# EPCGen2标准下安全的RFID认证协议

邓淼磊[1,3] 黄照鹤[2] 鲁志波[1]
(解放军信息工程大学理学院 郑州 450001)[1] (南阳理工学院网络中心 南阳 473004)[2]
(西安电子科技大学计算机学院 西安 710071)[3]

**摘 要** 现有的许多无线射频识别(RFID)协议或者不符合EPC Class-1 Gen-2(EPCGen2)标准的要求,或者存在某种安全隐患。通过对RFID协议安全需求的讨论,以及对近来提出的符合EPCGen2标准的安全协议的分析,提出了符合EPCGen2标准的RFID认证协议的设计原则,设计了一个新的符合EPCGen2标准的RFID认证协议。新的协议满足双向认证、匿名、不可追踪、抗假冒攻击、抗重放攻击等安全需求。

**关键词** 无线射频识别,认证协议,攻击,安全
**中图法分类号** TP309 **文献标识码** A

## Secure RFID Authentication Protocol for EPCGen2

DENG Miao-lei[1,3] HUANG Zhao-he[2] LU Zhi-bo[1]
(Institute of Science, PLA Information Engineering University, Zhengzhou 450001, China)[1]
(Network Information Center, Nanyang Institute of Technology, Nanyang 473004, China)[2]
(School of Computer, Xidian University, Xi'an 710071, China)[3]

**Abstract** Many of the existing protocols for radio frequency identification (RFID) either do not conform to the EPC Class-1 Gen-2 (EPCGen2) standards or suffer from security flaws. Safety requirements for RFID protocols were discussed and recently proposed EPCGen2 compliant cryptographic protocols were analyzed, and the design principles of EPCGen2 compliant authentication protocols were given. A new RFID authentication protocol based on the EPCGen2 standards was also proposed. The new protocol provides mutual authentication, anonymity, untraceability, anti-impersonation attack and anti-replay attack.

**Keywords** Radio frequency identification, Authentication protocol, Attack, Security

无线射频识别(RFID)是一种利用射频通信实现的非接触式自动识别技术。RFID系统一般由RFID标签、标签读写器和后端数据库构成。近年来,RFID技术已应用于供应链管理、交通管理、电子钱包、生产线自动控制等领域。

为进一步促进RFID技术的应用和支持互操作性,EPCGlobal组织制定了EPC Class-1 Gen-2(EPCGen2)标准[1]。标准中利用一个16bit的伪随机数生成器PRNG和一个16bit的循环冗余校验码CRC为RFID协议提供基本的可靠性保证,符合该标准的标签只采用硬件复杂度较低的PRNG和CRC,而不能采用加密函数和Hash函数。研究者提出了一些符合EPCGen2标准的RFID认证协议[2-8]。本文对这些协议进行分析,并提出一个满足匿名、不可追踪、抗假冒攻击等安全需求的应用于EPCGen2平台的RFID认证协议。

## 1 安全需求分析

在一般应用中,符合EPCGen2标准的RFID安全协议需要满足下面的安全属性。

(1) 双向认证。在许多应用中,不仅要求实现标写器对标签的认证,而且要求实现标签对读写器的认证,确保只有授权读写器能够访问相应的标签。

(2) 匿名。标签用户的真实身份等敏感信息,在通信中应保证机密性。匿名性保证了攻击者即使窃听到协议消息或者参与到协议中与标签直接交互,也不能获得标签的身份信息。

(3) 不可追踪。攻击者不能够根据协议消息,把某个标签同其他标签一直区分开来,从而进行追踪。

(4) 抗假冒攻击。攻击者即使能够观察到读写器和标签间的所有通信,也不能够根据以前获取的协议消息,假冒成一个读写器或者标签来运行协议。

(5) 抗重放攻击。攻击者不能够通过重发旧的消息而通过认证。

## 2 相关协议分析

EPCGen2标准给出的协议是不安全的,暴漏的标签标识(TID)将破坏用户的隐私,并且攻击者可以很容易对标签进行追踪和克隆[7]。随后研究者提出了一些其他符合EPC-

到稿日期:2009-09-04 返修日期:2009-11-09 本文受河南省科技攻关计划项目(102102210432)资助。
邓淼磊(1977—),男,博士生,主要研究方向为安全协议设计和分析,E-mail:dmlei2003@163.com;黄照鹤(1979—),女,讲师,主要研究方向为计算机应用和信息安全;鲁志波(1976—),男,博士,讲师,主要研究方向为信息处理。

