



## WSN 中基于物理不可克隆函数的簇内密钥分配

柳亚男, 张 正, 邱 硕, 程 远

(金陵科技学院 网络安全学院, 南京 211169)

**摘 要:** 解决无线传感器网络(WSN)安全通信问题的前提条件是轻量级的认证与密钥分配,但由于传感器节点的计算、存储和通信资源有限,传统基于公钥基础设施的认证与密钥分配机制并不适用。为此,提出基于物理不可克隆函数的 WSN 簇内密钥分配方案,实现网关节点、簇内传感器节点之间的双向认证与密钥分配。利用物理不可克隆函数的不可克隆性和不可预测性提供更安全高效的双向认证,通过直接与间接密钥分配,实现簇内 100% 的安全连通性。该方案由于无需预存储密钥,因此可降低节点存储开销和密钥泄露的风险,具备完全抗俘获性。此外,激励响应对不以明文形式传输,可抵抗对物理不可克隆函数实施的建模攻击。实验结果表明,与概率型密钥预分配方案相比,在相同的存储开销下,该方案能够提供更高的节点抗俘获性、安全连通性和认证性。

**关键词:** 认证;密钥分配;物理不可克隆函数;无线传感器网络;簇

开放科学(资源服务)标志码(OSID):



**中文引用格式:**柳亚男,张正,邱硕,等. WSN 中基于物理不可克隆函数的簇内密钥分配[J]. 计算机工程,2020,46(9):163-171.

**英文引用格式:**LIU Yanan,ZHANG Zheng,QIU Shuo,et al. Intra-cluster key distribution based on physical unclonable functions in WSN[J]. Computer Engineering,2020,46(9):163-171.

## Intra-Cluster Key Distribution Based on Physical Unclonable Functions in WSN

LIU Yanan,ZHANG Zheng,QIU Shuo,CHENG Yuan

(School of Network Security,Jinling Institute of Technology,Nanjing 211169,China)

**[Abstract]** The prerequisite for solving the problem of secure communication in Wireless Sensor Network(WSN) is lightweight authentication and key distribution. However, due to the limited computing, storage and communication resources of sensor nodes, the traditional authentication and key distribution mechanism based on the Public Key Infrastructure(PKI) is not suitable. Therefore, this paper proposes an intra-cluster key distribution scheme based on Physical Unclonable Function(PUF) in WSN to realize bidirectional authentication and key distribution between gateway nodes and sensor nodes in the cluster. The unclonable and unpredictable properties of PUF are used to provide more secure and efficient bidirectional authentication, implementing 100% secure connectivity in the cluster through direct and indirect key distribution. Since keys are not pre-stored, the scheme reduces the cost of storage and the risk of key leakage of nodes, providing the perfect anti-capture performance. Besides, the stimulus response pairs are not transmitted in clear text, and can resist the modeling attacks to the PUF. Experimental results show that the proposed scheme provides better anti-capture performance, secure connectivity and authentication for nodes than the probability key pre-distribution schemes under the same storage overhead.

**[Key words]** authentication; key distribution; Physical Unclonable Function(PUF); Wireless Sensor Network(WSN); cluster  
**DOI:**10.19678/j.issn.1000-3428.0057548

### 0 概述

无线传感器网络(Wireless Sensor Network, WSN)

的很多应用场景是战场环境或条件恶劣的无人区,传感器节点和无线信道都容易受到恶意攻击,如物理捕获节点、数据篡改、侧信道攻击等。数据加密是

**基金项目:**国家自然科学基金(61902163);国家重点研发计划“网络空间安全”重点专项(2017YFB0802800);江苏省高等学校自然科学基金(17KJD5200003,19KJB5200033);金陵科技学院科研启动基金(JIT-B-201639,JIT-B-201726,JIT-B-202001)。

**作者简介:**柳亚男(1984—),女,讲师、博士,主研方向为轻量级密码协议、传感器网络;张 正,研究员;邱 硕、程 远,讲师、博士。

**收稿日期:**2020-03-02 **修回日期:**2020-06-04 **E-mail:**yanan.liu@jit.edu.cn

保障安全通信的常用技术,而密钥分配和协商是加密的前提和基础。

2002 年,ESCHENAUER 等人针对传感器资源受限的缺点提出随机密钥预分配方案<sup>[1]</sup>。2007 年,DU 等人将 Eschenaue 方案应用到层次型传感器网络,提出非对称预分配(AP)<sup>[2]</sup>,这类“概率型”方案计算和通信开销低,但密钥存储量大,网络连通性和安全性差。2009 年,BOUJELBEN 等人基于 Blom 矩阵提出的密钥管理方案<sup>[3]</sup>,提高了节点抗俘获性,但矩阵运算的计算开销较高。2015 年,ERFANI 等人基于 Eschenaue 方案,提出一种结合密钥预分配和部署后密钥建立机制的动态传感器网络密钥管理方案<sup>[4]</sup>。在网络部署前,传感器节点中预存储一定数目的密钥;在网络部署后,无法建立共享密钥的邻居节点通过其他方式生成会话密钥。在 Erfani 的方案中,基站参与了簇内密钥分配过程,带来过多的通信开销。此外,基于共享密钥的方案缺乏有效的认证机制,当敌手通过物理俘获等手段而获取节点内容密钥时,可以进行克隆节点、假冒攻击,并进一步实施中间人攻击等恶意行为。在公钥算法方面,2012 年,ALAGHEBAND 等人提出基于椭圆曲线加密算法(ECC)的分层异构传感器网络的动态安全密钥管理模型(DSKM)<sup>[5]</sup>;2018 年,MA 等人提出基于 ECC 的分层密钥管理方案<sup>[6]</sup>,但是对于普通传感器而言,存储量以及公钥计算开销仍然较大。

针对上述方案存在的问题,本文提出一种基于物理不可克隆函数(PUF)的低能耗密钥分配方案,解决层次型传感器网络中传感器与网关之间的簇内密钥分配问题。利用 PUF 的激励响应对实现密钥分配和双向认证,提高节点抗俘获性。针对大规模传感器网络中节点随机部署的特征,提出直接和间接密钥协商两种具体方案,以提高网络安全连通性。

## 1 基于 PUF 的安全协议研究

物理不可克隆函数(PUF)是一种新兴的加密组件,能够提取集成电路内门电路或连接线间由于制造工艺的不一致性而引入的随机差异,并利用这些随机差异以一定规则生成加密(响应)信号<sup>[7]</sup>。物理对象中的随机差异可以理解成它的“指纹”,是该物理对象所特有的。除基于集成电路的 PUF 外,还有硅 PUF 和涂层 PUF 等。PUF 具有运算快、不可克隆性和不可预测性,在无线传感器网络的轻量级认证和安全密钥生成方面具有极高的研究价值。与使用数字证书不同,PUF 的认证基于激励响应对(CRP)机制,不仅提高了运算速度,而且能够减小密钥存储开销,进而降低密钥暴露的风险。

