基于HotStuff的高效量子安全拜占庭容错共识机制

程安东, 谢四江, 刘昂, 冯艺萌

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230600200

基于 HotStuff 的高效量子安全拜占庭容错共识机制

程安东[1]　谢四江[1,2,3]　刘　昂[1,4]　冯艺萌[1]
1 北京电子科技学院网络空间安全系　北京 100070
2 西安电子科技大学计算机科学及技术学院　西安 710000
3 中国科学技术大学网络空间安全学院　合肥 230026
4 北京邮电大学网络空间安全学院　北京 100876
(caddxy@foxmail.com)

摘　要　经典区块链中拜占庭容错共识机制使用的公钥数字签名在量子计算机的指数级加速下暴露出脆弱性,存在一定的安全风险。针对拜占庭容错共识机制不具有量子安全性的问题,提出了基于 HotStuff 的高效量子安全拜占庭容错共识机制 EQSH(Efficient Quantum-Secured HotStuff)。首先,为解决现有无条件安全签名(Unconditionally Secure Signatures,USS)通信复杂度高的问题,提出了一种高效的多方环形量子数字签名(Efficient Multi-party Ring Quantum Digital Signatures,EMRQDSs)方案,该方案基于一种环形量子网络,在保证量子安全性、不可伪造性、不可抵赖性以及可转移性的同时,通信复杂度为 $O(n)$。其次,为了消除量子敌手对门限签名的安全威胁,对 HotStuff 中使用的门限签名进行替换,提出了一种基于密钥分发中心的签名收集方案,该方案可以实现与门限签名同样的效果,通信复杂度为 $O(n)$,同时保证了量子安全性。最后,将上述两个方案相结合,应用于 HotStuff 中,提供了量子安全性;设计了一个起搏器保证了活性;简化了共识信息格式,使用流水线共识流程提高了共识效率。EQSH 中没有使用量子纠缠等成本较高的技术,可在现有技术条件下实现,实用价值较高。相较于 HotStuff,EQSH 具有量子安全性。相较于其他非纠缠型量子安全拜占庭容错共识机制,EQSH 首次将通信复杂度降为 $O(n)$,具有更佳的性能表现,且对于客户端量子线路数量的需求更低,有利于降低量子网络的架设成本。

关键词:拜占庭容错共识机制;非纠缠;量子安全;量子数字签名;环形量子网络
中图分类号　TP393

Efficient Quantum-secure Byzantine Fault Tolerance Consensus Mechanism Based on HotStuff

CHENG Andong[1],XIE Sijiang[1,2,3],LIU Ang[1,4] and FENG Yimeng[1]
1 Department of Cyberspace Security,Beijing Electronic Science and Technology Institute,Beijing 100070,China
2 College of Computer Science and Technology,Xi'an University of Electronic Technology,Xi'an 710000,China
3 School of Cyber Science and Technology,China University of Science and Technology,Hefei 230026,China
4 School of Cyberspace Security,Beijing University of Posts and Telecommunications,Beijing 100876,China

Abstract　The public-key digital signature used by Byzantine fault tolerance consensus mechanism in the classic blockchain exposes vulnerability to quantum computers that have the exponential acceleration of computing power,and therefore have security risks. To address the problem that the Byzantine fault tolerance consensus mechanism does not have quantum security,this paper proposes an efficient quantum secure Byzantine fault tolerance consensus mechanism based on HotStuff,known as EQSH(efficient quantum secure HotStuff). Firstly,an efficient multi-party ring quantum digital signatures(EMRQDSs) scheme is proposed to solve the problem of high complexity of unconditionally secure signatures(USS) communication. The scheme is based on a ring quantum network that guarantees post-quantum security,non-enforceability,non-repudiation,and transferability while the communication complexity is $O(n)$. Secondly,the gated signature used in HotStuff is improved,instead,we propose an alternative scheme for post-quantum security,i.e.,a signature collection scheme based on a key distribution center,which could achieve the same effect as gated signature while guaranteeing post-quantum security with a communication complexity of $O(n)$. Subsequently,the above two schemes are adopted in HotStuff to provide post-quantum security;a heartbeat is designed to ensure the activity;the consensus message format is simplified and the consensus efficiency is improved by using a pipelined consensus process. Costly techniques such as quantum entanglement are not used in EQSH,our scheme can be implemented under existing technolo-

到稿日期:2023-06-26　返修日期:2024-05-04
基金项目:科技创新 2030——"量子通信与量子计算机"重大项目(2021ZD0300705)
This work was supported by the Innovation Program for Quantum Science and Technology(2021ZD0300705).
通信作者:谢四江(xiesj@besti.edu.cn)

gy conditions and thusis of high practical value. Compared to HotStuff, EQSH has post-quantum security. Compared with other non-entangled quantum-secured Byzantine fault tolerance consensus mechanisms, EQSH reduces the communication complexity to $O(n)$ for the first time and has better performance which requires less quantum circuit resourcesfor the client, which is beneficial to the construction of quantum networks.

Keywords Byzantine fault tolerance consensus mechanism, Non-entanglement, Quantum security, Quantum digital signatures, Ring quantum network

1 引言

区块链是一种分布式账本技术,其需要确保系统中的各个节点达成一致。共识机制是确保区块链系统正确运行的核心。拜占庭容错共识机制是一类可以在存在故障节点与恶意节点的分布式系统中达成一致的共识机制,被应用于许多许可区块链中。

在拜占庭容错共识机制的早期研究[1]中,一直存在通信复杂度较高的问题,并且这些协议的通信复杂度普遍会随着拜占庭节点数目的增加呈指数级增长,共识效率低,不具备可扩展性。1999 年,Liscov 等提出了实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT[2])算法,该算法首次将通信复杂度降至 $O(n^2)$。PBFT 是应用最广泛的拜占庭容错共识机制,但其视图切换的通信复杂度为 $O(n^3)$。为了解决该问题,Buchman 等提出了Tendermint[3-4],将视图切换的通信复杂度降为 $O(n^2)$,但复杂度依然过高。由于 PBFT 和 Tendermint 均为适用于小型系统的通信密集型协议,在大规模系统中过高的通信复杂度会极大地降低系统性能。因此,2019 年 Yin 等提出了 HotStuff[5],使用门限签名对 Tendermint 进行改进,将通信复杂度降至 $O(n)$,使 Tendermint 可以应用于大规模系统。其中最典型的案例是 HotStuff 被应用于 Facebook 的 Libra 项目。

在拜占庭容错共识机制降低通信复杂度和提高效率的同时,量子计算技术也在加速发展。上述传统拜占庭容错共识机制的安全性基于公钥数字签名等密码技术,在以 Shor 算法[6]为代表的量子计算攻击下存在安全风险,从而导致建立在这些共识机制基础上的区块链系统同样存在被量子计算攻击破解的风险[7]。

为应对量子计算对区块链系统造成的威胁,学术界有两个研究方向。其一是后量子区块链[8],使用后量子签名算法[9]替换经典签名算法,为区块链系统提供量子安全性。此类方案基于目前某些不能被量子计算机有效解决的计算复杂性难题,不能从理论上严格证明[10],且不能保证未来不会被量子计算机破解。其二是量子区块链,该类方法使用量子力学的基本物理特性来保证安全,将量子技术引入区块链系统,为区块链提供了量子安全性。

