计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(10):195−201 [doi: 10.15888/j.cnki.csa.008117]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

智能工厂中基于区块链的超轻量级认证方案①

谢海宝[1], 吕　磊[2]

[1](河南省市场监督管理局 信息中心, 郑州 450008)
[2](河南工业大学 信息科学与工程学院, 郑州 450008)
通讯作者: 谢海宝, E-mail: xihaba81@163.com

摘　要: “工业 4.0”的目标之一便是将传统工厂打造成智能工厂, 随着智能工厂的出现, 传统的网络安全无法满足企业及用户的需求. 针对智能工厂及其产品中隐私信息易泄露等安全隐患, 文中结合射频识别技术及区块链技术, 提出一种超轻量级的适用于智能工厂系统的认证方案. 方案将经典的射频识别技术与刚兴起的区块链技术相结合, 即可保证安全的情况下, 减少计算量; 方案基于区块链去中心化的机制实现用户所需安全需求, 基于射频识别中双向认证机制可抵抗常见类型攻击, 具备较高的安全性及计算优势.

关键词: 物联网; 区块链; 工业 4.0; 射频识别技术; 超轻量级; 认证方案

引用格式: 谢海宝,吕磊.智能工厂中基于区块链的超轻量级认证方案.计算机系统应用,2021,30(10):195–201. http://www.c-s-a.org.cn/1003-3254/8117.html

Ultra-Lightweight Authentication Scheme Based on Blockchain in Intelligent Factory

XIE Hai-Bao[1], LYU Lei[2]

[1](Information Center, Administration for Market Regulation of Henan Province, Zhengzhou 450008, China)
[2](College of Information Science and Technology, Henan University of Technology, Zhengzhou 450008, China)

Abstract: One of the goals of “Industry 4.0” is to build traditional factories into intelligent ones. With the emergence of intelligent factories, traditional network security cannot meet the needs of enterprises and users. In view of the security risks in intelligent factories and their products, such as proneness to privacy disclosure, this study proposes an ultra-lightweight authentication scheme suitable for intelligent factory systems by combining the RFID technology with the Blockchain technology. The scheme combines the classic RFID technology with the emerging Blockchain technology to reduce the amount of calculation under the condition of ensuring security. It meets the security needs of users with the mechanism of Blockchain decentralization. Based on the bidirectional authentication mechanism in RFID, it can resist common attacks and has high security and computing advantages.

Key words: Internet of Things (IoT); Blockchain; Industry 4.0; RFID technology; ultra-lightweight; authentication scheme

进入新世纪之后, 伴随着科技不断发展, 新技术也不断产生, 工业体系逐步进入“工业 4.0”时代[1,2]. 在“工业 4.0”时代, 每个国家都在发展建设智能工厂. 智能工厂的研究主要是将新产生的区块链、物联网等技术与传统的工业系统进行深层次的融合, 从而实现生产线能够以无线方式与互联网设备互联, 使得制造业可以呈现出数值化、网联化[3–5].

在智能工厂中采用到最多的技术当属射频识别技术, 因射频识别系统中电子标签具有体积小、成本低、寿命长等优势, 广泛使用在智能工厂中[6–8]. 但因

① 基金项目: 国家自然科学基金 (61705060)
Foundation item: National Natural Science Foundation of China (61705060)
收稿时间: 2020-12-25; 修改时间: 2021-01-25, 2021-02-03; 采用时间: 2021-02-08

电子标签受限于低成本要求, 使得电子标签一端计算能力非常有限, 无法进行传统的加解密运算, 要保证电子标签中存放的用户隐私信息[9,10], 需设计低计算量安全的协议方案.

文中章节按照如下方式安排: 第 1 节介绍文中研究内容已有的相关工作及优缺点; 第 2 节介绍文中设计的加密算法具体实现步骤; 第 3 节介绍文中方案实现方法; 第 4 节对文中设计方案的安全性展开讨论; 第 5 节采用基于 GNY 逻辑形式化分析推理证明文中方案; 第 6 节从计算时间复杂度等方面分析文中方案性能; 第 7 节总结全文工作.

