****量子密码、后量子密码与WOTS****

1901210488 时绍森

1901210443 刘高原

## 1.量子密码

量子密码技术是传统密码学和量子物理学相结合的产物，利用光子偏振现象携带数据，利用海森堡测不准原理和量子不可复制定理实现密钥分发。相比传统数字密码技术，量子密码术拥有无条件安全性和对窃听者的可检测性，拥有巨大的发展前景。目前，国内外对量子密码学的研究处于蓬勃发展期，有大量学者对量子密码进行了研究。最早的研究始于20世纪80年代末期。1984年，Charles H.Bennett和Gilles Brassard 提出了著名的 BB84 量子密钥分配协议，此后量子密码研究课题如雨后春笋般地涌现。从2001年开始，对于量子密码的研究进入了快速发展期。此后，虽有起落，但总体呈现较快上升趋势，目前该领域仍处于研究的蓬勃发展期。

量子密码领域近5年发表的论文大多集中在以下这5个主题之中：

主 题1：量子认证研究主要包括认证协议、安全性分析、量子签名、仲裁量子签名、量子信道认证等。

主 题2：量子纠缠态研究主要包括量子纠缠态自检、量子纠缠态稳定性研究、量子纠缠态的确定性等。

主 题3：量子协议研究主要包括量子密钥分发 （BB84协议即为一种密钥分发协议）、安全直接通信（QSDC）及量子签名。用光子等粒子作为量子源，利用贝尔态、GHZ态和W态等纠缠态构建协议。

主 题4：计算攻击研究主要包括Fourier相关变换、量子因子分解、RSA算法攻击等。

主 题5：光子源研究主要指利用线性光学制备良好的可供通信的光源，包括量子比特制备、复合量子比特制备、量子比特变换、单光子信息检测技术等。

作为一种加密算法，OTP（一次性密码本）类似于其他现代密码系统，同样使用密钥来进行加密和解密，加密算法本身是公开的，其安全性由密钥的安全性来保证。OTP算法的实现需要满足 3 个条件，分别是密钥必须完全随机、密钥不能重复使用、密钥需与明文等长。其无条件安全性并不难以理解，因为与明文等长的同一密钥加密的密文只出现一次，这使得在无法获知明文的情况下，任何算法即使穷举也无法破译出该密钥；另外，密钥使用一次即丢弃，因此即便破译者得到了部分密钥也无法用于破译其他密文。

传统OTP加密美中不足之处是需要印刷大量的密码本，且实际分发操作难度很大。原则上牢不可破的OTP，一旦发送方Alice和接收方Bob用尽了预先共享的安全密钥，其安全通信将不得不中断，直到再次获取新的密钥。这就是众所周知的密钥分发难题，它涉及到经典物理中两个不可实现的任务：一是如何生成真正完全随机的密钥；二是如何在不安全的公共信道上无条件安全地分发密钥。随着量子信息技术的发展，人们发现基于量子物理学可以为这些问题提供答案：真正的随机数可以通过基本的量子物理过程生成，通过量子通信技术则可实现在公共信道上也无法窃听的密钥分发——量子密钥分发。

量子密钥分发（Quantum Key Distribution，QKD），基于量子物理的基本原理，QKD提供了一种理论上无条件安全的密钥分发方式，即使通过不安全的信道分发密钥也无法被窃听。QKD生成的安全密钥可以进一步应用于OTP方案或其他加密算法中，以提高信息安全性。量子密码学的研究源于Bennett和Brassard的开创性工作。不同于经典密码学，量子密码学的安全性保障并不来自于数学算法的计算复杂度，而是建立在量子物理学的基本定律之上。这些物理定律可以认为是永久有效的，使得QKD能够提供独特的长期安全性保障，这是量子密码学的重要特征和优势。

双方协商密钥的步骤为：Alice调制一串任意偏振的光子，并发送给Bob，Bob收到光子后随机给每个选择偏振方向，并将自己的选择告诉Alice，Alice告诉Bob他选择的正确位数是哪些，然后双方共同舍弃错误的位，留下的就是协商好的偏振方向序列，在用正确的偏振方向序列传输密钥即可。

