一种基于分组的区块链共识算法

张思贤 文 捷
(复旦大学计算机科学技术学院 上海 200433)

摘 要 区块链作为一门新技术,因为其去中心化、不可篡改等性质而被广泛研究。但由于公有链共识算法存在效率低、浪费资源等缺陷,研究者们转向对节点规模较小的联盟链的研究。目前联盟链使用的共识算法为传统的分布式共识算法,受制于节点的规模。当节点数目上升时,系统中的通信量也会上升。提出一种分组的共识算法,第一阶段通过盲签名投票选取胜利节点,第二阶段使用 PBFT 算法进行主节点的选取,有效缓解单纯使用 PBFT 算法带来的节点数目增多通信量过大的问题。最后使用该共识算法提出一种物联网系统的架构。

关键词 区块链共识算法 物联网 盲签名 POW PBFT

中图分类号 TP3 **文献标志码** A DOI:10.3969/j. issn. 1000-386x. 2020. 03. 044

A GROUP-BASE BLOCKCHAIN CONSENSUS ALGORITHM

Zhang Sixian Wen Jie
(*School of Computer Science, Fudan University, Shanghai 200433, China*)

Abstract Blockchain, as a brand new technology, has been widely studied because of its features of decentralization and non-tamperability. However, due to the low efficiency and waste of resources of public chain consensus algorithm, researchers turn to the research of small size consortium Blockchain. At present, the consensus algorithm used in the consortium Blockchain is a traditional distributed consensus algorithm, which is subject to the scale of nodes. As the number of nodes increases, so does the amount of traffic in the system. This paper proposes a consensus algorithm based on grouping. In the first stage, the winning node was selected by blind signature voting. In the second stage, we used the PBFT algorithm to select the host node, which could effectively alleviate the problem of increasing the number of nodes caused by simple use of the PBFT algorithm. Finally, this paper used the consensus algorithm to propose an architecture of the IoT system.

Keywords Blockchain consensus algorithm IoT Blind signature POW PBFT

0 引 言

区块链最先于文献[1]中提出,作为虚拟货币比特币的底层技术,因其去中心、不可篡改等特性而为大众所熟悉,但也因为其基于算力的 Pow 算法浪费大量算力进行共识运算和吞吐量低而为人所诟病。Pow 算法的出块时间为 10 分钟,一个交易从上链到确定不能被篡改,需要后续六个区块的确认,也就是一个小时确认时间。并且基于 Pow 共识算法的区块链系统每秒钟只能处理七笔交易,并不能适用于当今的物联网或者金融系统。为了缓解这一问题,Ethereum 平台尝试提出 Pos 共识算法。Pos 算法加入了币龄的概念,提高了出块的速度,但同时也引入了其他问题,如出块速度不稳定,导致分叉的出现,以及持币不出块等问题。另一方面,在联盟链系统中,以 IBM 的 Fabric 平台为例使用的为 PBFT 算法,其吞吐量能够比公有链系统高出上千倍,并且不需要后续 6 个区块的确认交易不可逆转。在联盟链系统中,交易一旦打包即可被认为不可逆,但随着系统中节点的增多,为了达成共识其系统中需要进行的通信量也将上升,不具备很好的扩展性。文献[3-4]尝试从两种途径对 PBFT 算法进行改进,

收稿日期:2019-03-28。国家自然科学基金项目(61672166);上海市优秀学术带头人计划项目(16XD1400200);上海市科技创新行动计划项目(16JC1402700)。张思贤,硕士生,主研领域:区块链与信息安全。文捷,工程师。

一个是引入 gossip 协议,另外一个是引入信用机制。文献[7]提出一种交替式的共识算法进行交替出块,文献[8]提出了一种 RMBC 的区块链使用 DBFT 共识算法,尝试以分组的形式提高用户节点进入区块链的数量。文献[10]尝试分析 Pow 类的共识算法以及 BFT 类的共识算法。

