一种Gen2v2标准下的高效隐私保护认证协议

吴 迭[1,2]，鲁 力[2]，张凤荔[1*]

(1. 电子科技大学信息与软件工程学院 成都 610054；2. 电子科技大学计算机科学与工程学院 成都 611731)

【摘要】EPC Class-1 Generation-2 Version-2(Gen2v2)标准不仅继承了原有标准的通信距离长和读取率高的优点，而且提出了一个全新的安全架构以提高系统的安全性。目前，Gen2v2标准安全架构下的安全认证协议设计已经成为该领域的研究热点之一。该文在分析现有符合Gen2v2标准的安全认证协议的基础上，提出了一种新的符合Gen2v2标准的高效隐私保护认证协议。该协议不仅具有数据机密性、标签匿名性和前向安全性，而且能够抵御假冒攻击、位置追踪攻击、嗅探攻击、重放攻击和去同步攻击。与现有协议相比，该协议具有较小的通信和时间开销，更加适合大规模的部署。

关 键 词 认证； 隐私保护； 射频识别； 安全协议

中图分类号 TP399 **文献标志码** A doi:10.3969/j.issn.1001-0548.2019.03.014

An Effective Privacy Preserving Authentication Protocol for Gen2v2 Standard

WU Die[1,2], LU Li[2], and ZHANG Feng-li[1*]

(1. School of Information and Software Engineering, University of Electronic Science and Technology of China Chengdu 610054;
2. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract EPC Class-1 Generation-2 Version-2 (Gen2v2 for short) not only inherits the advantages of the original standard in terms of long reading range and large reading volume, but proposes a new security framework to enhance the security of radio frequency identification (RFID) system. Nowadays, the authentication protocol designed under the security framework has emerged as a hot topic. Based on the analysis of the existing Gen2v2-compliant authentication protocols, a new effective privacy preserving authentication protocol for Gen2v2 standard is proposed. The protocol is able not only to provide data confidentiality, anonymity and forward security, but also to withstand the tag impersonation attack, tracking attack, sniffing attack, replay attack and desynchronization attack. Compared with the existing works, the protocol has a lower communication and time overhead, and is more suitable for large-scale deployment.

Key words authentication; privacy preserving; radio frequency identification(RFID); security protocol

射频识别技术(radio frequency identification, RFID)是一种利用无线射频信号在开放环境中与特定目标进行自动识别的技术，被广泛应用于物流管理、产品防伪、访问控制以及军事管理等诸多领域。其中，EPC Class-1 Generation-2(Gen2v1)标准[1]由于其成本低、通信距离长以及读取率高等优势，已经成为超高频段860～960 MHz的主流标准。然而，随着该标准的广泛应用，RFID系统所面临的隐私泄露、恶意追踪、非法读取、标签伪造[2-6]等安全问题也逐渐暴露。

为了解决这些问题，国内外学者虽然提出了很多安全认证协议[7-10]，但是，这些方案都需要对原有标准进行修改[11]，至今仍然没有一个行之有效的方案可以在不改变现有标准的前提下，保证RFID系统的安全。2013年11月，国际标准化组织EPCglobal发布了新版的RFID通信标准EPC Class-1 Generation-2 Version-2(Gen2v2标准)[12]。该标准不仅继承了原有标准的通信距离长和读取率高的优点，而且提出了一个全新的安全架构，以保证RFID系统的安全性。鉴于Gen2v2标准的优越性，Gen2v1标准正被逐步取代。因此，对Gen2v2标准安全架构下的安全认证协议的研究已经成为该领域的热点之一。

尽管目前已经出现了一些符合Gen2v2标准的安全认证协议[13-15]，但这些协议执行效率低下且大都

收稿日期：2018－01－18；修回日期：2018－03－15
基金项目：国家自然科学基金(61472068, 61602331)；四川省科技厅支撑计划(2016JZ0020)
作者简介：吴迭(1988－)，男，博士生，主要从事射频识别和无线通信方面的研究.
通信作者：张凤荔，E-mail: fzhang@uestc.edu.cn