近年来,有许多学者开展了关于量子区块链的相关研究。文献[11]提出了一种基于时间纠缠的量子区块链;文献[12]提出了一种将时间纠缠量子和 DPoS(委托权益证明)结合的区块链方案;文献[13]提出了一种使用量子哈希函数和量子交换测试电路的量子区块链;文献[14]提出了一种基于 QDPoS 的量子区块链;文献[15]提出了使用量子态公钥的 QBoT 量子区块链;文献[16]提出了基于改进的 DPoS 共识算法和量子签名的区块链方案;文献[17]提出了基于 Bell 态纠缠和量子权威证明(QPoA)共识机制的区块链方案。上述方案中涉及的量子纠缠等量子技术大多仍处于理论研究阶段,实现难度极大,可行性低[18]。量子区块链的部分研究使用 QKD[19]等发展较为成熟的量子技术[20]作为底层技术,文献[21]使用 QKD 结合原始状态机复制的共识机制[1]构造了 QB(Quantum-secured blockchain)区块链系统,其通信复杂度会随拜占庭节点数目的增加呈指数增长;文献[18]将无条件安全签名(Unconditionally Secure Signatures, USS[22])简化后提出 TGS(Toeplitz Group Signature)签名方案,在 QB 的基础上将简化后的 YAC[23](Yet Another Consensus)共识机制结合 TGS 提出 QSYAC 共识机制,构造了 LC 区块链,通信复杂度为 $O(n^3)$;文献[24]使用量子直接通信技术分发一种特殊的列表,提出了量子诚实-成功的拜占庭协议(Quantum honest-success Byzantine Agreement, QBA),构造了 QLB 区块链;文献[25]基于 QB 加入了 DPoS 机制,一定程度地降低了线路复杂度;文献[26]在 LC 区块链的基础上,改进了 TGS 签名方案的运算效率,提出了 MH-USS 签名方案,该方案将 QSYAC 替换为一种改进型 PBFT 协议(QS-BFT),通信复杂度为 $O(n^3)$,同时简化了视图转换的步骤,提高了共识效率;文献[27]提出了一种可以应用于区块链的新拜占庭容错共识机制,通过多次嵌套使用一种非纠缠的三方量子数字签名(QDS[28])首次突破了拜占庭共识的容错上限,可以容忍 1/2 的不诚实节点,通信复杂度为 $O(n^{f+1})$,f 是不诚实的节点数。

文献[18,21,24]在不使用量子纠缠等成本较高的技术的条件下,提出了量子安全拜占庭容错共识机制,进而构造了具有量子安全性的区块链方案,具有较高的实用性。但是这些协议的通信复杂度仍然较高,普遍在 $O(n^2)$ 以上,且部分协议存在一定的安全风险。如文献[18]和文献[26]使用的 USS 方案简化了验证等级和争端解决机制,存在被串通攻击的安全风险[29];Cholvi[30]指出文献[24]中的 QBA 方案存在安全风险。因此,对于量子安全区块链,目前仍缺少通信复杂度较低的无纠缠量子安全拜占庭容错共识机制。

为了解决上述问题,本文基于 HotStuff 提出了一种具有量子安全性的区块链共识机制。该方案提出在客户端中使用一种高效的多方环形量子数字签名(EMRQDSs)方案签署客户端的信息,可以抵御串通攻击和陷害攻击;在进行共识的节点间使用基于密钥分发中心的签名收集方案,代替 HotStuff 中的门限签名方案,且收集一次签名的通信复杂度和门限签名一致均为 $O(n)$。这两种签名的方案均使用了 QKD 的相关技术以及抗量子计算攻击[31]的全域哈希函数(Universal Hash[32]),保证了量子安全性。本文将具有量子安全性的

签名方案融入 HotStuff 中，并优化了 HotStuff 中的消息格式，进而设计了基于 HotStuff 的高效量子安全拜占庭容错共识机制（Efficient Quantum-SecuredHotStuff，EQSH）。相较于目前已有的无纠缠量子安全拜占庭容错共识机制，EQSH 降低了通信复杂度，提高了共识效率，减少了量子信道的数量，降低了网络的建设成本，提高了安全性，具有较高的实用性。

2 背景知识

2.1 HotStuff

HotStuff 相较于其他在 PBFT 基础上改进的拜占庭容错共识机制，使用三阶段确认代替两阶段确认，使用门限签名进行一对多通信，使通信复杂度降为 $O(n)$，将视图切换隐含在每一轮共识中，使视图切换的通信复杂度降至 $O(n)$。HotStuff 的每次共识有一个唯一的视图编号，视图编号单调递增，每个视图编号由特定的节点所有，由起搏器控制，将安全性和活性进行了解耦。当领导节点为拜占庭节点时，等待视图超时后，由起搏器控制更换领导节点并开始新视图编号的共识。基础 HotStuff（Basic HotStuff）达成一次共识需要经过 Prepare，Pre-Commit，Commit 和 Decide 4 个阶段，总共通信 $6(n-1)$ 次；链式 HotStuff（Chained HotStuff）达成一次共识平均需要一个阶段，通信 $2(n-1)$ 次；通信复杂度均为 $O(n)$。

2.2 无条件安全签名方案

无条件安全签名方案（USS）是一种具有量子安全性的签名方案[22]，其量子安全性由量子真随机性、量子不可克隆原理与一次一密共同保证[18]。USS 和传统基于公钥密码学的签名方案一样，可以签署任意长度的信息并保证不可伪造性、不可抵赖性和可转移性。不同之处在于 USS 使用对称密钥进行签名，这些对称密钥由 QKD 生成；结合 Universal Hash，USS 使用由 QKD 生成的不完美密钥也可以保证量子安全性[33]。USS 牺牲签名长度、可重复使用性和密钥大小等方面的效率获得了量子安全性[22]，其无需使用量子纠缠等成本较高的技术，且不依赖于可信第三方或匿名信道进行消息传输[26]。USS 一般需要一个准备阶段，在准备阶段，秘密密钥在所有验签者之间交换，之后才能签署或验证信息[22]。

下面简要分析文献[34]中的 USS 方案。

在准备阶段，首先签名者使用 QKD 产生的对称密钥，向不同的验签者共享一组不同的密钥，如图 1(a)所示；然后所有验签者同样使用 QKD 产生的对称密钥，互相秘密交换部分密钥，该过程也被称为密钥对称，如图 1(b)所示。经过准备阶段后每个验签者只知道部分密钥，因此无法伪造签名，只能进行验签；签名者知道所有密钥，但不知道特定验签者拥有的密钥子集，保障了签名的可转移性。

在信息传递阶段，签名者用自己掌握的所有密钥，通过 Universal Hash 对需要签署的信息 m 进行哈希值的计算，组合这些哈希值得到信息 m 的签名，将信息 m 和签名发送给验签者，验签者之间也可以互相传递信息 m 和签名；在验签时，验签者利用自己掌握的部分密钥，同样计算哈希值，然后进行对比，若一定比例的哈希值相同，则在一定的验证级别接受签名。当不同验签者对一个签名的有效性产生分歧，则进行一次多数票表决以解决争端[29]，并最终确定是否接受该签名。其中的多数票机制采用安全广播协议[35-36]。

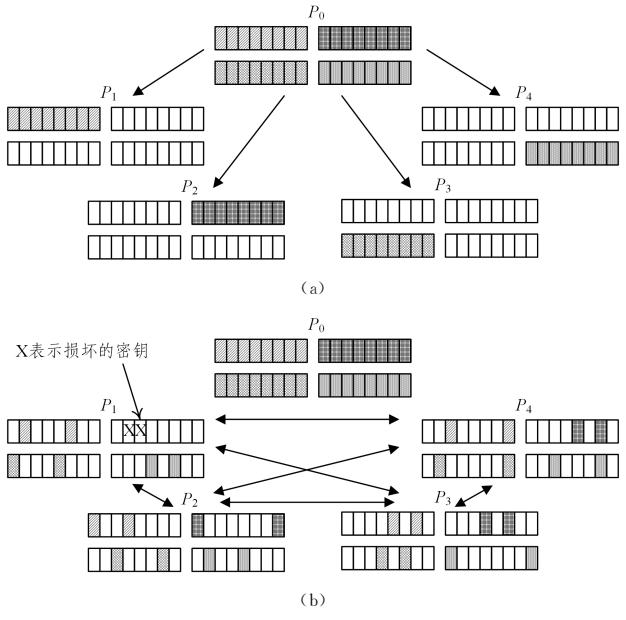

图 1 USS 的准备阶段

Fig. 1 Preparation phase of USS

定义 1（通信复杂度） 对于某一协议，完成一次协议各个节点需要通信的总次数称为通信复杂度。

设系统中有 n 个节点，其中 1 个节点进行一次 USS 签名需要 $(n-1)+(n-1)(n-2)$ 次通信，因此进行一次 USS 签名的通信复杂度为 $O(n^2)$。

当一个不诚实的验签者在准备阶段交换部分损坏的密钥，同时，不诚实的签名者用特定组的密钥签名，可以使诚实的验签者之间对签名的有效性产生分歧（如图 2 所示），进而使诚实的验签者发起多数票表决，实现陷害攻击[37]。陷害攻击并不会对 USS 的安全性造成破坏，但会消耗大量的系统资源。