由于现行区块链技术存在的瓶颈,并不适用于当今的物联网技术,现行的物联网技术都是厂商各自定义的标准,彼此之间并不能互联,数据不能打通,而区块具有可信任、不可篡改等特性,因此可以尝试将其应用于物联网系统中,用于处理涉及到两个物联网域的问题。

本文尝试从共识算法出发,提出一种两个阶段式的区块链共识算法,并以此算法提出一种物联网设备互联的架构。

1 预备知识

1.1 盲签名

盲签名[9]因为具有盲性这一特点,可以有效保护所签署的具体内容,广泛应用于电子选举的实现中。投票者先将自己所投的选票进行盲化,然后让签名者对于盲化信息进行签名。在投票系统中,盲化后的信息即为选票。

对签名进行盲化处理:

$$\text{盲化消息}:m' = mr^e \pmod N \tag{1}$$

$$\text{签名消息}:s' = (m')^d \pmod N \tag{2}$$

$$\text{除盲信息}:s = s' \times r^{-1} \pmod N \tag{3}$$

原理为:

$$r^{ed} \equiv r \pmod N$$

$$s \equiv s' \times r^{-1} \equiv (m')^d r^{-1} \equiv m^d r^{ed} r^{-1} \equiv m^d r r^{-1} \equiv m^d \pmod N$$

盲签名的盲化、签署及除盲过程如图 1 所示。

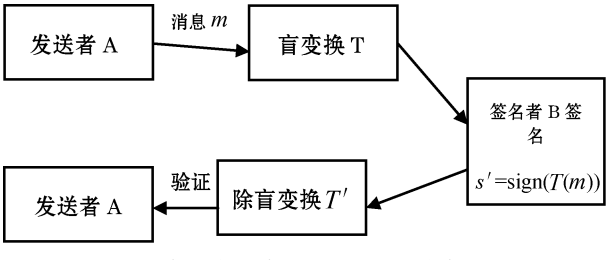

图 1 盲签名的盲化、签署以及除盲过程

1.2 实用拜占庭算法(PBFT)

文献[5]提出实用拜占庭算法,用于解决分布式系统中出现的拜占庭问题,其容错率为:$f \leqslant (n-1)/3$。其中:n 为系统的总节点数;f 为出现故障的节点数。

该算法的主要流程分为 3 个阶段:

pre-prepare:主节点向所有备份节点发送准备消息,此时节点状态为 pre-prepare。

prepare:包括主节点在内的所有备份节点在收到准备消息后,确定无误,向外广播信息,并且进入 prepare 阶段。

commit:当收到若干个来自其他副本的 prepare 信息后即可进入 commit 阶段。

实用拜占庭算法相对简单高效,但随着节点数目的增多,其通信量会急速上升,不适用于大规模的联盟链环境。文献[6]尝试在 Fabric 平台中对其进行测试节点与性能的关系,文献[13]尝试改造 Fabric 的架构,以此提高其吞吐量。

2 算法设计

2.1 算法介绍

整个算法大致分为三个阶段,前期阶段为进入该系统,然后将各节点分配到每个组中。第一阶段使用盲签名投票的形式进行主节点的选取。第二阶段使用实用拜占庭算法从上一个阶段中胜利的节点中选出主节点进行区块的生成。

第一阶段中,参与竞选的 i 到 $i+4$ 节点,将其选票以盲化的形式(盲化内容为竞选者的地址),连同区块信息传递至下一个节点,后续节点首先对区块信息进行验证,然后对各个节点盲化后的信息进行签署。

由于经过盲处理各个节点并不知道其为哪个节点投票,只需要对交易记录进行验证与传递。等到区块信息回到 i 至 $i+4$ 节点,i 至 $i+4$ 节点则可进行除盲处理,根据选票选出胜利节点,并且广播获胜信息,将交易数据连同签署信息写入区块链中。在传播的过程中,投票节点并不知道到底投的是 i 到 $i+4$ 中的哪一个节点。

1) 前期阶段。区块链网络中的各个节点都保存着一份列表,列表上面会出现一个联盟内节点的地址,这个地址标识着这些节点之间为一个联盟。此联盟内节点数存在一个上限,下文假设为 M。

