基于自组合交叉函数的组标签共存证明算法

熊 永 平
(广州科技职业技术大学信息工程学院 广东 广州 510550)

摘 要 针对现有的标签共存证明算法仅能证明单标签组共存缺陷,提出一种可证明多标签组共存证明算法。自组合交叉函数设计过程中充分利用自身加密信息携带的汉明权量,在提升安全的同时,也可减少参数的引入;算法采用先验证再操作机制,能够有效抵抗假冒等攻击。从安全及形式化角度分析算法,算法具备较高的安全性能,能够克服常见攻击;同时仿真实验数据表明,算法具备可观的时间复杂度。

关键词 物联网 射频识别技术 组标签 自组合交叉函数 汉明权量

中图分类号 TP393.08 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.05.048

GROUP TAG COEXISTENCE PROOF ALGORITHM BASED ON SELF-COMBINING CROSS FUNCTION

Xiong Yongping
(*School of Information Engineering, Guangzhou Vocational University of Science and Technology, Guangzhou 510550, Guangdong, China*)

Abstract Aiming at the defect that the existing tag coexistence proof algorithms can only prove the coexistence of single tag group, this paper proposes a multi tag group coexistence proof algorithm. In the design process of self-combining cross function, the Hamming weight of self encrypted information was fully used, which could improve the security and reduce the introduction of parameters. The algorithm adopted the mechanism of verification before operation, which could effectively resist attacks such as counterfeiting. From the perspective of security and formalization, the algorithm has high security performance and can overcome common attacks. The simulation results show that the algorithm has appreciable time complexity.

Keywords Internet of things Radio frequency identification (RFID) technology Group tag Self-combining cross Hamming weight

0 引 言

射频识别技术中识别装置与特定物品间不需要直接接触,识别装置即可读出特定物品中存放的信息,鉴于其便利性,射频识别技术现已被运用在各个领域中,比如一卡通系统、门禁系统等[1-2]。

进入新世纪,随着不同新技术产生及运用,射频识别技术与其他新技术相融合使用,得到了更为广泛的推广发展空间。之前只需要证明单个特定物品存在的需求,已无法满足当代各个领域的复杂要求[3-4]。例如:患者去医院看病,医生针对患者病情,给患者开的药品,患者不仅需要拿到该药品,同时还需要获取该药品相对应的使用说明书,即药品、药品相对应的使用说明书两者需时刻共存[5]。组标签共存证明算法即可解决上述问题。

根据验证装置对特定物品共存验证方式不同,可将组标签共存证明算法分为两大类,即链接式组标签共存证明算法、广播式组标签共存证明算法[6]。链接式组标签共存证明算法是在证明多个标签共存的时候,验证装置先与第一个标签进行通信,待收到第一个标签响应后,验证装置再与第二个标签进行通信,待收

收稿日期:2021-01-07。广东省教育部产学研合作专项基金项目-山区乡镇工艺品企业信息服务平台建设(2008B090500266)。
熊永平,讲师,主研领域:信息安全,计算机网络体系结构,软件工程。

到第二个标签响应后,验证装置再与第三个标签进行通信,按照此方式进行下去,直到验证装置收到最后一个标签响应后,验证装置才会生成一个群组共存证明。广播式组标签共存证明算法是在证明多个标签共存的时候,验证装置是以广播的形式向所有标签发送信息,所有标签将同时响应验证装置,验证装置收集齐所有标签响应信息后将会生成一个群组共存证明[7-8]。

链接式组标签共存证明算法中存在的主要缺陷问题是,当标签数量过多时,验证装置逐一与标签进行通信,当验证装置与最后一个标签通信时,因通信时间已过去多时,之前的响应标签可能已处于休眠状态,则整个过程将失败。广播式组标签共存证明算法中存在的主要缺陷问题是,若同时响应验证装置的标签数量过大,标签之间将会产生碰撞,碰撞发生后,验证装置则无法接收到正确的响应消息,故需采用良好的标签防碰撞算法[9]。现已有不少专家学者提出不同方式的组标签共存证明算法,但鉴于各算法或多或少存在安全隐患,文中给出一个超轻量级的基于自组合交叉函数的组标签共存证明算法。

1　相关工作

国内外专家学者已提出不少组证明算法,文中将选取部分经典算法进行描述分析。

Juels 是最早提出组证明算法,并同时在文献[10]中设计出一个可以解决单标签组共存的证明算法,具备里程碑的意义。Saito 等[11]则同时指出 Juels 设计的组证明算法存在安全隐患,比如 Juels 设计的组证明算法无法抵抗第三方人员发动的重放攻击,在此基础上,文献[11]提出一种基于时间戳的组证明算法。

Piramuthu 对文献[11]中算法进行分析[12],发现该算法同样存在缺陷,比如第三方人员可以通过对电子标签发动有关下次时间戳的挑战,可以不断收集电子标签的响应消息,从而造成重放攻击。

文献[13]提出了每组存在一个具有一定计算能力的电子标签构思,具备一定的创新价值,但该算法主要存在易遭受第三方人员发起的 DoS 攻击,且无法提供前向安全需求。

文献[14]给出了一个轻量级的组证明算法,算法可以达到轻量级的级别,能够在大多数 RFID 系统中得到推广使用,但算法存在不足,比如:算法中部分重要随机数信息采用明文方式发送,易被第三方人员窃听获取,从而造成第三方人员可通过穷举方式穷举出部分有用隐私信息,进而发起假冒攻击。

Kang 等[15]设计了一个组证明算法,但算法主要存在前向安全缺陷。文献[16]中算法无法提供会话实体间双向认证,使得第三方人员可发起假冒攻击。文献[17]中算法问题在于电子标签加密过程中未引入随机数,第三方人员可对电子标签进行定位追踪,同时亦可发起重放攻击。文献[18]中算法只能提供读写器对电子标签的单向认证,使得第三方人员可伪造群组证明。文献[19]中算法部分重要信息以明文方式发送,第三方人员监听获取,再结合其他消息,可穷举出部分隐私信息,进而发起假冒攻击。

