥Q_s, 计算得到$Q=d_cQ_s=d_cd_sG$, $k=f(Q)$. 移动端生成随机数r_1, 并将$ID_s\oplus r_1$, 移动端应用实例证书发送给服务器; 服务器收到移动端的消息, 首先验证移动端的证书, 若证书可信则通过$ID_s\oplus r_1\oplus ID_s$得到$r_1$的值, 利用服务器端私钥$d_s$, 移动端公钥$Q_c$, 计算$Q=d_sQ_c=d_sd_cG$, $k=f(Q)$. 服务器选择随机数r_2, 计算$h_s=h(k\|r_1)$, 并且把$ID_c\oplus r_2, h_s$发送给移动端.

(3) 密钥协商. 移动端收到服务器的消息, 计算$h(k\|r_1)$的值, 将其与h_s进行比较, 若相等, 则验证通过, 反之不通过. 验证通过后, 移动端计算$h_c=h(k\|r_2)$, 并将h_c发送给服务器; 服务器收到移动端的消息后, 计算$h(k\|r_2)$的值, 并将其与h_c比较, 然后将比较的结果发回给移动端.

(4) 生成会话密钥. 若 (3) 中的比较结果相同, 则移动端和服务器均计算$K=h(k\|r_1\|r_2)$, 作为其以后传输大量信息所使用的的会话密钥.

(5) 加密口令. 用户与移动端进行交互, 从登陆页面输入用户名和密码, 移动端将输入的信息以$EK(id,pwd)$(EK 表示通过会话密钥 K 进行加密), $id\oplus h(pwd)$的形式发送给服务器.

(6) 验证口令. 服务器收到消息后, 首先利用会话密钥 K 对消息进行解密, 得到 id, pwd 的值, 查看数据库表中是否有该 id, 若存在, 则利用哈希函数计算$h(pwd)$的值, 再通过$id\oplus h(pwd)\oplus id$计算得到$h(pwd)$, 最后再从数据库中取出相应 id 对应存储的$h(pwd)$的值, 三者进行对比.

(7) 若 (6) 中三者对比的结果是相同的, 则表示验证成功, 移动端和服务器建立连接, 服务器中的过程信息就可以被移动端成功访问到.

上述认证过程在利用椭圆曲线进行密钥生成时, 其理论基础就是椭圆曲线上的点乘运算. 而点乘运算在椭圆曲线上面定义为重复相加, 即$mP=P+P+\cdots+P$(m 个 P), 遵循椭圆曲线的加法法则, 故点乘运算的结果依然是椭圆曲线上的点[8]. 如果设 G 是椭圆曲线上的一个点, 则选择一个正整数 n 与其相乘, 则 T=nG 仍在椭圆曲线上. 在已知 T 和 G 的情况下, 是很难算出正整数 n 的值的. 这就是著名的椭圆曲线离散对数问题. 该问题在多项式时间内无法被破解, 也就是说即使公钥在消息传递过程中被截获, 其计算私钥的时间复杂度也是指数级别的, 就算是借助超算资源, 也无法在短时间内完成密钥破解.

对应于上述认证过程, 此处 n 就相当于私钥d_c或d_s, T 就相当于公钥Q_c或Q_s, 在图 5 中智能产线移动端与服务器通信过程中, 箭头上的信息即在通信过程中暴露在网络中的信息. 可见, 在消息传递的过程中, 即便公钥被截获, 也很难算出私钥的值, 再加上异或运算以及哈希函数的验证, 这就保证了密钥协商过程中消息传递的安全性. 另一方面, 在上述认证过程中, 由于随机数的加入, 使得每次密钥协商得出的会话密钥均不相同, 保证用户口令在传输过程中的安全性, 且用户口令在存储过程中使用哈希函数进行加密, 保证了其存储的安全性.

