文章编号：2095-4980(2017)01-0104-07

基于零知识证明的多实体 RFID 认证协议

白　煜[1a]，滕建辅[1b]，张立毅[1a,2]，刘彦龙[1a]

(1.天津大学 a.电气自动化与信息工程学院；b.微电子学院，天津 300072；2.天津商业大学 电子信息工程学院，天津 300134)

摘　要：物联网的发展对射频识别(RFID)系统的安全性能提出了越来越高的要求。虽然基于密钥阵列的 RFID 认证协议解决了传统 RFID 认证协议在多实体环境中存在的内部攻击问题，但基于交换实体身份信息的认证方式存在信息泄露的安全隐患。针对这一问题，设计了基于零知识证明的多实体 RFID 认证协议(MERAP)。该协议采用分布式密钥阵列抵御内部攻击，利用零知识证明方案实现双向认证时敏感身份信息零泄露。性能分析结果显示，MERAP 协议在维持一定复杂度和标签成本的基础上，可抵抗包括重传、跟踪、拒绝服务和篡改等多种外部攻击和内部攻击。

关键词：射频识别；内部攻击；零知识证明；密钥阵列；多实体

中图分类号：TN911.23；TP309　　**文献标志码：**A　　**doi：**10.11805/TKYDA201701.0104

Multiple entities RFID authentication protocol based on zero-knowledge proof

BAI Yu[1a]，TENG Jianfu[1b]，ZHANG Liyi[1a,2]，LIU Yanlong[1a]

(1a.School of Electronic and Information Engineering；1b.School of Microelectronics，Tianjin University，Tianjin 300072，China；
2.College of Information Engineering，Tianjin University of Commerce，Tianjin 300134，China)

Abstract：As the development of the Internet of Things(IOT), the security requirements of information for Radio Frequency Identification(RFID) system are increasing continuously. Although the RFID authentication protocols based on key array can solve the internal attack problem that is a security flaw of traditional RFID authentication protocols in the multiple entities environment, those protocols can cause the information leakage because they adopt the mechanism of switching entity information during authentication. To tackle with this problem, a Multiple Entities RFID Authentication Protocol(MERAP) based on zero-knowledge proof is designed. The protocol employs distributed key array structure to resist inner attack, and utilizes the zero knowledge proof scheme to realize the zero leakage sensitive of bidirectional authentication information. The security performance analysis results show the MERAP protocol can resist varied external attacks, including retransmission, tracking, denial of service and tampering, and internal attack with a slight increase at complexity and tag cost.

Keywords：Radio Frequency Identification；internal attack；zero-knowledge proof；key array；multiple entities

随着射频识别(RFID)技术的大范围应用，RFID 系统的网络化也成为一种趋势[1]。如物联网一般由众多参与公司构成，每个参与公司称为一个实体，其中每个实体都拥有各自的服务器和阅读器，组成多实体 RFID 系统。在该系统中，由于标签冲突、成本和贴附空间等限制，不可能在同一件货物上为每个实体配置专属的电子标签。因此，在多实体 RFID 系统，每件货物仅贴附一个电子标签供多个实体共享，是唯一可行的方式[2]。该系统中的标签可被分属于不同实体的阅读器读取。

由于参与公司间存在商业利益竞争，使得这种多实体读取同一标签的 RFID 系统引发新的安全问题，即内部攻击。内部攻击是指来自系统内部合法成员的攻击，其目的在于获得或篡改其他参与公司的保密数据[2-4]。传统的 RFID 协议都是针对单一实体系统，当它们被应用到多实体系统时，难以抵抗内部攻击[5]。针对 RFID 系统存在的内部攻击问题，2009 年 Ding 等[6]提出了密钥阵列方案，该方案利用密钥阵列之外的共享密钥来抵抗外部攻击，利用密钥阵列为每一对阅读器和标签提供唯一的会话密钥；2011 年，NING H.等[2]提出了基于分布式密钥阵列的 RFID 认证协议，在解决内部攻击问题的同时扩展了认证协议的适用范围；2014 年，JIANG Yi 等[7]提出了

