后量子密码技术在区块链系统中的应用

邓栊涛[1]，毛向杰[2]
（1.北京一〇一中学，北京 100091；2.杭州电子科技大学通信工程学院，浙江 杭州 310018）

摘要：随着数字货币的普及与发展，区块链技术得到了广泛的关注与极大的发展。然而，量子计算机的出现将在底层密码算法层面对区块链的安全性产生严重威胁。本文分析了量子计算机出现后对区块链技术的影响，量子计算机的出现将完全打破现有区块链技术的安全性，文章分析了后量子密码方案，在区块链系统中应用后量子数字签名技术，以保证区块链技术的在量子计算机出现后仍然安全。

关键词：后量子密码；数字签名；区块链；量子计算；去中心化
中图分类号：TP3-0 **文献标识码**：A **文章编号**：1673-1131(2018)12-0054-03

The Application of Post-quantum Cryptography in Blockchain Sysytem

Deng Longtao[1],Mao Xiangjie[2]
(1.Beijing No 101 Middle School, Beijing, 100091 China;
2.College of Communication Engineering,Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: With the popularity and development of digital currency, blockchain technology has received extensive attention and great development. However, the advent of quantum computers will pose a serious threat to the security of blockchains at the underlying cryptographic algorithm level. This paper analyzes the influence of quantum computer on the blockchain technology. The emergence of quantum computer will completely break the security of the existing blockchain technology. This paper analyzes the post-quantum cryptography scheme and applies the post-quantum digital signature in the blockchain system to ensure that blockchain technology is still safe after the emergence of quantum computers.

Key words: post-quantum cryptography; digital signature; blockchain; quantum compute; decentralization

自从中本聪在 2008 年提出比特币之后，以比特币，以太坊为代表的区块链系统得到了极大的发展和应用，而区块链系统的安全性建立在底层密码算法的安全性的基础上，如 Hash 函数的抗碰撞性，数字签名的存在不可伪造性。

与此同时，量子计算技术得到了空前的关注和极大的发展。原因之一便是量子计算机的出现将直接打破许多现有密码系统的安全性。比特币，以太坊等许多数字资产，将在量子计算机出现后面临严重威胁。所以，在区块链系统中应用在量子计算机出现后仍然安全的密码体制具有十分重要的意义。

1 后量子密码

量子计算机是一种应用量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的计算机。量子计算机以量子比特为储存载体存储信息，一个量子比特理论上可以储存无穷的信息，相较于经典计算机，具备更高的存储能力。现代物理学发展表明，量子纠缠态之间的关联效应提供了量子并行计算的能力。量子比特越多，并行计算能力越强，而要实现目前最强大计算机的功能，只需要 1000 个量子比特。在上个世纪九十年代 Shor[1]受 Simon 启发，利用数论中的一些定理，将大数的因子分解转化为求一个函数的周期问题，而后者可以用量子快速傅里叶变换(FFT)在多项式步骤内完成，同样求解离散对数问题也可以在多项式时间内求解。因此依赖于大整数分解和解离散对数问题的困难性假设将不再成立，如依赖于大整数分解的 RSA 假设、依赖于解离散对数的 DH 假设等。

后量子密码指的是通过合适的代数结构设计抵抗量子计算攻击的密码学，而量子密码学则是通过量子力学的性质创建安全的通信信道的密码学。量子密钥分发（Quantum Key Distribution，QKD）即是量子密码学中实现密钥交换的一种密码原语，其存在两个缺点：①只能运行在专门的量子通信信道下；②无法支持认证，不能抵御中间人攻击。本文考虑后量子密码体制，即在经典计算机上可运行的且被认为可以抵抗量子计算机攻击的密码体制。目前被认为具有抗量子计算特性的结构主要包括格、编码、多变量、哈希等。

2 区块链技术

区块链的概念最初由中本聪在 2008 年提出，根据中本聪的思路设计发布的开源软件以及建构其上的点对点计算机网络。点对点网络的传输意味着一个去中心化的支付系统。

比特币是一种建立在全球分布式网络上的、没有央行和第三方机构参与发行的、总量固定的加密电子货币。他是一种依据特定算法，通过大量的计算产生，比特币经济使用整个点对点计算机网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。