在安全协议设计中,可以将 PUF 结构看作是单向函数的硬件等价物,并具有易于制造、不可克隆和

不可预测的属性。将 PUF 结构看作一个黑盒的激励响应系统,针对任一激励值可产生唯一对应的响应值,而根据响应值却无法推导出激励值。利用函数  $P$  来表示 PUF 的单向性:

$$P: C \rightarrow R; P(c) = r, c \in C, r \in R \quad (1)$$

其中, $C$  和  $R$  分别是激励集合和响应集合,函数  $P$  是 PUF 结构的数学模型,激励值  $c$  与对应的响应值  $r$  称为该 PUF 结构  $P$  的一个激励响应对(CRP): $(c, r)$ 。

身份认证是物理不可克隆函数最常见的应用。不可克隆性、单向运算性和防篡改特性,使得 PUF 在身份认证协议设计中成为一种非常有效的技术手段。基于 PUF 身份认证分为注册阶段和认证阶段,在注册阶段中,认证服务器数据库中储存 PUF 的激励响应对以及嵌入 PUF 的物理设备的身份标识。认证阶段中,认证服务器从数据库中挑选一个激励并发送给设备,设备运行 PUF 输出对应的响应,认证服务器将 PUF 在线产生的响应与数据库中预存储的值进行比较,如果相同则认证成功,否则认证失败。为防止重放攻击,认证服务器将已经使用过的激励响应对删除。基于 PUF 的认证方案加快了认证过程,同时减少了密钥存储量,从而降低密钥暴露的风险,提高节点抗俘获性。

PUF 电路的实现方法产生的响应存在一定的错误概率。因此,通常引入纠错程序来降低错误响应生成<sup>[8]</sup>。2008 年,GUAJARDO 等人基于 PUF 结构,在可信第三方参与和不参与两种场景下提出两个安全密钥分配方案<sup>[9]</sup>。2013 年,BAHRAMPOUR 等人利用 PUF 结构实现公钥分发,由此实现传感器间的密钥协商,提高节点安全性的代价是较高的公钥计算开销<sup>[10]</sup>。2015 年,ABUTALEB 等人结合 PUF 和信道状态信息(CSI)提出一个点对点的物理层认证与密钥交换方案,避免使用预共享密钥,并降低了通信量<sup>[11]</sup>。2017 年,LIU 等人提出基于 SRAM PUF 的双向认证<sup>[12]</sup>。同年,WANG 等人提出基于 PUF 和 IPI 的可穿戴设备的双因子认证协议<sup>[13]</sup>,CHATTERJEE 等人提出了一种基于 PUF 的安全通信协议<sup>[14]</sup>,将 PUF 与双线性对相结合构造公钥生成器。2018 年,BRAEKEN 通过使用椭圆曲线 Qu-Vanstone(ECQV)<sup>[15]</sup>提高了 Chatterjee 协议的计算效率。2019 年,LI 等人利用双线性对提出基于 PUF 的物联网安全通信系统,实现消息认证<sup>[16]</sup>。研究人员还提出将 PUF 构造密钥生成器的认证协议,如 2006 年 TUYS 等人提出的 Schnorr 认证协议<sup>[17]</sup>,2007 年 BATINA 等人提出的 Okamoto 认证协议<sup>[18]</sup>,2019 年 USMANI 等人利用 FPGA 实现了 Anderson PUF 扩展,降低了密钥生成器的比特错误输出率<sup>[19]</sup>。在这些基于 PUF 的认证协议中,PUF 的激励响应对大多是明文传输,当敌手获得大量的 CRP 样本后,可能对 PUF 实施建模攻击。

## 2 网络模型和攻击模型

### 2.1 簇状网络模型

大规模无线传感器网络通常部署为层次型簇状结构, 包含多种异构节点, 如低能耗的传感器节点、负责成簇和数据融合的网关节点以及作为管理中心和安全中心的服务器。传感器被划分为不重叠的簇从周围环境中采集信息, 并通过短距离通信将原始数据发送给网关。网关是簇内的数据处理和融合的中心节点, 将处理后的数据通过长距离通信传送给服务器。与传感器相比, 网关通常具有更高的硬件配置, 包括更大的功率、内存和计算处理能力。

### 2.2 攻击模型

经典的 Dolev-Yao 模型<sup>[20]</sup>定义攻击模型如下: 敌手可任意侦听、截获、插入、删除或阻断流经公开信道中的消息。随着边信道攻击技术(如功耗攻击、电磁攻击和计时攻击)的发展<sup>[21]</sup>, 敌手可分析出智能卡内安全参数, 攻击能力得到增强。本文在此基础上主要考虑以下攻击:

**妥协攻击:**敌手通过物理入侵方式获取内部存储的标识、密钥等信息, 从而使节点妥协, 并进一步达到克隆节点、破解加密链路的目的。

**重放攻击:**敌手利用截获到的有效数据重复传输以欺骗数据中心、服务器或其他传感器节点。

**假冒攻击:**敌手投放非法节点以假冒正常节点, 从而欺骗数据中心窃取通信内容。认证协议的主要目标是阻止敌手对节点的假冒攻击, 完成服务器对节点的合法性认证。

**克隆攻击:**敌手利用非法获取合法节点的标识、密钥等信息, 伪造一个新的节点并投入网络, 从而达到欺骗数据中心以非法获取、篡改数据等目的。

**中间人攻击:**敌手通过假冒合法节点骗取其他节点、服务器的信任, 入侵网络数据交互过程, 从而非法获取数据。该攻击往往与假冒攻击、重放攻击、克隆攻击等结合实施。

**建模攻击:**是 PUF 面临的一种主要威胁<sup>[22]</sup>。文献[23]利用线性规划和进化策略等数学手段, 仿造出基于仲裁器 PUF 的一类线性模型。此类线性模型实际是一个简化压缩的激励响应对数据库。随后研究人员通过向 PUF 中添加噪声增加了敌手建立模型的难度, 但是仍然可以被模型化。在本文方案中, PUF 的激励响应对不是明文传输, 因此可以有效抵抗建模攻击。

## 3 基于 PUF 的密钥分配方案

本节针对大规模网络中节点随机部署的特征, 提出一个基于 PUF 结构的密钥预分配方案。在每个簇中, 实现网关对簇内传感器节点的双向认证与密钥分配。具体分为初始化阶段、直接密钥分配阶段