收稿日期：2015-11-05；修回日期：2015-12-07

基于分组的密钥阵列协议，该协议在密钥阵列方案的基础上将若干个标签和阅读器组成一个组，组内成员会话时使用同一密钥。该方案解决了密钥阵列协议扩展性差的缺点，适用于大规模的 RFID 系统，但是组内成员需要特殊的身份验证，否则难以避免组内成员之间的内部攻击。

上述协议中通信双方通过交换实体身份标识的方式确认对方的合法身份，属于非零知识认证，易泄露实体的隐私或保密数据。2011 年，LIU H.等[8]针对单一实体 RFID 系统，设计了基于零知识证明的 RFID 认证协议，实现了单一实体环境下的零知识认证。文献[9]和文献[10]也对零知识证明理论在 RFID 系统的应用进行了研究。2014 年，Saravanan Sundaresan 等[11]利用基于二次剩余的概率加密算法实现了零知识 yoking 协议，该协议适用于 EPC 标准。2015 年，Saravanan Sundaresan 等[12]利用伪随机数和二次剩余实现了零知识系统。但这些协议均为单一实体环境下的 RFID 认证协议，当应用于多实体环境时，均存在内部攻击漏洞。综上所述，本文将零知识证明理论引入密钥阵列认证协议，设计了基于零知识证明的多实体 RFID 认证(MERAP)协议。

1　MERAP 协议

多实体 RFID 系统由多个服务器、阅读器和电子标签构成。服务器和阅读器间的通信信道是安全的，而阅读器与标签之间的信道则容易遭受攻击。

1.1 密钥阵列结构

假设有 N 个实体(N 个服务器、N 个阅读器)和 M 个标签。阅读器 R_j(j=1,2,⋯,N）和标签 T_i(i=1,2,⋯,M)共享唯一的认证密钥 k_{ij}，k_{ij} 为密钥阵列 $\boldsymbol{K}$ 中的一个元素。R_j 存储密钥阵列 $\boldsymbol{K}$ 中第 j 列元素，即$\{k_{1j},k_{2j},\cdots,k_{Mj}\}$。$T_i$ 存储密钥阵列 $\boldsymbol{K}$ 中第 i 行元素，即$\{k_{i1},k_{i2},\cdots,k_{Ni}\}$。不同的阅读器代表不同的参与实体，根据认证密钥 k_{ij}，标签对每个阅读器开放不同的数据区域。

表 1 参数符号说明

Table1 The description of parameters and symbols

symbols	description
R_j	the legal reader of the entity j in RFID system
T_i	the ith legal tag of RFID system
S_j	the server of the entity j in RFID system
r_R,u_R	pseudo random integer produced by the reader R_j
PID_R, PID_T	the pseudonyms of R_j and T_i
L_R, L_T	access control list
k_{ij}	the authentication key of R_j and T_i
k_l, k_r	the left and right part of the authentication key k_{ij}
d	a random integer obtained by rounding operation
$g(\cdot)$	pseudo random function
$[\cdot]$	rounding operation
$x\|_d$	the first d bits of x
$\otimes$	xor operation
$\|\|$	connection operation
? =	compared for equality

1.2 协议参数

本协议中参数意义如表 1 所示。

1.3 认证过程

利用阅读器 R_j 和标签 T_i 的通信过程来描述 MERAP 协议的认证过程，如图 1 所示。初始化时，访问控制列表 L_R,L_T 分别被写入标签和阅读器内存中，包含系统中合法阅读器及标签的认证信息。服务器保存着所有合法阅读器的认证信息。本协议认证过程分为 5 个阶段：

第 1 阶段：发起问询。阅读器 R_j 生成随机整数 r_R，并以 r_R 及 g,p 为参数计算 A_R。然后，R_j 将 $r_R||F_R||A_R$ 作为问询信息发送给标签 T_i。

第 2 阶段：标签初步认证阅读器。当接到 R_j 的问询信息时，T_i 首先在访问控制列表 L_T 中检索是否存在相符的标识符 F_R 来初步认证 R_j。如果 F_R 不存在或不合法，则认证停止并报错。否则，T_i 对 r_R 做取整运算得到 d。接着 T_i 在内存中查找 k_{ij}，并将其分割为 $k_l||k_r$；其中高 d 位是 k_l，其余是 k_r。考虑到下溢，分割时将零填充在虚设位。T_i 计算完 g_R 及 A_T，将 $A_T||F_T$ 作为响应信息发送给 R_j。

