物联网环境下 UC 安全的组证明 RFID 协议

张 忠 徐秋亮
(山东大学计算机科学与技术学院 济南 250061)

摘 要 物联网的安全和隐私保护问题是制约其进一步发展的关键性问题,如何设计一个安全、高效的组证明 RFID 协议是物联网安全需要重点研究的一个问题.首先,文中对物联网环境下组证明 RFID 协议的交互模型和攻击模型做了分析和描述.然后,在通用可组合安全框架下,形式化定义了理想功能 F_{VS} 和 RFID 组证明理想功能 F_{GP}.最后,在 F_{VS}-混合模型下,设计了组证明 RFID 协议 π_{GP},并证明对于任意的攻击者而言,协议 π_{GP} 能安全实现理想功能 F_{GP}.根据组合定理表明新的组证明 RFID 协议具有通用可组合安全性.

关键词 物联网;RFID;组证明;通用可组合协议
中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2011.01188

Universal Composable Grouping-Proof Protocol for RFID Tags in the Internet of Things

ZHANG Zhong XU Qiu-Liang
(*School of Computer Science & Technology, Shandong University, Jinan* 250061)

Abstract Security and privacy block the development of the Internet of Things (IOT). How to design a RFID grouping-proof protocol with security and high efficiency is a key problem in the security of IOT. Firstly, we present an attack model and a interaction model, and give the analysis. Then, the ideal functionality F_{VS} and the grouping-proof ideal functionality F_{GP} are formally defined with the UC framework. Finally, a grouping-proof protocol π_{GP} is designed in the F_{VS}-hybrid model. It is proved that the protocol π_{GP} realizes the ideal functionality F_{GP} securely for any adversary. According to the composition theorem in the UC framework, the proposed grouping-proof protocol for RFID tags is UC secure.

Keywords Internet of Things; RFID; grouping-proof; universally composable protocol

1 引 言

物联网(Internet of Things,IOT)[1]通过射频识别(RFID)、红外感应器、全球定位系统(GPS)、激光扫描器等信息传感设备,按约定的协议,把任何物品与互联网连接起来;在强大的运算平台支持下进行信息交换和通信,实现智能识别、定位、跟踪、监控和管理.作为一个传感器网络、移动通信网络和因特网等多网融合的异构网络,物联网对隐私保护的安全需求日益迫切,给众多研究者提出了新挑战.

射频识别即 RFID(Radio Frequency Identification)是一种通信技术,可通过无线电信号识别特定目标并读写相关数据.在物联网中,RFID 系统实现对末端物体信息的感知.目前国内外对 RFID 安全协议的研究成果较为丰富,有形式化定义的安全模型[2-5]和比较典型实用的交互认证协议[6-10],但以上

收稿日期:2011-05-03;最终修改稿收到日期:2011-06-15.本课题得到国家自然科学基金(60873232)资助.**张 忠**,男,1978 年生,博士研究生,研究方向为安全协议.E-mail: zhangzhong@mail.sdu.edu.cn.**徐秋亮**(通信作者),男,1960 年生,博士,教授,博士生导师,研究领域为密码学与信息安全.E-mail: xuqiuliang@sdu.edu.cn.

这些成果都是基于独立应用系统假设建立的，是否满足物联网安全需求还需要重新审视.

在实际应用中，物联网的末端物体常常具有明显的群组特性，例如一个大型超市中所有接入物联网的商品对外声称属于同一家超市，某家医院的一组医疗器械针对某个特定手术等等. 这种群组性就要求我们设计的 RFID 安全协议具有能够处理群组通信的能力. Juels[11] 最早对多标签扫描问题做了研究，利用两个标签互相签名的思想，提出了一个两标签共存证明的 RFID 协议（称为联合证明协议）. Saito 和 Sakurai[12] 指出 Juels 的协议对重放攻击是不安全的，并通过为每一个会话引入时间戳设计了基于时间戳的联合证明协议. 但由于时间戳是可以预先猜测的，因此攻击者可以事先猜测多项式个时间戳，并让 RFID 标签进行签名，然后在下一个会话攻击中使用. 为克服这种弱点，Piramuthu 等人[13] 将时间戳换成了随机数以抵抗这种重放攻击. 但在 2007 年，Peris-Lopez 等人[14] 和 Lin 等人[15] 指出这种基于随机数的组证明协议对多会话干扰攻击是不安全的. 随后，Burmester 等人[16] 基于共享组 ID 的思想提出了 3 个组证明协议，其中第 3 个协议具有匿名性和前向安全性. 在 2009 年，Huang 等人[17] 针对病人用药安全问题提出了一个支持低成本 RFID 标签的在线组证明协议，协议中使用 CRC 校验代替常规的消息认证码和 Hash 函数. 同年，Chien 等人[18] 对 Juels 的联合证明协议进行了扩展，提出了基于树的联合证明协议，将后台的计算复杂度降低到了 $O(1)$. 但近来，Peris-Lopez 等人[19] 对上面的协议做了安全性分析，并指出 Burmester 等人[16] 的方案容易遭受假冒攻击，而 Huang 等人[17] 和 Chien 等人[18] 的方案对伪造攻击和隐私攻击是敏感的. Duc 等人[20] 基于 (n,n) 门限思想提出了一个组证明协议，但该协议的组证明结果随着群组规模的增大线性增长，不适宜于较大的群组，并且 Duc 等人[20] 的协议需要一个时刻在线的验证方发起证明，这对于接入形式比较复杂的网络也是很难保证的.

