超轻量级所有权转移算法研究

谢海宝[1],吕 磊[2]
(1. 河南省市场监督管理局信息中心,河南 郑州 450008;
2. 河南工业大学 信息科学与工程学院,河南 郑州 450008)

摘 要:RFID 系统中电子标签使用周期过程中,电子标签所有者经常发生变化,为确保所有者变化前后每位所有者存放在电子标签中隐私信息的安全,文中设计了一种满足后向安全性的算法。该算法采用基于位运算实现的异或交叉运算对传送信息加密,其中异或交叉运算具体实现过程中将依据加密信息汉明重量大小进行不同规则运算操作,以提升算法安全性;异或交叉运算采用按位运算方式实现,使得算法整体计算量大幅降低,算法可以达到超轻量级的级别。对文中算法及其他不同类型所有权转移算法进行安全及性能理论分析,表明文中算法具备推广所需的要求;同时进行相同环境下的仿真实验,表明文中算法在确保降低计算时间开销的情况下,具备更好的安全性能。

关键词:射频识别系统;电子标签所有权;所有权转移算法;后向安全;超轻量级
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2021)10-0116-06
doi:10.3969/j.issn.1673-629X.2021.10.020

Research on Ultra-lightweight Ownership Transfer Algorithm

XIE Hai-bao[1],LYU Lei[2]
(1. Administration for Market Regulation of Henan Province Information Center,Zhengzhou 450008,China;
2. School of Information Science and Technology,Henan University of Technology,Zhengzhou 450008,China)

Abstract:In the RFID system,the owner of the electronic tag often changes during its service life. In order to ensure the security of the privacy information stored in the electronic tag by each owner before and after the change of the owner,a backward security algorithm is designed. In this algorithm,XOR cross operation based on bit operation is used to encrypt the transmission information. In the specific implementation process of XOR cross operation,different rules of operation will be carried out according to the Hamming weight of encrypted information,so as to enhance the security of the algorithm. The XOR cross operation is implemented by bit operation,which can greatly reduce the overall calculation amount of the algorithm which can reach the ultra-lightweight level. The theoretical analysis of the security and performance of the proposed algorithm and other different types of ownership transfer algorithm can show that the proposed algorithm has the requirements of promotion. At the same time,the simulation under the same environment shows that the proposed algorithm has better security performance under the condition of reducing the computing time cost.

Key words:RFID system;electronic tag ownership;ownership transfer algorithm;backward security;ultra-lightweight

0 引 言

射频识别技术近些年伴随云计算、大数据、物联网等新技术的产生而得到进一步发展[1-2]。一个经典的 RFID 系统至少包含电子标签、读卡器、数据库三部分,电子标签在使用过程中,电子标签拥有者可能经常发生变化,拥有者发生变化之后,之前用户在电子标签里存放的隐私信息对当前用户来说应该是无权限访问之前用户存放的隐私信息[3-5]。为确保标签中隐私信息的安全,所有权转移协议是当前的热点研究方向。

文献[6]中 STATIO 等人首次提出标签所有权转移协议,并在该文献中设计一个所有权协议,协议引入可信第三方参与消息交换,具备一定安全性及一定价值意义。文献[7]中作者针对文献[6]的协议进行安全分析,指出该协议无法保证标签原所有者隐私信息的安全性,同时协议因缺少存放前后两次会话密钥,无法抗攻击者发起的去同步化攻击。文献[8]利用可信第三方设计一个协议,协议虽基于对称加密算法对隐私信息进行加密,但文献[9]指出文献[8]的协议存在攻击者可分析出下轮会话消息值可行性,即协议存在无法提供前向安全性的不足。文献[10]利用可信第

收稿日期:2020-12-23 **修回日期**:2021-04-23
基金项目:国家自然科学基金(61705060)
作者简介:谢海宝(1981-),男,高级工程师,研究方向为电子政务、信息安全、数据管理。

三方,同时结合哈希函数给出一个协议,但文献[11]指出文献[10]的协议无法保障用户后向隐私安全性,同时加密算法的选择使得协议推广受到局限性。文献[12]给出一个改进的协议,并对协议进行分析,得出协议仍无法提供去同步化攻击安全性。文献[13]给出的协议,虽是采用优化后的 RABIN 算法对信息进行加密,对优化后的 RABIN 算法实则还是模运算,使得计算量较大,同时文献[13]的协议设计过程中步骤计算冗余,增加了标签端计算量。

