doi:10.3969/j.issn.1000-436x.2013.z1.031

EPC 网络中可证明安全的 EPCIS 通信方案

李景峰[1]，潘恒[2]，郭卫锋[1]
（1. 解放军信息工程大学 密码工程学院，河南 郑州 450004；2.中原工学院 计算机学院，河南 郑州 450007）

摘 要：针对 EPC 信息服务存在的安全问题，提出一种 EPC 信息服务安全通信方案 ESCM，方案使用数字签名、消息认证码等安全机制，实现了分属查询应用程序和外域 EPCIS 服务器之间的相互认证服务与密钥协商服务，能够保护 EPCIS 通信的机密性和完整性。利用 Canetti-Krawczyk 模型证明了 ESCM 方案是会话密钥安全的。此外，性能分析表明该方案的通信开销、计算开销较少，适合 EPC 网络特性。

关键词：EPC 信息服务；射频标识；Canetti-Krawczyk 模型
中图分类号：TP393 **文献标识码**：B **文章编号**：1000-436X(2013)Z1-0235-05

Provable security EPC information service communication scheme for EPC network

LI Jing-feng[1], PAN Heng[2], GUO Wei-feng[1]
(1. Institute of Cryptographic Engineering, PLA Information Engineering University, Zhengzhou 450004, China;
2. Computer Science College, Zhongyuan University of Technology, Zhengzhou 450007, China)

Abstract: To resolve the security drawbacks of EPC information services, a provable security EPC information service communication scheme—ESCM was designed. By using some cryptographic mechanisms such as the digital signature and the message authentication code, the ESCM could implement mutual authentication and session key agreement between the EPC Information service servers and querying application belonging to a different trust domain. Security analysis shows that the session key agreement of ESCM is provably secure in the Canetti-Krawczyk model. Furthermore, the ESCM has efficient computation and communication cost.

Key words: EPC Information service; radio frequency identification; Canetti-Krawczyk model

1 引言

电子产品码（EPC, electronic product code）网络是在互联网基础上，利用射频识别（RFID, radio frequency identification）技术构造的全球物品信息实时共享系统[1]，目前已在全球物流领域、大型商贸供应链领域得到了广泛应用。在 EPC 网络体系架构中，EPC 信息服务器（EPCIS, EPC information service）负责存储 EPC 编码对应物品的具体信息，定义企业间信息交换的接口，是实现供应链上企业间信息共享的关键[2]。

在 EPC 网络中，每家企业都是独立、自治的信任域。为防止未授权的应用程序非法访问企业内部 EPCIS 服务器中的商业敏感信息，一般通过本地认证服务器对查询 EPCIS 服务器的应用程序进行身份验证。由于查询应用程序和做出响应的 EPCIS 服务器所处信任域不同，因此必须协商得到共享密钥，以确保后继交互数据的机密性和完整性。

针对查询 EPCIS 服务器阶段，Kyuhee 等人[3]提出了一种基于 Kerberos 和 GRBAC 的认证协议，为 EPC 网络中用户提供身份认证和访问控制服务。由于 Kerberos 采用基于对称密钥的架构，对称密钥管理问题复杂，所以该方案可扩展性较低。针对该问题，WEN 等人[4]和 Kim 等人[5]分别提出了基于 PKI 的身份认证方案。但这 2 种方案仅解决了单个信任域内的身份认证，没有考虑跨域身份认证问题。同时，基于 PKI 的安全机制会急剧增加系统开销，严重影响 EPC 网络整体性能。

收稿日期：2013-07-05

针对上述问题，本文设计了一种 EPCIS 安全通信方案—ESCM，该机制利用数字签名和消息认证码等机制，实现了查询应用程序和 EPCIS 服务器之间的相互认证和密钥协商，以确保数据跨域传输时的机密性和完整性，利用 Canetti-Krawczyk 模型证明了该方案是会话密钥安全的。此外，性能分析表明该方案通信开销和计算开销较小。

