doi:10.3969/j.issn.1000-436x.2014.11.015

基于 Edwards 曲线的移动 RFID 安全认证协议

杨玉龙[1,2]，彭长根[2,3]，周洲[1,2]，张晓培[2]
（1. 贵州大学 计算机科学与技术学院，贵州 贵阳 550025；
2. 贵州大学 密码学与数据安全研究所，贵州 贵阳 550025；3. 贵州大学 理学院，贵州 贵阳 550025）

摘 要：针对传统的 RFID 认证协议通常难以适应移动 RFID 系统的问题，提出了基于 Edwards 曲线的适用于移动 RFID 系统的安全认证协议，协议采用 Edwards 曲线提高了其防侧信道攻击的能力，并应用椭圆曲线离散对数问题实现安全认证。进一步采用可证明安全方法给出了标签和阅读器不可跟踪隐私的安全性证明，通过安全性分析指出协议能更有效抵抗已有各种攻击。与现有的结构类似 RFID 认证协议相比，该协议扩展性更好，安全性和性能优于其他方案。

关键词：移动 RFID 系统；Edwards；安全认证；隐私保护；可证明安全
中文分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)11-0132-07

Edwards curves based security authentication protocol for mobile RFID systems

YANG Yu-long[1,2], PENG Chang-gen[2,3], ZHOU Zhou[1,2], ZHANG Xiao-pei[2]
（1. College of Computer Science & Information, Guizhou University, Guiyang 550025, China;
2. Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China;
3. College of Science, Guizhou University, Guiyang 550025, China）

Abstract: Existing work about RFID authentication protocols is usually difficult to adapt to mobile RFID systems. In order to solve the problem, an Edwards curves based security authentication protocol for mobile RFID systems is proposed. The protocol can improve the ability of resisting the side channel attacks by using the Edwards curve and the elliptic curve discrete logarithm problem is applied to implement safety certification. Further the tag and reader's untraceable privacy is proved by using the provable security method, the security analysis shows that the protocol can be more effective against for various attacks which have existed. Compared with the existing structure similar to RFID authentication protocol, the protocol has better scalability and its security and performance is superior to other solutions.
Key words: mobile RFID systems; Edwards; security authentication; privacy protection; provable security

1 引言

移动 RFID 系统是 RFID（无线射频识别）技术的一种典型应用，其区别于传统的 RFID 系统。在传统的 RFID 认证方案中，阅读器一般是固定的，并且假设服务器（server）与阅读器（reader）之间的通信信道是安全的[1]。但是随着移动智能终端的快速发展，将阅读器嵌入移动智能终端中形成移动 RFID 系统，受到广大学者的关注。在移动 RFID 系统中，由于阅读器工作方式的改变，上述假设已经

收稿日期：2014-07-22；**修回日期**：2014-08-14
基金项目：国家自然科学基金资助项目（61262073）；全国统计科学研究计划基金资助项目（2013LZ46）；贵州省自然科学基金资助项目（20092113）；贵州省高层次人才科研条件特助经费基金资助项目（TZJF-2008-33）；贵州大学自然科学青年研究基金资助项目(2009092)
Foundation Items: The National Natural Science Foundation of China(61262073); The National Statistical Scientific Research Projects(2013LZ46); The National Science Foundation of Guizhou Province(20092113); The Special Scientific Research Facilities Fund for High-Level Talents in Guizhou Province(TZJF-2008-33); The Natural Science Youth Research Foundation in Guizhou University(2009092)

不适用，阅读器不再固定，后端服务器和阅读器之间的通信信道采用无线传输信息，导致二者之间的通信信道不再安全，这就需要研究适用于移动 RFID 系统的安全认证协议[2]。

2006 年，Tuyls 等人[3]首次提出了一个基于 ECC 的 RFID 认证协议，该方案建立在 Schnorr 识别方案基础上。2007 年，Batin 等人[4]应用 Okamoto 识别方案提出了一个基于 ECC 的认证方案，该方案与 Tuyls 等人方案类似。Lee 等人[5]指出 Tuyls 的方案存在安全漏洞，不能抵抗不可跟踪隐私、前向隐私等，扩展性较差，同时指出 Batin 等人的方案也存在标签可被跟踪、前向隐私、扩展性问题。在分析总结上面 2 个方案的基础上，Lee 等人提出了一个新的 RFID 认证方案，解决上述方案标签 ID 披露问题，但是该方案也存在扩展性问题。2007 年，Batina 等人[6]分析了 Okamoto 识别方案适用于 RFID 标签，指出公钥密码是可以应用在 RFID 标签中，而椭圆曲线密码在密钥长度相当的情况下拥有更高的安全性，比较适合应用在资源受限的 RFID 标签中。2010 年，Gódor 等人[7]提出了一个 RFID 双向认证协议，Chou 等人[8]指出该方案不能够抵抗服务器消息的重放攻击。2011 年，Chen 等人[9]提出了一个新的基于椭圆曲线的 RFID 认证协议，但是该协议只实现了标签的单向认证。同年，Chou 等人[10]提出了一个基于椭圆曲线的双向认证协议，并对协议进行了验证实现。

