改进的基于 R_LWE 密码体制的双向认证协议

徐 省 华
(广东技术师范大学网络信息中心 广东 广州 510665)

摘 要 针对射频识别系统中标签与读卡器会话存在易被攻击者窃听等安全问题,提出一种基于 R_LWE (Learning with Errors over Ring)密码体制加解密的 RFID 双向认证协议。协议采用 R_LWE 密码体制实现加密的同时引入交叉合成运算,既可确保安全性,亦可降低计算开销。结合不同攻击类型、逻辑形式化分析、性能角度综合分析,该协议具备安全等级高、计算量小等优势。

关键词 物联网 射频识别技术 R_LWE 密码体制 交叉合成运算 双向认证

中图分类号 TP393.08 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.11.051

IMPROVED MUTUAL AUTHENTICATION PROTOCOL BASED ON R_LWE CRYPTOSYSTEM

Xu Shenghua
(*Network Information Center, Guangdong Polytechnic Normal University, Guangzhou 510665, Guangdong, China*)

Abstract Aimed at the security problems that the session between tag and card reader in RFID system is easy to be eavesdropped by attackers, a method based on R_LWE encryption and decryption of RFID two-way authentication protocol is proposed. The protocol adopted R_LWE cryptosystem to implement encryption and introduce cross synthesis operation, which could ensure security and reduce computing overhead. Combined with different attack types, logical formal analysis and comprehensive analysis from the perspective of performance, it shows that the protocol in this paper has the advantages of high security level and small amount of calculation.

Keywords Internet of things RFID technology R_LWE cryptosystem Cross synthesis operation Mutual authentication

0 引 言

射频识别技术是一种不用与特定物体接触即可读出存放信息的技术[1-2],该技术起源于二十世纪,受限于当时科技等因素,该技术并未得到广泛发展。进入二十一世纪后,伴随着科技快速发展,射频识别技术在物联网等行业得到飞速发展应用。一个典型的射频识别系统包括但不限于标签、读卡器、服务器等设备[3-4]。相比较标签来讲,读卡器和服务器不论是在计算能力方面,还是在存储空间方面,都比标签强很多倍;同时读卡器与服务器间一般利用光纤等有线媒介进行数据交互,一般认为安全可信,且可将两者看成一个整体研究。但读卡器与标签间则采用无线信道交互数据,易被攻击者监听,从而获悉隐私信息数据,存在一定安全隐患[5-6]。

标签和读卡器间信道具有不对称的特征,从而导致易被窃听。读卡器可发出信号,一般将读卡器向标签发送信号的信道称之为前向链路,反之,标签向读卡器发送信号的信道称之为后向链路。因标签自身并未携带电源装置,因此标签只能反射读卡器信号,同时向读卡器发送信号,使得后向链路通信距离极短,而前向链路通信距离则可以很长,因此攻击者只要在一个合适的距离范围内,可同时对前向链路及后向链路进行窃听[7-8]。

Regev[9]受到 Ajtai-Dwork(AD)加密方案[10]启发,

收稿日期:2022-02-20。广东省普通高校重点领域专项项目(2021ZDZX1087)。**徐省华**,讲师,主研领域:信息安全,安全协议分析,密码学。

提出一种将格理论与学习理论相结合的算法设计思想,并引出一个在格理论上的新困难问题,即错误学习问题(Learning with Errors,LWE)。对该算法分析,发现该算法复杂度可以归约到格理论上的判定性最短向量问题以及最短无关向量问题,该算法在存在优势的同时,产生的缺陷也不容忽略,比如:所需密钥大,且随着参数的不断增加,各实体计算量也急剧增加,无法广泛推广应用。

Lyubashevsky 等[11]在 Regev 所提算法思想基础之上,提出了一个变体的 R_LWE 算法。经过多年的研究发展,基于 R_LWE 算法的密钥体制具备如下优势:加密和解密速度均很快、所需密钥长度小、计算效率高、能够提供严谨的安全证明。

文献[12]中基于 R_LWE 密码体制设计的认证协议,在具备上述优势的同时,因缺少标签对读写器的认证,使得攻击者可伪装成读写器,从而窃取交互数据信息,并进一步篡改随机数等数据信息。文献[13]中将 R_LWE 密码体制与模运算相结合设计认证协议,具备一定的安全性,但协议设计过程中,共享密钥值始终未更新过,将导致攻击者重放攻击存在成功的风险。文献[14]结合物理不可克隆技术及 R_LWE 密码体制提出一个认证协议,协议能够抵抗重放攻击等,但读卡器一端仅存放当前共享秘密值,无法抵抗攻击者发起的异步攻击。文献[15]中利用 R_LWE 密码体制给出一个认证协议,对该协议进行分析,协议无法实现最后一步中标签对服务器或标签对读卡器的验证,将导致攻击者可进行假冒攻击。

