·安全技术· 文章编号:1000-3428(2017)06-0097-04 文献标志码:A 中图分类号:TP309.7

基于 SM2 与零知识的射频识别双向认证协议

李子臣[1,2,3],刘博雅[2],王培东[2],杨亚涛[2]

(1.北京印刷学院 教务处,北京 102600;2.北京电子科技学院,北京 100070;
3.西安电子科技大学 通信工程学院,西安 710071)

摘 要: 为保证射频识别系统中阅读器与标签的无线通信安全,以国产公钥密码算法 SM2 为基础,引入零知识证明思想,提出一种双向认证协议。给出安全性分析和效率分析,并利用 BAN 逻辑进行形式化分析。结果表明,该协议在阅读器和标签只需交互 2 次的情况下即可完成双向认证,具有较高的安全性和通信效率。

关键词: SM2 算法;射频识别技术;零知识;双向认证协议;BAN 逻辑

中文引用格式: 李子臣,刘博雅,王培东,等. 基于 SM2 与零知识的射频识别双向认证协议[J]. 计算机工程,2017,43(6):97-100,104.

英文引用格式: Li Zichen, Liu Boya, Wang Peidong, et al. Two-way Authentication Protocol Based on SM2 and Zero Knowledge for Radio Frequency Identification[J]. Computer Engineering, 2017, 43(6): 97-100, 104.

Two-way Authentication Protocol Based on SM2 and Zero Knowledge for Radio Frequency Identification

LI Zichen[1,2,3], LIU Boya[2], WANG Peidong[2], YANG Yatao[2]

(1. Dean's Office, Beijing Institute of Graphic Communication, Beijing 102600, China;
2. Beijing Electronic Science and Technology Institute, Beijing 100070, China;
3. Communication Engineering Institute, Xidian University, Xi'an 710071, China)

【Abstract】 To ensure the wireless communication security of the reader and tag in the Radio Frequency Identification (RFID) system, based on domestic public key cryptography algorithm SM2 and introducing zero knowledge proof idea, this paper proposes a two-way authentication protocol. Then security and efficiency analysis are given. The formal analysis is made by using BAN logic. Results show that the two-way authentication of the proposed protocol is completed in the case that reader and tag just interact twice, and has high safety and communication efficiency.

【Key words】 SM2 algorithm; Radio Frequency Identification (RFID) technology; zero knowledge; two-way authentication protocol; BAN logic

DOI: 10.3969/j.issn.1000-3428.2017.06.016

0 概述

射频识别(Radio Frequency Identification,RFID)是一种非接触式的自动识别技术,典型的 RFID 系统由后台数据库、阅读器、标签三大部分组成。由于 RFID 技术的诸多优点,物流业、零售业、制造业、金融等领域中越来越多地引入 RFID 系统。在享受 RFID 技术便利的同时,RFID 系统暴露出的安全性问题也日益突出,成为制约其快速发展的重要问题。保障 RFID 系统安全方式主要有物理安全机制和基于密码技术的安全协议两大类。物理安全机制主要方式有:Kill 命令,Sleep 命令,静电屏蔽等,这类安全机制在实际应用中不尽如人意,基于密码算法的安全认证协议进入了人们的视野,到目前为止已经有多种 RFID 协议被提出,但这些协议都在不同程度上存在一些安全漏洞和效率问题[1]。

在文献[2]提出的 Hash-Lock 协议中,标签每次传输的响应消息 metaID 相同会引起跟踪攻击;文献[3]引入随机数解决了该问题,但明文传输的 ID 会引起冒充攻击;在基于杂凑的 ID 变化协议[4]中,标识信息的引入防范了中间人攻击,但容易引起去同步攻击;文献[5]提出的分布式 RFID 询问-应答认

基金项目: 国家自然科学基金(61370188)。

作者简介: 李子臣(1965—),男,博士,主研方向为密码学;刘博雅、王培东(通信作者),硕士研究生;杨亚涛,博士。

收稿日期: 2016-04-07 **修回日期:** 2016-05-20 **E-mail:** hellowpd@163.com

证协议[5],为 RFID 系统中认证双方分配随机数,但如果攻击者得到标签 ID 后会有前向安全问题。文献[6]设计出基于二维区间的 Hash-Chain 协议,为标签增加索引标识(A_i,B_i),提高了认证效率,但当标签 Hash 链长度有限时会引起冒充攻击和重放攻击的威胁。