鉴于现有的大多数经典组证明算法或存在安全漏洞或存在无法证明多标签共存或存在计算量大等缺陷不足,文中设计出一种基于按位运算实现的超轻量级的组证明算法。该算法不仅可证明单标签组共存,亦可证明多标签组共存,具备更广的使用范围;算法采用一种创新的加密算法实现信息加密,即自组合交叉函数;自组合交叉函数因采用基于按位运算机制实现,可极大程度上降低电子标签端计算量,同时加密时依据加密信息自身汉明权重,可在减少参数引入的同时,减低存储空间,且增加第三方人员破解难度。

2　自组合交叉函数

自组合交叉函数定义如下:

(1) 定义 X、Y、Z 是长度为 L 位长的二进制字符串。

(2) 定义 $H(X)$ 为二进制字符串 X 的汉明权量、$H(Y)$ 为二进制字符串 Y 的汉明权量、ΔH 为二进制字符串 X 的汉明权量与二进制字符串 Y 的汉明权量差值的绝对值(即 $\Delta H = |H(X) - H(Y)|$)。

(3) 当满足 $H(X) \geqslant H(Y)$ 时,进行下面操作。如果 $\Delta H = |H(X) - H(Y)| < (L-2)$,先将二进制字符串 X、二进制字符串 Y 进行“异或”运算得到二进制字符串 Z;保持二进制字符串 Z 的第一位、最后一位不变动,从第二位开始进行左移动 ΔH 位,即可得到自组合交叉函数运算结果。如果 $\Delta H = |H(X) - H(Y)| \geqslant L-2$,先将二进制字符串 X、二进制字符串 Y 进行“异或”运算得到二进制字符串 Z;保持二进制字符串 Z 的第一位、最后一位不变动,从第二位开始进行左移动 $\Delta H/2$ 位(ΔH 除 2 为小数时,可按照“取整向零”方式得到整数),即可得到自组合交叉函数运算结果。

(4) 当满足 $H(X) < H(Y)$ 时,进行下面操作。如果 $\Delta H = |H(X) - H(Y)| < L-2$,先将二进制字符串 X、二进制字符串 Y 进行“异或”运算得到二进制字符串 Z;保持二进制字符串 Z 的第一位、最后一位不变

动,从第二位开始进行右移动 ΔH 位,即可得到自组合交叉函数运算结果。如果 $\Delta H = |H(X) - H(Y)| < L-2$,先将二进制字符串 X、二进制字符串 Y 进行“异或”运算得到二进制字符串 Z;保持二进制字符串 Z 的第一位、最后一位不变动,从第二位开始进行右移动 $\Delta H/2$ 位(ΔH 除 2 为小数时,可按照“取整向零”方式得到整数),即可得到自组合交叉函数运算结果。

(5) 自组合交叉函数文中约定统一用 $Scf(X,Y)$ 表示。

此处将结合下面例子进行讲解。取 $L=8$、$X=01101101$、$Y=10100001$,则可得到 $Z=X\oplus Y=11001100$、$H(X)=5$、$H(Y)=3$、$\Delta H=|H(X)-H(Y)|=2$。满足 $H(X)\geqslant H(Y)$,故自组合交叉函数运算结果为 $Scf(X,Y)=10110101$。如图 1 所示。

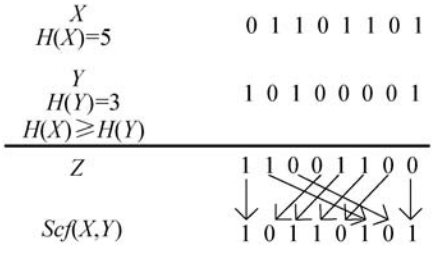

图 1 自组合交叉函数($H(X)\geqslant H(Y)$)

取 $L=8$、$X=10100100$、$Y=01101101$,则可得到 $Z=X\oplus Y=11001001$、$H(X)=3$、$H(Y)=5$、$\Delta H=|H(X)-H(Y)|=2$。满足 $H(X)<H(Y)$,故自组合交叉函数运算结果为 $Scf(X,Y)=10010011$。如图 2 所示。

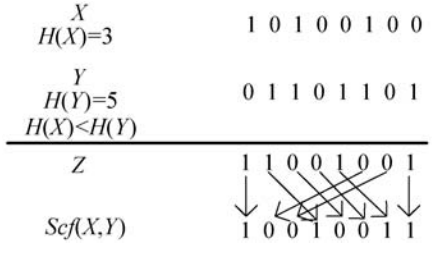

图 2 自组合交叉函数($H(X)<H(Y)$)

3 组标签证明算法

3.1 符号含义

对于文中设计的算法出现的符号给出下面的说明:

V:组标签验证者(具备充足的存储空间、强有力的计算及查询能力)。

R:读写器。

T_i:组标签中编号为 i 的标签。

K_{VT_i}:组标签验证者 V 与组标签中编号为 i 的标签 T_i 间共享秘密值。

TID_i:组标签中编号为 i 的标签 T_i 的假名。

K_{VR}:组标签验证者 V 与读写器 R 间共享秘密值。

ID_R:读写器 R 的标识符。

x:读写器 R 产生的随机数。

y:读写器 R 产生的随机数。

z_i:组标签中编号为 i 的标签 T_i 产生的随机数。

T_{ICKET} 组标签验证者 V 生成的授权票据。

3.2 算法步骤

算法在开始之前,各会话实体将会经过一个初始化过程,待初始化过程完成,组标签验证者 V 端储存的信息有 K_{VT_i}、TID_i、K_{VR}、ID_R;组标签中编号为 i 的标签 T_i 端储存的信息有 K_{VT_i}、TID_i;读写器 R 端储存的信息有 K_{VR}、ID_R。