鉴于上述经典协议存在或计算量大或认证失败等缺陷问题,本文在 R_LWE 密码体制下,结合自创算法给出一个认证协议。协议中标签一端仅利用 R_LWE 密码体制中加密算法,计算量较大的解密算法放在读卡器一端进行,可确保信息安全的同时,标签一端计算量在承受范围内;为确保实现标签对读卡器的验证,两者之间采用自创加密算法,即交叉合成运算对信息实施加密。从常见的攻击类型、逻辑形式化分析、标签一端计算量及存储量等方面对协议进行分析,表明本文协议能够提供常见类型的攻击,且标签一端计算量可满足现有计算能力受限制的系统中使用。

1 文献[15]协议安全性分析

有关刘涛等设计的协议详细步骤在此处不再分开阐述,具体描述步骤可参见文献[15]。本节主要分析刘涛等协议安全缺陷,具体分析如下:

服务器加密得到消息 Y_1 和 Y_2,然后将消息 Y_1 和 Y_2 发送给读写器,读写器通过消息 Y_2 验证服务器的真假,待完成验证,读写器将消息 Y_1 发送给标签。标签通过消息 Y_1 验证服务器真假,但无法验证读写器真假,主要原因在于:读写器相当于间接转发了消息 Y_1,即读写器并未对消息 Y_1 进行任何处理,而是直接转发给标签。

可以给出下列一种假冒攻击方式:攻击者阻塞服务器发送给读写器的消息 Y_1 和 Y_2,同时也阻塞读写器发送给标签的消息 Y_1 这两个步骤,由攻击者伪装成读写器。待攻击者收到服务器发送过来的消息 Y_1 和 Y_2 后,攻击者直接将消息 Y_1 发送给标签。按照原协议描述,标签将无法验证读写器的真伪,从而认定服务器为真,且读写器也为真,但事实并非如此。

本文所提协议,除了改进原协议无法抵抗假冒攻击缺陷之外,还从其他方面着手进行改进,比如:在现在的 RFID 系统中,服务器与读写器通过诸如光纤、同轴电缆等有线方式进行数据交换,有线方式具备较高的安全性,将服务器及读写器看作一个整体。

2 协议设计

1)协议符号含义。R_{eader} 是服务器与读卡器构成的整体;T_{ag} 标签;K 是 R_{eader} 与 T_{ag} 间共享秘密值;K^{new} 是 R_{eader} 与 T_{ag} 间的当前共享秘密值;K^{old} 是 R_{eader} 与 T_{ag} 间的上轮共享秘密值;$I_{D_{\text{tag}}}$ 是 T_{ag} 唯一的标识符;a 是 R_{eader} 产生的随机数;b 是 T_{ag} 产生的随机数;$E_h(x)$ 是 R_LWE 密码体制下的加密函数[16];$D_y(x)$ 是 R_LWE 密码体制下的解密函数;$Cro\text{-}Syn(X,Y)$ 是交叉合成运算函数;⊕是按位异或运算;& 是按位与运算;m_{eg_i} 是会话消息。

2)协议实现。协议在开始之前,存在一个初始化过程,待初始化过程完成,R_{eader} 一端存放的信息有 K、$I_{D_{\text{tag}}}$、$E_h(x)$、$D_y(x)$、$Cro\text{-}Syn(X,Y)$,T_{ag} 一端存放的信息有:K、ID_{tag}、$E_h(x)$、$Cro\text{-}Syn(X,Y)$,且 $K^{\text{new}}=K^{\text{old}}=K$。

本文设计的认证协议示意图如图 1 所示。

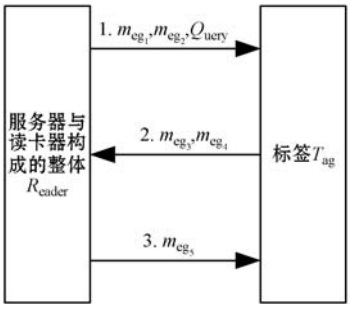


图 1 协议示意图

结合图 1 可将文中协议步骤描述如下。

Step1　$R_{\text{eader}} \rightarrow T_{\text{ag}}$

R_{eader}一端产生随机数 a,利用 a、$I_{D_{\text{tag}}}$计算得到 $m_{\text{eg}_1} = a \oplus I_{D_{\text{tag}}}$、$m_{\text{eg}_2} = Cro\text{-}Syn(a, a\&I_{D_{\text{tag}}})$,然后将 $m_{\text{eg}_1} = a \oplus I_{D_{\text{tag}}}$、$m_{\text{eg}_2} = Cro\text{-}Syn(a, a\&I_{D_{\text{tag}}})$、$Q_{\text{uery}}$一起发给 T_{ag}。