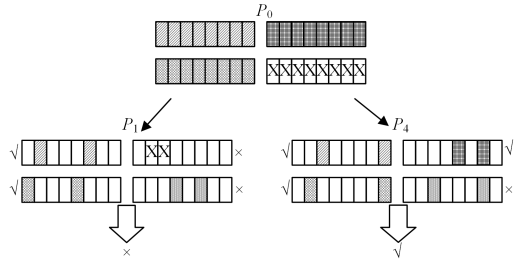

图 2 陷害攻击

Fig. 2 Framing attack

当 USS 省略了验证等级和争端解决机制，使用单一的阈值验证签名时，陷害攻击将会变为串通攻击[38]。串通攻击会使诚实的验签者对同一个签名的有效性产生分歧，从而直接破坏 USS 的可转移性，直接威胁 USS 的安全性。文献[18]提出的 TGS 签名方案和文献[26]提出的 MH-USS 签名方案均简化了验证等级和争端解决机制，存在被串通攻击的风险。

3 签名方案设计

3.1 高效的多方环形量子数字签名

本文在多方环形量子数字签名[39]的基础框架上进行了优化，结合 Universal Hash，提出了一种高效的多方环形量子数字签名(EMRQDSs)方案。该方案通过环形量子网络实现密钥的协商，通过经典网络完成签名信息及各种经典消息传输。相较于原多方环形量子数字签名方案，该方案通过一次签名就可以完成对任意长度信息的签名，效率更高，同时与原协议一样具有不可伪造性、不可抵赖性、可转移性以及量子安全性。

进行一次 EMRQDSs 主要包括 3 个阶段：密钥分配阶段、签名阶段和验签阶段。假设签名方案中有 1 个签名者和 n 个验签者，则将他们统称为参与者。

3.1.1 网络架构

所有的参与者之间通过一个环形的不安全的量子网络相连，每个节点只有 2 条量子信道和相邻的节点连接，如图 3 中的虚弧线所示，点弧线部分表示可以加入多个节点。所有参与者之间有全连接的经过认证的经典信道，如图 3 中的直线所示，用于传递经典信息。

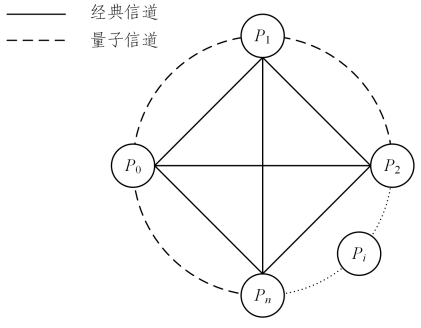

图 3 EMRQDSs 的网络架构

Fig. 3 Network structure of EMRQDSs

3.1.2 密钥分配阶段

密钥协商阶段需要确定签名者的“私钥”和各个验签者不同的“公钥”。该阶段和文献[39]中的分配阶段大致相同，具体分为 3 个步骤：

1)签名者随机生成一个包括 L 个密钥的序列 $K_M=\{k_1,k_2,\cdots,k_L\}$。$K_M$ 作为签名者的私钥，其中每一个 k_i 的长度均相等，用于 Universal Hash 计算哈希值，设 k_i 的长度为 x。对于每一个密钥 k_i，签名者随机选择 Z 基或者 X 基，生成一个密钥光子块 Q_{k_i}，Q_{k_i} 中的光子使用相同的基矢；每个密钥光子块 Q_{k_i} 包括多个光子块 $|k_i(j)\rangle^{\rho}$，$|k_i(j)\rangle^{\rho}$ 中的光子具有相同的相位 $|k_i(j)\rangle$ 和空间位置信息，其中 j 表示 k_i 的第 j 位。使用 k_i^j 表示密钥 k_i 第 j 位的经典比特，$k_i^j\in\{0,1\}$。如果 $k_i^j=0$，选择了 Z 基则 $|k_i(j)\rangle=|0\rangle$，选择了 X 基则 $|k_i(j)\rangle=|-\rangle$；如果 $k_i^j=1$，选择了 Z 基则 $|k_i(j)\rangle=|1\rangle$，选择了 X 基则 $|k_i(j)\rangle=|+\rangle$。Z 基和 X 基的关系如式(1)所示。然后签名者将密钥光子块 Q_{k_i} 组成编码光束 Q_{key}，Q_{k_i} 和 $|k_i(j)\rangle^{\rho}$ 的关系如式(2)所示，Q_{key} 与 Q_{k_i} 的关系如式(3)所示。签名者随机选择顺时针(或逆时针)方向发送编码光束 Q_{key}，同时在逆时针(或顺时针)方向发送诱骗态[40-42]的参考光束。编码光束和参考光束具有相同的偏振，以便在二者传输完成后返回签名者时进行干涉，从而判断密钥分配的过程是否被攻击。

$$\begin{cases}|+\rangle=\dfrac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\\ |-\rangle=\dfrac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\end{cases}\tag{1}$$

$$Q_{k_i}=\bigotimes_{j=1}^{x}|k_i(j)\rangle^{\rho}\tag{2}$$

$$Q_{key}=\bigotimes_{i=1}^{L}Q_{k_i}\tag{3}$$

2)所有验签者在收到编码光束 Q_{key} 或者参考光束后，对于每个光束中的密钥光子块 Q_{k_i} 以 $1/(n+1)$ 的概率抽样，对于每一个被抽样的 Q_{k_i} 则随机选择 Z 基或者 X 基，然后用一样的基观测其中每一个光子块 $|k_i(j)\rangle^{\rho}$ 的一个光子 $|k_i(j)\rangle$。最后记录自己的观察结果。

3)签名者通过返回的两个光束判断之前的步骤是否被攻击，具体方法和文献[39]一致。若没有被攻击，则在经典信道公布哪个方向(顺时针或者逆时针)的光束是编码光束，并指明对于每个密钥光子块 Q_{k_i} 所选取的基矢。验签者留下基矢对比一致的 k_i，组成自己验签的公钥 $K_{m,a}$，其中 a 表示 a 节点，$K_{m,a}$ 的长度 k 的数学期望是 $L/2(n+1)$。与此同时，验签者与文献[39]一样也要进行基于诱骗态的最小熵误差率[43-44]的估计，验证有无攻击发生，如果有则要求重启协议，以保证量子安全性。

经过密钥分配阶段，签名者确定了自己进行签名的私钥 $K_M=\{k_1,k_2,\cdots,k_L\}$，而每个验签者得到 K_M 中的一部分作为自己的公钥 $K_{m,a}$，如图 4 所示。验签者不知道全部密钥，因此无法伪造签名，保证了不可伪造性。签名者不知道验签者得到的是哪部分密钥，无法针对某一个签名者伪造特定的签名，从而保障了可转移性。

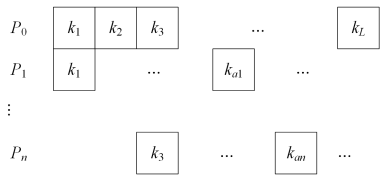

图 4 不同的参与者掌握的不同密钥

Fig. 4 Different keys held by different participants

3.1.3 签名阶段

签名者使用私钥 $K_M=\{k_1,k_2,\cdots,k_L\}$ 和 Universal Hash 生成信息 m 的签名 $Sign(m)$，如式(4)所示，其中的 $h(m)$ 采用 Universal Hash。

$$\begin{aligned}Sign(m)&=(h_{k_1}(m),h_{k_2}(m),\cdots,h_{k_L}(m))\\&=(t_1,t_2,\cdots,t_L)\end{aligned}\tag{4}$$

然后签名者将 $\langle m,Sign(m)\rangle$ 发送给各个验签者。

3.1.4 验签阶段

验签者 a 通过公钥 $K_{m,a}$、信息 m 和 Universal Hash 计算对应位置的哈希值，然后和 $Sign(m)$ 中对应位置的 t 进行对比，判断是否匹配，如式(5)所示。累计不匹配的数量 H，如式(6)所示。若不匹配数量 $H<V_{(a,s)}k$，则称验签者 a 在验证等级 s 接受该签名，阈值 $V_{(a,s)}$ 表示在允许签名中不能通过验证部分的最大比例，$0<V_{(a,s)}<1$。当一个签名被接受时，$s\geqslant 0$。