和间接密钥分配阶段。

### 3.1 初始化阶段

假设网络中有  $n$  个传感器节点  $S_1, S_2, \dots, S_n$  和  $m$  个网关节点  $G_1, G_2, \dots, G_m$ 。

1) 在网络部署之前, 每个传感器节点  $S_i$  被嵌入一个带有 PUF 结构的芯片, 表示为  $P_{S_i}$ 。

2) 为每个传感器节点  $S_i$  随机指定  $l$  个网关节点, 称为  $S_i$  的“逻辑网关”, 表示为  $S_i-LG_{1,2,\dots,l}$ 。

3) 为  $S_i$  生成  $l$  个  $P_{S_i}$  的激励响应对, 记为  $(c_j, r_j)_{S_i}$ , 其中  $j = 1, 2, \dots, l$ , 并将  $l$  个二元组  $\langle id_{S_i}, (c_j, r_j)_{S_i} \rangle$  分别保存到  $l$  个“逻辑网关” $S_i-LG_j$  中。

假设初始化阶段不存在窃听或物理俘获等攻击行为。如假设传感器网络中包括  $n = 6$  个传感器节点  $S_1 \sim S_6$  和  $m = 3$  个网关节点  $G_1, G_2, G_3$ 。令  $l = 2$ , 因此为每个传感器节点随机指定 2 个“逻辑网关”, 其对应关系如图 1 所示。如传感器节点  $S_1$  被指定的“逻辑网关”是  $G_1$  和  $G_3$ , 即  $S_1-LG_1 = G_1, S_1-LG_2 = G_3$ 。将  $S_1$  所嵌入的 PUF 结构  $P_{S_1}$  生成激励响应对的二元组  $\langle id_{S_1}, (c_1, r_1)_{S_1} \rangle$  和  $\langle id_{S_1}, (c_2, r_2)_{S_1} \rangle$  分别存入  $G_1$  和  $G_3$ 。

	$G_1$	$G_2$	$G_3$
$S_1$	$\langle id_{S_1}, (c_1, r_1)_{S_1} \rangle$		$\langle id_{S_1}, (c_2, r_2)_{S_1} \rangle$
$S_2$	$\langle id_{S_2}, (c_1, r_1)_{S_2} \rangle$	$\langle id_{S_2}, (c_2, r_2)_{S_2} \rangle$	
$S_3$	$\langle id_{S_3}, (c_1, r_1)_{S_3} \rangle$		$\langle id_{S_3}, (c_2, r_2)_{S_3} \rangle$
$S_4$		$\langle id_{S_4}, (c_1, r_1)_{S_4} \rangle$	$\langle id_{S_4}, (c_2, r_2)_{S_4} \rangle$
$S_5$	$\langle id_{S_5}, (c_1, r_1)_{S_5} \rangle$	$\langle id_{S_5}, (c_2, r_2)_{S_5} \rangle$	
$S_6$		$\langle id_{S_6}, (c_1, r_1)_{S_6} \rangle$	$\langle id_{S_6}, (c_2, r_2)_{S_6} \rangle$

图 1 传感器节点与其逻辑网关对应关系

Fig. 1 Corresponding relation of sensor nodes and its logical-gateway

### 3.2 随机部署与成簇

假设全体节点被随机部署在目标区域, 因此无法提前预测各节点(包括网关与传感器)的物理位置。网络部署后网关节点首先启动成簇算法(不在本文讨论范围, 可参考文献[24]), 将全体传感器节点以网关节点为单位划分成各不交叉覆盖的簇。每个簇中包括一个网关节点, 称为该簇中传感器节点的“物理网关”, 记为  $S-PG$ 。“物理网关”称为该簇的簇头, 簇中的传感器节点称为簇成员。为保障簇头与簇成员间的短距离安全通信, 簇头需要认证簇成员的身份, 并生成会话密钥分配给簇成员, 即簇内认证与密钥分配。

每个簇的平均规模是  $n/m$ , 对于任一传感器节点  $S_i$ , 如果其“逻辑网关”与“物理网关”相同, 即  $\exists j \in \{1, 2, \dots, l\}$ , 使得  $S_i-LG_j = S_i-PG$  成立, 则  $S_i$  与

“物理网关” $S_i$ -PG 执行直接密钥分配;反之,执行间接密钥分配。网络部署情况如图 2 所示,网关节点建立簇后,获得簇成员标识。例如,以网关节点  $G_1$  为簇头的簇中包括传感器节点  $S_1$  和  $S_4$ 。

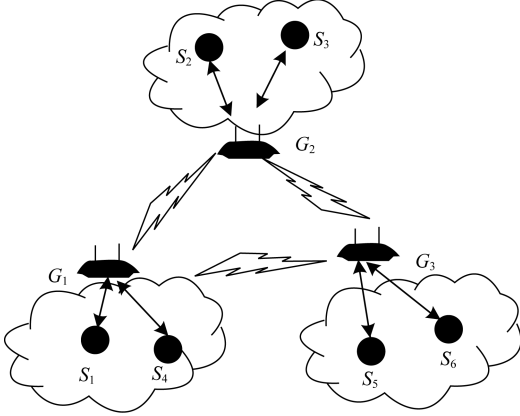


图 2 簇状传感器网络模型

Fig. 2 Clustered sensor network model

由图 2 可知,簇成员  $S_1$  的“逻辑网关”之一是  $G_1$ ,因此  $G_1$  可以通过直接密钥分配来实现对  $S_1$  的认证与密钥分配。簇成员  $S_4$  的“逻辑网关”分别是  $G_2$  和  $G_3$ ,即初始化阶段已将  $S_4$  的两个激励响应  $(c_1, r_1)_{S_4}$  和  $(c_2, r_2)_{S_4}$  分别存储在  $G_2$  和  $G_3$  中。此时,  $G_1$  通过间接密钥分配实现对  $S_4$  的认证与密钥分配。

### 3.3 直接密钥分配阶段

如果传感器  $S_i$  的“逻辑网关”与“物理网关”相同,则“物理网关” $S_i$ -PG 在初始化阶段存储了  $S_i$  的激励响应。

以图 2 中网关  $G_1$  与传感器  $S_1$  为例,直接密钥分配步骤如下:

1) 网络部署后,网关  $G_1$  从本地读取二元组  $\langle id_{S_1},$

$(c_1, r_1)_{S_1} \rangle$ , 将激励  $c_1$  明文发送给传感器节点  $S_1$ 。

2) 传感器节点  $S_1$  将激励值  $c_1$  输入 PUF 结构  $P_{S_1}$ , 得到相应的响应值  $r_{S_1}: r_{S_1} = P_{S_1}(c_1)$ 。