近年来,随着 RFID 技术的发展,RFID 的运算能力越来越强,公钥加密算法在 RFID 中的应用已经进入研究者的视野,与众多公钥密码算法相比,ECC 在相同密钥强度下加解密速度和存储空间上都有明显的优势。SM2 算法是 2010 年 12 月我国在 ECC 基础上提出的公钥密码算法,在解密正确性判断、待加密数据编码、对待加密数据长度的限制及加密计算效率上都要优于国际标准 ECC 算法。文献[7]提出了一个基于 ECC 的 RFID 认证协议,但其不可抵抗跟踪攻击,前向安全也不能得到保证;为改变标签 ID 泄露问题,文献[8]提出了一个新方案,但该方案存在扩展性问题。文献[9]提出了一个基于 ECC 的 RFID 单向认证协议。文献[10]提出一个基于椭圆曲线零知识的 RFID 双向认证协议,完成双向认证需要阅读器与标签交互 5 次。

目前,国内外针对 RFID 系统提出了较多安全认证协议,但大部分协议都存在一定的安全隐患,协议安全性分析[11-16]表明某些协议易受到冒充、重放、去同步等攻击。本文通过分析现有协议,提出一种基于 SM2 的 RFID 双向认证协议,引入零知识证明思想对协议过程进行描述,分析其安全性,并采用 BAN 逻辑进行形式化分析,最后给出效率分析结果。

1 基础知识

1.1 SM2 算法

SM2 是国家密码管理局在 2010 年 12 月 17 发布的公钥密码算法,是基于椭圆曲线上点群离散对数难问题,在 ECC 算法的基础上进行改进的算法。对于椭圆曲线的选择,推荐使用素数域 256 位的椭圆曲线。本文使用 SM2 算法进行数字签名,其中需要 SM3 杂凑算法,SM3 也是由国家密码管理局发布。

1.2 零知识证明基本原理

零知识证明思想于上世纪八十年代提出,假设我们知道某些秘密信息,如果想让别人相信我们知道这些秘密信息,同时还不想让别人知道这些秘密信息,则可以利用零知识证明来向别人证明我们知道这些秘密信息这是零知识证明的核心。假设 P 是某些秘密信息拥有者,想向 V 证明其拥有某种秘密 S,V 是验证者,向 P 发送若干只与 S 相关的问题,问题只能由 P 回答,且在证明过程中并不泄露任何有关 S 的信息,过程重复 n 次,全部成功即可证明 P 拥有 S。

2 协议设计

在 RFID 系统中,设计安全的 RFID 双向认证协议需要对阅读器和标签合法性进行有效认证,保障阅读器与标签无线通信过程的安全。本文将 SM2 密码算法与零知识证明有效结合,设计一种基于 SM2 的 RFID 零知识双向认证协议,协议仅需两步即可完成认证,在保障安全性的同时,适合目前 RFID 系统低成本、高效率的要求。

协议过程为 3 个阶段:初始化阶段,标签认证阶段和阅读器认证阶段。协议过程中涉及 2 个主体:阅读器和标签。

2.1 初始化阶段

在素数域 F_p 上选择一个椭圆曲线 $E(F_p)$,选择 $E(F_p)$上一个基点 P,P 的阶为 n。H 代表的安全杂凑函数为 SM3 算法,s 代表的签名值由 SM2 算法实现。

2.2 标签认证阶段

标签认证阶段步骤如下:

1)标签私钥 d_t,计算 $R_t = d_tP$ 作为公钥,公开公钥,标签标识 ID_t,选取随机数 $r_t \in [1, n-1]$,新鲜值 t。

2)标签计算 $h_1 = H(R_t + ID_t + t) \bmod n$;$s_t = ((1 + d_t)^{-1}(r_t - rd_t)) \bmod n$,并将计算所得的 h_1,签名值 s_t,自己的 ID_t 以及新鲜值 t 发送给阅读器。

