一种改进的基于标签部分ID的RFID密钥无线生成算法

黄 琪 凌 捷 何晓桃
(广东工业大学计算机学院 广州 510006)

摘 要 针对无线射频识别系统存在的初始密钥易泄露的安全问题,提出了一种基于标签部分ID的RFID密钥无线生成算法。在标签与读写器认证之前,通过标签部分ID与读写器生成的随机数进行异或运算生成共享密钥。安全性分析表明,该算法能够有效地抵抗重放攻击、中间人攻击和去同步化攻击等主动攻击及被动攻击,具有安全性高、成本低的优点。

关键词 RFID,标识符,密钥生成,隐私保护
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.01.033

Improved RFID Key Wireless Generation Algorithm Based on Tag Part ID

HUANG Qi LING Jie HE Xiao-tao
(School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China)

Abstract Aiming at the security problem that the initial key is easy to leak in the wireless radio frequency identification system, a RFID key wireless generation algorithm based on tag part ID was proposed. Before the tag and reader authentication, the sharing key is generated by the part of label ID and the random number reader generated XOR. Security analysis shows that the proposed algorithm can effectively resist replay attacks, man-in-the-middle attacks, desynchronization attacks and other active attacks, as well as passive attacks, with high security and low cost advantages.

Keywords RFID, ID, Key generation, Privacy protection

1 引言

随着无线射频识别技术的不断发展与完善,现有的RFID标签以其成本低、易部署、易携带、体积小等优点已被广泛应用于各个领域,如仓储物流管理[1,2]、资产跟踪管理[3,4]、访问控制[5,6]和智能感知[7,8]等。RFID系统一般包括3部分:标签、读写器和后端数据库[9]。标签由耦合元件及芯片组成,每个标签具有唯一的电子编码,附着在物体上标识目标对象。读写器可通过射频信号读取标签信息,然后把信息传输给后端数据库[10]。通常认为读写器与后端数据库之间的信息传输信道是安全可靠的,它们之间的通信安全可理解为传统的网络安全[11]。在RFID系统中,标签和读写器之间利用共享密钥进行认证和识别,一般情况是假设初始设置的密钥是安全的。但攻击者可能会通过某些特殊手段获得标签与读写器之间的共享密钥,进而获得标签隐私信息,引发隐私安全问题[12]。密钥无线生成的方法(Wireless Key Generation, WiKey)实现了在RFID标签上生成密钥。WiKey的基本思想是利用RFID系统中读写器向标签传输信息的信道(前向信道)与标签向读写器传送信息的信道(后向信道)的不对称性,标签和读写器分别生成密钥碎片,然后标签再混合这两部分的密钥碎片从而生成共享密钥[13]。WiKey中后向信道信号很弱,标签到读写器的后向信道的通信距离较短,敌手距离标签较远,敌手窃听较困难,因此定义的敌手模型中假设标签向读写器传输的信息是不可窃听的,但仍存在敌手通过特殊的信号增强器来增强信号进而窃听信息这一可能性。并且在WiKey设计中的密钥生成阶段,读写器与标签之间的信息以明文传输,而在实际应用场景中,明文传输的信息可能被窃听。

基于上述安全隐患,本文综合考虑后向信道可窃听和不可窃听两方面,提出了一种改进的密钥无线生成算法,在标签端不需要生成随机数,只需要利用部分ID和读写器生成的随机数来计算共享密钥,实现了读写器与标签间密钥的无线生成。安全性分析和性能分析表明,本文算法提高了密钥无线生成的安全性,减少了标签端的计算开销。

2 相关工作

信号隔离属于密钥生成安全方法中的物理方法[14],主要是利用法拉第笼来保护读写器与标签之间的通信。法拉第笼是由金属或者良导体形成的笼子,能够屏蔽笼内的无线信号,使标签与读写器之间以明文消息传输。但由于其容量较小,无法容纳大型物体中的RFID标签,因此难以运用在实际应用中。

到稿日期:2015-12-28 返修日期:2016-06-20 本文受广东省科技计划项目(2015B010128014,2015B010108002,2015B090906016,2014A010103029,2014B090908011),广州市科技计划项目(201508010026)资助。