第 3 阶段：阅读器初步认证标签。收到标签 T_i 的响应信息后，R_j 首先在访问控制列表 L_R 中检索是否存在相符的标识符 F_T 来判定 T_i 的合法性。如果 F_T 不存在，则 R_j 认为 T_i 是非法的，协议终止并报错。反之，阅读器 R_j 初步认证标签 T_i。接着，R_j 将 $r_R||A_T||A_R$ 转发给服务器 S_j。

第 4 阶段：阅读器对标签最终认证。当收到消息 $r_R||A_T||A_R$ 时，S_j 首先计算 d=[r_R]，S_j 检索认证密钥 k_{ij}，并将其分割为 $k_l||k_r$，继续计算 g_{Sj} 与 A_{Sj} 的值，并通过判断 A_{Sj} 与 A_R 是否相等来确认标签 T_i 的合法性。若等式成立，则 T_i 合法性得到阅读器 R_j 的最终认证，同时 S_j 将认证成功消息发送给 R_j。否则，协议认证终止并报错。

第 5 阶段：标签对阅读器最终认证。收到 S_j 发送的 OK 后，R_j 根据 g_{Sj} 求出认证密钥 k_{ij}。接着，R_j 生成随机整数 u_R 并取 $d'=[u_R]$，同时按照分割规则将 k_{ij} 分割为 $k_l'||k_r'$。之后，R_j 顺序计算 a,g_R 及 B_R，并将 $u_R||B_R$ 发送给标签 T_i 以便进一步认证。收到 $u_R||B_R$ 后，T_i 取 $d'=[u_R]$，并将 k_{ij} 分割为 $k_l'||k_r'$，同时计算 λ_T 且将其发送给 R_j。一旦

得到 λ_T，R_j 继续计算 S_R 和 C_R，完成之后将 C_R 发送给 T_i。得到 C_R 后，T_i 顺序计算 W_T,V_T 及 B_T。计算完成之后，T_i 通过判定等式 $B_T=B_R$ 是否成立，来最终认证阅读器 R_j。若该等式成立，则 R_j 的合法性得到标签 T_i 的最终认证，R_j 开始读取 T_i 对应认证区域的信息，通信顺利进行。否则，阅读器 R_j 被认为非法的，认证终止并报错。至此，协议整个认证过程完成。

新的认证协议基于挑战——响应机制，采用分布式密钥阵列存储认证信息，通过零知识证明实现认证过程，同时应用多种轻量级机制安全措施，如随机分割机制、访问控制列表机制等，实现了认证信息更新和协议的可扩展性。

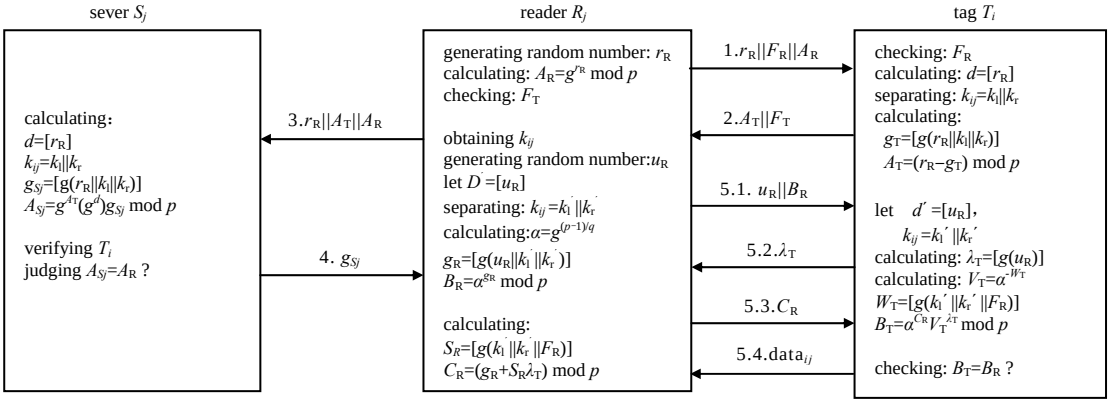

Fig.1 The authentication process of multiple entities RFID authentication protocol based on zero-knowledge proof
图1 基于零知识证明的多实体RFID认证协议认证过程

