



研究与开发

基于 Montgomery 型椭圆曲线密码的 RFID 安全认证方案

章武媚

(浙江同济科技职业学院, 浙江 杭州 310023)

摘要: 针对现有基于椭圆曲线密码 (elliptic curve cryptography, ECC) 体制的 RFID (radio frequency identification device) 安全认证方案不能满足相互认证、隐私保护和前向安全性等要求, 提出一种基于 Montgomery 型椭圆曲线密码的认证方案。利用 Montgomery 型椭圆曲线来降低计算量, 并提供标签和服务器之间的相互认证, 具有匿名性和前向安全性。通过分析表明, 该方案能够抵抗重放攻击、标签伪装攻击、服务器欺骗攻击、DoS 攻击、位置跟踪攻击和克隆攻击。与现有方案相比, 该方案在保证较低的内存、计算和通信需求的情况下, 提供了较高的安全性能, 能够满足 RFID 系统的安全性要求。

关键词: RFID; 安全认证; 椭圆曲线密码; Montgomery; 前向安全

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016107

RFID security authentication scheme based on Montgomery-form elliptic curve cryptography

ZHANG Wumei

Zhejiang Tongji Vocational College of Science and Technology, Hangzhou 310023, China

Abstract: For the issues that the existing RFID security authentication scheme based on elliptic curve cryptography (ECC) can not meet the requirements of mutual authentication, privacy protection and forward security, a RFID security authentication scheme based on Montgomery-form elliptic curve cryptography was proposed. This scheme uses the Montgomery elliptic curve to reduce the amount of computation, and to provide mutual authentication between the label and the server, and anonymity and forward security. The analysis showed that the scheme could resist replay attack, tag camouflage attack, server cheat attack, DoS attack, position tracking attack and clone attack. Compared with the existing schemes, the proposed scheme provides high security performance under low memory, computation and communication requirements, and it can meet the security requirements of the RFID system.

Key words: RFID, security authentication, elliptic curve cryptography, Montgomery, forward security

收稿日期: 2015-10-16; 修回日期: 2016-03-09

基金项目: 浙江省自然科学基金资助项目(No.RC1226)

Foundation Item: The Natural Science Foundation of Zhejiang Province(No.RC1226)



1 引言

无线射频识别 (radio frequency identification device, RFID) 是一种能够自动识别目标的技术^[1]。其主要包括 3 个关键组件: RFID 标签、RFID 阅读器和后端数据库服务器。阅读器用于查询标签 ID, 并将查询到的标签 ID 传输给后端服务器。一旦服务器检测到标签可用, 将进一步处理标签存储的信息。由于标签与阅读器之间的通信信道存在风险, 且 RFID 系统资源有限, 因此, 需要一种安全且轻量级的认证协议来满足安全等级要求和能量约束^[2]。

由于椭圆曲线密码 (elliptic curve cryptography, ECC) 体制^[3]的安全性高、占用带宽小、计算复杂度低等众多优势, 能够有效地保证各种通信网络的安全, 已成为公钥密码体制研究热点^[4]。为此, 学者提出了多种基于 ECC 的 RFID 认证协议。例如, 参考文献[5]提出了一种基于多元 ECC 的身份识别方案, 可以抵制标签伪造攻击。然而, 该方案仅仅考虑了标签的身份认证, 并没考虑阅读器的身份验证, 使得标签很容易遭受恶意查询。参考文献[6]也提出了一种基于 ECC 的认证方案, 然而, 该方案中攻击者可以利用公钥追踪目标标签, 存在前向保密缺陷。参考文献[7]提出了一种基于椭圆曲线离散对数问题 (elliptic curve discrete logarithm problem, ECDLP) 的认证协议, 然而, 该方案存在不能抵抗跟踪攻击和伪造攻击的缺陷。为此, 参考文献[8]对此进行改进, 提出了 ECDLP-RK 方案, 能够抵抗跟踪攻击。然而, 该方案在身份认证阶段更新数据库, 增加了后台服务器的成本, 且缺乏相互认证过程。