黄 琪(1993—),女,硕士生,主要研究方向为网络与信息安全,E-mail:871722971@qq.com;凌 捷(1964—),男,博士,教授,CCF会员,主要研究方向为网络与信息安全;何晓桃(1971—),女,硕士,副教授,主要研究方向为网络与信息安全。

文献[15]研究了基于散列链的密钥预分配方法。首先通过一系列长度相等的散列链构成密钥池，然后利用普通节点[16]预分发一些特殊密钥。但由于此种方法对设备的计算、存储能力要求较高，刚好与标签所具有的特征相反，因此不太适合 RFID 系统应用。

文献[17,18]提出了基于公钥密码学体制的密钥生成方法，使用如 RSA 加密算法[17]等进行密钥生成。但该类方法由于涉及较复杂的计算，而 RFID 标签资源严重受限，因此也不太适合 RFID 系统应用。

密钥无线生成方法利用信道不对称性[19]，让标签向读写器发送密钥碎片，读写器可将自身生成的另一密钥碎片与接收到的密钥碎片混合生成共享密钥。当标签接收到读写器生成的另一密钥碎片时，标签通过混合这些密钥碎片即可生成共享密钥。此方法的安全性依赖于后向信道的不可窃听性，而在实际应用场景中，该信道是有可能被窃听到的；而且读写器与标签之间的消息大都是明文传输的，容易受到攻击，运用于 RFID 系统时存在安全隐患。

针对上述方法存在的缺陷，本文提出一种改进的基于标签部分 ID 的密钥生成方法，利用部分 ID 和读写器产生的随机数进行异或运算生成共享密钥，不需要复杂的密码计算；同时由于标签端不用生成随机数，只需要进行简单的异或运算，减小了标签端的计算开销，降低了标签的成本，适用于资源受限的 RFID 标签。通过安全性分析，该方法能够抵抗重放攻击、去同步化攻击、中间人攻击等主动攻击和被动攻击，提高了密钥的安全性。

3　密钥无线生成算法设计

3.1　算法说明

本文主要考虑读写器与标签之间密钥无线生成的安全性，故假设读写器从后端数据库中读取信息的过程是安全的。文中符号描述如下。

R：读写器

T：标签

T_i：第 i 个标签

n：标签数量

r：读写器生成的随机数（长度为 $2L$）

r_l，r_r：r 的左右两部分值（每部分长度为 L）

ID：标签的身份标识

ID_l，ID_r：ID 的左右两部分值（每部分长度为 L）

ID_i：标签 T_i 的 ID

IDi_l，IDi_r：IDi 的左右两部分值（每部分长度 L）

$\oplus$：异或运算

$[x]_L$：取计算结果 x 的前 L 位

k：共享密钥

k_i：密钥生成因子

PRN：随机数生成函数

3.2　密钥生成过程

RFID 系统密钥生成的两种实际应用场景是：1）读写器为单个标签生成共享密钥；2）读写器为大量标签生成密钥，其中包括读写器为一组标签生成一个共同的组密钥和读写器为大量不同标签生成独立的个体共享密钥。以下是两种场景中密钥生成的具体实现过程。

场景 1　单个标签生成一个共享密钥

读写器为单个标签生成共享密钥的过程如图 1 所示。

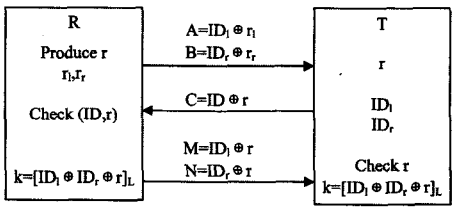

图 1　单个标签密钥生成

单个标签密钥生成的具体步骤如下：

（1）读写器 R 首先生成一个随机数 $r \in_R \{0,1\}^{2L}$，将其分为左右两部分 r_l 和 r_r，并从后台数据库中读取标签的 ID_l 和 ID_r，计算 $A=ID_l \oplus r_l$，$B=ID_r \oplus r_r$，之后将 A，B 作为挑战发送给标签 T。

（2）标签 T 收到 A，B 后，首先计算 $r=A \oplus ID_l$，$r_r=B \oplus ID_r$，由 r_l 和 r_r 可得到 r，然后标签 T 开始计算 $C=ID \oplus r$，最后将 C 作为响应信息传送给读写器 R。