文献[39]中给出了 $V_{(a,0)}$ 和 $V_{(a,1)}$ 的推荐值，如式(7)、式(8)所示，其中的 e^{guss} 和 e^{hone} 是和物理系统有关的常数。

$$H_{k_a}(t_a)=\begin{cases}0 & t_a=h_{k_a}(m)\\ 1 & t_a\neq h_{k_a}(m)\end{cases} \tag{5}$$

$$H=\sum_{k_a\in K_{m,a}} H_{k_a}(t_a) \tag{6}$$

$$V_{(a,0)}=\frac{1}{2}(e^{\text{guss}}+e^{\text{hone}}) \tag{7}$$

$$V_{(a,1)}=\frac{1}{2}(3e^{\text{guss}}-e^{\text{hone}}) \tag{8}$$

3.1.5 争端解决策略

在参与者对一个签名的有效性产生分歧时，使用争端解决策略做出对该签名有效性的最终判决。一般的方法主要分为可信第三方机制和多数票机制[29]。可信第三方机制的优势是效率更高；而多数票机制的优势是无需信任固定的节点，只需要假设系统中大部分节点为诚实节点。文献[39]中给出了该协议中使用多数票机制最多可以容忍的不诚实节点的比例 $d_f<1/3$，但没有给出具体的多数票机制。受到 PFBT 协议的启发，本文提出一种多数票机制，该方案需要节点间有经过认证的经典信道，且不诚实节点的比例 $d_f<1/3$。具体分为 3 个阶段，流程如图 5 所示。

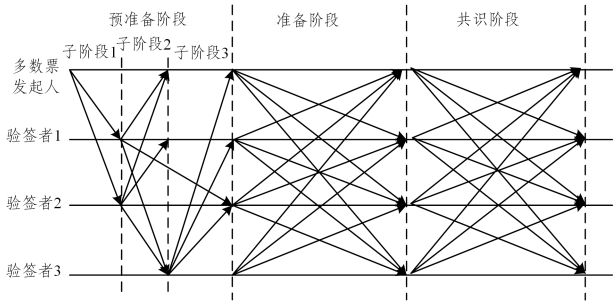

图 5 多数票机制的流程

Fig. 5 Process of majority vote mechanism

和签名方案的假设一致，下面以一个 $n+1$ 节点的系统来描述各个阶段。为了方便表示，假设 $n+1=3f+1$，f 是最多可以容忍的不诚实节点数，$f=d_f(n+1)-1$。

1)预准备阶段：该阶段用于各个节点发布自己对于某个签名的有效性的认可情况。由一个多数票表决发起人发起，为了防止发起人屏蔽部分节点参加投票，该阶段有 3 个子阶段。子阶段 1 中由发起人 i 向其他节点发送〈m，$sign$，s_i，$START1$〉，其中的 s_i 表示节点 i 对于该签名的验证等级；$START1$ 是一个字符串，表示现在是子阶段 1。子阶段 2 中收到 $START1$ 的节点发送自己对于该签名的验证等级〈m，$sign$，s，$START2$〉。子阶段 3 中只有没有收到过 $START1$ 的节点进行，发送〈m，$sign$，s，$START3$〉。如果在子阶段 2 完成后，节点收到 n 个不同节点(包括自己)的 $START2$ 信息，则等待一个子阶段的时间，然后进入下一阶段。如果在子阶段 3 完成后，节点收到至少 $2f+1$ 个不同节点(包括自己)的 $START2$ 或 $START3$ 信息，则进入下一阶段。其他情况认为协议失败，不继续执行。

预准备阶段完成后各个节点根据自己获得的信息得到一个各个节点验证等级的列表，没有收到的用⊥表示。这个列表确保了至少有 $2f+1$ 个元素和其他诚实节点相同，称为验证等级列表。如表 1 所列，每一行为某个节点本地的验证等级列表。

表 1 预准备阶段的验证等级

Table 1 Validation levels of the preparation phase

	s_0	s_1	…	s_n
P_0	0	1	…	1
…	…	…	…	…
P_n	⊥	−1	…	1

2)准备阶段：该阶段用于各个节点发布自己保存的验证等级列表。各个节点发送自己的验证等级列表给每个节点(包括自己)，信息格式为〈S，$PREPARE$〉，其中 $S=\{s_0,s_1,\cdots,s_n\}$ 表示一个验证等级列表。该阶段在一个阶段的时间后进入下一阶段。然后各个节点根据收到的信息更新自己的验证等级列表。如果收到来自不同节点的验证等级列表对于某个元素 s_i 有至少 $2f+1$ 个相同的值 s'，则设 $s_i=s'$，否则设 $s_i=\perp$，$i\in[0,n]$。

3)共识阶段：该阶段各个节点发布更新后的验证等级列表并确定最终的多数票结果。各个节点发送自己的验证等级列表给每个节点(包括自己)，信息格式为〈S，$COMMIT$〉。各个节点根据收到的信息更新自己的验证等级列表，规则和上一步一致。

更新完成后，各个节点独立完成对于多数票的统计，并对该签名是否有效做出最终判断。统计的规则如式(9)所示，对于签名有效性的判断如式(10)所示。

$$vote_i=\begin{cases}1, & s_i\geqslant 0\\ 0, & \text{其他}\end{cases} \tag{9}$$

$$MV(m,sign)=\begin{cases}\text{接受}, & \sum_{i=0}^{n} vote_i>\dfrac{n+1}{2}\\ \text{拒绝}, & \text{其他}\end{cases} \tag{10}$$

多数票机制并非每次进行签名的必要环节，只有参与者对一个签名产生分歧时才会执行。多数票机制的通信成本较高，需要对失败的一方进行一定的惩罚，防止恶意节点浪费系统资源。

3.2 安全性分析

本文提出的 EMRQDSs 方案具有不可伪造性、不可抵赖性、可转移性以及量子安全性。相较于同样满足这些安全特性的 USS 方案，EMRQDSs 还可以防止陷害攻击。

文献[39]中证明了签名者可以将一个二进制的序列，通过一个环形的量子网络，使用随机抽样的方式安全地使每个验签者获得其中的部分比特，而这些参与者不知道彼此获得的比特是哪部分，如图 6 所示。

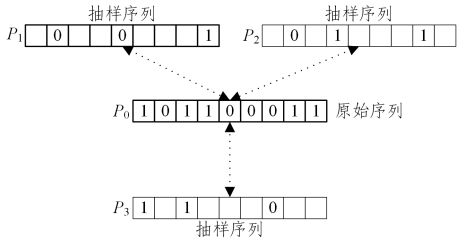

图 6 按比特的随机抽样

Fig. 6 Random sampling by bits

EMRQDSs 密钥分配的原理和文献[39]一致，只是改变了签名者的编码规则，将原来对每个比特均随机选择基矢改为对一组比特(一个密钥 k_i)随机选择一个基矢，这样当参与者恰巧猜中基矢时可以得到一组比特的信息，如图 7 所示。同时，参与者之间不知道彼此获得了哪些密钥。

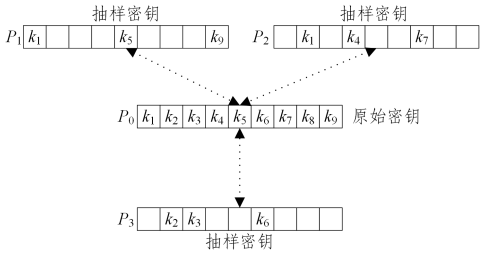

图 7 按密钥的随机抽样

Fig. 7 Random sampling by keys

EMRQDSs 通过随机抽样的方式实现了与 USS 签名密钥对称(如图 8 所示)相同的效果，减少了验签者获得的非必要信息，并且完全避免了不诚实的验签者控制诚实节点部分密钥的可能性，从而防止串通攻击破坏可转移性。

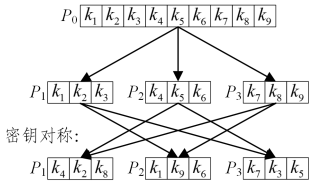

图 8 USS 的密钥对称

Fig. 8 Key symmetry of USS

EMRQDSs 使用全部密钥签名和部分密钥验签的原理和文献[22,29,34]的 USS 方案一致，只是改变了验签者部分密钥的获取方式，不影响签名的安全性，故 EMRQDSs 同样满足不可伪造性、不可抵赖性、可转移性以及量子安全性。此处省略证明过程。

USS 中签名者可以通过和一个验签者合作，破坏部分诚实验签者的部分密钥，诱导诚实验签者发起多数票机制，后使其失败并受到惩罚，完成陷害攻击。EMRQDSs 中验签者采用随机抽样的方式获取部分密钥，不诚实的验签者无法通过密钥交换使得其他验签者的密钥出错，从而破坏了实施陷害攻击的条件，进而防止了陷害攻击，具有更好的安全性。USS 中必须使用多数票机制或其他争端解决策略来保证可转移性，而在 EMRQDSs 中多数票机制并不是确保可转移性的必要部分，它只是用来解决争端，这将减少该机制被启用的可能，减少资源的浪费。