本文在物联网环境下系统地研究了组证明 RFID 协议，在第 2 节定义物联网环境下的组证明 RFID 协议交互模型、敌手攻击模型和安全性需求；第 3 节将给出组证明 RFID 协议的 UC 模型定义[21]，随后在第 4 节构造一个轻量级协议；第 5 节给出方案的安全性证明及效率分析；第 6 节总结全文.

2　组证明 RFID 协议模型和安全性需求

2.1　物联网环境下组证明 RFID 协议的交互模型

我们定义，在物联网环境下一个组证明 RFID 交互协议涉及 3 种实体：标签集合 TS、读写器集合 RS 和信息处理集合 VS. 其中 $TS=\{T_{ij}\}$，i 标示组号，T_{ij} 表示第 i 组中的第 j 个 RFID 标签；$RS=\{R_k\}$，为降低协议的复杂度，假定一组标签同时只和一个读写器进行交互，R_k^i 表示和第 i 组标签 T_i 发生交互的读写器；信息处理集合 VS 负责处理由 RS 采集到的 TS 数据，包含信息认证中心、密钥管理中心、数据处理中心以及数据存储中心等，方便起见，我们把这类集合抽象成理想功能 F_{VS}，它的具体定义将在 3.1 节给出.

初始化阶段由 F_{VS} 为标签集合 TS 和读写器集合 RS 分别生成初始参数 (BT_{ij},k_{ij}) 和 (BR_k,k_k)，其中 BT_{ij} 表示盲化后标签 T_{ij} 的身份 ID，k_{ij} 是与 T_{ij} 身份绑定的通信主密钥，BR_k 表示盲化后读写器 R_k 的身份 ID，k_k 是与 R_k 身份绑定的通信主密钥. 考虑到物联网环境的特异性，对普通的 RFID 协议模型进行了弱化，放宽了对 RS 以及 RS 和 VS 之间通信信道的安全假设，认为其都是不安全的. 读写器 R_k^i 执行组证明协议前需要向 F_{VS} 申请组证明读写资格，成功之后 F_{VS} 会为 R_k^i 生成一个读写授权 V_k^i. 但这种授权申请是一次性的，不需要在每次交互中都去申请，除非需要变更为对另一组标签 T_j 进行操作.

2.2　物联网环境下组证明 RFID 协议的敌手攻击模型

在组证明 RFID 交互协议中，敌手攻击的一个主要目的[22] 是获得能够通过 VS 验证的组证明 p，但被证明存在的标签 T_{ij} 并没有真正参与协议或并非该组合法成员；另一个目的是获取参与方 TS 和 RS 的隐私信息，如身份标识 ID、位置和组别等信息.

敌手 A 的攻击渠道可以分为对信道的攻击和对参与实体的攻击. 我们假设敌手 A 能够完全控制 TS 与 RS 之间以及 RS 与 VS 之间的通信信道，可以任意地读取、删除、篡改、延迟发送和重放信道中的任何消息，也可以在任何时候发起与任何实体的任意会话. 基于 UC 框架[21]，我们假定敌手 A 也可以在协议执行的任何时候攻陷参与方 TS 和 RS 中

的任意实体，对于攻陷后的实体，敌手 A 能够成功获取到它内部状态数据，但无法获得该实体的密钥（包括通信主密钥和授权密钥 V_k^i）.

敌手攻击的方法主要有：重放攻击[13]、子集重放攻击[19]、多会话干扰攻击[14]、假冒攻击、伪造攻击和隐私攻击[19]等等.

2.3 物联网环境下组证明 RFID 协议的安全性需求

强隐私保护. 只有获得授权 V_k^i 的读写器 R_k^i 才能读取到标签组 T_i 的共存证明 p_i，并且在所有的交互中即便是所有消息都被恶意截获，攻击者依然无法获得 R_k^i 和 T_i 的任何身份信息以及组信息.

