doi:10.11959/j.issn.1000-436x.2017174

大规模 RFID 系统中基于 CPK-ECC 的双向认证协议

潘耀民[1,2]，单征[1,2]，戴青[1,2]，岳峰[1,2]
（1. 解放军信息工程大学网络空间安全学院，河南 郑州 450001；2. 数学工程与先进计算国家重点实验室，河南 郑州 450001）

摘 要：针对现有射频识别（RFID, radio frequency identification）认证协议扩展性较差的问题，分析了大规模 RFID 系统认证协议的设计需求与 CPK 的技术优势，提出基于 CPK-ECC 的认证协议。协议采用椭圆曲线加密方案与改进的快速数字签名算法，实现了双向认证与离线认证。进一步给出安全性分析，指出协议可以有效抵御已有安全与隐私攻击。与其他基于 ECC 的认证协议相比，协议支持无后端服务器认证，扩展性好，性能更优，适用于大规模 RFID 系统。

关键词：射频识别；认证协议；组合公钥；无后端服务器；扩展性
中图分类号：TP309.1 **文献标识码**：A

CPK-ECC based mutual authentication protocol for large-scale RFID system

PAN Yao-min[1,2], SHAN Zheng[1,2], DAI Qing[1,2], YUE Feng[1,2]
（1. College of Cyberspace Security, PLA Information Engineering University, Zhengzhou 450001, China;
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China）

Abstract: The existing RFID authentication protocols were short of scalability. Taking advantage of combined public key(CPK), a CPK-ECC based authentication protocol was proposed considering the design demand of authentication protocols for large-scale RFID system. The protocol implements mutual and serverless authentication by adoption of the elliptic curve encryption scheme and the improved digital signature algorithm. Based on the security analysis, the protocol can resist the existing security and privacy attacks effectively. Compared with other ECC-based protocols, the serverless protocol has better scalability and performance, suitable for large-scale RFID systems.

Key words: RFID, authentication protocol, combined public key, serverless, scalability

1 引言

随着全球物联网产业的快速发展，无线射频识别技术已广泛应用于物流、交通、医药以及工业制造等诸多领域。然而，由于标签设计简单、造价低廉，RFID 系统也面临着严峻的安全与隐私威胁。采用逻辑运算、伪随机函数、散列运算以及对称加密算法等成本相对较低的操作来设计 RFID 认证协议，可以从一定程度上解决 RFID 系统的安全隐私问题。近年来，RFID 技术的广泛应用和不同系统之间的资源共享，使 RFID 系统管理的标签数目剧增。在标签数目巨大的大规模 RFID 系统中，认证协议面临的对称密钥管理难题愈加突出[1]。采用公钥密码体制（PKC, public key cryptosystem）解决 RFID 安全问题已成为必然趋势。在 PKC 中，当安全性能相同时，椭圆曲线密码（ECC, elliptic curve crypto）体制具有密钥长度短，计算速度快，占用带宽小等优势。因此，在文献[2,3]的识别方案被应用于 RFID 以来，ECC 逐渐成为 RFID 认证协议设计的一个热点。

2008 年，Lee 等[4]分析了 Schnorr 识别方案与 Okamoto 识别方案的不足，指出二者均不能抵抗位置隐私、前向隐私等攻击，且扩展性较差，提出了 EC-RAC 协议，引起了广泛关注。Lee 等[5,6]采用标

收稿日期：2016-11-29；**修回日期**：2017-04-18
基金项目：国家自然科学基金资助项目（No.61472447）
Foundation Item: The National Natural Science Foundation of China (No.61472447)

识传递、密钥传递与服务器认证三者独立设计，组合形成完整认证协议的方法，又提出了 3 个 EC-RAC 改进版本，但均被指出不能抵抗隐私攻击[7,8]。2011 年，Chou 等[7]提出了一个基于 ECC 与散列函数结合的双向认证协议。协议认证过程不涉及求逆运算，减少了计算量，但容易受到中间人攻击。2013 年，Liao 等[8]分析了安全性问题，提出了一个基于 ECC 的 RFID 双向认证协议，并证明了协议的安全性。然而，Zhao[9]指出该协议容易被推演出标签私钥，在该协议基础上进行了改进，提出了新的 RFID 认证协议，但仍无法保证隐私安全性。2014 年，杨玉龙等[10]针对移动 RFID 系统中阅读器与标签均需要保证隐私安全的特殊要求，提出了一种适用于移动阅读器认证的安全认证协议，并进行了隐私安全性证明，但服务器需要遍历数据库中的散列值，扩展性并没有得到有效提升。