存在着某些安全隐患。本文分析了现有协议的不足，在此基础上提出了一种新的符合Gen2v2标准的高效隐私保护认证协议。新协议基于Gen2v2标准的安全架构，并将高级加密标准(advanced encryption standard, AES)与挑战应答机制相结合，有效地保护了阅读器和标签的隐私。同时，通过将标签的认证消息作为标签ID传送，使得该协议能够在盘存阶段就完成认证，从而避免了标签信息的泄露。与现有协议相比，本文协议的安全性和执行效率更高。

1 背景知识

根据Gen2v2标准，阅读器和标签之间的通信可以分成选择、盘存和访问3个阶段。在选择阶段，阅读器发送选择指令筛选能够参与后续通信过程的标签。在盘存阶段，阅读器发送盘存指令设置标签响应的编码方式和数据率，再发送确认指令以获得标签的ID，并实现阅读器和标签的一对一通信。在访问阶段，阅读器需首先发送请求句柄指令，使标签进入开放状态，并将得到的句柄作为参数嵌入到访问指令中，以实现对标签的访问。

为了使基于密码学的安全机制在RFID系统中得到实际的应用，Gen2v2标准在其安全架构中提出了6个用户可选的指令：Challenge、Authenticate、SecureComm、AuthComm、KeyUpdate和ReadBuffer。其中，Challenge和Authenticate指令主要用于身份认证，SecureComm和AuthComm指令使得阅读器和标签可以进行安全的信息交互，KeyUpdate指令让阅读器可以安全地更新标签的密钥，而ReadBuffer指令使阅读器可以主动地从标签的响应缓冲区中取回标签的响应。

2 现有方案

由于国内外对Gen2v2标准的研究尚处于起步阶段，只有为数不多的安全认证协议符合Gen2v2标准。文献[13]首次提出了一种符合Gen2v2标准的安全认证机制。在该方案中，阅读器先通过发送选择和盘存指令使RFID系统进入访问阶段，再通过两次Authenticate指令及相应的两次延时响应实现认证信息的交换。然而，该方案的缺点是不能抵御伪造标签攻击和中间人攻击，同时由于该方案的认证过程发生在访问阶段，标签的ID在盘存阶段以明文信息传送，使得攻击者可以通过窃听或嗅探在盘存阶段得到标签的ID，并据此追踪标签。文献[14]在文献[13]的基础上提出了一种改进的认证协议，该方案虽然克服了文献[13]中存在的不能抵御标签假冒攻击的缺陷，但由于其协议流程与文献[13]相同，只是改变了传输的认证消息，因此，标签的ID依然在盘存阶段暴露，标签的隐私信息不能得到有效的保护，导致该方案依然面临中间人攻击、嗅探攻击和位置追踪攻击等安全隐患。为了解决这些问题，2017年，文献[15]提出了一种具有标签匿名功能的双向认证协议。在该方案中，阅读器通过Challenge指令将随机数广播给标签，并在盘存阶段以随机数替代标签ID，再通过ReadBuffer指令和Authenticate指令及其相应的响应实现认证信息的交换，最后通过SecureComm指令更新共享的秘密参数。然而，该方案不能抵御去同步攻击。同时，由于该方案过程复杂且通信开销大，使得协议的执行效率低，并不适合大规模的部署。

3 本文方案

针对现有方案的缺陷与不足，本文提出了一种新的符合Gen2v2标准的高效隐私保护认证协议。为了简化描述，相关符号的说明如表1所示。

表1 符号说明

符号	说明
R	阅读器
T	标签
k	阅读器和标签共享的128位密钥
ID	标签的128位唯一标识符
Index	标签ID的64位索引值(在每一轮中更新)
r	阅读器产生的64位随机数
Enc(k, p)	以k为密钥，p为明文的AES加密函数
Dec(k, c)	以k为密钥，c为明文的AES解密函数
$H_{\mathrm{L}}(a)$	取参数a的前半部分
$H_{\mathrm{R}}(a)$	取参数a的后半部分
C_1	阅读器传输的认证消息
C_2	标签传输的认证消息
P	AES解密得到的明文
||	比特串的连接运算符
⊕	异或运算符号