ECC 中, 影响计算速度的关键是曲线中的点乘运算。所以, 为了设计出适合资源有限的 RFID 系统的 ECC 快速认证算法, 降低点乘运算是其中的关键^[9]。目前, 出现了一种新兴的椭圆曲线类型: 蒙哥马利 (Montgomery) 型椭圆曲线^[10], 比传统 ECC 曲线具有更快的点乘计算速度, 而且不需要预计算, 可以在计算能力和存储空间有限的条件下实现, 非常适合应用于 RFID 系统中的标签计算。为此, 本文提出了一种基于 Montgomery 型椭圆曲线加密的 RFID 安全认证方案, 实现服务器和标签之间的相互认证, 并提供匿名性保护和前向安全性。通过分析表明, 本文方案在保持低计算量的同时能够抵御多种攻击, 实现了高安全性。

2 Montgomery 型椭圆曲线

2.1 传统椭圆曲线

传统 ECC 中, 输入两个点 P_1, P_2 , 且 P_1, P_2 满足椭圆曲

线方程, 然后生成 P_3 , 且 P_3 也满足曲线方程。这种点的标量乘法被定义为:

$$Q = k \cdots p = p + \cdots + p \quad (K \text{ 次}) \quad (1)$$

椭圆曲线生成了计算式 P 和执行次数 n 。给出 $(x, y) \in E(F_q)$, 找出整数 $c \in Z_n$, 由此得到的 $Y = c \cdot X$ 就是椭圆曲线的离散对数。

2.2 Montgomery 型椭圆曲线

Montgomery 型椭圆曲线与传统椭圆曲线相比, 其优势主要体现在 2 个方面^[11]: 由于在点乘计算时不需要计算 Y 轴值, 降低了计算量, 提高了计算速度; 对于简单的能量攻击和时间攻击具有更强的免疫力。

Montgomery 型椭圆曲线在 $\frac{E}{F_p}$ 的仿射坐标方程为 $By^2 = x^3 + Ax^2 + x$ 。假定 $P = (x_1, y_1), Q = (x_2, y_2)$ 是在 $E(k)$ 上的椭圆曲线的点, 其中 $P \neq \pm Q$, 则 Montgomery 型椭圆曲线的点加及倍点运算表示如下。

$P+Q=(x_3, y_3)$ 的值为:

$$\begin{aligned} \Lambda &= \frac{y_2 - y_1}{x_2 - x_1} \\ x_3 &= B\Lambda^2 - A - x_1 - x_2 \\ y_3 &= \Lambda(x_1 - x_2) - y_1 \end{aligned} \quad (2)$$

而点乘式为 ($P=Q$):

$$\begin{aligned} \Lambda &= \frac{3x_1^2 + 2Ax_1 + 1}{2By_1} \\ x_3 &= B\Lambda^2 - A - 2x_1 \\ y_3 &= \Lambda(x_1 - x_3) - y_1 \end{aligned} \quad (3)$$

3 本文提出的认证方案

本文提出了一种基于 Montgomery 型椭圆曲线密码体制的 RFID 相互身份认证方案。在典型 RFID 系统中, 标签和阅读器之间通信的无线信道是不安全的^[12], 典型 RFID 系统框架如图 1 所示。为了确保身份识别码从标签到服务器无线通信传输的安全性, 本文设计了一种安全的身份认证传输方案, 并采用回应机制来更新交流信息。其主要分为两个阶段: 设置阶段和身份认证阶段。

3.1 设置阶段

在设置阶段, 设定服务器和标签均知晓椭圆曲线参数。服务器持有私钥 $x_S \in Z_n$, 并将其与椭圆曲线上的点 P 相乘, 以此获得 ECC 加密的服务器公钥 $P_S (= x_S P)$ 。服务器为每个标签选择私钥 $x_T \in Z_n$, 并设置 ECC 加密的标签身份