新加入到网络中的节点 a,向周边发放自己的公钥 P,然后进入等待状态,网络中的其他节点 b 收到来自 a 的请求加入信息后,确定自己的联盟内节点数目仍未到达上限,将接受加入信息附带上时间戳,以及本节点的公钥 S,使用 P 加密,并以报文的形式传送,表示该节点已被加入至本联盟。

在收到确定报文后(可能同时会收到多个报文,以时间戳最早的为主),确定加入该联盟,并且发送回

执报文,使用 S 加密,表示接收成功。b 收到报文后向全组节点广播,更新联盟节点列表,并向节点 a 同步最新的节点列表,a 随即同步全网中区块的所有数据。

2）第一阶段。联盟中的节点以某种环的形式进行连接,如图 2 所示。

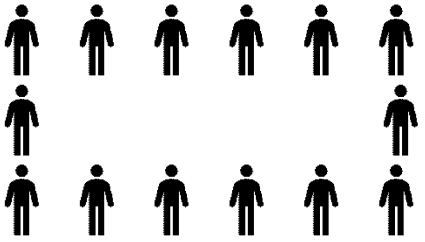

图 2　节点以环的形式进行连接

(1) 从联盟中随机选取一个节点 i 作为初始节点,i 以及 i 后序的 $i+1$、$i+2$、$i+3$、$i+4$ 将作为本轮的候选节点。

(2) 以环的形式从 $i+4$ 开始传递其投票信息,后续每个节点将从上写入其投票状况,其投票信息使用上文提及的盲签名进行生成,进行盲化。

(3) 当投票信息传递回 i 节点时可确认本轮投票结束,参与竞选的各节点依次对盲签名结果进行除盲处理,即可统计得到相应的票数。

(4) i 至 $i+4$ 节点可观察到投票的结果,确定自己是否获胜,并且对外传递信息。

(5) 参与本轮投票并且成功选出胜利者的节点,将能获得奖励。

(6) 下一轮的共识将从 $i+5$ 开始。

(7) 待下次循环进行至 i 节点,则可判定一次循环结束,重新排列其环状结构,再次进行主节点的选取。

(8) 胜出节点进入第二阶段共识。

3）第二阶段。由于使用分组的形式,因此将有若干个胜利节点进入第二阶段的共识。在第二阶段中将使用 PBFT 算法进行数据的同步,其中主节点的选取将以 $j=h\%N$ 的形式进行选取,h 为区块链的长度,N 为参与共识的节点个数,结束后回到第一轮共识。

2.2　算法分析

1）运行效率。将此节点应用于规模较大的联盟链环境中,能够有效降低网络中节点需要进行交流的通信量。使用 PBFT 算法,当节点数目上升的时候将导致性能的下降。在达成共识的过程中,需要进行信息的交换,节点数目越多需要的数据交换量就越多,在未限定节点数目的 PBFT 算法中需要的通信量为 $O(n^2)$;在节点数目为 1 000 的情况下所需要交换的通信量为 1 000 000,改进后,由于进入 PBFT 算法的节点由原来的 1 000 个分为现在的 5 组,每组中只存在一个节点的胜出,因此通信量为 25,为原本的 1/4 000。由于在第一阶段中,只需要进行一轮投票就能选出胜者,其通信量为 $O(n)$。若基于效率的原因考虑,胜出第一轮进入第二轮的节点可以选择复制后续若干个区块的生成,然后将出块权转给下一个 leader 节点,此时整个系统的运行效率与 PBFT 算法相仿,并且能够容纳更多的节点。

2）安全性。由于使用盲签名的形式进行投票,节点间并不知道彼此间投票的结果,并且投票结果不能篡改,这提高了选票结果的随机性。由于投票者并不知道其投票的候选人为哪一位,因此只能随机从候选节点中选取一人进行投票,直到最后结果公布,参与投票的候选节点才会知道知道自己所投选的节点为哪一个。

