基于数字签名的轻量级RFID认证协议

刘亚丽[1] 秦小麟[2] 赵向军[1] 郝国生[1] 董永权[1]
(江苏师范大学计算机科学与技术学院 徐州 221116)[1]
(南京航空航天大学计算机科学与技术学院 南京 210016)[2]

摘 要 RFID系统的安全和隐私问题已成为阻碍其进一步扩展的瓶颈。针对低代价标签提出了一种基于签名方案的轻量级RFID认证协议,它利用数字签名技术和RFID认证技术的恰当结合,成功实现了RFID系统的轻量级认证机制。性能评估表明新协议除了具有主要的安全隐私性能属性之外,还能够抵抗多种典型的恶意攻击和威胁,其安全性依赖于在有限域上求解离散对数问题的困难性和伪随机数生成器的安全性。新协议将公钥密码技术中代价较高的运算置于服务器端,确保了标签端运算的轻量性,促进了公钥密码技术在RFID系统中的进一步实施。

关键词 RFID,轻量级,认证协议,数字签名
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.2.020

Lightweight RFID Authentication Protocol Based on Digital Signature

LIU Ya-li[1] QIN Xiao-lin[2] ZHAO Xiang-jun[1] HAO Guo-sheng[1] DONG Yong-quan[1]
(College of Computer Science & Technology, Jiangsu Normal University, Xuzhou 221116, China)[1]
(College of Computer Science & Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)[2]

Abstract The issues of security and privacy in RFID systems become the handicap to the development of RFID technology and the bottle neck of their further pervasive usage. A lightweight RFID authentication protocol based on digital signature was proposed, which combines digital signature technology and RFID authentication technology properly to implement the lightweight authentication mechanism of RFID systems successfully. Performance evaluation shows that this protocol not only has main security and privacy properties, but also can resist a variety of typical malicious attacks and threats. The security of this protocol is based on the assumption of difficulty in solving the discrete logarithm hard problem in the finite field and the security of pseudo random number generator. The protocol puts the higher cost operations of public key cryptography over the server end, which ensures the lightweight operation of the tag end and promotes the further application of public key cryptography in RFID systems.

Keywords RFID, Lightweight, Authentication protocol, Digital signature

1 引言

无线射频识别RFID(Radio Frequency Identification)技术是普适计算环境的主要推动者,鉴于非接触式自动识别的便捷性和低成本等优势,目前RFID技术已被广泛部署于各种实际应用领域,带来了巨大的生产力效益,如:交通运输[1,2]、供应链管理[3,4]、库存监控[2]、支付系统[2]、防盗系统[2]、医疗管理[5]、护照控制[4,6,7]及跟踪文件[1,2]等。然而,由于阅读器和标签间的信息交互以挑战-应答的方式在开放的无线通信环境中进行,RFID系统的安全和隐私问题[8]逐渐成为值得关注的焦点,因此设计抗各种恶意攻击和安全威胁的RFID认证协议是非常必要的。

针对RFID标签在存储、计算以及电源等方面受限的特点,传统的密码技术难以实现轻量级RFID系统安全认证机制。非对称加密技术比对称加密技术需要更多的计算代价,但具有不需要阅读器和标签共同维护密钥对的优势。在被动无源RFID标签上非对称加密技术的集成易于实现标签在无线开放系统中的成功认证。因此,在资源受限的RFID应用领域,利用公钥密码技术实现轻量级RFID认证机制是一个具有挑战性的课题。根据公钥密码体制中的数字签名技术能够提供强认证性的特点,RFID技术和数字签名技术的集成可以有效地阻止流通贸易中假冒商品以提供强抗伪造性,还

到稿日期:2014-08-13 返修日期:2014-09-07 本文受国家高技术研究发展计划("863"计划)基金资助项目(2007AA01Z404),国家自然科学基金资助项目(61272297,61373015),2010年度国家教育部高等学校博士学科点专项科研基金资助项目(20103218110017),江苏高校优势学科建设工程资助项目(PAPD),南京航空航天大学基本科研业务费(NP2013307),国家自然科学青年基金资助项目(61100167),江苏省自然科学基金资助项目(BK20131130,BK2011204),江苏省高校自然科学研究项目(14KJB520010),江苏师范大学校级科研重点项目(11XLA09,11XLA10)资助。

刘亚丽(1981—),女,博士,讲师,主要研究方向为物联网安全及隐私保护技术,E-mail:liuyali@jsnu.edu.cn;秦小麟(1953—),男,教授,博士生导师,主要研究方向为分布式环境的数据管理与安全、信息安全等;赵向军(1974—),男,博士,教授,主要研究方向为智能计算与计算机图形学;郝国生(1972—),男,博士,副教授,主要研究方向为智能计算;董永权(1979—),男,博士,副教授,主要研究方向为数据集成与信息检索。

可以通过部署签名的方式防止标签和阅读器间所传递的信息被修改。此外，签名技术可以有效进行存货控制，可以实现对所追踪实体的有效性验证等。

鉴于此，本文提出一种基于前向安全盲签名方案的轻量级 RFID 认证协议，其通过恰当转化运算代价较高的公钥密码技术，成功实现了 RFID 系统的轻量级认证机制。协议充分考虑 RFID 系统资源受限的特点，确保标签运算的轻量性，恰当控制了整个系统的计算开销，提高了认证效率，加强了鲁棒性、可靠性和数据完整性，为公钥密码技术在 RFID 系统中的进一步扩展提供了可行的安全保障。本文主要创新之处如下：