不可追踪性. 攻击者无法通过截获的组证明集合 $\{p_i\}$ 判断任意两个证明 p_i 和 p_j 的关系，即无法关联任意两个组证明的生成者是否属于同一组，也无法确定两个证明的生成者中是否包含同一成员.

读写器匿名性. 协议执行过程中，任意的攻击者和协议交互方 T_i 都无法获得读写器 R_k^i 的身份信息.

标签匿名性. 类似于读写器匿名性，攻击者和协议交互方 R_k^i 都无法获取到标签 T_i 的身份信息和组信息.

授权认证. 只有被授权的读写器 R_k 和合法的组成员标签 T_i 正确执行协议才能得到合法的组证明 p_i，而对于任意未被授权的读写器将无法得到有效的组证明.

3 组证明 RFID 协议的 UC 模型

UC 框架最初是由 Canetti[21] 提出的，它是一种基于模块化协议设计的思想. 只要协议满足了 UC 安全，就能保证它与其它协议或是它自身的多个实例并行运行时的安全. 物联网是个非常复杂而庞大的综合性系统，如果把协议运行的外部环境（包括静态环境和运行时环境）全都考虑周全是十分复杂和极为困难的，因此我们拟借助 UC 框架这个工具来搭建整个物联网环境下的协议族.

3.1 理想功能 F_{VS}

为便于描述和分析协议，我们将物联网平台上的信息处理服务抽象出来用理想功能 F_{VS} 来描述，其主要功能是为每一个标签和读写器生成初始参数，处理读写器授权申请和验证组证明信息.

（1）当收到指令 $(Init, T_i)$ 时，F_{VS} 为标签组 T_i 中的每一个标签 T_{ij} 生成一对初始参数 (BT_{ij}, k_{ij})，其中 $BT_{ij}=H(T_{ij})$ 表示盲化后标签 T_{ij} 的身份 ID，$H()$ 是一个安全的 Hash 函数，k_{ij} 是一个随机数，用作 T_{ij} 的通信主密钥. 然后将 $(T_{ij}, BT_{ij}, k_{ij}, T_i)$ 进行序列化存储，并将 (BT_{ij}, k_{ij})、(BT_{ij}, T_{ij}) 分别安全地传送给 T_{ij} 和请求者.

（2）当收到指令 $(Init, R)$ 时，F_{VS} 为集合 RS 中的每一个读写器 R_k 生成一对初始参数 (BR_k, k_k)，其中 $BR_k=H(R_k)$ 表示盲化后读写器 R_k 的身份 ID，$H()$ 是一个安全的 Hash 函数，k_k 是一个随机数，用作 R_k 的通信主密钥. 然后将 (R_k, BR_k, k_k) 进行序列化存储，并将 (BR_k, k_k)、(BR_k, R_k) 分别安全地传送给 R_k 和请求者.

（3）当收到指令 $(QRead, T_i)$ 时，F_{VS} 会为 R_k^i 生成一个读写授权 V_k^i，V_k^i 为一个随机数. 然后将 (R_k, T_i, V_k^i) 进行序列化存储，并将 V_k^i 安全地传送给 R_k.

（4）当收到指令 $(Valid, BR_k, s_R, p_i, r, r_{i1}, \cdots, r_{in})$ 时，F_{VS} 令 $r'=r, r_i'=r_{i1}\oplus r_{i2}\oplus\cdots\oplus r_{in}$，搜索记录 (R_k, BR_k, k_k) 和 (R_k, T_i, V_k^i). 如果有一条记录不存在，返回失败. 否则取出对应的 k_k, T_i, V_k^i，并计算 $s_R'=MAC_{k_k}(BR_k, r', r_i')$，如果 $s_R\neq s_R'$，返回失败. 否则搜索 T_i 组的所有成员标签信息，取出对应的 T_{ij}，BT_{ij}, k_{ij}. 计算 $s_{ij}'=MAC_{k_{ij}}(BR_{ij}, T_i, r', r_i', r_{ij})$，$s_i'=s_{i1}'\oplus s_{i2}'\oplus\cdots\oplus s_{in}'$，$p_i'=MAC_{V_k^i}(s_i')$，如果 $p_i\neq p_i'$，返回失败. 否则返回成功.

3.2 理想功能 F_{GP}

基于第 2 节中描述的交互模型和敌手攻击能力，我们定义物联网环境下 RFID 组证明协议的理想功能 F_{GP}. 理想环境下攻击者 S 可以攻陷任意的标签 T_{ij} 和读写器 R_k 并获得参与方的内部状态数据（不包括密钥信息）. 环境机 Z 确定所有实体的输入，获得他们的输出，并指导各参与实体（包括攻击者 S）执行相应的操作.