1.4 协议说明

1) 零知识证明方案：本协议中，第 1 至 3 阶段的认证过程是基于离散对数问题的零知识证明方案。第 5 阶段，标签对阅读器的最终认证采用基于 Schnorr 身份识别协议的零知识证明方案[10,13]。2 种方案的安全性均是基于离散对数问题的难解性。因而，如果仔细选择 p，即使在开放的无线信道中传输 $\{A_R, A_T, B_R, \lambda_T, C_R\}$ 等认证信息，协议也能保证 RFID 系统的信息安全，因为攻击者无法求解离散对数问题。

2) 密钥阵列：分布式密钥阵列使得在标签 T_i 的内存中只保存与自己相关的认证密钥 $k_{i1},k_{i2},\cdots,k_{Ni}$，即密钥阵列 $\boldsymbol{K}$ 中的第 i 行密钥，减少了标签内存占用，降低了成本。认证密钥 k_{ij} 可以保护标签可访问区域信息的安全，即不同的阅读器授权不同，标签不同区域信息只能被认证的阅读器访问，故能抵制系统中合法实体假冒另一合法实体越权访问，即内部假冒攻击。

3) 随机分割机制：整数 $d(d')$用于随机分割。一方面，根据分割机制将认证密钥 k_{ij} 划分为 $k_l||k_r(k_l'||k_r')$。由于每次认证中阅读器生成的随机数不同，所以整数 $d(d')$也将不同，因而 $k_l||k_r(k_l'||k_r')$是自动更新的，这在保证安全性的同时也节省了标签的更新模块，节约了内存空间。另一方面，每次认证时提取阅读器和标签假名的前 d 位，降低了搜索强度，提高了效率。在零知识证明方案中引入随机分割机制，起到了认证信息动态更新的作用。

4) 访问控制列表机制：访问控制列表(L_R,L_T)用来在内存中检索待认证的阅读器或标签。一方面，所有标签和阅读器的伪随机标示符(F_R,F_T)存储在访问控制列表中，既能达到快速检索核查的目的，又能用时间戳区分不同次的认证过程。如果问询消息中含有不匹配的 F_R 或 F_T，那么待认证实体被认为非法而被拒绝。另一方面，存储在访问控制列表中的假名(PID_R, PID_T)，除作为索引实现了初级验证实体的目标外，动态分割假名使得快速搜索替代了穷尽搜索，降低搜索的时间复杂度，同时也有利于系统的扩展。此外，L_R,L_T 将最近一次收到的 F_R 或 F_T 作为临时文件存储，如果一定时间内，含有该 F_R 或 F_T 的问询信息频繁问询，那么合法实体拒绝响应问询。

另外，双向认证机制的引入实现了访问控制目的。R_j 与 T_i 通过初级、最终 2 次认证判定双方的合法性，第 3 阶段 S_j 独立对 R_j 与 T_i 分别进行认证。只有所有认证都成功，阅读器才能访问标签相应的信息。值得注意的是，本协议中标签无随机数发生器且未使用哈希函数，所有运算均是轻量级的，大大降低了标签的成本。

2 协议模型及性能分析

2.1 零知识证明模型

本协议采用 2 个零知识证明模型。认证的第 1 至 3 阶段采用基于离散对数问题的零知识证明模型；第 5 阶

段为基于 Schnorr 身份识别方案的零知识证明模型。两模型中参数要求如下:

1) p 及 q 是大素数，且 q 是 $p-1$ 的因子。p 的长度至少 1 024 位，q 至少 160 位。

2) $\alpha \in \mathbf{Z}_p$ 且阶数为 q，g 为 $\mathbf{Z}_p$ 的本原元。

3) 安全参数 t(一般取 40，Schnorr 建议 72)，作用是阻止攻击者在第 5 阶段伪装成阅读器猜测 $\lambda_{\mathrm{T}} \in \left[0,1,\cdots,2^{t-1}\right]$ 的值。攻击者能猜到 λ_{T} 的概率为 2^{-t}，如果 t 足够大，则 λ_{T} 是安全的，进而系统是安全的。为获得更高安全性，本协议取 t=72，且 $2^t<q$。