1 相关工作

在 2016 年, 文献 [11] 中详细分析了区块链技术在不同行业中的应用, 并强调了区块链技术与物联网相结合将会产生重大变革及影响. 在 2017 年, 文献 [12] 中首次提出了将区块链作为物联网服务的思想. 同年, 文献 [13] 中设计一个将区块链运用在物联网场景的轻量级架构, 同时实现了网络的可扩展性等优势.

在 2018 年, 文献 [14] 中首次提出物联网链的概念, 为物联网资源的安全授权访问提供了一种端到端的解决机制, 实现了物联网设备的访问权限管理理念. 在 2019 年, 文献 [15] 中设计了一个基于区块链的 RFID 轻量级认证机制方案, 该机制方案能够抵抗常见类型的攻击, 同时具备较低的通信和计算成本, 但机制方案对标签一端提出一些其他要求, 使得机制方案推广性受到制约.

在 2020 年, 文献 [16] 中将射频识别技术与区块链技术相结合提出一个轻量级认证机制, 该认证机制具有一定的安全需求, 同时也满足低计算量的标准, 但协议在每轮通信后, 对于共享秘密值及假名的更新操作过于复杂, 使得整体计算时间复杂度较大.

文中在分析众多机制方案的基础之上, 设计一个超轻量级的认证方案. 方案不仅可满足安全需求, 同时可适用于低计算量智能工厂系统中. 具体的, 方案采用循环移动运算对隐私信息进行加密, 循环移动运算可基于按位运算方式实现, 从而使得整体计算量得到一定程度降低; 同时为减少参数引入, 充分利用加密信息自身携带的汉明权重变量, 不仅节约了存储量, 也可增加破解难度.

2 循环移动运算的实现

循环移动运算分为循环左移运算、循环右移运算两种, 用符号$ROT_L(X,Y)$表示循环左移运算、$ROT_R(X,Y)$表示循环右移运算. 发送方若采用循环左移运算对重要信息加密, 则接收到可用循环右移运算对消息进行解密.

循环左移运算定义如下: X、Y 是长度为 L 位的二进制字符串, $hm(X)$、$hm(Y)$分别表示二进制字符串 X、二进制字符串 Y 的汉明权重, 将二进制字符串 X 向左循环移动二进制字符串 Y 的汉明权重$hm(Y)$位, 即可得到$ROT_L(X,Y)$的结果.

循环右移运算定义如下: X、Y 是长度为 L 位的二进制字符串, $hm(X)$、$hm(Y)$分别表示二进制字符串 X、二进制字符串 Y 的汉明权重, 将二进制字符串 Y 向右循环移动二进制字符串 X 的汉明权重$hm(X)$位, 即可得到$ROT_R(X,Y)$的结果.

可通过如下例子解释循环移动运算含义及实现过程.

循环左移运算: X= 100110、Y= 001100, 可得到 $hm(X)$= 3、$hm(Y)$= 2, 进一步可得到Z=$ROT_L(X,Y)$ = 011010. 假设另一方知晓 Y 的值, 现要对 X 进行解密, 则对循环左移运算的解密: $ROT_R(Y,Z)$, 即对收到消息 Z 进行循环右移二进制字符串 Y 的汉明权重$hm(Y)$ = 2位.

循环右移运算: X= 100010、Y= 001110, 可得到 $hm(X)$= 2、$hm(Y)$= 3, 进一步可得到Z=$ROT_R(X,Y)$ = 100011. 假设另一方知晓 X 的值, 现要对 Y 进行解密, 则对循环右移运算的解密: $ROT_L(Z,X)$, 即对收到消息 Z 进行循环左移二进制字符串 X 的汉明权重$hm(X)$ = 2 位.

3 认证方案设计

该章节将从方案的符号含义及实现步骤等角度展开对方案的描述.

3.1 认证方案符号含义

文中认证方案出现的各符号含义如下:

BN表示智能工厂系统中的区块链结点.

R 表示智能工厂系统中的读卡器.

T表示智能工厂系统中嵌有电子标签的产品.

t_R表示智能工厂系统中的读卡器端产生的时间戳

(使用在 T 端).

t_r表示智能工厂系统中的读卡器端产生的时间戳(使用在BN端).

t_T表示智能工厂系统中嵌有电子标签的产品端产生的时间戳.

t_{BN}表示智能工厂系统中的区块链结点端产生的时间戳.

t_R^*表示智能工厂系统中嵌有电子标签的产品端第一次收到智能工厂系统中的读卡器端消息的时间.

t_T^*表示智能工厂系统中的读卡器端第一次收到智能工厂系统中嵌有电子标签的产品端消息的时间.

t_{BN}^*表示智能工厂系统中的读卡器端第一次收到智能工厂系统中的区块链结点端消息的时间.

t_r^*表示智能工厂系统中的区块链结点端第一次收到智能工厂系统中的读卡器端消息的时间

ΔT表示该智能工厂系统中所允许的最大传输时延.