鉴于较多协议存在计算量大或无法提供相对应的安全需求等不足,文中给出一个超轻量级的所有权协议。先自定义设计一个创新型的加密算法,即异或交叉运算,将在下一章节给出该加密算法详细设计过程。结合算法实现描述,可以知晓算法基于位运算实现,能够降低计算量,使得设计协议能够使用在计算受限制的标签中。协议中引入标志位 STATUS 信息,将根据该信息量得知标签归属者,具有唯一性。将文中算法与其他算法在相同环境下进行仿真实验,仿真数据表明文中算法能够弥补其他算法存在的安全不足之处,同时在大规模电子标签信息交互时,文中算法在计算时间开销角度具备较大的优势,计算时间复杂度要少于其他算法。

1　超轻量级算法

1.1　异或交叉运算定义

异或交叉运算(exclusive or cross operation,ECO(X,Y))按如下方式实现:

(1) X、Y、Z、T 都表示二进制序列,长度都为 L 位;

(2)Wt(X)、Wt(Y)分别表示二进制序列 X、Y 的汉明重量;

(3)Px、Py 分别表示指向二进制序列 X、Y 的指针;

(4)当 Wt(X)≥Wt(Y)时,对二进制序列 X、Y 分别同时从第一位开始遍历,当指针 Px 指向二进制序列 X 的第 i 位 Xi 时,指针 Py 同时指向二进制序列 Y 的第 i 位 Yi,将 Xi 和 Yi 数值进行加法运算,结果为偶数,则 Xi 和 Yi 进行异或运算,并将运算结果放置于二进制序列 Z 的第 i 位上,得到 Zi;否则,将 Xi 放置于二进制序列 Z 的第 i 位上,得到 Zi;

(5)当 Wt(X)<Wt(Y)时,对二进制序列 X、Y 分别同时从第一位开始遍历,当指针 Px 指向二进制序列 X 的第 i 位 Xi 时,指针 Py 同时指向二进制序列 Y 的第 i 位 Yi,将 Xi 和 Yi 数值进行加法运算,结果为偶数,则 Xi 和 Yi 进行异或运算,并将运算结果放置于二进制序列 Z 的第 i 位上,得到 Zi;否则,将 Yi 放置于二进制序列 Z 的第 i 位上,得到 Zi。最后再将 Zi 逆序放置可得到二进制序列 T。

通过两个例子对上述异或交叉运算进行解释。取值 L=12 位,X=001011100110,Y=010000100001,则可以得到 Wt(X)=6、Wt(Y)=3,满足 Wt(X)≥Wt(Y)条件,按照(4)中操作所得到异或交叉运算的结果为 ECO(X,Y)=Z=001011000110。具体过程见图 1。

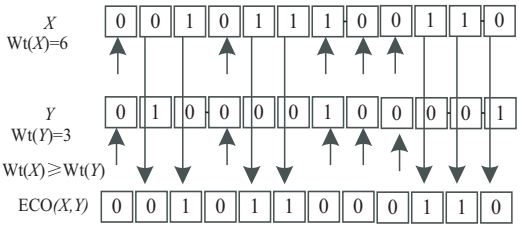

图 1　ECO(X,Y) Wt(X)≥Wt(Y)

再次取值 L=12 位,X=101000000101,Y=110101011110,则可以得到 Wt(X)=4、Wt(Y)=8,满足 Wt(X)<Wt(Y)条件,按照(5)中操作所得到异或交叉运算的结果为 Z=010101011010,ECO(X,Y)=T=010110101010。具体过程见图 2。

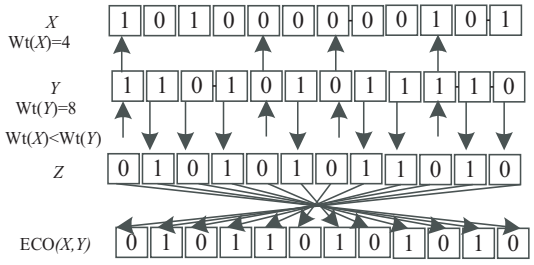

图 2　ECO(X,Y) Wt(X)<Wt(Y)

