

湖南大学学报(自然科学版)

Journal of Hunan University(Natural Sciences)

ISSN 1674-2974,CN 43-1061/N

《湖南大学学报(自然科学版)》网络首发论文

题目： 基于 PUF 实现物联网设备的轻量级密钥共享协议
作者： 王振宇，李少青，郭阳，曾健平
DOI： 10.16339/j.cnki.hdxzbzkb.2022352
收稿日期： 2021-11-11
网络首发日期： 2022-05-07
引用格式： 王振宇，李少青，郭阳，曾健平. 基于 PUF 实现物联网设备的轻量级密钥共享协议[J/OL]. 湖南大学学报(自然科学版).
<https://doi.org/10.16339/j.cnki.hdxzbzkb.2022352>



网络首发：在编辑部工作流程中，稿件从录用到出版要经历录用定稿、排版定稿、整期汇编定稿等阶段。录用定稿指内容已经确定，且通过同行评议、主编终审同意刊用的稿件。排版定稿指录用定稿按照期刊特定版式（包括网络呈现版式）排版后的稿件，可暂不确定出版年、卷、期和页码。整期汇编定稿指出版年、卷、期、页码均已确定的印刷或数字出版的整期汇编稿件。录用定稿网络首发稿件内容必须符合《出版管理条例》和《期刊出版管理规定》的有关规定；学术研究成果具有创新性、科学性和先进性，符合编辑部对刊文的录用要求，不存在学术不端行为及其他侵权行为；稿件内容应基本符合国家有关书刊编辑、出版的技术标准，正确使用和统一规范语言文字、符号、数字、外文字母、法定计量单位及地图标注等。为确保录用定稿网络首发的严肃性，录用定稿一经发布，不得修改论文题目、作者、机构名称和学术内容，只可基于编辑规范进行少量文字的修改。

出版确认：纸质期刊编辑部通过与《中国学术期刊（光盘版）》电子杂志社有限公司签约，在《中国学术期刊（网络版）》出版传播平台上创办与纸质期刊内容一致的网络版，以单篇或整期出版形式，在印刷出版之前刊发论文的录用定稿、排版定稿、整期汇编定稿。因为《中国学术期刊（网络版）》是国家新闻出版广电总局批准的网络连续型出版物（ISSN 2096-4188，CN 11-6037/Z），所以签约期刊的网络版上网络首发论文视为正式出版。

基于 PUF 实现物联网设备的轻量级密钥共享协议

王振宇¹, 李少青¹, 郭阳¹, 曾健平²

(1. 国防科技大学 计算机学院, 湖南 长沙 410000)

(2. 湖南大学 物理与微电子科学学院, 湖南 长沙 410000)

摘要：物联网作为一种新型通信网络的发展与应用, 承载着大量敏感信息的安全传输与存储. 由于物联网设备资源有限, 通信开销大、传输速率慢且需存储敏感信息的安全原语(如公钥算法、数字签名等)不适用于轻量级设备的认证. 本文利用硬件物理不可克隆函数(PUF)所具备防篡改防克隆的特性来生成共享密钥, 结合 MASK 算法、Hash 函数等安全原语, 为物联网设备提出一种轻量级匿名密钥共享认证协议. 通过 Ban 逻辑和形式化工具 ProVerif 进行安全分析验证, 证明该协议能够防御中间人攻击、去同步攻击、假冒攻击、建模攻击等. 通过对比其他协议, 该协议具备计算成本低、通信开销和存储容量小以及安全性能高的特点, 适合于资源受限设备的安全通信传输.

关键词：物理不可克隆函数; 轻量级; 密钥共享; 认证协议

中图分类号：TN918

文献标志码：A

A Lightweight Key Sharing Protocol for IoT Devices based on PUF

WANG Zhenyu¹, LI Shaoqing¹, GUO Yang¹, ZENG Jianping²

(1. College of Computer Science and Technology, National University of Defense Technology, Changsha 410000, China)

(2. School of Physics and Microelectronics Science, Hunan University, Changsha 410000, China)

Abstract: With the development and application of communication networks, the Internet of Things carries the safe transmission and storage of a large amount of sensitive information. Since devices are usually small in size and resource-constrained, complex security primitives are not suitable for authentication of lightweight IoT devices. This paper proposes a lightweight anonymous key shared authentication protocol for IoT devices, which generates a shared key by the physical unclonable function(PUF) and uses security primitives such as the MASK algorithm and the Hash function. The security analysis and verification are accomplished by Ban logic and ProVerif to prove that the protocol ensures security attributes such as anonymity, non-repudiation, and forward/backward confidentiality. Compared with other protocols, this protocol has the characteristics of low computing cost, small communication overhead and storage capacity, and high security performance, which is suitable for the secure communication transmission of resource-constrained devices.

Key words: Physical unclonable function; Lightweight; Key sharing; Authentication protocol

收稿日期：2021-11-11

基金项目：国家自然科学基金资助项目(61832018), National Natural Science Foundation of China(61832018)

作者简介：王振宇(1995—), 男, 湖南岳阳人, 国防科技大学博士研究生

*通信联系人, E-mail: wangzhenyu19a@nudt.edu.cn

随着传感、自动化和通信技术的飞速发展,物联网(Internet of Things, IoT)产生海量数据给设备之间有效安全传输、存储与保护带来了巨大的威胁^[1].传统的网络安全协议会采用加密算法^[2]、数字签名、Hash 函数^[3]、消息验证码等复杂安全原语来保证信息传输的机密性、完整性以及不可否认性等^[4].由于物联网设备通常体积小、资源约束且硬件处理能力低,因此传输速率慢、通信开销大的安全原语不适合轻量级设备的认证^[5].