文中设计的组标签证明算法过程如图 3 所示。

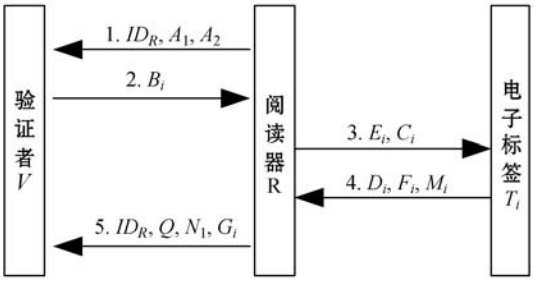

图 3 组标签证明算法示意图

结合图 3 可将文中设计算法步骤描述如下:

Step1 读写器 R 生成随机数 x,并依次计算会话消息 A_1、A_2,待会话消息 A_1、A_2 计算完成,将 ID_R、A_1、A_2 一并发送给组标签验证者 V。

$A_1=Scf(x\oplus ID_R,K_{VR})$、$A_2=x\oplus K_{VR}$。

将 ID_R 发送给组标签验证者 V 的目的是:能够使组标签验证者 V 快速验证当前会话的读写器是否合法,可缩短会话时间。

Step2 组标签验证者 V 查找自身存放的信息中是否存在与接收的 ID_R 相同的数据。

若不存在,算法即刻停止。若存在,组标签验证者 V 取出与 ID_R 相对应的 K_{VR} 数据,利用该数据可解密得到 $x'=A_2\oplus K_{VR}$,再将解密所得数据计算得到 A'_1,对比计算所得 A'_1 与收到的 A_1 大小关系。若关系为不等,算法即刻停止。反之,读写器 R 可通过组标签验证者 V 的验证,接着组标签验证者 V 生成授权票据 T_{ICKET},并计算会话消息 B_i,待会话消息 B_i 计算完成,组标签验证者 V 将 B_i 发送给读写器 R。

$$x'=A_2\oplus K_{VR},B_i=E_{K_{VR}}(T_{\text{ICKET}},TID_i)$$

$$A'_1=Scf(x'\oplus ID_R,K_{VR})=Scf(A_2\oplus K_{VR}\oplus ID_R,K_{VR})$$

组标签验证者 V 可能与多个读写器间有会话,因

此组标签验证者 V 可通过 ID_R 快速确定与之会话的读写器,从而缩短会话时间。

Step3　读写器 R 将根据对称加密算法对会话消息 B_i 进行解密,解密可得到授权票据 T_{ICKET}、组标签中编号为 i 的标签 T_i 的假名 TID_i;然后生成随机数 y,接着依次计算会话消息 E_i、C_i,待会话消息 E_i、C_i 计算完成,读写器 R 将 E_i、C_i 以广播的方式发送给组内的所有标签。

$E_i = y \oplus TID_i$、$C_i = Scf(y, y\&TID_i)$。

Step4　组内的标签收到信息对 E_i 进行变形处理可得到随机数 y',再将随机数 y' 结合 TID_i 计算得到一个 C'_i,对比计算所得 C'_i 与收到 C_i 大小关系。

若两者关系不等,算法即刻停止。

反之,读写器 R 通过组内标签的验证,组内标签 T_i 生成随机数 z_i,接着依次计算会话消息 D_i、F_i、M_i,待会话消息计算完成,组内标签 T_i 开始更新假名 TID_i,最后组内标签 T_i 将 D_i、F_i、M_i 发送给读写器 R。

$y' = E_i \oplus TID_i$、$TID_i = Scf(TID_i, K_{VT\_i})$、$C'_i = Scf(y', y'\&TID_i) = Scf(E_i \oplus TID_i, E_i \oplus TID_i \& TID_i)$、$F_i = y \oplus z_i$、$D_i = Scf(z_i, TID_i)$、$M_i = Scf(D_i, K_{VT\_i})$。

Step5　读写器 R 对收到的消息 F_i 进行变形处理可得到随机数 z'_i,结合随机数 z'_i 及解密 TID_i 计算得到一个 D'_i,对比计算所得 D'_i 与收到 D_i 大小关系。

若两者关系不等,算法即刻停止。

反之,组内标签通过读写器 R 验证,读写器 R 将依次接收 M_i,待接收全部 M_i 后,读写器 R 依次计算会话消息 Q、N_1、G_i,并最后将 Q、N_1、G_i、ID_R 发送给组标签验证者 V。

$z'_i = y \oplus F_i$、$D'_i = Scf(z'_i, TID_i) = Scf(y \oplus F_i, TID_i)$、$Q = Scf(K_{VR} \| TICKET \| M_1 \oplus M_2 \oplus \cdots \oplus M_n)$、$N_1 = E_{K_{VR}}(T_{\text{ICKET}})$、$G_i = K_{VR} \oplus z_i$。其中 n 表示组内标签的数量。

Step6　组标签验证者 V 查找自身存放的信息中是否存在与接收的 ID_R 相同的数据。

若不存在,算法即刻停止。若存在,组标签验证者 V 取出与 ID_R 相对应的 K_{VR} 数据,对会话消息 N_1 进行解密,将解密结果与自身之前产生的授权票据相比较。若结果不同,算法即刻停止;反之,读写器 R 通过组标签验证者 V 的验证,接着对会话消息 G_i 进行变形处理得到随机数 z'_i,由随机数 z'_i 及假名 TID_i 可计算得到 D'_i,再有 D'_i 及 K_{VT_i} 可计算得到 M'_i,接着由 M'_i、K_{VR} 及授权票据可计算得到 Q',最后对比计算得到 Q' 与收到的 Q 之间的大小关系。