去中心化是区块链最基本的特征，意味着区块链的不再依赖于中央处理器节点，实现了数据的分布式记录、存储和更新。由于使用了分布式的存储和算力，不存在中心化的硬件或管理机构，全网节点的权利和义务均等，系统中的数据本质是全网节点共同维护的。

由于每个节点都必须遵循同一规则，该规则基于密码算法，比如 Hash 函数、椭圆曲线密码算法等，而非信用，同时每次数据更新需要全网其他节点的验证，所以不需要第三方中介结构或信任机构。去中心区块链系统的信息一旦经过验证并添加至区块链后，就会得到永久存储，无法更改。

区块链的安全性依赖于底层密码算法的安全性。在底层

密码算法安全的前提下，攻击区块链系统最优的方法被认为是51%攻击。

51%的攻击指的是对区块链的攻击，通常是对比特币，这种攻击需要的假设很强：由一群矿工控制超过50%的网络挖掘哈希值或计算能力。攻击者可以阻止新交易获得确认，允许他们停止部分或全部用户之间的付款。他们还可以撤销在他们控制网络时完成的交易，这意味着他们可以实现双重花费。控制51%的计算能力在一个现实系统中很难实现，所以区块链系统被认为是安全的。

3 后量子密码技术在区块链中的应用

区块链的安全性基于密码算法，如Hash函数、椭圆曲线密码算法，而在量子计算机出现后，由于量子计算机可以高效求解离散对数问题。所以基于离散对数问题困难性的数字签名算法在量子计算机出现后将不再安全。

3.1 抗量子数字签名方案

在Random Oracle模型下构造签名方案(相比与标准模型下)较为高效，目前高效的后量子数字签名方案均是在Random Oracle模型下构造的。其构造方法主要通过两种范式----Fiat-Shamir变换与Hash-and-Sign签名。

一般情况，Hash-and-Sign范式利用陷门函数构造签名：公钥是一个陷门函数f，私钥是陷门f^{-1}。签名一个消息m，首先将消息m哈希到函数f的值域上，即y=H(m)，然后输出签名$\sigma=f^{-1}(y)$。验证签名需要验证$f(\sigma)=H(m)$是否成立。Bellare和Rogaway给出上述构造方式的形式化定义，称其为Full-domain hash，并证明了当f是一个陷门置换(trapdoor permutation)，H是一个Random Oracle时，上述方式构造的签名方案满足UF-CMA安全性。上述构造方式可以给出Hash-and-Sign签名在Random Oracle模型下的安全性。

最早的基于格的Hash-and-Sign签名----GGH签名的公钥是格的一组“坏基”，私钥是一组“好基”。其签名过程是利用Babai约化算法求解消息哈希值H(m)到格上的CVP问题。GGH签名的安全假设主要依赖于：①通过格的坏基很难求得它的好基；②利用坏基很容易验证签名是否是一个格点；③通过格的坏基，敌手很难求解CVP问题。

随后提出的NTRUSign可以看作是GGH签名在NTRU格上的高效实例化。但是，GGH签名和NTRUSign的消息-签名对并不满足零知识性，足够多的签名-消息对会泄露私钥“好基”的平行六面体的形状，进而使敌手可以完全恢复出私钥。解决办法是通过选取高斯分布签名的方式构造了第一个可证明安全的格签名。但是由于高斯采样的取样过程复杂，签名的效率是制约其方案实用化的最大瓶颈。

后续的基于格的Hash-and-Sign的签名方案的发展则主要沿着下述两条路线进行：

(1)尝试修补GGH签名、NTRUSign签名的泄露。

(2)努力提高高斯采样算法的效率。

另一种构造抗量子计算数字签名的方法是应用Fiat-Shamir变换。

Identification方案是一个交互协议，允许通信一方向另一方证明自己的身份。一个3轮Identification方案，也可以看作一个Σ－Protocol，包括“commitment-challenge-response”三个阶段。Fiat-Shamir变换是将抵抗被动攻击安全(secure against a passive attack)的Identification方案，结合Random Oracle，转换为安全的签名方案的一种通用构造。

