DOI:10.19729/j.cnki.1009-6868.2018.06.005
网上出版地址:http://kns.cnki.net/kcms/detail/34.1228.TN.20181119.1138.004.html

基于区块链的物联网密钥协商协议

Blockchain-Based Key Agreement Protocol for Internet of Things

张佳妮/ZHANG Jiani
何德彪/HE Debiao
李莉/LI Li
(武汉大学,湖北 武汉 430070)
(Wuhan University, Wuhan 430070, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2018) 06-0023-005

摘要: 针对传统物联网(IoT)交易场景下,双方使用椭圆曲线算法签名交易时证书颁发与维护的巨额开销问题,提出使用基于身份的Schnorr签名替换原有的椭圆曲线数字签名,以实现IoT设备间轻量级的身份认证。提出了基于Diffie-Hellman和基于YAK 2种比特币密钥协商协议,实现了交易后比特币用户间端到端的安全通信。其中,基于YAK的密钥协商协议通过零知识证明(ZKP)提供了前向安全。

关键词: 区块链;IoT;Schnorr;密钥协商;ZKP

Abstract: In view of huge cost of certificate issuance and maintenance in traditional Internet of things (IoT) transaction scenario where both parties use elliptic curve algorithm to sign transactions, an identity-based Schnorr signature is proposed to replace the original elliptic curve digital signature to realize the lightweight identity authentication between IoT devices. Two bitcoin key agreement protocols based on Diffie-Hellman and YAK have been proposed which achieve end-to-end secure communication between bitcoin users after transactions. Meanwhile, the YAK-based protocol can provide forward security through Zero-Knowledge Proof (ZKP).

Keywords: blockchain; IoT; Schnorr; key agreement; ZKP

国际电信联盟(ITU)将物联网(IoT)定义为:信息社会全球基础设施(通过物理和虚拟手段)将基于现有和正在出现的、信息互操作和通信技术的物质相互连接,以提供先进的服务。它起源于1999年美国麻省理工学院(MIT)提出的无线射频识别(RFID)的思想,并在2005年的信息社会世界峰会(WSIS)被正式确定概念[1]。IoT本质上是一个传感器智能网,它通过RFID、红外感应器、激光扫描仪等传感设备将物与互联网相连,从而实现智能化识别、定位、监测控制与管理。IoT被认为是信息产业继计算机、互联网之后的第3次浪潮,是实现智慧城市[2]的关键技术;但其自身存在一些技术瓶颈。传感网络的大规模和分布式特性使得IoT的安全运维成为一大挑战,例如:基于Mirai僵尸物联网的分布式拒绝服务(DDoS)攻击就曾使得Dyn瘫痪,Twitter、Paypal等人气网站停止服务。随着IoT设备的指数级增长,数据流的中心化管理负载过重,容易造成信息堵塞。此外,IoT还存在数据标准不一致引起的通信兼容问题。

区块链作为一种新兴的信息技术,具有公开可验证、可编程、可追溯、防篡改等性质。通过区块链技术构建IoT系统(如图1所示),由区块链充当通用的数字账本,节点设备广播交易,经区块共识后记录上链,可实现数据的可证溯源。同时,加密算法保障了交易数据的隐私性、完整性,共识算法实现了节点间数据的一致性。区块链去中心化的运行机制规避了高额的运维成本,数以亿计闲置设备的算力、存储被充分利用,实现了IoT安全扩容。此外,其激励机制促进了数据升值,点对点(P2P)网络打破了信息孤岛桎梏,促进了设备间的多方协作和信息交流。2015年出现的比特币电脑可实现区块链小

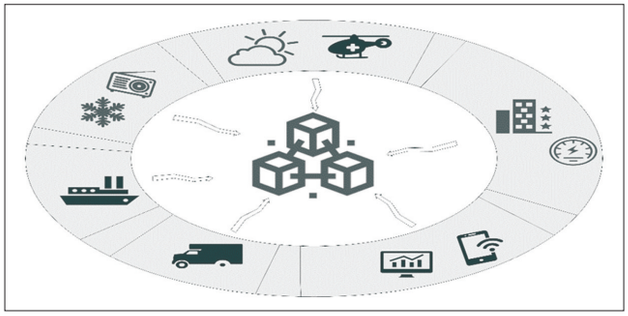


图1▶ 区块链在物联网的应用

收稿日期:2018-10-17
网络出版日期:2018-11-19
基金项目:国家重点研发计划基金资助项目(2018YFC1315404)、国家自然科学基金资助项目(61402339,61572370)