如两者不等,算法即刻停止。

反之,读写器 R 通过组标签验证者 V 的验证,且可以说明组内所有标签同时存在,最后组标签验证者 V 开始更新信息 TID_i。

$z'_i = K_{VR} \oplus G_i$、$D'_i = Scf(z'_i, TID_i) = Scf(K_{VR} \oplus G_i, TID_i)$、$Q' = Scf(K_{VR} \| TICKET \| M'_1 \oplus M'_2 \oplus \cdots \oplus M'_n)$、$M'_i = Scf(D'_i, K_{VT\_i})$、$TID_i = Scf(TID_i, K_{VT\_i})$。

4　算法逻辑形式化推理证明

本节将采用基于 GNY 逻辑形式化对文中算法进行推理分析,有关 GNY 逻辑形式化分析更多规则可参见文献[20]。

(1) 形式化模型。

为便于该章节形式化分析推理,约定 V 表示验证者,R 表示读写器,T 表示电子标签。对文中算法进行抽象可得到:

Msg1:$R \rightarrow V: ID_R、A_1、A_2$

Msg2:$V \rightarrow R: B_i$

Msg3:$R \rightarrow T: C_i、E_i$

Msg4:$T \rightarrow R: D_i、F_i、M_i$

Msg5:$R \rightarrow V: ID_R、Q、N_1、G_i$

将上述形式化信息更进一步抽象得到:

Msg1:$V \lhd *ID_R、A_1、A_2 \sim\!\!\mapsto R \mid\equiv \#ID_R、A_1、A_2$

Msg2:$R \lhd *B_i \sim\!\!\mapsto V \mid\equiv \#B_i$

Msg3:$T \lhd *C_i、E_i \sim\!\!\mapsto R \mid\equiv \#C_i、E_i$

Msg4:$R \lhd *D_i、F_i、M_i \sim\!\!\mapsto T \mid\equiv \#D_i、F_i、M_i$

Msg5:$V \lhd *ID_R、Q、N_1、G_i \sim\!\!\mapsto R \mid\equiv \#ID_R、Q、N_1、G_i$

(2) 初始化假设。

文中算法具有下面初始化假设:

A1:$T \ni K_{VT\_i}$

A2:$T \ni TID_i$

A3:$V \ni K_{VT\_i}$

A4:$V \ni TID_i$

A5:$V \ni K_{VR}$

A6:$V \ni ID_R$

A7:$R \ni ID_R$

A8:$R \ni K_{VR}$

A9:$T \mid\equiv \#(z_j)$

A10:$R \mid\equiv \#(x)$

A11:$R \mid\equiv \#(y)$

A12:$V \mid\equiv V \xleftrightarrow{K_{VT\_i}} T$

A13:$V \mid\equiv V \xleftrightarrow{TID_i} T$

A14:$V \mid\equiv V \xleftrightarrow{Scf} T$

A15:$V \mid\equiv V \xleftrightarrow{ID_R} R$

A16:$V \mid\equiv V \xleftrightarrow{K_{VR}} R$

A17:$V|\equiv V \xleftrightarrow{Scf} R$

A18:$V|\equiv V \xleftrightarrow{E()} R$

A19:$T|\equiv T \xleftrightarrow{Scf} R$

A20:$R|\equiv R \xleftrightarrow{Scf} T$

A21:$T|\equiv T \xleftrightarrow{K_{VT\_i}} V$

A22:$T|\equiv T \xleftrightarrow{TID_i} V$

A23:$T|\equiv T \xleftrightarrow{Scf} V$

A24:$R|\equiv R \xleftrightarrow{ID_R} V$

A25:$R|\equiv R \xleftrightarrow{K_{VR}} V$

A26:$R|\equiv R \xleftrightarrow{Scf} V$

A27:$R|\equiv R \xleftrightarrow{E()} V$

初始化假设 A1、A2 是电子标签 T 所拥有的。

初始化假设 A3、A4、A5、A6 是验证者 V 所拥有的。

初始化假设 A7、A8 是读写器 R 所拥有的。

初始化假设 A9 是电子标签 T 对拥有信息新鲜性的相信。

初始化假设 A10、A11 是读写器 R 对拥有信息新鲜性的相信。

初始化假设 A12、A13、A14 是验证者 V 与电子标签 T 间彼此相信共享信息。

初始化假设 A15、A16、A17、A18 是验证者 V 与读写器 R 间彼此相信共享信息，

初始化假设 A19 是电子标签 T 与读写器 R 间彼此相信共享信息。

初始化假设 A20 是读写器 R 与电子标签 T 间彼此相信共享信息。

初始化假设 A21、A22、A23 是电子标签 T 与验证者 V 间彼此相信共享信息。

初始化假设 A24、A25、A26、A27 是读写器 R 与验证者 V 间彼此相信共享信息。

(3) 证明目标。

文中协议需要证明的形式化目标有如下：

G1:$V|\equiv R|\sim \#(A_1)$

G2:$V|\equiv R|\sim \#(A_2)$

G3:$R|\equiv V|\sim \#(B_i)$

G4:$T|\equiv R|\sim \#(C_i)$

G5:$T|\equiv R|\sim \#(E_i)$

G6:$R|\equiv T|\sim \#(D_i)$

G7:$R|\equiv T|\sim \#(F_i)$

G8:$R|\equiv T|\sim \#(M_i)$

G9:$V|\equiv R|\sim \#(Q)$

G10:$V|\equiv R|\sim \#(N_1)$

G11:$V|\equiv R|\sim \#(G_i)$

(4) 推理证明。

文中算法进行抽象化抽离之后，需要推理证明的目标一共有 11 个。鉴于文中篇幅有限，加上 11 个证明目标的推理分析过程大致相似，故文中仅选择证明目标 G1:$V|\equiv R|\sim \#(A_1)$ 为例进行展开分析，其他证明目标推理分析过程这里不再阐述。有关目标 G1:$V|\equiv R|\sim \#(A_1)$，具体推理分析过程如下阐述：