3.1 初始化

在初始化阶段，系统首先给每一个标签分配唯一的128位的标识符ID和一个128位的共享密钥k，并将其存放在标签的只读存储器中，然后随机为每一个ID生成一个64位的索引值Index并将其存放在标签的非易失性存储器中，最后将每一个标签的密钥k、唯一标识符ID和索引值Index构成一个元组<Index, ID, k>，并存放到其后端数据库中。在本文的协议中，假设阅读器和后端服务器存在一个安全的秘密信道。

3.2 协议描述

本文协议如图1所示。

1) 选择标签

阅读器发送Select指令。其中，阅读器可以通过设置Select指令中的MemBank字段和Mask字段指定所要盘存的标签的类型。例如，在实际部署中，用户可以将MemBank字段设置成01，并将Mask字段设置成标签生产商的代码。这样，只有指定生产商的标签可以参与后续的通信过程。2) 标签对阅读器的认证

① 阅读器将选择待认证的标签，并根据待认证的标签的ID在后端数据库中找出相应的元组<Index, ID, k>。然后，阅读器将随机生成一个64位的随机数r，并计算认证消息C_1=Enc(k, Index||r)；

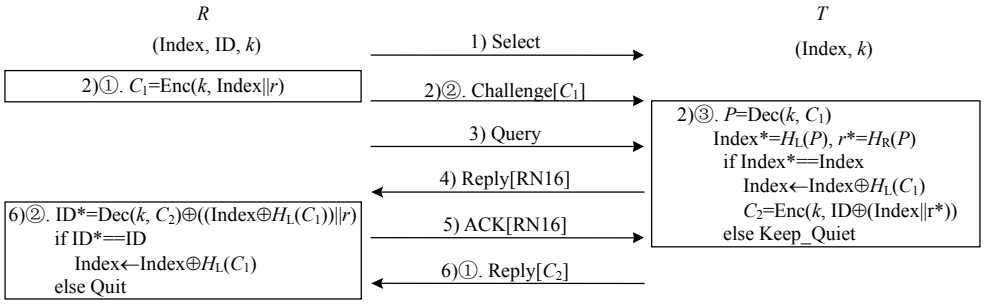

图1　本文协议

② 阅读器将认证消息C_1作为Challenge指令的参数放在Message字段中，并广播给读取范围内的所有标签；

③ 当收到Challenge指令时，标签将按照标准解析出Message字段中存放的认证消息C_1。然后，标签将用自身只读存储器中的共享密钥k解密出的明文P=Dec(k, C_1)，再通过计算Index*=$H_L(P)$和$r^*=H_R(P)$得到索引值Index*和随机数r*。此时，标签将会用存放在其非易失性存储器中的索引值Index与Index*作比较。如果Index ≠ Index*，则阅读器认证失败，标签进入暂时失效状态，并在完全掉电之前忽略所有来自阅读器的指令。如果Index = Index*，则阅读器认证成功。此时，标签会将索引值Index更新为Index= Index ⊕ $H_L(C_1)$。由于Gen2v2标准并不要求标签响应Challenge指令。因此，标签可以提前计算认证消息C_2 = Enc(k, ID ⊕ (Index||r*))。这样，标签不仅有足够的时间完成计算，而且可以在收到后续的ACK指令时，将认证消息立即传送给阅读器。