3 实验与分析

3.1 可行性验证

在 Android 系统上进行所提出的身份认证机制的可行性验证. 使用开发工具是 Android Studio3.0.1, 模拟器版本为 Nexus 5X API 27 (Android 8.1.0). 所用椭圆曲线为 elliptic curve 25 519, 使用 SecureRabdom 来获取随机数. 通过密钥协商获取到会话密钥以后, 使用 AES CBC 256 位元加密/解密, 使用 PKCS5 填充方式, 哈希函数 h 舍弃常用的 MD5 而选用 SHA-256, 因为对于 MD5 算法, 网上已经有很多可以查询的字典库, 安全性不高. 如图 6 给出基于 R-ECC 的智能产线移动终端身份认证方法在 Android 客户端上的实验结果.

实验结果表明, 本文所提出的面向智能产线移动终端的 R-ECC 身份认证方法可以 Android 上应用, 实现智能产线 Android 客户端与服务器的安全通信.

3.2 性能分析

3.2.1 安全性分析

(1) 实现双向认证. 实验利用所提出的 R-ECC 身份认证方法, 实现了智能产线移动端和服务器的双向认证, 并且通过密钥协商, 计算出共享密钥作为 OPC UA 会话创建过程中的会话密钥.

(2) 抵抗中间人攻击. 本文所提出的 R-ECC 身份认证方法是基于 ECC 算法, 相比于 RSA 算法, 它的破译难度非常高[9], 抗攻击性更强, 只截取到中间传输的信息, 几乎不可能算出私钥或共享密钥, 安全性更高.

(3) 抵抗重放攻击. 在密钥协商以及用户认证的过

程中, 都加入了随机数, 使得即使知道了以前的密钥也无法重新使用, 有效防止了重放攻击.

(4) 密钥前向安全. 由于随机数的加入, 使得每一次会话密钥均不相同, 如果移动端或者服务器的私钥甚至某次会话密钥被窃取, 也无法推断出之前会话的密钥, 所以密钥具有前向安全性.

(5) 安全的数据库存储. 在用户口令的传输过程中, 对用户密码直接进行了加密, 并且在数据库中存储的也是用户密码经过哈希运算的值, 保证了用户口令的安全性.

图 6 可行性实验测试结果

3.2.2 效率分析

(1) 移动设备的加解密计算能力有限, 内存和联网带宽都受到一定限制, 故所提出的面向智能产线移动终端的 R-ECC 身份认证方法不再采用 OPC UA SDK 包中普遍采用的 RSA 公钥体制, 而是采用基于椭圆曲线的 R-ECC 密码体制, 不仅提高了系统的安全性, 并且在同等安全强度下, 其密钥长度要更短, 对存储空间的要求更低[10]. 具体数据见表 1.

表 1 ECC 和 RSA 安全模长 (公钥长度) 的比较 (Bit)

安全级别	ECC	RSA
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	521	15 360

利用 Android Studio3.0.1 自带的 Android Profiler 工具分别对在 OPC UA 架构中, 基于 R-ECC 进行智能产线身份认证以及基于 RSA 进行智能产线身份认证两种方案的认证过程中硬件资源消耗做对比. 对比方法是两种方案分别进行 3 次身份认证连接, 记录认证过程中每种资源消耗的增长量, 并对每种资源 3 次消耗量做均值计算. 对比结果表明, 基于 R-ECC 的智能产线身份认证方法在 CPU 资源、内存资源以及网络资源的消耗上都具有一定的优越性. 对比结果见表 2.

表 2 R-ECC 和 RSA 两种方案资源消耗对比

	CPU(%)	内存(MB)	网络资源(KB/s)	
			Sending	Receiving
R-ECC方案	19.6	10.3	1.85	6.69
RSA方案	28.3	13	2.86	10.89

(2) 在 Android Studio3.0.1 中, 基于同一安全级别 128, 同一用户, 对所提出基于 R-ECC 的智能产线移动终端身份认证方法和 OPC UA SDK 包中所采用的基于 RSA 的身份认证方法的认证成功时间作对比. 通过系统运行日志获取用户认证开始和结束时间, 反复进行 3 次实验, 计算得出认证所需时间, 具体数据见表 3.