3)阅读器收到标签发送的 h_1,s_t,ID_t,t 后,首先判断 t 是否新鲜,若新鲜则继续执行协议,否则认证失败,协议终止。

4)阅读器计算 $T_t' = s_tR_t((1 + d_t)(r_t - rd_t)^{-1}) \bmod n$。

5)判断 $H(T_t' + ID_t + t) \bmod n$ 是否等于 h_1,若相等,则认定标签合法,标签认证完成。

2.3 阅读器认证

阅读器认证步骤如下:

1)阅读器私钥 d_R,计算 $R_R = d_RP$ 作为公钥,公开公钥,阅读器标识 ID_R,选取随机数 $r_R \in [1, n-1]$。

2)阅读器计算 $h_2 = H(R_R + ID_R + t) \bmod n$,$s_R = ((1 + d_R)^{-1}(r_R - rd_R)) \bmod n$,并将计算所得的 h_2,签名值 s_R,自己的 ID_R 以及新鲜值 t 发送给标签。

3)标签收到阅读器发送的 h_2,s_R,ID_R,t 后,首先判断 t 是否为发送者所发,若是,则继续执行协议,否则认证失败,协议终止。

4)标签计算 $T_R' = s_RR_R((1 + d_R)(r_R - rd_R)^{-1}) \bmod n$。

5)判断 $H(T_R'+ID_R+t) \bmod n$ 是否等于 h_2,若相等,则认定阅读器合法,阅读器认证完成。

阅读器和标签认证过程如图 1 所示。

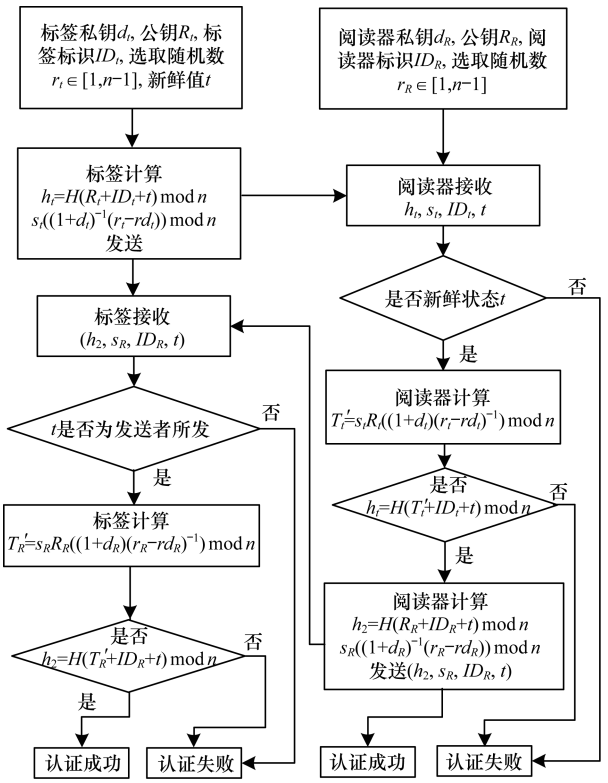

图 1　协议双向认证过程

3　协议正确性证明

在标签认证阶段,需要验证 $h_1=H(T_R'+ID_R+t) \bmod n$ 等式成立,才能认定标签合法,假设之前步骤完全按照协议执行,等式左端 $h_1=H(R_t+ID_t+t) \bmod n$,等式右端为:

$$\begin{aligned}&H(T_t'+ID_t+t) \bmod n\\&=H(s_tR_t(1+d_t)(r_t-rd_t)^{-1}+ID_t+t) \bmod n\\&=H((1+d_t)^{-1}(r_t-rd_t)R_t(1+d_t)(r_t-rd_t)^{-1}\\&+ID_t+t) \bmod n\\&=H(R_t+ID_t+t) \bmod n\end{aligned}$$