上述认证方案存在 2 个共同的问题：1) 都将服务器公钥预存在标签中，协议过程需要认证服务器参与，高度依赖通信网络的稳定性；2) 认证过程都需要搜索匹配密钥对，失去了 PKC 的密钥管理优势，扩展性较差。2008 年，针对无后端服务器认证问题，Tan 等[11]利用随机数生成、散列函数等基本操作，引入第三方认证实体和标签接入表机制，首次提出一个无服务器参与的 RFID 认证协议。然后，针对基于逻辑运算、散列函数、随机数生成等操作的轻量级无后端服务器认证协议，许多研究者都进行了深入研究。但基于 PKC 的无后端服务器认证协议没有较为成熟的解决方案。2007 年，Burmester 等[12]指出在匿名性要求下，采用对称密钥技术不可避免地要先将标签与密钥对应。大规模 RFID 系统中密钥查找问题极为耗时，只有公钥技术能够保证较高隐私安全性的同时，查找复杂度也保持在常量。2013 年，Liu 等[13]综合公钥基础设施（PKI）与基于身份的加密方案（IBE）的优势，提出了一种混合型物联网安全传输机制，在传输层与感知层分别采用 PKI 与 IBE 技术，实现整个物联网系统的数据安全传输。2015 年，张兵等[14]提出一种基于 PKI 与组合公钥（CPK）的混合密钥管理方案，在系统后端采用 PKI，在读写器与标签之间采用 CPK，实现身份认证和加密传输服务。但要建立起 2 种机制，实施较为复杂，也造成了资源浪费。

本文分析了大规模 RFID 系统中认证协议的设计需求与 CPK-ECC 的优越性，提出了一个隐私安全的 RFID 双向认证协议，并对协议的安全性与性能进行分析。协议实现了无后端服务器认证，有效避免了标签对应密钥查找过程。与现有基于 ECC 的认证协议相比，扩展性较好，安全性更高，适用于标签大规模部署与多系统协同运行。

2 准备知识

2.1 大规模 RFID 系统认证协议的设计需求

通常，RFID 系统由电子标签、读写器与后端服务器等实体组成，如图 1 所示。读写器与标签之间利用射频信号进行无线通信，容易受到窃听、假冒等攻击；读写器与后端服务器之间采用传统的计算机网络通信，面临着传统计算机网络带来的威胁。随着信息化和工业化融合不断深入，网络化的 RFID 系统被部署在生产、物流、销售、售后等产品生命全过程，跨系统的资源共享服务需求日趋明显，系统规模也随着管理标签数目不断增长。服务器与阅读器之间的计算机网络，由单一的有线专网向专网与公网交叉的复杂网络转变。

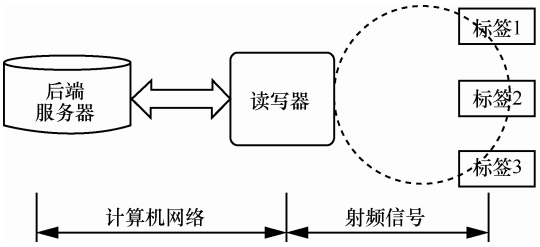

图 1 RFID 系统基本原理

现有基于 PKC 的 RFID 安全认证协议通常是标签、读写器与服务器的三者共同参与，并假定读写器与服务器之间的传输是安全的。在大规模 RFID 系统应用环境下，这种设计显然是不合理的。首先，复杂的计算机通信网络带来的传输时延难以保证认证的实时性，而建立专用网络会产生巨大成本；其次，传统计算机网络面临的安全威胁对认证协议的安全有极大影响，假设其安全是不合理的。设计无后端服务器参与的安全协议，可以实现快速认证，减少中间传输环节，从而可以有效减少网络延迟带来的时间消耗，消除计算机网络脆弱性对认证协议带来的威胁。