上述方案有一个共同点，都是针对传统 RFID 系统设计的安全认证协议，并不适用于移动 RFID 系统。2012 年，Zhou 等人[11]提出了一个基于椭圆曲线的双向认证协议，用于解决移动 RFID 系统中的隐私保护与安全问题，但是研究发现该方案不能保证阅读器的隐私，同时标签在认证中计算量过大。2013 年，Niu 等人[12]提出了适用于移动 RFID 的超轻量级隐私保护安全认证协议，分析发现该协议不能有效抵抗标签消息的重放攻击。

2008 年，张宝华等人[13]指出，由于 Edwards 曲线上的倍点运算和点加运算具有相同的公式，其符合抵抗简单能量分析 SPA（simple power analysis）防御措施的第二条线索，同时提出了一种 Edwards 曲线上的快速标量乘运算算法 EDSM。Coron 在文献[14]中指出可以通过随机化方法将抵抗 SPA 攻击的防御措施转变为抵抗差分能量分析 DPA（differential power analysis）的措施。因此，Edwards 曲线在防止侧信道攻击上具有较好效果，之后相继有学者研究 Edwards 曲线的防侧信道攻击和快速标量乘法[15,16]。

通过研究现有的 RFID 认证方案，发现在这些方案中大都采用一般化的 ECC，并且方案在隐私保护方面总存在不足之处，或者扩展性较差。针对移动 RFID 系统的研究方案，由于移动阅读器（以下统称移动阅读器）是由嵌入阅读器的智能终端充当，就需对移动阅读器进行认证，并保护移动阅读器的隐私，已有的方案无法令人满意。考虑 Edwards 曲线在运算效率和安全性方面都优于其他形式的椭圆曲线，本文研究基于 Edwards 曲线的适用于移动 RFID 系统的安全认证协议，并采用可证明安全方法对标签和移动阅读器的不可跟踪隐私进行了安全性证明，同时分析指出协议能更有效抵抗已有各种攻击。与现有的结构类似 RFID 认证协议相比，该协议扩展性更好，安全性和性能优于其他方案。

2　准备知识

本节首先介绍了 Edwards 曲线，指出其优点，然后建立了移动 RFID 系统的不可跟踪可证明安全模型。

2.1　Edwards 曲线

Edwards 曲线是椭圆曲线的一种形式，每条椭圆曲线都可以转换变形为 Edwards 形式的椭圆曲线，最早由 Edwards[17]提出并被 Bernstein 等人[18]引入到密码学应用中，其加法公式对称，统一（适用于倍点计算），在某些情况下加法公式是完全的（适用于任意点），而且加法公式的效率相较于其他形式的椭圆曲线更高。

设 F_q 是一个特征不为 2 的有限域，则 F_q 上的 Edwards 曲线[17]为

$$G_c: x^2 + y^2 = c^2(1 + x^2y^2) \tag{1}$$

其中，$c \in F_q, c \neq 0$。G_c 上的所有有理点构成的集合是一个加群，记为 $G_c(F_q)$。该群上的点记为 (x, y)，其中零元是 $(0, c)$，$-(x, y) = (-x, y)$。$P_1 = (x_1, y_1)$ 和 $P_2 = (x_2, y_2)$ 是 G 上的元素，则 P_1 和 P_2 的和 $P_3 = (x_3, y_3)$ 由式(2)计算得到。

$$(x_3, y_3) = \left(\frac{x_1y_2 + y_1x_2}{c\left(1 + x_1x_2y_1y_2\right)}, \frac{y_1y_2 - x_1x_2}{c\left(1 - x_1x_2y_1y_2\right)} \right) \tag{2}$$

上述公式同样适用于倍点计算，即当 $P_1 = P_2$

时，上述公式不需做任何改变，即 Edwards 曲线上的倍点运算和点加运算公式相同。2007 年 Bernstein 等人[18]对 Edwards 曲线的群运算进行详细分析，分析结果表明 Edwards 曲线在群运算的效率和安全性方面都优于其他形式的椭圆曲线。