2 安全通信方案 ESCM

2.1 应用背景和系统模型

图 1 描述了设计 ESCM 方案的应用背景和系统模型。设生产商和销售商接入基于互联网的 EPC 网络。每家企业构成独立信任域，使用本地认证服务器验证查询应用程序是否合法。当商品运到销售商处，销售商采集标签数据，并将 EPC 编码传送给本地应用程序。设本地应用程序已经通过查询 ONS 系统获得 EPCIS 服务器的地址，如何从该 ECPIS 服务器安全地获得商品数据，即实现商品数据跨域安全传输，这就是 ESCM 方案的目标。

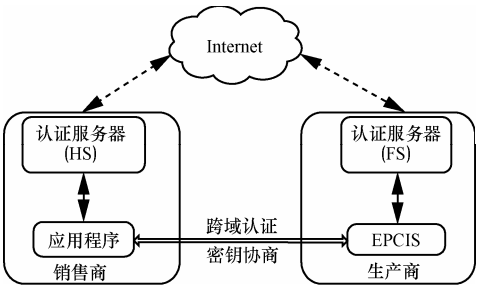

图 1 EPCIS 安全通信机制的系统模型

假设信任域中的本地认证服务器和该域每个查询应用程序共享全局唯一的一个秘密参数。利用该共享秘密参数，双方可获得确保彼此安全通信的密钥信息。假设可信 CA 为 EPC 网络中所有本地认证服务器颁发一张公钥证书。

查询应用程序 C (标识符为 ID_C)在本地认证服务器 HS (标识符为 ID_{HS})注册，C 与 HS 利用共享秘密参数 k_{C-HS}，由密钥导出函数 $prf()$ 计算得到加密密钥 k^1_{C-HS} 和消息认证码密钥 k^2_{C-HS}：

$$k^1_{C-HS} = prf(ID_C \| ID_{HS} \| k_{C-HS} \| \text{“Encryption key”}) \quad (1)$$

$$k^2_{C-HS} = prf(ID_C \| ID_{HS} \| k_{C-HS} \| \text{“Message authentication key”}) \quad (2)$$

类似地，假设 IS(标识符为 ID_{IS})在本地认证服务器 FS (标识符为 ID_{FS})注册，并且与本地认证服务器 FS 共享秘密参数 k_{IS-FS}，双方能够计算得到加密密钥 k^1_{IS-FS} 和消息认证码密钥 k^2_{IS-FS}。

2.2 安全方案描述

ESCM 方案中的查询应用程序和 EPCIS 服务器在通信前没有建立信任关系，必须借助各自的本地认证服务器才能实现认证和密钥协商等功能。方案可划分为 2 个阶段：1)跨域认证和密钥协商阶段：查询应用程序和 EPCIS 服务器使用预先共享秘密参数完成与本地认证服务器的相互认证，认证服务器间使用同一 CA 颁发的公钥证书实现相互认证。查询应用程序和 EPCIS 服务器利用扩展 Diffie-Hellman 密钥协商协议协商得到会话密钥。2)跨域数据安全传输阶段：EPCIS 服务器利用会话密钥实现对被查询商品数据的跨域安全传输。

2.2.1 跨域认证和密钥协商阶段

查询应用程序 C 在事先得到 EPCIS 服务器地址的情况下[6]，为得到商品详细数据，它必须向 EPCIS 服务器所在的本地认证服务器 IS 认证并协商得到会话密钥。

1) $C \to IS: M_1 = \{ID_C, ID_{IS}, ID_{HS}, g^x, T_C, MAC_C\}$

C 生成随机数 $x \in_R Z_p^*$ 并计算会话密钥参数 g^x，向 IS 发送访问请求消息 M_1，其中，T_C 是时间戳，MAC_C 是 C 计算的消息认证码 $MAC(k^2_{C-HS}, ID_C \| ID_{IS} \| ID_{HS} \| g^x \| T_C)$。