3) 传感器节点  $S_1$  使用  $r_{S_1}$  作为加密密钥加密  $c_1$  得到  $cipher = E(r_{S_1}, c_1)$ , 其中  $E$  表示加密函数, 使用对称加密算法可以有效降低计算开销。

4) 传感器节点  $S_1$  将密文  $cipher$  发送给网关  $G_1$ 。

5) 网关  $G_1$  利用  $\langle id_{S_1}, (c_1, r_1)_{S_1} \rangle$  中的  $r_1$  作为解密密钥得到  $plain = D(r_1, cipher) = D(r_1, E(r_{S_1}, c_1))$ , 并将  $plain$  与  $c_1$  进行比较。其中  $D$  表示解密函数, 并与  $E$  相对应。如果  $plain = c_1$  成立, 则  $r_1 = r_{S_1}$  成立, 由于响应值  $r_{S_1}$  是 PUF 结构  $P_{S_1}$  根据激励  $c_1$  在线产生, 且具有不可克隆和不可预测性, 可作为节点  $S_1$  的唯一性特征, 由此网关  $G_1$  对传感器节点  $S_1$  的身份认证通过; 反之, 认证不通过。

6) 传感器节点  $S_1$  的身份认证通过后, 网关  $G_1$  生成会话密钥, 表示为  $key_{GS_1}$ , 使用  $r_1$  作为加密密钥加密  $key_{GS_1}$  得到  $cipher2 = E(r_1, key_{GS_1})$ 。

7) 网关  $G_1$  将密文  $cipher2$  发送给传感器节点  $S_1$ 。

8) 传感器节点  $S_1$  使用  $r_{S_1}$  作为解密密钥对  $cipher2$  进行解密, 得到:  $plain2 = D(r_{S_1}, cipher2) = D(r_{S_1}, E(r_1, key_{GS_1})) = key_{GS_1}$ , 由此获得会话密钥  $key_{GS_1}$ , 完成密钥分配。

直接密钥分配具体步骤如图 3 所示。与密钥预分配方案不同, 在初始化阶段, 传感器节点嵌入的是 PUF 结构的芯片而非密钥, 因此, 节点投放后即使被敌手物理俘获, 也不会暴露密钥。基于 PUF 结构的身份认证, 比基于公钥算法的数字证书效率更高。

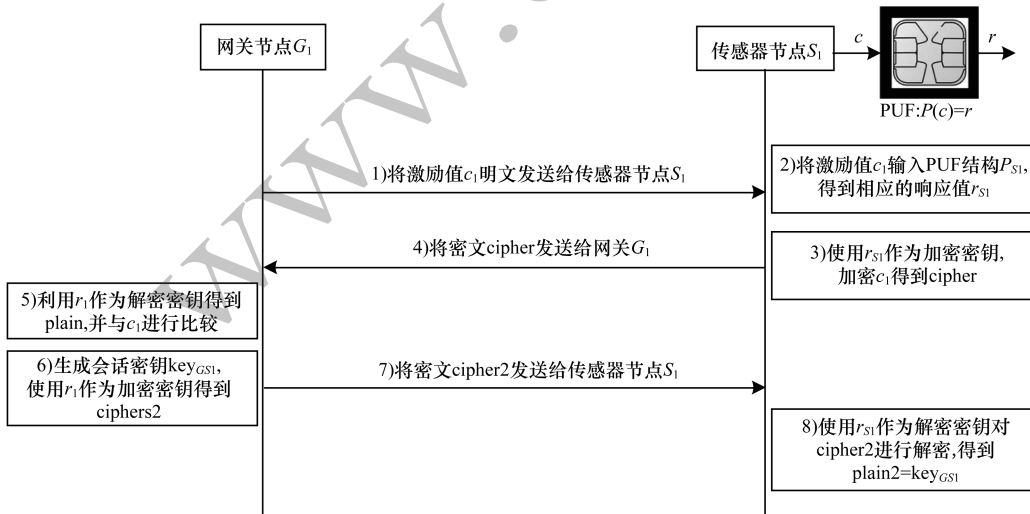


图 3 直接密钥的分配过程

Fig. 3 Distribution process of direct key

### 3.4 间接密钥分配

以图3中网关节点 $G_1$ 与传感器节点 $S_4$ 为例。间接密钥分配步骤如下:

- 1) 网关 $G_1$ 向其他网关节点广播 $S_4$ 的标识,目的是寻求 $S_4$ 的“逻辑网关”的帮助。
- 2)  $S_4$ 的“逻辑网关”之一 $G_3$ 从本地读取二元组 $\langle \text{id}_{S_4}, (c_2, r_2)_{S_4} \rangle$ ,将激励响应 $(c_2, r_2)_{S_4}$ 中的激励值 $c_2$ 明文发送给 $G_1$ 。
- 3)  $G_1$ 将激励值 $c_2$ 转发给 $S_4$ 。
- 4)  $S_4$ 将激励值 $c_2$ 输入嵌入的 PUF 结构 $P_{S_4}$ ,得到相应的响应值 $r_{S_4}: r_{S_4} = P_{S_4}(c_2)$ 。
- 5) 传感器节点 $S_4$ 使用 $r_{S_4}$ 作为加密密钥加密 $c_2$ 得到 $\text{cipher} = E(r_{S_4}, c_2)$ ,其中 $E$ 表示加密函数。
- 6)  $S_4$ 使将密文 $\text{cipher}$ 发送给“物理网关” $G_1$ 。
- 7)  $G_1$ 将 $\text{cipher}$ 转发给 $G_3$ 。
- 8)  $G_3$ 利用 $\langle \text{id}_{S_4}, (c_2, r_2)_{S_4} \rangle$ 中的 $r_2$ 作为解密密钥得到 $\text{plain} = D(r_2, \text{cipher}) = D(r_2, E(r_{S_4}, c_2))$ ,并将 $\text{plain}$ 与 $(c_2, r_2)_{S_4}$ 中的 $c_2$ 进行比较。其中 $D$ 表示解密函数,并与 $E$ 相对应。如果 $\text{plain} = c_2$ 成立,则

$r_2 = r_{S_4}$ 成立,由于响应值 $r_{S_4}$ 是 PUF 结构 $P_{S_4}$ 根据激励 $c_2$ 在线产生,且具有不可克隆和不可预测性,可作为节点 $S_4$ 的唯一性特征,由此“逻辑网关” $G_3$ 对传感器节点 $S_4$ 的身份认证通过;反之,认证不通过。