目前物联网的安全通信是假设硬件设备与系统是安全的,但是恶意攻击者可以通过芯片克隆、解剖等手段来破坏设备保密信息^[6].信息加密是保护信息安全认证的有效途径,但是加密算法的密钥通常存储在非易失性存储器(NVM)中,攻击者通过侧信道和物理攻击,可以成功读取存储器中的私密信息^[7].物理不可克隆函数(PUF)作为一种新兴的硬件安全原语,利用芯片在制造过程中无法控制的随机工艺偏差,来产生器件独有的数字签名^[8].PUF 采用特定的“激励-响应”(CRP)机制触发可以实时生成安全密钥,对物理篡改非常敏感,无需存储,硬件开销小,解决传统密钥面临的安全问题,并且适用于轻量级物联网设备安全认证协议^[9-11].

密钥共享认证协议通常在软件层采用公钥算法与数字签名完成,但是这些加密原语运行速度慢,通信开销大,且新型量子计算方法能够有效对公钥算法进行破解.为解决物联网设备在信道传输以及密钥存储的安全性问题,本文采用可重构 CRO PUF 防篡改防克隆的特性生成共享密钥,取代通信开销大的非对称加密算法和数字签名,结合 MASK 算法、Hash 函数等加密方法提出一种轻量级密钥共享安全认证协议.该协议确保匿名性,可用性,完整性、前向/后向保密性等安全属性.

1 数学理论知识与相关工作

1.1 基于PUF的密钥共享机制

Zhang 等人^[12]采用 CRO PUF 为设备生成相同的共享密钥,适用于一对多的安全认证协议.该机制通过两次阶段来获得设备之间的共享密钥.

阶段 1: 生成共享密钥的可靠响应.通过建模获取 CRO PUF 的高精度延迟矩阵 R : 计算所有路径之间的延迟差并按绝对值降序排序.考虑不

同温度的影响来确定阈值 T ,当两条路径之间的延迟差绝对值大于阈值时,则输出响应是稳定的.

阶段 2: 生成共享密钥的激励.将延迟矩阵 R 的所有路径存入集合 D ,列举共享密钥 K 的所有位.从集合 D 中随机选择两条不同的路径,对于共享密钥 K_i 的每一位,如果 K_i 等于 1 且延迟差大于 T ,则表示找到一个可以产生稳定响应 1 的配置激励 C_i ; 如果 K_i 等于 0 且延迟差小于 $-T$,则表示找到一个可以生成稳定响应 0 的配置激励 C_i ; 否则,重新选择共享密钥 K .

1.2 MASK 与 UNMASK 算法

Qureshi 等人^[13]提出的 MASK 算法包含三个参数: 长度 l 位的输入向量 $r = [r_1, r_2, r_3, \dots, r_l]$ 、 l 个正整数集 $K = \{k_1, k_2, k_3, \dots, k_l \mid k_i \in \mathbf{Z}^+\}$ 、以及产生 l 位的输出向量 $r_m = [r_{m1}, r_{m2}, r_{m3}, \dots, r_{ml}]$.MASK 算法是采用正整数集 K 作为辅助数据,将长度 l 位输入向量 r 生成一个等长度的输出函数 r_m .正整数集 K 是通过伪随机数发生器生成 $K \leftarrow \text{PRNG}_i(y)$,其中 y 是长度 n 位的输入向量 $y = [y_1, y_2, y_3, \dots, y_n]$.类似地, MASK 函数的可逆变换 UNMASK 函数,使用正整数集 K 将输出函数复原 r_m 为输出函数 r .其转换表达式如下:

$$\text{MASK}(r, K) : r \Rightarrow r_m$$

$$\text{UNMASK}(r_m, K) : r_m \Rightarrow r$$

算法 1 (Algorithm 1)总结了 MASK 函数的运算过程,包括整数集生成、函数范围变换和位混淆等三个步骤.其具体过程如下所示:

Algorithm 1: Mask 算法过程

```

输入 :
    l 位输入向量 x
    n 位输入向量 y
输出 :
    l 位输入向量 x_m
1: produce MASK(x, y)
2: interger Set K : {k_1, k_2, k_3, ... k_m} → PRNG_1(y)
3: for i ← 1 to m do
4:   N_new ← RANGE(k_i, m + 1 - i)
5:   x ← SWAP(x_new, x_{m-i+1})
6:   x_m ← x
7: end for
8: end procedure
    
```

1) **整数集生成:** 向量 y 作为伪随机数发生器 PRNG 电路的种子生成一组正整数 $K = \{k_1, k_2, k_3, \dots, k_l \mid k_i \in \mathbf{Z}^+\}$. 整数集 K 包含 l 个 n 位正整数,任何一位正整数得最大值为 $2^n - 1$.