4 基于密钥分发中心的签名收集方案

HotStuff 中使用门限签名作为签名收集方案，使得通信复杂度由 PBFT 的 $O(n^2)$ 降为 $O(n)$，提高了共识协议的通信效率。但是经典门限签名方案不具有量子安全性，不能直接应用在量子安全的共识协议中。受到 USS 签名方案的启发，本文提出了基于密钥分发中心的签名收集方案。该方案需要一个被各个参与方共同信任的密钥分发中心(Key Distribution Center，KDC)，KDC 事先分发密钥，然后离线，不参与之后的签名和验签过程，所有节点之间均需要不安全的量子信道和经过验证的经典信道全链接，具体分为 3 个步骤。下面以 n 个参与者和 1 个 KDC 的模型描述该方案，并且假设各个节点间已经通过 QKD 建立了足够的对称密钥。

1)密钥分配。KDC 向所有参与者分配用于签名的私钥和用于签名的公钥。和 USS 类似，参与者的公钥并不相同。KDC 随机生成 n 组密钥，每组密钥有 gn 个密钥，共计 gn^2 个密钥。这些密钥与 2.1 节中的密钥要求相同，同样是用于 Universal Hash 计算哈希值，其中 g 是一个较大的正整数。KDC 将每组密钥使用 QKD 生成的对称密钥进行 OTP 加密分别发送给不同的参与者，该密钥作为签名的私钥，如图9(a)所示。之后 KDC 进行 n 次随机抽取，每次抽取每组密钥的各 g 个密钥，然后使用 OTP 加密发送给一个不同的参与者，作为验签的公钥，如图 9(b)所示。

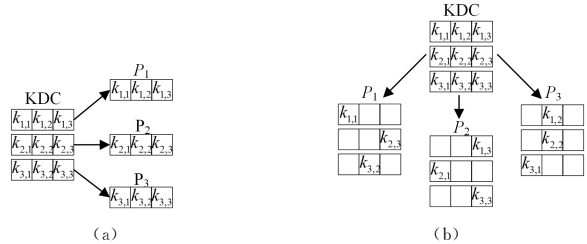

图 9 公钥与私钥的分配

Fig. 9 Distribution of public and private keys

2)生成并收集签名。每个参与者使用 Universal Hash 和自己的私钥对信息 m 计算哈希值，生成签名 $Sign_i(m)$，i 是正整数，表示第几个参与者，$i\in[1,n]$。所有参与者将签名发送给一个事先约定好的参与者，该参与者对每个签名进行验证。该参与者首先使用自己的公钥计算对应哈希值，然后和 $Sign_i(m)$ 对应位置的哈希值进行对比，如果每一组内至少 1/2 以上的哈希值对比一致，则认为该组签名有效，如果等待一定时间后收集到多于 $2n/3$ 的有效签名则认为收集签名完成，否则终止协议。

3)验证签名。将收集到的 $sig=Sign_1(m)\parallel Sign_2(m)\parallel\cdots\parallel Sign_n(m)$(“$\parallel$”表示连接)发送给各个参与者。各个参与者和上一步使用同样的方法验证各个签名 $Sign_i(m)$ 的有效性；同样，如果有多于 $2n/3$ 的有效签名则认为该次签名收集有效。

该签名收集方案是对 USS 的反向使用，USS 中签名者掌握的密钥信息和所有验签者掌握的信息一样，本方案将签名者替换为 KDC，每个验签者替换为参与者，参与者使用自己掌握的密钥信息，共同生成一个集体的签名，完成签名收集的效果。相较于每个节点进行 USS 签名再进行收集需要 $O(n^3)$ 通信复杂度的签名收集方案，本方案的通信复杂度仅为 $O(n)$。为了降低通信复杂度，本文方案没有争端解决策略。使用可信 KDC 使得各个参与者的密钥不受不诚实参与者的控制，避免了使用争端解决策略来保证安全性。本方案和 USS 一样可以满足不可伪造性、不可抵赖性、可转移性以及无条件安全性，可以容忍 $n/3$ 以下的不诚实参与者。

5 EQSH 共识机制设计

HotStuff 是一种高效的拜占庭容错共识机制，通过门限

签名将两阶段共识改为三阶段共识等手段，将通信复杂度从 $O(n^2)$ 降低至 $O(n)$，极大地提升了运行效率。但是 HotStuff 不具备抵抗量子计算攻击的能力。对此，本文提出基于 HotStuff 的高效量子安全拜占庭容错共识机制（EQSH），相较于 HotStuff，EQSH 做出了以下改进：

1）将客户端的经典签名方案替换为高效的多方环形量子数字签名（EMRQDSs），为交易信息提供了量子安全性。

2）将共识过程中的门限签名方案替换为基于密钥分发中心的签名收集方案，为共识过程提供了量子安全性。

3）优化共识策略，简化了部分共识的流程和消息格式，提出了一种简单的起搏器用于更换领导者，使得改进后的协议更适合在量子网络中运行。

5.1 系统模型

5.1.1 容错模型

设该系统中共有 $N=n+d+1$ 个节点，包括一个密钥分发中心（KDC），n 个信任该 KDC 用于达成共识的节点 $\{P_1,\cdots,P_n\}$，d 个产生交易数据的客户端节点 $\{Client_1,\cdots,Client_d\}$。将 $\{P_1,\cdots,P_n\}$ 统称为参与者，每次共识中用于收集签名的参与者称为领导者 *Leader*，其余参与者称为副本节点 *Replica*。参与者中拜占庭节点数小于 $n/3$，为了表示方便，假设 $n=3f+1$，f 是最多可以容忍的不诚实节点数；客户端可以有任意多的恶意节点；KDC 被所有参与者信任，只给参与者分发密钥，不参与共识，并且不会透露自己知道的任何信息。

5.1.2 网络模型

EQSH 的网络分为量子网络层和经典网络层。这两层网络都是无差错且同步的，各方共享一个离散的全局时钟。一个节点在每一轮发出的信息，目标节点都可以在该轮收到。量子网络是不安全的，经典网络是经过认证的。经典网络中除 KDC 外所有节点全连接，KDC 与参与者全连接，如图 10(a)所示。量子网络分为具有共同信任的 KDC 的量子内网和没有信任中心的量子外网，如图 10(b)所示。内网中的节点通过量子信道全连接，用于达成共识；量子外网中的节点通过 2 条量子信道和其中的 2 个参与者连接。

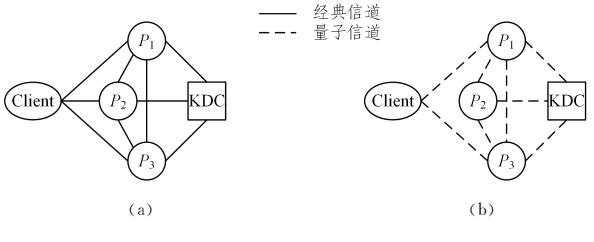

图 10 网络结构图

Fig. 10 Network structure diagram

5.1.3 密码技术

EQSH 中使用到了基于 QKD 的一次一密（OTP）、全域哈希函数（Universal Hash），以及量子密码技术。在此基础上构建了用于客户端签名的 EMRQDSs 和用于参与者的基于密钥分发中心的签名收集方案。假设协议开始前客户端已通过 EMRQDSs 的密钥分配阶段建立了足够的签名密钥，KDC 已向参与者分配了足够的密钥用于之后的收集签名。

5.1.4 消息格式

消息分为两大类：第一类是客户端发出的交易信息 $cmd=\langle m,Client_i,sign(m)\rangle$，$m$ 表示交易信息，$Client_i$ 表示签名的节点，$sign(m)$ 表示 $Client_i$ 对于该交易 m 的签名；第二类是参与者发出的用于共识的消息 $con=\langle viewNumber,node,justify\rangle$，其中 *viewNumber* 表示当前共识的视图编号，事先做出约定，每个 *viewNumber* 都被一个唯一的 *Leader* 使用。

node 是包含共识信息的字段，包括 $\langle nodeParent,nodeParentHash,cmd\rangle$ 这些信息。*nodeParent* 是 *node* 的父节点 QC 对应的 *viewNumber*，*nodeParentHash* 是 *node* 的父节点的哈希值，*cmd* 是当前 *node* 所共识的信息。

justify 是一个可变字段，*Leader* 用其携带 *QC*，*Replica* 用其携带部分签名。

QC（Quorum certificates）由 $\langle viewNumber,node,sig\rangle$ 构成，其中 *sig* 是对 $\langle viewNumber,node\rangle$ 的至少 $n-f$ 个部分签名的收集。