IDS表示智能工厂系统中嵌有电子标签的产品的假名.

IDS_{next}表示智能工厂系统中嵌有电子标签的产品的下轮通信假名.

ID表示智能工厂系统中嵌有电子标签的产品的标识符.

K表示智能工厂系统中嵌有电子标签的产品与智能工厂系统中的区块链结点间的共享密钥值.

K_{next}表示智能工厂系统中嵌有电子标签的产品与智能工厂系统中的区块链结点间的下轮通信共享密钥值.

x表示智能工厂系统中的读卡器端产生的随机数.

y表示智能工厂系统中嵌有电子标签的产品端产生的随机数.

z表示智能工厂系统中的区块链结点端产生的随机数.

$\oplus$表示异或运算.

$ROT_L(X,Y)$表示循环左移运算.

$ROT_R(X,Y)$表示循环右移运算.

3.2 认证方案步骤

认证方案可分为两个阶段, 第 1 个阶段是初始化阶段, 主要完成产品出厂之前各参数的初始化; 第 2 个阶段是认证阶段, 主要实现产品与区块链结点之间的彼此验证. 待初始化阶段完成, 产品端存放的信息有IDS、ID、K、ΔT; 区块链结点端存放的信息有IDS、ID、K、ΔT; 读卡器端存放的信息有ΔT.

与其他方案一致, 做出下面约定: 智能工厂系统中嵌有电子标签的产品与智能工厂系统中的读卡器间通信不安全, 易被攻击者监听; 智能工厂系统中的读卡器与智能工厂系统中的区块链结点间通信安全.

本文认证方案的流程可见图 1 所示.

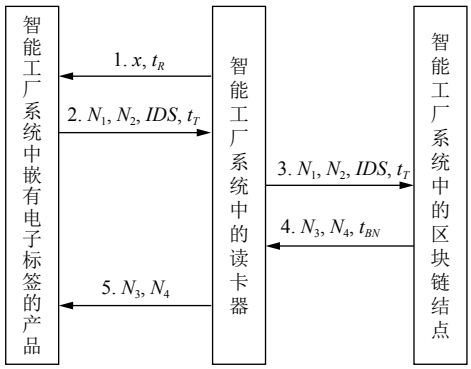

图 1 认证方案的流程图

结合图 1 可将文中方案具体实现步骤描述如下:

(1) 智能工厂系统中的读卡器端产生随机数x、时间戳t_R, 并将随机数x、时间戳t_R发送给智能工厂系统中嵌有电子标签的产品, 开启认证方案.

(2) 智能工厂系统中嵌有电子标签的产品端收到信息, 先计算$|t_R-t_R^*| \le \Delta T$是否成立.

若不成立, 表示通信延迟已超出系统所能允许的最大延时, 方案停止.

若成立, 智能工厂系统中嵌有电子标签的产品端产生随机数y、时间戳t_T, 然后取出自身存放的 ID、K 分别进行计算可得到消息N_1、N_2, 最后将N_1、N_2、IDS、t_T发送给智能工厂系统中的读卡器.

其中, 消息$N_1=ROT_L(K\oplus y,x)$、$N_2=ROT_L(ID\oplus y,x)$.

(3) 智能工厂系统中的读卡器端收到信息, 先计算$|t_T-t_T^*| \le \Delta T$是否成立.

若不成立, 表示通信延迟已超出系统所能允许的最大延时, 方案停止.

若成立, 智能工厂系统中的读卡器端产生时间戳t_r, 最后将N_1、N_2、IDS、t_r、x发送给智能工厂系统中的区块链结点.

(4) 智能工厂系统中的区块链结点端收到信息, 先计算$|t_r-t_r^*| \le \Delta T$是否成立.

若不成立, 表示通信延迟已超出系统所能允许的最大延时, 方案停止.