综上，针对大规模 RFID 系统安全认证协议的设计需求，本文可以通过以下几个方面进行描述。

1) 协议功能

协议的功能方面主要是实现双向认证与无后

端服务器认证。双向认证在保证阅读器与标签合法的同时，可以有效阻止攻击者对标签的非法访问。无后端服务器认证减少了中间环节，既消除了传统计算机网络带来的安全威胁，又有效降低了协议时延，有利于协议扩展。

2) 安全性

协议安全性是保证协议有效抵抗已知攻击，如假冒攻击、重放攻击、拒绝服务攻击以及中间人攻击等。本文假定攻击者可以通过窃听获取无线传输过程中所有的信息，也可以伪造消息，用以欺骗阅读器或标签。攻击者可以通过破坏标签或阅读器获得其内部信息，但被破坏的设备不能再进行通信。

3) 标签隐私性

标签隐私性包括匿名性以及位置隐私。标签匿名性是指攻击者无法确定标签的标识，主要保护标签的身份标识不被泄露。位置隐私是指攻击者无法判定 2 次会话对应的标签是否为同一标签，从而保证标签无法被追踪。本文对阅读器的隐私不做考虑。

4) 协议性能

协议的性能主要体现在认证过程的计算效率、计算成本、通信量、存储量以及扩展性等方面。计算效率是指协议双方的计算量；计算成本则由协议所需的计算部件复杂程度决定；通信量包括协议通信交互轮数以及传输信息量这 2 个方面；存储量是指为了完成协议所需的最小存储空间；扩展性是指随着标签数量增加协议的适用性变化，突出表现在协议搜索成本上。在现有的 RFID 系统中，阅读器的计算能力一般较强，协议性能瓶颈主要在计算资源有限的标签上。安全认证协议成本必须足够低以满足 RFID 系统的特殊需求。

2.2 基于椭圆曲线的组合公钥体制（CPK-ECC）

参数 $T=\{a, b, P, n, q\}$ 确定了一条定义在有限域 F_q 上的椭圆曲线 $E: y^2 \equiv x^3+ax+b$。其中，a,b 是系数，$a,b,x,y \in F_q$，$q \neq 2,3$ 为一大整数，P 为加法群的基点，n 是以 P 为基点的加法群的阶。令任意小于 n 的整数 r 为私钥，则 $R=rP$ 为对应公钥。

ECC 具有复合特性，即任意多对私钥之和与对应的公钥之和构成新的公、私钥对。设私钥之和为 $r=(r_1+r_2+\cdots+r_m) \bmod n$，对应公钥点加之和为 $R=R_1+R_2+\cdots+R_m$，那么 r 与 R 正好形成新的公、私钥对。根据这一特性，CPK 构建私钥矩阵 ***SSK*** 与公钥矩阵 ***PSK*** 如式(1)和式(2)所示。

$$\boldsymbol{SSK}=\begin{bmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,t} \\ r_{2,1} & r_{2,2} & \cdots & r_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ r_{s,1} & r_{s,2} & \cdots & r_{s,t} \end{bmatrix} \tag{1}$$

$$\boldsymbol{PSK}=\begin{bmatrix} R_{1,1} & R_{1,2} & \cdots & R_{1,t} \\ R_{2,1} & R_{2,2} & \cdots & R_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ R_{s,1} & R_{s,2} & \cdots & R_{s,t} \end{bmatrix} \tag{2}$$

SSK 中的元素 $r_{i,j}$ 与 ***PSK*** 中对应的元素 $R_{i,j}$ 互为公、私钥对。***SSK*** 由密钥管理中心（KMC）保管，***PSK*** 属于公开信息。对实体标识进行散列运算、置换等操作，CPK 可以确定一组个数为 $u(1 \leqslant v \leqslant u)$ 的密钥对序列。KMC 按照式(3)可以计算得到实体私钥，通信实体按照式(4)可以计算得到公钥。详细过程参见文献[15]。

$$SK=\sum_{v=1}^{u} r_{i_v,j_v} \tag{3}$$

$$PK=\sum_{v=1}^{u} R_{i_v,j_v} \tag{4}$$

CPK-ECC 机制将实体身份标识与密钥联系起来，通信时获得对方标识便可自行计算得到公钥，不再需要第三方就可对实体公钥进行认证，一次性完成了公钥的传递与认证，大大简化了密钥管理的难度。同时，少量的密钥因子组合后就可以得到数量庞大的密钥对，适用于大规模应用环境。