微支付网络与IoT的连接。通过分布式资源调配，构建起真正的分享经济模式。2017年全球首个IoT区块链（BOT）项目成立，定义了可信IoT服务平台框架。区块链与IoT的结合有效地解决了IoT缺乏隐私、运维高昂、通信不兼容等行业痛点，有力地推动了智慧城市[3]的发展。

为了实现IoT设备安全可靠的数据通信，亟需一个安全的密钥协商协议以提供身份认证。文献[4]首次提出2个比特币密钥交换协议，以实现交易后比特币用户间端到端的安全通信。然而在该方案中，交易双方使用椭圆曲线数字签名算法（ECDSA）确定交易的所有权。随着IoT设备的指数级增长，数以亿计的设备都需要生成和维护一个公钥证书。为了规避证书颁发与维护的巨额开销，我们提出使用基于身份的Schnorr签名替换原有的ECDSA签名，不再使用公钥证书，从而实现了物联网设备轻量级的身份认证。进一步地，我们提出了2种密钥协商方式：基于Diffie-Hellman的比特币密钥协商协议、基于YAK的比特币密钥协商协议。其中，基于YAK的比特币密钥协商协议通过零知识证明（ZKP）提供了前向安全性。

1 关键技术

1.1 基于身份的Schnorr签名方案

该方案由以下4个算法组成。

（1）*Setup*：输入安全参数 k，系统选择一个阶 q 为 $2^k \leqslant q < 2^{k+1}$ 的群 G，令 g 为 G 的生成元。系统选择2个安全的密码哈希函数 $H_1,H_2:\{0,1\}^* \to Z_q$，并随机选择 $s \in_R Z_q$ 作为系统主私钥。最后，系统秘密保存 s 并公开参数 $\{G,g,q,H_1,H_2,g^s\}$。

（2）*Extract*：给定用户身份 $id \in \{0,1\}^*$，系统随机选择 $r \in_R Z_q$，计算 $d_{id}=r+sH_1(g^r,id) \bmod q$，并通过安全信道发送 d_{id} 给用户。

（3）*Sign*：给定消息 $m \in \{0,1\}^*$，用户随机选择 $t \in_R Z_q$，计算 $e=t+d_{id} \cdot H_2(id,g^t,m) \bmod q$，用户输出消息 m 的签名 $\sigma=(g^t,e,g^r)$。

（4）*Verify*：给定消息签名对 (m,σ)，验证者通过式（1）验证签名 σ 的有效性：

$$Ver(id,m,\sigma)=1 \Leftrightarrow g^e=g^t\left(g^r g^{s \cdot H_1(g^r,id)}\right)^{H_2(id,g^t,m)}。\quad (1)$$

若签名 σ 有效，返回“1”；否则，返回“0”。

1.2 比特币

比特币[5]是区块链技术在数字金融领域的第一个应用，是一种基于P2P网络的虚拟加密货币。它为每个比特币用户生成公私钥对，其中私钥用于签名交易，公钥用于验证数据。比特币网络可以实现用户匿名识别、比特币转移，以及历史交易的记录上链，具有去中心化、匿名性、通胀预防等特点。目前，一些主流交易平台有：btc-e.com、bitstamp；中国的主流交易平台有比特币中国、OKCoin、火币等。截至日前，比特币的流通市值已达到7 743.97亿元人民币，日成交额达到280.328亿元人民币。

1.2.1 比特币交易

比特币交易是相互关联的输入输出交易事务，使用未经使用的交易的输出（UTXO）作为输入，并生成新的输出。同一笔交易可以有多个输入和多个输出，具体交易格式如表1所示。

比特币地址由公钥经一系列哈希、编码而来，即：

比特币地址=Base58{Hash160||前4字节（SHA256(SHA256(Hash160||地址版本号)))}

其中，Hash160=RIPEMD160(SHA256(65字节公钥))。

▼表1 比特币交易格式

交易类型与编号	输入	输出
Coinbase，001		序号为1，金额为10，地址为Alice
002	001	序号为1，金额为2，地址为Bob
002	001	序号为2，金额为8，地址为Alice