异或交叉运算破解的难度在于:其一,参与加密运算的两个参数信息攻击者不知晓,则无法进行后续的破解操作;其二,即便是攻击者可以获取部分参与加密的参数信息,但攻击者仍无法具体获悉两个参数汉明重量具体数值为多少,则攻击者不会知晓按照哪种方式进行交叉异或运算。因此,基于上述分析,新设计的异或交叉运算可以提供较好的安全需求,确保加密参数信息的安全性。同时,异或交叉运算在按照上述定义实现过程中,是基于位运算实现的,可以使得加密算法的计算量得到大幅度降低,从而使得算法可以得到超轻量级的级别,能够适用于低成本的 RFID 系统标签中。

1.2　算法符号含义

SN 表示标签新所有者;

SO 表示标签原所有者;

T 表示电子标签;

IDL 表示 T 标识符左半边;

IDR 表示 T 标识符右半边;

STATUS 表示 T 所有权归属标志位,当 STATUS = 0 时,表示所有权归属者为 SO,当 STATUS = 1 时,表示所有权归属者为 SN;

a 表示 SO 产生的随机数;

b 表示 T 产生的随机数;

c 表示 SN 产生的随机数;

K 表示 SO 与 T 之间共享密钥;

KO 表示 SO 与 T 之间当前共享密钥;

KO1 表示 SO 与 T 之间上轮共享密钥;

KT 表示 SN 与 T 之间共享密钥;

REQ 表示请求命令;

ACK 表示确定命令;

⊕表示异或运算;

&表示与运算;

ECO(X , Y)表示异或交叉运算。

1.3 算法具体设计

类似其他算法[14-16],做出如下假设规定:SN 与 SO 之间通信安全,SN 与 T 之间通信存在隐患,SO 与 T 之间通信同样存在隐患。文中超轻量级协议示意图见图 3。

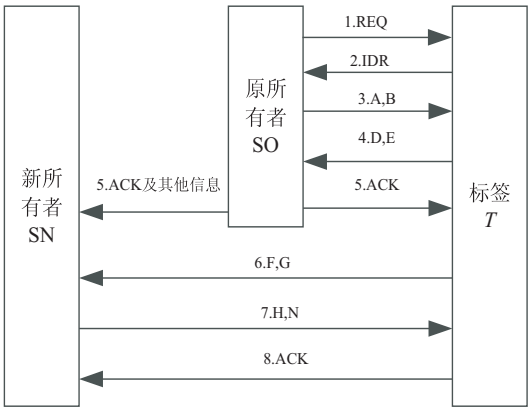

图 3 所有权转移算法实现过程

文中设计算法具体步骤如下:

STEP 1

由 SO 向 T 发送 REQ 请求命令开启所有权转移算法。

STEP 2

T 接到消息,查阅归属权标志位 STATUS 值,当前 STATUS 值为 0,表示当前所有权归属于 SO,因此 T 将 IDR 发送给 SO 以作为响应。

STEP 3

SO 接到消息,在数据库中查询是否存在与 IDR 相等的值,未找到,SO 对 T 验证失败,算法停止。找到,SO 立刻生成随机数 a ,接着分别计算会话消息 A 、B ,最后将 A 、B 传送给 T 。

其中 $A = a \oplus \mathrm{IDL}$、$B = \mathrm{ECO}(a, \mathrm{IDL})$。

STEP 4

T 接到消息,对 A 进行变形处理得到 $a' = A \oplus \mathrm{IDL}$,将 a' 再结合 IDL 进行相同运算法则计算得到 B' ,再对比 B' 与 B 。$B' \neq B$,算法停止。$B' = B$,表明 $a' = a$,且 T 验证 SO 通过, T 马上生成随机数 b ,再分别计算 D 、E 消息,最后将 D 、E 发送给 SO。

其中 $a' = A \oplus \mathrm{IDL}$、$B' = \mathrm{ECO}(a', \mathrm{IDL}) = \mathrm{ECO}(A \oplus \mathrm{IDL}, \mathrm{IDL})$、$D = b \oplus K$ 、$E = \mathrm{ECO}(b, a)$ 。

STEP 5

SO 接到消息,对 D 进行变形处理得到 $b' = D \oplus \mathrm{KO}$,将 b' 再结合 KO 进行相同运算法则计算得到 E' ,再对比 E' 与 E 。

