**Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions**

**（使用物理不可克隆函数的轻量级实用匿名RFID系统认证协议）**

**一、现有基于PUF方案存在的问题：**

1.没有能够实际有效地解决DoS攻击问题；

2.后端数据库验证tag身份时使用穷举搜索；

3.tag端存储密钥，带来安全隐患，且增大了存储代价。

**二、提出的解决方案的优势：**

1.提出一种新的轻量级协议，能够抵抗DoS等恶意攻击，保证几个关键的安全属性；

2.验证时只需比较server端的TID值，避免了对CRP的穷举搜索；

3.tag端不存储密钥信息，只存储临时ID。

4.提出了一种加强的协议，使之能用于带噪声环境下的PUF。

1. **协议的具体内容：**
2. 基于无噪声理想型PUF的RFID认证协议
3. Setup阶段：

Server 产生激励Ci和一组应急激励Cem={C1,C2,...,Cn},Server(后简称S)->Tag(后简称T):{Ci,Cem},T用PUF产生Ri,Rem,T->S:{Ri,Rem},S产生临时id TIDi和一组伪ID PID={pid1,pid2,...pidn},S->T:{TIDi,PID}。

Tag最终存储{TIDi,PID},Server最终存储{TIDi,(Ci,Ri),(Cem,Rem),PID};

1. Authentication 阶段：
2. Tag产生临时值COUNT,T->S:{TIDi,COUNT};
3. Server在存储中查找TIDi,并相应读出(Ci,Ri),产生随机数Ns,依据给定规则计算通信值Ri\*,ResS,并且S->T:{Ci,Ri\*,ResS}。若TIDi查找失败，认证请求被拒绝，S寻求T使用一个未使用的pid重新尝试，pid在使用后应在两段同时删除。S对应从(Cem,Rem)中选择一个未用的CRP，并删除之，用编码方式向T提供一个TIDnew。
4. Tag用PUF和Ci产生Ri，并验证通信值ResS是否正确。若不正确则认证失败；否则依据Ri\*反推出Ns,并依据规则计算第i+1轮值Ci+1,Ri+1,TIDi+1和通信值Ki,Ri+1\*,ResT,T->S:{Ri+1\*,ResT},然后更新第i+1轮值。
5. Server依据相同规则可以计算出Ki，并验证ResT的正确性。弱不正确则认证失败；否则同样计算第i+1轮值(Ci+1,Ri+1),TIDi+1。并最终更新第i+1轮值。
6. 基于考虑噪声PUF的RFID认证协议

在考虑噪声的情况下，引入了一个模糊提取器FE:=(FE.Gen,FE.Rec)，每一轮Server需要首先对Ri使用FE.Gen产生辅助数据hd和均匀随机值K，在认证时通过FE.Rec借助hd和带有噪声的Ri重新生成K，在某一个阈值范围内，可以保证前后生成的K是一致的。通过此种方法以消除噪声对数据的影响。

每一轮Tag不存储Ri而存储hdi，Server不存储Ri而存储Ki，更新i+1轮值时hdi，Ki同时更新，hdi在不安全信道上需要加密传输。其余步骤与理想PUF情况类似。

1. 安全性能

双向认证、不可跟踪、可扩展性、前向安全性、抗DoS攻击、不可克隆、抗物理攻击、无需额外密钥一致支持。

1. **本文收获**

本文相较以前基于PUF的RFID认证协议具有许多突出优势和亮点。首先，本文在标签端不存储密钥，只存储临时ID，这为我们改进传统的密钥加密协议提供了一种很好的改进思想。其次，本文通过使用一组应急激励响应对，解决了较难解决的DoS攻击问题。其次，以这种方式，达到了一种匿名认证的效果，攻击者不知道真实的TID是标识序列中的哪一个，很好地保护了Tag的标识信息。最后，该方案同时提出了在噪声环境下的认证方案，即引入了模糊提取器，这种方法也能为我们以后的协议提供思路。

1. **改进与展望**

通过分析，不难发现本文在优势较明显的情况下仍存在不足。比如认证协议中经常考虑的存储代价的问题，一组应急激励响应对保证了一定的安全性，同时带来了存储代价过高的隐患（它与序列中的个数有关），这对于低功耗的标签系统来说可能不太实用，因此如何权衡匿名性与代价花费之间的问题，是将来值得考虑改进的一个方向。