等式左端等于右端,标签合法。

在阅读器认证阶段,需要验证 $h_2=H(T_R'+ID_R+t) \bmod n$ 等式成立,才能认定阅读器合法,假设之前步骤完全按照协议执行,等式左端 $h_2=H(R_R+ID_t+t) \bmod n$,等式右端为:

$$\begin{aligned}&H(T_R'+ID_R+t) \bmod n\\&=H(s_RR_R(1+d_R)(r_R-rd_R)^{-1}+ID_R+t) \bmod n\\&=H((1+d_R)^{-1}(r_R-rd_R)R_R(1+d_R)(r_R-rd_R)^{-1}\\&+ID_R+t) \bmod n\\&=H(R_R+ID_R+t) \bmod n\end{aligned}$$

等式左端等于右端,阅读器合法。

4　BAN 逻辑证明

4.1　BAN 逻辑语法

BAN 逻辑语法具体说明如下:

1)$P \mid \equiv X$:P 相信 X,主体 P 相信 X 是真的。

2)$P \mid \sim X$:P 曾说过 X,主体 P 在某一个时刻曾传送过 X。

3)$P \lhd X$:P 曾看到过 X,有主体曾发送过来包含 X 的信息,主体 P 可以读出 X。

4)$\#(X)$:X 是新鲜的。

5)$\{X\}_K$:用密钥 K 加密 X 得到的密文。

6)$P \overset{K}{\longleftrightarrow} Q$:$P$ 和 Q 共享密钥 K,且若 K 是好的密钥,则除了 P,Q 以及 P 和 Q 共同信任的主体外,任何人都不知道 K。

7)$\overset{K}{\longrightarrow} P$ 或 $\mid \overset{K}{\longrightarrow} P$:$K$ 是 P 的公钥,且除 P 和他信任的主体外,任何人都不知道其相应的私密密钥 K^{-1}。

4.2　BAN 逻辑主要推理规则

BAN 逻辑主要推理规则有:

1)消息含义规则:

$$\frac{P \mid \equiv P \overset{K}{\longleftrightarrow} Q \wedge P \lhd \{X\}_K}{P \mid \equiv Q \mid \sim X}$$

$$\frac{P \mid \equiv \mid \overset{K}{\longrightarrow} Q \wedge P \lhd \{X\}_{K^{-1}}}{P \mid \equiv Q \mid \sim X}$$

2)临时值验证规则:

$$\frac{P \mid \equiv \#(X) \wedge Q \mid \sim X}{P \mid \equiv Q \mid \equiv X}$$

3)新鲜性规则:

$$\frac{P \mid \equiv \#(X)}{P \mid \equiv \#(X,Y)}$$

4)信任规则:

$$\frac{P \mid \equiv \#(X,Y)}{P \mid \equiv \#(X)}, \frac{P \mid \equiv X \wedge P \mid \equiv Y}{P \mid \equiv (X,Y)}$$

4.3　协议证明过程

使用 BAN 逻辑证明本文设计协议的安全性,形式化说明协议能够达到预期安全目标。先根据 BAN 逻辑需求对协议步骤进行表示,结果如表 1 所示。

表 1　协议过程与 BAN 逻辑表示的对应关系

协议过程	BAN 逻辑表示
$T \xrightarrow{h_1,s_t,ID_t,t} R$	$R<h_1,s_t,ID_t,t$
$R \xrightarrow{h_2,s_R,ID_R,t} T$	$T<h_2,s_R,ID_R,t$

假设 $R \mid \equiv \#(s_t)$,$R \mid \equiv \#(ID_t)$,$T \mid \equiv \#(s_R)$,$T \mid \equiv \#(t_2)$,$\#(t)$;需证明:1)$R \mid \equiv T \mid \sim \#(h_1)$;2)$T \mid \equiv R \mid \sim \#(h_2)$。

证明过程如下:

1)因 $R \mid \equiv \#(s_t)$,$R \mid \equiv \#(ID_t)$,结合新鲜性规则 $\frac{P \mid \equiv \#(X)}{P \mid \equiv \#(X,Y)}$ 可得 $R \mid \equiv \#(h_1)$;又因 $R<h_1$,结合消息