$E' \neq E$,则 SO 将用 KO1 替换 KO 再次计算得到 E'' ,并再次对比 E'' 与 E。仍不等,算法停止;若 $E'' = E$,表明 SO 对 T 验证通过,接着 SO 将向 T 发送 ACK 消息,告知 T 接下来可以与 SN 之间进行会话,同时 SO 向 SN 发送 T 相关信息及 ACK 消息,告知 SN 做好与 T 进行会话的准备。

$E' = E$,表明 SO 对 T 验证通过,接着 SO 将向 T 发送 ACK 消息,告知 T 接下来可以与 SN 之间进行会话,同时 SO 向 SN 发送 T 相关信息及 ACK 消息,告知 SN 做好与 T 进行会话的准备。

其中 $b' = D \oplus \mathrm{KO}$、$E' = \mathrm{ECO}(b', a) = \mathrm{ECO}(D \oplus \mathrm{KO}, a)$、$E'' = \mathrm{ECO}(b', a) = \mathrm{ECO}(D \oplus \mathrm{KO1}, a)$。

算法实现过程中,可能受到外界干扰或攻击者的蓄意破坏,使得算法中 T 与新旧所有者间短暂失去一致性,因此需要通过该步骤再次实现两者间的一致性。SO 首先用 KO 验证,如果验证失败,此时有可能是会话实体两端短暂失去一致性,则 SO 将立刻用 KO1 替换 KO 再次发起验证,再次验证通过,则就可以恢复二者之间的一致性。

STEP 6

T 接到消息, T 开始计算 F 、G 消息,并向 SN 发送 F 、G 。

其中 $F = b \oplus \mathrm{IDL}$、$G = \mathrm{ECO}(b, \mathrm{KT})$。

STEP 7

SN 接到消息,对 F 进行变形处理得到 $b' = F \oplus \mathrm{IDL}$,将 b' 再结合 KT 根据相同运算法则计算得到 G' ,再对比 G' 与 G 。$G' \neq G$,算法停止。$G' = G$,表明 $b' = b$,且 SN 验证 T 通过,SN 马上生成随机数 c ,再分别计算 H 、N 消息,最后将 H 、N 发送给 T 。

其中 $b' = F \oplus \mathrm{IDL}$、$G' = \mathrm{ECO}(b', \mathrm{KT}) = \mathrm{ECO}(F \oplus \mathrm{IDL}, \mathrm{KT})$、$H = c \oplus (b \& \mathrm{IDL})$、$N = \mathrm{ECO}(\mathrm{KT}, c)$。

STEP 8

T 接到消息,对 H 进行变形处理得到 $c' = H \oplus (b \& \mathrm{IDL})$,将 c' 再结合 KT 根据相同运算法则计算得

到 N',再对比 N' 与 N。$N' \neq N$,算法停止。$N' = N$,表明 $c' = c$,且 T 验证 SN 通过,T 将所有权归属标志位 STATUS 值由 0 置为 1,表明 T 所有权发生变更,变更后 T 所有权归属者变为 SN 所有,最后 T 向 SN 发送 ACK 命令。

其中 $c' = H \oplus (b\&IDL)$、$N' = ECO(KT, c') = ECO(KT, (H \oplus (b\&IDL)))$。

其中 T 一端的所有权归属标志位 STATUS 的值,攻击者是无法通过物理手段修改的。当且仅当,只有通过上述方式正确通过 T 的验证之后,T 一端才会进行对所有权归属标志位 STATUS 的值的变动修改,从而可以保证 T 归属权的归属者唯一性。

STEP 9

SN 接到消息,看到 ACK 命令,SN 得知当前自己已获取 T 的所有权归属权限。

文中算法主要的创新点或优势在于:其一,给出一种新的信息加密方式,即异或交叉运算;其二,对于新的信息加密方式,不仅给出详细定义及实现步骤,同时结合具体实例进行分析;其三,所有信息全部采用密文方式发送,即信息先加密再发送,使得攻击者难以破解;其四,摒弃冗余的计算步骤,简化算法实现步骤,提高算法效率。

2　算法安全性分析

(1)所有权唯一性。

需确保不论何时标签所有权归属者必须具备唯一性,不能出现某个时刻存在有两个或两个以上所有权归属者。文中算法设计过程中引入归属权标志位 STATUS,依据 STATUS 值来确定标签当前归属者。攻击者无法修改标签端 STATUS 值,标签端想修改 STATUS 值需通过若干轮会话验证,而攻击者无法通过验证,因此算法具备所有权唯一性要求。