3) 盘存标签

阅读器发送Query指令使标签进入盘存阶段，并在指令中指定标签的编码方式和数据率。

4) 响应随机数

按照Gen2v2标准，当标签收到Query指令时，会响应一个16位的随机数RN16。

5) 确认标签

阅读器通过将标签响应的16位随机数RN16作为ACK指令的参数回传给标签来确认标签。

6) 阅读器对标签的认证

① 当收到合法的ACK指令时，标签会将在标签对阅读器的认证阶段中(第2)③步)预先计算的认证消息C_2传送给阅读器。

② 当收到认证消息C_2时，阅读器会根据待认证标签的索引值Index，共享密钥k，认证消息C_1和随机数r计算ID*=((Index ⊕ $H_L(C_1)$)||r) ⊕ Dec(k,C_2)。若待认证的标签的ID ≠ ID*，则标签认证失败，会话结束。若ID = ID*，则标签认证成功。此时，阅读器将后端数据库中的相应的元组<Index, ID, k>更新为<Index ⊕ $H_L(C_1)$, ID, k>，以保证阅读器和标签两端存储的信息同步。

4 安全性与效率分析

4.1 安全性分析

针对RFID系统可能面临的各种攻击手段，对本文的认证协议进行安全性分析。

1) 数据机密性

在本文的协议中，由于阅读器和标签之间用于认证的私有信息，如共享密钥k，标签索引Index，以及标签标识符ID在认证过程中都是经过AES算法加密的，因此，即使攻击者即使能够通过窃听得到加密后的认证信息C_1和C_2，也无法从得到的密文中获得这些私有信息。因此，本文协议能够保证系统数据的机密性。

2) 标签匿名性

在本文协议中，当标签收到确认指令时，会用认证消息C_2代替标签的ID在盘存阶段传送，避免了标签隐私的暴露。同时，只有当阅读器被成功认证

时，由于认证消息C_2是经过AES加密的，且每轮认证过程都会有随机数r的参与，从而攻击者无法根据传输的认证消息识别标签的真实身份。因此，本文协议在确保只有合法的阅读器才能获得标签的ID的同时，保证了标签的匿名性。

3) 前向安全性

在本文的协议中，阅读器在每一次认证时都会产生一个新的随机数r，且无法预测，使得前后两次认证中传输的认证消息没有相关性。对于攻击者而言，由于每次窃听得到的认证消息是随机的，因此，无法从当前认证消息中推断出与之前的认证消息相关的信息，从而保证了前向安全性。

4) 防止假冒攻击

在本文的协议中，只有合法阅读器才能计算得到正确的认证消息C_1=Enc(k, Index||r)，并在标签端得到认证。同样只有合法的标签才能够正确解密出随机数r*并更新索引值Index，进而得到正确的认证消息C_2 = Enc(k, ID ⊕ (Index||r*))。对于攻击者而言，认证消息C_1和C_2是动态变化的，而对于拥有密钥k、标识符ID和索引值Index的合法阅读器和标签而言是唯一确定的，所以，在认证过程中，无论哪一条消息被攻击者修改，都会导致认证的失败。因此，本文协议不仅可以有效抵御非法阅读器和非法标签的假冒行为。

5) 防止位置追踪攻击

在位置追踪攻击中，攻击者通过记录阅读器和标签之间传送的信息，并由此追踪标签的位置。然而，在本文所提出的协议中，对于任意一次认证过程，阅读器会产生一个64位的随机数r，这会导致在每次认证时，阅读器和标签之间传输的认证信息C_1和C_2随着随机数的变化而产生动态的变化。不仅如此，标签ID的索引值Index在每次成功认证后都会更新。这一措施，将使得攻击者既无法将当前得到的认证信息与之前获得的认证信息建立联系，也无法将某个标签的认证信息与其他标签的认证信息区分开来。因此，本文协议可以有效抵御攻击者对标签位置的追踪。

6) 防止嗅探攻击

在嗅探攻击中，攻击者通常使用非法阅读器向标签发出指令来嗅探标签上存储的信息。然而，在本文的协议中，只有当阅读器被成功认证时，标签才会进入盘存阶段并响应阅读器的后续指令。否则，标签会进入暂时失效状态，并在完全掉电之前，忽略所有来自阅读器的指令。这一措施，会使得攻击者无法利用非法阅读器从合法标签中套取任何有用信息。因此，本文协议可以有效抵御嗅探攻击。