3 基于 CPK-ECC 的 RFID 认证协议

协议分为初始化和认证 2 个阶段。协议所使用的系统参数解释如表 1 所示。标签的存储空间为 {ID_T, SK_T, ***PSK***, P, n}，阅读器的存储空间为{ID_R, SK_R, ***PSK***, P, n}，攻击者的存储空间{ ***PSK***, P, n}。

表 1　　系统参数

符号	定义
PSK	公钥矩阵列
SK_T	标签的私钥
SK_R	阅读器的私钥
$PK_T(=SK_TP)$	标签的私钥
$PK_R(=SK_RP)$	阅读器的私钥
ID_T	标签标识，这里是散列运算后的值
ID_R	阅读器标识，这里是散列运算后的值
P	椭圆曲线上阶为 n 的基点
n	一个大素数

3.1 初始化阶段

在此阶段中，所有参与协议的实体进行内存单元初始化。ECC 体制的建立和密钥矩阵的生成由 KMC 完成。实体的密钥不再由自身随机生成，而是由发布代理通过安全信道从 KMC 获得对应阅读器和标签的 CPK 证书，然后以面对面的方式将 $\{ID_{\mathrm{R}}, SK_{\mathrm{R}}, \boldsymbol{PSK}, P, n\}$ 和 $\{ID_{\mathrm{T}}, SK_{\mathrm{T}}, \boldsymbol{PSK}, P, n\}$ 分别注入阅读器和标签，并立即将 CPK 证书销毁，确保密钥不被泄露。阅读器与标签使用相同的公钥计算函数 $f(\,)$，以实体标识 ID 为输入，利用 ***PSK*** 获得对应于实体标识 ID 的公钥。

3.2 认证阶段

在认证阶段，标签收到阅读器发来的激活信号后，开启协议认证流程。协议认证的流程如图 2 所示，详细描述如下。

1) 标签→阅读器： R_1

标签生成随机数 $k_1 \in [1, n-1]$，计算 $R_1 (= k_1 P)$，取 R_1 的横坐标模 n 可得 r_1。若 r_1 不为 0，则将其给阅读器，否则重新选择随机数进行计算。

2) 阅读器→标签： S, R_2, ID_{R}

阅读器收到标签发来的 R_1，取 R_1 的横坐标模 n 可得 r_1'。生成随机数 $k_2 \in [1, n-1]$，计算 $R_2 (= k_2 P)$。若 R_2 的横坐标模 n 不为 0，则继续，否则重新选择随机数。接着计算 $R_3 (= k_2 R_1)$、$R_4 (= SK_{\mathrm{R}} R_1)$、$S (= R_3 + R_4)$，分别取 R_3 和 R_4 的横坐标模 n 得 m 和 r_2。将 S、R_2 和阅读器的标识 ID_{R} 一起发送给认证标签。

3) 标签→阅读器： c, s

标签收到阅读器发来的消息，根据 ID_{R} 使用 $f(\,)$ 快速获得阅读器的公钥 PK_{R}。然后，计算 $R_3' (= k_1 R_2)$，$R_4' (= k_1 PK_{\mathrm{R}})$，验证 $S = R_3' + R_4'$ 是否成立。若成立，标签认定阅读器合法，分别取 R_3' 和 R_4' 的横坐标模 n 得 m' 和 r_2'，计算 $c (= r_2' \oplus ID_{\mathrm{T}})$ 和 $S (= k_1 - m' - r_1 SK_{\mathrm{T}} (mod\ n))$，并将二者发送给阅读器。否则，标签拒绝会话，协议终止。

4) 阅读器验证

阅读器收到标签发来的消息 c、s 后，将 c 与步骤 2)中的 r_2 按位模 2 加可得标签的标识 ID_{T}，然后，根据 ID_{T} 使用 $f(\,)$ 快速获得标签的公钥 PK_{T}。然后计算点 $R_1' (= (s+m)\ (mod\ n) P + r_1' PK_{\mathrm{T}})$，取 R_1' 的横坐标模 n，验证所得值是否与 r_1' 相等。若相等，则阅读器认定标签合法；否则，阅读器拒绝会话，协议终止。