部分签名 Sig_i 由一个 *Replica* 对一个 *con* 的 $\langle viewNumber,node\rangle$ 进行签名生成，如式(11)所示。签名收集 *sig* 由至少 $n-f$ 个 Sig_i 拼接而成。

$$Sig_i=sign_i(\langle viewNumber,node\rangle) \tag{11}$$

5.2 起搏器

起搏器用于确认每一次共识中哪个参与者为 *Leader* 节点。EQSH 中采用简单的轮流机制，并且每一次共识依次由一个参与者作为 *Leader* 节点，之后进行循环。对于第 j 次需要共识的 cmd_j，试图编号为 j，起搏器通过式(12)选择 *Leader* 节点。

$$P_i=Leader \text{ if } i=j \bmod n \tag{12}$$

5.3 EQSH 共识机制流程

EQSH 对一个 *cmd* 达成共识至少需要经历 3 个阶段，每个阶段都由一个提议子阶段（Propose）和一个投票子阶段（Vote）组成，如图 11 所示。

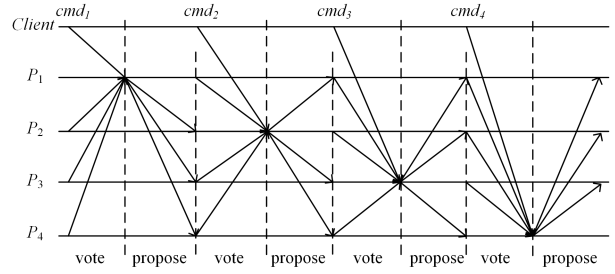

图 11 EQSH 共识过程

Fig. 11 EQSH consensus process

5.3.1 提议子阶段

提议子阶段中 *Leader* 先将收到的至少 $n-f$ 个签名验证正确的 Sig_i 组合成一个 *sig*，得到一个新的 QC_{new}，如式(13)所示：

$$QC_{new}=\langle viewNumber_{new},node_{new},sig\rangle \tag{13}$$

其中，$viewNumber_{new}$ 和 $node_{new}$ 均为上一阶段的 *viewNumber* 和 *node*，如果没有则为 $\perp$。

然后 *Leader* 节点对收到的 *cmd* 进行验签，并检查其中 *cmd* 交易信息 m 的合法性，选择其中一个通过验证的 *cmd*

作为本次共识的 *node* 中的 *cmd*，如式(14)所示：

$$node.cmd=cmd \tag{14}$$

Leader 节点在本地选择本地保存的 *viewNumber* 最大 *QC* 的 *node*，作为 *highQC*（通常为 QC_{new}）。*highQC* 中的 *viewNumber* 作为本次共识的 *node* 中的 *nodeParent*，如式(15)所示；*highQC* 中的 *node* 的哈希值作为本次共识的 *node* 中的 *nodeParentHash*，如式(16)所示。

$$node.nodeParent=highQC.viewNumber \tag{15}$$

$$node.nodeParentHash=Hash(highQC.node) \tag{16}$$

最后 *Leader* 节点选择当前的 *viewNumber*，并向所有 Replica 发送 con_L，如式(17)所示。*viewNumber* 是单调递增的，且唯一标识一个 *QC* 和一个 *node*。

$$con_L=\langle viewNumber, node, highQC\rangle \tag{17}$$

5.3.2 投票子阶段

Replica 在收到 con_L 后对其进行提议认证，如果认证通过则进行签名然后发送 *con* 给新的 *Leader* 节点，如式(18)所示；如果没有通过则不发送任何信息。

$$con=\langle viewNumber, node, Sig_i\rangle \tag{18}$$

$$Sig_i=sign_i(\langle viewNumber, node\rangle) \tag{19}$$

该阶段隐含试图切换，如何切换已由起搏器进行了约定。

提议认证：当 *Replica* 收到一个 $con=\langle viewNumber, node, highQC\rangle$ 时，首先检查 *viewNumber* 是否正确；然后要求 *highQC* 正确，且 *highQC* 的 *viewNumber* 大于等于 *lockedQC* 的 *viewNumber*；之后检查 *node* 的 *cmd* 是否合法，*nodeParent* 和 *nodeParentHash* 是否对应；最后，如果满足安全性规则或者有效性规则，则认为该 *con* 通过了提议认证。安全性规则指 *node* 可以向前指向当前的 *lockedQC* 同样的 *viewNumber*。有效性规则指 *highQC* 中的 *viewNumber* 比 *lockedQC* 的 *viewNumber* 大。

5.3.3 执行情况

该部分将讲述一个 *node* 中的 *cmd* 在什么情况下会被执行。

将已经被执行的 *node* 和对应的 *QC* 记为 $node_{exec}$ 和 *execQC*，将其中 *viewNumber* 最大的记为 $node_{hexec}$ 和 *hexecQC*。当一个拥有 *QC* 的 *node* 指向 $node_{hexec}$，且形成了一个二链，则将该 *node* 记为 $node_{locked}$，将 *QC* 记为 *lockedQC*，如图 12 所示。二链指一个 *node* 存在两个视图编号连续的后继 *node*（直接子节点 *node′* 和 *node′* 的直接子节点 *node″*）取得了对应的 *QC*，即当 $node_{locked}$ 的视图编号为 i 时，*node′* 的视图编号为 $i+1$，*node″* 的视图编号为 $i+2$。

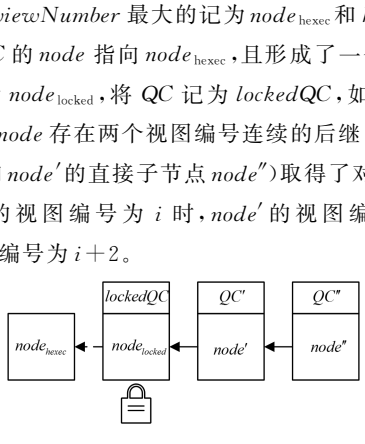

图 12 lockedQC

Fig. 12 lockedQC

当一个拥有 *QC* 的 *node* 指向 $node_{hexec}$，且形成了一个三链，则可以认为该 *node* 及其指向的所有 *node* 可以被执行，再向客户端反馈，客户端收到 $f+1$ 条反馈信息时可以认为执行成功。然后更新该 *node* 为新的 $node_{hexec}$，如图 13(a)所示。注意，形成三链的 *node* 不一定是上一次的 $node_{locked}$，如图13(b)所示。三链指一个二链存在一个后继 *node*（*node″* 的子节点 *node**）取得了对应的 *QC*。*node** 的视图编号不一定和 *node″* 的视图编号连续，但一定比 *node″* 的视图编号大。

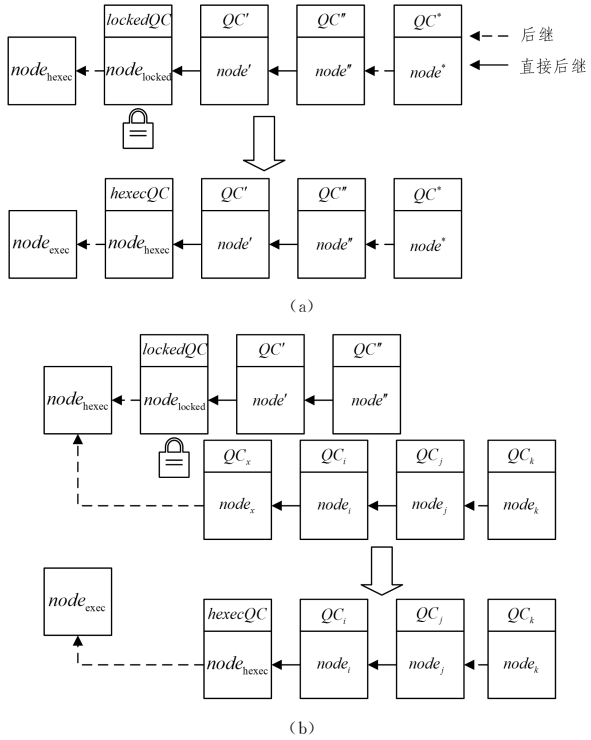

图 13 node 的更新

Fig. 13 Update of node

6 EQSH 共识机制分析

本章从安全性与活性两方面进行论证，最后分析算法的通信复杂度。

6.1 安全性

EQSH 中采用了量子安全的密码算法。客户端使用 EMRQDSs 对需要进行共识的信息进行签名。进行共识的参与者使用基于密钥分发中心的签名收集方案对共识中的签名进行部分签名、合成集体签名并验签。这两种签名方案均具备不可伪造性、不可抵赖性、可转移性以及量子安全性，即使攻击者拥有量子计算机提供的无限计算资源，签名方案仍然可以保证共识机制中数字签名和哈希指针的安全性。在 HotStuff 的协议框架的基础上，EQSH 使用 EMRQDSs 代替经典数字签名方案，使用基于密钥分发中心的签名收集方案代替门限签名方案，获得了量子安全性。