2.2 安全模型

移动 RFID 安全协议不仅要确保标签秘密信息不被泄露，保障标签的不可跟踪隐私，还要确保移动阅读器的不可跟踪隐私。本文在建立移动 RFID 系统的不可跟踪模型时，用 Oracle 查询来模型化敌手 A 的能力，用 T 表示 tag，用 R 表示移动阅读器，用 S 表示后端服务器，三者参与的协议为 P。协议参与方都可以发起 P 的多个实例，用 Π_T 表示标签的实例，用 Π_R 表示阅读器的实例，用 Π_S 表示后端服务器的实例，敌手 A 可以进行如下查询。

1) $Execute(\Pi_T,\Pi_R,\Pi_S,i)$ 查询

该查询刻画了敌手 A 执行协议 P 的一个实例，并获得第 i 轮会话中 T 与 R 之间、R 与 S 之间交互的所有信息。该查询模型化一个静态攻击。

2) $Send(\Pi_T,message,i)$ 查询

该查询刻画了敌手 A 在第 i 轮会话中向标签 T 发送一个消息，该查询模型化一个动态攻击。通过该查询，标签根据协议和存储的数据返回一个响应。

3) $Send(\Pi_R,message,i)$ 查询

该查询刻画了敌手 A 在第 i 轮会话中向移动阅读器 R 发送一个消息，该查询模型化一个动态攻击。通过该查询，移动阅读器根据协议和存储的数据返回一个响应。

4) $Corrupt(\Pi_T)$ 查询

该查询刻画了敌手 A 收买标签 T 的能力，使标签主动泄露自己的秘密信息，该查询模型化一个动态攻击。

5) $Corrupt(\Pi_R)$ 查询

该查询刻画了敌手 A 收买移动阅读器 R 的能力，使移动阅读器主动泄露自己的秘密信息，该查询模型化一个动态攻击。

在移动 RFID 系统中，RFID 安全认证协议不仅要保证标签和移动阅读器的隐私信息不被泄露，还需要确保标签 T_0、T_1 与移动阅读器 R_0、R_1 的不可识别和区分性。下面形式化描述了标签、移动阅读器的不可跟踪隐私。

定义 1 标签不可跟踪隐私（tag untraceable privacy）利用一个敌手 A 与服务器 S，一组阅读器 R 和若干标签 T 实例之间进行的游戏 g 来定义，敌手 A 所执行的游戏 g 的设置如下。

学习阶段（learning phase）：敌手 A 可以向任意标签 T 发送任意 $Execute$，$Send(\Pi_T,message,i)$，$Corrupt(\Pi_T)$ 查询。

挑战阶段（challenge phase）：

1) 在协议执行的第 i 轮会话中，敌手 A 选择 2 个未被收买的标签 T_0 与 T_1 给挑战者。然后挑战者随机选择一个比特 $b\in\{0,1\}$，发送 $T_b\in\{T_0,T_1\}$ 给 A；

2) 敌手 A 继续进行 $Execute$ 查询，获得第 i 轮会话所有交互信息。

猜测阶段（speculate phase）：敌手 A 结束游戏 g，输出一个比特 b' 作为对 b 的猜测。

如果 $|\Pr(b'=b)-1/2|=\varepsilon$ 是可忽略的，则说明协议 P 是安全的，即标签不可跟踪。

定义 2 移动阅读器不可跟踪隐私（reader untraceable privacy），是利用一个敌手 A 与服务器 S，一组阅读器 R 和若干标签 T 实例之间进行的游戏 g 来定义的，敌手 A 所执行的游戏 g 的设置如下。

学习阶段（learning phase）：敌手 A 可以向任意移动阅读器 R 发送任意 $Execute$，$Send(\Pi_R,message,i)$，$Corrupt(\Pi_R)$ 查询。

挑战阶段（challenge phase）：

1) 在协议执行的第 i 轮会话中，敌手 A 选择 2 个未被收买的移动阅读器 R_0 与 R_1 给挑战者，然后挑战者随机选择一个比特 $b\in\{0,1\}$，发送 $R_b\in\{R_0,R_1\}$ 给 A；

2) 敌手 A 继续进行 $Execute$ 查询，获得第 i 轮会话所有交互信息。

猜测阶段（speculate phase）：敌手 A 结束游戏 g，输出一个比特 b' 作为对 b 的猜测。

如果 $|\Pr(b'=b)-1/2|=\varepsilon$ 是可忽略的，则说明协议 P 是安全的，即移动阅读器不可跟踪。

3 方案介绍

方案中所用符号解释如表 1 所示。

3.1 初始阶段

在协议执行前，所有实体需初始化内存单元，后端服务器 S 首先选择一个有限域 F_q，定义在 F_q 上的 Edwards 曲线 G 和 G 上的基准点 P，其中 P 的阶为 n。S 选择一个随机数 y，计算 $Y=yP$，然后将 y 作为 S 的私钥，Y 作为 S 的公钥。后端服务器