(1)公钥密码和 RFID 认证的结合性

将公钥密码技术和 RFID 认证技术进行了恰当结合，成功完成了 RFID 系统认证过程。将计算代价较高的签名生成运算置于服务器端，实现标签签名的置入操作，并通过对置入签名的验证来检验标签的合法性。

(2)认证周期的前向安全性

签名密钥和随机数在签名和验证阶段均进行动态更新，使得签名具有动态性，且标签和阅读器间随机化的挑战-应答在不同认证周期中具有不可链接性和不可追踪性。恶意攻击者即使窃取了当前签名密钥，也不可能获取密钥被盗之前的有效签名密钥，之前阅读器和标签间交互认证过程仍然有效，从而确保了协议具有前向安全性。

(3)认证过程的鲁棒性

攻破签名方案的困难性以及随机化的挑战-应答过程使得协议在保障基本安全和隐私属性的同时，有效地抵抗了多种主动攻击和被动攻击。

(4)标签运算的轻量性

将运算代价较高的签名算法置于签名发行端，阅读器为签名发行者执行签名过程提前做好盲化和脱盲操作等准备工作，通过验证签名的有效性来证实标签的合法性；标签端仅涉及两种简单比特位运算和伪随机数产生(PRNG)[9]操作，满足了低代价 RFID 标签的轻量级运算需求。

本文第 2 节对相关工作进行回顾；第 3 节简要介绍一种前向安全盲签名方案；第 4 节详细描述我们提出的基于数字签名的轻量级 RFID 认证协议(FSWBLAP)；第 5 节对新协议进行详细的安全性分析和性能分析；最后总结全文。

2 相关工作

数字签名技术和哈希函数在确保通信中的数据安全方面发挥了极其重要的作用，为无线领域和普适计算环境提供了安全保障。近年来，非对称加密技术在 RFID 标签上的实现取得了大量的研究成果，首次在低代价 RFID 标签上使用非对称加密技术已被证实[10,11]。2003 年，Hoffstein 等人设计了一个权衡效率和存储的方案[12]，提出了一个基于格的密码系统 NTRU，宣称该方案在签名和验证过程中比 ECC 方案更加快速。2010 年 Hutter 等人在文献[13]中首次提出了一种适用于 RFID 系统的 192 位椭圆曲线数字签名算法(ECDSA)处理器并提供了协议的可伸缩性和通用算法的重用性，通过阅读器签署数字签名挑战和实体身份认证的方式提供重要的密码服务。文献[14]设计了一个具有 3600 个等价逻辑门或不到 1000 个等价逻辑门的伪随机数生成器(PRNG)，它适用于 RFID 系统中标签和阅读器的随机数产生操作。2008 年 Liang 等人在文献[15]中利用基于身份的密码技术提出了一种适用于 RFID 系统的安全管理解决方案，其提供了较好的隐私保护且完成了标签和阅读器间的认证，同时降低了 RFID 系统的资源需求，更加方便了密钥管理。

现有基于签名的 RFID 认证技术存在的问题：利用高代价 RFID 标签的认证机制导致整个系统的计算开销较高，无法在基于数字签名的 RFID 认证协议中采用低代价轻量级 RFID 标签以保护系统的安全性和隐私性。

3 前向安全盲签名方案

前向安全盲签名方案(FSWBS)由 6 个阶段构成：密钥生成、密钥进化、盲化过程、签名过程、脱盲过程、验证过程。其中，密钥生成和密钥进化两个阶段参见文献[16]，在此不再赘述。为了突出 FSWBS 方案的签名和验证过程，后 4 个阶段的构建过程如表 1 所列。

表 1 FSWBS 签名方案

签名验证阶段	FSWBS
盲化过程	A 随机选取 $\beta\in Z_p$ 作为盲化因子，计算 $\xi(m)=(\beta+1)^{-1}r^{-\beta}m \bmod (p-1)$ 并将盲化后的消息 $\xi(m)$ 发送给 S
签名过程	S 得到签名 $\delta=(-2^{T-j}\ell)^{-1}(\xi(m)-kr) \bmod (p-1)$
脱盲过程	A 计算 $r'=r^{1+\beta} \bmod (p-1)$ 和 $\delta'=(1+\beta)r^{\beta}\delta \bmod (p-1)$，得到脱盲后的签名 $(j,\lambda_j,(r',\delta',m))$ 并发送给验证者
验证过程	签名验证方程 $(PK_{\lambda_j}^{-2^{T-j}})^{\delta'}r'^{r'} \bmod p=g^m \bmod p$

4 基于数字签名的轻量级 RFID 认证协议

本节在前向安全盲签名方案[16](FSWBS)的基础上，构建了一种基于数字签名的轻量级 RFID 认证协议(FSWBLAP)，其利用公钥密码技术成功实现了 RFID 系统认证机制。