7) 防止重放攻击

在重放攻击中，攻击者通过窃听阅读器和标签之间的通信，并在之后将窃听得到的认证信息重传给阅读器(或者标签)以骗取阅读器(或者标签)的认证。然而，在本文协议中，当任意一次认证结束之后，阅读器和标签双方都会更新索引值Index，因此，当攻击者伪装成合法阅读器并重放认证消息C_1时，标签解密得到的索引值Index*与标签存储器中已经更新的索引值Index将无法匹配，进而导致认证失败。同样，由于阅读器在每一次认证中产生的随机数r无法预测，且后端数据库中相应的索引值Index已经更新，所以当攻击者伪装成合法标签并重放认证消息C_2时，阅读器根据索引值Index、共享密钥k和随机数r解密得到的标签ID*将无法与待认证标签元组中对应的ID相匹配，从而认证失败。因此，本文协议可以有效抵御重放攻击。

8) 防止去同步攻击

在去同步攻击中，攻击者通过拦截阅读器和标签之间的通信，使得阅读器和标签之间存储的信息不同步，从而导致整个系统无法正常工作。然而，在该协议中，当认证消息C_1被攻击者拦截时，标签会因为没有收到合法认证消息C_1而进入暂时失效状态。在下次认证开始时，阅读器和标签双方存储的信息仍然同步。当认证消息C_2被攻击者拦截时，标签中的索引值Index已经更新为Index=Index ⊕ $H_L(C_1)$，而阅读器后端数据库中相应的索引值Index会由于阅读器没有收到合法的认证消息C_2而保持不变。这会使得阅读器在下次认证时计算得到的认证消息C_1不合法。然而，在本文协议中，阅读器可以先根据上一轮的认证消息将后端数据库中相应的索引值Index更新，再重新计算认证消息C_1。这样，阅读器不仅可以准确发现去同步攻击，而且可以使认证双方信息重新保持同步。因此，本文协议可以有效抵御去同步攻击。

4.2 安全性比较

表2将本文协议与文献[13-15]中的协议进行比较。其中，“√”表示该协议满足此项安全性要求，“×”表示该协议不满足此项安全性要求。根据表2的结果，可以看出本文的协议能够更加全面地保证RFID系统的安全性。

表2　协议的安全性比较

安全性	文献[13]	文献[14]	文献[15]	本文
数据机密性	×	×	√	√
标签匿名性	×	×	√	√
前向安全性	√	√	√	√
防假冒	×	√	√	√
防位置追踪	×	×	√	√
防嗅探	×	×	√	√
防重放	√	√	√	√
防去同步	√	√	×	√

4.3　效率分析

为了验证本文协议的执行效率，对标签加解密次数、协议的通信步数、阅读器发送的比特数和标签发送的比特数这4个方面进行分析，并与已有协议进行比较，其结果如表3所示。

表3 协议的执行效率比较

	文献[13]	文献[14]	文献[15]	本文
*T*加解密次数	2	2	2	2
通信步数	11	10	13	6
*R*发送比特数	381	445	567	261
*T*发送比特数	576	465	377	188

根据表3的比较结果，可以看出虽然本文的协议和已有的协议都需要在标签上执行两次AES加密或者解密计算，但是由于本文协议通过将阅读器的认证信息用Challenge指令传送，并用标签的认证信息替代标签ID以响应阅读器，从而使得该协议的通信步数明显减少，仅需6步就可以完成双向认证。与文献[13]、文献[14]和文献[15]相比，阅读器发送的比特数分别减少了31.5%、41.3%和53.9%，而标签发送的比特数分别减少了67.4%、59.6%和50.1%。因此，本文协议能够有效减小通信开销，显著提高协议执行效率。