首先，因为初始化假设 $A10:R|\equiv \#(x)$ 和新鲜性规则 F1:$\dfrac{P|\equiv \#(X)}{P|\equiv \#(X,Y),P|\equiv \#(F(X))}$ 可得知：$V|\equiv \#(x、ID_R、K_{VR})$。

在 Msg1 中，$R \lhd *x$，即 $R \ni x$，同时结合初始化假设 A3、A4、A5、A6 和规则 P2 可得知：$V \ni (x、ID_R、K_{VR})$。

接着，由已推导出的 $V|\equiv \#(x、ID_R、K_{VR})$、$V \ni (x、ID_R、K_{VR})$，再根据新鲜性规则 F10:$\dfrac{P|\equiv \#(X),P \ni X}{P|\equiv \#(H(X,Y))}$ 可得知：$V|\equiv \#(A_1)$，即 $V|\equiv \#(Scf(x \oplus ID_R,K_{VR}))$。

最后，根据 Msg1、初始化假设 A15 和 A16 以及 A17、已推导出的 $V \ni (x、ID_R、K_{VR})$、已推导出的 $V|\equiv \#(A_1)$、消息解析规则 I3 可得到：$V|\equiv R|\sim (A_1)$，即 $V|\equiv R|\sim (Scf(x \oplus ID_R,K_{VR}))$。

由新鲜性的定义可推导出证明目标 G1:$V|\equiv R|\sim \#(A_1)$，即 G1:$V|\equiv R|\sim (Scf(x \oplus ID_R,K_{VR}))$。

5 算法安全性分析

本节将从假冒攻击、重放攻击、穷举攻击等角度展开分析文中算法的安全性。

(1) 前向安全。

前向安全性是要确保第三方人员无法从窃听的消息中逆推出上轮消息交换过程中用到的隐私信息。为了第三方人员分析出之前隐私信息，文中采用的方法是在消息加密时全部混入不同的随机数，比如 V 与 R 间消息混入随机数 x，这样就使得每次会话用到的随机数不同，则第三方人员就无法逆分析出之前用到的隐私信息，因每轮加密用到的随机数是随机产生而得，前后间无任何关联性。基于上述，文中算法可提供较好的前行安全性。

(2) 假冒攻击。

从理论上分析，第三方人员可以假冒成会话过程中任何一方会话实体，来与其他合法的会话实体间进行会话。文中鉴于篇幅有限因素，仅选择第三方人员假冒成读写器 R 为例进行展开分析。

当第三方人员伪装成读写器 R 与验证者 V 间进行会话交换消息时，第三方人员因自身无法获取 R 与

V 间共享的秘密值 K_{VR},使得第三方人员再进行消息 A_1、A_2 计算过程中,第三方人员只能随机选择一个量作为 K_{VR} 的数值进行计算。待验证者 V 收到消息后,验证者 V 只需要进行简单的验证,即可识别出消息来源方是第三方人员伪造的,算法停止。截止到算法停止时,第三方人员并未获取任何有用的隐私信息。基于上述,文中算法可以提供抵抗假冒攻击。

(3) 重放攻击。

第三方人员可以监听第 i 轮会话的完整过程,同时可获取该轮会话过程中所有会话消息。第三方人员可以在第 $i+1$ 轮会话开始前阻塞验证者 V 与读写器 R 或读写器 R 与电子标签间正常通信,然后第三方人员开始伪装成其中一个会话实体,重放监听获取的第 i 轮会话消息给其他会话实体,企图通过合法会话实体的验证,进而进行后续违法通信来获取隐私信息。

对于文中算法来说,第三方人员通过上述操作无法成功,即无法通过合法会话实体验证。原因在于,文中算法会话过程中,所有会话消息全部混入随机数,随机数每轮随机产生,根本不可能出现相同的情况,使得前后相邻的两轮会话用到的随机数截然不同,故第三方人员重放消息亦不会通过验证。基于上述,文中算法可以提供抵抗重放攻击。

(4) 双向认证。

对消息来源方的真伪性能够进行辨识,是算法需具备最基本的要求。

文中算法每步骤中都将会先对消息来源方进行验证,当且仅当验证成功,消息接收方才会进行后续操作。具体的分析见下:验证者 V 第一次通过 ID_R、A_1、A_2 发起对读写器 R 的验证,具体的验证过程可见算法 Step2;读写器 R 通过 B_i 发起对验证者 V 的验证,具体的验证说明可见算法 Step3;电子标签通过算法 Step4 完成对读写器 R 的验证,而读写器 R 则是通过算法 Step5 完成对电子标签的验证,最后 Step6 中则是验证者 V 同时验证读写器 R 及电子标签的合法性。基于上述,文中算法可以提供实现消息发送方真伪性的识别。

(5) 追踪攻击。

第三方人员可以持续监听会话过程,对会话过程中消息进行反复分析,企图确定追踪电子标签具体位置,对电子标签实施一些违法操作行为。文中算法为能够避免电子标签具体位置暴露,主要从三个方面进行采取措施:① 文中算法设计之时,未出现电子标签真实的标识符信息,而是用电子标签的假名替代真实的标识符参与消息计算及传递;② 即便是使用假名,亦存在安全隐患,因此文中算法在每轮会话完成后,假名也会进行更新,使得下轮出现的假名与相邻的上轮用到的假名不同;③ 电子标签所有发出的消息都是密文,且消息加密过程中加入随机数,使得前后轮会话消息存在巨大的差别,第三方人员无法分析出电子标签的具体位置。基于上述,文中算法可以提供抵抗追踪攻击。