(2)目标标签。

某用户可能某个时刻拥有多个标签的所有权限,当某标签所有权需进行转移时,要确保待转移的标签即为目标标签。文中协议前面几个步骤便是原所有者 SO 与标签 T 之间的相互认证过程,当且仅当两者相互认证都通过,才会进行 T 与 SN 之间的消息交换,从而可以确保待转移的标签即为目标标签。

(3)假冒攻击。

系统整个会话过程中,任何一个会话实体都可能被攻击者假冒,从而发起假冒攻击。文中算法在 SN 与 T 之间、SO 与 T 之间进行消息交互时,先对消息来源方进行验证,验证失败,算法就停止,只有验证通过,才会进行后续操作,因此攻击者发起的假冒攻击肯定失败。

(4)去同步化攻击。

在 SO 与 T 交换消息的过程中,为抵抗攻击者发起的去同步化攻击,在 SO 端特地存放有当前以及上轮会话过程用到的共享密钥信息。SO 首先用当前密钥发起对 T 的验证,验证通过,则进行后续操作;验证失败,SO 在采用上轮会话密钥再次发起对 T 的验证,通过前后两次验证,可以抵抗攻击者发起的去同步化攻击。

(5)后向安全性。

攻击者通过某种手段获取整个会话消息,通过对获取的消息进行分析,获取之前某轮会话中的隐私信息,从而造成用户隐私信息泄露。文中算法为确保攻击者无法分析出之前会话隐私信息,加密过程中混入随机数,随机数前后两次值不同,攻击者在不知晓上轮及本轮随机数情况下,攻击者根本无法分析出之前加密隐私信息,因此算法具备后向安全性。

(6)前向安全性。

攻击者通过某些手段获取当前会话消息,企图对获取消息进行分析,从而预测下一次会话消息,并提前计算好下轮会话消息,通过一方认证。文中算法通过加密消息过程中混入随机数的方式来抵抗攻击者的攻击,因混入随机数,可以使得每轮会话过程中消息具备新鲜性,即每轮消息值不同,因随机数是随机产生,无规律性,因此攻击者无法提前预测下轮会话消息值,从而算法具备前向安全性。

(7)穷举攻击。

穷举攻击也可以称之为暴力破解攻击,即攻击者采用超级计算机对获取的密文进行穷举的方式穷举出所有可能的情况,从而破解出隐私信息。穷举攻击需要考虑成本开销,同时也需要考虑时间开销,不论是成本开销,还是时间开销,只要其中任意一个开销过大,则攻击者采用穷举攻击就代价过大,得不偿失。

文中算法一个完整通信过程被攻击者监听,则攻击者可以获取该通信过程中所有会话消息。这里选择消息 $A = a \oplus IDL$、$B = ECO(a, IDL)$ 为例进行穷举攻击分析。攻击者可以对消息 A 进行变形,然后带入消息 B 中,可得到 $B = ECO(A \oplus IDL, IDL)$,在变形处理之后的 B 中,对于攻击者来说,看似好像只有 IDL 一个参量信息不知晓,攻击者以为可以穷举出 IDL 的值,但攻击者至少还有两个参量不知晓。其中一个是 IDL 参量自身携带的汉明重量值;另一个是 $A \oplus IDL$ 运算结果自身携带的汉明重量值。攻击者不知晓上述两个参数值,则无法在加密过程中涉及到如何进行异或运算或交叉运算,则攻击者穷举失败。

综上,攻击者无法穷举出有用隐私信息,故文中算法可抵抗攻击者发起的穷举攻击,确保信息的安全。

将文中算法与其他部分经典算法进行安全性对比,对比分析结果见表 1。

表 1 算法间安全性对比

攻击类型	文献[6]	文献[8]	文献[10]	文献[12]	文中算法
唯一性	√	√	√	√	√
目标标签	√	√	√	√	√
假冒攻击	√	√	√	√	√
异步攻击	×	√	√	×	√
前向安全	√	×	√	√	√
后向安全	√	√	×	√	√
穷举攻击	√	√	√	√	√