Step2　$T_{\text{ag}} \rightarrow R_{\text{eader}}$

T_{ag}一端收到消息,先对 $m_{\text{eg}_1} = a \oplus I_{D_{\text{tag}}}$进行处理得到 $a = m_{\text{eg}_1} \oplus I_{D_{\text{tag}}}$,然后将 $a = m_{\text{eg}_1} \oplus I_{D_{\text{tag}}}$代入得到 $m'_{\text{eg}_2} = Cro\text{-}Syn(m_{\text{eg}_1} \oplus I_{D_{\text{tag}}}, (m_{\text{eg}_1} \oplus I_{D_{\text{tag}}})\&I_{D_{\text{tag}}})$,接着开始比较 m_{eg_2}与 m'_{eg_2}关系。

m_{eg_2}与 m'_{eg_2}关系不等,则说明 R_{eader}是伪造的,协议无法继续进行。

m_{eg_2}与 m'_{eg_2}关系相等,可说明 R_{eader}是真实的,协议可继续。T_{ag}一端产生随机数 b,利用 a、$I_{D_{\text{tag}}}$、b、K 依次计算得到 $m_{\text{eg}_3} = a \oplus b$、$m_{\text{eg}_4} = E_h(a\&K, b\&I_{D_{\text{tag}}})$,最后将 $m_{\text{eg}_3} = a \oplus b$、$m_{\text{eg}_4} = E_h(a\&K, b\&I_{D_{\text{tag}}})$一起发送给 R_{eader}。

Step3　$R_{\text{eader}} \rightarrow T_{\text{ag}}$

R_{eader}一端收到消息,先对 $m_{\text{eg}_3} = a \oplus b$ 进行处理得到 $b = a \oplus m_{\text{eg}_3}$,接着用 K^{new}或 K^{old}计算得到 m'_{eg_4},然后对比 m'_{eg_4}与 m_{eg_4}关系。

当用 K^{new}计算所得关系为相等时,说明 T_{ag}是真实的,R_{eader}一端计算得到 $m_{\text{eg}_5} = Cro\text{-}Syn(a, b)$,同时更新 R_{eader}与 T_{ag}间共享秘密值 $K^{\text{old}} = K^{\text{new}}$、$K^{\text{new}} = E_h(a, b\&K^{\text{new}})$,最后将 $m_{\text{eg}_5} = Cro\text{-}Syn(a, b)$发送给 T_{ag}。

当用 K^{new}计算所得关系为不等,且用 K^{old}计算所得关系为相等时,也可说明 T_{ag}是真实的,R_{eader}一端计算得到 $m_{\text{eg}_5} = Cro\text{-}Syn(a, b)$,同时更新 R_{eader}与 T_{ag}间共享秘密值 $K^{\text{old}} = K^{\text{old}}$、$K^{\text{new}} = E_h(a, b\&K^{\text{old}})$,最后将 $m_{\text{eg}_5} = Cro\text{-}Syn(a, b)$发送给 T_{ag}。

当用 K^{new}计算所得关系为不等,且用 K^{old}计算所得关系也为不等时,则表明 T_{ag}是伪造的,协议无法继续进行。

Step4　T_{ag}

T_{ag}一端收到消息,利用之前步骤计算得到的信息验证 $m_{\text{eg}_5} = Cro\text{-}Syn(a, b)$ 的真伪。为真,则更新 T_{ag}与 R_{eader}间共享秘密值 $K = E_h(a, b\&K)$;否则,协议无法继续进行。

3　协议形式化分析

本节将采用基于 GNY 逻辑形式化[17]对本文协议进行形式化推理及分析,具体步骤如下。

1）协议形式化描述。

$MSG1: R_{\text{eader}} \rightarrow T_{\text{ag}}: m_{\text{eg}_1}、m_{\text{eg}_2}、Q_{\text{uery}}$

$MSG2: T_{\text{ag}} \rightarrow R_{\text{eader}}: m_{\text{eg}_3}、m_{\text{eg}_4}$

$MSG3: R_{\text{eader}} \rightarrow T_{\text{ag}}: m_{\text{eg}_5}$

用 GNY 形式逻辑语言规范以上协议,可以描述如下:

$MSG1: T_{\text{ag}} < * \{m_{\text{eg}_1}、m_{\text{eg}_2}、Q_{\text{uery}}\}$

$MSG2: R_{\text{eader}} < * \{m_{\text{eg}_3}、m_{\text{eg}_4}\}$

$MSG3: T_{\text{ag}} < * \{m_{\text{eg}_5}\}$

2）协议初始化假设。

$SUP1: (I_{D_{\text{tag}}}、K) \in T_{\text{ag}}$

$SUP2: (I_{D_{\text{tag}}}、K^{\text{new}}、K^{\text{old}}) \in R_{\text{eader}}$

$SUP3: T_{\text{ag}} \mid\equiv \#(a、b)$

$SUP4: R_{\text{eader}} \mid\equiv \#(a、b)$

$SUP5: T_{\text{ag}} \mid\equiv R_{\text{eader}} \overset{K}{\longleftrightarrow} T_{\text{ag}}$

$SUP6: T_{\text{ag}} \mid\equiv R_{\text{eader}} \overset{I_{D_{\text{tag}}}}{\longleftrightarrow} T_{\text{ag}}$

$SUP7: R_{\text{eader}} \mid\equiv T_{\text{ag}} \overset{K}{\longleftrightarrow} R_{\text{eader}}$

$SUP8: R_{\text{eader}} \mid\equiv T_{\text{ag}} \overset{I_{D_{\text{tag}}}}{\longleftrightarrow} R_{\text{eader}}$