4.1 协议基本思想及参数设置

(1)基本思想

FSWBLAP 协议由签名发行者(Issue)、阅读器(Reader)和标签(Tag)三者所组成，阅读器作为验证者(Verifier)，用于处理签名发行者和标签两者间的正常交互并执行签名验证过程。低代价轻量级 RFID 标签不支持基于公钥算法的签名生成和签名验证操作，仅支持简单比特位运算、随机数产生操作和简单函数[17]，因此将代价较高的签名产生过程置于签名发行端，签名验证过程置于阅读器端，而标签端仅涉及简单比特位运算和伪随机数产生(PRNG)操作以确保标签和阅读器间交互消息的保密性以及标签信息的匿名性和隐私保护性。FSWBLAP 协议采用两个阶段的随机化挑战-应答模式，通过签名置入过程成功地将签名发行者生成的签名置入标签，实现对合法标签的授权机制；阅读器利用签名验证过程以达到对标签的合法性认证。当标签或签名发行者被欺骗或者交互信息在无线信道中遭到恶意攻击时，验证者通过检验置入签名的有效性来认证标签的合法性。FSWBLAP 协议所基于的 FSWBS 方案可认为在盒内进行，由签名发行者负责完成签名过程并将签名通过阅读器置入待授权标签，签名操作作为挑战-应答认证协议的一部分，阅读器利用标签公钥通过验证签名的有效性以达到认证标签合法性的目的。

(2)参数设置

为简化描述，给出 FSWBLAP 协议中的相关符号和操作

说明，如表 2 所列。

表 2　FSWBLAP 协议符号说明表

R_1，R_2	阅读器	M	盲化前的消息，即原始消息
T	标签	ξ(M)	盲化后的消息
ISSUE	签名发行者	$Sign_{SK}(M)$	消息 M 的签名过程
PRNG	伪随机数生成器[9]	$Ver_{PK}(M)$	消息 M 的验证过程
SK_j^{issue}	签名发行者 j 认证周期的私钥	S′	在时段 j 关于盲化后消息 ξ(M)的签名
SK_{j+1}^{issue}	签名发行者 j+1 认证周期的私钥	S	逆盲变换后关于原始消息 M 在时段 j 的最终签名
PK_{issue}	签名发行者的公钥	+	模 2^q 加(mod 2^q(+)),q=96
ID	标签唯一的静态身份	⊕	比特位异或操作
K_{tag}	标签共享密钥	P	阅读器和标签间的一次单向认证

4.2　协议描述

4.2.1　认证过程

FSWBLAP 协议认证过程由 4 个阶段构成：初始化阶段、标签识别阶段、签名置入阶段、标签认证阶段。R_1 代表签名置入过程中参与签名生成的指定阅读器，R_2 代表签名认证过程中指定的签名验证阅读器；T 代表待授权和待认证标签。下面详细介绍 FSWBLAP 协议的认证过程。

4.2.1.1　初始化阶段

(1)ISSUE 选择一个伪随机数生成器[9] PRNG $g:\{0,1\}^k \to \{0,1\}^{2k}$ 产生伪随机数；

(2)ISSUE 利用 PRNG 产生 PK_{issue} 和 $SK_0^{issue} \in Z_p$ 作为初始密钥并保密，合法标签的密钥 K_{tag}；

(3)ISSUE 将公钥 PK_{issue} 置于合法 R_2，密钥 K_{tag} 置于合法 R_1 和 R_2 及合法 T 中；

(4)ISSUE 公开其公钥 PK_{issue}，合法 R_1 和 R_2 以及合法 T 存储并保密 T 对应的密钥 K_{tag}。

4.2.1.2　标签识别阶段

(1)$R_1 \to T$：R_1 利用伪随机数生成器[9] PRNG 生成一个随机数 n_1，并向 T 发送随机数 n_1 作为挑战，初始化一个新的签名预处理过程；

(2)$T \to R_1$：T 收到 R_1 挑战后，计算消息 $A=(ID \oplus n_1)+(K_{tag} \oplus n_1)$ 并作为应答返回 A 给 R_1；

(3)T 识别：R_1 收到应答后，利用 n_1 和 K_{tag} 从消息 A 抽取标签身份信息 ID，并查询后台数据库是否有匹配的 ID，只有被授权的 R_1 才能从后台数据库中获取合法 T 的密钥 K_{tag}。

若 R_1 查询到匹配的 ID，证明待认证 T 为系统中的合法标签，可以进行签名授权和认证，则将执行后续的签名置入阶段；否则由于此次 T 的应答无效或者 R_1 为未授权阅读器等因素，导致 R_1 无法从后台数据库中查询到匹配的 ID，此时 R 将终止当前操作，等待执行下一轮新的挑战。

4.2.1.3　签名置入阶段

(1)$R_1 \to$ ISSUE：R_1 获取匹配 ID 后，将 ID 作为签名消息 M，利用 FSWBS 中的盲化因子对消息 ID 执行盲化过程得到盲化后的消息 $\xi(ID)$，并将其发送给 ISSUE；