2) **函数范围变换:** 定义一个范围函数 Range() 为线性映射变换,给定一个 l 位整数 $\{k \mid k \in K\}$,其取值范围在 $[0, 2^l - 1]$,生成一个 m 位的新集合 $Q = \{q \mid q \in \mathbf{Z}^+\}$,其整数范围在 $[0, 2^m - 1]$ 其 $m \leq l$.线性范围映射由以下等式控制:

$$N_{\text{new}} = \left[\frac{(N_{\text{old}} - N_{\text{oldmin}}) \times (N_{\text{newmax}} - N_{\text{newmin}})}{(N_{\text{oldmax}} - N_{\text{oldmin}})} \right]$$

$N_{old} \in K$ 是 $\text{Range}()$ 函数的输入, N_{oldmin} 与 N_{oldmax} 是在范围 $[0, 2^l - 1]$ 内的最小值与最大值, N_{newmin} 与 N_{newmax} 是在新范围 $[0, 2^m - 1]$ 内的最小值与最大值.

3) **位混淆**: MASK 函数最后是基于 Fisher-Yates Shuffler 洗牌算法完成序列的位混淆, n 个不同元素的有限序列生成一个 $n!$ 个随机排列的算法.

MASK 算法有两个优点: 1) 它有效地隐藏了设备 PUF 激励与响应之间的关系; 2) 它为设备的输入提供了验证. 在不验证输入流的情况下, PUF 不会被激活, 因此设备不会产生任何响应, 这有效地防止了设备受到任何蛮力攻击.

2 协议设计与分析

本文基于嵌入 PUF 的物联网设备提出一种轻量级密钥共享认证协议, 包括协议注册阶段和双向认证与固件更新阶段. 协议相关符号如表 1 所示.

表 1 协议相关符号说明

Tab.1 Symbol Description

符号	含义
$CRO\ PUF$	可重构环形振荡器 PUF
$Delay\ Matrix\ M_A / M_B$	延时矩阵 M_A 或 M_B
(C, R)	PUF 产生的激励 C 与响应 R
$timestape()$	时间戳函数
(n_{i1}, n_{i2})	伪随机数
$\text{Hash}(\bullet)$	单向哈希函数
Fisher - Shuffler()	洗牌混淆算法
$\text{PRNG}() / \text{TRNG}()$	伪/真随机数发生器

2.1 协议注册阶段

协议的注册阶段采用 Zhang 等人^[12]所提出的基于可重构 CRO PUF 的密钥共享机制, 解决传统网络协议中公钥算法的开销大、处理速度低、以及密钥存储的安全问题. 注册阶段是在安全信道中传输, 执行算法 1, 如图 1 所示.

算法 1: 注册阶段

```

1: Device.PUFA, Device.PUFB ← Select.Device()
2: IDA, IDB ← Decide.random()
3: Delay.MatrixA, Delay.MatrixB ← Device.PUFA, Device.PUFB
4: TA, TB ← Algorithm1(Delay.MatrixA, Delay.MatrixB)
5: Shared.key R ← Server.random()
6: Challenge CA, CB ← Algorithm2{(TA, CA), (TA, CB)}
7: Store (CA, IDA), (CB, IDB)
    
```

1) 设备 A 与设备 B 通过建模 CRO PUF 分别获得延时矩阵 M_A 与延时矩阵 M_B , 并且将该延时矩阵发送到可信服务器 S.

2) 服务器 S 采用 1.1 中阶段 1 来获得稳定的响应值. 通过 PUF 的延时矩阵计算出所有路径之间的延迟差, 并将差值按降序排列得到延时期列 (T_A, T_B) . 通过阶段 2 与共享密钥 R 来获得 PUF_A 与 PUF_B 的激励 (C_A, C_B) , 即 $\{\text{PUF}(C_A) = \text{PUF}(C_B) = R, \text{其 } C_A \neq C_B\}$ 并存储于服务器中.

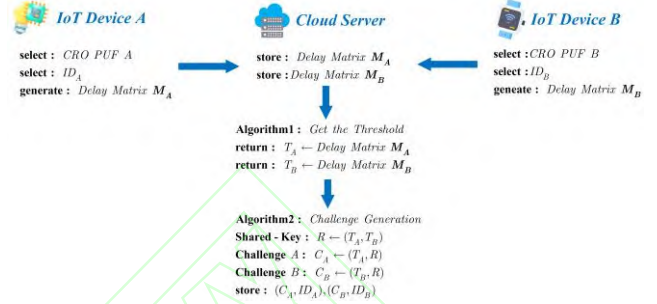


图 1 协议注册阶段

Fig.1 Registration phase of the proposed protocol

2.2 双向认证与固件更新阶段

双向认证与固件更新阶段是 PUF 产生的共享密钥在不安全的信道中完成设备之间的安全认证, 执行算法 2, 认证流程如图 2 所示.

1) 设备 A 与 B 记录当时时刻的时间戳 (T_1, T_2) , 分别作为随机数发生器的种子产生两对随机值 (n_{A1}, n_{A2}) 与 (n_{B1}, n_{B2}) , 并且发送到服务器 S.

2) 当服务器 S 接收到设备的随机值, 通过 MASK 算法保护 PUF 所产生的激励值 C_A 与 C_B , 即 $D_A = \text{MASK}(C_A, \text{PRNG}(n_{A1}))$ 与 $D_B = \text{MASK}(C_B, \text{PRNG}(n_{B1}))$. 然后将 D_A, n_{B2} 和 D_B, n_{A2} 分别发送到设备 A 与设备 B.