2) $IS \to FS: M_2 = \{ID_{IS}, ID_{FS}, T_{IS}, MAC_{IS}, M_1\}$

当 IS 收到访问请求消息 M_1 后，向 FS 发送消息 M_2，其中，T_{IS} 是时间戳，MAC_{IS} 是 IS 计算的消息认证码后 $MAC(k^2_{IS-FS}, ID_{IS} \| ID_{FS} \| T_{IS})$。

3) $FS \to HS: M_3 = \{ID_{FS}, ID_{HS}, T_{FS}, Cert_{FS}, Sig_{FS}, M_1\}$

当 FS 收到消息 M_2 后，首先检查 T_{IS} 是否有效，再利用密钥 k^2_{IS-FS} 验证 MAC_{IS} 是否正确。如果验证都通过，则 FS 认证 IS 成功；否则，认证失败。认证成功后，FS 从 M_2 中提取出 ID_{HS} 的相关信息，向 HS 发送消息 $M_3 = \{ID_{FS}, ID_{HS}, T_{FS}, Cert_{FS}, Sig_{FS}, M_1\}$，其中，$T_{FS}$ 是时间戳、$Cert_{FS}$ 是 FS 的公钥证书，Sig_{FS} 是 FS 对该消息的签名，$Sig_{FS} = Sig(SK\_FS, ID_{FS} \| ID_{HS} \| T_{FS} \| Cert_{FS})$。

4) $HS \to FS: M_4 = \{ID_{HS}, ID_{FS}, T_{HS}, Cert_{HS}, Sig_{HS}, M_5\}$

当 HS 收到消息 M_3 后，首先检查 T_{FS} 是否有效，

再验证证书 $Cert_{FS}$ 及签名 Sig_{FS}，若上述验证都通过，则 *HS* 认证 *FS* 成功；否则，协议终止。认证成功后，*HS* 首先认证 *C*，首先检查 T_C 是否有效，再使用 k^2_{C-HS} 验证 MAC_C 是否正确。若验证都通过，则 *HS* 认证 *C* 成功；否则，协议终止。当 *FS* 和 *C* 都认证成功后，*HS* 从消息 M_3 中提取时间戳 T_{HS}，生成消息 $M_4=\{ID_{HS},ID_{FS},T_{HS},Cert_{HS},Sig_{HS},M_5\}$，其中，$Cert_{HS}$ 是 *HS* 的公钥证书，$Sig_{HS}=Sig(SK\_HS, ID_{HS}\|ID_{FS}\|T_{HS}\|Cert_{HS})$ 是 *HS* 对消息 M_4 的签名，消息 $M_5=\{ID_{HS},ID_C,T_{HS},MAC_{HS}\}$，$MAC_{HS}=MAC(k^2_{C-HS},ID_{HS}\|ID_C\|T_{HS})$。最后，*HS* 将 M_4 发送给 *FS*。

5) $FS\rightarrow IS:\ M_6=\{ID_{FS},ID_{IS},T_{FS}',MAC_{FS},M_5\}$

当 *FS* 收到消息 M_4 后，首先验证 T_{HS}、$Cert_{HS}$ 和 Sig_{HS} 的有效性，若验证都通过，则 *FS* 认证 *HS* 成功；否则，协议终止。*FS* 提取时间戳信息 T_{FS}'，并将消息 $M_6=\{ID_{FS},ID_{IS},T_{FS}',MAC_{FS},M_5\}$ 发送给 *IS*，其中，$MAC_{FS}=MAC(k^2_{IS-FS},ID_{FS}\|ID_{IS}\|T_{FS}')$ 是 *FS* 计算的消息认证码。