4) 随机整数 $(r_{\mathrm{R}},u_{\mathrm{R}}) \in [1,2,\cdots,q-1]$。

虽然 2 个模型的安全性均是基于离散对数问题的难解性，但二者仍然存在区别。具体说明如下。

2.1.1 基于离散对数问题的零知识证明模型

该模型中，阅读器 R_j 作为验证者，而标签 T_i 作为证明者，标签向阅读器证明自己的合法性。R_j 生成随机整数 r_{R} 并计算 A_{R}:

$$A_{\mathrm{R}}=g^{r_{\mathrm{R}}} \bmod p \tag{1}$$

如果 R_j 通过了标签 T_i 的初级认证，则标签 T_i 计算 $g_{\mathrm{T}},A_{\mathrm{T}}$:

$$g_{\mathrm{T}}=\left[g\left(r_{\mathrm{R}}\|k_1\|k_{\mathrm{r}}\right)\right] \tag{2}$$

$$A_{\mathrm{T}}=\left(r_{\mathrm{R}}-g_{\mathrm{T}}\right) \bmod p \tag{3}$$

然后，T_i 将 $A_{\mathrm{T}}\|F_{\mathrm{T}}\|PID_{\mathrm{T}}|_d$ 发送给 R_j。假如 T_i 能通过 R_j 的初级认证，则 R_j 将 $r_{\mathrm{R}}\|A_{\mathrm{T}}\|A_{\mathrm{R}}\|PID_{\mathrm{R}}|_d$ 转发给服务器。如果服务器认证了 R_j 的合法性，则继续计算 g_{S_j} 与 A_{S_j}:

$$g_{S_j}=\left[g\left(r_{\mathrm{R}}\|k_1\|k_{\mathrm{r}}\right)\right] \tag{4}$$

$$A_{S_j}=g^{A_{\mathrm{T}}}\left(g^{d}\right)^{g_{S_j}} \bmod p \tag{5}$$

S_j 通过判断 $A_{S_j}=A_{\mathrm{R}}$ 是否成立来确认标签 T_i 的合法性。若等式成立，则 T_i 的合法性得到 R_j 的最终认证，同时服务器将 g_{S_j} 发送给 R_j。至此，阅读器 R_j 作为验证者认证了作为证明者的标签 T_i 的合法身份。整个认证过程中没有泄露秘密信息，安全而高效。

2.1.2 基于 Schnorr 协议的零知识证明模型

该模型应用在本协议认证过程的第 5 阶段。此模型中，T_i 作为验证者而 R_j 作为证明者，R_j 试图向 T_i 证明自己的合法身份。R_j 生成随机数 u_{R}，取 $d'=[u_{\mathrm{R}}]$，然后顺序计算 α,g_{R} 及 B_{R}:

$$\alpha=g^{(p-1)/q} \tag{6}$$

因为 α 是固定值，可以预先计算得出，并初始化在阅读器中，提高运行速率。

$$g_{\mathrm{R}}=\left[g\left(u_{\mathrm{R}}\|k_1'\|k_{\mathrm{r}}'\right)\right] \tag{7}$$

$$B_{\mathrm{R}}=\alpha^{g_{\mathrm{R}}} \bmod p \tag{8}$$

然后 R_j 将 $u_{\mathrm{R}}\|B_{\mathrm{R}}$ 发送给标签 T_i 以便进一步认证。T_i 计算 λ_{T}，并将其发送给 R_j。

$$\lambda_{\mathrm{T}}=\left[g\left(u_{\mathrm{R}}\right)\right] \tag{9}$$

收到 λ_{T} 后 R_j 继续计算 $S_{\mathrm{R}},C_{\mathrm{R}}$

$$S_{\mathrm{R}}=\left[g\left(k_1'\|k_{\mathrm{r}}'\|F_{\mathrm{R}}\right)\right] \tag{10}$$

$$C_{\mathrm{R}}=\left(g_{\mathrm{R}}+S_{\mathrm{R}}\lambda_{\mathrm{T}}\right) \bmod q \tag{11}$$

