后量子时代公钥密码算法概述

班级：30141806　学号：1120182525　姓名：梁瑛平

后量子密码概述

量子密码学是依靠物理学的理论基础作为密码学的安全模式的一种新概念。他的基础是单光子及其固有的量子特性，因此科学家希望以此来研究和开发一种相对先进和安全的新型密码系统。因为在不干扰量子系统的情况下，是不可能确定量子系统的量子状态的，而海森堡不确定性原理几乎保证了量子密码学成为一种无法破解的密码。

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（RSA、Diffie-Hellman、椭圆曲线等）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。也有人称之为“抗量子密码”。

后量子时代的公钥密码

公钥密码目前是足够安全的，但是量子计算机的进步和传统电子计算机的飞速发展对公钥密码的未来安全投下了阴影。为了确保互联网的长治久安，不断地完善和提高公钥密码的安全性，未雨绸缪作好充备的准备，这已经成了通信密码学界的共识。

对于密码算法安全性，主要是针对公钥密码算法：

1. 公钥密码算法安全性依赖的数学问题可以被高效的量子算法所解决。由于底层依赖的数学问题被解决，所以这些公钥密码算法不再安全。这些数学问题包括:离散对数 (及椭圆曲线版本)、大整数分解等。这直接影响目前使用的 RSA、Diffie-Hellman、椭圆曲线等算法。著名的量子算法是 1994 年的 Shor's algorithm。

2. 关于对称密码算法和哈希函数（例如 AES、SHA1、SHA2 等），虽然有量子算法可以理论上攻破，但这个算法的影响有限，且有很多限制条件。

实现后量子密码算法主要有以下 4 种途径 ：

1. 基于哈希 (Hash-based)：主要用于构造数字签名。例如 Merkle 哈希树签名、XMSS、Lamport 签名等

2. 基于编码 (Code-based)：主要用于构造加密算法。例如 McEliece

3. 基于多变量 (Multivariate-based)：主要用于构造数字签名、加密、密钥交换等。例如 HFE (Hidden Field Equations)、Rainbow (Unbalanced Oil and Vinegar (UOV) 方法)、HFEv- 等

4. 基于格(Lattice-based)：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，例如属性加密 (Attribute-based encryption)、陷门函数 (Trapdoor functions)、伪随机函数 (Pseudorandom functions)、同态加密 (Homomorphic Encryption) 等。

基于哈希的签名算法概述

基于哈希的签名算法由一次性签名方案演变而来，并使用 Merkle 的哈希树认证机制。哈希树的根是公钥，一次性的认证密钥是树中的叶子节点。并且基于哈希的数字签名算法的安全性不依赖某一个特定的哈希函数，即使目前使用的某些哈希函数被攻破，也可以用更安全的哈希函数直接代替被攻破的哈希函数。

并且基于哈希的签名算法的安全性依赖哈希函数的抗碰撞性。由于没有有效的量子算法能快速找到哈希函数的碰撞，因此（输出长度足够长的）基于哈希的构造可以抵抗量子计算机攻击。

哈希函数可以接受一串字符（任意长度）作为输入，经过“消化”后，产生固定长度的输出。常见的密码学哈希运算，像是 SHA2、SHA3 或 Blake2 等，经运算会产生长度介于 256 ~ 512 位的输出。并且一个函数 H(.) 要被称作“密码学”哈希函数，必须满足一些安全性的要求：

- 抗-原像攻击 Pre-image resistance （或俗称“单向性”）：给定输出 Y=H(X)，想要找到对应的输入 X 使得 H(X)=Y 是一件“极度费时”的工作。（这里当然存在许多例外，但最棒的部分在于，不论 X 属于什么分布，找到 X 的时间成本和暴力搜寻相同。）
- 抗-次原像攻击：这和前者有些微的差别。给定输入 X，对于攻击者来说，要找到另一个 X’ 使得 H(X)=H(X’) 是非常困难的。
- 抗-碰撞：很难找到两个输入 X1, X2，使得 H(X1)=H(X2)。要注意的是，这个假设的条件比 抗-次原像攻击还要严苛。因为攻击者可以从无垠的选择中寻找任意两个输入。