4 安全分析与性能比较

本节给出协议的安全性分析，并与部分已有基于 ECC 的 RFID 认证协议的性能进行比较。为了方便分析，可以将所提出的协议划分成阅读器认证和标签认证 2 个部分。假设协议中所用随机数生成器为 l 位真随机数生成器，则随机数生成器产生特定随机数 j 的概率为 $P(j) = \dfrac{1}{2^l}$。

4.1 阅读器认证

在设计阅读器认证时，本文主要解决的是阅读器非法访问标签的问题，对阅读器隐私不做要求。阅读器认证流程如图 3 所示。阅读器认证的安全性是建立在椭圆曲线计算性 Diffie-Hellman 难题（ECCDH）的基础上的。

1) 防假冒攻击

由于解决 ECCDH 是困难的，所以对于给定 R_1、R_2，求解 R_3 是困难的。实体私钥只存在于自身的物理芯片中，在不损坏实体设备时，攻击者难以

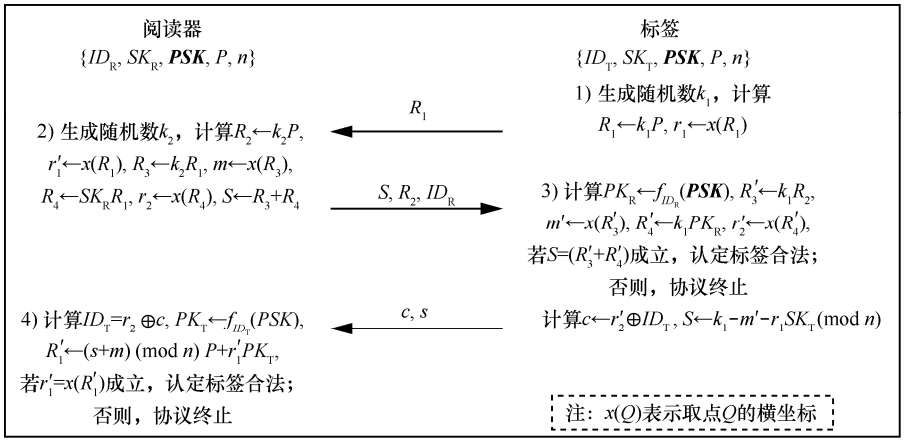

图 2 协议认证流程

获得 SK_R，所以在给定 R_1 时，求解 R_4 是困难的。在 R_3, R_4 未知时，求解 S 是困难的。因此假冒阅读器访问标签是困难的。

2) 防重放攻击

攻击者在获得来自标签的请求 $R_1^{(1)}$ 后，将以前窃听获得的 S, R_2, ID_R 发送给标签。标签收到信息后生成随机数 $k_1^{(1)}$ 计算验证 $S = k_1^{(1)}(R_2 + PK_R)$ 是否成立。如果此式成立，必有 $k_1(R_2 + PK_R) = k_1^{(1)}(R_2 + PK_R)$。由于标签产生的随机数 $k_1, k_1^{(1)} \in [1, n-1]$，所以必有 $k_1 = k_1^{(1)}$。对于确定的 k_1，$P(k_1^{(1)} = k_1) = \frac{1}{2^l}$，即重放攻击成功的概率为 $\frac{1}{2^l}$，可以忽略不计。所以，协议可以抵御重放攻击。

4.2　标签认证

相比阅读器，标签的安全与隐私要求较高。标签认证的流程如图 4 所示。标签认证算法主要由椭圆曲线加密（ECES）方案和快速椭圆曲线数字签名算法 T-ECDSA[15]组成。标签认证的安全性也建立在二者安全基础之上。

1) 标签的匿名性

从标签发出的信息有 R_1、c、s。ECES 被证明在选择明文攻击下是语义安全的，从而攻击者不可能计算出 ID_T。T-ECDSA[16]可以保证与经典 ECDSA 算法具有相同的安全性，所以攻击者无法伪造签名，也无法通过签名计算出 SK_T。