接着，将 C_{R} 发送给 T_i。标签 T_i 得到 C_{R} 后，顺序计算 $W_{\mathrm{T}},V_{\mathrm{T}}$ 及 B_{T}:

$$W_{\mathrm{T}}=\left[g\left(k_1'\|k_{\mathrm{r}}'\|F_{\mathrm{R}}\right)\right] \tag{12}$$

$$V_{\mathrm{T}}=\alpha^{-W_{\mathrm{T}}} \tag{13}$$

$$B_{\mathrm{T}}=\alpha^{C_{\mathrm{R}}}V_{\mathrm{T}}^{\lambda_{\mathrm{T}}} \bmod p \tag{14}$$

验证者 T_i 通过验证等式 $B_{\mathrm{T}}=B_{\mathrm{R}}$ 是否成立来最终认证阅读器 R_j 的合法性。如若该等式成立，则 R_j 的合法性得到标签 T_i 的最终认证，R_j 开始读取 T_i 的对应认证区域的信息，通信顺利进行。

以上 2 种零知识证明模型基于离散对数问题难解性，确保协议认证过程安全、高效。且通信量和计算量均较少，适用于计算能力有限的低成本标签。

2.2 协议性能分析

2.2.1 零知识特性

本文所设计的协议在认证中，无论是阅读器 R_j 还是标签 T_i 都未将自己的真实身份信息泄露。即使假名(PID_{R}, PID_{T})在信道中传输，但是进行了动态提取前 $d(d')$位，因而未泄露。此外，认证密钥 k_{ij} 动态分割后又参与了 g_{T} 的计算，而 g_{T} 又作为参数计算 A_{T}，最终只有 A_{T} 在信道中传输，攻击者截获 A_{T} 也无法解出 k_{ij}。更重要的是，随机数 $r_{\mathrm{R}},u_{\mathrm{R}}$ 在区间 $[1,q-1]$ 中均匀分布，λ_{T} 在区间 $\left[0,2^{t-1}\right]$ 中也是均匀分布，同样 $g_{\mathrm{S}},A_{\mathrm{R}},A_{\mathrm{T}},B_{\mathrm{R}},C_{\mathrm{R}}$ 在 $\mathbf{Z}_p^*$ 上也是均匀分布。因而所有在 R_j,T_{i} 与服务器之间交换的认证信息，因具有相同的分布而使攻击者无法区分，即使其截获认证信息也无法伪装成合法实体。可知，本协议具备零知识特性。

2.2.2 内部攻击

本协议采用分布式密钥阵列方案抵御系统内部攻击。系统为每对阅读器和电子标签设定了唯一的认证密钥 k_{ij}。阅读器通过 k_{ij} 识别电子标签的合法性，而电子标签利用 k_{ij} 判别阅读器的访问是否合法，且标签根据 k_{ij} 向合法阅读器开放对应的可访问数据区域。即不同授权的阅读器只能访问标签数据存储区某一部分区域的信息，这阻止了系统中合法实体假冒另一合法实体越权访问，即内部攻击。此外，零知识证明方案的设计使得实体在认证过程不泄露秘密信息，特别是身份信息和认证密钥 k_{ij}，这样即使系统内其他合法实体伪造或者截获认证信息也不能成功实施攻击。因此应用 MERAP 协议的 RFID 系统是可抵御内部攻击的。

2.2.3 其他攻击形式

1) 重放攻击

MERAP 协议中，阅读器对标签发起问询时总会产生随机数 r_{R}，标签的响应为 $A_{\mathrm{T}}=\left(r_{\mathrm{R}}-g_{\mathrm{T}}\right)\bmod p$，其中 $g_{\mathrm{T}}=\left[g\left(r_{\mathrm{R}}\|k_{\mathrm{l}}\|k_{\mathrm{r}}\right)\right]$。虽然密钥 k_{ij} 不变，但是由于采用随机分割机制，标签每次的响应都不同。可见攻击者重放在以前通信过程中窃听到的信息无法通过认证，所以 MERAP 协议可以有效抵抗重放攻击。

2) 拒绝服务攻击

MERAP 协议中，由于采用认证密钥随机分割机制，不存在密钥更新问题，故不会出现密钥更新失败导致阅读器与电子标签密钥更新不同步的问题，即 MERAP 协议可以抵抗拒绝服务攻击。