EQSH 的共识采用与 Chained HotStuff 相似的共识流程，即流水线共识流程。Chained HotStuff 将共识的逻辑和因果关系编码在链上，只要满足“三链”的条件就能达成共识，具体的安全性证明在文献[5]中已给出，此处不再赘述。

6.2 活性

和 HotStuff 一样，EQSH 将安全性和活性进行了解耦，

其活性由起搏器来保证。EQSH 将每次视图切换隐含在每个阶段的投票子阶段，每个阶段由起搏器更换 *Leader* 节点，防止一个不诚实的 *Leader* 节点阻碍共识的达成。EQSH 使用同步网络，保证了发出的信息一定能在规定时间内被收到。系统中最少有 $2f+1$ 个诚实节点，当 *Leader* 节点诚实时，则它提议的 *ode* 一定能得到一个相应的 *QC*，不诚实节点无法影响该 *QC* 的获取。当没有 *Leader* 节点作恶时，一个共识需要 3 个阶段达成；当出现连续的 f 个作恶节点的 *Leader* 节点这种最坏的情况，一个共识需要 $f+3$ 个阶段达成。总体来看每个阶段都有共识达成，最好的情况下平均每个共识达成只需要 1 个阶段。不论何种情况，系统都能在可以预期的时间内完成共识，说明 EQSH 保证了活性。

6.3 安全性及通信复杂度对比

依次分析 PBFT，HotStuff，QS-BFT，QSYAC 和 EQSH 的通信复杂度，并对其安全性进行了对比，结果如表 2 所列。

表 2 共识机制对比

Table 2 Comparison of consensus mechanisms

Consensus Mechanism	Communication Complexity	Anti-quantum Computing Attacks	Anti-collusion Attack	Anti-framing Attack
PBFT[2]	$O(n^2)$	×	√	√
HotStuff[5]	$O(n)$	×	√	√
QS-BFT[26]	$O(n^3)$	√	×	×
QSYAC[23]	$O(n^3)$	√	×	×
QS-BFT or QSYAC withsafety USS	$O(n^3)$	√	√	×
EQSH	$O(n)$	√	√	√

PBFT 和 HotStuff 是基于经典密码的拜占庭容错共识机制。PBFT 每轮共识中各个节点需要互相广播，因此通信复杂度为 $O(n^2)$。HotStuff 中使用门限签名代替了普通的数字签名，每一轮共识中 *Replica* 节点向 *Leader* 节点发送部分签名，*Leader* 节点收集足够的部分签名后合成集体签名再向所有 *Replica* 节点广播，因此通信复杂度为 $O(n)$。由于这两种拜占庭容错共识机制均基于经典密码，因此不具备量子安全性。

QS-BFT 和 QSYAC 是基于 USS 的拜占庭容错共识机制。USS 为其提供了量子安全性，但本身的通信复杂度较高。因为 USS 存在密钥对称的步骤，所以进行一次 USS 的通信复杂度为 $O(n^2)$。QSYAC 每轮共识中 n 个节点将一条信息进行一次签名($O(n\times n^2)$)，然后进行互相广播($O(n^2)$)，因此通信复杂度为 $O(n^3)$。QS-BFT 中 *Replica* 节点进行 USS 签名后发送给 *Leader* 节点($O(n^3)+O(n)$)，*Leader* 节点收集足够的签名后再向所有 *Replica* 节点广播($O(n)$)，因此通信复杂度为 $O(n^3)$。由于这两种拜占庭容错共识机制所采用的 USS 方案缺少了验证等级和多数票机制，因此并不能完美地保障可转移性，存在被串通攻击的风险。文献[29]中给出了 USS 需要验证等级和多数票机制来保证可转移性的具体证明，此处不再赘述。如果将 QS-BFT 和 QSYAC 中使用的简化的 USS 改为一个安全的 USS，则可以避免串通攻击，但由于 USS 存在被陷害攻击的风险，因此无法防御陷害攻击。攻击者可以通过陷害攻击消耗系统资源，从而降低整个系统的可用性。

EQSH 中客户端使用 EMRQDSs 方案签名，使用基于密钥分发中心的签名收集方案收集参与者的签名，这两种签名方案保证了量子安全性。因为没有密钥对称的步骤，EMRQDSs 和基于密钥分发中心的签名收集方案的通信复杂度均为 $O(n)$。EQSH 每轮共识中所有参与者进行一次签名收集，客户端进行 EMRQDSs，因此通信复杂度为 $O(n)$，并且不存在被串通攻击和陷害攻击的安全风险。

值得一提的是，客户端使用 EMRQDSs 作为签名方案，只需要 2 条量子信道和参与者相连，消除了冗余的量子信道，这极大地降低了量子网络的建设成本。而 QS-BFT 和 QSYAC 中客户端需要和所有参与者进行量子信道的链接(n 条量子信道)，当加入一个新用户时，EQSH 的线路复杂度为 $O(1)$，而 QS-BFT 和 QSYAC 的线路复杂度为 $O(n)$。因此 EQSH 有更优的可扩展性。

结束语 本文提出了一种基于 HotStuff 的高效量子安全拜占庭容错共识机制，即 EQSH。EQSH 可以用于构建量子安全区块链，所需的底层量子技术和较为成熟的 QKD 技术(光子束的生成、对光子的测量等)一致，没有使用量子纠缠等成本较高、实现难度较大的量子技术，对保障区块链系统的安全运行具有较好高践和理论价值。EQSH 使用 EMRQDSs 和基于密钥分发中心的签名收集方案作为签名方案保障了哈希指针和数字签名的量子安全性，进而为整个共识机制提供了量子安全性。与同类共识机制相比，本协议在通信复杂度、安全性和可扩展性上具有明显的优势。首先，本文使用的量子安全的签名方案的通信复杂度均为 $O(n)$，而同类共识机制使用的 USS 签名方案的通信复杂度为 $O(n^2)$，相较于其他使用 USS 签名方案的量子安全拜占庭容错共识机制通信复杂度为 $O(n^3)$，EQSH 的通信复杂度为 $O(n)$。其次，相较于简化的 USS 签名方案，本文使用的量子安全的签名方案没有串通攻击的风险；相较于安全的 USS 签名方案，本文使用的量子安全的签名方案没有陷害攻击的风险。最后，相较于同类共识机制新增客户端需要新增 $O(n)$的线路复杂度，本文只需要 $O(1)$的线路复杂度。综上，对比同类共识机制，EQSH 提高了共识效率、安全性和可扩展性。下一步工作将进一步研究量子门限签名方案代替该共识机制中的签名收集方案，降低对 KDC 等信任中心的依赖，以提高协议实用性，降低信任假设。

参 考 文 献

[1] LAMPORT L，SHOSTAK R，PEASE M. The Byzantine Generals Problem[J]. ACM Transactions on Programming Languages and Systems，1982，4(3)：382-401.

[2] CASTRO M，LISKOV B. Practical byzantine fault tolerance [C]// Proceedings of the Third Symposium on Operating Systems Design and Implementation. 1999：173-186.

[3] BUCHMAN E. Tendermint: Byzantinefault tolerance in the age of blockchains[D]. Guelph: University of Guelph, 2016.

[4] BUCHMAN E, KWON J, MILOSEVIC Z. The latest gossip on BFT consensus[J]. arXiv: 1807.04938, 2018.

[5] YIN M, MALKHI D, REITER M K, et al. Hot-stuff: Bft consensus with linearity and responsiveness[C]// Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing. 2019: 347-356.

[6] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM review, 1999, 41(2): 303-332.

[7] CHEN N, CUI S Y, YANG C G, et al. Blockchain facing quantum computing threats and countermeasures[J]. Network Security and Informatization, 2023(5): 15-17.

[8] FERNANDEZ-CARAMES T M, FRAGA-LAMAS P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks[J]. IEEE Access, 2020, 8: 21091-21116.