量子密钥分发为什么不会被窃听呢？主要由于海森堡测不准原理和量子的不可克隆性，光子被观测之后状态会发生改变，因此攻击者无法观察光子的状态，观察之后光子就会发生改变，因此没有办法尝试其偏振方向。同时由于无法完整复制光子，Bob必然会丢失接受信息，一旦Bob发现，就会立即终止信息传输。

量子计算机对于密码算法安全性的威胁，主要是针对公钥密码算法：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密钥交换协议、椭圆曲线等算法。著名的量子算法是 1994 年的Shor算法。因此需要全新的公钥密码算法。

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，著名的量子算法是1996年的Grover算法。对于对称密码算法，量子计算机对安全性的影响：降低现有算法的安全性：安全性从 k-bit 降低为 k/2-bit。解决办法只需把密钥长度或哈希的长度加倍即可，例如：AES-128 升级至 AES-256，SHA-256 升级至SHA-512 等。

## 2.后量子密码

由于量子信息的奇妙特性，使得量子计算具有天然的并行性，且其计算能力可随着量子比特位数的增加呈指数增长；量子计算机的这种超强计算能力，使得基于某些数学难题的传统公钥密码的安全受到挑战；然而，量子计算机并不能解决电子计算机难于求解的所有数学问题。基于量子计算机不擅长计算的那些数学问题构造密码，就可以抵抗量子计算的攻击，我们称能够抵抗量子计算机攻击的密码为抗量子计算密码，或后量子密码。

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”，说的都是一个意思。英文中的表述是："Post-quantum Cryptography (PQC)"，或者 "Quantum-resistant cryptography"。

四种主流的后量子密码算法及其优缺点：

第一种是基于hash的后量子密码的安全性依赖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。此外，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，则可以用更安全的哈希函数直接代替被攻破的哈希函数  
 优点：安全要求是最小的；  
 缺点：只能用于量子签名方案（签名/验签）。

第二种是基于多元二次方程式密码（Multivariate-quadratic-equations-cryptography），多变量密码体制（MPKC）被认为是能够抵御基于量子计算机攻击的新型公钥密码体制之 一，利用减扰动方法构造出了一种基于MPKC的新型签名方案，其计算效率，主要指中心映射求逆的效率高于两个著名的多变量签名体制Sflash和Quartz；其安全性依赖于求解非线性方程组的困难程度，即多变量二次多项式问题。该问题被证明为非确定性多项式时间困难。目前没有已知的经典和量子算法可以快速求解有限域上的多变量方程组。  
优点：与基于hash的签名方案相比，签名较短；  
缺点：与传统的RSA、ECC等系统相比，密钥非常大；还有在MPKCs的可证明安全性没有实质性的结果。

第三种是基于编码密码（Code-based cryptography），算法原语（底层单向函数）使用纠错码，第一个基于编码密码（公钥加密方案）是由Robert J. McEliece在1978年提出的。其安全性依赖于使用错误纠正码对加入的随机性错误进行纠正和计算，量子计算机对此没有很好的办法；  
 优点：加解密速度快；  
 缺点：大型公钥大小（100KBS-几MBS），签名/验签成本大，“基于编码密码体系没有实际应用是知道”；二元Goppa码是安全的（似乎是），而其他基于编码密码体系适用应仔细考虑，有些方案看上去并不是很牢靠的。