(2)ISSUE：ISSUE 收到 $\xi(ID)$ 后，利用 FSWBS 对其签名，得到盲化后的签名 $S'=SK_j^{issue}(\xi(ID))$；

(3)ISSUE$\to R_1$：ISSUE 将盲化后消息的签名 S' 发送给 R_1；

(4)R_1：R_1 收到签名 S' 后，利用 FSWBS 的脱盲过程进行逆盲变换，得到脱盲后消息的签名 S；

(5)$R_1 \to T$：R_1 计算消息 $B=S+n_1 \oplus K_{tag}$ 并发送给 T；

(6)T：T 收到消息 B 后，利用 n_1 和 K_{tag} 从 B 中抽取签名 S。

4.2.1.4　标签认证阶段

(1)$R_2 \to T$：R_2 向 T 发送“Hello”消息作为挑战，初始化一个新的认证过程；

(2)$T \to R_2$：T 收到 R_2 挑战后，利用伪随机数生成器[9] PRNG 生成一个随机数 n_2，计算消息 $C=n_2 \oplus K_{tag}$ 和消息 $D=(n_2 \oplus S)+K_{tag}$，并发送 $C \| D$ 返回给 R_2 作为应答；

(3)R_2：R_2 收到应答消息 $C \| D$ 后，先利用 K_{tag} 从 C 中抽取 n_2，再次从 D 中抽取授权标签的置入签名 S；根据 FSWBS 的实现过程，最终签名 S 为 $(j,\lambda_j,(r',\delta',m))$，其中 m 即为签名消息 ID，R_2 根据 FSWBS 的签名验证方程 $(PK\lambda_j^{-2^{T-j}})^{\delta'}r'^{r'} \bmod p=g^m \bmod p$ 判断 S 的有效性；若 $S=PK_{issue}(S)$，则授权标签的置入签名 S 有效，即 T 为合法标签，此次标签 T 的单向认证 P 有效；否则，签名 S 无效，即 T 为非法标签，此次标签 T 的单向认证 P 失败，R_2 将终止当前认证周期，等待执行下一轮新的签名置入过程。

至此，完成阅读器 R_2 对标签 Tag 的认证过程。

4.2.2　阅读器端算法

FSWBLAP 协议涉及两个不同的阅读器：参与签名预处理过程的 R_1 和参与验证过程的 R_2。

(1)阅读器 R_1 端算法

阅读器 R_1 端涉及 FSWBLAP 协议的标签识别阶段和签名置入阶段。

标签识别阶段：R_1 向 T 发送随机数 n_1 作为挑战以初始化新的签名预处理过程；R_1 接收 T 的应答 A 并抽取 T 的 ID 信息，查询后台数据库并判断是否存在匹配的 ID；若存在则 R_1 将终止当前操作，等待执行下一轮新挑战。

签名置入阶段：R_1 根据匹配的 ID 信息，执行 FSWBS 方案中的盲化过程产生盲化后消息 $\xi(ID)$，并将其发送给 ISSUE；R_1 接收 ISSUE 执行 FSWBS 方案后得到盲化后消息的签名 S'；R_1 执行 FSWBS 方案中的脱盲过程，得到脱盲后消息的签名 S；R_1 计算消息 B 并发送给 T。

阅读器 R_1 端的具体执行过程如算法 1 所示。

算法 1　FSWBLAP 阅读器 R_1 端算法

输入：盲化后消息的签名 S′，T 应答消息 A

输出：R_1 挑战 n_1，盲化后消息 ξ(ID)，消息 B

1. R_1 向 T 发送随机数 n_1 作为挑战；
2. R_1 接收 T 的应答 A；
3. R_1 从消息 A 中抽取 T 的 ID 信息；
4. IF ID 在后台数据库中匹配不到记录 THEN
5. 　　R_1 将终止当前操作，标签识别过程失败退出；
6. END IF
7. R_1 执行 FSWBS 方案中的盲化过程产生 ξ(ID)并发送给 ISSUE；
　　/ * ξ(ID)为盲化后消息 * /
8. R_1 接收 ISSUE 发送的签名 S′；
　　/ * S′为盲化后消息的签名 * /
9. R_1 执行 FSWBS 方案中的脱盲过程产生签名 S；
　　/ * S 为脱盲后消息的签名 * /
10. R_1 计算消息 B 并发送给 T。

(2)阅读器 R_2 端算法

阅读器 R_2 端仅涉及标签认证阶段。

标签认证阶段：R_2 向 T 发送“Hello”消息作为挑战以初始化新的认证过程；R_2 接收 T 的应答消息 $C \| D$；R_2 从消息 $C \| D$ 中抽取随机数 n_2 和标签置入签名 S；R_2 根据 FSWBS 的签名验证方程判断 S 的有效性；若验证方程成立，则 T 为合法标签，此次认证 P 有效；否则，签名 S 无效，即 T 为非法标签，此次认证 P 失败，R_2 将终止当前认证周期，等待执行下一轮签名置入过程。