为了进一步验证本文协议的性能，将本文协议和已有协议在多标签环境下的执行时间进行了仿真对比，仿真结果如图2所示。实验中，阅读器和标签的发送速率分别为128 kb/s和640 kb/s，工作时钟频率分别为1 GHz和2 MHz。根据Gen2v2标准的时序要求，规定标签从收到阅读器指令到发送响应的时间T_1为15.6～250 μs，阅读器从收到标签响应到发送下一条指令的时间T_2为4.7～31.2 μs，两条指令之间的最小时间间隔T_4为31.2 μs。阅读器和后端数据库的通信时间忽略不计。根据图2的比较结果，可以看出本文的协议在多标签环境下的执行时间显著低于已有协议，更加适合大规模的RFID系统。

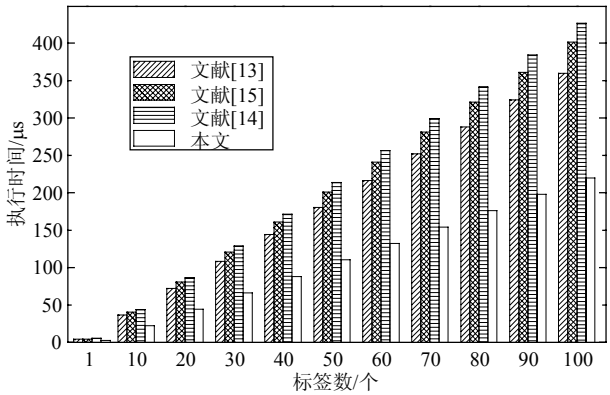

图2　在多标签环境下执行时间比较

5　结 束 语

本文在分析现有符合Gen2v2标准的安全认证协议的基础上，提出了一种新的符合Gen2v2标准的高效隐私保护认证协议。该协议不仅具有数据机密性、标签匿名性和前向安全性，而且能够抵御假冒攻击、位置追踪攻击、嗅探攻击、重放攻击和去同步攻击。与现有协议相比，该协议具有较小的通信和时间开销，更加适合大规模的部署。

参 考 文 献

[1] EPCGLOBAL Inc. EPC radio-frequency identity protocols Class-1 Generation-2 UHF RFID protocol for communications at 860 MHz–960 MHz, version 1.2.0 [EB/OL]. (2008-10-18)[2017-04-15]. http://www.gs1.org/sites/default/files/docs/epc/uhfc1g2_1_2_0-standard-20080511.pdf.

[2] MA D, SAXENA N, XIANG T, et al. Location-aware and safer cards: Enhancing RFID security and privacy via location sensing[J]. IEEE Transactions on Dependable and Secure Computing, 2013, 10(2): 57-69.

[3] NIU B, ZHU X, CHI H, et al. Privacy and authentication protocol for mobile RFID systems[J]. Wireless Personal Communications, 2014, 77(3): 1713-1731.

[4] JING Q, VASILAKOS A V, WAN J, et al. Security of the internet of things: Perspectives and challenges[J]. Wireless Networks, 2014, 20(8): 2481-2501.

[5] CHOI E Y, LEE D H, LIM J I. Anti-cloning protocol suitable to EPCglobal Class-1 Generation-2 RFID systems[J]. Computer Standards & Interfaces, 2009, 31(6): 1124-1130.

[6] HUANG J, LI X, XING C C, et al. DTD: a novel double-track approach to clone detection for RFID-enabled supply chains[J]. IEEE Transactions on Emerging Topics in Computing, 2017, 5(1): 134-140.

[7] TIAN Y, CHEN G, LI J. A new ultralightweight RFID authentication protocol with permutation[J]. IEEE Communications Letters, 2012, 16(5): 702-705.

[8] DARCO P, DE S A. On ultralightweight RFID authentication protocols[J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(4): 548-563.