含义规则$\frac{P|\equiv|\xrightarrow{K}Q \wedge P\lhd\{X\}_{K^{-1}}}{P|\equiv Q|\sim X}$得 $R|\equiv T|\sim h_1$；最后结合 $R|\equiv\#(h_1)$得 $R|\equiv T|\sim\#(h_1)$，得证。

2）因 $T|\equiv\#(s_R)$，$T|\equiv\#(ID_R)$，结合新鲜性规则$\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$可得 $T|\sim\#(h_2)$；又因 $T<h_2$，结合消息含义规则$\frac{P|\equiv|\xrightarrow{K}Q \wedge P\lhd\{X\}_{K^{-1}}}{P|\equiv Q|\sim X}$得 $T|\equiv R|\sim h_2$；最后结合 $T|\sim\#(h_2)$得 $T|\equiv R|\sim\#(h_2)$，得证。

综上，可证明本文方案可以达到预期认证目标，本文协议是安全的。

5 安全性分析

本文协议提供如下的安全特性：

1）零知识性

本文协议的零知识性证明只需一次验证，就可取得有效信息，无需步骤重复 n 次。攻击者企图通过窃听获得信息，在整个协议执行过程中，攻击者有可能获得交互信息：h_1，h_2，s_t，s_R，ID_t，ID_R，t，并以此试图分析出阅读器和标签的核心信息：私钥 d。由于本文协议基于 SM2 算法，计算值是基于 $E(F_p)$ 上的运算得来，协议的零知识性使得攻击者窃听到的信息对其目的毫无用处。

2）双向认证

在标签认证阶段，阅读器对标签发来的 h_1，s_t，ID_t，t，需要计算 T_t'，并判断等式 $h_1=H(T_R'+ID_R+t)\bmod n$ 是否成立，完成阅读器对标签的认证。之后在阅读器认证阶段，标签收到阅读器发送的 h_2，s_R，ID_R，t，标签计算 T_R'，将计算结果代入 $H(T_R'+ID_R+t)\bmod n$，判断等式 $h_2=H(T_R'+ID_R+t)\bmod n$。综上完成双向认证。并可抵抗标签冒充攻击，阅读器冒充攻击。

3）防范重放攻击

攻击者实施重放攻击时，捕获阅读器与标签之前的交互信息，将认证信息再次发送以达到通过认证的目的，即捕获之前的信息，冒充交互时传输数据进行重放攻击，但是本文协议在每一次会话认证时会产生随机数，所以可防范重放攻击。

4）防范中间人攻击

中间人攻击是攻击者入侵通信双方的通信过程，冒充阅读器或者标签进行攻击，类似于重放攻击。在本文协议设计中，通信过程中引入 SM2 算法对数据进行签名，传输的各个参数都是经过严格计算得来，互相之间有着紧密的逻辑关系。另外，之前经分析，本文协议可以防范重放攻击，因此，本文协议也可以防范中间人攻击。

现今比较有代表性的各种 RFID 认证协议对比结果如表 2 所示，其中，√表示抵抗；×表示不抵抗。文献[9]协议达到双向认证时交互次数为5 次，而本文协议仅需 2 次，可见本文协议具有明显优势。

表 2 各种协议安全性对比

协议	冒充攻击	窃听攻击	重放攻击	中间人攻击	认证方式
文献[1]协议	×	×	×	×	单向
文献[2]协议	×	×	×	×	单向
文献[4]协议	√	√	√	×	单向
文献[5]协议	×	√	×	√	单向
文献[8]协议	√	√	√	√	单向
文献[9]协议	√	√	√	√	双向
本文协议	√	√	√	√	双向

6 效率分析

认证协议效率主要从信息交换次数、计算复杂度来考虑。本文方案仅经过 2 次信息交换即可完成双向认证，执行过程中只需要进行椭圆曲线上的点乘、点加以及一些普通运算，计算复杂度较低，在保证高安全性的同时，能够实现 RFID 系统环境中的双向认证，这个效率是比较优良的。

7 结束语

针对现有 RFID 系统中面临的主要安全问题，本文结合 SM2 算法和零知识证明，设计了一种基于 SM2 零知识的 RFID 双向认证协议，并给出了正确性证明。经过安全性分析和对比，证明本文协议在抵抗冒充攻击、窃听攻击、重放攻击、中间人攻击等主流攻击手段方面具有优势，并且在保障安全性的同时可明显减少信息交互次数，提高通信效率。

参考文献

[1] 刘博雅，郭国辉，李子臣. 基于端到端协议的 RFID 双向认证协议[J]. 北京电子科技学院学报，2014，22(4)：29-33.