阅读器 R_2 端的具体执行过程如算法 2 所示。

算法 2 FSWBLAP 阅读器 R_2 端算法

输入：T 应答消息 C ‖ D

输出：R_2 挑战“Hello”，P 是否为有效认证

1. R_2 向 T 发送“Hello”请求；
2. R_2 接收 T 的应答消息 C ‖ D；
3. R_2 从消息 C 中抽取随机数 n_2 并从消息 D 中抽取标签置入签名 S；
4. R_2 根据 FSWBS 的签名验证方程判断 S 的有效性；
5. IF 验证方程成立 THEN
6. T 被成功认证，P 为有效认证，输出“P 有效”；
7. ELSE
8. T 未被成功认证，R_2 将终止当前认证周期，
   输出“P 无效”，认证过程失败退出；
9. END IF

4.2.3 FSWBLAP 协议实现过程图

FSWBLAP 协议的具体步骤如图 1 所示。

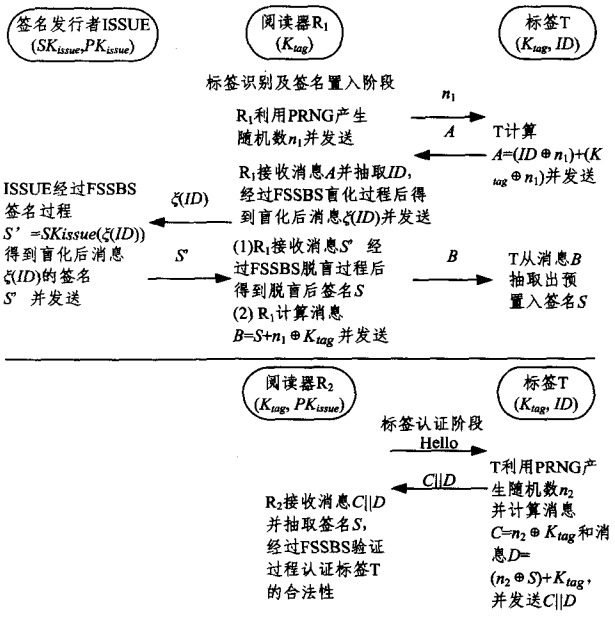

图 1 FSWBLAP 实现过程

5 协议性能评估

本节从 RFID 认证协议的主要安全隐私性能属性和对典型恶意攻击的抵抗能力等两个方面对 FSWBLAP 协议进行详细的安全性分析，并从资源消耗方面对其进行性能分析。

5.1 安全性分析

5.1.1 安全性与隐私性分析

(1)数据机密性

FSWBLAP 协议在阅读器和标签间无线信道上传输的交互消息均被秘密值或者随机数所保护，包括标签密钥 K_{tag}、标签身份 ID、每个周期动态产生的随机数 n_1 和 n_2 以及签名发行者在每个签名置入阶段生成的签名 S。n_1，n_2 和 S 随不同周期动态变化以随机化阅读器和标签间的挑战-应答过程，在未知标签密钥 K_{tag} 的情况下，不可能得到 n_2 和 ID 以及 S。因此，攻击者不可能通过截获的交互消息获取合法标签的 K_{tag} 和 ID 等秘密信息，从而确保了数据机密性。

(2)数据完整性

FSWBLAP 协议的数据完整性通过验证从交互信息中所抽取的秘密信息和签名的有效性进行保障。在签名置入阶段，标签密钥 K_{tag} 和标签身份 ID 参与标签应答信息 A 的构建，且根据阅读器产生的随机数 n_1 进行周期性的动态更新，仅有合法阅读器才能从消息 A 中抽取合法标签的 ID 信息。若攻击者试图通过修改消息 A 的方式进行恶意攻击，则阅读器抽取的 ID 信息与后台数据库匹配失败，进而识别攻击者并终止协议执行。类似地，消息 B 和消息 $C \| D$ 由秘密信息 K_{tag} 和签名 S 构成，在签名验证阶段通过验证抽取签名 S 的有效性同样保证了消息 B 和 $C \| D$ 的完整性。因此，FSWBLAP 协议确保了秘密信息和交互消息的数据完整性。

(3)前向安全性

FSWBLAP 协议的前向安全性通过签名发行者所执行的签名方案和动态产生的随机数 n_1，n_2 保证。在 FSWBS 中，每个签名周期结束后，签名发行者根据密钥进化算法 $SK_j = SK_{j-1}^2 \bmod (p-1)$ 进行更新，确保签名置入阶段所产生签名 S 的动态性；此外，在签名置入阶段和签名验证阶段，n_1 和 n_2 分别由阅读器和标签随机生成，确保了阅读器和标签间随机化的挑战-应答过程。由于所有的交互信息均涉及随不同周期动态更新的秘密信息（SK_j，n_1，n_2），SK_j 具有周期性，n_1，n_2 具有随机性等特点，即使 SK_j 在当前签名周期被泄露，攻击者也不可能根据当前签名置入阶段的签名记录推导出前一轮签名周期中的有效密钥 SK_{j-1}。详细分析过程与 FSWBS 方案[16]中的前向安全性分析类似，在此不再赘述。因此，即使标签在当前周期被捕获，之前认证周期的签名认证仍然有效，FSWBLAP 协议的密钥进化和签名认证过程均具有前向安全性。