算法 2: 认证与固件更新阶段

```

1: (T1, T2) ← Device.timestape()
2: (nA1, nA2), (nB1, nB2) ← Device.TRNGA(T1), Device.TRNGB(T2)
3: Server ← Device.(nA1, nA2), Device.(nB1, nB2)
4: (KA, KB) ← Server.PRNG(nA1), Server.PRNG(nB1)
5: (DA, DB) ← Server.MASK(CA, KA), Server.MASK(CB, KB)
6: Update (Rnew, CAnew, CBnew)
7: Device.A, Device.B ← Server.(DA, nB2), Server.(DB, nA2)
8: (CA, CB) ← Device.UNMASKA(DA, PRNG(nB2)), Device.UNMASKB(DB, PRNG(nA2))
9: (RA, RB) ← Device.PUFA(CA), Device.PUFB(CB)
10: (rA1, rA2), (rB1, rB2) ← Device.Fisher-shuffler(RA, RB)
11: (dA, dB) ← Device.HashA(rA1, PRNG(nB2)), Device.HashB(rB1, PRNG(nA2))
12: Device.A ← dB, Device.B ← dA
13: rB2 ← Device.HashA(rA2, PRNG(nA2)), rA1 ← Device.HashB(rB1, PRNG(nB2))
14: if (dB, rB2) ≤ Device.εA, if (dA, rA1) ≤ Device.εB
15: else abort
16: Update (T1new, T2new) ← Device.timestape()
17: (nA1new, nA2new), (nB1new, nB2new) ← Device.TRNGA(T1new), Device.TRNGB(T2new)
18: Store (nA1old, nA2old), (nB1old, nB2old)
    
```

- 3) 设备 A 通过随机数 n_{A1} 解析激励 C_A , 即 $C_A \leftarrow \text{UNMASK}(D_A, \text{PRNG}(n_{A1}))$, 再通过 PUF 计算出响应值 R_A . 同样, 设备 B 通过随机数 n_{B1} 解析激励 C_B 并计算出响应值 R_B .
- 4) 通过 Fisher - Shuffler 洗牌混淆算法分别将响应 R_A 与 R_B 分解为 (r_{A1}, r_{A2}) 与 (r_{B1}, r_{B2}) , 该算法高效且等概率生成随机序列. 设备 A 通过随机数 n_{B2} 计算 PUF 响应值 r_{A1} 的 Hash 值, 即 $d_A \leftarrow \text{Hash}(r_{A1}, \text{PRNG}(n_{B2}))$; 同样, 设备 B 计算出 Hash 值.
- 5) 当设备 A 接收到数据 d_B 之后, 计算 \tilde{r}_{B2}
- 6) 当服务器 S 完成对设备激励 C_A 与 C_B 的发送, 则更新密钥 R^{new} 和激励对 (C_A^{new}, C_B^{new}) .
- 7) 设备记录时间戳来更新随机数, 从而设备 A 与 B 分别产生新的随机对 $(n_{A1}^{new}, n_{A2}^{new})$ 与 $(n_{B1}^{new}, n_{B2}^{new})$, 并且存储旧的随机值 $(n_{A1}^{old}, n_{A2}^{old})$ 与 $(n_{B1}^{old}, n_{B2}^{old})$.

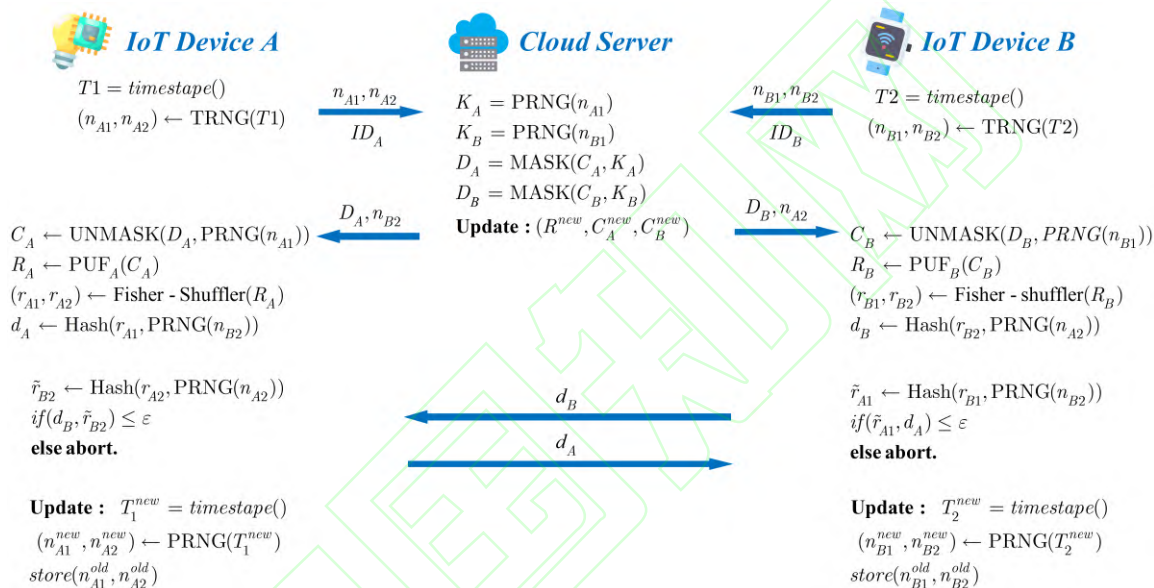


Fig.2 Authentication and Update phase of the proposed protocol

3 形式化安全证明

3.1 形式化安全分析

该协议保证物联网设备的信道传输安全, 也可以防御攻击者对 PUF 进行物理攻击. 其具体安全分析如下:

1) **建模攻击.** 机器学习建模攻击是针对具有可公开访问的 CRP 接口的强 PUF, 攻击者通过收集大量 CRP, 训练、学习和优化一个精确的模型, 从而在给定的激励中预测出响应. 但是, 本文采用可重构 CRO PUF 是用作密钥生成的弱 PUF, 没有访问接口来读取芯片内部生成的密钥, 密钥不会暴露给攻击者. 同时, 由于协议机制的保护, 通过 MASK 算法保护 (C_A, C_B) 值, 以及 Fisher - Shuffler 混淆算法将响应值分为两部分 (r_{A1}, r_{A2}) 与 (r_{B1}, r_{B2}) , 同时采用 Hash 算法与随机数发生器保护设备其中部分的响应值 r_{A1} . 由于 Hash 函数单向性的特点, 攻击者通过窃听内容 d_A 获取不到真实的 CRP 值,

因此, 攻击者很难对 PUF 进行机器学习建模攻击.

2) **不可追溯性.** 在物联网设备认证过程中, 如果攻击者无法对两次有效的身份认证请求和响应相关联, 则认为设备是无法追踪的. 攻击者通过窃听获取消息 D_A 与 D_B 时, 因为激励 C_A 与 C_B 通过 MASK 函数进行加密防护, 攻击者不能推断出激励 C_A 与 C_B 的值. 攻击者窃听消息 d_A 与 d_B 之后, 即 $d_A \leftarrow \text{Hash}(r_{A1}, \text{PRNG}(n_{B2}))$, $d_B \leftarrow \text{Hash}(r_{B2}, \text{PRNG}(n_{A2}))$. 由于哈希函数单一性, 攻击者不能获取共享密钥 R_A 与 R_B 的值. 因此该协议可以防止位置跟踪.

3) **去同步攻击.** 在协议的更新阶段, 设备端产生新的随机数 $(n_{A1}^{new}, n_{A2}^{new})$ 与 $(n_{B1}^{new}, n_{B2}^{new})$, 同时也存储上一轮认证的随机数 $(n_{A1}^{old}, n_{A2}^{old})$ 与 $(n_{B1}^{old}, n_{B2}^{old})$. 当设备 B 被去同步攻击时, 设备 A 的随机数会正常更新, 但是设备 B 的随机数不会进行更新. 当进行下一轮认证, 服务器会返回值 D_A, n_{B2}^{old} 给设备 A, 同时返回值 D_B, n_{A2}^{new} 给设备 B. 由于设备 A 所返回的验证值 d_A^{old} 与上一轮认证一致, 而设备 B 返回的 d_B^{new} 与上一轮不同. 因此可以检测出设备之间未同步.

4) **重放攻击**.该协议机制采用时间戳和更新的随机数 (n_{A1}, n_{A2}) 与 (n_{B1}, n_{B2}) 来防御重放攻击.以设备 A 认证为例,假定第 i 次和 $i+1$ 次的随机数分别为 (n_{A1}^i, n_{A2}^i) 与 $(n_{B1}^{i+1}, n_{B2}^{i+1})$,当攻击者获得第 i 次的会话消息 D_A^i, d_B^i 之后,进行第 $i+1$ 认证时,设备 A 收到的会话消息已经更新为 D_A^{i+1}, d_B^{i+1} ,因此,攻击者认证将会失败,重放攻击将被检测.

5) **假冒攻击**.当攻击者伪装成合法设备时,需要发送有效消息 d_A 与 d_B .以设备 A 为例,因为信息 d_A 的生成需要有效的 r_{A1} ,通过 MASK 函数来保护 PUF 的输入激励 C_A ,同时通过混淆算法将响应 R_A 进行防护.由于 Hash 函数具有单一性,获得信息 d_A 仍然不能得到有效信息 r_{A1} .因此在该协议机制中,攻击者不能假冒成合法设备与服务器认证.同理,当攻击者伪装成服务器时,也不能获取激励 C_A 与 C_B 的值,从而不能与设备相互认证.

6) **中间人攻击**.该协议可以对中间人攻击进行防御,攻击者窃听消息 $D_A, n_{B2}, D_B, n_{A2}, d_A$ 与 d_B 是不能获取有效信息.因为所窃听的消息都是加密后的信息,攻击者若替换新的消息之后,从而设备之间将不能识别导致认证失败.若攻击者想解析加密后的信息,由上面假冒攻击可知,攻击者不能获取 PUF 的 CRP 对 (C_A, R_A) ,因此设备之间认证会失败.

3.2 协议证明

本节使用 BAN 逻辑来证明 PUF 产生共享密钥的安全性.BAN 逻辑是认证协议形式化分析方法,可以提示一些非形式化方法很难发现的缺陷.BAN 逻辑中常用的逻辑符号如表 2 所示,与本节相关的 BAN 逻辑常用的逻辑规则如表 3 所示.