说明:表 1 中,√符号表示可以抵抗该种类型的攻击方式,×符号表示无法抵抗该种类型的攻击方式。

3 算法性能分析

从一轮完整会话通信量、标签端计算量对多个算法进行对比分析,见表 2。

表 2 算法间性能对比

算法	计算量	存储空间
文献[7]	6Ha+5Hd+1Hf	10 L +1La
文献[12]	7Ha+3He+2Hf	10 L +1La
文献[13]	6Ha+5Hc+1Hf	11 L +1La
文中算法	5Ha+4Hb+1Hf	10 L +4La

针对表 2 中出现的符号给出下面的含义说明:Ha 表示位运算(比如异或运算)的计算量大小,Hb 表示异或交叉运算的计算量大小,Hc 表示模运算的计算量大小,Hd 表示哈希函数的计算量大小,He 表示物理不可克隆函数的计算量大小,Hf 表示产生随机数的计算量大小。L 表示会话消息的长度,La 表示会话过程中相关命令长度(比如 REQ 命令等)。

文中算法一轮完整会话消息包含 IDR、A 、B 、D 、E 、F 、G 、H 、N 以及 SO 向 SN 发送的内容同 10L ;另外还包含一个 REQ 命令、三个 ACK 命令,共计 4La,因此文中算法一个完整会话的通信量为 10L +4La。

标签端计算量由来:计算 a' 过程中第一次用到 Ha、计算消息 D 过程中第二次用到 Ha、计算消息 F 过程中第三次用到 Ha、计算 c' 过程中第四次、第五次用到 Ha(其中一次是按位异或运算,另一次是按位与运算),共计用到五次 Ha 运算。计算 B' 过程中第一次用到 Hb、计算消息 E 过程中第二次用到 Hb、计算消息 G 过程中第三次用到 Hb、计算 N' 过程中第四次用到 Hb,因此共计用到四次 Hb 运算。算法在整个过程中 T 需要产生一个随机数 b ,因此需要用到一次 Hf 运算。基于上述,文中算法标签一端总计算量为 5Ha+4Hb+Hf。

从表 2 中可以看出,从通信量角度出发,文中算法与其他算法大致相当;从标签端计算量角度出发,文中算法具有较大的改进,原因在于文中算法采用超轻量级自定义的加密算法,而没有采用传统的类似哈希函数、模运算等加密算法,同时文中算法可以弥补其他算法在安全性方面的不足。

4 算法仿真实验

文中选择后台数据库搜索特定标签成功所花费时间指标进行性能分析。好的加密算法,除了会话实体计算量减少之外,也会带来后台数据库对标签搜索时间的降低。

进行仿真实验相关的实验环境如下:电脑选择惠普笔记本、2013 年 9 月购买、I 5 处理器、内存 2 GB、硬盘 500 GB;以 C 语言作为仿真实验过程中部分算法编程实现的语言;选择小型数据库 MySQL 用来存放仿真实验过程中产生的相关数据;用 MATLAB 软件作为仿真实验用到的仿真平台。

系统在一个时间段内会对多个标签进行会话,单个标签与系统进行会话时,标签被搜索成功的时间长度会存在一定的差别。为减少误差,提升仿真实验的准确性,仿真实验时,假定系统中共有 6 000 个特定标签,依次对每组不同数量(1 000 个、2 000 个、3 000 个、4 000 个、5 000 个、6 000 个)的标签进行 200 次搜索,记录每一次搜索成功时间值,并求取平均值作为最终的仿真实验结果。

将文中算法与文献[7,12-13]中的算法在相同的仿真实验环境下进行仿真实验,绘制出如图 4 所示的仿真结果。

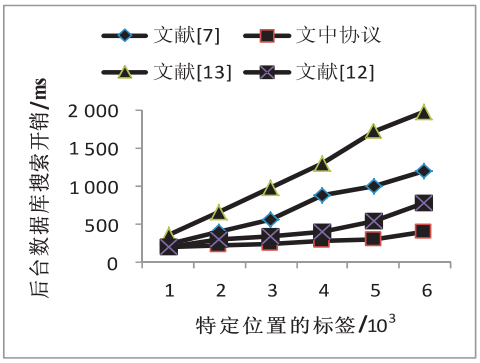

图 4 特定位置标签数量与搜索时间开销对比

从图 4 中可以看出,最开始标签数量不多的时候,后台数据库搜索时间相差不大。但随着搜索标签数量的不断增加,不同算法中后台数据库搜索标签成功的时间都在增加,但各算法增加的趋势并不相同。可以看出,文献[7,13]中算法随着标签数量增多,搜索标签时间几乎成线性增长;而文献[12]中算法搜索时间相对于上述算法搜索时间有所降低,但与文中算法的搜索时间相比,文中算法的搜索时间仍优于文献[12]