[2] Sarma S E，Weis S A，Engels D W. RFID Systems and Security Implications[M]//Koç C K，Paar C. Cryptographic Hardware and Embedded Systems. Berlin，Germany：Springer，2003：454-469.

[3] Weis S A，Sarma S E，Rivest R L，et al. Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems[M]//Ferrari G. Security in Pervasive Computing. Berlin，Germany：Springer，2004：201-212.

[4] Henrici D，Muller P. Hash-based Enhancement of Location Privacy for Radio-frequency Identification Devices Using Varying Identifiers[C]// Proceedings of the 2nd IEEE Annual Conference on Pervasive Com-puting and Communications. Washington D.C.，USA：IEEE Press，2004：149-153.

[5] Rhee K，Kwak J，Kim S，et al. Challenge-response Based RFID Authentication Protocol Distributed Database Environment[C]//Proceedings of International Conference on Security in Pervasive Computing. Berlin，Germany：Springer，2005：70-84.

（下转第 104 页）

分$(x_0 \oplus (y_0 <<< k)) \oplus ((x_0 + y_0) <<< k)$,要分析其线性化条件,只需分析$(x_0 + y_0) <<< k$的线性化条件。下面将证明$(x_0 + y_0) <<< k$的线性化条件与$x_0 + y_0$相同。由于$x_0 + y_0 = x_0 \oplus y_0$等价于:$(x_0 + y_0) <<< k = (x_0 \oplus y_0) <<< k$,因此变换$g$对定理 2 的结果没有影响。

由定理 2 和定理 3 可得推论 2。

推论 2 满足$f(g(f(x,y)))$线性化条件成立的概率为$(2^{\frac{n}{[n,k]}} + (-1)^{\frac{n}{[n,k]}})^{[n,k]-1} \times 2^{\frac{n}{[n,k]}-2n+1}$。

2 结束语

本文通过考察两轮迭代之间的不独立性,给出二元 ARX 函数两轮迭代同时线性化的条件及其成立概率的计算公式,并说明两轮迭代之间增加一个左右块变换并不会对其线性化条件产生影响。比较了在两轮迭代独立和不独立情况下二元 ARX 函数两轮迭代线性化条件成立的概率,结果表明本文方法得到的结果可准确刻画影响两轮迭代线性化条件成立概率的因素,更有利于对密码算法进行线性分析。

参考文献

[1] Ferguson N, Lucks S, Schneier B, et al. The Skein Hash Function Family [EB/OL]. (2008-10-29). http://www.schneier.com/skein1.3.pdf.

[2] Aumasson J P, Henzen L, Meier W, et al. SHA-3 Proposal BLAKE [EB/OL]. (2010-10-10). http://csrc.nist.gov/groups/ST/hash/sha-3/index.html.

[3] Berstein D J. The Salsa20/8 and Salsa20/12 [EB/OL]. (2006-01-16). http://cr.yp.to/snuffle/812.pdf.

[4] Biham E, Seberry J, Gonzalez N. A Fast and Secure Stream Cipher Using Rolling Arrays [EB/OL]. (2005-01-29). http://www.uow.edu.au/~jennie/WEB/WEB05/py-submission.pdf.

[5] Lai Xuejia, Massey J L. A Proposal for a New Block Encryption Standard[C]//Proceedings of Workshop on the Theory and Application of Cryptographic Techniques. Berlin, Germany: Springer, 1990: 389-404.

[6] 郭建胜,金晨辉. 逐位模 2 加运算与模 2^n 加运算的相容程度分析[J]. 高校应用数学学报,2003,18(2):247-250.