若成立, 区块链结点开始搜索存放的数据中是否

有与接收到的IDS相等的数据信息. 未找到, 表明消息的来源方是第三方伪造的, 方案停止. 找到, 区块链结点则取出与IDS相对应的ID、K参数, 接着分别对N_1、N_2进行解密运算, 通过解密N_1可以得到一个随机数y_1、通过解密N_2可以得到一个随机数y_2, 然后判断$y_1=y_2$是否成立.

若$y_1=y_2$不成立, 表明消息来源方是第三方伪造的, 方案停止.

若$y_1=y_2$成立, 表明消息来源方通过区块链结点验证, 同时说明$y_1=y_2=y$. 待验证通过, 智能工厂系统中的区块链结点端产生随机数z、时间戳t_{BN}, 然后通过约定好的计算法则计算得到消息N_3、N_4, 接着开始更新信息$IDS_{\text{next}}=ROT_L(IDS\oplus y,z)$、$K_{\text{next}}=ROT_L(K\oplus z,y)$, 最后将$N_3$、$N_4$、$t_{\text{BN}}$发送给智能工厂系统中的读卡器.

其中,消息$N_3=ROT_L(K\oplus z,y)$、$N_4=ROT_L(ID\oplus z,y)$、$y_1=ROT_R(N1,x)\oplus K$、$y_2=ROT_R(N2,x)\oplus ID$.

(5) 智能工厂系统中的读卡器端收到信息, 先计算$|t_{BN}-t_{BN}^*|\le\Delta T$是否成立.

若不成立, 表示通信延迟已超出系统所能允许的最大延时, 方案停止.

若成立, 智能工厂系统中的读卡器将N_3、N_4转发给智能工厂系统中嵌有电子标签的产品.

(6) 智能工厂系统中嵌有电子标签的产品端收到信息, 分别对N_3、N_4进行解密运算, 通过解密N_3可以得到一个随机数z_1、通过解密N_4可以得到一个随机数z_2, 然后判断$z_1=z_2$是否成立.

若$z_1=z_2$不成立, 表明消息来源方是第三方伪造的, 方案停止.

若$z_1=z_2$成立, 表明消息来源方通过产品验证, 同时说明$z_1=z_2=z$. 待验证通过, 智能工厂系统中嵌有电子标签的产品端开始更新信息$IDS_{\text{next}}=ROT_L(IDS\oplus y,z)$、$K_{\text{next}}=ROT_L(K\oplus z,y)$, 待信息更新完成, 则正常的认证方案过程顺利结束.

其中, $z_1=ROT_R(N_3,y)\oplus K$、$z_2=ROT_R(N_4,y)\oplus ID$.

4 方案安全性分析

本小节将从不同角度分析文中超轻量级方案安全指标.

(1) 双向鉴别

虽然文中方案中有 3 个会话实体, 但仔细分析发现, 智能工厂系统中的读卡器更多的像是一个转发实体, 因此, 方案中主要是要实现智能工厂系统中嵌有电子标签的产品与智能工厂系统中的区块链结点间实现双向鉴别性. 其中智能工厂系统中嵌有电子标签的产品是基于N_3、N_4实现对智能工厂系统中的区块链结点的鉴别, 而智能工厂系统中的区块链结点是基于N_1、N_2实现对智能工厂系统中嵌有电子标签的产品的鉴别. 故方案可提供实体间双向鉴别.

(2) 匿名性

文中方案引入智能工厂系统中嵌有电子标签的产品的假名, 每次通信时传递的都是假名, 且每次通信介绍后, 假名会进行更新, 使得每轮假名都不同; 其他需要发送的隐私信息都是加密之后再发送, 使得攻击者无法获取有用有效信息, 因此攻击者无法获知智能工厂系统中嵌有电子标签的产品的真实身份信息. 故方案可提供实体的匿名性.

(3) 重放攻击

攻击者可以通过窃听的方式, 获悉第i轮通信的所有信息, 比如: N_1、N_2、N_3、N_4等. 当通信实体间进行第i+1轮通信时, 攻击者可以向智能工厂系统中嵌有电子标签的产品重放窃听获取第i轮通信信息N_3、N_4, 以企图通过该产品的验证; 或攻击者向智能工厂系统中的区块链结点重放窃听获取第i轮通信信息N_1、N_2, 以企图通过区块链节点的验证, 进而获取更多隐私信息.