表 3 用户认证成功时间测试 (ms)

测试顺序	R-ECC方案	RSA方案
1	366	458
2	342	501
3	363	452
均值	357	470

实验结果表明, 所提出的基于 R-ECC 的智能产线身份认证方法在智能产线 Android 客户端中的认证效率较快, 适用于移动端. 从理论上分析, 一方面, ECC 在解密、签名、私钥的处理以及密钥生成速度上, 都比 RSA 快得多; 另一方面, 在认证过程中, 基于 R-ECC 的 OPC UA 身份认证方法在用户认证过程中除了证书

验证, 只涉及到两次椭圆曲线上的点乘运算, 其他运算都是运算量较小的哈希函数、随机数生成和异或运算, 所以基于 R-ECC 的面向智能产线移动终端的 OPC UA 身份认证方法在移动端上的认证效率是很高的.

4 总结

本文在智能产线移动终端的设计与实现中, 应用 OPC UA 架构, 研究实现了一种面向智能产线移动终端的 R-ECC 身份认证方法. 该方案在身份认证过程中运用椭圆曲线密码学, 并在密钥协商在过程中引入随机数、哈希函数等, 不仅降低了 OPC UA 架构应用于智能产线时在无线通信中的资源损耗, 而且提高了认证的安全性和认证速度. 通过实验验证表明, 所提出方案在工业物联网智能产线移动终端的课题研究中, 适用于 Android 客户端与智能产线 OPC UA 服务器通信过程的身份认证, 实现了移动端与服务器之间的双向认证, 安全的消息交换, 安全的本地存储, 满足移动端轻量级、低功耗以及安全性要求高的特点. 本文所提出的 R-ECC 身份认证方法也为 OPC UA 安全通信的改进提供了新的思路.

参考文献

1 刘薇. 基于 OPC UA 的 MES 数据管理系统的研究 [硕士学位论文]. 北京: 北京邮电大学, 2019.

2 金希, 张为民, 费丽娜, 等. 基于 OPC UA 技术的质量数据监测系统. 机械制造, 2018, 56(11): 104–108. [doi: 10.3969/j.issn.1000-4998.2018.11.027]

3 王树东, 高雅南. OPC UA 系统安全的需求分析和设计. 工业仪表与自动化装置, 2014, (3): 98–101. [doi: 10.3969/j.issn.1000-0682.2014.03.028]

4 宫芳涛. 基于二进制通信的 OPC UA 客户端及安全机制的研究与开发 [硕士学位论文]. 北京: 华北电力大学, 2012.

5 Wang D, Ma CG. Cryptanalysis of a remote user authentication scheme for mobile client–server environment based on ECC. Information Fusion, 2013, 14(4): 498–503. [doi: 10.1016/j.inffus.2012.12.002]

6 He DB. An efficient remote user authentication and key agreement protocol for mobile client–server environment from pairings. Ad Hoc Networks, 2012, 10(6): 1009–1016. [doi: 10.1016/j.adhoc.2012.01.002]

7 Cavalieri S, Salafia MG, Scroppo MS. Towards interoperability between OPC UA and OCF. Journal of Industrial Information Integration, 2019, 15: 122–137. [doi: 10.1016/j.jii.2019.01.002]

8 Gharib M, Moradlou Z, Doostari MA, *et al*. Fully distributed ECC-based key management for mobile ad hoc networks. Computer Networks, 2017, 113: 269–283. [doi: 10.1016/j.comnet.2016.12.017]

9 Sood SK, Sarje AK, Singh K. A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Applications, 2011, 34(2): 609–618. [doi: 10.1016/j.jnca.2010.11.011]

10 王魁, 李立新, 余文涛, 等. 基于 ECC 算法的 TLS 协议设计与优化. 计算机应用研究, 2014, 31(11): 3486–3489. [doi: 10.3969/j.issn.1001-3695.2014.11.065]