(4)标签匿名性

FSWBLAP 协议利用对标签 ID 的匿名化处理方法来确保标签匿名性。阅读器和标签间的挑战-应答过程并不是以明文方式传送标签身份 ID，无线信道上传送的交互消息 A，B 和 $C \| D$ 根据标签置入的签名 S 以及随机数 n_1 和 n_2 的动态变化进行更新。在未知 S，K_{tag} 以及 n_1，n_2 的情况下，攻击者试图通过截获交互信息达到获取合法标签 ID 的攻击目的是根本不可行的。因此，对非法实体来说标签是匿名的。

5.1.2 抗恶意攻击分析

(1)抗重放攻击

FSWBLAP 协议通过动态随机化的挑战-应答抵抗重放攻击。为了达到重放攻击的目的，攻击者存储第 $j-1$ 个成功认证周期中的交互消息，通过伪装标签或者阅读器在无线信道上重放消息，主要有以下 3 种情况。

情况 1：攻击者重放应答消息 A

假设攻击者在第 j 个周期的签名置入阶段，伪装标签重

放第 $j-1$ 个周期的应答消息 A，由于随机数 $(n_1)_j \neq (n_1)_{j-1}$，阅读器从消息 A 中抽取的 $(ID)_j \neq (ID)_{j-1}$，因此 $(ID)_j$ 不能在后台数据库中查询到匹配记录，从而发现攻击者对消息 A 的重放性，签名置入阶段终止退出。

情况 2：攻击者重放签名置入消息 B

假设攻击者在第 j 个周期的签名置入阶段，伪装阅读器重放第 $j-1$ 个周期的签名置入消息 B，由于随机数 $(n_1)_j \neq (n_1)_{j-1}$，标签从消息 B 中抽取的 $(S)_j \neq (S)_{j-1}$；当标签在签名认证阶段发送由签名消息 $(S)_j$ 所构成的应答消息 $C \parallel D$ 后，阅读器抽取 $(S)_j$，同时利用第 j 个周期的验证参数 $(j,\lambda_j,(r',\delta',m))$ 和 FSWBS 签名方案验证 $(S)_j$ 为第 j 个周期的无效签名，签名验证阶段终止退出。

情况 3：攻击者重放签名认证消息 $C \parallel D$

假设攻击者在第 j 个周期的签名认证阶段，伪装标签重放第 $j-1$ 个周期的签名认证消息 $C \parallel D$，由于消息 $C \parallel D$ 是由签名消息 $(S)_{j-1}$ 所构成，阅读器从中抽取 $(S)_{j-1}$，但利用第 j 个周期的验证参数 $(j,\lambda_j,(r',\delta',m))$ 和 FSWBS 签名方案验证 $(S)_{j-1}$ 为第 j 个周期的无效签名，签名验证阶段终止退出。

根据以上 3 种情况的分析可以得出，重放交互消息 A，B 和 $C \parallel D$ 均不能成功认证，从而确保了 FSWBLAP 协议能够抵抗重放攻击。

(2)抗追踪攻击

由于动态随机数 n_1 和 n_2 及签名 S 在每个签名置入阶段和签名认证阶段均进行更新，因此确保了不同认证周期中阅读器和同一标签间的交互消息 $(A,B,C \parallel D)$ 均为随机化，攻击者试图截获同一标签和阅读器间相同交互消息并发起对同一标签的追踪攻击是不可行的。因此，FSWBLAP 协议能够抵抗恶意追踪攻击，保护了合法标签的位置隐私。

(3)抗伪造攻击

伪造攻击主要分为标签伪造和阅读器伪造两种攻击形式。

①标签伪造

情况 1：攻击者伪造标签密钥 K'_{tag} 发送应答消息 A'

攻击者试图通过伪造标签密钥 K'_{tag} 假冒一个合法标签以接收置入的签名。在签名置入阶段，当伪造标签收到合法阅读器发送的挑战 n_1 后，计算应答消息 $A'=(ID \oplus n_1)+(K'_{tag} \oplus n_1)$ 并发送给阅读器。由于伪造密钥 $K'_{tag} \neq K_{tag}$，因此阅读器从消息 A' 中抽取的 $ID' \neq ID$，在后台数据库中不能查询到匹配的 ID' 记录。因此，在未知合法标签密钥 K_{tag} 的情况下，伪造标签不可能产生有效的应答消息 A，标签伪造攻击失败，签名置入阶段终止退出。

情况 2：攻击者伪造标签密钥 K'_{tag} 和签名 S'' 发送应答消息 $C' \parallel D'$

攻击者试图通过伪造标签密钥 K'_{tag} 和签名 S'' 假冒一个合法标签以发送待验证的签名。在签名验证阶段，当伪造标签收到合法阅读器发送的挑战“Hello”后，计算消息 $C'=n_2 \oplus K'_{tag}$ 和 $D'=(n_2 \oplus S'')+K'_{tag}$ 并发送应答消息 $C' \parallel D'$ 给阅读器。由于伪造密钥 $K'_{tag} \neq K_{tag}$，因此阅读器从消息 D' 中抽取的 $S'' \neq S$，利用第 j 个周期的验证参数 $(j,\lambda_j,(r',\delta',m))$ 和 FSWBS 签名方案验证 S'' 为无效签名。因此，在未知合法标签密钥 K_{tag} 的情况下，伪造标签也不可能产生有效的应答消息 $C \parallel D$，标签伪造攻击失败，签名验证阶段终止退出。