（1）当收到指令 $(Activate, sid)$ 时，F_{GP} 通过向理想功能 F_{VS} 发送指令 $(Init, T_i)$ 和 $(Init, R)$ 对标签组 T_i 和读写器 R_k 进行初始化，并存储返回结果 (BT_{ij}, T_{ij}) 和 (BR_k, R_k)，然后向 F_{VS} 发送指令 $(QRead, T_i)$ 为 R_k 申请授权.

（2）当从 R_k 收到指令 $(Init, sid, BR_k)$ 时，F_{GP} 查找 (BR_k, R_k)，确定读写器身份 R_k，如果 R_k 已经被攻破，则忽略此消息. 否则生成一个子会话标识 $ssid$ 并记录 $(ssid, BR_k, R_k)$，然后发送 $(ssid, BR_k)$ 给攻击者 S.

（3）当从 T_{ij} 收到指令 $(Init, sid, BT_{ij})$ 时，F_{GP} 查找 (BT_{ij}, T_{ij})，确定标签身份 T_{ij}，如果 T_{ij} 已经被攻破，则忽略此消息. 否则生成一个子会话标识 $ssid$ 并记录 $(ssid, BT_{ij}, T_{ij})$，然后发送 $(ssid, BT_{ij})$ 给攻

击者 S.

(4) 当从攻击者 S 收到指令($Product$, $ssid$, BR_k)时，F_{GP} 生成随机数 r 并将其发送给 T_i.

(5) 当从攻击者 S 收到指令($Product$, $ssid$, BT_{ij})时，如果存在记录($ssid$, BR_k, R_k)，则 F_{GP} 生成随机数 r_{ij} 并将其发送给 R_k.

(6) 当从攻击者 S 收到指令($Proof$, $ssid$, BT_{ij}, s_{ij})时，如果 T_{ij} 已经被攻破，F_{GP} 查找记录($ssid$, BR_k, R_k)，并把 s_{ij} 发送给 R_k. 否则计算 $s_i = s_{i1} \oplus s_{i2} \oplus \cdots \oplus s_{in}$ 并将其发送给 R_k，其中 $s_{ij} = H_{k_{ij}}(BT_{ij}, T_i, r, r_i, r_{ij})$，$r_i = r_{i1} \oplus r_{i2} \oplus \cdots \oplus r_{in}$.

(7) 当从攻击者 S 收到指令($Verify$, sid, BR_k, P)时，如果 R_k 已经被攻破，F_{GP} 把 P 发送给 F_{VS}. 否则，删除记录($ssid$, BR_k, R_k)、($ssid$, BT_{ij}, T_{ij})并发送 BR_k, s_R, p_i, r, r_{i1}, $\cdots$, r_{in} 给理想功能 F_{VS}，其中 $s_R = H_{k_k}(BR_k, r, r_i)$，$p_i = H_{V_k^i}(s_i)$.

3.3　安全分析

下面我们证明理想功能 F_{GP} 和理想功能 F_{VS} 满足 2.3 节中定义的安全性需求.

(1) 强隐私保护. 在理想环境下，所有由理想功能 F_{GP} 发送给攻击者 S 的信息里的 BR_k 和 BT_{ij}，都是由理想功能 F_{VS} 返回的盲化后读写器 R_k 或标签 T_{ij} 的身份. 因此在整个交互过程中，S 无法区分读写器或标签的身份和某个随机数.

(2) 不可追踪性. 在理想环境下，攻击者 S 可以攻陷读写器 R_k，因此他有可能获得多个组证明 $\{p_i\}$，但由于每次组证明里的参数 $r, r_1, \cdots, r_n$ 都是由多个标签独立选择的随机数，因此 S 无法确定任意两个组证明的生成者是否为同一组，或是否包含同一成员.

(3) 读写器匿名性. 证明与(1)类似.

(4) 标签匿名性. 证明与(1)类似.

(5) 授权认证. 在理想环境下，攻击者 S 无法通过理想功能 F_{VS} 获得授权 V_k^i，却可以通过理想功能 F_{GP} 获得 T_i 的共同签名 $s_i = s_{i1} \oplus s_{i2} \oplus \cdots \oplus s_{in}$. 但由于无法获得 V_k^i，故 S 得不到能够通过 F_{VS} 验证的合法组证明 p_i.