2) 标签的位置隐私

在认证过程中，攻击者可以窃听得到的信息有 R_1、R_2、ID_R、c、s。攻击者假冒阅读器向标签发送挑战信息时，随机数 k_1 保证了 R_1、c、s 是新鲜的。攻击者无法从协议获得的信息中得到固定的输出，从而保证了标签的位置隐私。

3) 前向安全

即使获取了标签当前的内存数据，攻击者也无法区分标签以前的会话信息。假设攻击者获取了标签当前的内存信息用 $\{ID_T, SK_T, \boldsymbol{PSK}, P, n\}$ 表示，标签之前的对话参数用 $\{R_1, k_1, m', r_2', c, s\}$ 表示。由于椭圆曲线上的离散对数问题（ECDLP），攻击者难以通过计算得到 k_1，也就无法得到 m'。在二者未知的情况下，攻击者无法区分标签以前的会话信息。

4) 抗假冒攻击

由 ECES 与 T-ECDSA 的安全性可知，求解 ID_T 与 SK_T 是困难的。在 ID_T 和 SK_T 未知情况下，求解匹配的 c, s 是困难的。因此假冒标签是困难的。

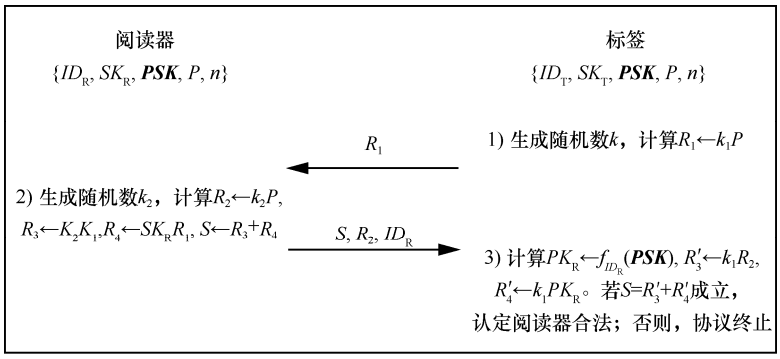

图 3　阅读器认证流程

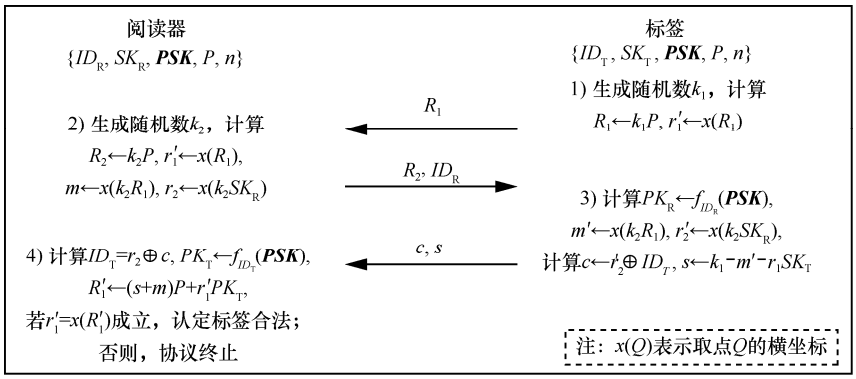

图 4　标签认证流程

5) 抗重放攻击

在以前的标签认证过程中，攻击者通过窃听获得信息 R_1,c,s。攻击者伪装标签向阅读器发送请求 R_1。阅读器生成随机数 $k_2^{(1)}$，计算可得对应的 $R_2^{(1)}$ 和 $m^{(1)}$ 并回应攻击者的请求。获得响应 $R_2^{(1)},ID_R$，然后将 c,s 发送给阅读器。阅读器收到信息后计算可得 PK_T，进行计算验证 $R_1=(s+m^{(1)})P+r_1'PK_T$ 是否成立。如果此式成立，必有 $(s+m)P+r_1'PK_T=(s+m^{(1)})P+r_1'PK_T$，进而 $k_1k_2P=k_1k_2^{(1)}P$。由于实体产生的随机数 $k_1,k_2,k_2^{(1)}\in[1,n-1]$，所以必有 $k_2=k_2^{(1)}$。对于确定的 k_2，$P(k_2=k_2^{(1)})=\frac{1}{2^l}$，即重放攻击成功的概率为 $\frac{1}{2^l}$，可以忽略不计。所以，协议可以抵御重放攻击。