我们的目标是使用哈希函数构造数字签名方案。数字签名方法源于公钥的使用，使用者（签署人）生成一对密钥：公钥和私钥。使用者自行保管私钥，并能够用私钥“签署”任何消息，从而产生相应的数字签名。任何一个持有公钥的人都能验证该消息正确性和相关签名。

从安全的角度来说，我们希望签名是不可伪造的，或是说“存在不可伪造性”。这意味着攻击者（没有私钥控制权的人）无法在某段消息上伪造签名。

基于哈希的签名算法原理

我们假设以下条件：一个哈希函数，它能接受 256 位的输入并产生 256 位的输出。假设我们的目标是对 256 位的消息进行签名。要得到我们需要的密钥，首先需要生成随机的 512 个位字符串，每个位字符串长度为 256 位。为了便于理解，我们将这些字串列为两个独立的表，并以符号代指：

sk0= sk10, sk20, ...,sk2560
sk1= sk11, sk21, ...,sk2561

我们以列表 (sk~0~, sk~1~) 表示用来签名的 密钥。接下来为了生成公钥，

我们将随机的位字符串通过 H(.) 进行哈希运算，得到公钥如下表：

pk0= H(sk10), H(sk20), ...,H(sk2560)

pk1= H(sk11), H(sk21), ...,H(sk2561)

现在我们可以将公钥 (pk~0~,pk~1~) 公布给所有人知道。比如说，我们可以把公钥发给朋友，嵌入证书中，或是发布在 Keybase 上。

接着我们使用密钥对 256 位消息 M 进行签名。首先我们得将消息 M 重现为独立的 256 位元（Bit，又称“比特”）：

M1, M2, ..., M256 ∈ {0, 1}

签名算法的其余部分非常简单。我们从消息 M 的第 1 位至第 256 位，逐一相应在密钥列表中的其中一个密钥上取出字符串。而所选密钥取决于我们要签名的消息每一位（bit）的值。

具体一点地说，对于 i = [1,256]，如果第 i 位的消息位元 Mi = 0，我们会从 sk0 表中选择第 i 个字符 (ski0) ，作为我们签名的一部分；如果第 i 位的消息位元 Mi = 1，我们则从 sk1 表进行前述过程（即，如果我们要对消息 M 中的第 3 位进行签名，而该位值为 0，则使用 sk0 中的第三位，sk03，作为我们签名的一部分）。对每个消息位元完成此操作后，我们将选中的字符串连接，得到签名。

后量子密码算法标准化的难点

- 更广的范围：同时制定公钥加密、密钥交换和数字签名算法
- 在经典/量子计算机的攻击下，算法的安全性评估：CPA/CCA；经典/量子计算机攻击复杂度；安全性证明；其他 Cryptanalysis 结果
- 理论安全模型和实际攻击的 gap
- 安全性、性能、公约大小、签名长度、侧信道攻击等各个方面间的 tradeoff
- 应用至现有和新的安全应用中的困难程度，例如 TLS、IKE、PKI
- 由于基于多变量的陷门构造相对更为可行和高效，因此基于多变量的构造主要集中于数字签名方案，公钥加密方案较少
- 由于基于哈希的构造方案中树状结构的使用，因此目前只有数字签名的构造，缺少公钥加密算法

参考文献

[1] Bernstein D J， D Hopwood, A Hülsing, et al. SPHINCS: practical stateless hash-based signatures[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2015.

[2] Pirandola S， Andersen U L， Banchi L，et al. Advances in Quantum Cryptography[J]. Advances in Optics and Photonics, 2020, 12(4).

[3] 李益发，索敏杰，姜放. 浅谈后量子公钥密码的发展[J]. 保密科学技术，2011, 000(007):50-53.