3）奖励机制。在 Pow 类型的共识算法中,奖励机制是基于挖矿的性质,节点进行哈希运算,成功挖掘出区块就能获得奖励。本文算法由于不存在挖矿这一环节,可以将奖励的机制加入至前期投票的过程中,参与投票并且成功票选出胜利的节点以及胜出节点将能获得奖励,以降低节点间的相互竞争,使系统稳定运行下去。

4）硬分叉。由于节点的最终出块是基于 PBFT 算法,因此能够有效避免分叉的问题。因为区块的节点都是经过最终投票来决定的,不存在像 Pow 算法中节点同时挖块成功所导致的分叉问题。

5）联盟链。该算法能在联盟链环境下进行使用,以此缓解 PBFT 算法带来的通信量大的问题,以此容纳更多的节点进入网络。

6）使用环进行连接。该算法在分组中使用环进行连接的主要原因在于,分组中的节点相对于全网节点,数量较少,使用环传递数据更加高效,若在全网进行环的连接,传递投票信息与区块信息将受网络的严重影响。数据的传递时间将随着节点数目的上升而上升,节点越多这个环就越大,不能保证稳定的出块速度。

3　应　用

可尝试将该算法应用于物联网[11]系统中。现行的物联网系统中,并没有一个严格的标准,还处于不同的厂商之间互相制定标准,并且大多数为一些性能较弱的设备。另一方面由于节点的性能相对较弱,不能进行较为复杂的共识算法,如 Pow 与 Pos 共识算法。

文献[2]提出基于物联网系统进行改造的算法,改变 Pow 算法的计算公式,让节点更加容易计算出结果。我们尝试从上文中提出的共识算法出发,提出一种新的基于区块链物联网共识架构。

我们所提出的物联网系统将分为两层:内部系统与外部系统。内部系统负责管理一系列性能相对较弱的节点,外部系统负责管理一系列性能相对较强的节点。内部系统对应一系列性能较弱的设备,如:灯、共享自行车等,其主节点为一系列性能较好的节点,对应一些性能相对较好、对于电力不是瓶颈的设备,如路由器、平板电脑等。

3.1 内部系统

内部系统的组成为一系列性能相对较差的节点以及一部分性能相对较好的节点,彼此组成环的形式,其中内部系统负责维护一条关于自身内部系统的区块链用于记录每一笔交易操作。

性能较差节点:负责投票,不负责数据的存储以及与外部系统直接交互。若需要数据,则需向性能较好的节点发起查询操作即可,可部署智能合约,进行投票以及数据的自动转发至下一个节点。当发起主节点选取时,投票信息在节点间进行传递,性能较差的节点需要调用智能合约随机地从候选地址中进行选取,并且对候选地址生成的信息进行盲签,然后将数据传递至下一个节点中。

性能较好节点:负责打包交易,负责与外部系统进行交互。一般情况下,一个内部系统中将存在若干个性能较好的节点,彼此间互相参与竞选成为本回合的胜利节点,彼此对本系统的所有数据进行备份,并且与外部系统进行交互。基于性能的考虑,一次节点竞选成为本回合的胜出节点后,需要负责后续若干个区块的生成,以此减少节点间来回投票所带来的消耗。对于内部系统来说,其效率较高,一旦主节点被选取成功,后续任何打包数据上链的操作,将不需要进行耗费资源的 Pow 计算,只要副本节点间没有任何异议,则可直接进行数据的上链。性能较差的节点只需要接受来自主节点的指令或者查询交易记录即可,无需进行数据的全量备份。

具体流程如下:

1) 内部系统中的每个节点将以某种环的形式进行连接,彼此只需知道下一个节点的地址。

2) 参与竞选的 i,$i+1$、$i+2$、$i+3$、$i+4$ 等若干个性能较好的节点,发起竞选操作,将其公钥使用盲签的形式,生成一个地址,同时写进一个区块中,连同交易进行传递。