3）协议证明目标。

$GOAL1: T_{\text{ag}} \mid\equiv R_{\text{eader}} \mid\sim \#\{m_{\text{eg}_1}、m_{\text{eg}_2}\}$

$GOAL2: R_{\text{eader}} \mid\equiv T_{\text{ag}} \mid\sim \#\{m_{\text{eg}_3}、m_{\text{eg}_4}\}$

$GOAL3: T_{\text{ag}} \mid\equiv R_{\text{eader}} \mid\sim \#\{m_{\text{eg}_5}\}$

4）协议证明过程。鉴于文中篇幅有限等因素,仅选择第一个证明目标 GOAL1 $: T_{\text{ag}} \mid\equiv R_{\text{eader}} \mid\sim \#\{m_{\text{eg}_1}、m_{\text{eg}_2}\}$ 为例进行证明。

$\because$ $MSG1: R_{\text{eader}} \rightarrow T_{\text{ag}}: m_{\text{eg}_1}、m_{\text{eg}_2}、Q_{\text{uery}}$和规则 $P1: \dfrac{P < X}{X \in P}$

$\therefore$ $\{m_{\text{eg}_1}、m_{\text{eg}_2}\} \in T_{\text{ag}}$

$\because$ $SUP4: R_{\text{eader}} \mid\equiv \#(a、b)$以及规则 $F1$:

$$\frac{P \mid\equiv (X)}{P \mid\equiv (x, y), P \mid\equiv \#F(X)}$$

$\therefore$ $T_{\text{ag}} = \#\{m_{\text{eg}_1}、m_{\text{eg}_2}\}$

$\because$ 规则 $P2: \dfrac{X \in P, Y \in P}{(X, Y) \in P, F(X, Y) \in P}$,$SUP1: (I_{D_{\text{tag}}}、K) \in T_{\text{ag}}$、$SUP2: (I_{D_{\text{tag}}}、K^{\text{new}}、K^{\text{old}}) \in R_{\text{eader}}$

$\therefore$ $\{m_{\text{eg}_1}、m_{\text{eg}_2}\} \in T_{\text{ag}}$

$\because$ 规则 $F10: \dfrac{P \mid\equiv (X), X \in P}{P \mid\equiv \#(H(X))}$以及推导出来的 $T_{\text{ag}} = \#\{m_{\text{eg}_1}、m_{\text{eg}_2}\}$、$\{m_{\text{eg}_1}、m_{\text{eg}_2}\} \in T_{\text{ag}}$

$\therefore$ $T_{\text{ag}} \mid= \#\{m_{\text{eg}_1}、m_{\text{eg}_2}\}$

$\because$ 规则 $I3: \dfrac{P < H(X, <S>) >, (X, S) \in P, P \mid\equiv P \leftrightarrow Q, P \mid\equiv \#(X, S)}{P \mid\equiv Q \mid\sim (X, S), P \mid\equiv Q \sim H(X, <S>)}$

又$\because$ $SUP7: R_{\text{eader}} \mid\equiv T_{\text{ag}} \overset{K}{\longleftrightarrow} R_{\text{eader}}$、$SUP8: R_{\text{eader}} \mid\equiv T_{\text{ag}} \overset{I_{D_{\text{tag}}}}{\longleftrightarrow} R_{\text{eader}}$、$SUP5: T_{\text{ag}} \mid\equiv R_{\text{eader}} \overset{K}{\longleftrightarrow} T_{\text{ag}}$、$SUP6: T_{\text{ag}} \mid\equiv R_{\text{eader}} \overset{I_{D_{\text{tag}}}}{\longleftrightarrow} T_{\text{ag}}$以及 $MSG1: R_{\text{eader}} \rightarrow T_{\text{ag}}: m_{\text{eg}_1}、m_{\text{eg}_2}、Q_{\text{uery}}$

$\therefore$ $T_{\text{ag}} \mid= \{m_{\text{eg}_1}、m_{\text{eg}_2}\}$

∵ 新鲜性定义以及推导出来的 $T_{ag}=\#\{m_{eg_1}、m_{eg_2}\}$、$T_{ag}|\equiv R_{eader}\sim\{m_{eg_1}、m_{eg_2}\}$

∴ $GOAL1:T_{ag}|\equiv R_{eader}|\sim\#\{m_{eg_1}、m_{eg_2}\}$ 得证明。

证毕。

4 协议安全性分析

本节将从常见的攻击类型角度展开对文中协议安全性分析,具体如下。

1)假冒攻击。假设攻击者假冒成 R_{eader} 给 T_{ag} 发消息,攻击者并不知道 $I_{D_{tag}}$,所以无法计算正确的 m_{eg_1},更进一步也无法计算正确的 m_{eg_2}。当 T_{ag} 收到攻击者发送的 m_{eg_1}、m_{eg_2} 时,通过正确的 $I_{D_{tag}}$ 无法验证 m_{eg_1}、m_{eg_2} 的正确性,从而识别攻击者假冒。