1.2.2 区块

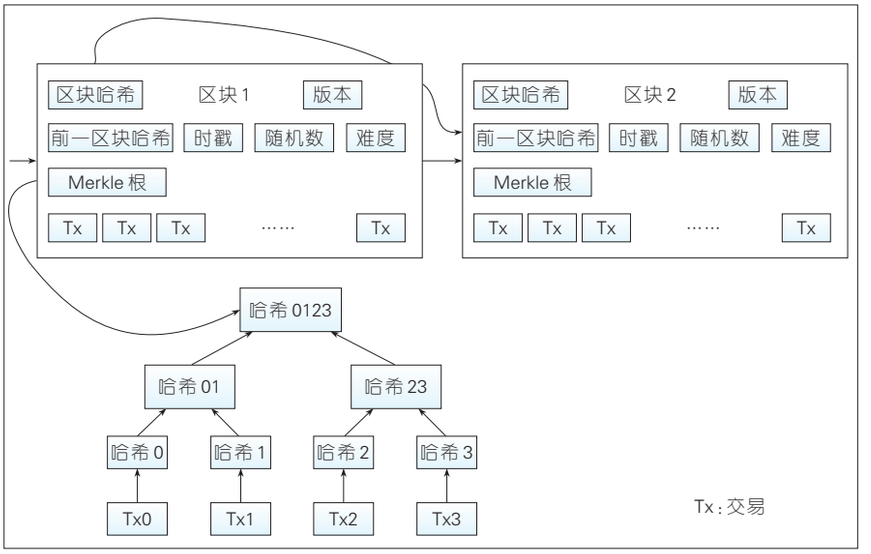
网络中的所有交易由背书节点收集验证打包上链，经过6个区块确认后交易不可逆转。平均每10 min生成一个新区块链接到最长的链尾部。整个区块链是一个链式结构[6]，如图2所示，其中Tx表示交易。

1.2.3 共识机制

共识机制[7-8]是分布式网络中互不信任节点间建立共识的规则与方法。现有的共识机制根据通信方式可分为异步通信共识机制和同步通信共识机制。异步通信共识机制的代表为有向无环图（DAG），与定期检查同步点的日志机制不同，DAG采用异步处理事务操作的方式，极大地提高了系统吞吐量。区块链主要使用同步通信共识机制。其中，同步通信共识机制包括强一致性共识算法和最终一致性共识算法。最终一致性共识算法多用于私有链、联盟链的共识，可进一步细分为具备拜占庭容错特性[9]的一类，如授权拜占庭容错（DBFT）、实用拜占庭容错（PBFT）、资产证明（PoA）、Ripple、Pool验证池等；不具备拜占庭容错特性的一类，如Paxos、Raft等。强一致性共识算法多用于公有链的共识，包括工作量证明（PoW）、权益证明（PoS）、股份授权证明（DPoS）、重要性证明（PoI）等，具体分类参见表2。

比特币区块链的共识主要采用强一致性算法中的PoW、PoS、DPoS。

（1）PoW。寻找随机数 n，使得：$SHA(SHA(v||h_p||t||n||h_m))$ < 目标哈希，最先找到随机数 n 的矿工获得记账权并获得比特币奖励，这一过程也称



▲图2 区块链的链式结构

▼表2 共识机制的分类

算法类型	同步通信	异步通信
最终一致性共识算法（具备拜占庭容错（私链/联盟链））	DBFT、PBFT、PoA、Ripple、Pool 验证池	DAG
最终一致性共识算法（不具备拜占庭容错（公有链））	Paxos、Raft	DAG
强一致性共识算法	PoW、PoS、DPoS、PoI	DAG

DAG：有向无环图　DPoS：股份授权证明　PoA：资产证明　PoS：权益证明
DBFT：授权拜占庭容错　PBFT：实用拜占庭容错　PoI：重要性证明　PoW：工作量证明

“挖矿”。挖矿难度的调整周期为2周，目的是使区块的生成时间稳定在10 min左右。PoW具有完全去中心化、节点可自由进出等优点，但挖矿行为造成大量的资源浪费，且共识周期较长，存在51%攻击，不适合商业应用。