表 2 BAN 逻辑中常用的逻辑符号

Tab.2 Symbols Description in BAN logic

$P \models X$: P 相信 X 是真实的;	$P \vdash X$: 实体 P 对 X 有管辖权;
$P \sim X$: P 曾经发送消息 X;	$\#(X)$: X 是新鲜的;
$P \triangleleft X$: 实体 P 收到消息 X;	(X, Y) : X 或 Y 是 (X, Y) 一部分
$\{X\}_K$: 使用密钥 K 对消息 X 执行加密操作;	$P \xrightarrow{K} Q$: K 是 P 和 Q 之间的共享密钥;

表 3 BAN 逻辑常用的逻辑规则

Tab.3 Common logic rules of BAN logic

规则说明	逻辑表达式
规则 1: 消息含义规则	$\frac{P \models P \xrightarrow{K} Q, P \triangleleft \{X\}_K}{P \models Q \sim X}$
规则 2: 新鲜性规则	$\frac{P \models \#(X)}{P \models \#(X, Y)}$
规则 3: 临时值校验规则	$\frac{P \models \#(X), P \models Q \sim X}{P \models Q \models X}$
规则 4: 信任规则	$\frac{P \models Q \models (X, Y)}{P \models Q \models X}$

为便于分析,将设备 A 与 B 表示为 $D1$ 与 $D2$,服务器表示为 S,对协议进行理想化后,消息发送规则调整如下:

- M1: $D1 \rightarrow S : n_{A1}, n_{A2}$; M2: $D2 \rightarrow S : n_{B1}, n_{B2}$
M3: $S \rightarrow D1 : \{c_A, n_{A1}\}_{n_{A1}}, n_{B2}$; M4: $S \rightarrow D2 : \{c_B, n_{B1}\}_{n_{B1}}, n_{A2}$
M5: $D1 \rightarrow D2 : \{r_{A1}, n_{B2}\}_{n_{B2}}$; M6: $D2 \rightarrow D1 : \{r_{B1}, n_{A2}\}_{n_{A2}}$

协议初始化假设如下:

- A1: $D1 \models \#(n_{A1}, n_{A2})$ A2: $D2 \models \#(n_{B1}, n_{B2})$
A3: $D1 \models D1 \xleftarrow{n_{A1}} S; D1 \models D1 \xleftarrow{n_{A2}} S$
A4: $D2 \models D2 \xleftarrow{n_{B1}} S; D2 \models D2 \xleftarrow{n_{B2}} S$
A5: $D1 \models D1 \xleftarrow{n_{A2}} D2; D2 \models D1 \xleftarrow{n_{B2}} D2$

目标公式如下:

- G1: $D1 \models S \models \{c_A\}$; G3: $D2 \models D1 \models \{r_{A1}\}$;
G2: $D2 \models S \models \{c_B\}$; G4: $D1 \models D2 \models \{r_{B1}\}$;

如果目标公式成立,则说明设备与服务器 S 都与对方协商并确认秘密密钥,并且秘密密钥与平台完整性报告及通信信道绑定.逻辑推理如下:

由规则 1 与 A3、M3 可知:

$$\frac{D1 \models D1 \xleftarrow{n_{A1}} S, D1 \triangleleft \{c_A, n_{A1}\}_{n_{A1}}}{D1 \models S \sim \{c_A, n_{A1}\}} \quad (1)$$

由规则 2 与 A1 可知:

$$\frac{D1 \models \#(n_{A1})}{D1 \models \#(c_A, n_{A1})} \quad (2)$$

由规则 3 与消息 (1) 与 (2) 可知:

$$\frac{D1 \models \#(c_A, n_{A1}), D1 \models S \sim \{c_A, n_{A1}\}}{D1 \models S \models \{c_A, n_{A1}\}} \quad (3)$$

由规则 4 与消息 (3) 可知:

$$\frac{D1 \models S \models \{c_A, n_{A1}\}}{D1 \models S \models \{c_A\}} \quad (4)$$

因此,可证得目标公式 G1: $D1 \models S \models \{c_A\}$,设备 A 与服务器 S 共享密钥 c_A .

由规则 1 与 A4、M4 可知:

$$\frac{D2 \models D2 \xleftarrow{n_{B1}} S, D2 \triangleleft \{c_B, n_{B1}\}_{n_{B1}}}{D2 \models S \sim \{c_B, n_{B1}\}} \quad (5)$$

由规则 2 与 A2 可知:

$$\frac{D2 \models \#(n_{B1})}{D2 \models \#(c_B, n_{B1})} \quad (6)$$

同理,由规则 3 和 4,与式 (5), (6) 可证明目标公式: $G2: D2 \models S \models \{c_B\}$.

由规则 1 与 A5、M5 可知:

$$\frac{D2 \models D1 \xleftarrow{n_{B2}} D2, D2 \triangleleft \{r_{A1}, n_{B2}\}_{n_{B2}}}{D2 \models D1 \sim \{r_{A1}, n_{B2}\}} \quad (7)$$

由规则 2、3 与消息 A2、(7) 可知:

$$\frac{D2 \models \#\{r_{A1}, n_{B2}\}, D2 \models D1 \sim \{r_{A1}, n_{B2}\}}{D2 \models D1 \models \{r_{A1}, n_{B2}\}} \quad (8)$$

由规则 4 与消息 (8) 可知:

$$\frac{D2 \models D1 \models \{r_{A1}, n_{B2}\}}{D2 \models D1 \models \{r_{A1}\}} \quad (9)$$

因此,可证得目标公式 G3: $D2 \models D1 \models \{r_{A1}\}$,设备 B 与设备 A 共享密钥 r_{A1} .

由规则 1 与 A5、Meaasge6 可知:

$$\frac{D1 \models D1 \xleftarrow{n_{A2}} D2, D1 \triangleleft \{r_{B1}, n_{A2}\}_{n_{A2}}}{D1 \models D2 \sim \{r_{B1}, n_{A2}\}} \quad (10)$$

由规则 2 与 A1 可知:

$$\frac{D1 \models \#\{n_{A2}\}}{D1 \models \#\{r_{B1}, n_{A2}\}} \quad (11)$$

同理,由规则 3 和 4,与式 (10), (11) 可证明目标公式: G4: $D1 \models D2 \models \{r_{B1}\}$.