文中通信信息N_1、N_2在加密过程中混有随机数y和随机数x, 通信信息N_3、N_4在加密过程中混有随机数y和随机数z. 上述随机数全部都是随机数产生器随机产生得到, 且前一轮与后一轮随机数间没有任何关联. 当攻击者在第i+1轮通信中重放窃听获取的第i轮通信信息时, 攻击者必然失败, 因第i+1轮通信信息虽加密方法未发生变动, 但加密用到的随机数却发生变化, 而攻击者重放的信息却还是上轮信息, 故重放失败.

基于上述, 攻击者发起的重放攻击失败告终.

(4) 异步攻击

在本文方案中, 智能工厂系统中的区块链结点一端不仅存放有当前正在通信用到的共享秘密值, 同时还存放有上轮通信用到的共享秘密值. 当智能工厂系统中的区块链结点对智能工厂系统中嵌有电子标签的产品进行鉴别时, 区块链节点会先用存放的当前通信用到的共享秘密值来验证消息来源的真假.

若验证成功, 则进行后续操作步骤. 若验证失败, 则区块链节点将会调用存放的上轮通信用到的共享秘密值重新发起对消息来源真伪的验证. 只有在当且仅当上述两次验证都失败的情况下, 区块链结点才会认定消息来源方是伪造的; 如果第 1 次验证失败, 而第 2 次验证成功, 则区块链结点仍会认为消息来源方真实可靠, 会继续进行后续操作步骤.

基于上述, 文中方案可抵抗攻击者发起的异步攻击.

(5) 暴力破解

攻击者获取方案中任意消息可采用穷举的方式获取该消息中加密的隐私信息, 从而发起后续其他攻击, 以获取更多隐私信息. 选择以消息N_1=$ROT_L(K \oplus y, x)$为例进行详细分析, 在消息N_1=$ROT_L(K \oplus y, x)$中, 隐私信息便是共享秘密值, 攻击者窃听可以获取随机数x和消息N_1, 其他参数攻击者无法获取, 共享秘密值 K 和随机数y于攻击者来说均不知晓, 因此攻击者无法穷举出共享秘密值 K 的正确数值. 故方案可抵御暴力破解.

(6) 前向/后向安全

方案中所有消息加密之时全部混入随机数, 随机数是随机产生, 且具有前后无法预测性及不一样特征, 使得攻击者无法从截获当前消息中分析出下轮通信消息值或逆推出上轮通信消息中用户隐私信息, 使得方案较为安全. 故方案可以提供前向/后向安全.

文中消息加密时混入的随机数, 都是采用密文的方式发送的, 在整个通信过程中, 未出现明文随机数, 因此, 对于攻击者来说, 攻击者想要破解某个通信消息的话, 攻击者需要先想办法获取随机数. 基于密文方式传送随机数, 使得攻击者无法直接得到随机数, 则攻击者又需要借助其他参量来破解获取随机数, 从而使得攻击者陷入一个死循环, 既无法破解消息, 也无法破解得到随机数. 而对于通信实体一方来说, 得到加密的随机数比较简单, 因通信实体双方会共享一些参数信息, 发送方会用这些共享的参数信息与随机数共同加密, 再发送给接收者; 接收者收到信息后, 按照相同的运算法则, 再结合事前共享的参数信息, 即可计算得到发送者产生的随机数, 再进行其他后续操作. 综上, 混入随机数, 对正常的通信实体来说, 加密及解密时间开销都在可接受范围内, 而对于攻击者来说, 则无法进行可接受范围内的时间开销破解.

5 方案形式化推理证明

本小节将采用基于 GNY 形式逻辑化对文中方案进行逻辑形式推理.

