

研究问题

- 随着物联网技术在生产生活和工业制造中的广泛应用，海量终端设备被部署到水下，形成规模庞大的水下物联网生态系统。然而水下物联网节点在进行水下监测作业的同时，面临数据篡改、非法节点侵入等严峻安全威胁，亟需身份认证保障安全



- 水下物联网网络具有信道时延高、节点能量受限等特殊性，使得传统认证协议因交互频繁、计算存储开销大而难以适用。因此，开发轻量级身份认证技术至关重要

技术路线

- 基于非对称加密的短数字签名首次入网认证机制：网络预配置认证白名单，发起方根据私钥计算短签名，接收方根据白名单验证签名
- 基于点对点独立共享秘密的双向哈希挑战后续认证机制：首次认证后启用共享参数码本，发起方根据参数计算哈希挑战，接收方根据参数验证挑战信息
- 基于派生函数HKDF的动态混淆分片存储机制：对认证凭证进行派生，对派生凭证动态混淆，分片存储混淆凭证及相关参数
- 基于多节点信息融合的身份认证攻击智能检测机制：身份认证过程中，轻节点局部认证异常行为检测，汇聚节点全局认证异常行为检测，实现异常认证攻击类型识别，类型主要包括认证过程中易受到的诱骗攻击、重放攻击以及虫洞攻击。

短数字签名技术

目前已有的成熟数字签名技术难以将签名长度缩减至单个字节，提出一种**基于CRC32的非对称短数字签名技术**，其原理如下：

- ❑ CRC32函数数学特性

➤ 公私钥关系：公钥Q = CRC32(私钥P，种子值S)

➤ CRC32数学表示： $CRC32(M,S)=[M(x) \cdot x^{32} + S(x) \cdot x^{len(M)}] \bmod P_{crc}(x)$

➤ 原理：在CRC32线性性质下，在已有公私钥关系基础上，存在 **$CRC32(私钥||DATA, 私钥)=CRC32(公钥||DATA, 公钥)$** ，证明：

$$CRC32(Q||D, Q) = [(P+S) \cdot x^{32}] \cdot x^{\{len(D)+32\}} + D \cdot x^{32} + [(P+S) \cdot x^{32}] \cdot x^{\{len(D)+32\}} \bmod P\_crc$$
$$= D \cdot x^{32} \bmod P\_crc = CRC32(P||D, P);$$

➤ 关键：在CRC32中数据被表示为GF(2)上的多项式，而在GF(2)运算下相同值相加相当于异或，即抵消
- 改进：私钥16字节，拆分为4组4字节私钥部分；公钥16字节 = CRC32(完整16字节私钥，种子值)

➤ 核心思想：通过四轮CRC32计算和结果混合，保证安全性同时压缩签名长度至**4字节**，即：

➤ 发起方生成：短认证签名 = 四轮混合(CRC32(私钥部分||设备ID||时间戳||坐标||签名轮数, 私钥部分))

➤ 接收方验证：期望短签名 = 四轮混合(CRC32(公钥部分||设备ID||时间戳||坐标||签名轮数, 公钥部分))

签名生成与认证不局限于四轮，先暂定；此外，其中CRC32用于数字签名的安全性还有待讨论

实验进度

目前各个技术点代码功能基本实现与聚合完善，部分内容如下，同时正在查找网上已有相关身份认证论文，寻找与补充对比实验

- 密钥对初始化配置，生成4组4字节公私钥、拼接为16字节公私钥对：

```
【阶段1】设备密钥对生成（16字节 = 4×4字节）
-----
设备A（ID=0x1001）密钥派生过程：
私钥生成过程：
  生成16字节真随机数：9D 31 10 4C 9E 1F 68 B8 BD B4 F1 AC 92 29 6E B8
  私钥部分1：0x4C10319D
  私钥部分2：0xB8681F9E
  私钥部分3：0xACF1B4BD
  私钥部分4：0xB86E2992
公钥计算过程：
  公钥部分1 = CRC32(16字节私钥, 0x89ABCDEF) = 0xBBABB7FF
  公钥部分2 = CRC32(16字节私钥, 0x23456789) = 0x9D48DD20
  公钥部分3 = CRC32(16字节私钥, 0xFEDCBA98) = 0x4C4C4A7C
  公钥部分4 = CRC32(16字节私钥, 0x87654321) = 0xB9E9F3B7

最终设备密钥信息：
设备ID：0x1001
私钥(16字节)：9D 31 10 4C 9E 1F 68 B8 BD B4 F1 AC 92 29 6E B8
公钥(16字节)：FF B7 AB BB 20 DD 48 9D 7C 4A 4C 4C B7 F3 E9 B9
设备坐标：12 34 56 78
```

- 短认证签名的构建，对数据进行四轮私钥签名，最终生成4字节短签名：

```
【阶段3】设备认证过程 - 四轮签名生成
-----
步骤3.1 - 设备生成短认证签名：
输入参数：
私钥(16字节)：9D 31 10 4C 9E 1F 68 B8 BD B4 F1 AC 92 29 6E B8
设备ID：0x1001
时间戳：54 BE 76
设备坐标：12 34 56 78
签名输入数据格式(每轮14字节)：[4字节密钥部分][2字节设备ID][3字节时间戳][4字节坐标][1字节密钥版本]
四轮签名生成过程：
  第1轮：私钥部分=0x4C10319D，密钥版本=0，结果=0x045A7D7D
  第2轮：私钥部分=0xB8681F9E，密钥版本=1，结果=0x735D4DEB
  第3轮：私钥部分=0xACF1B4BD，密钥版本=2，结果=0xEA541C51
  第4轮：私钥部分=0xB86E2992，密钥版本=3，结果=0x9D532CC7
最终短认证签名(4字节)：76 2F DB 82 (0x82DB2F76)
```