4　物联网环境下 UC 安全的组证明 RFID 协议

本节给出一个物联网环境下组证明 RFID 协议 π_{GP}，见图 1. 该协议在 RFID 标签集合 $\{T_{ij}, j = 1, 2, \cdots, n\}$ 和读写器 R_k 上执行计算量很少的操作：T_{ij} 只需要生成 m 比特的随机数和计算一次带 key 的消息认证码 $MAC_k(\cdot)$. 其中 m 根据一定标准选取(例如按 EPC C1G2 标准，m 取值为 16)；读写器端除了上述两种操作外，还需要执行按位异或操作. 绝大多数计算量都由后端的 F_{VS} 来完成，这是非常适合物联网体系架构及其基本特征的.

方案 π_{GP} 共分为 4 个阶段：初始化、授权、组证明生成和组证明验证. 其中初始化过程只需在系统建立之初使用一次，但需要 F_{VS}、读写器 R_k 和标签组 $\{T_i\}$ 在线状态下完成. F_{VS} 为每一个标签 T_{ij} 和每一个读写器 R_k 生成并分发 l 比特的随机通信密钥. 授权过程满足 2.1 节中定义的交互模型，授权申请在不变更权限的条件下只需要一次在线申请，不需要每次执行组证明都去交互申请. 组证明生成过程完全是标签组 T_i 和读写器 R_k 两方的交互，适用于 F_{VS} 不在线或是没有条件在线的情况. 首先由读写器发起挑战，标签对挑战进行签名响应，读写器收集所有标签的签名承诺，然后生成自己的签名承诺. 最后是组证明验证过程，由 F_{VS} 集中验证读写器 R_k 和标签组 T_i 的合法性、R_k 授权访问的合法性以及组证明的合法性.

5　安全性证明及效率分析

5.1　安全性证明

通过在理想模型中构造一个理想敌手 S，使得没有环境 Z 能够区分现实模型中的执行和理想模型中的执行，从而证明协议 π_{GP} 实现了理想功能 F_{GP}，即协议 π_{GP} 具有 UC 安全性.

定理 1.　对于任意的攻击者 A，在 F_{VS}-混合模型下，协议 π_{GP} 安全地实现了理想功能 F_{GP}.

证明.　对于任意的攻击者 A，可以构造一个仿真器 S，S 能够将 A 在 F_{VS}-混合模型下与真实协议 π_{GP} 交互的行为模拟成理想环境下攻击者 S 对理想功能 F_{GP} 交互的行为. 也就是说，对于任意的环境图灵机 Z 而言，它与攻击者 A 和协议 π_{GP} 以及攻击者 S 和理想功能 F_{GP} 的交互都是不可区分的.

(1) 构建仿真器 S. 在理想环境下仿真一份真实环境下的攻击者 A、读写器 R_k 和标签组 T_i 以及理想功能 F_{VS} 的拷贝. 当理想攻击者 S 被激活以后，将环境机 Z 发送来的消息 m 作为仿真的攻击者 A 的输入，协议 π_{GP} 执行完成后的输出作为理想攻击者 S 的输入，并返回给 Z，这样就好像所有真实环境下的参与方都和环境机 Z 直接相连一样.