(1) 形式化模型

基于 GNY 逻辑形式化分析方案, 需对方案进行形式化, 约定 T 表示智能工厂系统中嵌有电子标签的产品, BN表示智能工厂系统中的区块链结点, R 表示智能工厂系统中的读卡器, 方案形式化之后如下:

$Msg1$: $R \rightarrow T : x, t_R$

$Msg2$: $T \rightarrow R : N_1, N_2, IDS, t_T$

$Msg3$: $R \rightarrow BN : N_1, N_2, IDS, t_r, x$

$Msg4$: $BN \rightarrow R : N_3, N_4, t_{BN}$

$Msg5$: $R \rightarrow T : N_3, N_4$

将上述章节中有关具体通信消息计算带入上述形式化中, 可得到:

$Msg1$: $T \triangleleft *x, t_R \sim\!\!\mapsto R| \equiv \#x, t_R$

$Msg2$: $R \triangleleft *N_1, N_2, IDS, t_T \sim\!\!\mapsto T| \equiv \#N_1, N_2, IDS, t_T$

$Msg3$: $BN \triangleleft *N_1, N_2, IDS, t_r, x \sim\!\!\mapsto R| \equiv \#N_1, N_2, IDS, t_r, x$

$Msg4$: $R \triangleleft *N_3, N_4, t_{BN} \sim\!\!\mapsto BN| \equiv \#N_3, N_4, t_{BN}$

$Msg5$: $T \triangleleft *N_3, N_4 \sim\!\!\mapsto R| \equiv \#N_3, N_4$

(2) 初始化假设

$A1$: $R \ni ID$

$A2$: $T \ni K$

$A3$: $T \ni ID$

$A4$: $T \ni IDS$

$A5$: $BN \ni K$

$A6$: $BN \ni ID$

$A7$: $BN \ni IDS$

$A8$: $R| \equiv \#(x)$

$A9$: $T| \equiv \#(y)$

$A10$: $BN| \equiv \#(z)$

$A11$: $T| \equiv T \overset{ID}{\longleftrightarrow} BN$

$A12$: $T| \equiv T \overset{K}{\longleftrightarrow} BN$

$A13$: $T| \equiv T \overset{IDS}{\longleftrightarrow} BN$

$A14$: $BN| \equiv BN \overset{K}{\longleftrightarrow} T$

$A15$: $BN| \equiv BN \overset{IDS}{\longleftrightarrow} T$

$A16$: $BN| \equiv BN \overset{ID}{\longleftrightarrow} T$

初始化假设 $A1$ 是智能工厂系统中的读卡器R所拥有的, 初始化假设 $A2$、$A3$、$A4$ 是智能工厂系统中嵌

有电子标签的产品T所拥有的, 初始化假设$A5$、$A6$、$A7$是智能工厂系统中的区块链结点BN所拥有的, 初始化假设$A8$是智能工厂系统中的读卡器R对拥有信息新鲜性的相信, 初始化假设$A9$是智能工厂系统中嵌有电子标签的产品T对拥有信息新鲜性的相信, 初始化假设$A10$是智能工厂系统中的区块链结点BN对拥有信息新鲜性的相信, 初始化假设$A11$、$A12$、$A13$是智能工厂系统中嵌有电子标签的产品T与智能工厂系统中的区块链结点BN间彼此相信共享信息, 初始化假设$A14$、$A15$、$A16$是智能工厂系统中的区块链结点BN与智能工厂系统中嵌有电子标签的产品T间彼此相信共享信息.

(3) 证明目标

结合上述, 可以分析得出, 方案中需要推理证明的目标有 4 个, 即:

$G1$: $BN|\equiv T|\sim \#(N_1)$

$G2$: $BN|\equiv T|\sim \#(N_2)$

$G3$: $T|\equiv BN|\sim \#(N_3)$

$G4$: $T|\equiv BN|\sim \#(N_4)$

(4) 推理证明

因需推理证明的 4 个目标证明原理大致相同, 因此文中这里仅选择目标$G1$: $BN|\equiv T|\sim \#(N_1)$进行详细分析, 其他证明目标推理证明过程不再阐述, 目标$G1$: $BN|\equiv T|\sim \#(N_1)$证明推理过程如下:

首先, 因为初始化假设$A8$: $R|\equiv \#(x)$、$A9$: $T|\equiv \#(y)$和新鲜性规则$F1$: $\dfrac{P|\equiv \#(X)}{P|\equiv \#(X,Y),P|\equiv \#(F(X))}$可得知: $BN|\equiv \#(K,x,y)$.

在$Msg3$: $R\rightarrow BN:N_1,N_2,IDS,t_r,x$中, $BN\triangleleft *x$, 即$T\ni *x$, 同时结合初始化假设$A5$、$A6$、$A7$和规则$P2$可得知: $BN\ni (K,x,y)$.