3.3 形式化工具分析

ProVerif^[14]是应用于验证形式模型中的密码协议的工具,支持对称和非对称加密、数字签名、哈希函数、Diffie-Hellman 密钥协议等许多密码原语进行自动有效的安全分析.在本节中,使用 ProVerif 来正式证明提出的协议的保密性和身份验证属性.

协议定义服务器与设备之间的共享激励 skc,以及设备 A 与设备 B 的共享密钥 skr.在 Dolev-Yao 模型^[15]下,图 3 是协议对设备与服务器的认证所建模四个事件: UserStarted 和 UserAuthenticated, Server-Started 和 ServerAuthenticated,以及会话密钥 skc 与 skr 的安全查询.Proverif 查询协议的结果如图 4 所示,通过结果可得该协议保持身份验证属性和长期秘密的保密性,会话密钥对模拟攻击者具有鲁棒性.

```

event UserStarted(bitstring).
event UserAuthenticated(bitstring).
event ServerStarted(bitstring).
event ServerAuthenticated(bitstring).
query id: bitstring; inj-event(UserAuthenticated(id)) ==> inj-event(UserStarted(id)).
query attacker(skc).
query attacker(skr).
    
```

图 3 设备与服务器的认证事件以及密钥安全查询

Fig.3 Authentication events and key security query

```

Verification summary:
Query inj-event(UserAuthenticated(id)) ==> inj-event(UserStarted(id)) is true.
Query not attacker(skc[]) is true.
Query not attacker(skr[]) is true.
    
```

图 4 协议查询结果

Fig.4 Query result in proposed protocol

4 协议性能分析

本节从安全属性、存储容量以及通信成本等方面对认证协议进行分析与评估.通过 Python 编写设备和服务器之间的认证协议程序,网络交互

是通过抽象 TCP 客户端/服务器连接的套接字完成,服务器等待与指定 IP 地址上的设备连接.一旦设备成功与服务器建立连接,该协议就执行一次相互认证会话.服务器和设备运行在 Windows 10,采用 Intel Core i7-9750 CPU,频率为 2.60 GHz,配备 8 GB RAM,模拟所提出的身份验证方案.

表 4 协议安全属性分析与比较

Tab.4 Comparison of protocol security attributes

	Hossain ^[2]	Akgün ^[16]	Ayu ^[9]	Huang ^[10]	Aysu ^[11]	Zhou ^[3]	Daisuke ^[17]	Bian ^[5]	本协议
双向认证	T	T	T	T	T	T	T	T	T
位置跟踪	F	T	F	F	F	F	F	T	T
可扩展性	F	F	T	F	F	T	F	F	T
前向不可追溯性	F	F	F	T	T	F	F	T	T
克隆攻击	T	T	T	T	T	F	T	T	T
建模攻击	F	F	T	F	F	无	F	T	T
假冒攻击	F	T	F	F	T	F	T	T	T
中间人攻击	F	T	F	F	T	F	T	T	T
去同步攻击	T	F	F	F	T	T	T	T	T

在安全属性方面与其他协议进行对比分析,其结果如表 4 所示.协议^[2,10,11,16,17]机制中,攻击者可以通过窃听、假冒以及物理攻击可以获取 PUF 的 CRP 对,从而不能防御建模攻击.协议^[9]通过 d 次锁定机制可以防御 PUF 攻击,但信道传输中的信息未加密,导致设备认证中被窃听、去同步以及重放攻击等安全威胁.协议^[2,3,9,16,17]中的设备存储了新旧两个身份,攻击者通过访问内存获取当前身份信息,从而跟踪到前一轮或下一轮的认证信息,因此协议不具备不可追溯性.但是本协议采用 PUF 生成的共享密钥,采用 MASK 算法与 Hash 函数的加密保证设备的隐私性与不可追溯性.

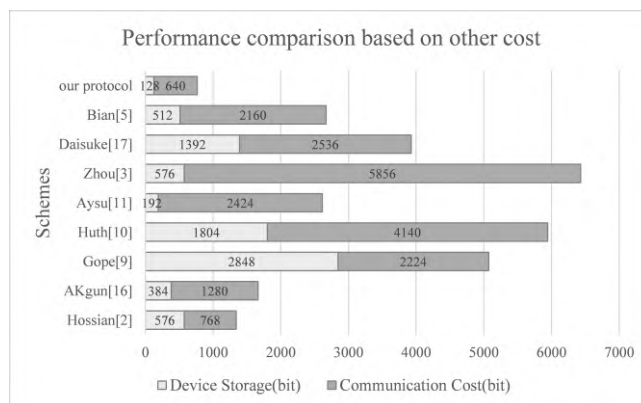


图 5 协议中设备存储与通信开销对比图

Fig.5 Performance comparison based on other costs

图列出与其它协议在设备存储与通信开销方面进行比较.参考 Aysu^[11]的论文,伪随机身份 PID_D^i 的字节长 128bit,CRP 对 (C_i, R_i) 的字节长均为 128bit,密钥的字节长度为 96 bit.本协议只存储了

128bit 随机数 (n_1^{old}, n_1^{old}), 远远低于其它协议的存储容量. 协议只传输信息 ($n_{A1}, n_{A2}, D_A, n_{B2}, d_A, d_B$), 通信开销为 640 bit. 相比较协议^[3,5,9-11,16,17], 所提出协议的通信成本均低于其他方案的通信成本, 适用于轻量级设备的安全认证场景.