Gen2 标准的协议。符合 EPCGen2 标准的协议，是泛指采用 PRNG，CRC 校验和算术逻辑运算等简单操作的 RFID 安全协议。下面对这些协议的安全性进行分析。

(1) Duc 等人使用 PRNG，CRC 和异或运算设计了一个低复杂度的符合 EPCGen2 标准的安全协议[2]。但该协议不能阻止拒绝服务攻击，不能检测非法标签，也不能提供前向安全功能[6]。攻击者还可以对标签进行追踪[7]。而且，在该协议的最后一步，由读写器分别向后端服务器和标签发出会话结束的信息，以更新后端数据库和标签的密钥。如果后端数据库和标签其中之一没有接收到该信息，将会导致后端数据库和标签的密钥不一致，出现数据不同步问题，该标签将不能再通过认证。另外，该协议还是一个单向认证协议，只能实现对标签的认证。

(2) 基于 Duc 等人的工作，Chien 等人提出了一个 RFID 双向认证协议[3]。在该协议中，后端数据库为一个标签随机选取一个初始认证密钥 $K_0$ 和一个初始访问密钥 $P_0$，这样每个标签中初始存储 3 个数值：标签标识符 TID、初始认证密钥 $K_0$ 和初始访问密钥 $P_0$。在第 $i$ 次成功地回话后，标签的认证密钥和访问密钥分别更新为 $K_i$ 和 $P_i$。在后端数据库中，同时存储标签更新前的认证密钥和访问密钥以及更新后的认证密钥和访问密钥。但该协议仍然会受到拒绝服务攻击[8]。

(3) 基于 EPCGen2 标准，Cai 等人设计了一个 RFID 双向认证协议[4]，并使用 BAN 逻辑对协议进行了形式化分析。在该协议中，服务器(即后端数据库)为每个标签分配一个唯一的 32bit 标识 TID，并分别存储在服务器中(表示为 $TID_x$)和标签中(表示为 $TID_i$)；服务器还为每个标签生成一个 32bit 访问密钥 $W$，分别存储在服务器中(表示为 $W_x$)和标签中(表示为 $W_i$)。$TID_{xl}$ 和 $TID_{xh}$ 分别表示 TID 的左 16bit 和右 16bit。协议描述如下：1)读写器选取一个随机数 $R_r$，向标签发送(Query，$R_r$)。2)标签在接收到(Query，$R_r$)后，选取一个随机数 $R_t$，计算 $M_{xl}=\mathrm{CRC}(TID_{xl}\oplus R_t\oplus R_r)$，$M_{xh}=\mathrm{CRC}(TID_{xh}\oplus R_t\oplus R_r)$，然后计算 $M_x=(M_{xl}||M_{xh})\oplus W_x$。标签向读写器发送($M_x$，$R_t$)，读写器接收到这个消息后把($M_x$，$R_t$，$R_r$)发送给服务器。这里||是级联运算，⊕是异或运算。3)服务器接收到消息后，对于数据库中存储的每一个 $TID_i$ 和 $W_i$，验证是否 $M_x\oplus W_i=\mathrm{CRC}(TID_{il}\oplus R_t\oplus R_r)||\mathrm{CRC}(TID_{ih}\oplus R_t\oplus R_r)$，如果成立，那么相应的标签就被识别和认证，协议转到第 4 步；否则，认证失败，停止操作。4)服务器计算 $M_{il}=\mathrm{CRC}(TID_{il}\oplus R_t)$，$M_{ih}=\mathrm{CRC}(TID_{ih}\oplus R_t)$，然后计算 $M_i=(M_{il}||M_{ih})\oplus W_i$。服务器通过读写器向标签发送 $M_i$。5)接收到 $M_i$ 后，标签验证是否 $M_i\oplus W_x=\mathrm{CRC}(TID_{xl}\oplus R_t)||\mathrm{CRC}(TID_{xh}\oplus R_t)$，如果成立，则认证通过，否则，认证失败。