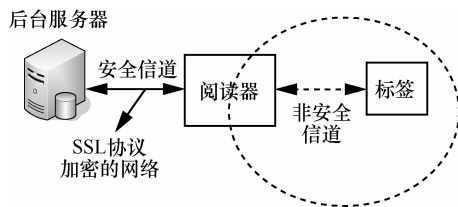


图 1 典型 RFID 系统框架

识别码或公钥 $Z_T(=x_T P)$ 。接下来,服务器将每个标签的入口值 $\{Z_T, x_T\}$ 记录到数据库中。此外,每个标签存储 $\{Z_T, x_T\}$ 、服务器公钥 P_S 及域参数 D 。

3.2 身份认证阶段

身份认证阶段中,标签和服务器之间交互的步骤如下。

步骤 1 服务器生成随机数 $r_2 \in Z_n$, 并计算 $R_2 = r_2 P$, 然后服务器将附有查询信息的 R_2 发送给标签。

步骤 2 标签收到查询信息 $\langle Query, R_2 \rangle$ 后, 选择一个随机数 $r_1 \in Z_n$, 并计算 $R_1 = r_1 P$ 。然后计算两个临时密钥 $TK_{T1} = r_1 R_2, TK_{T2} = r_1 P_S$ 。接下来, 标签通过计算 $Auth_T = Z_T + TK_{T1} + TK_{T2}$ 将身份识别码 Z_T 译成密码, 并返回结果 $\langle Auth_T, R_1 \rangle$ 到服务器。

步骤 3 服务器接收到 $\langle Auth_T, R_1 \rangle$ 后, 通过计算 $TK_{S1} = r_2 R_1, TK_{S2} = x_S P_1$ 重新获得两个临时密钥。接着, 服务器利用这两个临时密钥通过以下计算重新获得身份认证码 Z_T :

$$\begin{aligned} Auth_T - TK_{S1} - TK_{S2} &= (Z_T + TK_{T1} + TK_{T2}) - TK_{T1} - TK_{T2} \\ &= (Z_T + r_1 R_1 + r_2 R_2) - r_2 R_1 - x_S R_1 \\ &= (Z_T + r_1 r_2 P + r_1 x_S P) - r_2 r_1 P - x_S r_1 P \\ &= Z_T \end{aligned} \quad (4)$$

然后, 服务器在数据库中搜索标签的身份认证码。如果找到认证码, 则服务器确认该标签是合法的, 并且获得私钥 x_T 。接着, 服务器计算 $Auth_S = x_T R_1 + r_2 Z_T$, 并发回 $\langle Auth_S \rangle$ 给标签。

步骤 4 标签计算 $r_1 Z_T + x_T R_2$, 并核对其结果是否等于接收到的 $\langle Auth_S \rangle$ 。如果相等, 则标签将确认该服务器是可信的。其中, $Auth_S$ 的计算式推导如下:

$$Auth_S = x_T r_2 Z_T = x_T r_1 P + r_2 x_T P = r_1 Z_T + x_T R_2 \quad (5)$$

本文方案的身份认证阶段过程如图 2 所示。

4 安全性

4.1 系统功能

4.1.1 提供标签与服务器间的相互认证

服务器通过核对接收到的 $Auth_T$ 的正确性来确认标签是否可信。如步骤 3 中, 服务器接收到信息 $\langle Auth_T, R_1 \rangle$, 根