(下转第461页)

2004.
[12] 陈关荣. 复杂网络及其新近研究进展简介[J]. 力学进展, 2008, 38(6): 653-662.
CHEN Guan-rong. Introduction to complex networks and their recent research progress[J]. Progress in Mechanics, 2008, 38(6): 653-662.
[13] BARABÁSI A, ALBERT R. Emergence of scaling in random networks[J]. Science, 1999, 286(5439): 509-512.
[14] GOH K I, KAHNG B, KIM D. Packet transport and load distribution in scale-free networks[J]. Physica A, 2003, 318(1): 72-79.
[15] MAY R M, LLOYD A L. Infection dynamics on scale-free networks[J]. Physical Review E: Statistical, Nonlinear, and Soft Matter Physics, 2001, 64(6 Pt 2): 066112.
[16] 丁明, 韩平平. 基于小世界拓扑模型的大型电网脆弱性评估算法[J]. 电力系统自动化, 2006, 30(8): 7-10.
DING Ming, HAN Ping-ping. Large-scale grid vulnerability assessment algorithm based on small world topology model[J]. Automation of Electric Power Systems, 2006, 30(8): 7-10.
[17] NEWMAN M E J. Models of the small world[J]. Journal of Statistical Physics, 2000, 101(3-4): 819-841.
[18] BARZEL B, BARABÁSI A. Universality in network dynamics[J]. Nature Physics, 2013, 9(10): 673-681.
[19] KHER K K, SCHNAPER W H, GREENBAUM L A. Clinical pediatric nephrology[M]. 2nd ed. Boca Raton, FL, USA: CRC Press, 2006.
[20] BERLOW E L, DUNNE J A, MARTINEZ N D, et al. Simple prediction of interaction strengths in complex food webs[J]. Proceedings of the National Academy of Sciences of the United States of America, 2009, 106(1): 187-191.
[21] HOLLAND J N, DEANGELIS D L, BRONSTEIN J L. Population dynamics and mutualism: Functional responses of benefits and costs[J]. American Naturalist, 2002, 159(3): 231-244.
[22] PASTORSATORRAS R, VESPIGNANI A. Epidemic spreading in scale-free networks[J]. Physical Review Letters, 2001, 86(14): 3200-3203.
[23] DAVIS C. The norm of the Schur product operation[J]. Numerische Mathematik, 1962, 4(1): 343-344.
[24] WATTS D J, STROGATZ S H. Collective dynamics of 'small-world' networks[J]. Nature, 1998, 393(6684): 440-442.

编 辑 蒋 晓

(上接第401页)

[9] SUN D Z, ZHONG J D. A hash-based RFID security protocol for strong privacy protection[J]. IEEE Transactions on Consumer Electronics, 2012, 58(4): 1246-1252.
[10] ALOMAIR B, LAZOS L, POOVENDRAN R. Securing low-cost RFID systems: an unconditionally secure approach[J]. Journal of Computer Security, 2011, 19(2): 229-257.
[11] LEE C F, CHIEN H Y, LAIH C S, et al. On the security of several Gen2-based protocols without modifying the standards[J]. Journal of the Chinese Institute of Engineers, 2012, 35(4): 391-399.
[12] EPCGLOBAL Inc. EPC radio-frequency identity protocols Generation-2 UHF RFID Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHz Version 2.0.0 Ratified[EB/OL]. (2013-11-20) [2017-04-15]. https://www.gs1.org/sites/default/files/docs/epc/uhfc1g2_2_0_0_standard_20131101.pdf.
[13] ENGELS DW, KANG YS, WANG J. On security with the new Gen2 RFID security framework[C]//2013 IEEE International Conference on RFID. Orlando: IEEE, 2013, 4: 144-151.
[14] CHIEN H Y. New Gen2v2-based mutual authentication schemes[C]//IEEE 8th International Conference on Software Security and Reliability-Companion. San Francisco: IEEE, 2014, 6: 88-96.
[15] CHIEN H Y. Efficient authentication scheme with tag-identity protection for EPC class 2 generation 2 version 2 standards[J]. International Journal of Distributed Sensor Networks, 2017, 13(3): 61-70.

编 辑 刘飞阳