|  |
| --- |
| **1．密码技术的发展怎么样，现在美国NIST征集后量子密码算法是基于什么数学原理的多？进行调研分析，解析说明。** |

后量子密码，是能够抵抗量子计算机对现有密码算法攻击的新一代密码算法。所谓“后”，是因为量子计算机的出现，现有的绝大多数公钥密码算法能被足够大和稳定的量子计算机攻破，所以可以抵抗这种攻击的密码算法可以在量子计算和其之后时代存活下来，所以被称为“后”量子密码。

实现后量子密码算法主要有以下 4 种途径：

1. 基于哈希：最早出现于 1979 年，主要用于构造数字签名。代表算法：Merkle 哈希树签名、XMSS、Lamport 签名等
2. 基于编码：最早出现于 1978 年，主要用于构造加密算法。代表算法：McEliece
3. 基于多变量：最早出现于 1988 年，主要用于构造数字签名、加密、密钥交换等。代表方法/算法：HFE (Hidden Field Equations)、Rainbow (Unbalanced Oil and Vinegar (UOV) 方法)、HFEv- 等
4. 基于格：最早出现于 1996 年，主要用于构造加密、数字签名、密钥交换，以及众多高级密码学应用，如：属性加密 (Attribute-based encryption)、陷门函数 (Trapdoor functions)、伪随机函数 (Pseudorandom functions)、同态加密 (Homomorphic Encryption) 等。代表算法：NTRU 系列、NewHope (Google 测试过的)、一系列同态加密算法 (BGV、GSW、FV 等)。由于其计算速度快、通信开销较小，且能被用于构造各类密码学算法和应用，因此被认为是最有希望的后量子密码技术

|  |  |  |  |
| --- | --- | --- | --- |
|  | 公钥大小 | 计算速度 | 功能多样性 |
| 哈希 | 大 | 较快 | 有限 |
| 编码 | 较小 | 较快 | 好 |
| 多变量 | 大 | 较快 | 较好 |
| 格 | 小 | 快 | 很好 |

|  |
| --- |
| **2．围绕密码学的发展和信息隐藏的基本原理，描述一下密码学与信息隐藏相结合的可能方式，并具例子说明。** |

加密技术通常用于实现信息存储与传输过程中的隐私保护，而信息隐藏通常用于隐藏信息的外部特征。二者结合一般表现为密文域的信息隐藏。可主要用于加密数据管理与认证，隐蔽通信等。

如：医学图像在远程诊断的传输或存储过程中通常经过加密来保护患者隐私，同时需要嵌入患者的身份、病历、诊断结果等来实现相关图像的归类与管理，但是医学图像任何一处修改都可能成为医疗诊断或事故诉讼中的关键，因此需要在嵌入信息后能够解密还原原始图片；军事图像一般都要采取加密存储与传输，同时为了适应军事场合中数据的分级管理以及访问权限的多级管理，可以在加密图像中嵌入相关备注信息，但是嵌入过程不能损坏原始图像导致重要信息丢失，否则后果难以估计；云环境下，为了使云服务不泄露数据隐私，用户需要对数据进行加密，而云端为了能直接在密文域完成数据的检索、聚类或认证等管理，需要嵌入额外的备注信息。

|  |
| --- |
| **3．我们讲了信息隐藏的载体需要有冗余空间来存放秘密信息，这个怎么理解？请举例子说明。** |

无损信息隐藏技术的实质就是找到可逆的算法规则产生有效的冗余空间，并在冗余空间中进行隐藏信息嵌入。如果没有冗余空间就无法嵌入隐藏信息；如果没有可逆规则就无法恢复不失真的原始图像。

例如，空间域方法就是在数字图像的空间范围内（例如像素值，颜色空间分量，为平面等）直接用隐藏信息来替换载体信息中的冗余部分。