假设攻击者假冒成 T_{ag} 给 R_{eader} 发消息,攻击者缺少共享秘密值 K 信息,因此攻击者无法正确计算 m_{eg_4} 的值。待 R_{eader} 收到攻击者发送来的消息 m_{eg_4} 之后,R_{eader} 用 K^{new} 或 K^{old} 验证均无法通过,进而识别出发送方是假冒的。

基于上述描述,攻击者假冒 R_{eader} 失败,且假冒 T_{ag} 失败,协议可抵抗假冒攻击。

2)定位攻击。攻击者需要持续对 T_{ag} 发出的消息进行追踪,并进行分析,才可能知道 T_{ag} 具体位置,从而发起定位攻击。消息 m_{eg_3}、m_{eg_4} 中都含有随机数 a、b 将使得每轮值都不同,于攻击者而言,分析发现 T_{ag} 位置处于变动之中,将无法进行定位攻击,从而保障 T_{ag} 位置隐私安全。

3)异步攻击。协议步骤 Step3 中,R_{eader} 一端为防止攻击者发起的异步攻击,R_{eader} 将会采用 K^{new} 或 K^{old} 两种共享秘密值进行验证,并且根据协议步骤描述得知,所用的共享秘密值不同,后续进行秘密值更新操作也不同,从而可恢复 R_{eader} 与 T_{ag} 间暂时的不一致性,攻击者异步攻击失败。

4)双向认证。在 Step2 中,T_{ag} 同时通过 m_{eg_1}、m_{eg_2} 实现对 R_{eader} 的验证;在 Step3 中,R_{eader} 同时通过 m_{eg_3}、m_{eg_4} 实现对 T_{ag} 的验证;在 Step4 中,T_{ag} 通过 m_{eg_5} 实现对 R_{eader} 的验证。于此可知,协议每步骤中,消息接收方都是先验证消息发送方真伪,再进行后续操作。

5)穷举攻击。以消息 $m_{eg_1}=a\oplus I_{D_{tag}}$、$m_{eg_2}=Cro\text{-}Syn(a,a\&I_{D_{tag}})$ 为例进行穷举攻击分析。攻击者可以先对消息 $m_{eg_1}=a\oplus I_{D_{tag}}$ 进行变形处理得到 $a=m_{eg_1}\oplus I_{D_{tag}}$,随后将随机数以及标识符按照相同的计算规则运算得到 $m'_{eg_2}=Cro\text{-}Syn(m_{eg1}\oplus I_{D_{tag}},(m_{eg_1}\oplus I_{D_{tag}})\&I_{D_{tag}})$。在消息 $m'_{eg_2}=Cro\text{-}Syn(m_{eg_1}\oplus I_{D_{tag}},(m_{eg_1}\oplus I_{D_{tag}})\&I_{D_{tag}})$ 中,表面上看,攻击者好像只有 $I_{D_{tag}}$ 一个参数不知晓,攻击者以为可以采用穷举的方式穷举 $I_{D_{tag}}$ 的可能取值,但攻击者是无法成功的。原因在于,根据前文中交叉合成运算的定义可知,在进行加密过程中,还会涉及到每个参数的自身汉明重量,攻击者在不知晓 $I_{D_{tag}}$ 的前提下,更不会知晓 $I_{D_{tag}}$ 自身的汉明重量值,从而使得攻击者不知晓的参数个数瞬间增加好几个,故攻击者穷举攻击失败。

6)后向安全及前向安全。所有消息加密过程中都加入了不同的随机数,随机数具备随机性、互异性、不可预测性等特点,使得攻击者无法从获取的当前会话消息中逆推出上一轮或上几轮加密用到的隐私信息,同时攻击者也无法预测下一轮或未来进行会话时会话消息值,从而确保了用户隐私信息的安全,故协议可提供后向安全及前向安全。

7)重放攻击。攻击者可通过监听的方式获取当前一个完整会话所有消息,并企图在下轮会话开始的时候,假冒其中一方重放监听的上轮消息,达到通过验证的目的,但本文协议中,攻击者无法成功。所有消息加密过程中混入不同个数的随机数,有些消息中仅混入一个,但有些消息中混入两个,使得攻击者找不到任何可分析的规律,使得前后两轮会话消息值完全不同,且无法预测或逆推,攻击者重放攻击失败。

本文协议与其他经典协议之间安全性对比如表 1 所示。表 1 中√表示可以抵抗该种类型攻击,×表示无法抵抗该种类型攻击。

表 1 协议间安全性对比

攻击类型	文献[12]	文献[13]	文献[14]	文献[15]	本文协议
假冒攻击	×	√	√	×	√
定位攻击	√	√	√	√	√
异步攻击	√	√	×	√	√
双向认证	√	√	√	√	√
穷举攻击	√	√	√	√	√
前向安全	√	√	√	√	√
后向安全	√	√	√	√	√
重放攻击	√	×	√	√	√

5 协议性能分析

在 RFID 系统中包含有读卡器、服务器、标签,读

卡器和服务器在计算速度和存储空间方面都有明显的优势,因此这里仅选择标签作为性能分析对象。将从标签一端的存储量、标签一端的计算量、标签一端的随机数产生个数等角度进行展开分析,具体分析结果如表 2 所示。