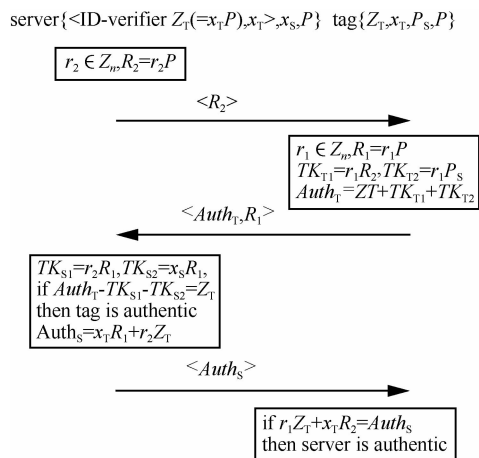


图 2 提出的基于 Montgomery 型 ECC 的认证方案

据椭圆曲线离散对数问题(ECDLP), 服务器可以通过计算 $(Auth_T - TK_{S1} - TK_{S2})$ 解密 Z_T 。如果解密结果与数据库中的记录相吻合, 则标签通过服务器的认证。另一方面, 标签通过核对接收到的 $Auth_S$ 的正确性来确认服务器是否可信。如步骤 4 中, 标签接收到信息 $Auth_S(=x_T R_1 + r_2 Z_T)$ 后, 利用 (r_1, R_2) 进行 $r_1 Z_T + x_T R_2$ 计算。如果计算结果与接收到的 $Auth_S$ 匹配, 则标签认证服务器成功, 即完成相互认证过程。

4.1.2 提供匿名性保护

RFID 系统中, 匿名性是隐私保护的重要安全需求。在身份认证步骤中, 攻击者不能从收集到的信息 $\langle Auth_T, Auth_S \rangle$ 中得到 Z_T , 所以, 攻击者不能够通过监控交换消息来获得身份认证码 Z_T 。此外, 由于两个随机数 (r_1, r_2) 是新数, 所以每个环节的交换信息 $\langle Auth_T, Auth_S \rangle$ 是变化且不可预知的。尽管攻击者可通过随机数 r_2^* 和椭圆曲线点 $R_2^* = r_2^* P$ 向目标标签发送恶意查询, 但是攻击者在不知道 $TK_{T2}(=r_1 P_S = x_S R_1)$ 的情况下, 仍然不能解析交换信息。

4.1.3 提供前向安全性

本文方案中, 攻击者不能利用目前传输的标签信息来追踪之前的传输信息, 提供了前向安全性。本文假设攻击者知道标签密钥 Z_T 和 x_T 。尽管如此, 攻击者仍然无法知道临时生成的随机数, 因此无法获知之前的交流信息。

4.2 抵抗攻击

4.2.1 抵抗重放攻击

重放攻击中, 攻击者拦截了之前的交流信息后, 通过重放这些信息, 尝试通过认证系统。攻击者可伪装成服务器或标签, 通过重复使用之前的 $Auth_S$ 或 $Auth_T$ 发起重放攻击。本文系统中, 利用两个随机数 (r_1, r_2) 控制信息 $Auth_T$



和 $Auth_s$ 信息,且 (r_1, r_2) 在每个环节都是不同且不可预知的。也就是说,攻击者不能重复利用先前的信息去欺骗标签或服务器。所以,本文方案能够抵抗重放攻击。

4.2.2 抵抗标签伪装攻击

标签伪装攻击中,攻击者通过拦截或修改之前合法标签的信息,并使这些信息经过服务器的身份认证。本文方案中,如果攻击者想构建一个有效的身份认证信息 $\langle Auth_T, R_1 \rangle$,则需要从之前的 $Auth_T$ 中获得身份认证码 Z_T 。由于存在椭圆曲线离散对数问题,攻击者不能从收集到的信息中推断出 (TK_{T1}, TK_{T2}) 和 (TK_{S1}, TK_{S2}) 。也就是说,攻击者不能通过之前的 $Auth_T$ 解密获得 Z_T 。因此,攻击者不能构建有效的身份认证消息,本文方案能够抵抗标签伪装攻击。