（2）PoS。系统中具有最高权益的节点（如币龄最长）获得记账权。PoS的优点在于减少了PoW的资源消耗，缩短了共识时间，且恶意节点只有掌握超过全网1/3的资源，才能破坏整个共识过程；但共识过程需等待多个确认，容易产生分叉。

（3）DPoS。记账权由101位受托人轮流实现。其中，受托人由股东根据股份权益选出，且需保证99%以上的在线时间。DPoS机制大幅度缩减了验证和记账节点的数量，可以达到秒级验证；但其去中心化的程度不足，依赖于代币的特性限制了其应用领域。

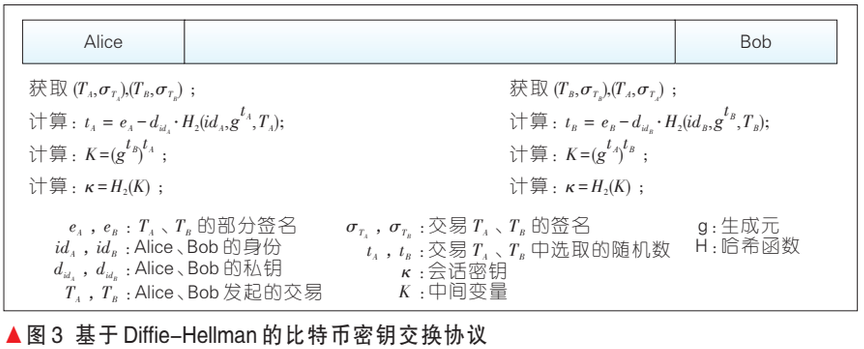
2 方案设计

考虑IoT中的2台设备Alice和Bob。区块链充当数据管理系统，IoT中所有的交易都记录上链。Alice和Bob通过以下方式实现密钥协商。

2.1 基于Diffie-Hellman的比特币密钥协商协议

如图3所示，协议的具体执行过程如下：首先，Alice利用私钥 d_{id_A} 提取出与交易 T_A 相关的一次性随机数 t_A。然后，Alice在链上获取Bob的交易签名对 (T_B,σ_{T_B})，并从 σ_{T_B} 中提取与公钥相关的 g^{t_B}。Alice根据 t_A，g^{t_B} 计算会话密钥 κ。同理，Bob计算一次性随机数 t_B，从 σ_{T_A} 中提取 g^{t_A}，进一步计算会话密钥 κ。

本协议实现了IoT设备基于交易的密钥协商，任意2个设备节点只需从链上获取自身及对方的交易签名对，就能线下计算会话密钥 κ。本协议中，与交易相关的随机数可直接利用私钥计算，避免了随机数存储的开销，克服了IoT设备资源受限的缺陷。

