前向隐私安全的低成本 RFID 认证协议

马昌社

(华南师范大学计算机学院 广州 510631)

摘 要 标签成本和隐私安全是制约 RFID 技术在物联网中得到广泛应用的主要因素.因此,设计隐私安全且标签生产成本低的 RFID 认证协议是学术界和工业界共同追求的目标.针对这一目标,利用只需要实现伪随机数发生器的标签构造了简单的 RFID 认证协议 SFP,并在标准模型下证明了 SFP 协议具有前向隐私安全性.为了说明在保证前向隐私的条件下 SFP 协议的标签生产成本低,证明了标签具有产生伪随机数的能力是保证 RFID 前向隐私的必要条件.因此,与现有 RFID 协议相比较,SFP 协议不但计算和通信效率高,而且同时保证了前向隐私安全和低标签生产成本,实现了 RFID 技术低标签成本和高隐私安全的结合.

关键词 RFID;认证协议;前向隐私性;可证明隐私;伪随机数发生器;物联网
中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2011.01387

Low Cost RFID Authentication Protocol with Forward Privacy

MA Chang-She

(*School of Computer, South China Normal University, Guangzhou* 510631)

Abstract Tag cost and privacy of RFID technology are two main factors that determine whether it will be applied to Internet of Things on a large scale. Recently, RFID industry and research community have focused on RFID authentication protocols with provable privacy and low tag cost. In this paper, we firstly construct a simple RFID authentication protocol SFP using tags only equipped with pseudorandom generator. Secondly, we have proven that SFP is forward private in the standard model. Finally, we provide a comparatively rigorous proof of the necessary condition (i.e. each tag is able to generate pseudorandom numbers) to guarantee RFID forward privacy. In this sense, the tag of SFP protocol will be produced with low cost. Compared with currently existing RFID protocols, SFP not only is efficient in both computation and communication but also guarantees both forward privacy and low tag cost. Hence, protocol SFP has realized the integration of low tag cost and high security of RFID technology.

Keywords radio frequency identification; authentication protocol; forward privacy; provable privacy; pseudorandom generator; Internet of Things

1 引 言

物联网被称为继计算机、互联网之后,世界信息产业的第三次革命.而 RFID(Radio Frequency IDentification)[1]技术即射频识别技术是物联网感知层的关键技术之一,它为物体和对象提供非接触式、即时识别的功能[2-3].尽管物联网的潜在商业应用前景美好[4],但是成本和隐私安全始终制约着物联网应用的广泛开展,该问题主要涉及 RFID 技术的低成本与高隐私安全结合的问题[5-6].工业界从低标签成本要求出发设计出来的 RFID 技术不能保证

收稿日期:2011-03-23;最终修改稿收到日期:2011-06-26.本课题得到国家自然科学基金(61070217)资助.**马昌社**,男,1974 年生,博士,副教授,主要研究方向为信息安全及物联网安全技术.E-mail: changshema@gmail.com.

隐私安全性[7]；而学术界从隐私安全角度出发设计的 RFID 技术不能满足人们对低标签成本的要求. 因此，一个亟待解决的问题是：能否设计出同时具有低标签成本和隐私安全的 RFID 认证协议？因为标签的成本主要取决于其计算能力①，因此换一句话说，能否设计出标签计算能力要求低且隐私安全的 RFID 认证协议？对这个问题的回答，有助于工业界和学术界的结合，以较低的代价获得 RFID 隐私安全，为物联网的应用和发展奠定理论基础.

为了得到同时具有隐私安全和低标签生产成本的 RFID 认证协议，本文专门研究前向隐私安全[6]的 RFID 认证协议的构造和 RFID 前向隐私安全对标签计算能力的要求. 首先，利用只需要实现伪随机数的标签构造了一个简单的 RFID 认证协议 SFP (Simple and Forward Private)，并在标准模型下证明了 SFP 协议具有前向隐私安全. 其次，为了说明在保证前向隐私安全的条件下 SFP 协议的标签生产成本低，证明了标签具有产生伪随机数的能力是保证前向隐私的必要条件②. 从这点来看，SFP 协议的标签恰好满足前向隐私对标签计算能力的最低要求，这意味着 SFP 协议的标签具有更低的生产成本. 因此，与现有可证明隐私安全的 RFID 认证协议相比较，SFP 协议不但计算和通信效率高，而且能够同时保证前向隐私和低标签生产成本. 本文工作不但实现了 RFID 前向隐私安全和低标签生产成本的结合，而且为 RFID 隐私安全协议的设计提供了蓝本.

本文第 2 节回顾 RFID 隐私相关研究工作；第 3 节介绍描述 SFP 协议和分析其安全性需要的数学符号和安全模型；第 4 节提出前向隐私安全的 RFID 认证协议 SFP，并对其进行安全和成本分析；第 5 节对新协议 SFP 和现有协议进行效率比较；最后，第 6 节总结全文.

2 RFID 隐私相关研究

目前，业界对 RFID 隐私的研究主要从两个方面进行. 一方面，设计轻量级的 RFID 认证协议，提出了若干兼容 EPC C1 G2 标准的 RFID 隐私安全解决方案和协议[8-10]，但是它们都不具有完善的隐私安全性. 另一方面，研究 RFID 隐私安全模型，目前已提出了分别基于不可区分性和不可预测性的安全模型[5].

在轻量级 RFID 协议设计方面，采用简单操作(比如：比特异或、比特内积、16 bits 的随机数发生器等)，文献[9-10]分别设计了简单的 RFID 双向认证协议. 然而，这两个协议都容易遭到隐私攻击[11]. 采用对称密码技术，文献[12]首次提出了一个基于树的 RFID 认证系统，然而该系统不能抵抗主动攻击. 实际上，在基于树的 RFID 系统中，所有标签之间需要或多或少地共享某些秘密信息，读取某一标签的内部状态后，可以利用它攻击其它标签的隐私性，因此基于树的 RFID 系统[13]都不能抵抗主动跟踪攻击. 基于 Hash 函数，文献[14]设计了一个具有前向隐私安全的 RFID 系统(OSK 协议)，但是该系统的可扩展性不好，因为阅读器端识别标签所需要的计算量与 RFID 系统中标签的数目成线性关系. Avoine 和 Oechslin[15]利用时间存储权衡技术对 OSK 协议进行了优化. 然而，优化后的协议仍然不具有良好的可扩展性，同时易于遭受身份假冒攻击[16-17]. 此后，研究者们采用状态同步技术并结合 Hash 链提出了各种各样的 RFID 认证协议，比如：Tsudik 提出了基于时间同步的 YATRAP 协议[18]，分析表明 YATRAP 协议易于遭受异步攻击；随后，Burmester 等人[19]提出了 YATRAP+协议和 OTRAP 协议，这两个协议克服了异步攻击. 然而，文献[7]指出了现有 RFID 协议中的大部分仍不具有隐私安全性. 另外，文献[20]设计了基于 LPN 问题的 RFID 认证方案，与所有基于 LPN 问题的 RFID 认证协议一样，该方案只提供认证性，不具有隐私安全性. 因此，如何设计高效且隐私安全的 RFID 认证协议仍需进一步研究.

在 RFID 安全模型方面，早在 2006 年，周永彬和冯登国[21]对 RFID 协议的认证安全性进行了分析，提出了 RFID 协议的认证模型. Avoine[22]对 RFID 协议的隐私性进行了抽象并提出相应的隐私安全模型(简称 Avoine 模型)，然而该模型没有考虑主动攻击. 后来，在 Avoine 模型的基础上，Juels 等人[23]提出了基于不可区分性的 RFID 隐私模型(简称 Ind-privacy)；Vaudenay[24]考虑了边信道攻击，提出了 8 种 RFID 隐私安全模型；Ng 等人[25]把这 8 种

① 这里的计算能力是指计算某种函数的能力，而不是指 CPU 频率的高低，比如：计算单向函数的能力、计算对称加密的能力等. 这种计算能力直接决定了标签中实现该函数所需要的门电路数目，从而决定了标签的生产成本.