在 G 上随机选择一个点 R_i 作为第 i 个移动阅读器 R 的标识，后端服务器在 G 上随机选择一个点 X_i 作为第 i 个标签 T 的标识。然后， S 通过安全信道将 $\{R_i,P,Y\}$ 与 $\{X_i,P,Y\}$ 分别分发给阅读器 R 和标签 T，并计算阅读器的标识 R_i 与标签标识 X_i 的笛卡尔积 $\{R_i,X_i\}$，对每个标识组合进行 $h(R_i,X_i)$ 运算，形成三元组 $\{R_i,X_i,h(R_i,X_i)\}$。

表 1　　方案中所有符号的解释

符号	含义
F_q	有限域
G	Edwards 曲线上阶为 q 的群
P	Edwards 曲线上的基准点
y	后端服务器的私钥
$Y(=yP)$	后端服务器的公钥
R_i	在 G 上随机选择的点作为阅读器标识
X_i	在 G 上随机选择的点作为标签标识
h	从 $G\times G$ 到 Z_q 的单向散列函数
s，r，k	在 Z_q 上的 3 个随机数
$\oplus$	异或操作符

3.2　认证阶段

协议认证的流程图如图 1 所示，其详细描述如下。

1) $R\rightarrow T$： B_0

阅读器生成一个随机数 $s\in_R Z_q$ 作为会话的临时私钥，计算 $B_0=sP$，然后通过广播信道向标签发送 B_0 开始一轮会话。

2) $T\rightarrow R$： C_0， C_1， C_2

标签收到阅读器发送的 B_0，利用随机数产生器生成一个随机数 $r\in_R Z_q$ 作为会话的临时私钥，计算 $C_0=rB_0$， $C_1=h(B_0,rP)$， $C_2=X_i+rY$，然后发送响应消息 C_0， C_1， C_2 给阅读器。

3) $R\rightarrow S$： B_2， B_3， B_4， C_2

阅读器收到消息 C_0， C_1， C_2 后，计算 $B_1=s^{-1}C_0(=rP)$，并验证 $h(B_0,B_1)?=C_1$，验证通过，阅读器利用随机数产生器生成一个随机数 $k\in_R Z_q$ 作为会话的临时私钥，计算 $B_2=kP+R_i$，$B_3=kY-C_2$， $B_4=B_1+R_i$，然后发送响应消息 B_2，B_3， B_4， C_2 给阅读器。如果验证失败，直接终止