4.3 性能比较

与其他基于 ECC 的 RFID 认证方案相比，在安全性与隐私性方面，本文提出的协议具有明显优势，比较结果如表 2 所示（其中，×表示不提供；√表示提供）。

在计算效率与计算成本方面，这里主要比较耗时的标量乘运算、点加运算、模逆运算、模乘运算和散列运算等 5 种操作，忽略其他较为简单的运算，如随机数的产生运算、异或运算、模加运算等。用 T_{EM}、T_{EA}、T_{INV}、T_M、T_H 分别表示标量乘运算、点加运算、模逆运算、模乘运算和散列运算的耗时。根据文献[17]，当 $q=2^{163}$，基点 P 选定时，假定 $T_{INV}\approx 8T_M$，而平方运算由于效率较高可忽略不计，以仿射坐标形式进行曲线上点的计算，可以得到 $T_{EM}\approx 1\,220T_M$，$T_{EA}\approx T_{INV}+2T_M\approx 10T_M$。

这里主要通过比较协议的所有会话传输次数和数据传送量以反映通信开销。通信开销与存储开销依赖于协议中随机数、曲线上点的坐标、实体标识等采用的长度。这里统一用 l 表示存储长度。由于曲线上的点包含横纵坐标，所以点的存储长度为 $2l$。另外，为了说明协议的扩展性，这里也对搜索成本进行了比较，用 N 表示系统中标签的总数。具体的性能比较如表 3 所示。

通过比较分析可以发现，协议增加较小的标签存储开销，换来了计算开销、通信开销等方面的减小，且无需散列运算，降低了计算成本。同时，协议过程实现了公钥的实时传递与认证，不再需要耗时的查找过程，具有良好的扩展性。

5 结束语

大规模 RFID 系统应用环境下，设计认证协议时，不只要考虑安全与隐私问题，还必须充分考虑到标签的资源限制以及协议的扩展性。本文在分析已有 RFID 认证协议的基础上，指出现有基于 PKC 的 RFID 认证协议假设要求过高，也未能充分利用 PKC 的密钥管理优势，扩展性较差。为了满足大规模 RFID 系统应用的安全与隐私需求，本文利用

表 2 安全性比较

方案	标签匿名性	标签位置隐私	前向安全	双向认证	假冒攻击	重放攻击	大规模环境
EC-RAC IV[6]	√	×	×	×	√	√	×
文献[8]方案	√	×	×	√	×	×	×
文献[9]方案	√	×	×	√	√	×	×
文献[10]方案	√	√	√	√	√	√	×
本文方案	√	√	√	√	√	√	√

表 3 性能比较

方案	传输次数	标签计算量	总计算量	标签存储开销	通信开销	搜索成本
EC-RAC IV[6]	6	$5T_{EM}+2T_{EA}+3T_M\approx 6\,123T_M$	$10T_{EM}+4T_{EA}+3T_{INV}+4T_M\approx 12\,268T_M$	$4l$	$18l$	$o(N)$
文献[8]方案	6	$5T_{EM}+3T_{EA}\approx 6\,130T_M$	$10T_{EM}+6T_{EA}\approx 12\,260T_M$	$5l$	$16l$	$o(N)$
文献[9]方案	6	$5T_{EM}+3T_{EA}+2T_M\approx 6\,132T_M$	$10T_{EM}+6T_{EA}+4T_M\approx 12\,264T_M$	$5l$	$16l$	$o(N)$
文献[10]方案	5	$3T_{EM}+T_{EA}+2T_H\approx 3\,670T_M+2T_H$	$10T_{EM}+11T_{EA}+2T_{INV}+6T_H\approx 12\,326T_M+6T_H$	$4l$	$17l$	$o(N)$
本文方案	3	$3T_{EM}+uT_{EA}+T_M\approx(3\,661+10u)T_M$	$8T_{EM}+(2u+1)T_{EA}+T_M\approx(9\,771+2u)T_M$	$2l+2l\times s\times t$	$9l$	$o(1)$

CPK-ECC 机制一次性完成公钥传递与认证的优势，提出了一个无后端服务器的安全认证协议，并进一步通过安全性分析指出协议可以有效抵抗已有的各种攻击。与现有基于 ECC 的认证协议相比，该协议安全性和性能更优，无需密钥查找，扩展性较好，适用于大规模部署的 RFID 系统。由于条件有限，本文提出的认证协议并未结合硬件系统具体实现。下一步工作的重点是在具体的应用环境中验证与改进协议功能，以期该协议真正在 RFID 系统中得到应用。

参考文献：

[1] HEIN D, WOLKERSTORFER J, FELBER N. ECC is ready for RFID–a proof in silicon[C]//Selected Areas in Cryptography. Springer Berlin Heidelberg. 2008: 401-413.