该协议是不安全的，攻击者 $A$ 可以进行下面的攻击：$A$ 窃听某次会话中读写器发送给标签的随机数 $R_r$ 和标签发送给读写器的消息($M_x$，$R_t$)；再次会话时，当 $A$ 接收到读写器发送的随机数 $R_r'$ 时，$A$ 生成一个随机数 $R_t'$，计算 $P_t=R_t'\oplus R_t$，$P_r=R_r'\oplus R_r$，$Q=\mathrm{CRC}(00\oplus P_t\oplus P_r)$ 以及 $M_x'=M_x\oplus(Q||Q)=[(M_{xl}||M_{xh})\oplus W_x]\oplus(Q||Q)=[\mathrm{CRC}(TID_{xl}\oplus R_t'\oplus R_r')||\mathrm{CRC}(TID_{xh}\oplus R_t'\oplus R_r')]\oplus W_x$；然后 $A$ 向读写器发送($M_x'$，$R_t'$)。由于($M_x'$，$R_t'$)是对 $R_r'$ 有效的响应，这样 $A$ 就成功地假冒为一个合法的标签。

(4) Choi 等人提出了一个符合 EPCGen2 标准的安全协议[5]。该协议容易受到两种攻击：读写器假冒攻击和相关密钥攻击[9]。另外在该协议中，每个标签都需要和后端数据库共享 3 个 32bit 的秘密数据，并且标签端的 PRNG 运算次数较多，因此相对来讲，协议过于复杂。

(5) Seo 等人提出了两个符合 EPCGen2 标准的认证协议：方案Ⅰ和方案Ⅱ[6]。在方案Ⅰ中，标签发送给读写器的认证消息中没有包含读写器的随机数值，即协议中的随机数都是由标签生成的，因而容易受到消息重放攻击。攻击者可以在第 2 步向读写器重发它在之前会话中窃听到的消息，在第 3 步，读写器对重发消息进行验证，并能验证是正确的。接着，攻击者可以向读写器发送一个会话结束消息，使得读写器对标签的鉴别码(PIN)进行更新，而相应的标签没有对其鉴别码进行更新，这样导致数据不同步问题。方案Ⅱ也存在同样的问题。

(6) 在 Sun 等人提出的基于 EPCGen2 标准的认证协议 $Gen2^+$ 中[7]，消息中的随机数也都是由标签生成的，因此和 Seo 等人的协议一样，$Gen2^+$ 也容易受到消息重放攻击。

(7) 文献[8]中设计的协议与文献[4]中的协议结构相似，因此文献[8]中的协议也容易受到相似的假冒攻击。

## 3 EPCGen2 协议设计原则

从上面的分析可以看出，符合 EPCGen2 标准的 RFID 认证协议的设计除了需要遵循一般安全协议的设计原则外，还需要符合下面的几个具体原则。

(1) 标签的固定参数信息不能未加保护地出现在协议消息中。例如标签的身份标识 TID，一般是固定不变的，如果未加保护地出现在协议消息中，不仅泄露标签用户的隐私，而且攻击者可以很容易对标签进行追踪和克隆。

(2) 对于读写器向某个标签发出的多次相同挑战，标签每次的响应之间不存在相关性。这是因为如果同一个标签对于相同的挑战，每次的响应都是相同的或者相关的，那么攻击者就可以通过向标签发送相同的挑战来追踪某个标签。

(3) 不同主体发送的消息应具有不同的结构。针对 Cai 等人协议的攻击，就是利用了不同主体发送的消息中的 $M_x$ 和 $M_i$ 具有相同结构这个缺陷。

(4) 随机信息应由读写器和标签共同提供。这主要是为了防止重放攻击。

(5) 慎重对待数据更新问题，后端数据库应存储足够信息，以保证数据同步。不少协议都是因为标签和后端数据库对共享信息的更新没有一致进行，导致数据不同步。

## 4 新的 EPCGen2 协议

本文提出一个新的符合 EPCGen2 标准的 RFID 认证协议 NewGen2。初始时，后端数据库为每个标签分配一个 16bit 密钥 $k$ 和一个 32bit 临时身份标识 $P$，每个标签和后端数据库都共享标签的 TID 以及 $k$ 和 $P$。在认证协议中，每次成功地认证后，都要对 $k$ 和 $P$ 进行更新。为了防止主动攻击者对认证协议的攻击，在后端数据库中，同时存储 $k$ 和 $P$ 更新前的值和更新后的值以及一个标志位 $F$($F=0$ 表示是更新前的值，$F=1$ 表示是更新后的值)，即存储记录(TID，$P_{old}$，$k_{old}$，$F=0$)和(TID，$P_{new}$，$k_{new}$，$F=1$)。用 $D$ 表示后端数据库，