②阅读器伪造

攻击者试图通过伪造签名置入消息 B' 假冒一个合法阅读器 R_1 达到标签签名置入的目的。在签名置入阶段，伪造阅读器 R_1' 收到合法标签发送的应答消息 A 后，通过伪造签名 S'' 和标签密钥 K'_{tag} 计算消息 $B'=S''+n_1 \oplus K'_{tag}$ 并发送给合法标签。由于伪造密钥 $K'_{tag} \neq K_{tag}$，因此标签从消息 B' 中抽取的 $S'' \neq S$；在签名验证阶段，当标签发送由签名 S'' 所构建的应答消息 $C' \parallel D'$ 给合法阅读器 R_2 后，阅读器 R_2 利用第 j 个周期的验证参数 $(j,\lambda_j,(r',\delta',m))$ 和 FSWBS 签名方案验证 S'' 为无效签名。因此，在未知合法标签密钥 K_{tag} 的情况下，伪造阅读器 R_1' 也不可能产生有效的签名置入消息 B，阅读器 R_1 伪造攻击失败，签名置入阶段终止退出。

根据以上两种伪造攻击分析可以得出，FSWBLAP 协议不仅可以抵抗标签伪造攻击，而且可以抵抗阅读器伪造攻击，具有较强的抗伪造性。

(4)抗中间人攻击

中间人攻击主要有以下 3 种情况。

情况 1：篡改应答消息 A

在签名置入阶段，若攻击者通过无线信道窃听合法标签应答消息 A 并篡改为 A'' 后发送给合法阅读器，阅读器从 A'' 中利用标签密钥 K_{tag} 和随机数 n_1 抽取标签身份信息 ID。由于篡改消息 A'' 和原始标签应答消息 A 不一致，导致阅读器从 A'' 中抽取的 $ID' \neq ID$，不能查询到匹配的 ID' 记录。因此，攻击者篡改应答消息 A 无效，不能被合法阅读器授权置入签名，中间人攻击失败，签名置入阶段终止退出。

情况 2：篡改签名置入消息 B

在签名置入阶段，若攻击者通过无线信道窃听签名置入消息 B 并篡改为 B'' 后发送给标签，标签从 B'' 中利用标签密钥 K_{tag} 和随机数 n_1 抽取置入签名 S。由于篡改消息 B'' 和原始签名置入消息 B 不一致，导致标签从 B'' 中抽取的 $S'' \neq S$；在签名验证阶段，当标签发送由 S'' 计算的应答消息 $C'' \parallel D''$ 给阅读器后，阅读器利用第 j 周期的验证参数 $(j,\lambda_j,(r',\delta',m))$ 和 FSWBS 方案[16]验证 S'' 为无效签名。因此，攻击者篡改签名置入消息 B 无效，合法标签不能成功验证置入签名，中间人攻击失败，签名置入阶段终止退出。

情况 3：篡改签名待验证消息 $C \parallel D$

在签名验证阶段，若攻击者通过无线信道窃听签名待验证消息 $C \parallel D$ 并篡改为 $C'' \parallel D''$ 后发送给阅读器，阅读器从 $C'' \parallel D''$ 中利用标签密钥 K_{tag} 抽取待验证签名 S''。由于篡改消息 $C'' \parallel D''$ 和原始签名待验证消息 $C \parallel D$ 不一致，导致阅读器从 $C'' \parallel D''$ 中抽取的 $S'' \neq S$，阅读器利用第 j 个周期的验证参数 $(j,\lambda_j,(r',\delta',m))$ 和 FSWBS 方案[16]验证 S'' 为无效签名。因此，攻击者篡改签名待验证消息 $C \parallel D$ 无效，不能被合法阅读器验证置入签名，中间人攻击失败，签名验证阶段终止退出。

根据以上 3 种情况的分析可以得出，中间人篡改交互消息 A，B 和 $C \parallel D$ 均不能成功实现签名置入和签名验证，因此，FSWBLAP 协议能够有效抵抗中间人攻击。

5.2 性能分析

FSWBLAP 协议充分考虑了 RFID 系统资源受限的特

(下转第 107 页)

[13] Shyu S J. Visual Cryptograms of Random Grids for General Access Structures[J]. Circuits and Systems for Video Technology, 2013,23(3):414-424

[14] Fu Z X, Yu B. Visual Cryptography and Random Grids Schemes [C]// Poceedings of 12th International Workshop on Digital-Forensics and Watermarking. CBD Auckland, New Zealand, Oct 2013:109-122

[15] Wu X T, Sun W. Improving the visual quality of random grid-based visual secret sharing[J]. Signal Processing, 2013, 93(5): 977-995

[16] Chen T H, Lee Y S. A New Random-grid-based Visual Secret Sharing by Edge Enhancement[J]. Journal of Computational Information Systems, 2012, 8(4): 1507-1513

[17] Tuyls P, Hollmann H D L, Lint J H V, et al. XOR-based visual cryptography schemes[J]. Designs, Codes and Cryptography, 2005, 37(1): 169-186