[2] TUYLS P, BATINA L. RFID-tags for anti-counterfeiting[C]//Crypto Topics in Cryptology. 2006:115-131.

[3] BATINA L, GUAJARDO J, KERINS T, et al. Public-key cryptography for RFID-tags[C]//International Workshop on Pervasive Computing & Communication Security-PERSEC. 2007: 217-222.

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

[5] YONG K L, BATINA L, VERBAUWHEDE I. Untraceable RFID authentication protocols: revision of EC-RAC[C]//IEEE International Conference on RFID. 2009:178-185.

[6] YONG K L, BATINA L, SINGELÉE D, et al. Wide-weak privacy-preserving RFID authentication protocols[M]. Mobile Lightweight Wireless Systems, Springer Berlin Heidelberg, 2010:254-267.

[7] 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.

[8] LIAO Y P, HSIAO C M. A secure ECC-based RFID authentication scheme using hybrid protocols[M]. Advances in Intelligent Systems and Applications-Volume 2, 2013:1-13.

[9] ZHAO Z. A Secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem[J]. Journal of Medical Systems, 2014, 38(5):1-7.

[10] 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):132-138.
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):132-138.

[11] TAN C C, SHENG B, LI Q. Secure and serverless RFID authentication and search protocols[J]. IEEE Transactions on Wireless Communications, 2008, 7(4):1400-1407.

[12] BURMESTER M, MEDEIROS B D, MOTTA R. Robust, anonymous RFID authentication with constant key-lookup[C]//ACM Symposium on Information, Computer and Communications Security. 2008: 283-291.

[13] YANG L, YU P, BAILING W, et al. IOT secure transmission based on integration of IBE and PKI/CA[J]. International Journal of Control & Automation, 2013, 6(2):245-253.

[14] 张兵, 秦志光, 万国根. 基于 PKI 和 CPK 的 RFID 系统混合密钥管理机制研究[J]. 电子科技大学学报, 2015, 44(3):415-421.
ZHANG B, QIN Z G, WAN G G. Study on hybrid key management mechanisms of RFID system based on PKI and CPK[J]. Journal of University of Electronic Science and Technology of China, 2015, 44(3): 415-421.

[15] 南相浩. CPK 公钥体制与标识鉴别[M]. 北京：电子工业出版社, 2012.
NAN X H. CPK Cryptosystem and identity authentication[M]. Beijing: Publishing House of Electronics Industry, 2012.

[16] 高伟, 张国印, 王欣萍, 等. 一种改进的椭圆曲线数字签名算法[J]. 黑龙江大学自然科学学报, 2010, 27(3):775-780.
GAO W, ZHANG G Y, WANG X P, et al. An improved elliptic curve digital signature algorithm[J]. Journal of Natural Science of Heilongjiang University, 2010, 27(3): 775-780.

[17] HANKERSON D, MENEZES A, VANSTONE S. Guide to elliptic curve cryptography[M]. Guide to elliptic curve cryptography, Springer Berlin Heidelberg, 2004.

作者简介：

潘耀民（1993-），男，河南新乡人，解放军信息工程大学硕士生，主要研究方向为网络安全、物联网安全。

单征（1977-），男，辽宁沈阳人，博士，解放军信息工程大学副教授、硕士生导师，主要研究方向为先进计算、网络安全。

戴青（1963-），男，辽宁沈阳人，解放军信息工程大学副教授、硕士生导师，主要研究方向为网络安全、物联网安全和高性能计算。

岳峰（1985-），男，山西长治人，博士，解放军信息工程大学讲师，主要研究方向为高性能计算与信息安全。