3) 接收到的节点,将从 i 到 $i+4$ 的所生成的数据中随机选取一个进行盲签,然后往下一个区块进行传递。

4) 若下一个接收到的节点并不为 i,则重复 3)的操作。

5) 当区块传递到 i 至 $i+4$ 节点时,可将区块中被盲签化的数据进行除盲处理,统计结果并选出胜利节点,向网络中广播本轮胜出的节点。

6) 胜出的节点,将交易进行打包,生成区块,并且广播至相邻的 $i+1$ 至 $i+4$ 节点,待若干个区块成功生成后,则重新发起竞选操作。

3.2 外部系统

外部系统为一系列性能较好的节点,在这里我们可以理解为不同的系统,作为联盟间的系统共同维护着一条联盟之间的区块间的区块链。由于节点数目相对内部系统较少,因此可直接使用 PBFT 算法进行数据的同步与写入,其中主节点的选取沿用 $j = h\% N$ (h 仍然为区块链的长度,N 为涉及到的厂商的数目)的形式进行选取。基于视图切换带来消耗等原因,假如在外部系统的主节点不存在作恶的情况下,将负责若干个回合区块的生成,再重新选取。

3.3 跨链操作

外部系统可作为系统间跨链操作的媒介。跨链指的是两个相互独立的区块链系统进行互操作,大多用于虚拟货币的交换。文献[12]指出了区块链跨链系统中架构,在物联网系统中我们可以使用内部系统的主节点作为内部系统以及外部系统之间的调节点。在此可以理解为两个互为独立的系统之间的互操作或者两个不同的物联网系统之间数据的传递,区块链技术保证了数据的正确性。由于使用两层的形式,任何来自外部的指令都能经被内部系统的主节点拦截,并且由于使用了区块链技术可溯源不可篡改等性质,保证了交易数据的真实性,操作一旦发生并且上链,将不能被篡改与抵赖,可使用智能合约的形式进行数据格式的转换。

具体流程如下:

1) 首先内部系统 A 中的某一节点向当前的 leader 节点发起一笔向外部节点进行操作。

2) leader 将其广播至外部系统中,涉及到的相关内部系统 B 的主节点,对相应信息进行验证,若无任何异议,则发送至相应的内部节点中进行操作。

3) 相应的内部节点接收到请求后,若确认无误执行操作,并要求主节点将其交易打包进块,内部系统 B 的主节点将数据打包上链,结果最终写进区块链中。

4) 外部系统接收到该结果已被 B 系统执行后,将该交易记录上链,并且通知 A 系统。

5) A 系统将交易上链,确定本次跨链操作执行完毕。

3.4 出错处理

1) 若中间某一环节出现错误,整个系统将进行回滚,若在外部系统中涉及到的相关节点将操作回绝,则内部系统 A 将立即得到反馈,并将其反馈至相应的内部节点。若此笔操作由于某种原因被取消,交易信息可自行选择记录上链。

2) 若内部系统 B 中将操作进行回绝,则 B 中的节点则会将操作失败以及其原因回调给内部系统 A,后续操作如 1)。

3.5 整体优势

1) 由于使用了三层区块链的形式,其操作数据将全程上链,此时各个区域的节点都能从区块链中获取交易信息,若对历史操作记录存疑,可直接在链上进行查询。

2) 该系统相对稳定,若系统出现宕机或其他问题,则可由其他性能相差无几的节点接替其主节点的位置。性能较差的节点并不需要进行区块链的维护,只需要接受来自主节点的指令,以及进行主节点的选取。

3) 由于使用 leader 节点代为跟踪后续的操作,因此内部系统中发起交易的节点可以继续做相应的操作,等待事件执行完毕后,会得到回传。

4) 使用层层验证的机制,涉及到三个环节的校验:内部系统 A 的主节点,内部系统 B 的主节点,以及内部系统相应执行的节点。这保证了跨域系统中的节点不会频繁收到恶意的指令。