② 现有大部分密码算法和安全协议中都使用了伪随机数发生器，于是安全界普遍认为伪随机数发生器是提供安全的必要条件(实际上并非如此，比如产生消息认证码就不需要伪随机数发生器)，但安全界对这一结论并没有给出严格的数学证明. 因此有必要从理论上来找到并证明保证 RFID 前向隐私的必要条件.

安全模型简化到了 4 种安全模型；而 Ha 等人[26]提出了基于不可预测性(Unpredictability)的 RFID 隐私安全模型(简称 unp-privacy). 在 ACM CCS'09 上，Ma 等人[5]研究了 ind-privacy 和 unp-privacy 之间的关系. 最近，在 ACNS'10 上，Lai 等人[27]对 unp-privacy 模型进行了修正，并提出了一个具有 unp-privacy 的双向 RFID 认证协议. 在 ESORICS'10 上，Deng 等人[28]提出了基于零知识的 RFID 隐私安全模型zk-privacy，并设计了一个满足该模型的双向认证协议. 张帆等人在文献[29]中提出了通用可组合的 RFID 隐私认证模型并设计了相应的认证方案.

3　预备知识

假设 S 表示一个集合，$s\in_R S$ 表示从集合 S 中随机选取一个元素 s；$\{0,1\}^l$ 表示所有比特长度为 l 的二进制比特串的集合；如果 $x_1,x_2,\cdots$ 表示比特串，那么 $x_1\|x_2\|\cdots$ 表示这些串按比特的链接；$|x_1|$ 表示比特串 x_1 的比特长度；符号 $y\leftarrow A^{O_1,\cdots,O_n}(x_1,\cdots,x_n)$ 表示算法 A 的输入是 $x_1,\cdots,x_n$，并且算法 A 可以查询语言机 $O_1,\cdots,O_n$，其输出赋值给 y；$Pr[E]$ 表示事件 E 发生的概率；假设 $F:D\to D$ 是一个函数，那么 $F^n(x)$ 表示对函数 F 的复合，也就是说

$$\forall x\in D,\ F^n(x)=\overbrace{F(\cdots F}^{n}(x)).$$

定义 1.　称函数 $\varepsilon:\{0,1\}^n\to R$ 是可以忽略不计的，如果它满足：对任意一个多项式 $p(n)$，当 n 充分大时有 $\varepsilon(n)<1/p(n)$.

3.1　RFID 系统

不失一般性，假设 RFID 系统中共有 n 个标签，它们是 $T=\{T_1,\cdots,T_n\}$，只有一个阅读器 R 和一个后端数据库系统 DB. 每一个标签由一个唯一的 ID 所标识，阅读器有一个或者多个射频收发器，后端数据库系统 DB 维护认证标签所需要的所有数据，比如标签的密钥、ID、状态信息等. 这里假设阅读器和后端数据库之间的通信是安全的，并且后端数据库属于安全数据库.

由于现有大部分 RFID 协议只有两轮或者三轮通信，因此本文仅考虑不超过三轮通信的 RFID 协议，如图 1 所示. 每一个标签中存储状态信息 s_T(包含标签的密钥)，并赋有一个计算函数 $F_T:\{0,1\}^{l_S}\times\{0,1\}^{l_1}\times\{0,1\}^{l_C}\to\{0,1\}^{l_S}\times\{0,1\}^{l_2}$，这里 l_S 和 l_C 分别表示状态信息和标签内部抛币消息的比特长度；l_1 和 l_2 分别表示协议第 1 轮和第 2 轮消息的比特长度. 当标签收到协议的挑战消息 $m_1\in\{0,1\}^{l_1}$ 之后，它利用函数 F_T(以 m_1 和 s_T 为输入参数)计算出一个应答消息 $m_2\in\{0,1\}^{l_2}$ 和一个状态更新消息 s'_T(可能为空串，意味着状态不更新)，也就是 $(m_2,s'_T)\leftarrow F_T(s_T,m_1,cn_T)$，这里 cn_T 是标签的内部抛币(它可能为空串). 此外，一个 RFID 系统 $RS=\{T,R,DB\}$ 还包含以下算法和协议.

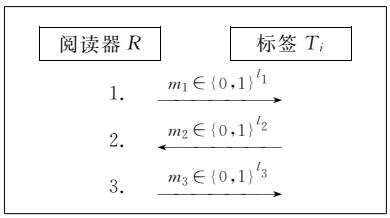

图 1　RFID 认证协议

Initialize(κ)：它为系统中每一个标签 T_i 产生密钥 k_i 并设置其初始状态(这里 κ 是一个安全参数)，同时，它把该标签的 ID 和相应的认证数据保存在后端数据库 DB 中；

ReaderStart()：调用阅读器产生一个会话标识 sid 和该会话的第 1 轮协议消息 m_1；

TagCompute(sid,m_1,T_i)：以消息 m_1 作为输入调用标签 T_i 产生协议第 2 轮消息 m_2；

ReaderCompute(sid,m_2)：调用阅读器，其输入是消息 m_2 和会话标识 sid，阅读器根据 sid 找到其对应的第 1 轮协议消息 m_1，然后计算出协议第 3 轮消息 m_3，最后输出 m_3；

$\pi(R,T_i)$：调用 R 和 T_i 执行一次完整的认证协议(如图 1 所示)，返回协议消息(m_1,m_2,m_3).

3.2　RFID 安全定义

由于低成本的 RFID 标签不具有任何防篡改的能力，因此攻击者可以很容易地通过破解标签来获得标签的内部状态，并利用获得的内部状态信息来攻击标签在被破解之前的通信隐私性(比如：跟踪标签、获取标签身份信息等). 前向隐私正是为了保证 RFID 系统在上述情况下的隐私安全性. 简单地说，在一个 RFID 系统中，攻击者可以窃听、篡改、伪造、阻断协议消息，它甚至可以破解任何一个标签从而获得该标签当前的内部状态信息(这些攻击能力在以下的隐私游戏中用预言机来模拟)，但是攻击者仍然不能跟踪(或者识别)标签在没有被破解之前的通信(或者身份)，这就是前向隐私，它指的是即使攻击者破解了某一个标签，但是该标签在被破解之前的所有通信隐私安全性仍能得到保证. 准确地说，前向隐私由下面的隐私游戏 $Game_A^{FP}$(见图 2)来定义，这

里 FP(Forward Privacy)表示前向隐私,A 表示攻击者,符号 $Game_A^{FP}$ 表示有攻击者 A 参与的前向隐私游戏.本文定义结合了文献[5-6]中定义隐私安全的方法.定义前向隐私的方法如下:首先利用隐私游戏 $Game_A^{FP}$ 模拟现实的 RFID 攻击环境;然后利用对两个标签行为的不可区分性定义隐私安全.隐私游戏 $Game_A^{FP}$ 包含一个攻击者和一个 RFID 系统.

$Game_A^{FP}(\kappa,n,q)$
1. 建立一个阅读器 R 和 n 个标签 $T=(T_1,\cdots,T_n)$;
2. $(T_0,T_1,st)\leftarrow A_1^{O_1,O_2,O_3,O_4}(R,T)$;
3. $\beta\in_R\{0,1\}$, $T'=T-\{T_0,T_1\}$
4. $\beta'\leftarrow A_2^{O_1,O_2,O_3,O_4}(R,T',T_\beta,st)$;

图 2 前向隐私游戏

攻击者. 这里假设任何一个攻击者都是一个概率多项式时间(PPT)算法,它可以完全控制阅读器和标签之间的通信.此外,攻击者 A 还可以和协议参与方之间进行交互,这些交互用以下预言机来刻画.