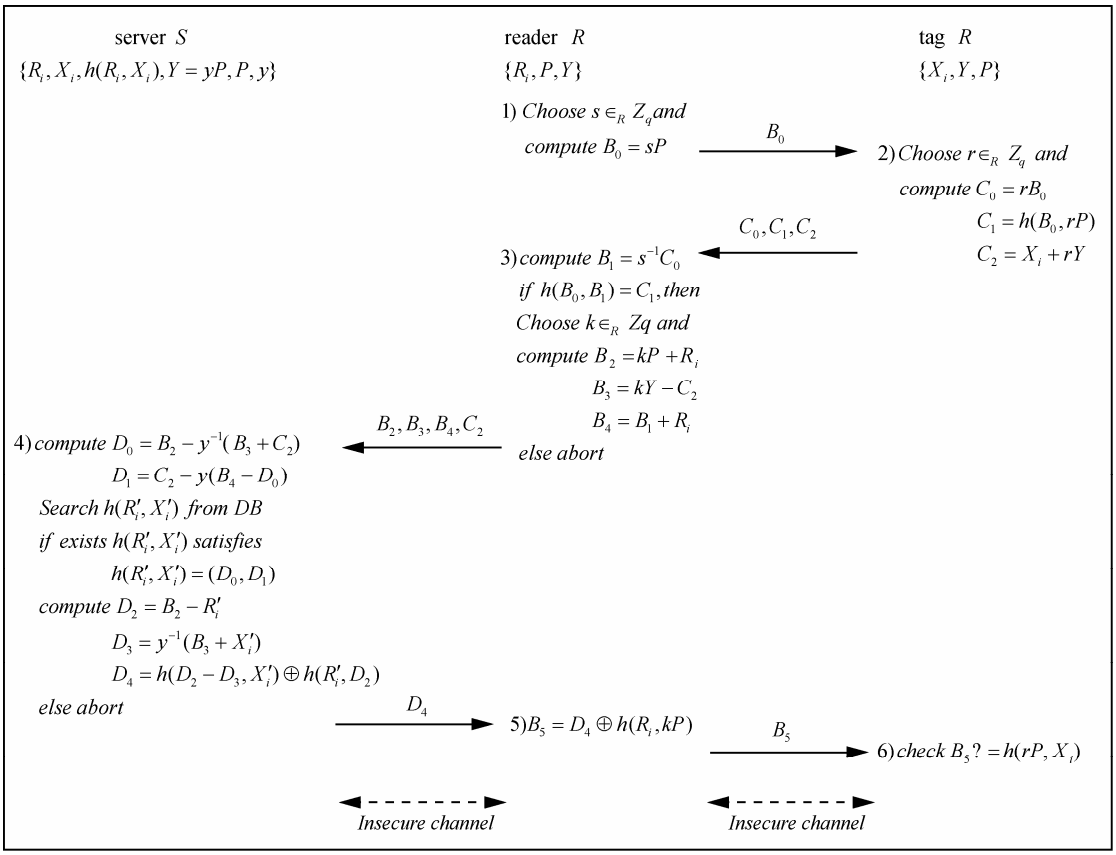

图 1　协议流程

会话。

4) $S \to R$： D_4

后端服务器接收到阅读器的响应消息 B_2， B_3，B_4， C_2 后，进行如下操作。

a) 服务器计算 $D_0 = B_2 - y^{-1}(B_3 + C_2)$， $D_1 = C_2 - y(B_4 - D_0)$，然后求 D_0，D_1 的散列值 $h(D_0, D_1)$。

b) 服务器遍历数据库中 $h(R_i', X_i')$，即移动阅读器与标签的标识对的散列值，然后与上述散列值 $h(D_0, D_1)$ 比对。

c) 如果存在 $h(R_i', X_i') = h(D_0, D_1)$，则后端服务器对标签与阅读器的合法性验证通过，继而计算 $D_2 = B_2 - R_i'$， $D_3 = y^{-1}(B_3 + X_i')$， $D_4 = h(D_2 - D_3, X_i') \oplus h(R_i', D_2)$，然后发送 D_4 给移动阅读器 R。

d) 如果不存在，则验证失败，终止会话。

5) $R \to T$： B_5

移动阅读器收到后端服务器的消息 D_4 后，计算 $B_5 = D_4 \oplus h(R_i, kP)$，然后发送 B_5 给标签。

6) T

标签 T 接收到消息 B_5 后，验证 $B_5 ? = h(rP, X_i)$，若相等，则标签对后端服务器与移动阅读器的验证通过；若不相等，则验证失败。

4 协议分析

本节从安全性证明、安全性分析、性能分析 3 方面对上述协议进行分析。

4.1 安全性证明

定理 1 根据定义 1，本文所提出方案可以保证标签的不可跟踪隐私。

证明 在执行完定义 1 中的游戏 g 之后，敌手 A 获得了协议 P 执行过程中的交互信息 $\{B_0^{(b)}, C_0^{(b)}, C_1^{(b)}, C_2^{(b)}, B_2^{(b)}, B_3^{(b)}, B_4^{(b)}, D_4^{(b)}, B_5^{(b)}\}$，其中来自标签的信息有 $C_0^{(b)}(= r^{(b)} sP)$， $C_1^{(b)}(= h(sP, r^{(b)} P))$， $C_2^{(b)}(= X^{(b)} + r^{(b)} Y)$。敌手 A 想要从获得的交互信息中区分出 T_0 和 T_1，首先需要获得移动阅读器的随机数 s 与标签的随机数 $r^{(b)}$，然后通过 s 和 $r^{(b)}$ 的逆、$C_0^{(b)}$、$C_2^{(b)}$ 去推测出 $X^{(b)}$，但是这在计算上是不可行的。假设可以推导出 $X^{(b)}$，表示敌手 A 能够构造算法 Q 从 $C_0^{(b)}$ 提取出 $r^{(b)} Y(= r^{(b)} yP)$，那么算法 Q 就可以用来解决椭圆曲线离散对数问题（ECDLP），显然这是矛盾的。