$R$ 表示读写器，$T$ 表示标签，不失一般性，假设 $D$ 和 $R$ 之间的连接是安全的。NewGen2 描述如下。

(1) $R \rightarrow T$: $R$ 生成一个随机数 $n_r$，向 $T$ 发送认证请求，同时将 $n_r$ 发送给 $T$。

(2) $T \rightarrow R \Rightarrow D$: $T$ 生成一个随机数 $n_t$，计算 $M_1 = \mathrm{CRC}(P \oplus (n_r || n_t)) \oplus k$，并向 $R$ 发送 $(M_1, n_t)$。$R$ 把 $(M_1, n_t, n_r)$ 转发给 $D$。

(3) $D$: $D$ 接收到 $(M_1, n_t, n_r)$ 后，搜索数据库中的记录，并对每条记录 $(\mathrm{TID}, P', k', F)$ 计算 $W = M_1 \oplus k'$，验证 $W$ 是否等于 $CRC(P' \oplus (n_r || n_t))$。如果存在记录，使得 $W = \mathrm{CRC}(P' \oplus (n_r || n_t))$，那么 $D$ 完成对 $T$ 的识别，$T$ 认证通过，协议转到第 4 步；否则认证失败，停止操作。

(4) $D \Rightarrow R \rightarrow T$: 对于通过认证的 $T$，$D$ 检查相应记录 $(\mathrm{TID}, P', k', F)$ 中 $F$ 的取值。1) 如果 $F=1$，即 $P' = P_{new}$，$k' = k_{new}$，那么 $D$ 计算 $M_2 = (\mathrm{CRC}(k_{new} || n_r) || \mathrm{CRC}(k_{new} || n_t)) \oplus P_{new}$，并查找具有相同 TID 值的另一条记录 $(\mathrm{TID}, P_{old}, k_{old}, F=0)$，方便起见，这里把记录 $(\mathrm{TID}, P_{old}, k_{old}, F=0)$ 记作 $L_1$，把记录 $(\mathrm{TID}, P_{new}, k_{new}, F=1)$ 记作 $L_2$。$D$ 对 $L_1$ 和 $L_2$ 做如下更新：用 $L_2$ 中 $P_{new}$ 和 $k_{new}$ 的值分别替换 $L_1$ 中 $P_{old}$ 和 $k_{old}$ 的值，然后对 $L_2$ 中 $P_{new}$ 和 $k_{new}$ 进行更新：$P_{new} = \mathrm{PRNG}(P_{new}) || \mathrm{CRC}(P_{new})$，$k_{new} = \mathrm{PRNG}(k_{new})$。最后 $D$ 把 $M_2$ 和 $T$ 的相关参数发送给 $R$，$R$ 把 $M_2$ 转发给 $T$。2) 如果 $F=0$，即 $P' = P_{old}$，$k' = k_{old}$，那么 $D$ 计算 $M_2 = (\mathrm{CRC}(k_{old} || n_r) || \mathrm{CRC}(k_{old} || n_t)) \oplus P_{old}$，然后把 $M_2$ 和 $T$ 的相关参数发送给 $R$，$R$ 把 $M_2$ 转发给 $T$。

(5) $T$: $T$ 接收到 $M_2$ 后，验证 $M_2 \oplus P = (\mathrm{CRC}(k || n_r) || \mathrm{CRC}(k || n_t))$ 是否成立，如果成立，则认证通过，并更新 $P$ 和 $k$: $P = \mathrm{PRNG}(P) || \mathrm{CRC}(P)$，$k = \mathrm{PRNG}(k)$；否则认证失败，停止操作。

## 5 安全性分析

设 NewGen2 协议的攻击者为 $A$，$A$ 具有一般 RFID 安全协议攻击者的能力[10]。下面说明 NewGen2 协议能够满足第 2 节定义的安全需求。

### 5.1 双向认证

在 NewGen2 中，只有拥有相应 $P$ 和 $k$ 值的标签，才能计算出正确的 $M_1$，也只有存储有相应 $P$ 和 $k$ 值的后端数据库，才能计算出正确的 $M_2$。通过发送 $M_1$ 和 $M_2$，标签和后端数据库(包括读写器)实现了相互认证。

### 5.2 匿名

NewGen2 协议很好地实现了匿名性。标签的身份标识存储在后端数据库中，只有授权的读写器可以获悉通过认证的标签的真实身份。并且在消息的传输过程中，标签的身份标识并没有被传输，一个随机数用作了标签的临时身份标识，$A$ 无法把这个随机数和标签的真实身份关联起来。