$Launch(R)$:触发阅读器产生一个新的协议会话,输出会话标识 sid 和协议的第 1 轮消息 m_1,它模拟搭线窃听获取协议第 1 轮消息;

$SendTag(sid,m_1,T_i)$:模拟篡改协议消息、搭线窃听和标签的计算 $TagCompute(sid,m_1,T_i)$,输出协议的第 2 轮消息 m_2;

$SendReader(sid,m_2)$:模拟篡改协议消息、搭线窃听和阅读器的计算 $ReaderCompute(sid,m_2)$,输出协议的第 3 轮消息 m_3;

$Reveal(T_i)$:模拟对标签的破解攻击,输出标签 T_i 的内部状态包括其密钥和状态信息.

假设 O_1,O_2,O_3,O_4 分别表示以上 4 个预言机,本文假设攻击者对这 4 个预言机的查询次数总共不超过 q 次.

前向隐私. 简单地讲,在 RFID 系统中尽管攻击者可以对 RFID 协议进行窃听、篡改、阻断,甚至可以破解标签获得其内部状态,但攻击者仍不能对两个标签的行为加以区分,这就是前向隐私.实际上,RFID 前向隐私由隐私游戏 $Game_A^{FP}$(见图 2)所定义,在该游戏中,攻击者 A 由算法 A_1 和 A_2 组成,A 对 RFID 系统的隐私攻击分两阶段实施.在第 1 阶段(也就是学习阶段),攻击者 A_1 初始化一个 RFID 系统 RS,并可以随意调用预言机 O_1,O_2,O_3,O_4.在这一阶段末,A_1 输出两个没有被调用过 Reveal 预言机的标签 T_0、T_1 和状态信息 st,并把 T_0 和 T_1 递交给游戏 $Game_A^{FP}$ 作为自己的候选挑战标签.在第 2 阶段(也就是挑战阶段),游戏首先选择一个随机比特 β,把 T_β 交个攻击者作为挑战标签,接下来攻击者实施第 2 阶段的攻击.在这一阶段,A_2 仍然可以对 T_β 随意调用预言机 O_1,O_2,O_3,O_4 进行查询.

最后,要求攻击者 A_2 猜测游戏选择的随机数 β,假设 A_2 的输出是 β'.如果 $\beta=\beta'$,则称攻击者 A 攻击 RFID 系统的前向隐私性成功.

定义 2. 在以上的前向隐私游戏中,攻击者 A 的优势定义为

$$\left|Pr[\beta=\beta']-\frac{1}{2}\right|.$$

定义 3(前向隐私性). 前向隐私性是指在游戏 $Game_A^{FP}$ 中,不存在一个多项式时间攻击者 A,其优势至少是 ε(不可忽略不计),且攻击时间不超过 t(多项式时间).或者称该 RFID 系统是 (ε,t,q)-前向隐私安全的.

认证性游戏[5]. A 是一个概率多项式时间攻击者,它可以对 RFID 系统进行预言机 O_1,O_2,O_3,O_4 的查询,最后 A 输出协议消息 (m_1,m_2,m_3) 和标签 T_c.如果标签 T_c 没有被查询过 Reveal 预言机,且 (m_1,m_2,m_3) 不是标签 T_c 和阅读器 R 之间的协议输出,即不存在会话标识 sid 满足 $(m_1,m_2,m_3)\leftarrow\pi(R,T_c,sid)$,则称 A 成功.

定义 4(认证性). 认证性是指对任何一个多项式时间攻击者 A,其在以上描述的认证性游戏中成功的概率是可以忽略不计的.或者称该 RFID 协议具有认证性.

4 前向隐私安全的 RFID 认证协议

本节首先利用具有少量存储空间、能够计算伪随机数发生器和比特异或的标签来构造一个具有前向隐私的 RFID 认证协议 SFP.然后扩充 SFP 协议为双向认证协议 MSFP,最后证明协议 SFP 具有前向隐私性和认证性并说明其标签生产成本低.

定义 5[30]. 称函数 $g:\{0,1\}^n\rightarrow\{0,1\}^l$ 是一个伪随机数发生器,如果它满足以下条件:

(1) $l>n$,并且对每一个 $x\in\{0,1\}^n$,存在多项式时间算法计算 $g(x)$;

(2) 对任意一个多项式时间算法 A 和测试值 y,概率 $|Pr[A(y)=1|y=g(s)]-Pr[A(y)=1|y=r]|$ 是可以忽略不计的,这里 $s\in_R\{0,1\}^n$ 且 $r\in_R\{0,1\}^l$.

4.1 RFID 认证协议 SFP

系统初始化. 根据安全参数 κ，首先选择一个伪随机数发生器 $g:\{0,1\}^{\kappa}\to\{0,1\}^{2\kappa}$ 和一个阈值 w，假设 $g=(g_1,g_2)$，这里 $g_1(s)$ 和 $g_2(s)$ 分别表示 $g(s)$ 的左半部分和右半部分，即

$$g(s)=g_1(s)\,\|\,g_2(s)\text{且}|g_1(s)|=|g_2(s)|=\kappa,$$

设置每一个标签使之具有计算伪随机数发生器 g 的能力，然后为每一个标签 T_i 选择其伪随机数发生器的初始种子 s_i 和一个身份 ID_i，最后把 s_i 存储在标签 T_i 中做为它的状态信息 st，同时把 (s_i,ID_i) 存储在后端数据库中以便在未来的通信中对标签 T_i 做出认证.

阅读器和标签间的认证协议 $\pi(\boldsymbol{R},\boldsymbol{T}_i)$（如图 3 所示，标签 T_i 的内部状态处于已经被认证了 u 次之后的状态，接下来进行第 $u+1$ 次认证）

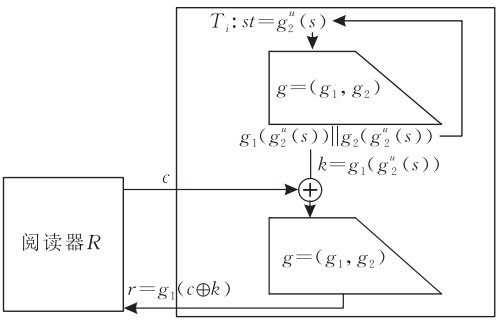

图 3　SFP 协议

(1) $ReaderStart()$：阅读器随机选择一个挑战消息 $c\in\{0,1\}^{l_1}$，然后把 c 发送给标签 T_i；

(2) $TagCompute(sid,c,T_i)$：假设标签 T_i 的当前内部状态信息 $st=g_2^u(s)$，即伪随机数发生器的当前种子为 st. 标签 T_i 收到挑战消息 c 后，按如下计算产生应答消息并更新其内部状态信息：首先计算 $g(st)=g_1(st)\,\|\,g_2(st)=g_1(g_2^u(s))\,\|\,g_2(g_2^u(s))$，令 $k=g_1(g_2^u(s_i))$，然后计算 $r=g_1(c\oplus k)$，并更新状态信息 $st=g_2(g_2^u(s_i))$；最后发送 r 给阅读器 R.

(3) $ReaderCompute(sid,r)$：阅读器收到应答消息 r 之后，对每一个 (s_i',ID_i') 计算 $r'=g_1(c\oplus g_1(s_i'))$，如果 $r=r'$ 则对标签 T_i 做出认证并更新 $s_i'=g_2(s_i')$. 否则，从 $j=2$ 到 w，依次对每一个 (s_i',ID_i') 计算 $r'=g_1(c\oplus g_1^j(s_i'))$，如果 $r=r'$ 则对标签 T_i 做出认证并更新 $s_i'=g_2^j(s_i')$. 最后，如果 $j>w$，则认证失败①.