4.2.3 抵抗服务器欺骗攻击

服务器欺骗攻击中,攻击者创建一个嵌有身份认证码 Z_T 的有效信息 $Auth_s$,伪装成服务器来获得标签信任。本文方案中,服务器发给标签的 $Auth_s (= x_T R_1 + r_2 Z_T)$ 为有着临时密钥 $x_T R_1$ 的密钥 $r_2 Z_T$ 。换句话说,标签计算的 $Auth_s (= r_1 Z_T + x_T R_2)$ 可为有着临时密钥 $x_T R_2$ 的密码 $r_1 Z_T$ 。由于 (r_2, x_T) 和 (r_1, x_T) 均不能被攻击者通过椭圆曲线离散对数问题得知,所以身份验证码 Z_T 不能通过 $Auth_s$ 得出。所以,本方案能够抵抗服务器欺骗攻击。

4.2.4 抵抗 DoS 攻击

DoS 攻击中,攻击者通过阻断每次通信中的会话,导致服务器更新了随机数,而标签没有更新,使标签和服务器失去同步,从而形成 DoS 攻击。然而,通过上述可知,本方案不需要同步更新密钥信息来提供标签和后端服务器之间的隐私保护。因此,本方案可以抵抗 DoS 攻击。

4.2.5 抵抗位置跟踪攻击

在位置跟踪攻击中,攻击者截听会话信息,并根据信息内容将其与特定的标签相关联,以此跟踪标签位置。然而,在本方案中,服务器和标签之间传输的数据被保护,所以标签身份认证码 Z_T 不能从信息流中解码获得。此外,信息流在每个环节都会发生不可预知的变化。因此,可以抵抗位置跟踪攻击。

4.2.6 抵抗克隆攻击

如果许多标签共享相同的密钥,并用该密钥进行身份认证,这很容易导致克隆攻击。克隆攻击中,攻击者利用捕获标签的密钥尝试控制其他标签。然而,在本文方案中,每个标签拥有它自己唯一的密钥 x_T 和身份认证码 Z_T 。即使很多标签被捕获,攻击者也不能用一个标签的密

钥 $\{x_T, Z_T\}$ 去获得其他标签的密钥。也就是说,攻击者不能利用这些泄露的密钥去攻击其他标签,从而实现抵抗克隆攻击。

5 性能比较

在 RFID 认证过程中,RFID 标签和后台服务器需要进行各种认证计算,由于后台服务器能源、计算和存储资源较为丰富,所以服务器的计算复杂度可不考虑。然后,RFID 标签的资源有限,因此,在实际应用中,认证方案在 RFID 标签上的资源性能非常重要。认证方案的资源性能指标包括存储需求、计算成本和通信开销^[13]。内存需求由标签的存储量(包括私钥和公钥)决定。其中,私钥为标签的密钥,公钥包括标签的公钥、服务器的公钥及椭圆曲线的基准点。计算成本根据有限域内的点标量乘法数量来估计。通信成本为身份认证阶段的信息流量。

本文利用 163 bit Montgomery 型椭圆曲线定义有限域 $F(2^{163})$,一个 5 MHz 的标签在 32 ms 内可以完成一个 163 bit 标量乘法运算^[14],可以以此来估计协议所需的计算时间。本文利用的 Montgomery 型椭圆曲线,其输入为不完整的点,仅需要仿射 x 坐标。所以,在方案运行过程中,不需要曲线点的 y 坐标,从而减少了信息的数量,降低了认证协议的运算量。参考文献[15]证明, Montgomery 型椭圆曲线点乘运算比传统椭圆曲线的计算量降低约 30%。

本方案中,内存需求包括 $\{x_T, Z_T, P_s, P\}$,其中 x_T 私钥为 163 bit,公钥 $\{Z_T, P_s, P\}$ 为 489 bit(一个公钥的 x 坐标为 163 bit)。这是因为本文使用了 163 bit 的 Montgomery 型椭圆曲线加密公钥,致使每个公钥为 163 bit,这导致了较大的公钥位数,但会使求解 ECDLP 的难度更大,即提供更高的安全性。