表 2　协议间性能对比

参考文献	存储量	计算量	随机数个数
文献[12]	$4l$	$3L_a+2L_b+2L_c+1L_h$	1
文献[13]	$2l$	$4L_a+1L_g+2L_c+2L_h$	2
文献[14]	$3l$	$1L_a+3L_f+2L_d+2L_h$	2
文献[15]	$3l$	$3L_a+1L_c+2L_e+1L_h$	1
本文协议	$2l$	$2L_a+2L_i+2L_c+1L_h$	1

表 2 中部分符号的含义如下:L_a 表示 R_LWE 密码体制下的加密函数运算量、L_b 表示 R_LWE 密码体制下的解密函数运算量、L_c 表示按位异或运算的运算量、L_d 表示按位与运算的运算量、L_e 表示按位截联运算的运算量、L_f 表示物理不可克隆函数运算量、L_g 表示模运算的运算量、L_h 表示产生一次随机数的运算量、L_i 表示交叉合成运算的运算量、l 表示消息长度。

在上述不同运算量中,L_c、L_d、L_e、L_i 四种运算均是基于按位运算实现,计算量最小,四者之中 L_i 的计算量相对来说略大;L_a、L_b、L_h 三者运算量大致相当,比上述四种运算的运算量要大,且大很多,其中,L_a 计算量是三者之中略小的;L_f、L_g 两者运算量是所有运算中计算量最大的。

通过上述分析可发现,本文协议在标签一端的计算量方面要远少于文献[13]和文献[14]中计算量;与文献[12]、文献[15]计算量相当,但深入分析会发现,本文协议计算量仍少于文献[12]、文献[15]计算量,原因在于本文协议采用 R_LWE 密码体制下的加密函数计算次数少于其他文献。在标签存储量和随机数个数方面与其他协议大致相当,对比一些经典协议,仍有改进。

6　协议仿真实验

本节主要从两个方面展开仿真实验:面对相同的网络攻击环境,各个协议所达到的安全情况;面对相同的标签数量,各个协议进行认证的时间长短。前者主要用于验证各个协议之间的安全对比,而后者主要用于说明各个协议性能优劣。

进行仿真实验的环境如下:一台惠普笔记本电脑,11th Gen Intel Core i5-1135G7 @ 2.40 GHz 处理器配置,512 GB 固态硬盘、8 GB 内存,MATLAB 软件,所需要的算法用 C 语言编写实现。

根据所学知识可知,实验仿真过程中或多或少将会存在一定误差。为减少误差,在本次仿真实验过程中,相同的环境下、相同的时间点进行 100 次仿真实验,并同时记录该 100 次实验数据,最后计算该 100 次实验数据的平均数值,且将平均数值作为此时刻的最终仿真实验结果。整理数据,绘制表格,最终得到如图 2 所示结果。

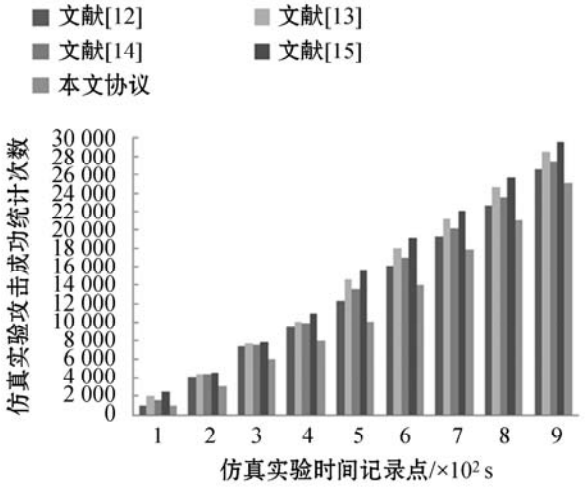


图 2　协议间安全性仿真实验对比

图 2 中,选择文献[12]、文献[13]、文献[14]、文献[15]、本文协议进行安全性角度的仿真实验。横坐标表示仿真实验选择记录仿真实验数据的时间点,从左到右依次为 0、100、200、300、400、500、600、700、800、900 s 时间点的数据。纵坐标表示仿真实验过程中攻击者攻击成功的统计次数,从下往上依次划分为 0、2 000、4 000、6 000、8 000、10 000、12 000、14 000、16 000、18 000、20 000、22 000、24 000、26 000、28 000、30 000 次。

对图 2 进行分析可知,文献[15]中协议在相同情况的网络环境下,面对同样的网络攻击,攻击者成功的次数最多,即表明该协议安全性最糟糕。同时分析可以看出,本文协议则在每次相同的环境下,攻击者攻击成功的次数最少,即表明本文协议具备较高的安全性,可以提供良好的安全需求。

在上述相同的配置环境下继续完成性能相关的仿真实验。同样为了减少误差所带来的实验影响,每次仿真实验次数仍为 100 次,仍记录 100 次仿真实验数据,并求取 100 次仿真实验数据平均值,且将平均值作为最终该次实验数据。整理最终所有数据,绘制出如图 3 所示的仿真实验认证时间长短对比。