(6) 穷举攻击。

第三方人员可通过窃听等手法获取正常的会话消息,并对会话消息进行穷举分析,以企图穷举出部分有用的隐私信息。通过对单个消息可成功,对多个消息亦可成功,但文中算法于第三方人员而言,不论哪种情况,都是无法成功的。

先对单个消息进行穷举攻击进行分析。这里仅选择消息 $A_1 = Scf(x \oplus ID_R, K_{VR})$ 为例展开分析,在消息 $A_1 = Scf(x \oplus ID_R, K_{VR})$ 中,第三方人员可以获悉已公开的加密算法、可以通过窃听获取 ID_R,但第三方人员无法获取秘密值 K_{VR}、随机数 x;当一个消息中有两个或两个以上参量第三方人员无法知晓时,则第三方人员便无法穷举出任何有用的隐私信息。

再对多个消息进行联合穷举攻击进行分析。这里仅选择消息 $A_1 = Scf(x \oplus ID_R, K_{VR})$、$A_2 = x \oplus K_{VR}$ 为例展开分析,第三方人员可以对消息 $A_2 = x \oplus K_{VR}$ 进行变形处理,并将变形处理之后的结果代入消息 $A_1 = Scf(x \oplus ID_R, K_{VR})$ 中,从而可以得到消息形式 $A'_1 = Scf(x' \oplus ID_R, K_{VR}) = Scf(A_2 \oplus K_{VR} \oplus ID_R, K_{VR})$;此时,在消息 $A'_1 = Scf(x' \oplus ID_R, K_{VR}) = Scf(A_2 \oplus K_{VR} \oplus ID_R, K_{VR})$ 中,第三方人员误以为只有秘密值 K_{VR} 一个参量不知晓,以为可以进行穷举攻击,但依据文中对自组合交叉函数的设计可得知,第三方人员其实也不知晓秘密值 K_{VR}、$A_2 \oplus K_{VR} \oplus ID_R$ 这两者汉明权重的具体数值,这样分析,其实第三方人员相当于有三个参数是不知晓,同理,第三方人员无法穷举出有用隐私信息。

基于上述,文中算法可以提供抵抗穷举攻击。

(7) 共存证明。

共存证明是一个组标签存在证明算法的必须实现要求。

文中算法将在 Step6 中实现标签组共存的证明,具体的分析如下:验证者 V 通过 ID_R 首先验证读写器 R 的真伪;待通过验证,验证者 V 会取出与 ID_R 相对应的 K_{VR} 值;为确保读写器 R 的真实性无误,验证者 V 将再次对消息 N_1 进行解密,以来再次验证读写器 R 真伪;读写器 R 再次通过验证,则验证者 V 对消息 G_i 进行变形处理,从而可以得到随机数 z_i;再由计算所得随机数 z_i,验证者 V 将开始依次计算得到 D_i;再由计算所得

D_i,验证者 V 将开始依次计算得到 M_i;最后验证 V 将计算所得所有 M_i、K_{VR}、T_{ICKET}按照相同运算法则计算得到一个 Q,并将计算得到 Q 与收到 Q 相比较。

上述计算过程中,但凡验证者只要有一处计算错误,则验证者 V 绝不可能计算得到正确的 Q;若验证者 V 无法通过计算得到正确的 Q,则最后一步的相比较过程,验证者 V 对所有标签的存在验证将失败。当且仅当,整个会话过程中无第三方人员的参与,所有会话均处于正常情况下,验证者 V 可正确计算 Q 的值,最后一步相比较可正确无误,验证者 V 对所有电子标签共存验证证明成功。

基于上述,文中算法可以提供实现正确的共存证明。

文中算法与其他算法的安全性对比结果如表 1 所示。

表 1 不同算法间安全性对比分析

攻击类型	文献[17]	文献[18]	文献[19]	文中算法
前向安全	√	√	√	√
假冒攻击	√	√	×	√
重放攻击	×	√	√	√
双向认证	√	×	√	√
追踪攻击	×	√	√	√
穷举攻击	√	√	×	√
共存证明	√	×	√	√

6 算法性能分析

将文中算法与其他算法进行性能方面的对比分析,选择电子标签端的计算量、会话通信量、会话次数、电子标签端的存储量等角度分析,对比分析结果如表 2 所示。

表 2 不同算法间性能对比分析

对比算法	计算量	会话消息量	会话次数	存储量
文献[17]	*XOR*,*AND*,*HASH*	18*L*	9	3*L*
文献[18]	*XOR*,*PUF*	15*L*	7	2*L*
文献[19]	*PRNG*,*HASH*	19*L*	11	3*L*
本文算法	*XOR*,*Scf*( ),*E*( )	13*L*	5	2*L*

对表 2 中出现的部分符号所表示的含义给出如下解释说明:*XOR* 表示异或运算的计算量;*E*( )表示对称加解密算法的计算量;*PRNG* 表示伪随机函数的计算量;*HASH* 表示哈希函数的计算量;*AND* 表示与运算的计算量;*PUF* 表示物理不可克隆函数的计算量;*Scf*( )表示自组合交叉函数的计算量。*L* 表示每个参量的长度。

从计算量角度分析各算法,上述众多算法中,只有 *XOR*、*AND*、*Scf*( )、*E*( )属于超轻量级的加密算法,其中 *E*( )所表示的对称加解密算法也可采用按位运算实现,其他算法属于轻量级的加密算法。文中算法对信息加密时所选用的加密算法均是超轻量级的,因此,文中算法电子标签端的计算量要少于其他算法。

从会话消息量角度分析各算法,会话消息量是指在一个完整的会话过程中,所有会话实体间全部的会话消息数量。从表 2 中可以看出,文中算法一个完整的会话过程中会话量为 13*L*,其他算法的会话量均多于文中算法的会话量。

从会话次数角度分析各算法,文中算法仅需要 5 次会话即可实现各会话实体间验证,与文中算法会话次数最为相接近的是文献[18]算法,其他算法中会话次数也都多于文中算法会话次数。