5) 所有存储在区块上的信息,使用 Merkle Tree (默克尔树)[3] 的形式进行组织,用于快速验证和快速查找。

6)使用了智能合约进行数据格式的转换,解决不同厂商之间存在的数据格式不一致的问题。

7)为了防止节点的作恶,可使用保证金的形式,每当涉及到跨链的操作,需要向内部系统中的主节点发一笔交易以及保证金,其保证金在交易已经确定正式被执行之前将锁定。随着操作记录的上链,保证金将解锁。在确定交易记录被上链之前,可使用智能合约对保证金进行锁定。

8) 使用分域的形式,可实现两个物联网设备域之间跨域操作,使用 leader 节点进行后续交易的跟踪,各个域内的其他节点可继续其自身的其他任务,而无需时刻跟踪其发出去的操作,待后序操作成功 leader 节点将会告知。

4 结　语

本文提出一种两阶段式的共识算法,在第一阶段中使用投票的形式选取胜利节点,在第二阶段中进行 PBFT 算法实现区块的生成,解决了 PBFT 算法无法适用于节点规模较大的情况。未来将尝试从第二阶段进行改进。基于此算法提出一种物联网设备的架构体系,内部系统组织性能较低的节点,只负责随机进行投票,选举出主节点和执行主节点,或者对外部系统分发命令,外部系统使用性能较好的节点管理内部系统的数据上链、外部系统的数据上链以及跨链操作等,使用智能合约进行数据格式的转换,用于解决各个产商之间数据格式不兼容的问题。

参　考　文　献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [OL]. 2008. https://bitcoin.org/en/bitcoin-paper.

[2] Zoican S, Vochin M, Zoican R, et al. Blockchain and consensus algorithms in Internet of Things[C]//2018 International Symposium on Electronics and Telecommunications (ISETC), 2018.

[3] 张仕将, 柴晶, 陈泽华, 等. 基于 Gossip 协议的拜占庭共识算法[J]. 计算机科学, 2018, 45(2): 20-24.

[4] Lei K, Zhang Q C, Xu L M, et al. Reputation-based Byzantine Fault-Tolerance for consortium blockchain[C]//2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), 2018:604-611.

[5] Castro M, Liskov B. Practical Byzantine fault tolerance[C]//OSDI '99: Proceedings of the third symposium on Operating systems design and implementation, 1999:173-186.

[6] Sukhwani H, Martinez J M, Chang X, et al. Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)[C]//2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS). IEEE, 2017:253-255.

[7] Duong T, Fan L, Zhou H S. 2-hop blockchain: Combining proof-of-work and proof-of-stake securely[EB]. Cryptology ePrint Archive: Report 2016/716, 2016.

[8] Jeon S, Doh I, Chae K. RMBC: Randomized mesh blockchain using DBFT consensus algorithm[C]//2018 International Conference on Information Networking (ICOIN). IEEE Computer Society, 2018:712-717.

(下转第 309 页)

-3094.
[7] 张建航,胡予璞,齐新社. 具有前向安全性和公开可验证性的签密方案[J]. 计算机应用研究,2011,28(2):733-737.
[8] 周克元. 公开验证和前向安全数字签密方案的分析和改进[J]. 西北师范大学学报(自然科学版),2015,51(6):50-53.
[9] 刘志远. 一个安全的无证书签密方案[J]. 计算机应用研究,2013,30(5):1533-1535.
[10] 俞惠芳,杨波. 可证安全的无证书混合签密[J]. 计算机学报,2016,38(4):804-813.
[11] 周才学. 几个签密方案的密码学分析与改进[J]. 计算机工程与科学,2016,38(11),2246-2253.
[12] 周彦伟,杨波,王青龙. 安全的无双线性映射的无证书签密机制[J]. 软件学报,2017,28(10):2757-2768.
[13] 祁正华,王翔. 高效的无证书混合环签密[J]. 南京邮电大学学报(自然科学版),2018,38(1):98-105.
[14] 周克元. 基于双难题的数字签密方案研究[J]. 计算机应用与软件,2017,34(10):316-319.
[15] 张平,栗亚敏. 前向安全的椭圆曲线数字签名方案[J/OL]. 计算机工程与应用:1-8[2019-02-28]. http://kns.cnki.net/kcms/detail/11.2127.TP.20190119.1157.004.html.
[16] 李靳元,缪祥华. 对前向安全数字签名方案的分析与改进[J]. 吉林大学学报(信息科学版),2017,35(6):608-611.
[17] 杨波. 现代密码学[M]. 2 版. 北京:清华大学出版社,2007.
[18] Al-Somani T F, Ibrahim M K, Gutub A. High performance elliptic curve GF(2m) crypto-processor[J]. Information Technology Journal, 2006, 5(4):742-748.
[19] Wan S S, Chen H W, Cao R J. An analogic selection sorting algorithm for synthesis of reversible logic circuits[J]. Chinese Journal of Computers, 2010, 33(12):2343-2352.
[20] 孙奕,陈性元,杜学绘,等. 一种用于流交换的代理重签名方案[J]. 软件学报,2015,26(1):129-144.
[21] 黎忠文,黎仁峰,钟迪,等. 一个高效的多方混合签密方案[J]. 科学技术与工程,2014,14(17):83-86.
[22] 梁艳,张筱,郑志明. 基于无证书群签名方案的电子现金系统[J]. 通信学报,2016,37(5):184-190.