接下来讨论Fiat-Shamir数字签名方案的量子安全性，原有的Fiat-Shamir签名是考虑在经典Random Oracle模型下，利用Forking Lemma进行安全证明。而面对量子敌手时，敌手可以向Random Oracle访问量子叠加态，因此我们需要考虑Fiat-Shamir变换在量子Random Oracle下的安全性。

在经典Random Oracle模型下，假设Σ－Protocol满足zero-knowledge和special soundness的性质，那么Fiat-Shamir签名是zero-knowledge proof of knowledge。但是在量子Random Oracle模型下，上述结论并不一定成立。目前，证明了满足一些额外假设下，Fiat-Shamir变换在量子Random Oracle下是安全的。但是这个构造是渐进安全的，无法给出高效的实例化。后来证明了如果基于的Identification方案是“有损”Identification方案，那么Fiat-Shamir签名在量子Random Oracle模型下是安全的。但是，实现“有损”Identification方案可能需要更大的参数，因此方案的公钥长度与签名长度，相比于经典Random Oracle模型下，将会成倍增长。

基于格的Fiat-Shamir签名主要依赖于下述Identification方案，其结构与Schnorr-Type的签名非常相似。

我们将区块链中的数字签名算法应用后量子数字签名算法替换。以保证区块链系统的后量子安全性。

3.2 共识算法的量子安全性

共识算法是区块链的关键组成部分。它用于在分布式系统中实现各节点数据的一致性。竞争共识和协作共识算法是共识算法的两种主要类型。

比特币使用的“工作量证明”是一种竞争性共识算法。每个节点首先竞争解决难题。解决困难问题的矿工有权产生一个块，能够产生块的矿工会获得比特币奖励。该块是写入和确认事务(数据的值)的地方。然而，这场比赛对于那些没有获胜的人来说是浪费时间和金钱。除非你是第一个解决难题的人，否则你什么也得不到。由于没有人想失去，节点开始一起解决难题，并根据您的计算能力(哈希率)分享奖励。

对于量子计算机而言，相对于非对称密码系统，散列函数比较难以破解。然而，还有一种量子算法可能会使找到Hash函数的碰撞变得相对容易，即降低破解密码学散列函数的安全级别。

这种量子算法就是Grover的算法，Grover的算法允许用户在无序列表中搜索特定项。Grover的算法是概率算法：它衡量系统各种潜在状态的概率。给出了一定数量元素的无序列表，并要求找到满足某个条件的元素。可以使用经典计算机遍历每个元素以找到满足条件的元素。

然而，量子计算使用叠加来同时测试多个输入。量子计算机将使用Grover算法进行几轮计算。通过每轮计算，某些项具有所需条件的概率增加。该算法随着进展而缩小选择范围，并在结束时输出一个高概率结果。

假设在经典计算机上我们需要进行N次运算来找到一个Hash函数的碰撞，那么应用Grover算法，在量子计算机上，需要大致N/2次操作，我们就能以一个很高的概率输出一个

5kW 发射机机柜设计

魏志强，陈炳榛，林兰修
（同方电子科技有限公司，江西 九江 332002）

摘要：介绍一种有分流风道的大风量结构紧凑的强迫风冷机柜。将热设计理论计算、模拟仿真、实测样机数据进行对比分析论证。对机柜的风冷散热结构设计作了理论和实际的阐述。

关键词：结构；计算；仿真；实测
中图分类号：TN948 **文献标识码**：A **文章编号**：1673-1131(2018)12-0056-02

0 引言

5kW 发射机外形尺寸为 1.6m×0.58m×0.55m(高×宽×深)，大功率设备主要由 3 个损耗功率为 1600W 的功放模块插箱和 1 个 1200W 的电源单元插箱组成。5kW 发射机的发热器件和插箱集中布置在机柜内，由于上层的器件受到底部热流的蒸笼效应，散热困难并且受干扰。大功率的设备需要在有限空间内避开热流互相影响，且要进行大风量散热冷却，因此必须设计有效的结构方式进行通风散热。为了解决这个问题课题组设计了一种可调节风量的风道分流机柜，如图 1 所示。经过样机的运行和测试，达到预期效果。