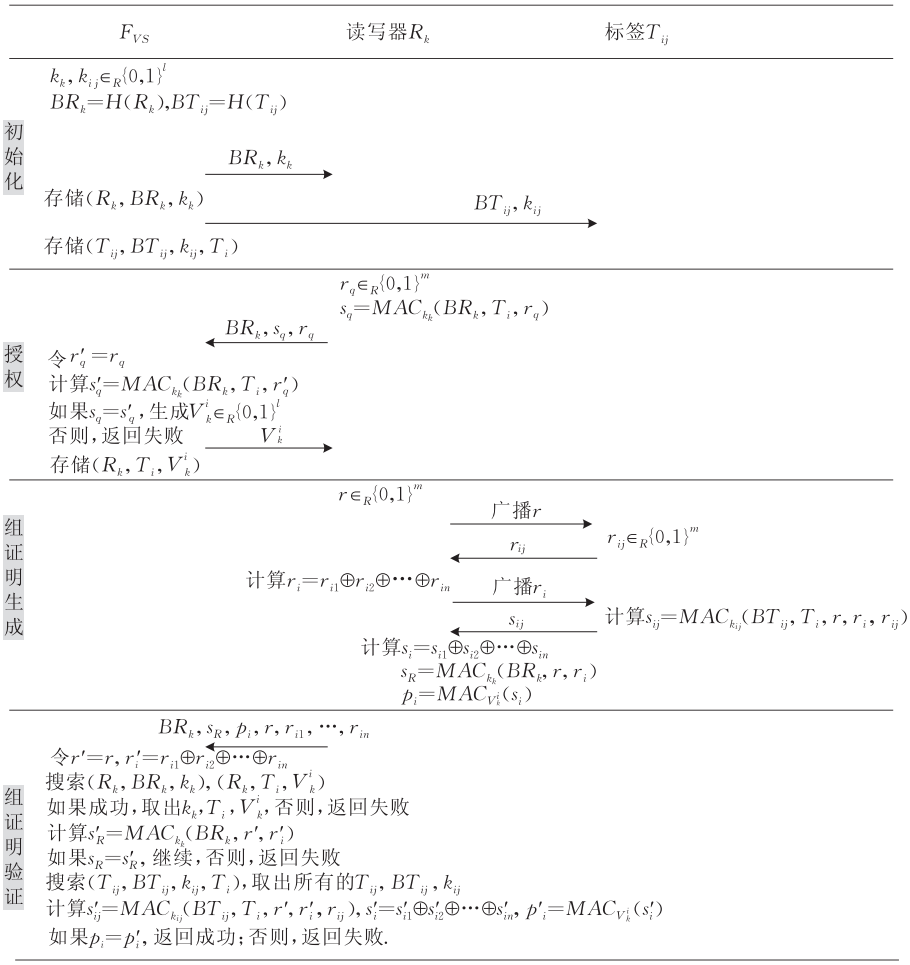

图 1 物联网环境下组证明 RFID 协议 π_{GP}

(2)理想攻击者 S 的具体操作. 当 S 从 F_{GP} 处收到$(ssid, BR_k)$时，生成一个新的子会话 $ssid$，然后将$(ssid, BR_k)$发送给仿真的攻击者 A. 当 S 从 F_{GP} 处收到$(ssid, BT_{ij})$时，生成一个新的子会话 $ssid$，然后将$(ssid, BT_{ij})$发送给仿真的攻击者 A. 当仿真的标签 T_{ij} 输出 s_{ij} 时，S 获得 s_{ij} 并向理想功能 F_{GP} 发送指令$(Proof, ssid, BT_{ij}, s_{ij})$. 当仿真的读写器 R_k 输出 $BR_k, s_R, p_i, r, r_{i1}, \cdots, r_{in}$ 时，S 获得 $BR_k, s_R, p_i, r, r_{i1}, \cdots, r_{in}$ 并向 F_{GP} 发送指令$(Verify, sid, BR_k, BR_k, s_R, p_i, r, r_{i1}, \cdots, r_{in})$.

(3)仿真器的有效性. 令 CTI 表示标签 T_{ij} 被攻陷的事件，CRI 表示读写器 R_k 被攻陷后进行非授权访问的事件，下面我们证明无论 CTI 和 CRI 发生与否，对于环境机 Z 而言，真实协议 π_{GP} 和理想功能 F_{GP} 都是不可区分的.

当 CTI 发生时，环境机 Z 触发指令$(Activate, sid)$后，S 从 F_{GP} 处收到$(ssid, BT_{ij})$，然后把$(ssid, BT_{ij})$发送给仿真的攻击者 A. 当仿真的读写器 R_k 输出 $BR_k, s_R, p_i, r, r_{i1}, \cdots, r_{in}$ 时，S 获得相同的输入给理想功能 F_{GP}. 因此，对于环境机 Z 而言，仿真的协议 π_{GP} 和理想功能 F_{GP} 得到的是同样的输出，是不可区分的.

同理得证，当 CRI 发生时，对于环境机 Z 而言，真实协议 π_{GP} 和理想功能 F_{GP} 也是不可区分的.

下面证明：当 CTI 和 CRI 都没有发生时，对于环境机 Z 而言，真实协议 π_{GP} 和理想功能 F_{GP} 是不可区分的.

假设存在一个环境机 Z' 能以不可忽略的概率区分 F_{VS}-混合模型下攻击者 A 和协议 π_{GP} 的交互以及理想环境下攻击者 S 和理想功能 F_{GP} 的交互，那么对于构建的仿真器 S 也可以区分真实协议 π_{GP} 和理想功能 F_{GP}. 在理想环境下仿真一份真实环境下的攻击者 A、读写器 R_k 和标签组 T_i 以及理想功能 F_{VS} 的拷贝，仿真的协议 π_{GP} 正常执行后，由 R_k 输出的 $p_i = MAC_{V^i_k}(s_i)$ 和 S 访问理想功能 F_{GP} 得到的输出 $p_i = H_{V^i_k}(s_i)$ 是可区分的. 显然，可以利用 Z' 构造一个算法 A，使得 A 能够找到带 key 的消息认证码 $MAC_k(\cdot)$ 的一个碰撞，从而违背了 MAC 函数的无碰撞假设. 所以假设不成立.

定理得证. 证毕.