9)  $G_3$ 对传感器节点 $S_4$ 的身份认证通过后,生成会话密钥,表示为 $\text{key}_{GS_4}$ 。 $G_3$ 使用 $\text{key}_{G_1-G_3}$ 作为加密密钥加密 $\text{key}_{GS_4}$ 得到 $\text{cipher2} = E(\text{key}_{G_1-G_3}, \text{key}_{GS_4})$ ;使用 $(c_2, r_2)_{S_4}$ 中的 $r_2$ 作为加密密钥加密 $\text{key}_{GS_4}$ 得到 $\text{cipher3} = E(r_2, \text{key}_{GS_4})$ 。

10)  $G_3$ 将 $\text{cipher2}$ 和 $\text{cipher3}$ 发给 $G_1$ ,并删掉 $\text{key}_{GS_4}$ 。

11)  $G_1$ 用 $\text{key}_{G_1-G_3}$ 作为解密密钥解密 $\text{cipher2}$ 得到 $\text{key}_{GS_4} = D(\text{key}_{G_1-G_3}, \text{cipher2})$ 。

12)  $G_1$ 将 $\text{cipher3}$ 转发给 $S_4$ 。

13)  $S_4$ 利用 $r_{S_4}$ 作为解密密钥解密 $\text{cipher3}$ 得到 $\text{key}_{GS_4} = D(r_{S_4}, \text{cipher3}) = D(r_{S_4}, E(r_2, \text{key}_{GS_4}))$ 。 $S_4$ 由此获得会话密钥 $\text{key}_{GS_4}$ ,完成密钥分配。

间接密钥分配的具体步骤如图4所示。

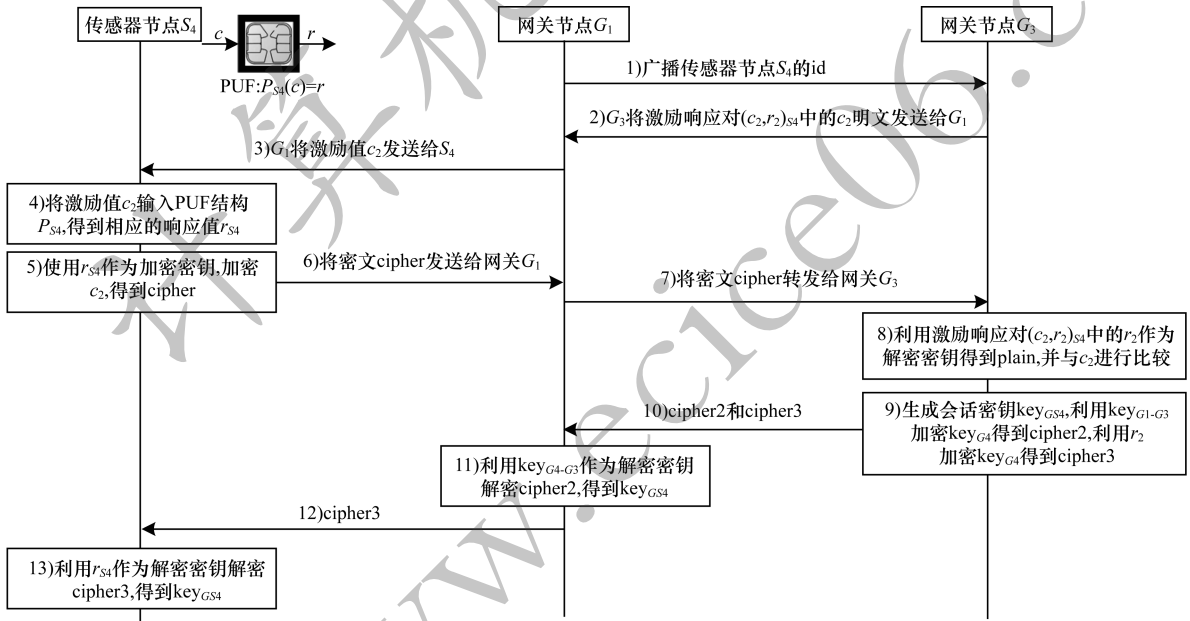


图4 间接密钥的分配过程

Fig. 4 Distribution process of indirect key

## 4 安全性和性能分析

### 4.1 认证性

网关节点通过将本地存储的 PUF 激励响应 $(c, r)$ 中的响应值 $r$ 与传感器节点返回的响应值 $r_s$ 进行比较,来对传感器节点进行身份认证。若 $r = r_s$ 成立,则认证成功;反之,认证不成功。网关仅对身份认证成功的传感器节点进行密钥分配。

与基于公钥基础设施(PKI)的数字证书的认证方式相比,基于 PUF 的认证从硬件底层出发,因此,运算速度快、存储量低。在当前文献中所提出的

PUF 认证方案<sup>[15-16]</sup>中,认证方明文发送激励值 $c$ ,被认证设备根据 $c$ 在线生成响应值 $r$ ,并将 $r$ 明文返回服务器端。发送和返回过程将激励和响应全都暴露。为抵抗重放攻击,通常一对 CRP 只使用一次。如果服务器需要对客户端进行多次认证,则使用多个不同的激励响应。但是,如果针对某一 PUF 的大量激励响应被暴露在网络中,容易被敌方实施建模攻击,并试图对 PUF 响应值进行猜测。

在本文方案中,激励响应 $(c, r)$ 被预存储到网关中,PUF 结构被嵌入到传感器,传感器中并不存储

激励响应对。当网关需要认证传感器身份时,将  $(c, r)$  中的激励值  $c$  明文发送给传感器,传感器通过 PUF 在线生成一个响应值  $r_s$ 。将  $r_s$  作为加解密钥生成  $c$  的密文并发送给网关进行比较,而非传统方案中明文发送响应值,可以有效抵抗 PUF 的建模攻击,并进一步确保  $r_s$  的唯一性与有效性以及传感器节点的认证性。

#### 4.2 节点抗俘获性

传感器网络通常部署在无人值守环境中,敌手通过俘获节点等物理攻击手段非法获取节点中的秘密信息。“节点的抗俘获性”表示敌手根据一定数目的被俘节点能够直接或间接获得未俘节点中密钥的概率,用  $F(x)$  表示,  $x$  表示被俘获节点个数。

$$F(x) = \frac{\text{未俘节点被暴露的密钥量}}{\text{未俘节点中密钥的总存储量}} \quad (1)$$

与经典的“概率型”随机密钥预分配方案<sup>[1-2]</sup>不同,本文方案中传感器节点不预存储任何形式的密钥,这不仅降低了节点的存储开销,而且提高了传感器节点的抗俘获性。因为即使节点被物理俘获,敌手无法获取被俘获节点以外其他节点中的密钥,所以传感器节点具有完全抗俘获性,即  $F(x_s) = 0$ , 其中  $x_s$  表示被俘获传感器节点个数。