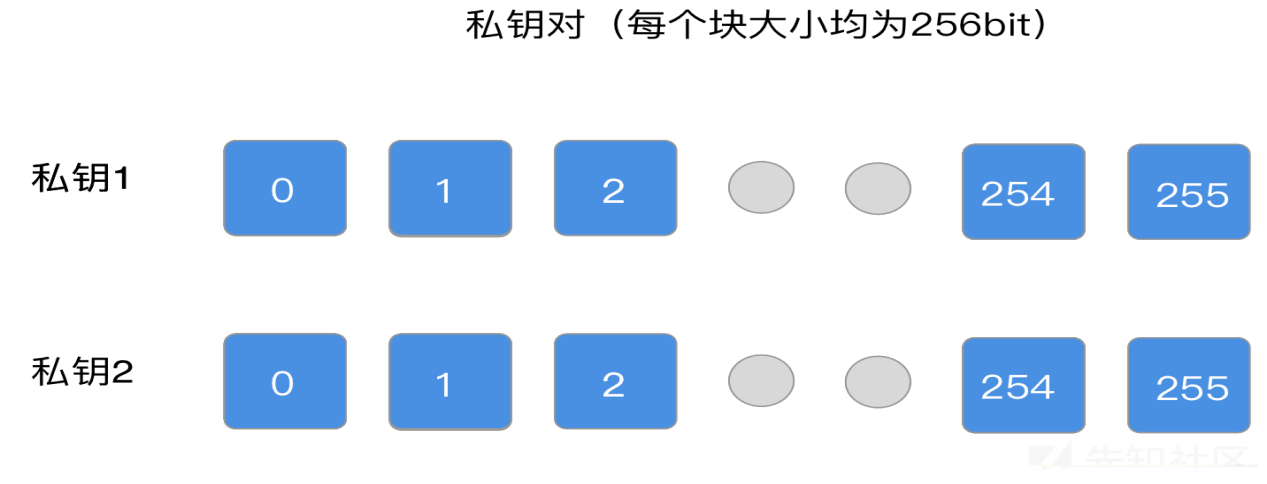
第四种是基于格密码（Lattice-based cryptography），安全性是基于最坏情况下格问题的困难，Ajtai在1996年提出“Collision-Resistant Hash Function”，Goldreichet al.在1997年提出“PKE and signature schemes”，Ajtai和Dwork在1997年提出“PKE scheme”；其安全性 依赖于求解格中问题的困难性。由于其计算速度快、通信开销较小，且能被用于构造各类密码学算法和应用，因此被认为是最有希望的后量子密码技术。  
 优点：可证明安全：基于最坏情况硬度的强安全性证明；相对高效的实现；非常简单；多用途，许多先进的密码体制的提出，例如：IBE、ABE、FHE；  
 缺点：暂无。

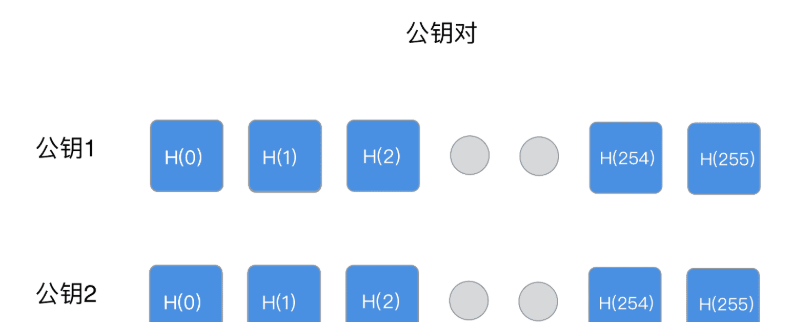
现在密码学术界，对于后量子密码的方案基本上是基于哈希函数签名和基于格密码两者结合的，基于哈希函数签名用于抗量子密码体系的签名/验签，基于格密码用于抗量子密码体系的加密/解密。下面介绍一个具体的后量子密码签名算法。

## 3.WOTS签名

WOTS，这是一种hash签名，虽然几十年前就已经提出来了，不过一直没什么人用，因为生成的签名实在太长了，而且也看不到什么明显的优点，不过近几年因为量子密码的研究以及区块链技术倒是捞了这类签名一把，因为这种基于hash的签名算法被认为是可以抵抗量子计算的，不过这种算法也存在地址不能重用的问题，每次签名都会暴露私钥的一半，下面我们就介绍一下WOTS。

先简单介绍一下Hash签名的一种——OTS(Lamport One Time Signature)：首先我们随机生成一对私钥，每个私钥都包含256个随机数，这里每个随机数都取256bit大小。