[18] Chao K Y, Lin J C. Secret image sharing: A Boolean operations based approach combining benefits of polynomial-based and fast approaches[J]. International Journal of Pattern Recognition and Artificial Intelligence, 2009, 23(2): 263-285

[19] [美]冈萨雷斯, 等. 数字图像边缘检测(第二版)[M]. 阮秋琦等译. 北京: 电子工业出版社, 2007: 460-479

(上接第 99 页)

点,在签名置入过程和签名验证过程中,标签端仅需两种简单的比特位运算(模 2^m 加(mod 2^m(+))和比特位异或(XOR))以及伪随机数产生(PRNG)[9]操作,这 3 种操作均符合低代价被动 RFID 标签的轻量级运算能力[17]。此外,将计算代价相对较高的盲化操作、脱盲操作以及签名验证操作置于阅读器端进行,由签名发行端执行前向安全盲签名算法[16](FSWBS),在实现轻量级标签运算的同时恰当地控制了整个 RFID 系统的开销。因此,FSWBLAP 协议是利用公钥密码技术实现低代价 RFID 标签轻量级认证的有效方案,适合应用于供应链管理、无线信用卡、电子护照(E-passport)、电子不停车收费系统(ETC)以及电子票(E-ticket)等商业、工业和民用等应用领域的轻量级 RFID 安全访问控制系统以及轻量级 RFID 认证系统,在此应用领域中被动低代价轻量级 RFID 标签需符合 EPC Class-1 Gen-2 标准,能够执行少量等价逻辑门运算和伪随机数产生操作(PRNG)[9]。

结束语 为了解决公钥密码技术大量的计算开销难以实现低代价 RFID 标签的轻量级认证问题,本文提出了一种基于数字签名方案的轻量级 RFID 认证协议(FSWBLAP),其利用数字签名技术成功实现了 RFID 系统的轻量级认证机制。FSWBLAP 协议的突出优势是恰当转化公钥密码技术中代价较高运算的执行位置,在加强 RFID 系统安全性和鲁棒性的同时,成功降低了标签端的计算开销,满足了资源受限设备的轻量级运算需求,其安全性建立在有限域上的离散对数困难问题和伪随机生成器的基础之上。

参 考 文 献

[1] Schneider M. Radio frequency identification (RFID) technology and its applications in the commercial construction industry[D]. University of Kentucky, 2003

[2] Chawla V, Dong-Sam H. An overview of passive RFID[J]. Communications Magazine, IEEE, 2007, 45(9): 11-17

[3] Roussos G, Kostakos V. rfid in pervasive computing: State-of-the-art and outlook[J]. Pervasive and Mobile Computing, 2009, 5(1): 110-131

[4] Want R. The Magic of RFID[J]. Queue, 2004, 2(7): 40-48

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

[6] Hlavá č. Known-Plaintext-Only Attack on RSA-CRT with Montgomery Multiplication[C]// Cryptographic Hardware and Embedded Systems(CHES 2009). Springer, 2009: 128-140

[7] Nithyanand R. The evolution of cryptographic protocols in electronic passports: Cryptology ePrint archive[R]. Report 2009/200

[8] Yanjun Z. Survivable RFID Systems: Issues, Challenges, and Techniques[J]. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 2010, 40(4): 406-418

[9] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. LAMED-A PRNG for EPC Class-1 Generation-2 RFID specification[J]. Comput. Stand. Interfaces. , 2009, 31(1): 88-97

[10] Batina L, Guajardo J, Kerins T, et al. Public-Key Cryptography for RFID-Tags[C]// Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2007(PerCom Workshops'07). 2007: 217-222

[11] McLoone M, Robshaw M J B. New Architectures for Low-Cost Public Key Cryptography on RFID Tags[C]// IEEE International Symposium on Circuits and Systems, 2007(ISCAS 2007). 2007: 1827-1830

[12] Hoffstein J, Howgrave-Graham N, Pipher J, et al. NTRUSign: Digital Signatures Using the NTRU Lattice[C]// Joye M, ed. Topics in Cryptology(CT-RSA 2003). Springer Berlin Heidelberg, 2003: 122-140

[13] Hutter M, Feldhofer M, Plos T. An ECDSA Processor for RFID Authentication[C]// Yalcin S O, ed. Radio Frequency Identification: Security and Privacy Issues. Springer Berlin Heidelberg, 2010: 189-202

[14] Calmels B, Canard S, Girault M, et al. Low-Cost Cryptography for Privacy in RFID Systems[C]// Domingo-Ferrer J, Posegga J, Schreckling D, eds. Smart Card Research and Advanced Applications. Springer Berlin Heidelberg, 2006: 237-251

[15] Liang Y, Rong C. RFID System Security Using Identity-Based Cryptography[C]// Presented at the Proceedings of the 5th international conference on Ubiquitous Intelligence and Computing. Oslo, Norway, 2008: 482-489

[16] Liu Ya-li, Qin Xiao-lin, Li Bo-han. Forward-Secure Blind Signature Schemes Based on the Variants of ElGamal[J]. China Communications, 2010, 7(4): 58-64

[17] C Hung-yu. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4 (4): 337-340