定理 2 根据定义 2，本文所提方案可以保证移动阅读器的不可跟踪隐私。

证明 在执行完定义 2 中的游戏 g 之后，敌手 A 获得了协议 P 执行过程中的交互信息 $\{B_0^{(b)}, C_0^{(b)}, C_1^{(b)}, C_2^{(b)}, B_2^{(b)}, B_3^{(b)}, B_4^{(b)}, D_4^{(b)}, B_5^{(b)}\}$，其中，来自于移动阅读器的信息有 $B_2^{(b)}(= k^{(b)} P + R^{(b)})$，$B_3^{(b)}(= k^{(b)} Y - C_2^{(b)})$，$B_4^{(b)}(= rP + R^{(b)})$，$C_2^{(b)}(= X^{(b)} + rY)$。敌手 A 想要从获得的交互信息中区分出移动阅读器 R_0 和 R_1，首先需要知道移动阅读器产生的随机数 k，然后通过 k 的逆、$B_2^{(b)}$、$B_3^{(b)}$ 去推测出 $R^{(b)}$，但是这在计算上是不可行的。假设可以推导出 $R^{(b)}$，表示敌手 A 能够构造算法 Q' 从 $B_3^{(b)} + C_2^{(b)}(= k^{(b)} Y)$ 提取出 $k^{(b)} P$，那么算法 Q' 就可以用来解决椭圆曲线离散对数问题（ECDLP），显然这是矛盾的。

4.2 安全性分析

本文协议建立在椭圆曲线离散对数问题基础上，采用 Edwards 曲线上的点加和标量乘运算，散列运算、异或等实现。在上节中采用可证明安全方法对协议的不可跟踪隐私进行了证明，本节将对协议的安全性进行分析。

1) 标签的匿名性

每个标签 T 中存储有标签的标识 X_i，Edwards 曲线的基准点 P，后端服务器的公钥 Y，在执行协议过程中，敌手 A 通过窃听通信信道，对标签进行跟踪或者获取敏感信息。在标签一方，从标签发出的信息包含 C_0、C_1 和 C_2，由于椭圆曲线上的离散对数问题（ECDLP），要想对 C_0、C_1 和 C_2 进行运算推导出 X_i，在计算上也是不可行的。

2) 标签的位置隐私

与标签相关的交互信息主要是 B_0、C_0、C_1、C_2 和 B_5，由于这些信息的生成都依赖于随机数 s、r，这保证了每轮会话 B_0、C_0、C_1、C_2 和 B_5 的新鲜性。当敌手假冒移动阅读器向标签发送挑战信息时，由于 s、r 由随机数产生器随机产生，这保证了在每轮会话中，标签的回应信息 $C_0(= rsP)$、$C_1(= h(sP, rP))$ 与 $C_2(= X_i + rY)$ 都是新鲜的。

3) 阅读器隐私

在传统的 RFID 认证协议中，阅读器是固定的，仅作为信使传递服务器与标签之间的信息，阅读器不存在隐私保护问题。在移动 RFID 系统中，由于阅读器的不固定性和无线信道的不安全性，协议执行过程中需要保护移动阅读器的隐私，防止阅读器的标识被克隆攻击。

在本文协议的初始化阶段，后端服务器随机选

择 G 上的一个点 R_i 作为移动阅读器的标识，在移动阅读器端，对标签的标识 R_i 进行点加运算 $B_2 = kP + R_i$，敌手 A 通过窃听通信信道获得 $\{B_2, B_3, B_4, C_2\}$，由于椭圆曲线上的离散对数问题（ECDLP），要想从 $B_3 + C_2$ 中提出 kP 再进行运算推导出 R_i，在计算上也是不可行的。

4) 前向安全

敌手 A 无法区分标签 T_i 的过去会话信息，即使通过收买标签获得其当前内存数据。假设标签当前内存单元数据为 $\{X_i, P, Y\}$，标签之前的通信信息用 $\{B_0, C_0, C_1, C_2, B_5\}$ 表示，$B_0 (= sP)$ 由移动阅读器产生的随机数经过 Edwards 曲线的标量乘运算得到，其不能联系到标签当前内存单元 $\{X_i, P, Y\}$。$C_0 (= rsP)$ 同 B_0，不能从标签当前内存单元 $\{X_i, P, Y\}$ 推导出。$C_2 (= X_i + rY)$，其中 rY 同 C_0，仅 X_i 依赖于当前的内存单元数据，所以 C_2 也无法联系到标签内存单元。同理，信息 $C_1 (= h(B_0, rP))$ 与 $B_5 (= h(rP, X_i))$ 都不能由标签当前内存单元 $\{X_i, P, Y\}$ 推导出。因此，敌手 A 无法区分标签 T_i 的过去会话信息。

5) 双向认证

对标签来说，标签接收到响应消息 B_5，可以对后端服务器和移动阅读器进行验证。只有有效的后端服务器才能产生原始的响应消息 $D_4 = h(rP, X_i') \oplus h(R_i', kP)$，有效的阅读器通过异或运算得到 $B_5 = D_4 \oplus h(R_i, kP) = h(rP, X_i')$，然后将 B_5 发送给标签，标签通过 $B_5 ? = h(rP, X_i)$ 对后端服务器和阅读器同时进行了验证。对后端服务器来说，服务器接收到移动阅读器发送的消息 $\{B_2, B_3, B_4, C_2\}$，可以对标签和移动阅读器进行验证，服务器通过自己的私钥计算出 D_0、D_1，然后遍历数据库中 $h(R_i', X_i')$，即移动阅读器与标签的标识对的散列值，与 $h(D_0, D_1)$ 比对。只有有效的标签和移动阅读器才能计算出合法的散列值在后端服务器端通过验证。