（3）R 收到标签 T 传送的 C 后，首先通过自身生成的随机数 r 和从后台数据库中读取的标签 ID 来计算 $ID \oplus r$，并将计算结果与 C 相比较。若相等，则 R 开始计算 $M=ID_l \oplus r$，$N=ID_r \oplus r$，并将 M，N 传送给标签，最后计算共享密钥 $k=[ID_l \oplus ID_r \oplus r]_L$；反之，说明标签 T 是伪造的，此时立即终止通信。

（4）T 接收到 M 和 N 后，首先通过自身的 ID_l 和 ID_r 来计算 $M \oplus ID_l$ 和 $N \oplus ID_r$，将得到的两个结果相比较，判断是否相等。若相等，则说明 R 是合法的，标签 T 开始计算共享密钥 $k=[ID_l \oplus ID_r \oplus r]_L$；若不相等，则说明 R 是伪造的，通信立即终止。

场景 2　大量标签生成共享密钥

该场景又包括两种情况：1）读写器为一组标签生成一个唯一的共享密钥；2）读写器为大量不同标签同时独立地生成个体密钥。下面就这两种情况详细阐述密钥无线生成的过程。

（1）读写器为一组标签生成一个唯一的共享密钥过程，如图 2 所示。

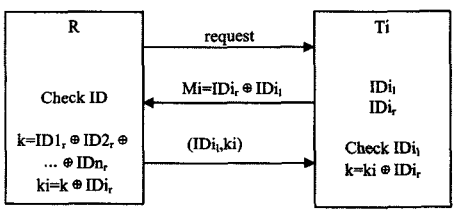

图 2　群组密钥生成

群组密钥生成过程如下：

1）读写器 R 首先向全组标签 T_1，…，T_n 广播一个“密钥生成请求”来通知所有标签开始进行群组密钥生成。

2）组内标签 T_i 收到请求后，计算 $M_i=ID_{i_r} \oplus ID_{i_l}$，并将其发送给读写器 R 作为应答。

3）R 接收到标签 T_i 传送过来的 M_i 后，首先通过从后台数据库中读取的 ID_{i_l} 和 ID_{i_r} 来逐一计算 $ID_{i_r} \oplus ID_{i_l}$，并将计算结果与收到的相对应的 M_i 进行比较。若不完全相等，则

说明有标签没有响应此次请求，或者标签是伪造的，此时读写器将再次发送“密钥生成请求”；若完全相等，说明组内所有标签均已应答，可以开始进行密钥生成，然后接着计算共享群组密钥 $k=ID_{1_r}\oplus ID_{12_r}\oplus\cdots\oplus ID_{n_r}$，再为每个标签 T_i 计算密钥生成因子 $k_i=k\oplus ID_{i_r}$，最后读写器 R 将 (ID_{i_l},k_i) 广播给组内标签。

4）标签 T_i 收到消息 (ID_{i_l},k_i) 之后，首先比较该消息中的 ID_{i_l} 是否与标签 T_i 自身的 ID_l 一致。若一致，则计算共享群组密钥 $k=k_i\oplus ID_{i_r}$；否则 T_i 丢弃该消息。

（2）读写器为大量不同标签同时独立地生成个体密钥过程，如图 3 所示。

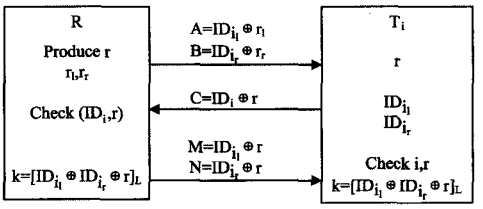

图 3 批量密钥生成

批量密钥生成的详细过程如下：

1）读写器 R 首先生成一个随机数 $r\in_R\{0,1\}^{2L}$，将其分为左右两部分 r_l,r_r，并从后台数据库中读取标签的 ID_l 和 ID_r，然后计算 $A=ID_{i_l}\oplus r_l$，$B=ID_{i_r}\oplus r_r$，最后将 A,B 作为挑战发送给标签 T_i。