效率的改进. 为了方便安全分析，上面仅给出了基于伪随机数发生器构造的 RFID 认证协议 SFP 的基本框架. 为了进一步提高协议认证的效率，SFP 协议可以按如下方式进行扩充：选取伪随机函数 $g=(g_1,g_2,g_3):\{0,1\}^{\kappa}\to\{0,1\}^{3\kappa}$，然后用 g_1 来生成对挑战消息的应答消息 r，用 g_2 来更新标签内部状态信息，用 g_3 来生成一个索引信息 $I=g_3(st)$，后端数据库中存储信息 (I,s_i,ID_i). 认证时，标签返回 (I,r) 给阅读器，后端数据库利用 I 进行检索找到相应元组 (I,s_i,ID_i)，判断 $r=g_1(c\oplus g_1(s_i))$？因此，仅需计算一次伪随机数发生器就可以实现对标签的认证. 从而使协议具有良好的可扩展性，以便适用于大规模的 RFID 应用场合.

4.2 双向认证协议 MSFP

SFP 仅提供对标签进行认证的功能，考虑到某些 RFID 应用场合同时需要对阅读器进行认证，因此这里把 SFP 扩充为双向认证协议 MSFP(Mutual SFP). 在 MSFP 中，选取伪随机数发生器 $g=(g_1,g_2,g_3):\{0,1\}^{\kappa}\to\{0,1\}^{3\kappa}$，MSFP 由三轮协议消息组成，其第 1 轮和第 2 轮协议消息与 SFP 完全一样，其第 3 轮协议消息的产生和标签对阅读器的认证按如下方式进行：

在第 2 轮通信中如果阅读器端对标签认证成功，那么它计算

$$f=g_2(g_1(s_i')\oplus g_3(s_i')),$$

然后更新 $s_i'=g_2(s_i')$ 并发送 f 给标签.

在第 2 轮通信中如果阅读器对标签认证失败，那么它计算

$$f=g_2(r),\ r\in_R\{0,1\}^{3\kappa},$$

然后发送 f 给标签.

最后，标签 T_i 收到消息 f 后，验证

$$f=g_2(k\oplus g_3(g_2^u(s))),$$

如果上述等式成立，则接受阅读器；否则，拒绝阅读器.

4.3 安全证明

这里仅对 RFID 协议 SFP 的安全性进行证明，协议 MSFP 的安全性证明以此类推. 协议 SFP 的安全性由以下定理 1 和 2 所保证.

定理 1（SFP 协议的认证性）. 假设 g 是一个伪随机数发生器且标签能够存储并更新 g 的种子，那么协议 SFP 具有认证性.

证明. 见附录 A.

定理 2（SFP 协议的前向隐私安全）. 假设 g 是一个伪随机数发生器且标签能够存储并更新 g 的种子，那么协议 SFP 具有前向隐私安全性.

① 保证标签能够被正确识别，协议 SFP 假设标签和阅读器之间的异步次数不能超过 w 次. 在安全性证明时，我们仍然假设每一个标签被查询 $SendTag$ 预言机的次数也不超过 w 次.

证明. 见附录 A.

4.4 SFP 协议标签成本低特性

因为标签的主要生产成本取决于其计算能力的高低,因此要说明 SFP 协议的标签生产成本低,只需要说明在保证 RFID 前向隐私安全的条件下标签的计算能力需求低即可. 为此,本节特证明标签具有计算伪随机数发生器的能力是保证 RFID 认证协议前向隐私的必要条件. 这里假设标签只有非常有限的存储空间.

定理 3(前向隐私的必要条件). 假设 RFID 认证协议 π 具有认证性和前向隐私性,那么 RFID 系统中每一个标签的计算能力可以用来计算一个伪随机数发生器.

证明. 见附录 B.

必要条件的含意如下:

(1)能够产生伪随机数是 RFID 协议前向隐私安全对标签计算能力的最低要求,而协议 SFP 仅要求标签产生伪随机数. 协议 SFP 采用保证 RFID 前向隐私的最低标签计算能力设计,生产成本低.

(2)必要条件只是表明标签的计算能力等价于计算伪随机数发生器的能力,这并不意味着标签内部一定实现了伪随机数发生器. 实际上,标签内部可以采用比伪随机数发生器计算能力更高的函数(比如:对称加密函数等)来计算 RFID 协议消息,但是这意味着增加了标签的生产成本.

(3)定理 3 一方面解释了为什么现有 RFID 系统中采用简单操作(比特异或等,这些操作的计算能力都低于伪随机数发生器的计算能力)设计的协议不具有隐私安全性;另一方面为设计具有前向隐私性的 RFID 认证协议提供了参考依据,可以避免通过盲目地降低标签计算能力来设计具有隐私安全的轻量级 RFID 认证协议.

作为本文研究的派生,结合定理 2 和 3,可以得出如下关于 RFID 前向隐私和标签计算能力之间的关系.

定理 4(前向隐私的充要条件). 如果 RFID 认证协议 π 具有认证性且标签具有存储并更新伪随机数发生器种子的能力,那么 π 具有前向隐私性的充分必要条件是:标签的计算能力能够用来计算伪随机数发生器.

证明. 从定理 2 和定理 3 可以直接看出定理 4 成立.

充要条件的含意如下:

(1)在设计具有前向隐私安全的 RFID 协议时,仅需要标签能够产生伪随机数即可,而不需要标签具有其它计算功能(比如 Hash 函数、对称加密、公钥加密等). 但这并不意味着每一个能够产生伪随机数的标签都具有前向隐私性. 在标签能够产生伪随机数的前提条件下,仍需合理地设计标签和阅读器之间的认证协议,才能得到具有可证明前向隐私的 RFID 认证协议.

(2)伪随机数是安全技术的基础,现有的密码构件中大部分含有伪随机数发生器. 因此,定理 4 保证了人们可以从现有密码技术和设备出发很容易地获得具有前向隐私安全的 RFID 应用系统.

5 效率分析和比较

前面设计了简单的认证协议 SFP 并在标准模型下证明了其安全性,这里讨论该协议参数的选取和效率比较分析.

5.1 协议 SFP 的参数选择

主要是关于伪随机数发生器的选择,最近欧盟的 eStream 项目为我们提供了多种选择. 该项目中的流密码算法 Grain 和 Trivium 都可以做为协议 SFP 中伪随机数发生器的候选算法. 根据文献[31],Grain 和 Trivium 的硬件实现分别只需要 3360 和 3090 个 GE(Gate Equivalents),就可以达到 80 bits 的安全水平. 实际上,它们的硬件实现中都包含初始向量的存储,而协议 SFP 中的伪随机数发生器不需要初始向量,因此,它们在协议 SFP 中的实现会更简单,可以减少到 1294 个 GE[6]. Grain 和 Trivium 的密钥长度为 64~128 bits,这意味着协议 SFP 中的伪随机数发生器的种子可以选择 64~128 bits.

5.2 效率比较

在 RFID 系统中,标签容易成为系统的效率瓶颈. 因此,这里主要比较标签的计算和通信开销以及标签完成计算所需的门电路复杂性. SFP 协议和其它协议(学术界具代表性的 4 个协议:OSK[14]、OTRAP[19]、MLDL[5] 和 PFP[6])的比较结果见表 1. 表中的数据由下面的计算得出.