根据 UC 框架的定义以及定理 1，我们在第 3 节中已经证明了 F_{GP} 可以满足所有的安全性需求. 因此协议 π_{GP} 也可以满足所有的安全性需求，即强隐私保护、不可追踪性、读写器匿名性、标签匿名性和授权认证.

5.2　效率分析

下面将本文提出的协议和已有的最新类似成果进行比较(见表 1 和表 2). 由于系统初始化和授权部分属于一次性执行过程，故在下表中未做统计. 其中 F 表示满足，D 表示不满足，Pr 表示调用随机数运算，Po 表示按位异或运算，Ph 表示 Hash 运算，Pc 表示冗余校验运算，$|r|$ 表示随机数的长度，$|h|$ 表示 Hash 函数的输出长度，$|ID|$ 表示身份标识的长度，N 表示组成员数.

表 1　类似协议安全属性比较

方案	强隐私保护	不可追踪性	匿名性	授权认证	可扩展性
文献[16]	D	D	F	D	D
文献[17]	D	D	D	D	D
文献[18]	D	D	F	F	D
文献[19]	F	F	F	D	D
文献[20]	F	F	F	D	D
新协议	F	F	F	F	F

表 2　类似协议性能比较

方案	T 的运算量	T 的存储需求①	R 的运算量	R 的存储需求①	DB 运算量②	组证明长度/Byte②
文献[16]	$N(Pr+3Ph)$	4	Pr	1	$O(N)$	$\|ID\|+N(\|r\|+2\|h\|)$
文献[17]	$2(Pr+Po)+Pc$	1	—	1	$O(N^2)$	$N(\|ID\|+\|r\|)$
文献[18]	$5Ph+2Po$	5	$2Ph$	4	$O(1)$	$N(\|ID\|+5\|h\|)$
文献[19]	$11Pr+9Po$	2	—	0	$O(N)$	$N(\|ID\|+2\|r\|)$
文献[20]	Ph	1	$N(Pr+Po)$	0	$O(N)$	$N(\|ID\|+\|r\|+\|h\|)$
新协议	$Pr+Ph$	1	$Pr+2Ph+2NPo$	1	$O(1)O(N)$	$\|ID\|+N\|r\|+2\|h\|$

注：① 按照除 ID 外需要存储的额外参数数量统计；② 基于 1 个读写器对 N 个标签的情况的统计.

从表 1 和表 2 可以看出，新协议不仅满足了强隐私保护、不可追踪性、匿名性、授权认证和可扩展性等物联网环境下组证明 RFID 协议的安全需求，而且组证明长度是最小的. 通过比较，在我们的方案中，RFID 标签的计算复杂度和存储需求都比较小，而后端的验证压力相比其它方案略有增加，这是非常适合物联网的体系结构的.

6　结束语

物联网是一个具有多网融合、海量数据采集和处理等特征的综合环境. 作为接入层协议的重要组成部分，组证明 RFID 协议在设计时，必须要考虑物联网的特异性和安全需求. 本文对物联网环境下组证明 RFID 协议的交互模型和攻击模型做了分析和描述，并在 UC 框架下，形式化定义了理想功能 F_{VS} 和 RFID 组证明理想功能 F_{GP}. 然后，设计了一个组证明 RFID 协议 π_{GP}，并证明对于任意的攻击者而言，协议 π_{GP} 安全地实现了理想功能 F_{GP}.

参　考　文　献

[1] International Telecommunication Union. ITU Internet Reports 2005: The Internet of Things, ITU, 2005

[2] Zhou Yong-Bin, Feng Deng-Guo. Design and analysis of cryptographic protocols for RFID. Chinese Journal of Computers, 2006, 29(4): 581-589 (in Chinese)
(周永彬，冯登国. RFID 安全协议的设计与分析. 计算机学报，2006，29(4)：581-589)

[3] van Deursen T, Mauw S, Radomirovic S. Untraceability of RFID protocols//Proceedings of the 2nd International Workshop on Information Security Theory and Practice. Seville, Spain, 2008: 1-15

[4] Ha J, Moon S, Zhou J, Ha J. A new formal proof model for RFID location privacy//Proceedings of the 13th European Symposium on Research in Computer Security. Málaga, Spain, 2008: 267-281

[5] van Deursen T, Radomirovic S. On a new formal proof model for RFID location privacy. Information Processing Letters, 2009, 110(2): 57-61

[6] Lim C H, Kwon T. Strong and robust RFID authentication enabling perfect ownership transfer//Proceedings of the 8th International Conference on Information and Communications Security. Raleigh, NC, USA, 2006: 1-20

[7] Le T V, Burmester M, de Medeiros B. Universally composable and forward-secure RFID authentication and authenticated key exchange//Proceedings of the 2007 ACM Symposium on InformAtion, Computer and Communications Security. Singapore, 2007: 242-252