6) $IS\rightarrow C:\ M_7=\{ID_{IS},ID_C,g^y,MAC_{IS}',M_5\}$

当 *IS* 收到消息 M_6 后，首先验证 T_{FS}' 和 MAC_{FS} 的有效性。若验证都通过，则 *IS* 认证 *FS* 成功；否则，协议终止。*IS* 生成随机数 $y\in_R Z_p^*$，计算会话密钥 $k_{C-IS}=(g^x)^y=g^{xy}$。接下来，*IS* 计算加密密钥 k^1_{C-IS} 和消息认证码密钥 k^2_{C-IS}。

$$k^1_{C-IS}=prf(ID_C\|ID_{IS}\|g^{xy}\|\text{“Encryption key”}) \quad (3)$$

$$k^2_{C-IS}=prf(ID_C\|ID_{IS}\|g^{xy}\|\text{“Message authentication key”}) \quad (4)$$

最后，*IS* 向 *C* 发送 $M_7=\{ID_{IS},ID_C,g^y,MAC_{IS}',M_5\}$，其中，$MAC_{IS}'=MAC(k^2_{C-IS},ID_{IS}\|ID_C\|g^y)$ 是 *IS* 计算的消息认证码。

当 *C* 收到消息 M_7 后，首先验证 T_{HS} 和 MAC_{HS} 是否有效。若验证都通过，则 *C* 认证 *HS* 成功。然后，*C* 计算 $k_{C-IS}=(g^y)^x=g^{xy}$，得到加密密钥 k^1_{C-IS} 和消息认证码密钥 k^2_{C-IS}。最后，使用 k^2_{C-IS} 验证 MAC_{IS}' 是否正确，若验证通过，则 *C* 与 *IS* 之间的相互认证成功，协议执行完毕；否则，协议终止。

2.2.2　跨域数据安全传输阶段

在 2.2.1 节描述的阶段结束后，*C* 可以使用 k^1_{C-IS} 加密 EPC 编码，使用密钥 k^2_{C-IS} 计算待传输消息认证码，并将加密结果和消息认证码一起发送给 *IS*。*IS* 收到查询请求后，使用密钥 k^2_{C-IS} 验证消息认证码的正确性，使用密钥 k^1_{C-IS} 解密消息，得到待查询商品的 EPC 编码。然后，EPCIS 服务器将使用密钥 k^1_{C-IS} 加密数据库中与该 EPC 编码相关的数据，同时使用密钥 k^2_{C-IS} 计算消息认证码，将加密结果和消息认证码反馈给 *C*。应用程序收到反馈消息后，使用密钥 k^2_{C-IS} 验证消息认证码是否正确，使用密钥 k^1_{C-IS} 解密出商品数据。至此，跨域数据安全传输完成。

3　形式化安全性分析

本节使用 CK 模型证明 ESCM 方案的安全属性。

3.1　会话密钥安全性分析

为证明 ESCM 方案是会话密钥安全的，首先需设计 AM 模型中的密钥协商协议 π_3，证明其在 AM 模型中是会话密钥安全的；然后构造消息传输认证器 $\lambda_{sig,T}$ 和 $\lambda_{MAC,T}$；最后将 $\lambda_{sig,T}$ 和 $\lambda_{MAC,T}$ 应用于协议 π_3 并优化得到 UM 模型中协议 π_4 [6]。

3.1.1　AM 模型中的协议

AM 模型中协议是一个扩展 Diffie-Hellman 协议 π_3，如图 2 所示。

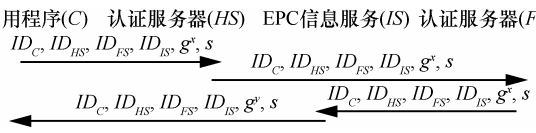

图 2　AM 模型中的协议 π_3

1) *C* 选择随机数 $x\in_R Z_p^*$，计算参数 g^x，将消息 $m_1=\{ID_C,ID_{HS},ID_{FS},ID_{IS},g^x,s\}$ 发送给 *HS*，其中，*s* 是会话标识。

2) *HS* 认证 *C*，若认证成功，则将消息 $m_2=\{ID_C,ID_{HS},ID_{FS},ID_{IS},g^x,s\}$ 发送给 *FS*；否则，协议终止。