表 1 效率和安全比较

协议	计算时钟周期数	标签的门复杂度	通信/bits	前向隐私
OSK[14]	2548	16240	240	是
OTRAP[19]	2064	3400	160	是
MLDL[5]	2064	3400	240	否
PFP[6]	264	5578	160	是
SFP	208	1294	160	是

关于标签的计算开销，因为它主要由对称密码操作的计算开销所决定，因此我们以协议中对称密码操作所需要的时钟周期(Clock Cycle，CC)数目来衡量协议的计算复杂性，忽略简单操作(比如：比特内积、比特异或等). 根据文献[31-32]中的结果可知：Hash 操作(SHA-1)的时钟周期数目为 1274[32]，伪随机函数(用对称加密 AES-128 来实现)的时钟周期数目为 1032[32]，伪随机数发生器(用流密码 Grain 来实现)的时钟周期为 104[31]. 根据文献[6](详见文献[6]的 6.2 节)，基于 $m\times l$ 阶 Toeplitz 矩阵实现的 Uinversal Hash 的时钟周期数目是 m. 协议 OSK 中的标签需要计算两个 Hash 函数，因此它的计算开销是 $1274\times 2=2548$ 个时钟周期；协议 OTRAP 和 MLDL 中的标签都需要计算两个伪随机函数，因此它们的计算开销均为 $1032\times 2=2064$ 个时钟周期；协议 PFP 中的标签需要计算一次伪随机数发生器和一次 Universal Hash 函数，因此它的计算开销是 $m+104$，要达到 80 bits 的安全，m 至少为 160，因此协议 SFP 的计算开销是 264 个时钟周期；协议 SFP 中的标签需要计算两个伪随机数发生器，因此它的计算开销是 $104\times 2=208$ 个时钟周期.

关于通信开销，我们考虑整个协议通信的比特数目. 如果选取安全水平为 80 bits，那么根据密码学常识易知：协议 SFP 中的安全参数 $\kappa\geq 80$；各个协议中的挑战消息、对称加密的输出、伪随机函数的输出以及伪随机数发生器的种子均至少为 80 bits；而 Hash 函数的输出至少为 160 bits. 协议 OSK 和 PFP 的消息都包括一个挑战消息和一个 Hash 函数的输出，因此它们通信开销均为 $80+160=240$ bits；协议 OTRAP 的消息包含一个挑战消息和一个伪随机函数的输出，因此其通信开销是 $80+80=160$ bits；协议 MLDL 的消息包括一个挑战消息和两个伪随机函数的输出，所以通信开销为 $80+160=240$ bits；协议 SFP 的消息包括一个挑战消息和半个伪随机数发生器的输出，因此其比特长度为 $|c|+\kappa=160$.

关于标签门电路复杂性，这里仅考虑密码操作所需要的门电路(GE)数目，而忽略简单计算所需门电路数目. 根据文献[32]，计算 Hash 函数(SHA-1)的门电路数目 $C_{\mathrm{H}}=8120$ 个 GE；计算伪随机函数(用对称加密 AES-128 来实现)的门电路数目为 $C_{\mathrm{PRF}}=3400$ 个 GE. 根据文献[6](详见文献[6]的 6.1 和 6.2 节)，计算伪随机数发生器(用流密码 Grain v1 来实现)的门电路数目为 $C_{\mathrm{PRG}}=1294$ 个 GE；计算基于 $m\times l$ 阶 Toeplitz 矩阵实现的 Universal Hash 的门电路数目为

$$C_{\mathrm{UH}}=12(m+l-1)+12m=4284$$

个 GE(根据 80 bits 安全需求选择 $m=160$，$l=38$). OSK 协议中的标签需要计算两个不同的 Hash 函数，因此其复杂度为 $2C_{\mathrm{H}}=16\,240$；OTRAP 协议和 MLDL 协议中的标签需要计算伪随机函数，因此它们的复杂度均为 $C_{\mathrm{PRF}}=3400$；PFP 协议中的标签需要计算伪随机数发生器和 Universal Hash 函数，因此其复杂度为 $C_{\mathrm{PNG}}+C_{\mathrm{UH}}=5578$；而 SFP 协议中的标签仅需要计算伪随机数发生器，因此其复杂度为 $C_{\mathrm{PNG}}=1294$.

通过表 1 可以看出：协议 SFP 不但在计算方面比协议 OSK、OTRAP、MLDL 以及 PFP 要高效，而且标签的门电路复杂度要远小于其它 4 个协议；在通信开销方面，协议 SFP 和协议 OTRAP 以及 PFP 保持一致，但是它比协议 OSK 和 MLDL 要高效. 总之，本文协议 SFP 在保持高效的同时，降低了对标签的计算要求，从而简化了标签的电路复杂性，降低了标签的生产成本.

6　结束语

安全和低成本是工业界对 RFID 技术的两个基本要求，但又是两个互相冲突的要求. 低成本的 RFID 不能保证安全性，满足一定安全要求的 RFID 标签成本较高. 能否设计出既具有隐私安全又具有低标签成本的 RFID 认证协议呢？这是人们急需解决的问题. 本文针对这个问题研究了前向隐私安全的 RFID 认证协议的设计和标签计算复杂度. 设计了一个优化的 RFID 认证协议 SFP. 与其它协议相比较，SFP 协议不但简单、高效、具有标准模型下的可证明前向隐私安全，而且对标签的计算要求低，从而协议 SFP 中的标签具有较低的生产成本. 同时，归纳出了保证 RFID 系统前向隐私的充分必要条件，解决了前向隐私和标签计算能力(也就是生产成本)之间的关系问题. 本文研究丰富了 RFID 隐私安全理论，为工业界生产具有前向隐私安全的 RFID 系统提供了指导.

本文结论表明：保证 RFID 前向隐私的充分必要条件是标签具有计算伪随机数发生器的能力. 而 EPC C1 G2 标准中的标签具有 16 bits 的伪随机数发生器，如何根据这种输出短的伪随机数发生器来构造满足一定安全强度的前向隐私的 RFID 认证协议，也就是说如何构造兼容 EPC C1 G2 标准的前向

隐私安全的 RFID 认证协议仍是一个值得进一步研究的问题.另一个值得研究的问题是:保证 RFID 协议一般 ind-隐私性的充分必要条件是什么? 我们将进一步对这两个问题进行研究.

致 谢 本文作者衷心感谢编辑部和审稿人提出的宝贵意见,帮助我们改正了本文的不足之处.

参 考 文 献

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

[2] Juels A, Pappu R, Parno B. Unidirectional key distribution across time and space with applications to RFID security// Proceedings of the 17th USENIX Security Symposium. San Jose, Canada, 2008: 75-90

[3] Molnar D, Wagner D. Privacy and security in library RFID: Issues, practices, and architectures//Proceedings of the Conference on Computer and Communications Security (ACM CCS'04). Washington, USA, 2004: 210-219

[4] Li Y, Ding X. Protecting RFID communications in supply chains//Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS'07). Singapore, Singapore, 2007: 234-241

[5] Ma C, Li Y, Deng R, Li T. RFID privacy: Relation between two notions, minimal condition, and efficient construction// Proceedings of the 16th ACM Conference on Computer and Communications Security (ACM CCS'09). Chicago, USA, 2009: 54-65

[6] Berbain C, Billet O, Etrog J, Gilbert H. An efficient forward private RFID protocol//Proceedings of the 16th ACM Conference on Computer and Communications Security (ACM CCS'09). Chicago, USA, 2009: 43-53

[7] Deursen T V, Radomirović S. Security of RFID protocols—A case study//Proceedings of the 4th International Workshop on Security and Trust Management (STM'08). Trondheim, Norway, 2009: 41-52

[8] Chien H-Y, Huang C-W. A lightweight RFID protocol using substring//Proceedings of the Embedded and Ubiquitous Computing (EUC2007). Taipei, China, 2007: 422-431

[9] Chien H-Y, Chen C-H. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. Computer Standars and Interfaces, 2007, 29(2): 254-259

[10] Konidala D, Kim Z, Kim K. A simple and cost-effective RFID tag-reader mutual authentication scheme//Proceedings of the Conference on RFID Security 2007. Malaga, Spain, 2007: 141-152

[11] Pietro R D, Molva R. Information confinement, privacy, and security in RFID systems//Proceedings of the 12th European Symposium on Research in Computer Security (ESORICS). Dresden, Germany, 2007: 187-202