[7] 张 龙,吴文玲,温巧燕. Mod2^n 加运算与 F_2 上异或运算差值的概率分布和递推公式[J]. 北京邮电大学学报,2007,30(1):85-89.

[8] 陈士伟,金晨辉. 模 2 加整体逼近二元和三元模 2^n 加的噪声函数分析[J]. 电子与信息学报,2008,30(6):1445-1449.

[9] 陈士伟,金晨辉,李席斌. 模 2^n 加与模 2 加相对于交换律的相容程度分析及其应用[J]. 北京邮电大学学报,2010,33(3):44-47.

[10] 买应霞,陈士伟,李席斌. 异或加整体逼近模 2^n 加差值函数的和概率分布[J]. 计算机工程,2013,39(4):128-131.

[11] Matsui M. Linear Cryptanalysis Method for DES Cipher[C]//Proceedings of Workshop on the Theory and Application of Cryptographic Techniques. Berlin, Germany: Springer, 1993: 386-397.

[12] Wallen J. Linear Approximations of Addition Modulo 2^n[C]//Proceedings of International Workshop on Fast Software Encryption. Berlin, Germany: Springer, 2003: 261-273.

[13] Sekar G, Paul S, Preneel B. Distinguishing Attacks on the Stream Cipher Py[C]//Proceedings of the 13th International Conference on Fast Software Encryption. New York, USA: ACM Press, 2005: 405-421.

[14] Yu Hongbo, Chen Jiazhe, Jia Keting, et al. Near-collision Attack on the Step-reduced Compression Function of Skein-256[M]. Berlin, Germany: Springer, 2011.

[15] Aumasson J P, Leurent G, Meier W, et al. Tuple Cryptanalysis of ARX with Application to BLAKE and Skein[C]//Proceedings of ECRYPT Workshop on Hash Functions. Berlin, Germany: Springer, 2011: 1-13.

编辑 顾逸斐

(上接第 100 页)

[6] 熊宛星,薛开平,洪佩琳,等. 基于二维区间 Hash 链的 RFID 安全协议[J]. 中国科学技术大学学报,2011,41(7):594-598.

[7] Tuyls P, Batina L. RFID-tags for Anti-counterfeiting[M]. Berlin, Germany: Springer, 2006.

[8] Lee Y K, Batina L, Verbauwhde I. EGRAC (ECDLP based Randomized Access Control): Provably Secure RFID Authentication Protocol[C]//Proceedings of IEEE International Conference on RFID. Washington D. C., USA: IEEE Press, 2008: 97-104.

[9] Chen Yalin, Chou Jue-sam, Lin Chi-fong, et al. A Novel RFID Authentication Protocol Based on Elliptic Curve Crypto System[EB/OL]. (2011-01-13). http://eprint.iacr.org/2011/381.pdf.

[10] 王笑梅,张秋剑. 基于椭圆曲线零知识的 RFID 双向身份认证[J]. 计算机工程与应用,2013,49(15):97-100.

[11] Piramuthu S. RFID Mutual Authentication Protocols[J]. Decision Support Systems, 2011, 50(2): 387-393.

[12] Abyaneh M R S. Security Analysis of Lightweight Schemes for RFID Systems [D]. Bergen, Norway: University of Bergen, 2012.

[13] Cho J S, James J, Park J H. High Attack Cost: Hash Based RFID Tag Mutual Authentication Protocol[M]//Chao H C, Obaidat M, Kim J. Computer Science and Convergence. Berlin, Germany: Springer, 2012.

[14] Piramuthu S. Vulnerabilities of RFID Protocols Proposed in ISF[J]. Information Systems Frontiers, 2012, 14(3): 647-651.

[15] Moriyama D, Matsuo S, Ohkubo M. Relations Among Notions of Privacy for RFID Authentication Protocols[J]. IEICE Transactions on Fundamentals of Electronics Communications & Computer Sciences, 2014, 97(1): 225-235.

[16] Wang Shaohui, Liu Sujuan. Attacks and Improvements on the RFID Authentication Protocols Based on Matrix[J]. Journal of Electronics, 2013, 30(1): 33-39.

编辑 顾逸斐