接着, 由已推导出的$BN|\equiv \#(K,x,y)$、$BN\ni (K,x,y)$, 再根据新鲜性规则$F10$: $\dfrac{P|\equiv \#(X),P\ni X}{P|\equiv \#(H(X,Y))}$可得知: $BN|\equiv \#(N_1)$, 即 $BN|\equiv \#(ROT_L(K\oplus y,x))$.

最后, 根据$Msg3$、初始化假设$A14$、已推导出的$BN\ni (K,x,y)$、已推导出的$BN|\equiv \#(N_1)$、消息解析规则$I3$可得到: $BN|\equiv T|\sim (N_1)$,即 $BN|\equiv T|\sim (ROT_L(K\oplus y,x))$.

由新鲜性的定义可推导出证明目标$G1$: $BN|\equiv T|\sim (N_1)$, 即$G1$: $BN|\equiv T|\sim (ROT_L(K\oplus y,x))$.

6 方案性能分析

将文中方案与其他经典方案进行性能对比, 选择智能工厂系统中嵌有电子标签的产品为对象, 对比结果见表 1 所示.

表 1 不同方案对比性能

对比方案	计算量	通信量	存储量
文献[12]	5PUF+5AND+1PRT	14	3
文献[13]	7MOD+2AND+2PRT	10	4
文献[14]	6HASH+3AND+1PRT	16	5
文献[15]	7PNG+4AND+2PRT	13	3
文献[16]	11ROT+4AND+1PRT	13	3
本文方案	6ROT+2AND+1PRT	15	4

对表 1 中符号的含义说明如下: PUF 符号表示的含义是物理不可克隆函数的计算量; AND 符号表示的含义是按位运算的计算量 (比较常见的按位运算有: 按位与运算、按位异或运算等); PRT 符号表示的含义是产生随机数的计算量; MOD 符号表示的含义是模运算的计算量; HASH 符号表示的含义是哈希函数的计算量; PNG 符号表示的含义是伪随机数函数的计算量; ROT 符号表示的含义是循环移动运算的计算量.

约定通信量长度与存储参数的长度都是一致的, 文中方案智能工厂系统中嵌有电子标签的产品一端存放的信息有IDS、ID、K、ΔT, 因此存储量大小为 4. 文中方案一个完整的会话过程中一共有 14 个会话消息, 因此通信量大小为 14. 不论是从通信量角度出发, 还是从存储量角度出发, 文中方案与其他方案相比较, 并未有优势, 甚至比某些方案开销还大, 但文中方案主要优势在于能够提供较高的安全性及低计算量成本.

从智能工厂系统中嵌有电子标签的产品一端的计算量角度出发分析, 除了文献 [16] 中方案与文中方案加密算法属于超轻量级的, 其他文献中采用的算法都属于轻量级的, 因此文中计算量有较大降低及优势. 重点比较文献 [16] 中方案与文中方案, 因文献 [16] 中方案在共享密钥及假名更新时计算复杂, 使得 ROT 运算次数增多, 从而整体计算量也高于文中方案, 故文中方案仍存在一定优势.

文中方案智能工厂系统中嵌有电子标签的产品一端计算量的由来如下描述: 因需要产生一个随机数x, 故需要一个 PRT 运算. 在计算消息N_1、N_2过程中, 分别需要用到第 1 次 ROT 运算、第 2 次 ROT 运算; 在对消息N_3、N_4解密过程时, 分别需要用到第 3 次 ROT 运算、第 4 次 ROT 运算; 在最后更新共享秘密值、假名时, 分别需要用到第 5 次 ROT 运算、第 6 次 ROT

运算, 故一共需要 6 个 ROT 运算. 在对消息N_3、N_4解密过程时, 分别需要用到第 1 次 AND 运算、第 2 次 AND 运算, 故一共需要两个 AND 运算. 基于上述, 文中方案智能工厂系统中嵌有电子标签的产品一端计算量为 6ROT+2AND+1PRT.