网关节点担任簇头的角色,对内负责与簇成员安全通信,对外与其他簇头保持安全连通。初始化阶段预存储了激励响应对,密钥分配过程结束后又存储了大量的与簇成员建立的会话密钥。当网关节点被物理俘获后,整个簇被迫解散,簇内通信中断。簇成员(传感器节点)可能成为孤立节点,也可能加入到其他簇中,重复认证与密钥分配过程并获取一个新的会话密钥。因此,敌手从被俘网关节点中无法获取未俘节点的有效密钥,网关节点具有完全抗俘获性,即  $F(x_g) = 0$ , 其中  $x_g$  表示被俘获网关节点个数。

簇状传感器网络中经典的随机密钥预分配方案是 DU 等人提出的 AP<sup>[2]</sup>。这类随机型方案对节点的计算和通信要求低,但很难平衡节点的存储负载、网络连通性和抗俘获性这 3 个性能指标。文献[3]对 AP 进行改进,结合 Blom 矩阵提高了节点抗俘获性,但是同时也对节点的存储提出了更高的要求。

图 5 比较了不同方案传感器节点的抗俘获性  $F(x_s)$ , 横轴是被俘获的传感器节点数量  $x_s$ 。

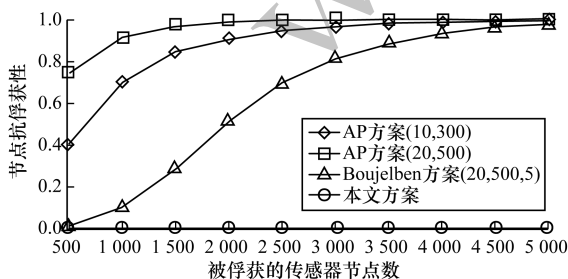


图 5 传感器节点抗俘获性比较

Fig.5 Comparison of anti-capture performance of sensor nodes

图 6 比较了不同方案中网关节点的抗俘获性  $F(x_g)$ 。

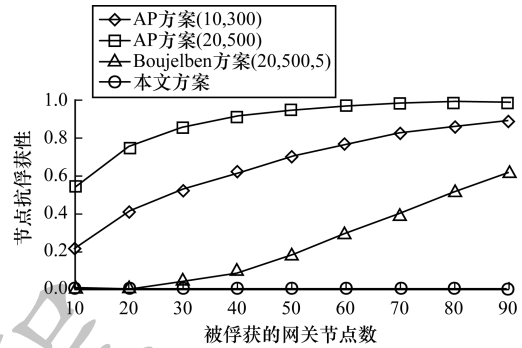


图 6 网关节点抗俘获性比较

Fig.6 Comparison of anti-capture performance of gateway nodes

实验结果表明,随机型密钥预分配方案中由于节点存储了大量密钥,随着被俘节点的增多,抗俘获性越来越差。Boujelben 方案中节点存储的是矩阵而非密钥,因此抗俘获性优于 AP 方案,其存储开销是 AP 的  $\lambda$  倍( $\lambda$  是矩阵参数)。在本文方案中,传感器节点并不存储密钥,网关节点存储的 CRP 也并非密钥本身,因此,节点具备完全抗俘获性。

#### 4.3 安全连通度

网络的安全连通度定义为通信双方能够建立会话密钥的概率。本文分别给出实现密钥分配的直接和间接两种情况。任意一个传感器节点最终可以与其“物理网关”(即簇头)成功建立起会话密钥,因此,安全连通度为 1。

从能耗角度来看,间接密钥分配过程比直接密钥分配的通信量更高。如果提高直接密钥分配后的安全连通性,可以有效提高整个方案的实施速度和效率。当网络部署后,一个传感器节点恰好能够落在其任一“逻辑网关”所管理的簇中的概率是  $p = l/n$ , 即该传感器能够与其“物理网关”通过直接密钥分配方案建立会话密钥的概率为:

$$p_d = p = l/n \quad (2)$$

其中,  $p_d$  为直接连通度,  $p_i = 1 - p_d$  为间接连通度。

模拟实验计算网络直接安全连通度结果如图 7 所示。由于伪随机数生成器及边界问题等因素,实验结果略低于理论值,但  $l$  对  $p_d$  的影响趋势与理论分析结果一致。因此,在给定规模的网络中,可以通过提高“逻辑网关”的数量  $l$  来提高直接连通度  $p_d$ , 进而降低方案的整体能耗。

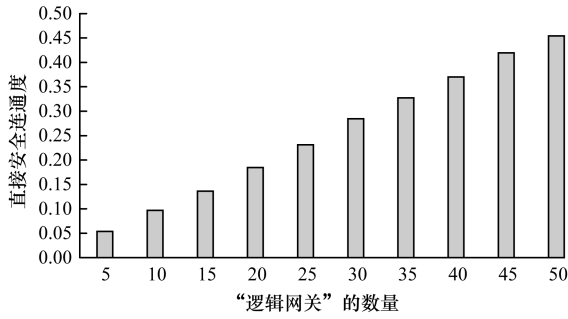


图7 直接连通度与“逻辑网关”数量的关系

Fig.7 Relationship of direct connectivity and the number of "logical gateways"

图8比较了两种方案在网关存储负载相同的前提下安全连通度的实验结果。模拟环境为:传感器节点个数  $m = 10\ 000$ , 网关节点个数  $n = 100$ , AP方案密钥池大小为  $10\ 000$ , 传感器节点密钥环大小分别为10、20、30这3种情况。值得强调的是, 本文方案中传感器节点的密钥预存储量为0, 明显低于AP方案, 连通度却显著高于AP。随机型方案必须通过提高节点的密钥存储量来获得较高的安全连通度。

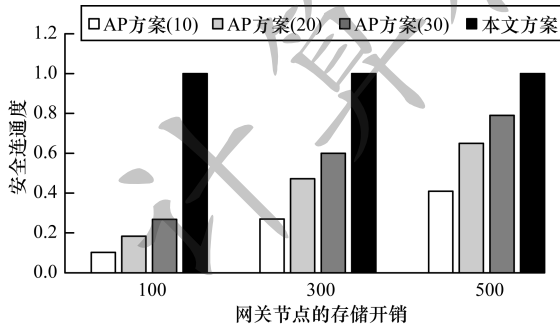


图8 安全连通度比较

Fig.8 Comparison of security connectivity

#### 4.4 开销与能耗

本文主要从存储、通信和计算3个方面考虑节点开销, 其中  $LEH_{key}$  表示密钥长度,  $LEH_{id}$  表示节点id长度。

##### 1) 存储开销

在传感器节点方面, 初始化阶段嵌入 PUF 结构, 预存储量为0。密钥分配完成后, 需要存储与“物理网关”建立1个会话密钥。而密钥分配过程中产生的中间数据在使用完后被删除以释放存储空间。