2）标签 T_i 收到 A,B 后，首先计算 $r_l=A\oplus ID_{i_l}$，$r_r=B\oplus ID_{i_r}$，由 r_l 和 r_r 可得到 r，然后标签 T_i 开始计算 $C=ID_i\oplus r$，最后将 C 作为响应信息传送给读写器 R。

3）读写器 R 收到标签 T_i 传送的 C 后，首先通过自身生成的随机数 r 和从后台数据库中读取的标签 ID_i 来计算 $ID_i\oplus r$，并将计算结果与 C 相比较。若相等，则 R 开始计算 $M=ID_{i_l}\oplus r$，$N=ID_{i_r}\oplus r$，并将 (M,N,i) 传送给标签 T_i，最后计算共享密钥 $k=[ID_{i_l}\oplus ID_{i_r}\oplus r]_L$；若不相等，说明标签 T_i 是伪造的，此时立即终止通信。

4）标签 T_i 接收到 (M,N,i) 后，首先比对 i 是否与自身序号相等。若不相等，标签就舍弃该消息；若相等，则 T_i 通过自身的 ID_l 和 ID_r 来计算 $M\oplus ID_{i_l}$ 和 $N\oplus ID_{i_r}$，将得到的两个结果进行比较，判断是否相等。若相等，则说明 R 是合法的，标签 T 开始计算所生成的共享密钥 $k=[ID_{i_l}\oplus ID_{i_r}\oplus r]_L$；若不相等，则说明 R 是伪造的，通信立即终止。

4 安全性与性能分析

4.1 主动攻击

攻击者可通过篡改、伪造消息数据等向读写器和标签之间的通信信道注入错误信息，从而欺骗读写器和标签，使其生成错误的密钥。

（1）重放攻击：每次认证时读写器都产生随机数 r，消息 A 中包含 r_l，B 中包含 r_r，若攻击者使用旧的 A 和 B，从而使得标签得到错误的 r，但由于下一步会有对标签 ID 和 r 的验证，当无法匹配出正确的 ID 或 r 时，读写器就会发现信息被篡改而终止通信；若攻击者使用旧的 M 和 N，当标签通过 M，N 验证出 r 不一致时，便会发现信息被篡改而终止通信，故本算法能抵抗重放攻击。

（2）去同步化攻击：若攻击者阻断消息 M 和 N，会使标签和读写器之间信息更新不同步。由于消息 M 和 N 是读写器发送给标签的最后一条消息，当读写器正常更新时，标签不执行更新操作，但此种情况下两者的不同步更新并不会影响下一轮周期的密钥生成。因为共享密钥 k 是由随机数 r 以及部分标签 ID_{i_l} 和 ID_{i_r} 共同计算得来的，在下一轮密钥生成过程中，标签会存储读写器产生的随机数的更新值，从而可计算出正确的共享密钥；若攻击者阻断消息 (ID_{i_l},k_i)，会使标签与读写器之间信息更新不同步。但由于共享组密钥 k 是所有标签 ID_{i_r} 通过异或运算得来的，而标签 ID_{i_r} 是不变的，即使更新不同步，也不会影响密钥生成。因此，本算法能够抵抗去同步化攻击。

（3）中间人攻击：若攻击者篡改了 A 或 B，从而使得标签得到错误的 r，但由于后面的过程中读写器会对标签 ID 和 r 进行验证，当无法匹配出正确的 ID 或 r 时，读写器就会发现标签是伪造的或者信息被篡改而终止通信；若攻击者篡改了 M 或 N，由于其事先无法获悉标签 ID_l 和 ID_r，因此在标签验证 r 的正确性时，会发现信息被篡改或者读写器是伪造的而终止通信；若攻击者伪装成合法标签篡改了 M_i，由于其不知道标签 ID，因此在读写器 R 验证 ID 时便会发现错误信息；若攻击者篡改了 (ID_{i_l},k_i)，由于每个标签 T_i 都会对自身的 ID_l 进行验证，从而会发现伪造的读写器而终止通信。因此本文算法能够抵抗中间人攻击。