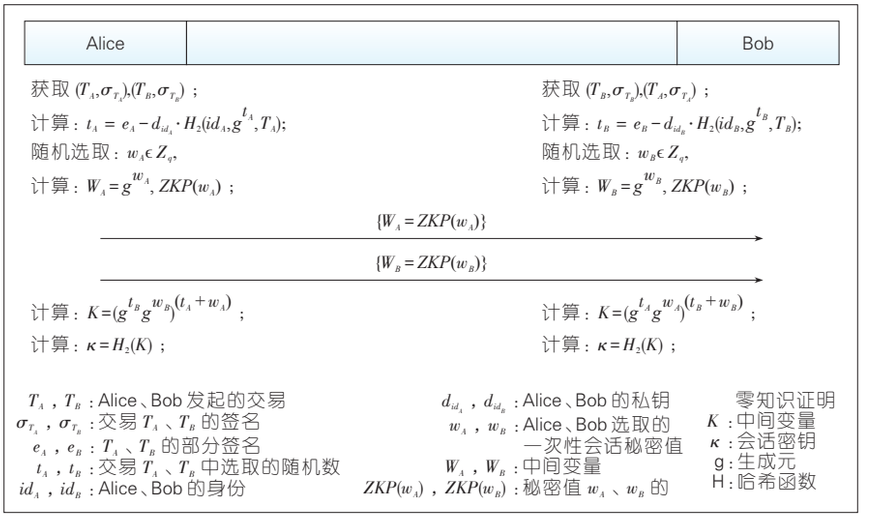


▲图3 基于Diffie-Hellman的比特币密钥交换协议

2.2 基于YAK的比特币密钥协商协议

如图4所示，协议的具体执行过程如下：首先，Alice（Bob）利用私钥 d_{id_A}（d_{id_B}）提取出与交易 T_A（T_B）相关的一次性随机数 t_A（t_B）。然后，Alice（Bob）在链上获取Bob（Alice）的交易签名对 (T_B,σ_{T_B})（(T_A,σ_{T_A})）。Alice（Bob）选取随机数 $w_A\in Z_q$（$w_B\in Z_q$），计算 W_A（W_B）以及 w_A（w_B）的零知识证明 $ZKP(w_A)$（$ZKP(w_B)$）并发送给对方。Alice（Bob）通过 $ZKP(w_B)$（$ZKP(w_A)$）验证随机数 w_B（w_A）的真实性并计算会话密钥 κ。

同2.1类似，本协议中节点可直接利用私钥计算与交易相关的随机数。不同的是：此协议是交互性的，双方进行密钥协商时需选取随机数 w_A、w_B 作为与会话相关的秘密值并做ZKP，对方通过ZKP验证随机数的真实性后方可计算 κ。假设IoT节点



▲图4 基于 YAK的比特币密钥交换协议

私钥的安全性被攻陷，敌手截获了交易后的某次会话。由于每次会话都重新选取随机数，则实现了后续会话的不可追踪，提供了前向安全性。

本文中我们采用了 Schnorr ZKP 方案[10]，假设 Alice 对秘密值 w_A 做了零知识证明 $ZKP(w_A)$，可通过如下方式使 Bob 相信自己拥有这一秘密而不向 Bob 泄露秘密 w_A 的任何信息。

（1）ZKP 产生（$ZKP-Gen$）

1）Alice 随机选取 $l\in_R Z_q$，计算 $L=g^l$，$h=H(g,L,w_A,id_A)$，$r=l-w_Ah$；

2）Alice→Bob：W_A，$\{id_A,L,r\}$。

（2）ZKP 验证（$ZKP-Verify$）

给定 W_A，$\{id_A,L,r\}$，Bob 相信 Alice 拥有秘密值 w_A 当且仅当式（2）成立：

$$Alice\text{拥有秘密值}w_A \Leftrightarrow L=g^r(W_A)^h \quad (2)$$

同理，Alice 通过此方式验证 Bob 确实拥有秘密值 w_B。

3 安全分析

对于密钥协商协议的安全，我们考虑以下3种安全特性。

（1）私钥安全：一次性会话中秘密值的泄露不影响设备节点静态私钥的安全性。

（2）前向安全：即使用户私钥被攻陷，已建立会话的会话密钥的安全性不受影响。

（3）会话密钥安全：攻击者冒充用户，但无法访问用户的私钥，则无法计算会话密钥。

3.1 基于 Diffie-Hellman 的比特币密钥协商协议

假设 Alice 和 Bob 分别从链上获取了交易签名对 (T_A,σ_{T_A})，(T_B,σ_{T_B})，我们证明所提协议可以提供私钥安全和会话密钥安全。

（1）私钥安全的证明

假设存在一个概率多项式时间的被动敌手 A，已掌握 Bob 的与交易相关的随机数 t_B。若 A 获得了 Alice 的秘密值 w_A，A 可通过 $K=(g^{t_A})^{t_B}$ 计算得到会话密钥，然而 A 无法获得 d_{id_A} 的任何信息。

（2）会话密钥安全证明

假设存在一个概率多项式时间的主动敌手 B，冒充 Bob 与 Alice 进行通信。现假定 Alice 和 Bob 选取的与交易相关的随机数分别为 $t_A=\varphi$，$t_B=\phi$。给定一个计算型 Diffie-Hellman 问题 $(g^{\varphi},g^{\phi},g^{\varphi\phi})$，假定敌手 B 能成功计算 K，由 $K=(g^{t_A})^{t_B}$，可得 $g^{\varphi\phi}=K$，则困难问题计算型 Diffie-Hellman（CDH），与实际矛盾。