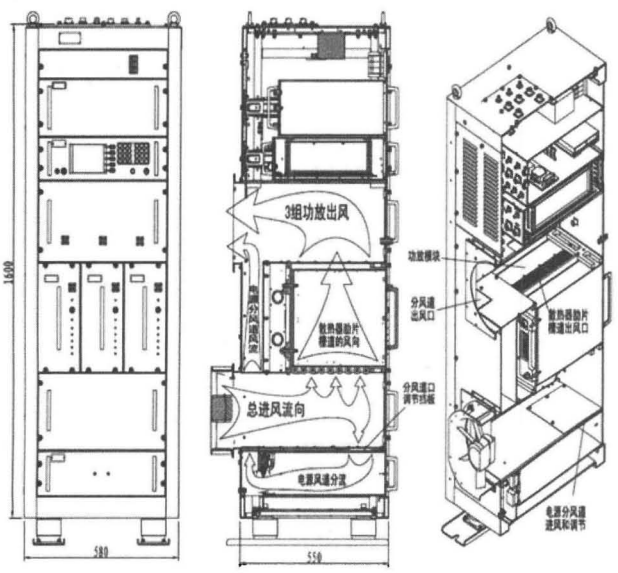

图 1 5kW 发射机机柜风道布局图

1 机柜结构方式

机柜结构主要采用钣金折弯焊接组合方式。这种结构形式设计灵活多样、加工方便，而且组成的机柜能适应多种环境。本机柜在立柱与横档的三通连接处，设计有厚板加工的连接块。这种连接块容易制造、结构牢固，在焊接时有很好的定位作用。机柜内主要运用板材加工的零部件组成热分流风道。本机柜可以采用外接风源的风道接口，也可外挂风机，进出风口均设在后部。

机柜底部放置电源单元抽屉，为解决它的热风吹过上部的器件专门设计有热空气分流风道。风道前端的进风处设计有可调节的挡板来控制风量和平衡风压。电源抽屉的后部有两个风道将热风绕过上面的三组功放模块。电源抽屉的上面是功放模块的进风道，其上部一层是三组功放散热器，再上部是出风道，这样的风道结构布局较好的解决了大风量的冷却通风。三组功放插箱各自都设置有滑轮导轨和定位导钉，方便功放插箱插拔和固定。

5kW 发射机柜的设计重点是大功率通风散热。本机柜除了设计分流风道之外，关键是有效的解决功放散热器强迫风冷的结构设计。功放散热器和风道设置有多种形式和方案，经过多次热设计的理论计算和计算机仿真模拟，我们采取的结构形式是：散热器采用整块铜材作基板上面用铝板制作肋片，肋片前端框在功放插盒内，形成封闭的蜂巢式通风槽，强迫冷风在肋片组成的风槽内吹过，散热器通风槽竖立放置。

2 散热计算

本机柜由于有热风分流的风道，解决了电源散热和功放散热互相干扰的问题。电源的散热量小于功放的散热量，本文主要针对大热量的功放模块进行热设计计算分析。

2.1 通风量计算

5kW 发射机机总损耗功率为：功放管损耗功率每个 400W，400W×4 个×3 组=4800W；电源损耗功率 1200W，=6000W。根据风量公式，取△t=15℃，计算出功放需散热通风量 Q_n=0.3m³/

碰撞。

所以对于区块链的共识机制，在量子计算机出现后，由于 Grover 算法，我们需要增加 hash 函数的安全强度，应用安全强度在 SHA-256 以上的 Hash 函数来保证共识机制的安全。

4 结语

综上所述，本文分析了量子计算机出现后对区块链技术的影响，量子计算机的出现将完全打破现有区块链技术的安全性，本文分析了后量子密码方案，在区块链系统中应用后量子数字签名技术，以保证区块链技术的在量子计算机出现后仍然安全。

参考文献：

[1] Shor, Peter W.(1997),"Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer",SIAM J. Comput.,26(5):1484-1509

[2] 吴振宇. 区块链技术的特点以及应用方法分析[J]. 网络安全技术与应用, 2017(4):121-121.

[3] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4):481-494.

作者简介：邓桄涛(2001-)，男，研究方向：网络空间安全；毛向杰(1994-)，男，单位：杭州电子科技大学通信工程学院。