3) *FS* 认证 *HS*，若认证成功，则将消息 $m_3=\{ID_C,ID_{HS},ID_{FS},ID_{IS},g^x,s\}$ 发送给 *IS*；否则，协议终止。

4) *IS* 认证 *FS*，若认证成功，则选择随机数 $y\in_R Z_p^*$，计算参数 g^y，将消息 $m_4=\{ID_C,ID_{HS},ID_{FS},ID_{IS},g^y,s\}$ 发送给 *C*。此时，*IS* 计算得到 $k_{IS-C}=(g^x)^y=g^{xy}$、k^1_{C-IS} 和 k^2_{C-IS}；否则，协议终止。

5) *C* 认证 *IS* 与 *HS*，若 *IS* 是期望的 EPCIS 服务器且 *HS* 合法，则认证成功，*C* 计算 $k_{C-IS}=(g^y)^x=g^{xy}$、k^1_{C-IS} 和 k^2_{C-IS}；否则，协议终止。

DDH 假设：设 p 和 q 是 2 个素数，且满足 $q \mid p-1$，g 是 Z_p^* 中阶数为 q 的生成元，随机选择 $x,y,z \in_R Z_p^*$，对于任意多项式时间算法，$\{p,g,g^x,g^y,g^{xy}\}$ 和 $\{p,g,g^x,g^y,g^z\}$ 在概率分布上是计算不可区分的。

定理 1 在 DDH 假设下，协议 π_3 在 AM 模型中是会话密钥安全的。

证明 当协议完成时，若 C 和 IS 未被攻陷，得到未篡改的 g^x 与 g^y，则双方能够计算相同的参数 $k_{C-IS}=k_{IS-C}=g^{xy}$，使用式(3)、(4)计算得到相同的 2 个会话密钥，满足 AM 模型中会话密钥安全定义的第一个条件[6]。

假设存在一个 AM 模型中的攻击者 $\mathcal{A}$，$\mathcal{A}$ 能够以不可忽略的优势 ε 区分会话密钥和等长的随机字符串。因此，构造算法 D，通过运行一个子过程 $\mathcal{A}$，能够以不可忽略的优势区分 $Q_0=\{p,g,g^x,g^y,g^{xy}\}$ 和 $Q_1=\{p,g,g^x,g^y,g^z\}$。

设算法 D 的输入为 (p,g,a^*,b^*,c^*)，为 Q_0 和 Q_1 的概率均为 0.5，并按照以下规则运行[7]。

1) D 执行协议交互中实体间调度操作，$\mathcal{A}$ 控制所有信道。D 执行初始化运行环境操作，将参数 p、g 发送给 $\mathcal{A}$。

2) D 选择随机会话 r 作为测试会话，其中，$r \in \{1,\cdots,l\}$，l 是可能的最大会话数量。

3) 若 r 被激活，则 C 将 a^* 发送给 HS，HS 将 a^* 转发给 FS，FS 再将 a^* 转发给 IS；IS 将 b^* 发送给 C。

4) 若 $\mathcal{A}$ 选中 r，并对其执行测试会话查询，则 D 发送 c^* 给 $\mathcal{A}$。

5) 若 $\mathcal{A}$ 攻陷某个参与者，则 D 将该参与者信息发送给 $\mathcal{A}$；若某个会话暴露，则 D 将该会话信息发送给 $\mathcal{A}$。

6) 若 $\mathcal{A}$ 选择的测试会话不是 r 或 r 已暴露，则 D 放弃 $\mathcal{A}$ 的执行，随机猜测比特 b 为 $b' \in_R \{0,1\}$。