由于本方案中需要 5 个点标量乘法运算,所以大约需要 112 ms $(32 \text{ ms} \times 5 \times 30\%)$ 。通信开销为阅读器和标签之间的 82 bit 交流信息 $\langle R1, R2, Auth_s, Auth_T \rangle \left(163 \times \frac{4}{8} = 82 \right)$ 。本文方案与现有基于 ECC 方案在 RFID 标签上的计算、存储和通信开销比较见表 1。可以看出,在标签的资源性能上,本方案和其他方案相近,但是本方案提供了很高的安全性能。其中,为了提高安全性,本方案执行 5 次点乘运算,但并没有明显增加计算时间,这是因为本文 Montgomery 型 ECC 点乘运算比其他方案采用的传统 ECC 点乘的计算复杂度低。另外,在协议执行轮数上,本方案在服务器和标签之间

表 1 基于 ECC 认证方案在 RFID 标签上资源性能比较

性能指标		参考文献[5]	参考文献[6]	参考文献[7]	参考文献[8]	本方案
内存需求/bit	私钥	163	326	326	326	163
	公钥	163	326	326	326	489
	合计	41	82	82	82	82
计算成本/ms	标量点乘次数	4	4	3	3	5
	时间/ms	128	128	96	96	113
通信开销/bit		61	82	82	82	82
协议执行轮数(信息交换次数)		5	3	4	4	3

只需要执行 3 次信息交换即可完成相互认证。减少信息交互次数能够降低通信开销和通信信息被非法截取的概率。

将本文方案和现有基于 ECC 的方案的安全性能比较见表 2。可以看出,本方案具有多种系统功能且能够抵御多种针对 RFID 的攻击类型。

6 结束语

针对现有基于 ECC 的 RFID 安全认证方案不能满足系统的认证、隐私保护和前向安全性等要求。提出了一种基于 Montgomery 型椭圆曲线密码的认证方案,提供标签和服务器之间的相互认证,具有匿名性和前向安全性,能够抵抗重放攻击、标签伪装攻击、服务器欺骗攻击、DoS 攻击、位置跟踪攻击和克隆攻击。与现有方案相比,本文所提方案在保证较低的内存、计算和通信需求下,提供了较高的安全性能,非常适用于 RFID 认证系统。

本方案虽然没有增加计算量,但公钥位数较大。在今后的工作中,将考虑采用较低位数 Montgomery 型椭圆曲线或其他简化型椭圆曲线来加密密钥,在保证安全性前提下减小公钥位数,进一步降低资源开销。

参考文献:

[1] 张学军,陈彦君,常昆.改进型 RFID 相互认证协议研究[J].计算机技术与发展,2013,23(8):129-132.
ZHANG X J, CHEN Y J, CHANG K. An improved RFID mutual authentication protocol [J]. Computer Technology and Development, 2013, 23(8): 129-132.

[2] 张兵,马新新,秦志光.轻量级 RFID 双向认证协议设计与分析[J].电子科技大学学报,2013,42(3):425-430.
ZHANG B, MA X X, QIN Z G. Design and analysis of a lightweight mutual authentication protocol for RFID [J]. Journal of University of Electronic Science and Technology of China, 2013, 42(3): 425-430.

[3] 张文芳,王小敏,郭伟,等.基于椭圆曲线密码体制的高效虚拟企业跨域认证方案[J].电子学报,2014,42(6):1095-1102.
ZHANG W F, WANG X M, GUO W, et al. An efficient inter-enterprise authentication scheme for VE based on the elliptic curve cryptosystem [J]. Acta Electronica Sinica, 2014, 42(6): 1095-1102.

[4] 王明辉,王建东.高效的 RFID 双向认证协议 [J]. 计算机应用,2011,31(10):2694-2696.
WANG M H, WANG J D. Efficient RFID mutual authentication protocol [J]. Journal of Computer Applications, 2011, 31(10): 2694-2696.