4.2 被动攻击

攻击者通过窃听等手段获取读写器与标签之间的通信信息，进而可能获取标签的密钥。

若攻击者窃听到 A,B 和 C，但由于其不知道 ID_l,ID_r,r_l 和 r_r，因此无法得到任何有用信息；若攻击者获得 M 和 N，由于无法获得 ID_l,ID_r 和 r，因此无法得到密钥 k，假设攻击者试图采用暴力破解方式获取密钥，但由于密钥 k 由 ID_l,ID_r,r 3 者共同计算得出，若要利用穷举法列举出所有的 ID_l,ID_r,r，并将其正确组合，难度相当大，几乎不可能得出正确的共享密钥；若攻击者窃听到 M_i，由于其无法知道 ID_{i_l} 和 ID_{i_r}，因此也无法获取其他有用信息；若攻击者窃听到 (ID_{i_l},k_i)，由于在整个通信过程中攻击者都不能够得到 ID_{i_r}，而共享密钥 k 正是由 ID_{i_r} 与 k_i 通过异或运算得到的，因此无法获悉共享密钥。另外，即使攻击者获得了部分标签的 ID_{i_r}，但由于密钥 k 是所有标签 ID_{i_r} 通过异或运算得到的，攻击者若想使用穷举法在 n 个变量中组合出正确的共享密钥，运算量非常大，几乎是不可能实现的。因此，该方法能够抵抗被动攻击。

本文方法与 WiKey 中的密钥生成方法相比，不仅能够抵抗被动攻击和去同步化攻击，还能够抵抗重放攻击和中间人攻击等主动攻击，两种方法的安全性比较结果如表 1 所列。

表 1 安全性比较

项目	WiKey	本文算法
重放攻击	×	√
去同步化攻击	√	√
中间人攻击	×	√
被动攻击	√	√

4.3 性能分析

以下主要从标签的计算量、存储空间和通信量 3 个方面来对算法的性能进行评估。

计算需求：本文算法中标签端不需要生成随机数，只需要进行简单的异或运算提取信息，使标签的计算量得到了有效降低。

存储空间：标签存储着自身的有效 ID 的左右两部分 ID_l 和 ID_r，以及读写器生成的随机数 r 的左右两部分 r_l 和 r_r，每部分的长度均为 L，则标签所需存储空间为 $4L$。

通信量：在本文算法的密钥生成过程中，单个密钥生成过程与批量密钥生成过程总共传输了消息 A,B,C,M 和 N，群组密钥生成过程总共传输了消息 M_i 和 (ID_{i_l},k_i)，而标签的传输消息只有 C 或 M_i。若传输的消息长度为 L，则标签的总通信量为 L。

本文算法与 WiKey 中的密钥生成方法的性能比较如表 2 所列。从表 2 可看出，本文算法需要更少的计算量，因此更适合低成本的 RFID 标签应用。

表 2　性能比较

项目	计算需求	存储空间	通信量
WiKey	⊕+PRN	4L	L
本文算法	⊕	4L	L

结束语　本文提出了一种 RFID 系统密钥无线生成算法，它可提高标签与读写器之间密钥无线生成的安全性。文中针对 RFID 系统不同的实际应用场景分别分析了对应的密钥生成方法，弥补了原有算法的不足，不仅能够抵抗重放攻击、去同步化攻击、中间人攻击和被动攻击，还降低了标签端的成本，适用于低成本、资源受限的 RFID 系统标签。

参 考 文 献

[1] MAMUN M S I, MIYAJI A, RAHMAN M S. A secure and private RFID authentication protocol under SLPN problem[C]// Proc of the 6th Int Conf on Network and System Security. Berlin: Springer, 2012: 476-489.

[2] ALOMAIR B, CUELLAR J, POOVENDRAN R. Scalable RFID systems: A privacy-preserving protocol with constant time identification[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(8): 1536-1550.

[3] ZHOU S J, ZHANG W Q, LUO J Q. Overview of radio frequency identification (RFID) privacy protection technology [J]. Journal of Software, 2015, 26(4): 960-976. (in Chinese)
周世杰，张文清，罗嘉庆. 射频识别(RFID)隐私保护技术综述[J]. 软件学报，2015，26(4)：960-976.