7) 若 $\mathcal{A}$ 停止攻击，输出的结果是 b'，则 D 停止，输出结果也是 b'。

从上述规则可以看出，算法 D 能够模拟 AM 模型中攻击者 $\mathcal{A}$ 的行为。

下面根据 $\mathcal{A}$ 选取的测试会话是否是 r 而分别进行了讨论。

1) $\mathcal{A}$ 选择 r 作为测试会话：根据规则(4)，$\mathcal{A}$ 能够得到 c^*。若输入为 Q_0，则 $c^*=g^{xy}$，$\mathcal{A}$ 得到真实会话密钥 g^{xy}。如果输入为 Q_1，则 $c^*=g^z$，$\mathcal{A}$ 得到一个随机数。因此，$\mathcal{A}$ 区分会话密钥与随机数的概率等同于算法 D 区分 Q_0 与 Q_1 的概率。因为 $\mathcal{A}$ 成功猜测会话密钥的概率为 $0.5+\varepsilon$，所以 D 区分 Q_0 与 Q_1 的概率也为 $0.5+\varepsilon$。

2) $\mathcal{A}$ 选择的测试会话不是 r：根据规则 6)，D 放弃 $\mathcal{A}$ 的执行，并输出一个随机值。$\mathcal{A}$ 不能帮助 D 区分 Q_0 与 Q_1，D 区分 Q_0 与 Q_1 的概率为 0.5。

考虑到 D 在执行时最多涉及 l 个会话，则情况 1)发生的概率为 $1/l$，情况 2)发生的概率则为 $1-1/l$。因此，D 成功区分 Q_0 与 Q_1 的概率是 $(0.5+\varepsilon)/l+0.5(1-1/l)=0.5+\varepsilon/l$。由于 ε 在安全参数范围内是不可忽略的，所以 ε/l 也不可忽略的，从而推断出 D 能够以不可忽略的优势 ε/l 区分 Q_0 与 Q_1。显然，该结论与 DDH 假设矛盾。因此，协议 π_3 满足 AM 模型中会话密钥安全定义的第 2 个条件[9]。

从上述讨论可知，协议 π_3 满足 AM 模型中会话密钥安全全部定义。

3.1.2 构造消息传输认证器

在协议 π_3 中，IS 认证 C 是通过 HS 认证 C、FS 认证 HS 以及 IS 认证 FS 来实现的。类似地，C 认证则是通过 FS 认证 IS、HS 认证 FS 以及 C 认证 HS 来实现的。因此，需要为 HS 与 C、FS 与 HS、IS 与 FS 的相互认证构造消息传输认证器。

首先，本文使用郭卫峰等人[8]构造的一种基于签名和时间戳的消息传输认证器 $\lambda_{sig,T}$ 实现 HS 与 FS 之间的相互认证；使用另一种基于消息认证码和时间戳的消息传输认证器 $\lambda_{MAC,T}$ [8]实现 HS 与 C 之间、IS 与 FS 之间的相互认证。

定理 2 如果签名算法 Sig 是选择明文攻击安全的，则 $\lambda_{sig,T}$ 是一个消息传输认证器[7]。

定理 3 如果消息认证码算法 MAC 是选择明文攻击安全的，则 $\lambda_{MAC,T}$ 是一个消息传输认证器[7]。

3.1.3 UM 模型中的协议

将 $\lambda_{sig,T}$ 和 $\lambda_{MAC,T}$ 应用到 AM 模型中协议 π_3，得到 UM 模型中优化后的协议 π_4，如图 3 所示。

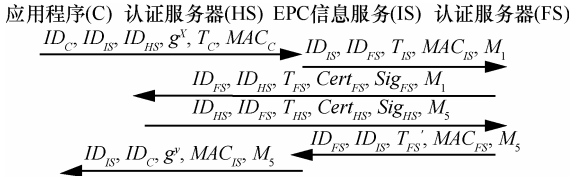

图 3 UM 模型中协议 π_4

定理 4　在 DDH 假设下，如果数字签名算法 *Sig* 和消息认证码算法 *MAC* 都是在选择明文攻击下安全的，协议 π_4 在 UM 模型中是会话密钥安全的。