[12] Molnar D, Soppera A, Wagner D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags//Proceedings of the Selected Areas in Cryptography (SAC 2005). Kingston, Canada, 2005: 276-290

[13] Lu L, Han J, Hu L, Liu Y, Ni L. Dynamic key-updating: Privacy-preserving authentication for RFID systems//Proceedings of the 5th IEEE International Conference on Pervasive Computing and Communications. New York, USA, 2007: 13-22

[14] Ohkubo M, Suzuki K, Kinoshita S. Cryptographic approach to "Privacy-Friendly" tags//Proceedings of the RFID Privacy Workshop 2003. Cambridge, USA, 2003: 624-654

[15] Avoine G, Oechslin P. A scalable and provably secure hash-based RFID protocol//Proceedings of the Pervasive Computing and Communications Workshops (PerCom 2005 Workshops). Kauai Island, USA, 2005: 110-114

[16] Dimitriou T. A lightweight RFID protocol to protect against traceability and cloning attacks//Proceedings of the Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm'05). Athens, Greece, 2005: 59-66

[17] Dimitriou T. A secure and efficient RFID protocol that could make big brother (partially) obsolete//Proceedings of the Pervasive Computing and Communications 2006. Pisa, Italy, 2006: 269-275

[18] Tsudik G. YA-TRAP: Yet another trivial RFID authentication protocol//Proceedings of the International Conference on Pervasive Computing and Communications (PerCom 2006). Pisa, Italy, 2006: 310-316

[19] Burmester M, val Le Tri, de Medeiros Breno. Provably secure ubiquitous systems: Universally composable RFID authentication protocols//Proceedings of the Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm'06). Baltimore, USA, 2006: 1-9

[20] Tang Jing, Ji Dong-Yao. Design and analysis of security protocols for RFID based on LPN problem. Journal of Electronics & Information Technology, 2009, 31(2): 439-443 (in Chinese)
(唐静, 姬东耀. 基于 LPN 问题的 RFID 安全协议设计与分析. 电子与信息学报, 2009, 31(2): 439-443)

[21] 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)

[22] Avoine G. Adversary model for radio frequency identification. Swiss Federal Institute of Technology (EPFL). Lausanne, Switzerland: Security and Cryptography Laboratory (LASEC), Technical Report LASEC-REPORT-2005-001, 2005

[23] Juels A, Weis S. Defining strong privacy for RFID//Proceedings of the International Conference on Pervasive Computing and Communications (PerCom 2007). New York, USA, 2007: 342-347

[24] Vaudenay S. On privacy models for RFID//Proceedings of the Advances in Cryptology(Asiacrypt 2007). Kuching, Malaysia. 2007: 68-87

[25] Ng C Y, Susilo W, Mu Y, Safavi-Naini R. RFID privacy models revisited//Proceedings of the 13th European Symposium on Research in Computer Security (ESORICS'08). Malaga, Spain, 2008: 251-266

[26] 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 (ESORICS'08). Malaga, Spain, 2008: 267-281

[27] Lai J, Deng R H, Li Y. Revisiting unpredictability-based RFID privacy models//Proceedings of the 8th International Conference on Applied Cryptography and Network Security (ACNS'10). Beijing, China, 2010: 475-492

[28] Deng R, Li Y, Yung M, Zhao Y. A new framework for RFID privacy//Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10). Athens, Greece, 2010: 1-18

[29] Zhang Fan, Sun Xuan, Ma Jian-Feng, Cao Chun-Jie, Zhu Jian-Ming. A universally composable secure RFID communication protocol in supply chains. Chinese Journal of Computers, 2008, 31(10): 1754-1767(in Chinese)
(张帆，孙璇，马建峰，曹春杰，朱建明. 供应链环境下通用可组合安全的 RFID 通信协议. 计算机学报，2008，31(10)：1754-1767)

[30] Blum M, Micali S. How to generate cryptographically strong sequences of pseudo-random bits. SIAM Journal on Computing, 1984, 13: 850-864

[31] Feldhofer M. Comparison of low-power implementations of Trivium and Grain//Proceedings of the Workshop on the State of the Art of Stream Ciphers (SASC 2007). Bochum, Germany, 2007: 236-246

[32] Feldhofer M, Wolkerstorfer J. Strong crypto for RFID tags—A comparison of low-power hardware implementations//Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS 2007). New Orleans, USA, 2007: 27-30

[33] Haitner I, Reingold O, Vadhan S. Efficiency improvements in constructing pseudorandom generator from any one-way function//Proceedings of the 42nd ACM Symposium on Theory of Computing (STOC 2010). Cambridge, USA, 2010: 437-446

附录 A.　RFID 协议 SFP 的安全证明.

为了证明协议 SFP 的认证性和前向隐私性，这里首先证明一个关于伪随机数发生器的结论. 假设 $g=(g_1,g_2)$: $\{0,1\}^\kappa\to\{0,1\}^{2\kappa}$是一个伪随机数发生器，且对于任意的 $s\in_R\{0,1\}^\kappa$满足 $|g_1(s)|=|g_2(s)|=\kappa$.

引理 A.1.　考察如下两个序列

$$D_0=\{g_1(s),g_1(g_2(s)),\cdots,g_1(g_2^{n-1}(s))\},$$

$$D_1=\{r_1,r_2,\cdots,r_n\},$$

这里 $r_i\in_R\{0,1\}^\kappa$, $i=1,2,\cdots,n$. 则 D_0 和 D_1 是计算不可区分的.

证明.　假设 D_0 和 D_1 不是计算不可区分的，我们将构造一个算法 B 来区分伪随机数发生器 g 的输出分布和随机均匀分布. 令 $y=(u,v)\in\{0,1\}^{2\kappa}$，首先定义序列

$$Y_i=r_1,\cdots,r_{i-2},u,g_1(v),g_1(g_2(v)),\cdots,g_1(g_2^{n-i}(v)),$$

这里 $i=2,\cdots,n$, $r_j\in_R\{0,1\}^\kappa$ $(j=1,2,\cdots,i-2)$，然后定义

$$Y_{n+1}=\{r_1,r_2,\cdots,r_{n-1},u\},$$

$$Y_{n+2}=\{r_1,r_2,\cdots,r_n\}=D_1,$$

$$Y_1=\{g_1(v),g_1(g_2(v)),\cdots,g_1(g_2^{n-1}(v))\}=D_0.$$

假设 A 是可以区分 D_0 和 D_1 多项式时间算法，其成功的优势为 ε. 接下来构造如下统计测试实验：

$Exp_A^i(y)(y=(u,v))$:

(1) 按上面的定义构造 Y_i;

(2) $b\leftarrow A(Y_i)$;

(3) 输出 b.

令 $p_i=Pr[Exp_A^i(y)=1]$. 当算法 B 收到来自伪随机数发生器的安全实验中的测试值 $y=(u,v)$之后，它随机选择一个指标 $i\in_R\{2,\cdots,n+2\}$，然后进行统计测试实验 $Exp_A^i(y)$. 于是

$$Pr[B(y)=1\,|\,y=g(s)]=\frac{1}{n+1}\sum_{i=2}^{n+2}Pr[Exp_A^i(g(s))=1]$$
$$=\frac{1}{n+1}(p_1+p_2+\cdots+p_{n+1}),$$

同理可得

$$Pr[B(y)=1\,|\,y=r]=\frac{1}{n+1}\sum_{i=2}^{n+2}Pr[Exp_A^i(r)=1]$$
$$=\frac{1}{n+1}(p_2+p_3+\cdots+p_{n+2}),$$

因此

$$|Pr[B(y=1)\,|\,y=g(s)]-Pr[B(y=1)\,|\,y=r]|$$
$$=\frac{1}{n+1}|p_1-p_{n+2}|\geq\frac{\varepsilon}{n+1}.$$

因此算法 B 以至少 $\varepsilon/(n+1)$ 的优势区分伪随机数发生器 g 的输出分布和均匀分布. 所以引理 A.1 成立.　证毕.