(上接第 265 页)

[9] 张方国, 王常杰, 王育民. 基于椭圆曲线的数字签名与盲签名[J]. 通信学报, 2001, 22(8):22-28.
[10] Vukolić M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication[C]//International workshop on open problems in network security, 2015:112-125.
[11] Yu S, Lv K, Shao Z, et al. A high performance blockchain platform for intelligent devices[C]//2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018:260-261.
[12] Jin H, Dai X, Xiao J. Towards a novel architecture for enabling interoperability amongst multiple blockchains[C]//2018 IEEE 38th International Conference on Distributed Computing Systems(ICDCS). IEEE Computer Society,2018:1203-1211.

(上接第 298 页)

算法不可能差分分析的复杂度,使得其时间复杂度低于穷举搜索的攻击复杂度。

参 考 文 献

[1] Daesung K, Jaesung K, Sangwoo P, et al. New block cipher: ARIA[C]//International Conference on Information Security and Cryptology, 2003:432-445.
[2] Stinson D. 密码学原理与实践[M]. 冯登国,译. 3 版. 北京:电子工业出版社,2009.
[3] 李超,孙兵,李瑞林. 分组密码的攻击方法与实例分析[M]. 北京:科学出版社,2010.
[4] Liu Y, Gu D, Liu Z, et al. New improved impossible differential attack on reduced-round AES-128[C]//Computer Science and Convergence. Berlin:Springer, 2012:453-461.
[5] Dunkelman O. Techniques for cryptanalysis of block ciphers[D]. Haifa, Israel Institute of Technology, Faculty of Computer Science,2006.
[6] Biryukov A, Wagner D. Slide attacks[C]//Proceedings of the 6th International Workshop on Fast Software Encryption. Springer-Verlag, 1999:245-259.
[7] 杜承航. 分组密码算法 ARIA 的不可能差分分析和中间相遇攻击[D]. 济南:山东大学,2011.
[8] Wu W L, Zhang W T, Feng D G. Impossible differential cryptanalysis of reduced-round ARIA and Camellia[J]. Journal of Computer Science and Technology,2007,22(3):449-456.
[9] Li S, Song C. Improved impossible differential cryptanalysis of ARIA[C]//2008 International Conference on Information Security and Assurance(isa 2008). IEEE Computer Society, 2008:129-132.
[10] Du C, Chen J. Impossible differential cryptanalysis of ARIA reduced to 7 rounds[C]//Cryptology and Network Security - 9th International Conference, CANS 2010, Kuala Lumpur, Malaysia, December 12-14, 2010. Proceedings. DBLP, 2010.
[11] Su C M. New impossible differential attack on 7-round reduced ARIA[J]. Journal od Computer Applications,2012,32(1):45-48.
[12] 谢高淇,卫宏儒. ARIA 分组密码算法的不可能差分攻击[J]. 计算机研究与发展,2018,55(6):1201-1210.