### 5.3 不可追踪

假设 $A$ 企图追踪标签 $T$。如果 $A$ 能够持续地把 $T$ 与其他标签区分开来，$A$ 的攻击就成功。$A$ 的这种攻击通常是通过重复使用一个能使 $T$ 产生固定响应的挑战来实现的。在 NewGen2 协议中，$A$ 可以重复使用相同的 $n_r$，但是每次标签响应的 $M_1$ 值都不相同，并且没有相关性(对 $A$ 而言)，因此 $A$ 的攻击不会成功。

### 5.4 抗假冒攻击

假设 $A$ 能够观察到 $R$ 和 $T$ 之间所有的交互，即 $A$ 能够获取 $n_r$，$n_t$，$M_1$ 和 $M_2$。由于这 4 个数值在每次协议运行中都是随机变化的，$A$ 无法根据它们过去的值推导出当前的值，并且每次成功地认证后，$D$ 和 $T$ 都要更新 $k$ 和 $P$，对于 $A$ 来讲 ($k$ 和 $P$ 是保密的)，$n_r$，$n_t$，$M_1$ 和 $M_2$ 这 4 个数值是相互独立的，因此 $A$ 不能假冒成 $R$ 或 $T$。

### 5.5 抗重放攻击

$A$ 的具体执行如下：当 $R$ 向 $T$ 发送 $n_r$ 进行认证请求后，$A$ 可以窃听到 $T$ 发送给 $R$ 的响应 $(M_1, n_t)$，其中 $M_1 = \mathrm{CRC}(P \oplus (n_r || n_t)) \oplus k$；在下一次认证过程中，当 $R$ 向 $T$ 发送 $n_r'$ 进行认证请求 $n_r'$ 时，$A$ 假冒成 $T$ 用旧的 $(M_1, n_t)$ 来响应此次 $R$ 的认证请求，由于两次的随机数 $n_r$ 和 $n_r'$ 相同的概率极小，并且 $k$ 和 $P$ 在每次成功认证后都进行了更新，因此重发的消息，将不能通过验证。

**结束语** 随着 RFID 技术的广泛应用，越来越多的安全和隐私问题也随之出现。现有的安全协议方案，大多都存在某种安全隐患或不符合 EPCGen2 标准的要求，无法成为实际可用的 RFID 系统安全机制。本文提出的 NewGen2 认证协议，符合 EPCGen2 标准，并且能够满足 RFID 协议的各种安全需求。NewGen2 协议存在的不足是：对于存在较多标签的场合，后端数据库在查找匹配的记录时，涉及大量的匹配计算。因此设计高性能的查找算法是下一步的研究工作。

## 参 考 文 献


[1] EPC Class 1 Gen 2 standard[OL]. http://www.epcglobalinc.org/standards/uhfc1g2/

[2] Duc D C, Park J, Lee H, et al. Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning[C] // The 2006 Symposium on Cryptography and Information Security. Hiroshima: ACM Press, 2006: 269-277

[3] Chien H Y, Chen C H. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards[J]. Computer Standards & Interfaces, 2007, 26(2): 254-259

[4] Cai Q L, Zhan Y J, Wang Y H. A minimalist mutual authentication protocol for RFID system & BAN logic analysis[C] // ISECS International Colloquium Computing, Communication, Control, and Management. Guangzhou: IEEE Press, 2008: 449-453

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

[6] Seo D H, Baek J M, Cho D S. Secure RFID authentication scheme for EPC Class Gen2[C] // International Conference on Ubiquitous Information Management and Communication. Suwon: IEEE Press, 2009: 221-227

[7] Sun H M, Ting W C. A Gen2-based RFID authentication protocol for security and privacy[J]. IEEE Transactions on Mobile Computing, 2009, 8(1): 1-11

[8] 张辉，侯朝焕，王东辉. 一种基于部分 ID 的新型 RFID 安全隐私相互认证协议[J]. 电子与信息学报，2009，31(4)：853-856

[9] Burmester M, Munilla J. A flyweight RFID authentication protocol[OL]. http://eprint.iacr.org/2009/212.pdf

[10] Rotter P. A framework for assessing RFID system security and privacy risks[J]. Pervasive Computing, 2008, 7(4): 70-77