引理 A.2.　考察如下两个序列

$$D_0=g_1(s_x),g_1(g_2(s_x)),\cdots,g_1(g_2^n(s_x)),$$
$$g_1(s_y),g_1(g_2(s_y)),\cdots,g_1(g_2^\lambda(s_y)),g_2^{\lambda+1}(s_y),$$

$$D_1=x_0,x_1,\cdots,x_n,y_0,y_1,\cdots,y_\lambda,z,$$

这里 $s_x,s_y\in_R\{0,1\}^\kappa$ 且 $x_i,y_i,z\in_R\{0,1\}^\kappa$. 则序列 D_0 和 D_1 是计算不可区分的.

证明.　证明方法类似于引理 A.1 的证明.

接下来将在标准模型下证明本文协议 SFP 的安全性.

定理 1 的证明.

证明. 首先,由于标签具有存储并更新伪随机数发生器 g 的种子的能力,所以标签能够完成 SFP 协议要求标签存储状态信息的功能.其次,采用反正法.假设协议 SFP 不具有认证性,也就是说存在一个多项式时间攻击者 A,它能以不可忽略不计的优势 ε 成功地伪造一个有效的协议消息 $(\bar{c},\bar{r})\leftarrow\pi(R,T_c)$.假设 A 总共查询了 q 次预言机,那么可以构造一个算法 B 来区分序列 D_0 和 D_1,这里

$$D_0=\{g_1(s),g_1(g_2(s)),\cdots,g_1(g_2^{p-1}(s))\},$$

$$D_1=\{r_1,r_2,\cdots,r_p\},p>q.$$

算法 B 的构造如下:算法 B 首先通过随机选取种子来设置 $n-1$ 个标签,然后设置一个计数器 ctr,其初始值为 1,当接收到测试序列 $(y_1,y_2,\cdots,y_p)$ 后,B 用它来模拟对标签 T_c 的查询,对于其它 $n-1$ 个标签,算法 B 知道其初始内部状态,因此可以直接回答攻击者 A 的查询.如果攻击者 A 查询 $SendTag(sid,m_1,T_c)$,算法 B 返回 $g(y_{ctr}\oplus m_1)$ 给 A,并设置 $ctr=ctr+1$.最后,攻击者 A 输出一个协议消息 $(\bar{c},\bar{r})$,如果 $(\bar{c},\bar{r})$ 是伪造的有效协议消息,那么算法 B 输出 0 表示测试序列来自 D_0,否则输出 1 表示测试序列来自 D_1.

下面分析算法 B 成功的概率,分两种情况加以讨论.

情形 1. 如果测试序列 $(y_1,y_2,\cdots,y_p)$ 来自 D_0,那么算法 B 提供给攻击者 A 的攻击环境和认证性游戏完全一样,因此攻击者 A 能够以至少 ε 的优势成功.这意味着算法 B 能够以不小于 ε 的优势区分 D_0 和 D_1.

情形 2. 如果测试序列 $(y_1,y_2,\cdots,y_p)$ 来自 D_1,那么攻击者没有获得任何关于标签 T_c 当前内部状态的信息,根据伪随机数发生器的安全定义,成功猜测 $g(s)$(这里 $s\in_R\{0,1\}^\kappa$)的概率是可以忽略不计的,因此攻击者 A 成功的概率也是可以忽略不计的.

综合上述两种情形可知,算法 B 至少以 $\varepsilon/2$ 的优势来区分序列 D_0 和 D_1.这与 D_0 和 D_1 是不可区分的相矛盾.因此定理 1 成立. 证毕.

定理 2 的证明.

证明. 首先,由于标签具有存储并更新伪随机数发生器 g 的种子的能力,所以标签能够完成 SFP 协议要求标签存储状态信息的功能.其次,采用反正法.假设协议 SFP 不是前向隐私安全的,也就是说存在一个多项式时间攻击者 A 能够以不可忽略不计的优势攻击协议 SFP 的前向隐私性.假设 A 总共查询了 q 次预言机.那么可以构造一个多项式时间算法 B 来区分如下两个序列 D_0 和 D_1,其中

$$D_0=\{g_1(s_x),g_1(g_2(s_x)),\cdots,g_1(g_2^{\delta}(s_x)),$$
$$g_1(s_y),g_1(g_2(s_y)),\cdots,g_1(g_2^{\lambda}(s_y)),g_2^{\lambda+1}(s_y)\},$$

$$D_1=\{x_0,x_1,\cdots,x_n,y_0,y_1,\cdots,y_\lambda,z\},$$

这里 $\lambda\in_R\{1,2,\cdots,q\}$ 且 $\delta\geq q$.

算法 B 的构造如下:

接收到测试序列 $(z_1,\cdots,z_\delta,\omega_1,\cdots,\omega_\lambda,z)$ 之后,算法 B 选择 $n-2$ 个随机种子来初始化 $n-2$ 个标签,对于标签 T_x 和 T_y,算法 B 用测试序列来模拟对他们的查询.同时,随机选择一个抛币 $\beta\in_R\{0,1\}$,设置 $T_\beta=T_y$,$T_{1-\beta}=T_x$.最后,算法 B 设置两个计数器 $ctr1$ 和 $ctr2$,他们的初始值都为 1.接下来,算法 B 按如下方式模拟对 A 的查询的回答.在第 1 阶段,每当 A 查询 $SendTag(sid,c,T_x)$,算法 B 返回 $g(c\oplus z_{ctr1})$,同时设置 $ctr1=ctr1+1$;每当 A 查询 $SendTag(sid,c,T_y)$,算法 B 返回 $g(c\oplus\omega_{ctr2})$,同时设置 $ctr2=ctr2+1$.在第 2 阶段,算法 B 把 T_β 交给攻击者 A,然后按上面的方法模拟对 A 的查询的回答,当 A 查询 $Reveal(T_\beta)$ 时,算法 B 直接把 z 返回给 A.最后,攻击者输出一个比特 β',如果 $\beta=\beta'$,那么算法 B 输出 0 表示测试序列来自 D_0;否则,输出 1 表示测试序列来自 D_1.

下面分析算法 B 成功的优势.分两种情形讨论.

情形 1. 测试序列 $(z_1,\cdots,z_\delta,\omega_1,\cdots,\omega_\lambda,z)$ 来自 D_0,根据上面的模拟算法可知,B 模拟给 A 的攻击环境和前向隐私游戏的攻击环境完全一样.因此,攻击者 A 能够以优势 ε 成功的攻击协议 SFP 的前向隐私性.这意味着,算法 B 至少以 ε 的优势识别 D_0.

情形 2. 测试序列 $(z_1,\cdots,z_\delta,\omega_1,\cdots,\omega_\lambda,z)$ 来自 D_1,由于该序列中各个元素之间的独立性和随机性,攻击者 A 即使能够得到 z,但是仅以此信息它不能获得关于 z_i 和 ω_j 的任何有效信息,这里 $i=1,\cdots,\delta$,$j=1,\cdots,\lambda$.另一方面,z_i 和 ω_j 统计不可区分.因此,$g(z_i)$ 和 $g(\omega_j)$ 计算不可区分.所以,攻击者 A 只能以可以忽略不计的优势区分标签 T_x 和 T_y.

综合上述两种情形,可以看出,算法 B 能够以不可忽略的优势区分 D_0 和 D_1.这与 D_0 和 D_1 的不可区分性相矛盾.因此定理 2 成立. 证毕.

附录 B. 定理 3 的证明.

这里先回顾单向函数的定义.