6) 重放攻击

敌手 A 通过窃听通信信道，获取标签过去会话信息 $\{C_0 = rsP, C_1 = h(sP, rP), C_2 = X_i + rY\}$。在当前协议执行过程中，$A$ 拦截消息 $\{C_0' = r's'P, C_1' = h(s'P, r'P), C_2' = X_i + r'Y\}$，重放 $\{C_0, C_1, C_2\}$ 给移动阅读器，阅读器接收到重放的信息，计算 $B_1 = s'^{-1} rsP$，可以看出 $h(B_0', B_1') (= h(s'P, s'^{-1} rsP)) \neq C_1 (= h(sP, rP))$，所以重放攻击无效。

7) 假冒攻击

如果敌手 A 假冒标签 T，发送消息给移动阅读器，由于假冒的标签不知道标签标识 X_i，故不能计算出有效的 C_2，其将不可能在服务器端用服务器的私钥解密出有效的标签标识，通过服务器验证。如果敌手 A 假冒移动阅读器 R，同样，假冒的移动阅读器不知道有效阅读器的标识 R_i，也无法计算出有效的 B_2 与 B_4，在服务器端得到有效的移动阅读器标识。如果敌手假冒后端服务器，没有有效的移动阅读器与标签的标识对 $\{R_i, X_i\}$，将不可能得到有效的 D_4 在标签方通过标签的验证。

本文的方案和其他 RFID 认证方案（基于椭圆曲线，非椭圆曲线）就安全性进行比较，比较结果如表 2 所示，通过比较发现本文方案在安全性方面具有明显优势。

表 2　　安全性能比较

安全性能	文献[3]	文献[4]	文献[7]	文献[11]	文献[12]	本文方案
移动 RFID 环境	×	×	×	√	√	√
标签的匿名性	×	×	√	√	√	√
标签的位置隐私	×	×	√	√	√	√
阅读器隐私	×	×	×	×	√	√
前向安全	×	×	×	√	√	√
双向认证	×	×	×	√	√	√
重放攻击	√	√	×	√	×	√
假冒攻击	√	√	√	√	√	√

注：×表示不提供；√表示提供。

4.3　性能分析

本文方案是基于 Edwards 曲线设计的，其适用于移动 RFID 系统。在本文的引言部分提到文献[5,7,10,11]同样采用随机数与椭圆曲线点加与标量乘运算实现，其效率对比如表 3 所示，在这里本文就协议的交互轮数、标签的计算量、标签的存储开销、系统通信开销、服务器的计算量和服务器的搜索成本 6 方面进行对比。计算量的对比只比较 3 种计算量比较大的操作标量乘运算（包含点减操作）、对称密码、散列运算，而忽略其他计算成本低的运算比如随机数产生、点加运算、异或运算等[8]。存储开销和通信开销依赖于协议中散列运算、加解密运算、随机数产生、曲线上点的坐标等采用的位数，这里协议中采用统一的 l 位来表示其长度，由于曲

表 3 效率比较

指标	文献[5]	文献[7]	文献[10]	文献[11]	本文方案
协议执行轮数	4	4	3	7	5
标签的计算量	3M	2M+2E	2M+2H	4M+H	3M+2H
标签的存储开销	$k+l$（$=3l$）	$3k+2l$ ($=8l$)	$3k+l$ ($=7l$)	k ($=2l$)	$3k$ ($=6l$)
系统通信开销	$2k+2l$ ($=6l$)	$2k+3l$ ($=7l$)	$3k+3l$ ($=9l$)	$7k+8l$ ($22l$)	$7k+3l$ ($=17l$)
服务器的计算量	1M+N2M	(bN/a)(2M+1E)	4M+NH	9M+2H	8M+3H
服务器搜索成本	$O(N)$	$O(N)$	$O(N)$	$O(1)$	$O(1)$

注：M（标量乘运算），E（AES 操作），H（散列运算），l（采用位数），k（曲线上的点数）。

线上的点包含横纵坐标，可得到 $1k=2l$。通过对协议交互轮数，标签的计算量和存储开销，系统的通信开销，服务器的计算量和搜索成本进行分析发现，本文方案在扩展性和效率上都具有明显优势。