循环移动运算可以确保加密隐私信息的安全性, 能够达到用户需要的认证效果. 具体分析原因如下: 其一, 循环移动运算分为循环左移运算和循环右移运算两种, 通信实体在进行加密时, 到底选择哪种方式进行加密, 是不对外公开的, 这点可以增加外界破解的难度; 其二, 不论通信实体选择哪种方式进行加密, 都会用到加密参数自身具备的汉明权重, 加密参数未明文出现过, 攻击者因此无法获取, 攻击者只能采用穷尽的方法一个一个尝试汉明重量去破解, 但可以肯定, 此种方法时间开销巨大; 其三, 所有消息加密时混入随机数, 每轮加密用到随机数都发生变更, 即便是攻击者侥幸穷举出某轮加密用到的部分信息, 但当前正在通信的轮次与攻击者破解的通信轮次间, 早已相隔甚远, 因此, 于攻击者而言, 穷举出的信息早已过时, 失去了原本的意义.

7 结论与展望

文中将传统的射频识别技术与新产生的区块链技术相结合, 提出一种可适用于智能工厂的超轻量级认证方案. 方案采用超轻量级的循环移动运算实现对隐私信息加密, 在确保安全的前提下, 结合加密隐私信息自身特有的汉明权重参数, 可增加破解难度的同时, 也能减少参量引入, 减低存储开销. 对方案从不同的攻击角度分析, 方案能够达到预期的安全要求; 采用 GNY 逻辑形式化分析, 对方案进行严谨的逻辑形式化推理证明分析; 最后从性能角度出发, 分析文中方案在计算时间复杂度方面优于其他经典方案.

参考文献

1 张朝晖, 刘悦, 刘道微. 基于标签 ID 的 RFID 系统密钥无线生成算法. 计算机应用研究, 2017, 34(1): 261–263, 269. [doi: 10.3969/j.issn.1001-3695.2017.01.059]

2 Yang MH. Secure multiple group ownership transfer protocol for mobile RFID. Electronic Commerce Research and Applications, 2012, 11(4): 361–373. [doi: 10.1016/j.elerap.2012.01.004]

3 原变青, 刘吉强. 通用可组合安全的 RFID 标签组所有权转移协议. 计算机研究与发展, 2015, 52(10): 2323–2331. [doi: 10.7544/issn1000-1239.2015.20150555]

4 Zuo YJ. Changing hands together: A secure group ownership transfer protocol for RFID tags. Proceedings of the 43rd Hawaii International Conference on System Sciences. Honolulu: IEEE, 2010. 1–10.

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. 计算机科学, 2016, 43(8): 128–130, 158. [doi: 10.11896/j.issn.1002-137X.2016.08.027]

6 陶源, 周喜, 马玉鹏, 等. 基于 Hash 函数的移动双向认证协议. 计算机应用, 2016, 36(3): 657–660. [doi: 10.11772/j.issn.1001-9081.2016.03.657]

7 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. 计算机研究与发展, 2013, 50(6): 1276–1284. [doi: 10.7544/issn1000-1239.2013.20121268]

8 He L, Gan Y, Yin YF. Secure group ownership transfer protocol for tags in RFID system. International Journal of Security and its Applications, 2014, 8(3): 21–30. [doi: 10.14257/ijsia.2014.8.3.03]

9 鲁力. RFID 系统密钥无线生成. 计算机学报, 2015, 38(4): 822–832.

10 Molnar D, Soppera A, Wagner D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. Proceedings of the 12th International Workshop on Selected Areas in Cryptography. Berlin Heidelberg: Springer, 2006. 276–290.

11 Goswami A, Ghoshal N. Imperceptible image authentication using wavelets. International Journal of Network Security, 2016, 18(5): 861–873.

12 Ahmed AA, Zaman NAK. Attack intention recognition: A review. International Journal of Network Security, 2017, 19(2): 244–250.

13 Xie R, Jian BY, Liu DW. An improved ownership transfer for RFID protocol. International Journal of Network Security, 2018, 20(1): 149–156.

14 Chiou SY, Ko WT, Lu EH. A secure ECC-based mobile RFID mutual authentication protocol and its application. International Journal of Network Security, 2018, 20(2): 396–402.

15 Ming Y, Yuan HP. Fully Secure anonymous identity based broadcast encryption with group of prime order. International Journal of Network Security, 2019, 21(1): 7–16.

16 曹舒雅, 姚英英, 常晓林. 基于区块链的智能工厂 RFID 系统轻量级身份认证机制. 网络空间安全, 2020, 11(9): 70–77, 93. [doi: 10.3969/j.issn.1674-9456.2020.09.010]