**Physical Unclonable Function-based Key**

**Sharing via Machine Learning for IoT Security**

**（物联网安全中基于物理不可克隆函数和机器学习的密钥共享）**

**一、现有PUF密钥方案存在的问题：**

传统的弱PUF（如RO PUF）利用PUF的特性可以为每个设备生成一个唯一的密钥，但却无法做到在多个资源受限的设备上生成相同的共享密钥，这极大地限制了这种密钥生成方案在安全协议中的应用（安全协议中通常要求密钥为多方共享）。

**二、提出的解决方案的优势：**

1.使用一种可配置的弱PUF，通过配置交叉层路由，以实现延时路径的多样化；

2.通过给定的密钥和延时矩阵，通过配置路径，使不同PUF在不同PUF作用下产生相同响应；

3.考虑设计一个门限值算法计算门限值，使PUF在受温度影响的环境下仍能产生可靠的响应。

**三、方案的具体内容：**

1.可配置PUF

本文使用一种交叉环形震荡PUF（CRO PUF），具有n个环形震荡器（RO）,

m-1层交叉层，每个RO包含m个反向器。反向器由于物理因素而具有不同的延时参数，因而该结构可简化看为一个n\*m的延时矩阵。可以通过交叉层改变第i-1层与第i层反向器之间的路径选择，以使每个RO的延时路径和（RO的m个反向器延时总和）具有多样性。

1. 使用可配置PUF生成共享密钥的原理

我们假设m-1个交叉层的选择S={S1,S2,...Sm-1}为一个函数f，同时从n个RO中选择两个RO记为函数g，选择的两条延时路径的延时路径和会被计入counter器件中，最终比较两个counter中的值以得到输出。在合适的激励和配置f、g下，能使不同的PUF也能得到相同的响应，以作为共享密钥。

3.机器学习建模

由于CRO PUF的原始延时矩阵基于硬件来实现，在实际中，我们很难得到原始的延时矩阵。但我们能很容易得到两个counter中的数，因此可以枚举所有延时路径并得到它们的counter中的值来对原始的延时矩阵建模，得到一个预测延时矩阵。预测延时矩阵与原始延时矩阵具有相同的输出。

1. 门限值与可靠性

已经证明较大的延时路径差具有较好的稳定性。通过一个算法，对枚举的延时路径差进行递减排序，然后依次遍历，当恰好不能产生稳定输出时，前一个差值即为门限值。通过这种方法得到的门限值可以确保，在温度影响下大于该门限值的延时路径差都能产生可靠的响应输出。

1. 产生共享密钥的激励

让一个可信第三方（TTP）拥有CRO PUF的延时矩阵和门限，通过算法生成稳定的响应，用以生成共享的密钥。对于给定密钥的每一位，随机选择两条配置路径，若能产生稳定输出，则说明该配置激励能产生稳定的密钥位。以此枚举密钥的每一位，最终组合得到产生共享密钥的对应激励。

1. 共享密钥协议

通过共享密钥产生方案的到的共享密钥能够用于资源受限节点的多方通信。假设A与B之间需要使用共享密钥通信，A和B先将各自CRO PUF的延时矩阵发送给TTP，TTP使用各自的延时矩阵和选定的共享密钥，产生各自对应的激励并将其发回给A和B。A和B使用各自得到的激励就能生成共享的密钥。在通信时，A和B各自拥有一份相同的密钥，可以对通信信息进行加密解密操作，即可用于多方参与的基于共享密钥的通信协议中。

**四、本文收获**

本文提出了一种全新的基于PUF的共享密钥生成方案，在生成过程中不涉及密钥的传输，且有可信第三方参与，而配置信息存储于SRAM中，具有高安全性、低代价的特点。这给我们设计密钥协议方案提供了一个很好的思路，传统的共享密钥方案在资源受限的设备上很难适用。同时，方案设计时引入了门限值，考虑了PUF受温度影响的稳定性和可靠性。这也告诉我们在设计方案时要考虑健壮性和鲁棒性。

**五、改进与展望**

可以很明显地看出，本文只提供了一种共享密钥的产生方案，而并未直接将其运用到具体的通信协议中。因此，在未来我们可以充分考虑该方案的优势，加以利用而设计出一个基于PUF共享密钥的认证协议，这相较传统的PUF认证协议和共享密钥协议而言，将具备更大的优势，在低成本的资源受限的设备上将具有更大的适用性。同时，该方案只考虑了温度对PUF响应的影响，我们也可以从这点出发，改进该方案，使之在更多的物理因素影响下也能表现出稳定性，从而增强其实用性。