3) 中间人攻击

无论是认证的第 1 至 3 阶段采用的基于离散对数问题的零知识证明模型，还是第 5 阶段采用的基于 Schnorr 的身份识别方案的零知识证明模型，通过无线传输的信息都受到了随机分割机制和加密算法的保护，具有不可预测性。对于攻击者来说，通过对截获的信息进行替换或修改来干扰合法通信是行不通的。

4) 双向认证

MERAP 协议中，需要对通信双方身份的合法性进行认证，只有知道正确的非对称密钥和身份标识 F_{R} 才能通过对方的身份认证。

5) 窃听攻击

整个通信过程中，攻击者能窃听到的信息只有 $r_{\mathrm{R}}\|F_{\mathrm{R}}\|A_{\mathrm{R}}$，$A_{\mathrm{T}}\|F_{\mathrm{T}}$，$u_{\mathrm{R}}\|B_{\mathrm{R}}$，$\lambda_{\mathrm{T}},C_{\mathrm{R}}$ 和 data_{ij}。它们均受到非称加密函数、随机数和随机分割机制的保护，攻击者无法利用这些信息获得标签的有用信息，所以 MERAP 协议可以抵抗窃听攻击。

6) 位置隐私

标签发出的信息是随机数 r_{R} 和密钥 k_{ij} 的高级加密结果，都是随机变化的，并且不可破解的。攻击者无法将窃听到的信息与某个特定的标签相关联，也无法将某个标签的响应信息和其他标签的响应信息区分开。因此，提出的协议可以保护用户的位置隐私。

本文所设计认证协议的安全性和隐私性由分布式密钥阵列结构和零知识证明方案予以保证。分布式密钥阵列结构的应用解除了系统内部攻击的威胁。零知识证明方案的实施使得认证过程中实体不泄露敏感信息，攻击者从而无法窃取有效认证信息，不能实施有威胁的攻击。此外，零知识证明方案的设计废除了已有密钥阵列结构协议的双密钥机制——本协议中阅读器和标签之间不使用共享密钥，这不仅解决了共享密钥泄露的问题，而且提高了系统的安全性。同时，将随机数机制引入零知识证明方案中，不仅起到动态更新的作用，更重要的是使攻击者通过合法实体的概率可忽略不计。随机分割机制和访问控制列表在零知识证明方案中的应用，进一步加强了动态更新机制，达到了初级认证的目的；另外也提高了检索效率，增加协议灵活性。因而，基于以上方法的应用，本协议能够有效抵御重放攻击、中间人攻击、跟踪攻击、拒绝服务攻击以及内部假冒攻击，实现高安全性。表 2 所

示为本协议和相关协议抵抗攻击性能的对比。

表 2 与同类协议抵御攻击性能比较

Table2 The anti-attack capability comparison of similar protocols

protocols	M	P	A1	A2	A3	A4	A5	A6
Peris-Lopez,et al.[14]	Y	N	Y	N	Y	Y	N	N
LIU H.,et al.[8]	Y	Y	Y	Y	Y	Y	Y	N
NING H.,et al.[2]	Y	Y	Y	Y	Y	Y	N	Y
JUANG,et al.[15]	Y	Y	Y	Y	N	Y	Y	Y
S. Sundaresan,et al.[11]	Y	Y	Y	Y	Y	Y	Y	N
S. Sundaresan,et al.[12]	Y	Y	Y	Y	Y	Y	Y	N
LIU H.,et al.[8]	Y	Y	Y	Y	Y	Y	Y	N
MERAP	Y	Y	Y	Y	Y	Y	Y	Y

note:M:two-way authentication; P:forward security; A1:anti eavesdropping attack; A2:anti tracking attack; A3:anti denial of service attacks; A4:anti replay attack; A5:anti man-in-the-middle attack; A6:anti internal attack; Y:can resist; N: can not resist.