中算法的搜索时间。基于上述阐述,文中算法具备一定的推广使用价值及意义。

5　结束语

针对存放在电子标签中的隐私信息易泄露问题,文中设计一种超轻量级的算法。不同于其他算法,文中算法并未采用经典的哈希函数或 PUF 函数或伪随机函数对信息加密,而是采用一种自己设计的异或交叉运算算法实现信息加密;异或交叉运算将基于加密信息汉明重量不同进行不同方式的交叉操作,从而提升加密算法安全性,同时该运算设计思想基于位运算实现,使得文中算法整体计算时间开销得到一定程度的降低。通过理论及仿真实验将文中算法与其他算法进行对比分析,表明文中算法在安全性角度优于其他算法,能够弥补其他算法存在的安全缺陷,同时在性能上文中算法在对标签搜索时间开销上优于其他算法,降低了搜索时间开销。

参考文献:

[1] HONG X Y. Network security situation prediction based on grey relational analysis and support vector machine algorithm [J]. International Journal of Network Security,2020,22(1):177-182.

[2] SAFKHANI M, BAGHERI N, HOSSEINZADEH M, et al. On the security of an RFID based parking lot management system[J]. International Journal of Communication Systems, 2017,30(15):e3313.

[3] TANG Dan, WANG Yaqiang, YANG Haopeng. Array erasure codes with preset fault tolerance capability[J]. International Journal of Network Security,2018,20(1):193-200.

[4] CHIEN H Y, YANG C C, WU T C, et al. Two RFID-based solutions to enhance inpatient medication safety[J]. Journal of Medical Systems,2011,35(3):369-375.

[5] 刘道微,凌　捷,杨　昕. 一种改进的满足后向隐私的 RFID 认证协议[J]. 计算机科学,2016,43(8):128-130.

[6] SAITO J, IMAMOTO K, SAKURAI K. Reassignment scheme of an RFID tag's key for owner transfer[C]//Embedded and ubiquitous computing—EUC 2005 workshops. Nagasaki, Japan: Springer, 2005:1303-1312.

[7] OSAKA K, TAKAGI T, YAMAZAKI K, et al. An efficient and secure RFID security method with ownership transfer [M]//Computational intelligence and security. Guangzhou, China: Springer, 2008:778-787.

[8] ZHOU W, YOON E J, PIRAMUTHU S. Simultaneous multi-level RFID tag ownership & transfer in health care environments[J]. Decision Support Systems, 2012, 54(1):98-108.

[9] RAY B R, ABAWAJY J, CHOWDHURY M, et al. Universal and secure object ownership transfer protocol for the Internet of Things[J]. Future Generation Computer Systems, 2018, 78:838-849.

[10] ZUO Y. Changing hands together: a secure group ownership transfer protocol for RFID tags [C]//Proceedings of the 2010 43rd Hawaii international conference on system sciences. Hawaii: IEEE, 2010:1-10.

[11] LIANG W, XIE S, LONG J, et al. A double PUF-based RFID identity authentication protocol in service-centric Internet of Things environments [J]. Information Sciences, 2019,503:129-147.

[12] XIE R, JIAN B Y, LIU D W. An improved ownership transfer for RFID protocol[J]. International Journal of Network Security, 2018, 20(1):149-156.

[13] 吴伟民,陈超雄,蓝炯江,等. 基于 Rabin 加密算法的 RFID 标签所有权转移协议[J]. 计算机应用研究,2017,34(5):1531-1535.

[14] ZHU F, LI P, XU H, et al. A lightweight RFID mutual authentication protocol with PUF[J]. Sensors, 2019, 19(13):2957-2978.

[15] WEI C H, HWANG M S, CHIN A Y H. A secure privacy and authentication protocol for passive RFID tags[J]. International Journal of Mobile Communications, 2017, 15(3):266-277.

[16] XIE R, LING R, LIU D W. Wireless key generation algorithm for RFID system based on bit operation[J]. International Journal of Network Security, 2018, 20(5):938-949.