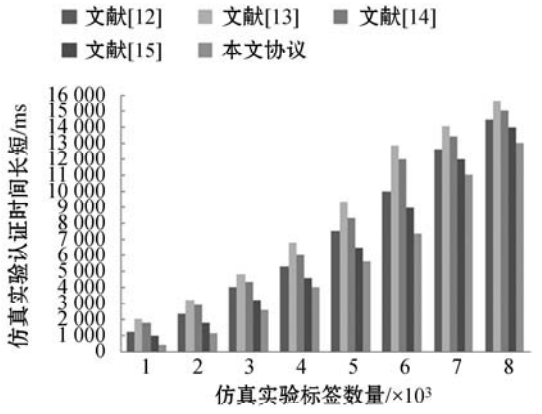


图 3 协议间认证时间长短仿真实验对比

在图 3 中,仍然选择文献[12]、文献[13]、文献[14]、文献[15]、本文协议为对象,进行性能角度仿真实验。图 3 中的横坐标表示仿真实验进行时,参与验证的标签数量,从左往右标签数量依次选择 100、200、300、400、500、600、700、800 个。纵坐标则表示仿真实验环境下通信认证时间总长度,从下往上依次选择分段为 0、1 000、2 000、3 000、4 000、5 000、6 000、7 000、8 000、9 000、10 000、11 000、12 000、13 000、14 000、15 000、16 000 ms。

对图 3 进行分析可知,本文协议不论标签数量多少时,通信认证所需总时间长度最短;同时文献[13]所用时间最长。分析原因如下:文献[13]中协议除了用到 R_LWE 密码体制的加密函数,同时还用到计算量较大的模运算,因此在众多对比协议中,文献[13]中协议计算量最大,导致通信认证时间自然最长。本文协议只用到 R_LWE 密码体制的加密函数,未用到其他计算量大的算法,再加上交叉合成运算的计算量则属于超轻量级的,使得本文协议计算量方面最优,因此仿真实验显示通信认证时间最短。

上述仿真实验表明本文协议不论是在安全性角度,还是在计算量等性能角度,与所对比的协议均存在一定优势。

7 结 语

分析 RFID 系统中存在的问题,并重点分析刘涛等设计的协议,在其协议框架基础之上给出一种改进的基于 R_LWE 密码体制的双向认证协议。R_LWE 密码体制具备加解密速度快、计算量小等优点,在确保隐私信息安全的同时,还可一定程度上减少计算量;为进一步减少标签一端的计算成本,标签一端只采用 R_LWE 密码体制加密,计算量较大的解密过程则在读卡器一端完成,同时协议加密过程中引入交叉合成运算,标签对读卡器的验证可基于交叉合成运算实现,可确保安全性。将本文协议与其他经典协议从不同攻击类型对比分析,本文协议具备较高的安全性;综合分析不同协议标签一端计算量、存储量等指标,表明本文协议计算方面优于对比协议,具备一定推广价值。

参 考 文 献

[1] 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.

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

[3] Fan K, Jiang W, Li H, et al. Lightweight RFID protocol for medical privacy protection in IoT[J]. IEEE Transactions on Industrial Informatics,2018,14(4):1656 - 1665.

[4] 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.

[5] Molnar D, Soppera A, Wagner D. A scalable, Delegatable pseudonym protocol enabling ownership transfer of RFID tags [C]//12th International Workshop on Selected Areas in Cryptography,2006:276 - 290.

[6] 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.

[7] Xie R, Ling J, Liu D W. A wireless key generation algorithm for RFID system based on bit operation[J]. International Journal of Network Security,2018,20(5):938 - 950.

[8] 罗韶杰,张立臣. 改进的基于位运算的 RFID 标签所有权转移协议[J]. 兵器装备工程学报,2019,40(8):157 - 164.

[9] Regev O. On lattices, learning with errors, random linear codes, and cryptography[C]//37th Annual ACM Symposium on Theory of Computing,2005.

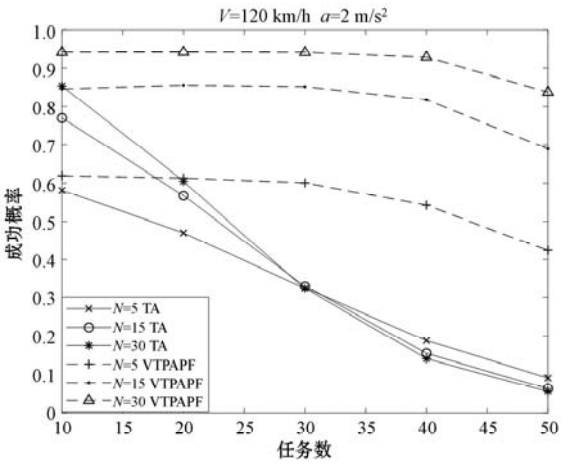
[10] Ajtai M, Dwork C. A public-key cryptosystem with worst-case average-case equivalence[C]//29th Annual ACM Symposium on Theory of Computing,1997:284 - 293.

[11] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings[C]//29th Annual International Conference on the Theory and Applications of Cryptographic Techniques,2010.