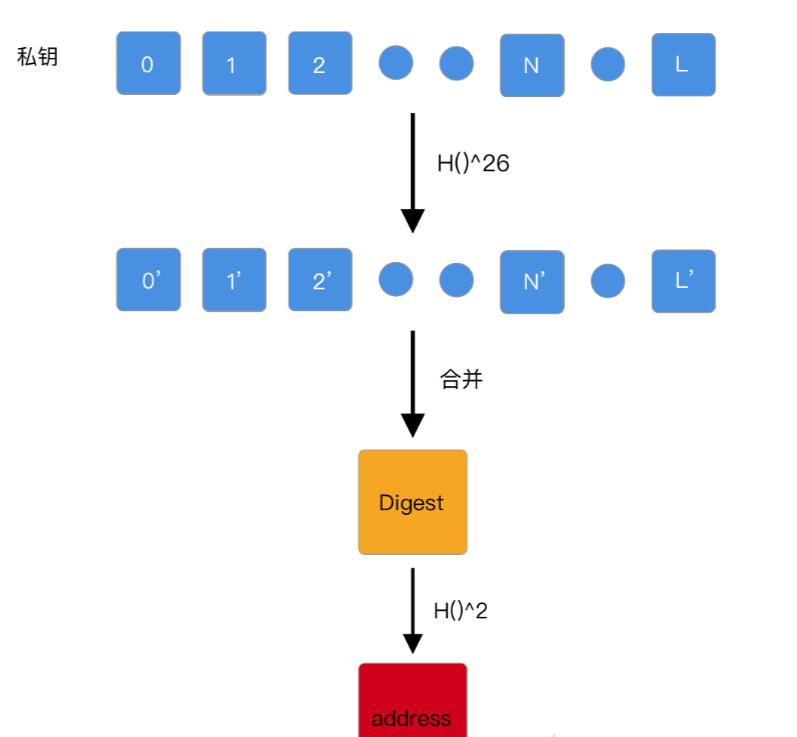


然后我们将这一对私钥中每个随机数都进行hash，得到了公钥对。

然后我们就可以开始签名了，对于文件M，首先计算得到它的hash值，H(M)，这里H(M)也是256bit长的，然后我们检查H(M)的每一个bit，对于第n个bit，当其为0时，我们就取私钥串1的第n个数，当其值为1时，我们就取私钥串2的第n个数。如M的Hash为110...10，则其签名为下图中取红色块即可。

至于该签名的验证也非常简单，我们计算出M的hash后依据同样的算法再从公钥对中取值，将公钥中的hash合并后看是否跟签名相同即可。

下面我们进入正题，在IOTA中使用的签名方案是WOTS，跟Lamport方案一样，它每次签名也会暴露私钥的一半，不过它的暴露形式却不那么一样。我们先简要了解一下IOTA中的私钥与地址的产生模式，因为每个地址都只使用一次，所以在钱包中每次都会产生一个新的地址来进行交易，一般是使用一个种子来生成这一系列的私钥。IOTA的种子也是遵循三进制的，其使用的字母就是我们前面提到的26个字母加9，长度为81。由种子我们可以产生私钥，值得一提的是在IOTA中还包含了三种安全等级，代表了不同的私钥长度。然后我们来看看派生出私钥后如何得到公钥地址，首先将私钥划分成L份，每份都是81 trytes，所以L = 安全等级 \* 27，然后我们将每一块都hash 26次，然后再合并得到digest，这是IOTA的说法，然后hash digest两次即可得到地址，也就是公钥。