定义 B.1. 称函数 $f:D\rightarrow R$ 是一个单向函数,如果它满足以下条件:

(1)对每一个 $x\in\{0,1\}^n$,存在多项式时间算法计算 $f(x)$;

对任意一个多项式时间算法 A,概率 $Pr[A(f(x))\in f^{-1}(f(x))]$ 是可以忽略不计的,这里 $x\in_R D$,$f^{-1}(y)$ 表示 y 的所有原像的集合,即 $f^{-1}(y)=\{x\in R\mid f(x)=y\}$.

引理 B.1.[33] 如果 $f:D\rightarrow R$ 是一个单向函数,那么利用 f 可以构造一个伪随机数发生器 g.

定理 3 的证明.

证明. 分两种情形来讨论.

情形 1. 标签 T_i 内部的随机抛币 cn_T^i 不是空串.根据随机抛币的安全性要求,那么该抛币函数的输出分布和随机均匀分布具有不可区分性.因此直接利用抛币生成函数就可以构造一个伪随机数发生器.

情形 2. 标签 T_i 内部的随机抛币 cn_T^i 为空串.我们首先

证明标签 T_i 的计算函数 F_T^i 是单向函数，然后根据引理 B.1 就可以构造出一个伪随机数发生器 g.

假设标签标签 T_i 的计算函数 F_T^i 不是单向函数. 那么可以构造一个算法 $A=(A_1,A_2)$，它能够以不可忽略不计的优势攻击该协议的前向隐私性. 算法 A 的构造如下：在第 1 阶段，A_1 选择两个标签 T_0 和 T_1，然后对 T_0 和 T_1 分别查询预言机 O_1，O_2，O_3，记录得到的回答. 假设关于 T_0 的回答为 $(sid_0, m_1^0, m_2^0, m_3^0)$，关于 T_1 的回答为 $(sid_1, m_1^1, m_2^1, m_3^1)$；最后 A_1 把 T_0 和 T_1 交给前向隐私游戏做为自己的候选挑战标签. 接下来在第 2 阶段，算法 A_2 获得挑战标签 T_β 之后，直接对其查询 Reveal 预言机，获得其内部状态 s_T^β 和计算函数 F_T^β，然后计算函数 F_T^β 在点 (m_2^0, s_T^β) 和 (m_2^1, s_T^β) 处的原像，假设这两个原像分别是 (s', m') 和 (s'', m'')，如果 $m'=m_1^0$，那么 A_2 输出 0；如果 $m''=m_1^1$，那么 A_2 输出 1；如果都不相等，那么 A_2 输出一个随机比特.

接下来，分析算法 A 成功的概率. 假设 Ω_0 表示函数 F_T^β 在点 (m_2^0, s_T^β) 处的所有原像的第 2 部分的集合，即

$$\Omega_0=\{m_1\in\{0,1\}^{l_1} \mid F_T^\beta(\bar{s}_T, m_1)=(m_2^0, s_T^\beta)\},$$

这里 $\bar{s}_T$ 为标签 T_β 的上一个状态信息. Ω_1 表示函数 F_T^β 在点 (m_2^1, s_T^β) 处的所有原像的第 2 部分的集合. 接下来证明集合 Ω_0 和 Ω_1 仅含有多项式个元素. 为此，先证明如下引理 B.2.

引理 B.2.　对任意一个标签 T_i 和任意的 (m_2, s_T^i)，假设 Ω_i 表示函数 F_T^i 在点 (m_2, s_T^i) 处的所有原像的第 2 部分的集合，那么 $\frac{|\Omega_i|}{2^{l_1}}$ 是可以忽略不计的.

证明.　假设存在某个标签 T_c 和某个点 (m_2^c, s_T^c)（这里 s_T^c 是标签 T_c 的内部状态信息）使得 $\frac{|\Omega_c|}{2^{l_1}}$ 不是可以忽略不计的，那么我们就可以构造一个算法 B 来攻击 RFID 协议的认证性. 算法 B 的构造如下：

假设 RFID 协议只包含两轮消息 (m_1, m_2)，算法 B 选取标签 T_c 做为攻击的目标标签，然后查询预言机 $Launch(R)$ 得到会话标识随机的挑战消息 (sid, m_1^c)，最后算法 B 输出 (m_1^c, m_2^c, T_c). 根据假设，

$$Pr[m_1^c\in\Omega_c]\geq\frac{|\Omega_c|}{2^{l_1}}$$

是不可忽略不计的，也就是说函数 F_T^c 在点 (m_1^c, s_T^c) 的原像的第 2 部分是 m_2^c 的概率是不可忽略不计的，即 (m_1^c, m_2^c) 属于 R 和 T_c 之间的合法协议消息的概率是不可忽略不计的. 因此，算法 B 以不可忽略不计的优势攻击了 RFID 协议的认证性. 这意味着违背了 RFID 协议的认证性.

所以，引理 B.2 成立.　　证毕.

根据上述引理 B.2，易知 $\frac{|\Omega_i|}{2^{l_1}}(i=0,1)$ 是可以忽略不计的. 因此，存在一个多项式 $p_i(l_1)$ 满足

$$|\Omega_i|=p_i(l_1),\ i=0,1.$$

如果 $\beta=0$，那么 $m'=m_1^0$ 的概率至少为 $1/p_0(l_1)$，而 $m''=m_1^1$ 的概率是可以忽略不计的. 类似的，如果 $\beta=1$，那么 $m''=m_1^1$ 的概率至少为 $1/p_1(l_1)$，而 $m'=m_1^0$ 的概率是可以忽略不计的. 所以算法 A 以不可忽略不计的优势攻击了 RFID 系统的前向隐私性.

所以标签 T_i 计算函数 F_T^i 是一个单向函数. 再根据引理 B.1，从该单向函数可以构造一个伪随机数发生器 g.

综合情形 1 和情形 2 可以知道，标签 T_i 的计算能力可以用来计算一个伪随机数发生器 g. 从而定理 3 成立.　　证毕.

MA Chang-She, born in 1974, Ph.D., associate professor. His research interests include cryptography, information security and security and privacy in Internet of Things.

Background

RFID (Radio Frequency Identification) is an automated object identification technology, where a reader identifies tags via wireless channels. However, the absence of physical contact during the identification process causes privacy issues of the tags. Many efforts have been made to guarantee the privacy of RFID systems. The research on RFID system privacy has been focused on two aspects: one is to construct RFID protocols that are compatible with the constraints of tags and the other is to formalize privacy models for RFID systems. In the former aspect, there are dozens of protocols being proposed, while many of them are reported to have privacy flaws. In the latter aspect, forward privacy has been introduced to be a basic privacy requirement for RFID systems since the tag is not tamperproof. In this paper, we concerned with the following fundamental problems.

Which kind of minimal cryptographic function in tags do

we need in order to guarantee the forward privacy of RFID systems? This problem must be clarified because of the following reasons. Firstly, many RFID protocols have been proposed, while the majority of them are found to be vulnerable to privacy related attacks, including all of the protocols (of no more than three rounds) without implementing cryptographic functions on tags and those based on symmetric key cryptography. It is therefore vital to investigate how RFID protocols should be designed to ensure RFID privacy. In particular, we want to know what the minimal computational power each tag should be equipped to ensure RFID forward privacy. A definite answer to this question will lead to the optimal tag design.

In this paper, we investigate the relations between the computational ability of tag and its forward privacy. We have found the sufficient and necessary conditions for guaranteeing the forward privacy of tags. Specifically, we have proven that if the RFID protocol is forward private then the tag is able to compute a pseudorandom generator and vice versa. According to such a theory, we presented an optimal forward private RFID authentication protocol SFP which is the simplest protocol so far in RFID community.

This research is supported by the National Natural Science Foundation of China under grant No. 61070217. This project is mainly focused on key issues of RFID privacy.