[8] Ouafi K, Phan R C W. Traceable privacy of recent provably-secure RFID Protocols//Proceedings of the 6th International Conference on Applied Cryptography and Network Security. New York, NY, USA, 2008: 479-489

[9] Phan R C W, Wu J, Ouafi K, Stinson D R. Privacy analysis of forward and backward untraceable RFID authentication schemes. Wireless Personal Communications, Springer, Netherlands, 2010: 1-13

[10] Song B, Mitchell C J. Scalable RFID security protocols supporting tag ownership transfer. Computer Communications, 2011, 34(4): 556-566

[11] Juels A. "Yoking-Proofs" for RFID tags//Proceedings of the

2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops. Washington, DC, USA, 2004: 138-143

[12] Saito J, Sakurai K. Grouping proof for RFID tags//Proceedings of the 19th International Conference on Advanced Information Networking and Applications. Xinbei, Taiwan, China, 2005: 621-624

[13] Piramuthu S. On existence proofs for multiple RFID tags// Proceedings of the ACS/IEEE International Conference on Pervasive Services. Lyon, France, 2006: 317-320

[14] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador M J, Ribagorda A. Solving the simultaneous scanning problem anonymously: Clumping proofs for RFID tags//Proceedings of the 3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing. Istanbul, Turkey, 2007: 55-60

[15] Lin C C, Lai Y C, Tygar J D, Yang C K, Chiang C L. Coexistence proof using chain of timestamps for multiple RFID tags//Proceedings of the 9th Asia-Pacific Web Conference/8th International Conference on Web-Age Information management. Huangshan, China, 2007: 634-643

[16] Burmester M, de Medeiros B, Motta R. Provably secure grouping-proofs for RFID tags//Proceedings of the 8th International Conference on Smart Card Research and Advance Applications. London, UK, 2008: 176-190

[17] Huang H H, Ku C Y. A RFID grouping proof protocol for medication safety of inpatient. Journal of Medical Systems, 2009, 33(6): 467-474

[18] Chien H Y, Liu S B. Tree-based RFID yoking proof//Proceedings of the 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing. Wuhan, China, 2009: 550-553

[19] Peris-Lopez P, Orfila A, Hernandez-Castro J C, van der Lubbe J C A. Flaws on RFID grouping-proofs. Guidelines for future sound protocols. Journal of Network and Computer Applications, 2011, 34(3): 833-845

[20] Duc D N, Konidala D M, Lee H, Kim K. A survey on RFID security and provably secure grouping-proof protocols. International Journal of Internet Technology and Secured Transactions, 2010, 2: 222-249

[21] Canetti R. Universally composable security: A new paradigm for cryptographic protocols//Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science. Las Vegas, Nevada, USA, 2001: 136-145

[22] Sun H M, Ting W C, Chang S Y. Offlined simultaneous grouping proof for RFID tags//Proceedings of the 2nd International Conference on Computer Science and its Applications. Jeju, Korea, 2009: 404-409

ZHANG Zhong, born in 1978, Ph.D. candidate. His research interests include information security and protocol formal proof.

XU Qiu-Liang, born in 1960, professor, Ph. D. supervisor. His main research interests include information security and cryptology.

Background

The grouping-proof protocols enables multiple RFID tags to be scanned simultaneously by a reader within its broadcast range. A typical application of the grouping-proof protocol is to scan tags that are supposed to stay together. For example, RFID tags attached on different parts of a car should be located near each other. Recently, more and more scholars paid attention to this topic and proposed their grouping-proof protocols. However, most of the proposals were analyzed and proved to be insecure.

In recent years, with the rapid development of the Internet of Things, provable secure RFID protocol is becoming a hot topic. However, as far as we know, the research of grouping-proof protocols in the IOT is still relatively few. So, It's important to design a RFID grouping-proof protocol of security and high efficiency in the security for the IOT.

The main contribution of this paper is to present an attack model and identify the unique set of security requirements for RFID grouping-proof protocols. Then we propose a universally composable model that satisfies the security requirements, and a novel grouping-proof scheme that is proved UC secure.

This research is supported by the National Natural Science Foundation of China (No. 60873232). The main task of the project is to design and analyze multiparty-oriented cryptosystems, which includes multiparty-oriented encryption schemes, multiparty-oriented signature schemes and multiparty-oriented authentication schemes etc. The research results are mainly to meet security requirements of multiparty-oriented applications. The team has published several research papers and scientific reports in important journals and international conference, such as Chinese Journal of Computers, Journal on Communications, ASIACRYPT 2010 etc. The scheme proposed is an important part of the project.