[9] LONE A H, NAAZ R. Demystifying cryptography behind blockchains and a vision for post-quantum blockchains[C]// 2020 IEEE International Conference for Innovation in Technology (INOCON). IEEE, 2020: 1-6.

[10] HANAOKA G, SHIKATA J, ZHENG Y, et al. Efficient unconditionally secure digital signatures[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2004, 87(1): 120-130.

[11] RAJAN D, VISSER M. Quantum blockchain using entanglement in time[J]. Quantum Reports, 2019, 1(1): 3-11.

[12] GAO Y L, CHEN X B, XU G, et al. A novel quantum blockchain scheme base on quantum entanglement and DPoS[J]. Quantum Information Processing, 2020, 19: 1-15.

[13] WEN X J, CHEN Y Z, FAN X C, et al. Quantum blockchain system[J]. Modern Physics Letters B, 2021, 35(20): 2150343.

[14] LI Q, WU J, QUAN J, et al. Efficient Quantum Blockchain With a Consensus Mechanism QDPoS[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3264-3276.

[15] YE F, ZHOU Z, LI Y. Quantum-assisted blockchain for IoT based on quantum signature[J]. Quantum Information Processing, 2022, 21(9): 1-22.

[16] WANG W, YU Y, DU L. Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm [J]. Scientific Reports, 2022, 12(1): 8606.

[17] LIU A, CHEN X B, XU S, et al. A Secure Scheme Based on a Hybrid of Classical-Quantum Communications Protocols for Managing Classical Blockchains[J]. Entropy, 2023, 25(5): 811.

[18] SUN X, SOPEK M, WANG Q, et al. Towards quantum-secured permissioned blockchain: Signature, consensus, and logic[J]. Entropy, 2019, 21(9): 887.

[19] BENNET C H. Quantum Cryptography: Public Key Distribution and Coin Tossing[C]// Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore. 1984: 175-179.

[20] ZHANG X, GAO F, QIN S, et al. Current Status and Future Development of Quantum Cryptographic Protocols[J]. Strategic Study of Chinese Academy of Engineering, 2022, 24(4): 145-155.

[21] KIKTENKO E O, POZHAR N O, ANUFRIEV M N, et al. Quantum-secured blockchain[J]. arXiv: 1705.09258, 2018.

[22] AMIRI R, ABIDINA, WALLDEN P, et al.: Efficient Unconditionally Secure Signatures Using Universal Hashing[M]// Applied Cryptography and Network Security. Cham: Springer International Publishing, 2018: 143-162.

[23] MURATOV F, LEBEDEV A, IUSHKEVICH N, et al. YAC: BFT consensus algorithm for blockchain[J]. arXiv: 1809.00554, 2018.

[24] SUN X, WANG Q L, KULICKI P, et al. Quantum-enhanced logic-based blockchain i: Quantum honest-success byzantine agreement and qulogicoin[J]. arXiv: 1805.06768, 2018.

[25] CHEN B E, WANG B H, LAO N X. A quantum cryptographic blockchain based on DPoS extensions[J]. Journal of Guangdong University of Technology, 2021, 38(2): 34-38.

[26] REN C, ZHAO H, JIANG H. Quantum Secured-Byzantine Fault Tolerance Blockchain Consensus Mechanism[J]. Computer Science, 2022, 49(5): 333-340.

[27] WENG C X, GAO R Q, BAO Y, et al. Beating the fault-tolerance bound and security loopholes for Byzantine agreement with a quantum solution[J]. arXiv: 2206.09159, 2022.

[28] YIN H L, FU Y, LI C L, et al. Experimental quantum secure network with digital signatures and encryption[J]. National Science Review, 2023, 10(4): nwac228.

[29] ARRAZOLA J M, WALLDEN P, ANDERSSON E. Multiparty quantum signature schemes[J]. arXiv: 1505.07509, 2015.

[30] CHOLVI V. Detectable quantum Byzantine agreement for any arbitrary number of dishonest parties[J]. arXiv: 2112.09437, 2021.

[31] KRENDELEV S, SAZONOVA P. Parametric hash function resistant to attack by quantum computer[C]// 2018 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2018: 387-390.

[32] CARTER J L, WEGMAN M N. Universal classes of hash functions[C]// Proceedings of the Ninth Annual ACM Symposium on Theory of Computing. 1977: 106-112.

[33] LI B H, XIE Y M, CAO X Y, et al. One-Time Universal Hashing Quantum Digital Signatures without Perfect Keys[J]. arXiv: 2301.01132, 2023.

[34] KIKTENKO E O, ZELENETSKY A S, FEDOROV A K. Practical quantum multiparty signatures using quantum-key-distribution networks[J]. Physical Review A, 2022, 105(1): 012408.

[35] PEASE M, SHOSTAK R, LAMPORT L. Reaching agreement in the presence of faults[J]. Journal of the ACM (JACM), 1980, 27(2): 228-234.

[36] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine Generals Problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.

[37] CAI X Q，WANG T Y，WEI C Y，et al. Cryptanalysis of multi-party quantum digital signatures[J]. Quantum Information Processing，2019，18：1-12.

[38] WALLDEN P，DUNJKO V，KENT A，et al. Quantum digital signatures with quantum-key-distribution components[J]. arXiv：1403.5551，2015.

[39] QU W，ZHANG Y，LIU H，et al. Multi-party ring quantum digital signatures[J]. JOSA B，2019，36(5)：1335-1341.

[40] LIM C C W，CURTY M，WALENTA N，et al. Concise security bounds for practical decoy-state quantum key distribution[J]. arXiv：1311.7129，2014.

[41] CAI R Y Q，SCARANI V. Finite-key analysis for practical implementations of quantum key distribution[J]. arXiv：0811.2628，2009.

[42] LUCAMARINI M，PATEL K A，DYNES J F，et al. Efficient decoy-state quantum keydistribution with quantified security [J]. Optics Express，2013，21(21)：24550-24565.

[43] VITANOV A，DUPUIS F，TOMAMICHEL M，et al. Chain rules for smooth min-and max-entropies[J]. IEEE Transactions on Information Theory，2013，59(5)：2603-2612.

[44] TOMAMICHEL M，LEVERRIER A. A largely self-contained and complete security proof for quantum key distribution[J]. arXiv：1506.08458，2017.

CHENG Andong，born in 1998，postgraduate. His main research interests include quantum security blockchain and so on.

XIE Sijiang，born in 1971，master，professor，postgraduate supervisor. His main research interests include cryptosystems and quantum confidentiality communication network security system.

（责任编辑：何杨）

【征集通知】第五期“CCF 科普阅读推荐图书”

“CCF 科普阅读推荐图书”征集活动以普及计算机知识、弘扬科学精神为核心，旨在拓宽公众视野、推动计算机知识普及，满足人民群众日益增长的知识需求，提升全社会科学文化素养。

诚邀各位科普作者和图书组织编写单位对符合要求的图书作品进行申报。

图书精品推荐结果将于 2024 年 10 月下旬 CNCC2024 科普论坛上正式发布，并进行 CCF 科普图书集中展示。入选图书，择优向中国科协推荐典赞·2024 科普中国——科普作品奖项，并成为 CCF 科普基地、CCF 走进中小学选用的科普图书。

一、申请条件和要求

1）图书作品征集范围为国内公开出版发行的科普图书，包括著作、编选作品、翻译作品、编译作品、画册；计算机类教材、职业教育类图书。

2）图书作品应符合国家《出版管理条例》及《图书质量管理条例》所规定的相关要求；知识产权清晰，符合著作权法的有关规定；具有普及计算机知识、倡导计算思维、传播科学思想、弘扬科学精神的深厚内涵，并有较高的科学性和趣味性，语言生动流畅、形式活泼、内容丰富、通俗易懂，为公众所喜闻乐见；反映时代要求，具有较高的社会认同度。

二、申请方式和时间

即日起至 2024 年 8 月 31 日 24：00 前，图书作者或图书组织编写单位下载并填写《CCF 科普阅读推荐图书申请表》，并将扫描件发送至邮箱 pop.sci@ccf.org.cn。

纸质版申请表和样书（2 本）请邮寄至如下地址：

北京市海淀区中关村科学院南路 6 号中国计算机学会　王颖　18515230996

三、联系方式

CCF 秘书处

联系人：王颖

联系电话：010-62562503-24，18515230996

CCF 科学普及工作委员会

联系人：李林晓

联系电话：16619927190

（扫码下载申请表）

据 CCF 微信公众号