3　结论

本文提出了基于零知识证明的 RFID 密钥阵列认证协议，即 MERAP 协议。MERAP 协议采用分布式密钥阵列结构抵御多实体 RFID 系统中的内部攻击，利用零知识证明方案避免了 LIU H.[8]协议中共享密钥 k_u 的使用，解决了已有密钥阵列协议共享密钥泄露的问题,更重要的是认证双方在完成认证的过程中未泄露任何敏感信息，与以往通过牺牲匿名性来完成实体认证的设计方案相比，MERAP 协议具有更高的安全性。此外，通过将随机数机制、随机分割机制及访问控制列表引入零知识证明方案中，不仅增强了 MERAP 协议的零知识特性，而且实现了协议的动态更新和快速检索，提高了 MERAP 协议的执行效率和灵活性。同时，轻量级算法的采用降低了协议实现成本。综上所述，MERAP 协议将零知识证明理论引入 RFID 分布式密钥阵列认证协议中，在保证 RFID 系统认证信息不泄露的同时，实现了对内部攻击和多种外部攻击手段的有效抵抗。

参考文献:

[1] 徐鹤. 基于对等计算的无线射频识别网络若干问题研究[D]. 南京:南京邮电大学, 2012. (XU He. Research on several problems of wireless radio frequency identification network based on peer to peer computing[D]. Nanjing,China: Nanjing University of Posts and Telecommunications, 2012.)

[2] NING H,LIU H,MAO J,et al. Scalable and distributed key array authentication protocol in radio frequency identification based sensor systems[J]. IET Communication, 2011,5(12):1755–1768.

[3] 轩秀巍. 超高频射频识别系统的关键技术研究[D]. 天津:天津大学, 2012. (XUAN Xiuwei. Research on key techniques of ultra high frequency radio frequency identification system[D]. Tianjin,China:Tianjin University, 2012.)

[4] 彭辉,陈红,张晓莹,等. 无线传感器网络位置隐私保护技术[J]. 软件学报, 2015,26(3):617–639. (PENG Hui,CHEN Hong, ZHANG Xiaoying,et al. Location privacy preservation in Wireless Sensor Networks[J]. Journal of Software, 2015,26(3): 617–639.)

[5] HENSELER M,ROSSBERG M. Credential management for automatic identification solutions in supply chain management[J]. IEEE Transactions on Industrial Informatics, 2008,4(4):303–314.

[6] DING Z,GUO L,WANG Y. An authentication protocol based on key array for RFID[J]. Electron. Inf. Technol., 2009,31, (3):722–726.

[7] JIANG Yi,CHENG Wei,DU Xiaojiang. Group-based key array authentication protocol in radio frequency identification systems[J]. IET Inf. Secur., 2014,8(6):290–296.

[8] LIU Hong,NING Huansheng. Zero-knowledge authentication protocol based on Alternative Mode in RFID Systems[J]. IEEE Sensors Journal, 2011,11(12):3235–3245.

[9] 黎彤亮. 物联网中的 RFID 安全协议与可信保障机制研究[D]. 天津:天津大学, 2013. (LI Tongliang. Research on RFID security protocol and trusted security mechanism in the Internet of Things[D]. Tianjin,China:Tianjin University, 2013.)

[10] 林巧民. 物联网安全及隐私保护中若干关键技术研究[D]. 南京:南京邮电大学, 2014. (LIN Qiaomin. Research on some key technologies in the security and privacy protection of the Internet of Things[D]. Nanjing,China:Nanjing University of Posts and Telecommunications, 2014.)

[11] SUNDARESAN S,DOSS R. Secure yoking proof protocol for RFID systems[C]// 2014 International Conference on Advances in Computing,Communications and Informatics(ICACCI). [S.l.]:IEEE, 2014:1585–1591.

[12] SUNDARESAN S,DOSS R,ZHOU W. Zero knowledge grouping proof protocol for RFID EPC C1G2 tags[J]. IEEE Transactions on Computers, 2015,64(10):2994–3008.

[13] 付章杰,束建钢,孙星明,等. 利用文本鲁棒特征的零知识水印安全检测方案[J]. 西安电子科技大学学报, 2015,42(4): 176–181. (FU Zhangjie,SHU Jiangang,SUN Xingming,et al. Secure zero knowledge watermark detection scheme based on the text robust feature[J]. Journal of Xidian University, 2015,42(4):176–181.)

(下转第 119 页)