表 2 基于 ECC 方案之间的安全性能比较

安全性能	参考文献[5]	参考文献[6]	参考文献[7]	参考文献[8]	本方案
相互认证	无	有	无	无	有
匿名性	无	无	无	有	有
向前保密性	无	无	有	有	有
可扩展性	无	有	有	无	有
抵抗重放攻击	有	有	有	有	有
抵抗标签伪装攻击	有	无	无	有	有
抵抗服务器欺骗攻击	有	无	无	有	有
抵抗 DoS 攻击	无	有	有	有	有
抵抗位置跟踪攻击	无	无	无	有	有
抵抗克隆攻击	无	有	有	无	有



- [5] ARBIT A, OREN Y, WOOL A. Toward practical public key anti-counterfeiting for low-cost EPC tags [C]// 2011 IEEE International Conference on RFID, April 12-14, 2011, Orlando, FL, USA. New Jersey: IEEE Press, 2011: 184-191.
- [6] GODOR G, IMRE S. Elliptic curve cryptography based authentication protocol for low-cost RFID tags [C]//2011 IEEE International Conference on RFID-Technologies and Applications(RFID-TA), Sept 15-16, 2011, Sitges, Spain. New Jersey: IEEE Press, 2011: 386-393.
- [7] CHEN Z, LI L, WU Y, et al. A mutual authentication improvement for traditional unidirectional ECDLP-based RFID authentication protocols[C]//2012 Second International Conference on Electric Information and Control Engineering-Volume 02, 2012. Washington: IEEE Computer Society, 2012: 421-432.
- [8] FARASH M S. Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography[J]. Journal of Supercomputing, 2014, 70(2): 987-1001.
- [9] 吴焘, 李树国, 刘理天. 一种新的余数系统下快速计算素域椭圆曲线点乘的方法 [J]. 计算机工程与科学, 2014, 36(10): 1839-1845.
- WU T, LI S G, LIU L T. A new RNS approach for fast Fp elliptic curve point multiplication[J]. Computer Engineering and Science, 2014, 36(10): 1839-1845.
- [10] 庞世春, 刘淑芬, 从福仲, 等. 一种 Montgomery 型椭圆曲线的高效标量乘算法[J]. 电子学报, 2011, 39(4): 865-868.
- PANG S C, LIU S F, CONG F Z, et al. An efficient scalar multiplication algorithm on Montgomery-form elliptic curve[J]. ACTA Electronica Sinica, 2011, 39(4): 865-868.
- [11] ALKHATIB M, JAAFAR A, MRM S, et al. Parallelizing GF (p) Montgomery elliptic curve crypto-system operations to improve security and performance [J]. Advanced Materials Research, 2012, 36(7): 1906-1911.
- [12] 杨玉龙, 彭长根, 周洲, 等. 基于 Edwards 曲线的移动 RFID 安全认证协议[J]. 通信学报, 2014, 35(11): 133-138.
- YANG Y L, PENG C G, ZHOU Z, et al. Edwards curves based security authentication protocol for mobile RFID systems [J]. Journal on Communications, 2014, 35(11): 133-138.
- [13] HUO L, JIANG Y L, HU L Q. Research on hash-based low-cost RFID security authentication protocol [J]. Advanced Materials Research, 2013, 46(2): 1524-1530.
- [14] LIU Z, LIU D, ZOU X, et al. Design of an elliptic curve cryptography processor for RFID tag chips[J]. Sensors, 2014, 14(10): 883-904.
- [15] 王潮, 时向勇, 牛志华. 基于 Montgomery 曲线改进 ECDSA 算法的研究[J]. 通信学报, 2010, 31(1): 9-13.
- WANG C, SHI X Y, NIU Z H. The research of the promotion for ECDSA algorithm based on Montgomery-form ECC [J]. Journal on Communications, 2010, 31(1): 9-13.

[作者简介]



章武媚(1971-), 女, 浙江同济科技职业学院副教授, 主要研究方向为网络安全、信息安全等。