从存储量角度分析各算法,文中算法仅需要在初始化阶段存放两个参数,因此电子标签端的存储量为 2*L*,除了文献[18]算法与文中算法存储量一样,其他算法电子标签端存储量均多于文中算法。

综合上述分析,文中算法虽在部分角度无法存在优势,但综合对比分析而言,在电子标签一端的计算量要优于其他算法,同时文中算法可以弥补其他算法存在的安全不足,整体考虑而言,具备推广使用价值。

7 算法仿真实验

文中进行仿真实验环境条件如下:同一台笔记本电脑,i5 处理器,Windows 10 操作系统,64 位,4 GB 内存,无线网络下连接互联网,C ++ 语言实现部分算法源代码程序编写,小型数据库 MySQL 来存放仿真实验数据,MATLAB 软件进行仿真平台。

考虑到会有偶然因素对仿真实验的准确性造成干扰,因此在进行仿真实验过程时,每个相同的状态下,进行仿真实验的次数不少于 500 次,并依次记录这 500 次仿真实验数据,取 500 次仿真实验的平均数据作为该状态下的最终仿真实验结果。仿真实验进行时,依次记录仿真实验的时间点为 100 s、200 s、300 s、400 s、500 s、600 s、700 s 时,不同算法面对相同环境下网络攻击,攻击成功的次数统计数据。对仿真实验数据进行整理,最终绘制出如图 4 所示的仿真实验结果图。

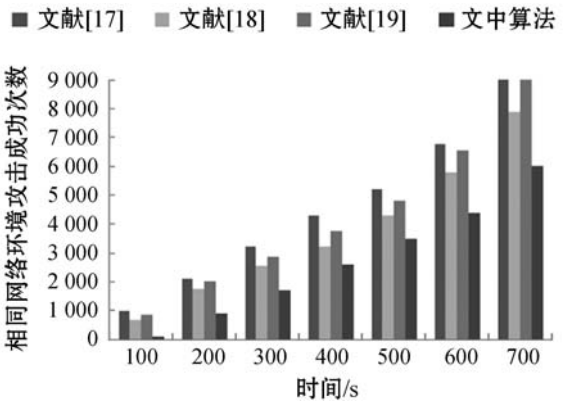

图 4　不同算法相同网络环境下攻击成功次数对比

结合图 4 对各算法安全性进行分析,横轴所表示的含义是仿真实验的时间点,依次为 100 s、200 s、300 s、400 s、500 s、600 s、700 s 时,具有相同的时间间隔;纵轴所表示的含义是不同算法面对相同网络环境下,在上述仿真实验的时间点攻击成功次数的统计数据。

可以看出,文中算法不论在任何一个时间点,面对相同网络环境下,第三方人员发起攻击时,攻击成功次数均是最少的。其他文献中的算法攻击成功数据则远远多于文中算法数据结果。更进一步分析可以发现,在最开始的 400 s 内,各算法在相同网络环境下,仿真实验数据结果间相差并不大,但随着仿真实验的时间越久,各算法被攻击成功的次数间差距逐渐明显。

综合上述阐述,文中算法与其他算法在面对相同网络环境时,面对第三方人员发起的不同类型的网络攻击,文中算法被攻击成功的次数最少,安全性能要优于其他算法。

8　结　语

文中在介绍近年来经典组证明共存算法的同时,指出其算法存在的各种不同方面的缺陷,提出一个超轻量级的基于自组合交叉函数的标签组证明算法。该算法即可对单标签组共存证明适用,亦可对多标签组共存证明适用;文中设计出一种创新的加密算法,自组合交叉函数基于超轻量级的按位运算实现,同时实现过程中充分且巧妙运用加密信息自身固有的汉明权重,在减少参量引入的同时,亦可实现较高的安全性。采用基于 GNY 逻辑,对算法进行严谨的形式化推理分析;对比各算法安全性,表明文中算法可提供抵抗假冒攻击、异步攻击等常见类型的安全威胁。仿真实验结果表明文中算法具备更好的计算时间开销,优于其他算法。

参　考　文　献

[1] Tang D, Wang Y Q, Yang H P. Array erasure codes with preset fault tolerance capability[J]. International Journal of Network Security,2018,20(1):193 – 200.

[2] Rahman F, Hoque M E, Ahamed S I. AnonPri: A secure anonymous private authentication protocol for RFID systems [J]. Information Sciences,2017,379(2):195 – 210.

[3] Tang F, Huang D. A BLS signature scheme from multilinearmaps[J]. International Journal of Network Security,2020, 22(5):728 – 735.

[4] 段艳萍. 轻量级 RFID 群组标签生成协议[J]. 控制工程, 2020,27(4):751 – 757.

[5] Zuo C. Defense of computer network viruses based on datamining technology[J]. International Journal of NetworkSecurity,2018,20(4):805 – 810.

[6] 石乐义,贾聪,宫剑,等. 基于共享秘密的伪随机散列函数 RFID 双向认证协议[J]. 电子与信息学报,2016,38(2): 361 – 366.

[7] Siqueira E C,Souza M J F,Souza S R D. A multi objective variable neighborhood search algorithm for solving the hybrid flow shop problem[J]. Electronic Notes in Discrete Mathematics,2018,66:87 – 94.

[8] Meena D K. Identification of cybercriminal by analysing the users profile[J]. International Journal of Network Security, 2018,20(4):738 – 745.

[9] 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 – 130,158.

[10] Juels A. "Yoking-proofs" for RFID tags[C]//2nd IEEE Annual Conference on Pervasive Computing and CommunicationWorkshops,2004:138 – 143.

[11] Saito J, Sakurai K. Grouping proof for RFID tags[C]//19th International Conference on Advanced Information Networking and Applications,2005:621 – 624.