3.2 基于 YAK的比特币密钥协商协议

假设 Alice 和 Bob 分别从链上获取了交易签名对 (T_A,σ_{T_A})，(T_B,σ_{T_B})。与3.1节不同，此协议会话密钥的产生依赖于与交易相关的随机数（t_A，t_B），以及交互过程中选取的秘密值（w_A，w_B）。我们证明了此协议可以提供私钥安全、会话密钥安全以及前向安全。

（1）私钥安全

证明如下：假设存在一个概率多项式时间的主动敌手 A，已掌握 Bob 的与交易相关的随机数 t_B 以及 Bob 某一次会话选取的秘密值 w_B。若 A 获得了 Alice 的秘密值 w_A，A 可通过 $K=(g^{t_A}g^{w_A})^{(t_B+w_B)}$ 计算会话密钥，然而 A 无法获得 d_{id_A} 的任何信息。

（2）前向安全

证明如下：假设存在一个概率多项式时间的被动敌手 A，已获取 Alice 和 Bob 的与交易相关的随机数 t_A 和 t_B。现假定 Alice 和 Bob 交互过程中选取的随机数分别为 $w_A=\varphi$，$w_B=\phi$。给定一个计算型 Diffie-Hellman 问题 $(g^{\varphi},g^{\phi},g^{\varphi\phi})$，假定敌手 A 能成功计算 K，由 $K=(g^{t_A}g^{w_A})^{(t_B+w_B)}=$ $=g^{t_At_B}g^{\varphi t_B}g^{t_A\phi}g^{\varphi\phi}$，可得 $g^{\varphi\phi}=K/g^{t_At_B}g^{\varphi t_B}g^{t_A\phi}$，则困难问题 CDH 可解，与实际矛盾。

（3）会话密钥安全

证明如下：假设存在一个概率多项式的主动敌手 B，冒充 Bob 与 Alice 进行通信。B 已获取 Alice 的与交易相关的随机数 t_A，并从公开信道上截获了 W_B。现假定 Alice 交互过程中选取的随机数为 $w_A=\varphi$，Bob 选取的与交易相关的随机数为 $t_B=\phi$。给定一个计算型 Diffie- Hellman 问题 $(g^{\varphi},g^{\phi},g^{\varphi\phi})$，假定敌手 B 能成功计算 K，由 $K=(g^{t_A}g^{w_A})^{(t_B+w_B)}==g^{t_A\phi}g^{\varphi\phi}g^{t_Aw_B}g^{\varphi w_B}$，可得 $g^{\varphi\phi}=K/g^{t_A\phi}g^{t_Aw_B}g^{\varphi w_B}=K/g^{t_A\phi}(W_B)^{(t_A+\varphi)}$，则困难问题 CDH 可解，与实际矛盾。故会话密钥不能被成功计算，此协议可以提供会话密钥安全。

4 性能分析

文章中，我们在 Ubuntu 平台搭建 regtest 测试链，基于 c++版本的比特

币代码，使用 make 编译器编译程序。我们采用的仿真平台如表 3 所示，测试链参数如表 4 所示。

假定交易查询阶段记为 P1，密钥协商阶段记为 P2，原始交易检索时间为 t_{gtx}，交易解析时间为 t_{dtx}，协议执行的总时间为 *Total*。我们通过 bitcoin-cli 查询测试链 1 000 次得到了交易的平均检索时间 $t=t_{gtx}+t_{dtx}$ 为：real（21.212 s）、user（0.164 s）、sys（0.196 s），我们实际采用 user 时间。同时，我们通过运行 miracl 库 10 000 次得到了协议的平均执行时间，实验结果如表 5、6 所示。

由表 6 可知：文中提出的 2 种比特币密钥协商协议都具有合理的运行开销，适用于设备资源受限的 IoT 环境。

5 结束语

我们使用基于身份的 Schnorr 签名替换比特币交易原有的 ECDSA 签名，提出了 2 种密钥协商协议，避免了设备资源受限的 IoT 环境下公钥证书管理的巨额开销。我们分析了所提协议的安全性，并搭建了比特币测试链模拟了交易查询及密钥协商过程，结果表明协议在实际应用中是切实可行的。