5 结论

由于物联网产生海量数据给资源受限的终端设备带来信息传输安全威胁, 同时硬件设备通常面临着芯片克隆、设备伪造以及密钥存储的安全问题. 因此, 运行速率慢、通信开销大的传统网络协议不适合轻量级物联网设备的安全认证. 本文面向物联网设备提出一种轻量级匿名密钥共享认证协议. 该机制采用 PUF 防篡改防克隆的特性在硬件端生成共享密钥, 结合混淆算法、MASK 算法、Hash 函数等安全原语来保证信息传输的匿名性、不可跟踪、不可否认和前向/后向保密等安全属性. 通过形式化验证工具 ProVerif、BAN 逻辑以及非形式化的安全性分析验证, 证明协议运行的安全性、可靠性以及抗信道攻击能力. 相比较于其它现有协议, 所提出的协议具备计算成本低、通信开销和存储容量小以及高安全性的特点, 适合轻量级物联网设备的安全通信传输.

参考文献

- [1] HASSIJA V, CHAMOLA V, SAXENA V, *et al.* A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures[J]. *IEEE Access*, 2019, 7: 82721–82743.
- [2] HOSSAIN M, NOOR S, HASAN R. HSC-IoT: A Hardware and Software Co-Verification Based Authentication Scheme for Internet of Things[C]//2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud). San Francisco, CA, USA: IEEE, 2017: 109–116.
- [3] ZHOU L, LI X, YEH K-H, *et al.* Lightweight IoT-Based Authentication Scheme in Cloud Computing Circumstance[J]. *Future Generation Computer Systems*, 2019, 91: 244–251.
- [4] 王鑫, 贾庆轩, 高欣, 等. 可证明安全的轻量级无服务型 RFID 安全搜索协议[J]. *湖南大学学报(自然科学版)*, 2014, 41(8): 117–124.
WANG X, JIA Q, GAO X, *et al.* Provable Security Lightweight Service-less RFID Security Search Protocol[J]. *Journal of Hunan University(Natural Sciences)*, 2014, 41(8): 117–124(In Chinese).
- [5] BIAN W, GOPE P, CHENG Y, *et al.* Bio-AKA: An Efficient Fingerprint Based Two Factor User Authentication and Key Agreement Scheme[J]. *Future Generation Computer Systems*, 2020, 109: 45–55.
- [6] 胡锦, 谢立红, 邹望辉, 等. 基于低功耗 SoC 的微型图像采集系统设计[J]. *湖南大学学报: 自然科学版*, 2019, 46(2): 6–13.
HU J, XIE L, ZOU W, *et al.* Design of Miniature Image Acquisition System Based on Low Power System on Chip[J]. *Journal of Hunan University(Natural Sciences)*, 2019, 46(2): 6–13 (In Chinese).
- [7] ZEITOUNI S, OREN Y, WACHSMANN C, *et al.* Remanence Decay Side-Channel: The PUF Case[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(6): 1106–1116.
- [8] CHANG C-H, ZHENG Y, ZHANG L. A Retrospective and a Look Forward: Fifteen Years of Physical Unclonable Function Advancement[J]. *IEEE Circuits and Systems Magazine*, 2017, 17(3): 32–62.
- [9] MD Yu, Hiller M, Delvaux J, *et al.* A Lockdown Technique to Prevent Machine Learning on PUFs for Lightweight Authentication[J]. *IEEE Transactions on Multi-Scale Computing Systems*, 2017, 2(3):146–159.
- [10] HUANG Z, WANG Q. A PUF-Based Unified Identity Verification Framework for Secure IoT Hardware via Device Authentication[J/OL]. *World Wide Web*, (2020) 23:1057–1088.
- [11] Aysu A, Gulcan E, Moriyama D, *et al.* End-To-End Design of a PUF-Based Privacy Preserving Authentication Protocol[C]//International Workshop on Cryptographic Hardware & Embedded Systems. Springer, Berlin, Heidelberg, 2015.556–576.
- [12] ZHANG J, QU G. Physical Unclonable Function-Based Key Sharing via Machine Learning for IoT Security[J]. *IEEE Transactions on Industrial Electronics*, 2020, 67(8): 7025–7033.
- [13] QURESHI M A, MUNIR A. PUF-RAKE: A PUF-based Robust and Lightweight Authentication and Key Establishment Protocol[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021: 1–1.
- [14] XIE Q, HU B, TAN X, *et al.* Robust Anonymous Two-Factor Authentication Scheme for Roaming Service in Global Mobility Network[J]. *Wireless Personal Communications*, 2014, 74(2): 601–614.
- [15] DOLEV D, YAO A. On the security of public key protocols[J]. *IEEE Transactions on Information Theory*, 1983, 29(2): 198–208.
- [16] AKGÜN M, ÇAĞLAYAN M U. Providing Destructive Privacy and Scalability in RFID Systems Using PUFs[J]. *Ad Hoc Networks*, 2015, 32: 32–42.
- [17] MORIYAMA D, MATSUO S, OHKUBO M. Relation among the security models for RFID authentication protocol[C]//ECRYPT Workshop on Lightweight Cryptography. Berlin: Computer Science, 2013: 333–349.