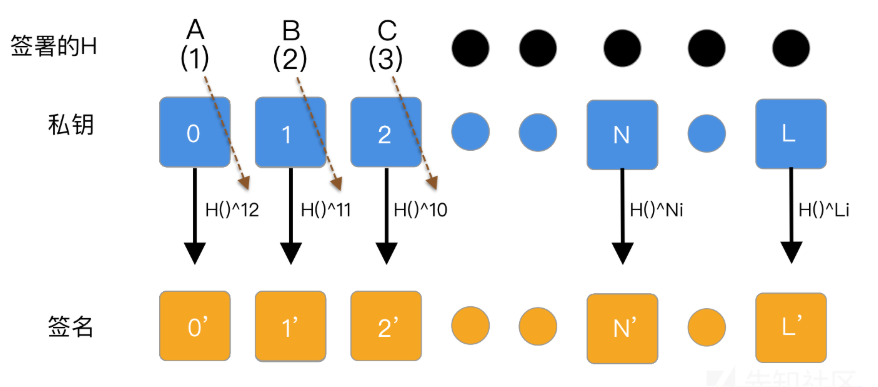


Tryte表：

下面我们来看看IOTA中的签名过程，对于消息M，我们首先计算出它的hash H(M)，不过这里使用的是IOTA中的基于三进制的hash算法，跟前面使用的hash算法一样，所以它的输出也是三进制的Tryte字母串。对于要签署的hash值H，首先我们依然是按照前面计算地址的方法将私钥分成L份，然后根据H中第N个Tryte的值来计算第N份的hash次数Ni，计算方式如下

Ni = 13 - TtoD(H[N])，(TtoD表示将该Tryte转换为10进制，转换表见上)。

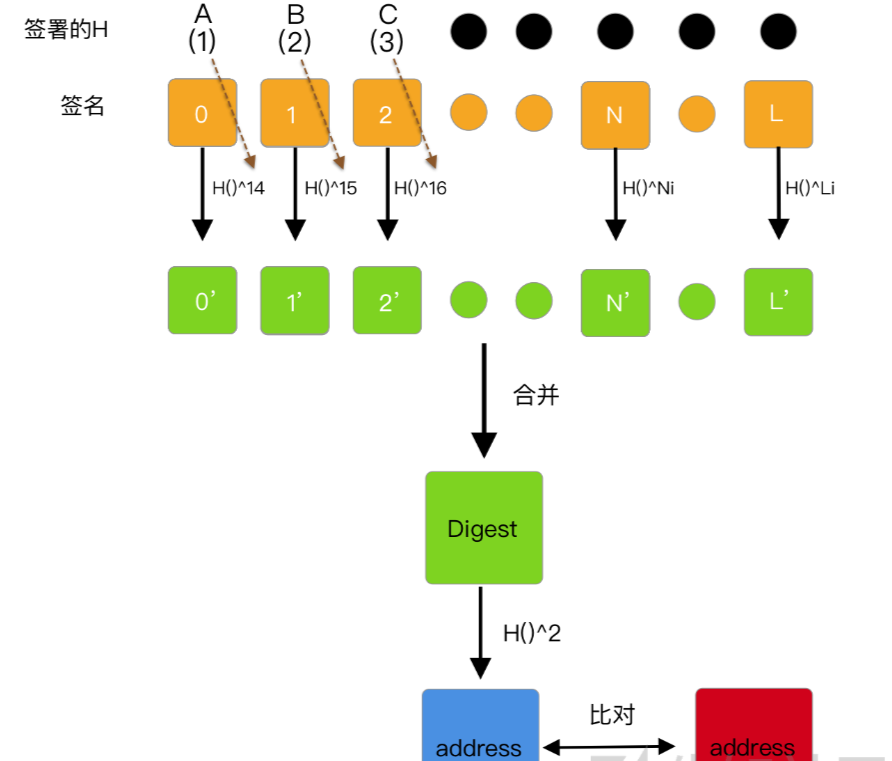
比如我们随便取一串hash，如ABC...



之后的验证过程也很简单，我们将签名划分为L份，然后根据H中第N个Tryte的值来计算第N份的hash次数Nj，计算方式如下

Ni = 13 + TtoD(H[N])。

对于上面的签名验证过程如下



当签名值正确时我们验证过后得到的digest就相当于把私钥hash了26次，所以这样与公钥验证就是符合的。

引用文献：

1. 《量子时代的网络安全挑战及其应对研究》——马彰超——2019
2. 《量子密码技术发展概述》——陆炳旭——2014
3. 《人类社会正在进入“量子技术”时代》——孙柏林——2019
4. 《量子密码技术国际研究态势分析》——李海英——2019
5. 《新量子技术时代下的信息安全》——张亮亮、张翌维、梁洁、孙瑞一、王新安——2017

6.《基于编码的后量子公钥密码研究进展》——王丽萍、戚艳红——2019

7.《IOTA Signatures, Private Keys and Address Reuse?》—2018