证明　由定理 1 可知，协议 π_3 在 AM 模型中是会话密钥安全的。由定理 2 和定理 3 可知，$\lambda_{sig,T}$ 和 $\lambda_{MAC,T}$ 是消息传输认证器；使用消息传输认证器 $\lambda_{sig,T}$ 和 $\lambda_{MAC,T}$ 编译 π_3，得到协议 π_4。由 CK 模型基本定理[6]可知，协议 π_4 在 UM 模型中也是会话密钥安全的。

由上述安全性证明可知，ESCM 方案能够为查询应用程序和 EPCIS 服务器提供安全会话密钥协商服务。

3.2　其他安全属性分析

本节分析 ESCM 方案满足其他安全属性。

1) 相互认证：*C* 和 *IS* 利用各自的本地认证服务器 *HS* 和 *FS* 实现相互认证，能够防止非授权用户的非法访问，同时也能够防止攻击者伪造 EPCIS 服务器为合法用户提供虚假商品数据。

2) 前向保密性：查询应用程序和 EPCIS 服务器之间是使用扩展 Diffie-Hellman 协议协商得到会话密钥。只要双方没有同时泄露了各自与本地认证服务器共享的秘密参数，攻击者就无法恢复先前的会话密钥。

3) 防重放攻击：ESCM 方案规定实体间每次通信都必须使用时间戳机制，能够有效防止攻击者进行重放攻击。

综上所述，ESCM 方案利用相互认证、时间戳机制有效抵御了主动攻击；利用安全密钥协商机制有效抵御了被动攻击。

3.3　性能比较

为降低用户和 EPCIS 服务器的计算开销，ESCM 方案将计算量比较大的数字签名操作交给计算能力强大的认证服务器实现；而查询应用程序和 EPCIS 服务器仅执行随机数生成、指数运算和 MAC 运算等计算开销较少的操作。由于目前 EPC 网络中还没有成熟的 EPCIS 安全解决方案，所以本文选择 2 种典型的多信任域认证协议 IDAKE-MA[9]、SKAP[10] 和 ESCM 方案进行性能比较，结果如表 1 所示。

表 1　性能比较

安全机制	通信次数	域间通信次数	非对称加密	非对称解密	数字签名	验证签名	MAC 运算	验证 MAC
IDAKE-MA[9]	14	6	6	6	5	5	0	0
SKAP[10]	10	4	4	4	3	3	0	0
ESCM	6	4	0	0	2	2	5	5

从表 1 可以看出，在通信开销方面，ESCM 方案中实体通信次数少于其余 2 个协议，其域间通信次数与 SKAP 协议相当，少于 IDAKE-MA 协议。在计算开销方面， ESCM 方案未使用公钥加密机制，而是使用 MAC 运算代替签名运算，MAC 运算和签名次数与 SKAP 协议中公钥加密和签名次数相当，少于 IDAKE-MA 协议。由于使用对称密码算法，因此计算开销小于 SKAP 和 IDAKE-MA 协议。

4　结束语

本文针对 EPC 网络中 EPCIS 服务器查询过程，设计了一种 EPCIS 安全通信方案 ESCM，实现了查询应用程序和 EPCIS 服务器之间的相互认证和密钥协商功能，确保了 EPCIS 通信的机密性和完整性。利用 CK 模型对该方案进行了形式化安全性证明。此外，性能分析表明该方案具有较低的通信开销与计算开销，有助于开发人员研发安全、高效的 EPC 网络跨域应用系统。

参考文献：

[1] The EPCglobal architecture framework version 1.4[EB/OL]. http://www.gs1.org/gsmp/kc/epcglobal/ archi-tecture/architecture_1_4-framework-20101215.pdf. 2010, 12.

[2] EPC information services (EPCIS) version 1.0.1[EB/OL]. http://www.gs1.org/gsmp/kc/epcglobal/epcis/epcis_1_0_1-standard-20070921.pdf. 2007, 9.