[12] Piramuthu S. On existence proofs for multiple RFID tags [C]//IEEE International Conference on Pervasive Services, 2006:317 – 320.

[13] Ham H, Kim I, Song J. An efficient offline grouping proof protocol using multiple types of tags[C]//9th International-Conference on Ubiquitous Information Management and Communication,2015:94.

[14] 郭奕旻,李顺东,陈振华,等. 一种轻量级隐私保护的 RFID 群组证明协议[J]. 电子学报,2015,43(2):289 – 292.

[15] Kang HY. Analysis and improvement of ECC-based grouping-proof protocol for RFID[J]. International Journal of Control and Automation,2016,9(7):343 – 352.

(下转第 349 页)

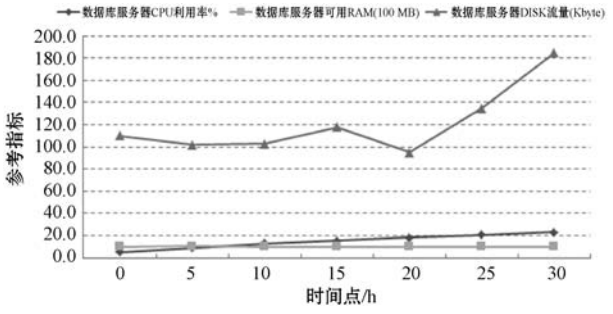

图 6　数据库服务器稳定性测试参数

从整体来看,C2TP 平台整体性能完全能够满足各项参数的要求,可以平稳运营在真实环境中。

5　结　语

C2TP 吸取了现有云培训技术的优点,尤其是在 ECS 弹性服务器方面,突破传统培训模式,为企业量身打造了与之相契合的云培训平台。针对企业私属性的特点及特色,科学地规划了与其需求相对应的培训功能模块,以积累知识、提升技能、岗前考核等为核心主导,实现企业闭环培训需求,与企业的持续发展相适应,提高从业人员的技能水平和对职业的满足感,为企业的生产与经营提供良好服务,从而不断提升企业的竞争力。今后的技术工作重点将集中在代码持续智能化集成方面,尤其是在性能监控方面。

参　考　文　献

[1] 闵丹. 支持云培训的教学资源管理平台设计与关键技术实现[D]. 北京:北京邮电大学,2019.

[2] Yu W, Kuang R, Xing R. Design and development of SCORM-based mobile learning system[C]//8th International Conference on Information Technology in Medicine and Education (ITME),2017:482 - 485.

[3] 李超,周泓. 学习管理系统综述和发展趋势展望[J]. 现代教育技术,2018,28(2):113 - 119.

[4] Liu Y, Li B, Niu J, et al. A Cloud-Based experiment platform for computer-based education[C]//2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing,2014:626 - 629.

[5] 黄乐辉,盛艳微,罗英. 基于云教育平台的移动学习模式研究[J]. 现代信息科技,2019,3(21):115 - 116,119.

[6] 刁兆勇,周建华. 大型企业标准化培训体系的构建与实施[J]. 中国标准化,2021(4):42 - 45.

[7] 塔娜. 基于云计算技术的大规模数据聚类分析[J]. 现代电子技术,2020,43(15):123 - 126.

[8] 贾琦. 云环境服务质量模型研究及应用[D]. 四川:电子科技大学,2016.

[9] Trabay D, Asem A, El-Henawy I, et al. A hybrid technique for evaluating the trust of cloud services[J]. International Journal of Information Technology,2021,13:687 - 695.

[10] 吴佩莉,张弢,张泉. 基于 SCORM 技术的多媒体课件统一播放框架与实现[J]. 计算机应用与软件,2019,36(5):108 - 111.

[11] 吴佩莉. 服务型云培训平台的闭环培训设计与实现[J]. 兰州文理学院学报(自然科学版),2020,34(3):88 - 92.

(上接第 318 页)

[19] Chen Q, Hu Q M, Huang J, et al. CA-RNN: Using context-aligned recurrent neural networks for modeling sentence similarity[C]//32nd AAAI Conference on Artificial Intelligence,2018:1232 - 1243.

[20] Quan X J, Kit C Y, Ge Y, et al. Short and sparse text topic modeling via self-aggregation[C]//24th International Joint Conference on Artificial Intelligence,2015:2270 - 2276.

[21] Zhao W Y, Jiang J, Weng J S, et al. Comparing twitter and traditional media using topic models[C]//33rd European Conference on Information Retrieval Research,2011:338 - 349.

[22] Řehůřek R, Petr Sojka. Software framework for topic modelling with large corpora[C]//Workshop on New Challenges for NLP Frameworks,2010: 45 - 50.

[23] New articles[EB/OL]. [2021 - 01 - 21]. https://dataverse.harvard.edu/dataset.xhtml? persistentId = doi:10.7910/DVN/GMFCTR.

[24] Vallejo-Huanga D, Morillo P, Ferri C. A dataset of attributes from papers of a machine learning conference[J]. Data in Brief,2019,24:103836.

(上接第 339 页)

[16] 尹毅峰,刘扬,徐明明. 一种具有可扩展性的 RFID 标签轻量级组证明协议[J]. 现代电子技术,2017,40(17):86 - 90.

[17] 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.

[18] Zhu F, Li P, Xu H, et al. A lightweight RFID mutual authenticationprotocolwithPUF[J]. Sensors, 2019, 19(13): 2957 - 2978.

[19] 史志才,王益涵,张晓梅,等. 一种具有隐私保护与前向安全的 RFID 组证明协议[J]. 计算机工程,2020,46(1):108 - 113.

[20] Liang W, Xie S Y, Long J, et al. A double PUF-based RFID identity authentication protocol in service-centricInternet of Things environments[J]. Information Sciences,2019,503:129 - 147.