在网关节点方面, 初始化阶段预存储  $ml/n$  个激励响应对二元组  $\langle id_s, (c, r)_s \rangle$ 。假设激励和响应值的长度与密钥长度相同, 则预存储量为  $(2LEH_{key} + LEH_{id})ml/n$ 。

##### 2) 通信开销

通信开销由交换轮次和数据包的长度来度量。

在传感器节点方面, 只在直接密钥分配的步骤4和间接密钥分配的步骤6各发送一次数据, 密钥和明文长度为  $LEH_{key}$ , 对称加密算法 AES 保证密钥长度等于明文长度, 因此传输的数据包长度为  $LEH_{key}$ 。

在网关节点方面, 直接密钥分配中在步骤1和步骤7中各自发送一个长度为  $LEH_{key}$  的数据包。间接密钥分配中作为“物理网关”在步骤1、步骤3、步骤7、步骤12共发送了  $3LEH_{key} + LEH_{id}$  长度的数据, 作为“逻辑网关”在步骤2和步骤10共发送了  $2LEH_{key}$  长度的数据, 综合网关通信开销是  $(3LEH_{key} + LEH_{id})p + 2LEH_{key}(1-p)$ 。

##### 3) 计算开销

计算开销主要集中于 PUF 响应和加解密过程(如 AES)。其中  $CAL_{ED}$  表示加密或解密的计算量,  $GEN_{PUF}$  表示传感器产生一个 PUF 响应的计算量。

在传感器节点方面, 在直接密钥分配的步骤2和间接密钥分配的步骤4产生一个 PUF 响应; 在直接密钥分配的步骤3和步骤8、间接密钥分配的步骤5和步骤13各有一次加(解)密计算。因此, 计算开销是  $GEN_{PUF} + 2CAL_{ED}$ 。

在网关节点方面, 直接密钥分配中在步骤5和步骤6各有一次加(解)密计算。在间接密钥分配中, 作为“物理网关”在步骤11有一次加(解)密计算, 作为“逻辑网关”在步骤8和步骤9共有3次加(解)密计算。综合网关的计算开销是  $2pCAL_{ED} + 4CAL_{ED}(1-p)$ 。

#### 4.5 安全性综合分析

在本文方案中, PUF 是认证和密钥分配的核心, 因此 PUF 的安全性至关重要。传感器网络通常部署在无人值守的环境中, 敌手对节点实施的物理俘获攻击是无法抵抗的。攻击模型假设敌手可以通过物理入侵方式获取内部存储的标识、密钥等信息, 本文方案并非基于随机密钥预存储, 即使节点被妥协也不会泄露其他节点的信息或密钥, 因此不会破坏安全节点间的加密链路, 即提供完全的抗俘获性。PUF 本身具备不可克隆性和不可预测性, 因此能够抵抗假冒攻击和克隆攻击。本文方案中 PUF 响应值不以明文形式传输, 敌手通过窃取的相关密文无法有效实施重放攻击或中间人攻击。在一些经典的基于 PUF 认证协议中, PUF 激励响应



对是以明文形式传输,当对手获得某个 PUF 足够数量的激励响应对后,发起建模攻击,对 PUF 响应进行猜测。一旦敌手能够猜测出超过 75% 的响应比特时,PUF 被认为失效的。在本文方案中,由传感器 PUF 生成的响应被转换成加密密钥并传输相应密文给网关,这种设计保护 PUF 免受克隆攻击、建模攻击和旁道攻击(包括电磁分析攻击和差分故障攻击等)。由于所有传输消息都是加密的,因此窃听无效,攻击者无法获取有关响应或密钥的任何明文信息。

表 1 将不同传感器网络认证和密钥分配方案进行综合比较。其中,一符号表明该特性不适合于此方案,×符号表示该方案不具备该性能,√符号表示该方案具备该性能,P1 为基于公钥算法,P2 为

基于密钥预分配,P3 为基于 PUF,A1 为提供双向认证,A2 为提供密钥分配(协商),D1 为抵抗妥协攻击,D2 为抵抗重放攻击,D3 为抵抗假冒攻击,D4 为抵抗节点克隆攻击,D5 为抵抗中间人攻击,D6 为抵抗建模攻击。与密钥预分配方案(如 AP<sup>[2]</sup>)不同,本文方案的传感器节点中不预存储任何密钥,会话密钥采取临时生成的方式,因此能够提供完全抗节点俘获性。基于 PUF 挑战应答机制的一类认证方案,都具备抗克隆、抗篡改的优点,但文献[14]不提供双向认证,而且激励和响应值是公开传输,使得 PUF 容易受到建模攻击,这个威胁在文献[9-10]等方案中也存在,在文献[5-6,10,14-16]中,使用公钥算法来实现密钥协商,计算复杂度比 AP<sup>[2]</sup>和本文方案都高。

表 1 不同密钥分配方案性能比较

Table 1 Performance comparison of different key distribution schemes

方案	年份	P1	P2	P3	A1	A2	D1	D2	D3	D4	D5	D6
本文方案	2020	×	×	√	√	√	√	√	√	√	√	√
文献[1]方案	2007	×	√	×	—	√	×	×	×	×	—	—
文献[2]方案	2009	×	√	×	—	√	×	×	×	×	—	—
文献[4]方案	2015	×	√	×	√	√	×	×	×	×	×	—
文献[5]方案	2012	√	√	×	√	√	√	√	√	×	—	—
文献[6]方案	2018	√	×	×	×	√	—	—	—	—	—	—
文献[9]方案	2008	×	×	√	×	√	—	—	—	√	√	×
文献[10]方案	2013	√	×	√	√	√	√	—	—	√	—	×
文献[11]方案	2015	×	×	√	√	√	√	—	√	√	—	√
文献[12]方案	2017	×	×	√	√	×	—	√	√	√	—	√
文献[13]方案	2017	×	×	√	√	×	√	√	√	√	—	√
文献[14]方案	2017	√	×	√	√	√	—	√	√	√	—	—
文献[15]方案	2018	√	×	√	×	√	—	√	√	√	—	—
文献[16]方案	2019	√	√	√	√	√	—	√	√	√	√	—