[12] Wang J Q, Zhang Y F, Liu D W. Provable secure for the ultra-lightweight RFID tag ownership transfer protocol in the context of IoT commerce[J]. International Journal of Network Security,2020,22(1):12 - 23.

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

(下转第 397 页)



(e)

图 2　不同速度下任务执行的成功率

4　结　语

本文设计基于移动边缘计算的车联网网络架构,构建车辆预测机制。由于 MEC 资源的有限性该机制主要针对低时延且小任务量,研究车辆行驶过程与 RSU 之间的连接,其核心思想是采用粒子滤波对车辆进行移动预测,通过预测位置选择连接最合适的 RSU,保证车辆与 RSU 之间信息传输顺利进行。本文成功解决了车联网中车辆快速行驶时连接不稳定的问题。仿真结果表明,本文方案从 RSU 数量、任务处理数量、车辆移动速度等多方面验证 VTPAPF 的有效性。

参　考　文　献

[1] 施巍松,张星洲,王一帆,等. 边缘计算:现状与展望[J]. 计算机研究与发展,2019,56(1):69 – 89.

[2] 施巍松,孙辉,曹杰,等. 边缘计算:万物互联时代新型计算模型[J]. 计算机研究与发展,2017,54(5):907 – 924.

[3] 李林哲,周佩雷,程鹏,等. 边缘计算的架构挑战与应用[J]. 大数据,2019,5(2):3 – 16.

[4] Chen C, Wang C, Qiu T, et al. Caching in vehicular named data networking: Architecture, schemes and future directions [J]. IEEE Communications Surveys & Tutorials, 2020, 22 (4):2378 – 2407.

[5] Liu L, Chen C, Pei Q, et al. Vehicular edge computing and networking: A survey[J]. Mobile Networks and Applications,2020,26:1 – 24.

[6] Ojima T, Fujii T. Resource management for mobile edge computing using user mobility prediction[C]//International Conference on Information Networking,2018:718 – 720.

[7] Zhang K, Mao Y M, Leng S P, et al. Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading[J]. IEEE Vehicular Technology Magazine,2017,12(2):36 – 44.

[8] Yang C, Liu Y, Chen X, et al. Efficient mobility-aware task offloading for vehicular edge computing networks[J]. IEEE Access,2019,7:26652 – 26664.

[9] 王秋宁,谢人超,黄韬. 移动边缘计算的移动性管理研究[J]. 中兴通讯技术,2018,24(1):37 – 41.

[10] 刘亮,刘星,曾帅,等. 移动边缘计算中基于用户移动的虚拟机迁移策略研究[J]. 重庆邮电大学学报(自然科学版),2019,31(2):158 – 165.

[11] 吴迪,凌艳,朱红松,等. VANET 中解决 RSU 接入问题的演化博弈方法:CN103458482A[P]. 2013 – 05 – 28.

[12] Aranaud D, Simon G, Christophe A. On sequential monte Carlo sampling methods for Bayesian filtering[J]. Statistics and Computing,2000,10(3):197 – 208.

[13] 贺利乐,陈奕昕,贺宁,等. 基于粒子滤波的管道泄漏检测与定位方法[J]. 控制工程,2021,28(4):787 – 798.

[14] 秦川,陶忠,桑蔚,等. 基于粒子滤波的运动目标光电定位仿真研究[J]. 应用光学,2020,41(1):10 – 17.

[15] 姚婷,郭永峰,樊顺厚,等. 非高斯噪声激励下非线性漂移 Fokker-Planck 方程的非稳态解及其应用[J]. 工程数学学报,2020,37(3):303 – 313.

[16] 吴迪. 基于线性回归模型的贝叶斯方法的应用[D]. 长春:长春理工大学,2020.

[17] 张媚,焦巍. 基于粒子滤波的雷达海面目标检测前跟踪算法[C]//第六届高分辨率对地观测学术年会,2019:16.

[18] Zhang J Y, Deng B L, Hong Y, et al. Static/Dynamic filtering for mesh geometry[J]. IEEE Transactions on Visualization and Computer Graphics,2019,25(4):1774 – 1778.

[19] 赖际舟,熊剑,刘建业,等. 分层近似粒子滤波及其在陀螺寻北中的应用[J]. 仪器仪表学报,2011,32(10):2342 – 2347.

[20] Makhdum M, Sanaullah A, Muhammad H. A modified regression-cum-ratio estimator of population mean of a sensitive variable in the presence of non-response in simple random sampling[J]. Journal of Statistics and Management Systems, 2020,23(3):495 – 510.

(上接第 378 页)

[14] 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.

[15] 刘涛,贾浪峰,郭苹. 基于 R_LWE 密码体制的 RFID 认证协议研究[J]. 机床与液压,2021,49(13):13 – 18.

[16] Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption[C]//Topics in Cryptology-CT-RSA 2011,2011:319 – 339.

[17] Jiang Q, Chen Z R, Li B Y, et al. Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems[J]. Journal of Ambient Intelligence and Humanized Computing,2018,9 (4):1061 – 1073.