▼表 3 仿真平台参数信息

操作系统	Ubuntu 16.04 虚拟机 64 bit
处理器	Intel(R) Core(TM) i7- 6700@ 1.70 GHz
内存	8 GB

▼表 4 测试链参数信息

参数名称	参数值	参数描述
链	regtest	当前网络名
区块数	0	初始区块数为 0
头部数	0	初始有效验证头部数为 0
最佳区块哈希	7341bb55f89d6774ecbbafe378eac694abfa8539551f7f3d42aff2aebd6e0ee4	最佳块的哈希值
难度	4.656542373906925e-10	当前难度值
中间时间	1538012902	当前最佳块的中间时间
验证进度	1	验证进度估计
链工作量	0000000000000000000000000000000000000000000000000000000000000011a	主链的工作量，十六进制
修剪	false	是否修剪区块

▼表 5 操作的执行时间

操作	时间/ms
哈希运算	0.004
模乘运算	1.063
模指数运算	0.009

▼表 6 协议的执行时间

时间	基于 Diffie-Hellman 的比特币密钥协商协议	基于 YAK 的比特币密钥协商协议
P1	164×2=328 ms	164×2=328 ms
P2	2h+4m+6e≈4.314 ms	6h+6m+12e≈6.510 ms
Total	332.314 ms	334.510 ms

e：模指数运算　m：模乘运算　P2：密钥协商阶段
h：哈希运算　P1：假定交易查询阶段

参考文献

[1] 孙其博, 刘杰, 黎彝, 等. 物联网: 概念、架构与关键技术研究综述[J/OL]. (2010-12-17) [2018-10-17]. http://www.wanfangdata.com.cn/details/detail.do?_type=perio&id=bjyddx201003001
[2] 谢润桦, 王滨, 张蕴明, 等.面向智慧城市的物联网传感器状态监测与可视化应用[J]. 物联网技术, 2018, (3): 18-20
[3] FAN L J, GIL-GARCIA J R, WERTHMULLER D, et al. Investigating Blockchain as A Data Management Tool for IoT Devices in Smart City Initiatives[C]// 19th Annual International Conference on Digital Government Research: Governance in the Data Age- dgo '18 2018. Netherlands: DGS, 2018, 100:1-2. DOI: 10.1145/3209281.3209391
[4] MCCORRY P, SHAHANDASHTI S F, CLARKE D, et al. Authenticated Key Exchange over Bitcoin[M]. Switzerland: Springer, 2015. DOI: 10.1007/978-3-319-27152-1_1
[5] ZHENG B K, ZHU L H, MENG S, et al. Malicious Bitcoin Transaction Tracing Using Incidence Relation Clustering[C]// International Conference on Mobile Networks and Management 2017. Australia: MONAMI, 2017, 235: 313-323. DOI: 10.1007/978-3-319-90775-8_25
[6] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学, 2016, 42(4): 481-494
[7] 刘敖迪, 杜学绘, 王娜, 等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报,2018, (7):2092-2115. DOI:10.13328/j.cnki.jos.005589
[8] 钱卫宁, 邵奇峰, 朱燕超, 等. 区块链与可信数据管理: 问题与方法[J]. 软件学报, 2018, 29 (1): 150-159. DOI: 10.13328/j.cnki.jos.005434
[9] MILUTINOVIC M, HE W, WU H, et al. Proof of Luck: An Efficient Blockchain Consensus Protocol [J]. IACR Cryptology ePrint Archive, 2017: 249. DOI: 10.1145/3007788.3007790
[10] HAO F. On Robust Key Agreement Based on Public Key Authentication [EB/OL]. [2018-10-17]. https://link.springer.com/chapter/10.1007%2F978-3-642-14577-3_33

作者简介

张佳妮，武汉大学国家网络安全学院在读硕士研究生；主要研究方向为密码学与区块链技术。

何德彪，武汉大学国家网络安全学院教授、博士生导师；主要研究方向为密码算法的设计与实现、区块链安全；主持国家自然科学基金、国家科技部“网络空间安全”重点专项子课题等科研项目 10 余项；发表论文 100 余篇。

李莉，武汉大学国家网络安全学院副教授、硕士生导师；主要研究方向为物联网安全；主持或参与国家、自然科学基金 3 项，教育部专项科研基金项目 1 项，“863”项目 2 项；参与《信息安全原理与技术》的编写。