[4] CALMELS B, CANARD S, GIRAULT M, et al. Low-Cost Cryptography for Privacy in RFID Systems[M]// Domingo-Ferrer J, Posegga J, SchrecklingD, eds. Smart Card Research and Advanced Applications. BerlinHeidelberg: Springer, 2006: 37-251.

[5] DING Z H, LI J T, FENG B. Research on hash-based RFID security authentication protocol [J]. Journal of computer Research and Development, 2009, 46(4): 583-592. (in Chinese)
丁振华，李锦涛，冯波. 基于 Hash 函数的 RFID 安全认证协议研究[J]. 计算机研究与发展，2009，46(4)：583-592.

[6] MA C S. Low cost RFID authentication protocol with forward privacy[J]. Chinese Journal of Computers, 2011, 34(8): 1387-1397. (in Chinese)
马昌社. 前向隐私安全的低成本 RFID 认证协议[J]. 计算机学报，2011，34(8)：1387-1397.

[7] SADIKIN M F, KYAS M. Security and privacy protocol for emerging smart RFID applications[C]// Proceeding of the 15th IEEE/ACIS Int'l Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. Atlanta: IEEE Computer Society, 2014: 1-7.

[8] YEH K H, LO N W, WINATA E. An efficient ultralightewight authentication protocol for RFID systems[C]// Proc of RFID Sec Asia 2010. Piscataway, NJ: IEEE, 2010: 49-60.

[9] WANG S H, LIU S J, CHEN D W. Scalable RFID Mutual Authentication Protocol with Backward Privacy [J]. Journal of Computer Research and Development, 2013, 50(6): 1276-1284. (in Chinese)
王少辉，刘素娟，陈丹伟. 满足后向隐私的可扩展 RFID 双向认证方案[J]. 计算机研究与发展，2013，50(6)：1276-1284.

[10] BURMESTER M, MUNILLA J. Lightweight RFID authentication with forward and backward security [J]. ACM Transactions on Information and System Security (TISSEC), 2011, 14(1): 1-11.

[11] JIN Y M, WU Q Y, SHI Z Q, et al. RFID Lightweight Authentication Protocol Based on PRF[J]. Journal of Computer Research and Development, 2014, 51(7): 1506-1514. (in Chinese)
金永明，吴棋澄，石志强，等. 基于 PRF 的 RFID 轻量级认证协议研究[J]. 计算机研究与发展，2014，51(7)：1506-1514.

[12] SHEN J W, LING J. An improved ultra lightweight RFID authentication protocol[J]. Computer Applications and Software, 2015, 32(2): 304-306. (in Chinese)
沈金伟，凌捷. 一种改进的超轻量级 RFID 认证协议[J]. 计算机应用与软件，2015，32(2)：304-306.

[13] LU L. Wireless Key Generation for RFID System[J]. Chinese Journal of Computers, 2015, 38(4): 822-832. (in Chinese)
鲁力. RFID 系统密钥无线生成[J]. 计算机学报，2015，38(4)：822-832.

[14] CANTALICE R, MARCELO L, et al. Low power, high-sensitivity clock recovery circuit for LF/HF RFID applications[C]// Proceedings of the 28th Symposium on Integrated Circuits and Systems Design. NewYork: ACM, 2015.

[15] KUO C, LUK M, NEGI R, et al. Message-in-a-botle: User friendly and secure key deployment for sensor nodes[C]// Proceedings of the 5th International Conference on Embedded Networked Sensor Systems. Sydney, Australia, 2007: 233-246.

[16] SHAMIR A. SQUASH-A new MAC with provable security properties for highly constrained devices such as RFID tags [C]// Proc of Fast Software Encryption. Berlin: Springer, 2008: 144-157.

[17] SHAMIR A. SQUASH-A new MAC with provable security properties for highly constrained devices such as RFID tags[C]// Proc of Fast Software Encryption. Berlin: Springer, 2008: 144-157.

[18] ZUO Y. Survivable RFID Systems: Issues, Challenges, and Techniques [J]. IEEE Transactionson Systems, Man, and Cybernetics, Part C: Applications and Reviews, 2010, 40(4): 406-418.

[19] FINKENZELLER K. RFID Handbook: Fundamentals and Applications in Comtactless, Smart Cards and Identification(2nd Edition)[M]. John Wiley & Sons Ltd, 2003.