5 结束语

本文首先给出了移动RFID系统与传统的RFID系统的区别，指出现有的大多数 RFID 认证协议假设性太强，不适用于移动 RFID 应用环境。为了保障移动 RFID 系统中通信的隐私与安全问题，本文在分析已有 RFID 认证协议的基础上，同时考虑 Edwards 曲线群运算效率和安全性优势，提出了一个适用于移动 RFID 系统的基于 Edwards 曲线的安全认证协议，并进一步采用可证明安全方法证明了标签和移动阅读器的不可跟踪隐私，通过安全性分析指出协议能更有效抵抗已有的各种攻击。与现有的结构类似 RFID 认证协议相比，该协议扩展性更好，安全性和性能都优于其他方案。

近场通信 NFC（near field communication）是一种短距离无线通信技术，基于 NFC 的智能终端为解决移动 RFID 系统的硬件实现提供了平台。将本文协议应用基于双线性对的密码学算法库 PBC（pairing-based cryptography）[19]实现，最后部署在 NFC 手机上是下一步研究重点。

参考文献：

[1] JUELS A. RFID security and privacy: a research survey[J]. Selected Areas in Communications, IEEE Journal, 2006, 24(2): 381-394.

[2] LEE H, KIM J. Privacy threats and issues in mobile RFID[A]. Availability, Reliability and Security[C]. 2006. 5.

[3] TUYLS P, BATINA L. RFID-tags for Anti-Counterfeiting[M]. Springer Berlin Heidelberg, 2006.

[4] BATINA L, GUAJARDO J, KERINS T, *et al*. Public-key cryptography for RFID-tags[A]. Pervasive Computing and Communications Workshops, PerCom Workshops' 07 Fifth Annual IEEE International Conference[C]. 2007.217-222.

[5] LEE Y K, BATINA L, VERBAUWHEDE I. EC-RAC (ECDLP based randomized access control): provably secure RFID authentication protocol[A]. RFID, 2008 IEEE International Conference on IEEE[C]. 2008. 97-104.

[6] BATINA L, GUAJARDO J, KERINS T, *et al*. Public-key cryptography for RFID-tags[A]. Pervasive Computing and Communications Workshops PerCom Workshops' 07 Fifth Annual IEEE International Conference[C]. 2007.217-222.

[7] GÓDOR G, GICZI N, IMRE S. Elliptic curve cryptography based mutual authentication protocol for low computational complexity environment[A]. Wireless Pervasive Computing (ISWPC), 2010 5th IEEE International Symposium on IEEE[C]. 2010.331-336.

[8] CHOU J S. An efficient mutual authentication RFID scheme based on elliptic curve cryptography[J]. The Journal of Supercomputing, 2014, 70(1):75-94.

[9] CHEN Y, CHOU J S, LIN C F, *et al*. A novel RFID authentication protocol based on elliptic curve crypto system[J]. IACR Cryptology ePrint Archive, 2011, 2011: 381.

[10] CHOU J S, CHEN Y, WU C L, *et al*. An efficient RFID mutual authentication scheme based on ECC[J]. IACR Cryptology ePrint Archive, 2011, 2011:418.

[11] ZHOU J, ZHOU Y, XIAO F, *et al.* Mutual authentication protocol for mobile RFID systems[J]. Journal of Computational Information Systems, 2012, 8(8): 3261-3268.

[12] NIU B, ZHU X, LI H. An ultralightweight and privacy-preserving authentication protocol for mobile rfid systems[A]. Wireless Communications and Networking Conference (WCNC)[C]. 2013.1864-1869.

[13] 张宝华, 殷新春, 张海灵. Edwards 曲线安全快速标量乘法运算算法——EDSM[J]. 通信学报, 2008, 29(10): 76-81.
ZHANG B H, YIN X C, ZHANG H L. EDSM: secure and efficient scalar multiplication algorithm on Edwards curves[J]. Journal on Communications, 2008, 29(10):76-81.

[14] CORON J S. Resistance against differential power analysis for elliptic curve cryptosystems[A]. Cryptographic Hardware and Embedded Systems[C]. Springer Berlin Heidelberg, 1999.292-302.

[15] BATINA L, HOGENBOOM J, MENTENS N, *et al*. Side-channel evaluation of FPGA implementations of binary Edwards curves[A]. Electronics, Circuits, and Systems (ICECS), 2010 17th IEEE International Conference[C]. 2010.1248-1251.

[16] CHATTERJEE A, SENGUPTA I. Design of a high performance binary Edwards curve based processor secured against side channel analysis[J]. Integration, the VLSI Journal, 2012, 45(3): 331-340.

（下转第 145 页）