## 5 结束语

本文基于物理不可克隆函数(PUF)提出簇内认证与密钥分配方案。该方案不需要传感器节点预存储任何密钥,利用 PUF 的激励响应对完成节点间双向身份认证,并将 PUF 响应值转换成会话密钥的加密密钥,能够保证密钥分配过程的机密性,节省传感器节点的存储开销和降低密钥泄露的风险,实现完全抗俘获性。同时可保护 PUF 的激励响应对不被敌手获取,因此,能够抵抗攻击者对 PUF 实施建模攻击。PUF 的不可克隆性、不可预测性、计算能耗低等特点使其在传感器网络、物联网等低能耗网络环境中具有良好的应用前景。本文方案主要使用加密的方式来保护激励响应

对,下一步将利用 PUF 构造轻量级对称计算单元来实现密钥协商和密钥交换。

## 参考文献

- [1] ESCHENAUER L, GLIGOR V D. A key management scheme for distributed sensor networks [C]// Proceedings of the 9th ACM Conference on Computer and Communication Security. New York, USA: ACM Press, 2002: 41-47.
- [2] DU X J, XIAO Y, GUIZANI M, et al. An effective key management scheme for heterogeneous sensor networks[J]. Ad Hoc Networks, 2007, 5(1): 24-34.
- [3] BOUJELBEN M, CHEIKHROUHOU O, ABID M, et al. Establishing pairwise keys in heterogeneous two-tiered wireless sensor networks [C]// Proceedings of IEEE International Conference on Sensor Technologies. Washington D. C., USA: IEEE Press, 2009: 687-698.



- [4] ERFANI S H, JAVADI H H S, RAHMANI A M. A dynamic key management scheme for dynamic wireless sensor networks [J]. *Security and Communication Networks*, 2015, 8(6): 1040-1049.
- [5] ALAGHEBAND M R, AREF M R. Dynamic and secure key management model for hierarchical heterogeneous sensor networks [J]. *IET Information Security*, 2012, 6(4): 271-280.
- [6] MA Mingxin, LI Fengfua, SHI Guozhen, et al. ECC based hierarchical key management scheme for perceptual layer of IoT [J]. *Journal on Communications*, 2018, 39(S2): 5-12. (in Chinese)  
马铭鑫, 李凤华, 史国振, 等. 物联网感知层中基于ECC的分层密钥管理方案 [J]. *通信学报*, 2018, 39(S2): 5-12.
- [7] DELVAUX J, PEETERS R, GU D, et al. A survey on lightweight entity authentication with strong PUFs [J]. *ACM Computing Surveys*, 2015, 48(2): 26-39.
- [8] BRAUSKA C, FISCHLIN M, SCHRODER H, et al. Physically unclonable functions in the universal composition framework [C]//*Proceedings of IEEE CRYPTO'11*. Washington D. C., USA: IEEE Press, 2011: 51-70.
- [9] GUAJARDO J, KUMAR S, TUYLS P. Key distribution for wireless sensor networks and physical unclonable functions [C]//*Proceedings of International Conference on Secure Component and System Identification Workshop*. Berlin, Germany: Springer, 2008: 334-346.
- [10] BAHRAMPOUR R, ATANI R E. A novel key management protocol for wireless sensor networks based on PUFs [J]. *International Journal of Future Generation Communication and Networking*, 2013, 6(2): 93.
- [11] ABUTALEB M, ALLAM A. FPGA-based authenticated key exchange scheme utilizing PUF and CSI for wireless networks [C]//*Proceedings of the 10th IEEE International Conference on System of Systems Engineering*. Washington D. C., USA: IEEE Press, 2015: 170-175.
- [12] LIU Dan, GUO Limin, YU Jun, et al. A secure mutual authentication protocol based on SRAM PUF [J]. *Journal of Cryptologic Research*, 2017, 4(4): 58-69. (in Chinese)  
刘丹, 郭丽敏, 俞军, 等. 一种基于 SRAM PUF 的安全双向认证协议 [J]. *密码学报*, 2017, 4(4): 58-69.
- [13] WANG Jun, LIU Shubo, LIANG Cai, et al. Two-factor wearable device authentication protocol based on PUF and IPI [J]. *Journal on Communications*, 2017, 38(6): 127-135. (in Chinese)  
王俊, 刘树波, 梁才, 等. 基于 PUF 和 IPI 的可穿戴设备双因子认证协议 [J]. *通信学报*, 2017, 38(6): 127-135.
- [14] CHATTERJEE U, CHAKRABORTY R S, MUKHOPATHYAY D. A PUF based secure communication protocol for IoT [J]. *ACM Transactions on Embedded Computing Systems*, 2017, 16(3): 1-25.
- [15] BRAEKEN A. PUF based authentication protocol for IoT [J]. *Symmetry*, 2018, 10(8): 352.
- [16] LI Sensen, HUANG Yicai, YU Bin, et al. A PUF-based low cost secure communication scheme for IoT [J]. *Acta Electronica Sinica*, 2019, 47(4): 46-51. (in Chinese)  
李森森, 黄一才, 郁滨, 等. 基于 PUF 的低开销物联网安全通信方案 [J]. *电子学报*, 2019, 47(4): 46-51.
- [17] TUYLS P, BATINA L. RFID-tags for anti-counterfeiting [C]//*Proceedings of RSA'06*. Berlin, Germany: Springer, 2006: 115-131.
- [18] BATINA L, GUAJARDO J, KERINS T, et al. Public-key cryptography for RFID-tags [C]//*Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*. Washington D. C., USA: IEEE Press, 2007: 217-222.
- [19] USMANI M A, KESHAVARZ S, MATTHEWS E, et al. Efficient PUF-based key generation in FPGAs using per-device configuration [J]. *IEEE Transactions on Very Large Scale Integration Systems*, 2019, 27(2): 364-375.
- [20] DOLEV D, YAO A C. On the security of public key protocols [J]. *IEEE Transactions on Information Theory*, 1983, 29(2): 198-208.
- [21] VEYRAT-CHARVILLON N, FRANCOIS-XAVIER S. Generic side-channel distinguishers; improvements and limitations [C]//*Proceedings of the 31st Annual Cryptology Conference*. Santa Barbara, USA: [s. n.], 2011: 14-18.
- [22] AMAN M N, CHUA K C, SIKDAR B. Position paper: physical unclonable functions for IoT security [C]//*Proceedings of ACM International Workshop*. New York, USA: ACM Press, 2016: 10-13.
- [23] GHAITH H, ÖZTURK E, SUNAR B. A tamper-proof and lightweight authentication scheme [J]. *Pervasive & Mobile Computing*, 2008, 4(6): 807-818.
- [24] MOHAMED Y, MOUSTAFA Y, KHALED A. Energy-aware management for cluster-based sensor networks [J]. *Computer Networks*, 2003, 43(5): 649-668.