[3] KYUHEE A, KIYEAL L, MOKDONG C. Design and implementation of an RFID-based enterprise application framework based on abstract BP and kerberos[J]. International Journal of Information Processing Systems, 2006, 2(3):170-177.

[4] WEN J, TIAN W H, WANG W D. An authentication approach to enhance RFID security[A]. Proceedings of Communication, Circuits and Systems[C]. 2010. 144-146.

[5] KIM D J, KIM J J, LEE S M, *et al*. Design and implementation for EPC system method to authentication and cryptography[A]. Proceedings of Information Security and Assurance[C]. 2008. 137-141.

[6] 王刚. 基于 HMIPv6 的无线 Mesh 网络安全切换方案研究[D]. 郑州: 解放军信息工程大学, 2011.
WANG G. Research on the Secure Switching Schema based on HMIPv6 for the Wireless Mesh Networks[D]. Zhengzhou: PLA Information Engineering University, 2011.

[7] 郭卫锋. EPC 网络数据跨域传输安全机制研究[D]. 郑州: 解放军信息工程大学, 2013.

（下转第 245 页）

Transactions on Vehicular Technology. 2012, 61(1):86-96.

[7] MA C Y T, YAU D K Y, YIP N K, Privacy vulnerability of published anonymous mobility traces[A]. Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking (Mobicom'10)[C]. New York, USA, 2010. 185-196.

[8] RAYA M, MANSHAEI M H, FELEGYHAZI M, *et al*. Revocation Games in Ephemeral Networks[A]. ACM Conference on Computer and Communications Security (CCS)[C]. New York, NY, USA, 2008. 199-210.

[9] REIDT S, SRIVATSA M, *et al*. The fable of the bees: incentivizing robust revocation decision making in ad hoc networks[A]. ACM Conference on Computer and Communications Security (CCS)[C]. New York, NY, USA, 2009. 291-302.

[10] ALPCAN T, BUCHEGGER S, Security games for vehicular networks[J]. IEEE Transactions on Mobile Computing, 2011, 10(2): 280-290.

作者简介：

杨卫东（1977-），男，内蒙古集宁人，博士，河南工业大学副教授，主要研究方向为车联网、信息安全等。

何云华（1987-），男，湖北荆门人，中国科学院信息工程研究所博士生，主要研究方向为车联网、信息安全等。

孙利民（1966-），男，河南淮阳人，中国科学院信息工程研究所研究员，主要研究方向为无线传感器网络、信息安全等。

（上接第 239 页）

GUO W F. Research on the Secure Crossing-domains Transmission Schema for the EPC Networks [D]. Zhengzhou: PLA Information Engineering University, 2011.

[8] 郭卫锋, 李景峰, 张来顺. EPC 网络中一种可证明安全的跨域认证协议[J]. 小型微型计算机系统, 2013, 34(5):983-986.
GUO W F,LI J F, ZHANG L S. A provable secure crossing-domains authentication protocol for the EPC networks[J]. Journal of Chinese Computer Systems, 2013, 34(5):983-986.

[9] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8):1271-1281.
PENG H X. An Identity-based authentication model for multi-domain[J]. Chinese Journal of Computers, 2006, 29(8):1271-1281.

[10] 朱辉, 李晖, 杨加喜等. 一种可证明安全的通用多信任域认证协议[J]. 武汉大学学报（信息科学版）, 2008, 33(10):1051-1054.
ZHU H, LI Y, YANG J X, *et al*. A universal provable security authentication protocol for multi-domain[J]. Geomatics and Information Science of Wuhan University, 2008, 33(10):1051-1054.

作者简介：

李景峰（1977-），男，江苏南京人，解放军信息工程大学副教授、硕士生导师，主要研究方向为信息系统安全技术、无线移动通信网网络等。

潘恒（1977-），女，河南新乡人，中原工学院计算机学院副教授、硕士生导师，主要研究方向为信息系统安全测评等。

郭卫锋（1987-），男，河南周口人，解放军信息工程大学硕士生，主要研究方向为物联网安全基础设施。