**A Stable Consensus Protocol in Wireless Blockchain System**

**Abstract**

# Introduction

With the rapidly development of wireless communication technology and blockchain technology, many researches focus on the applications of blockchain technology in wireless field, such as mobile edge computing [1], intelligent 5G technology [2], Internet of vehicles [3], and others. Reliable and secure resource sharing services can be provided in distributed environment by using blockchain, which has received great attention from both academia and industry. Applications that built on wireless network face with significantly challenge of security and trust. Blockchain that is decentralization, persistence and traceability provide a new way to solve these problems. In this case, secure, trust and efficient services of data interaction, secure access control, data traceability, identity authentication in wireless field can be supported by integrating blockchain technology into wireless networks.

Currently, many studies on wireless blockchain system are directly enabling popular blockchain protocols that are deployed in the Internet to wireless network environment. Such blockchain protocols make use of consensus algorithm that always rely on massive resources consumption(e.g. Proof of Work[4]), complicated design(e.g. Proof of Stake [5]), and reliable communication(e.g. Practical Byzantine Fault Tolerant [6] ). Although theses consensus algorithms work well in the Internet, they are not suitable for wireless networks with limited resources and unstable channel. The open communication of wireless networks is heavily impacted by environment. Both unstable channel bandwidth and vulnerable to Jamming attacks are the bottlenecks of wireless communication network. Theses barriers limit the application of combining traditional blockchain consensus algorithms and wireless networks, which is the motivation of researching blockchain protocol over wireless networks.

Recently, some researches on wireless blockchain systems leverage the natures of wireless networks to design efficient wireless blockchain consensus protocols. In order to adapt to the high dynamics of the mobile ad-hoc network, Z.Jiao et al. [7] design a PoW-based stability-aware consensus protocol, whose leader election is based on node information and proof of work. This novel design can make sure wireless blockchain system work efficiently and steadily. According to the characteristics of wireless communication network, Z. Jiang et al. [8] propose a Sybil-proof-based Byzantine fault-tolerant consensus protocol, which can realize real-time consensus in wireless networks. Considering the low-powered wireless devices and instability wireless transmission, Q. Xu et al. [9] propose an efficient and fair Proof-of-Communication consensus protocol in wireless blockchain system. And Y. Zou et al. [10] propose a fast consensus protocol for permissioned wireless blockchain system. This protocol can achieve k-times consensus in unreliable and multi-access wireless environment. Besides, to overcome the interference of wireless broadcast communication, M. Xu et al. propose a single-hop wireless blockchain consensus protocol under an adversarial SINR model BLOWN, which is based on a Proof-of-Channel consensus algorithm [11]. To solve the challenges of multi-hop wireless communication networks, M.Xu et al. design a fast fault-tolerant for wireless blockchain network wChain[12]. To accelerate data aggregation, this protocol constructs communication spanner by the maximum independent set. These blockchain protocols achieve consensus by either consuming massive resources or reliable interaction. In this way, the security of these protocols relies on the correctness of leader, which means malicious leader can interrupt consensus process arbitrarily.

To overcome the mentioned challenge of wireless blockchain system, we propose a blockchain consensus protocol that can reach consensus in instability wireless environment. Stable wireless blockchain consensus protocol is analogy with Proof-of-Stake consensus algorithm, which means nodes can achieve consensus without consuming massive resources. Our protocol combines verified random selection scheme and threshold signature scheme to make sure all nodes in wireless blockchain system can reach consensus randomly and steadily. Stable wireless blockchain consensus protocol operates round by round. In each round, a single block proposer is randomly and non-interactively selected according to nodes' probability, which is depended upon nodes' stability that defined by the lifetime and the number of recent generated blocks of nodes. In block proposer election phase, all nodes only know whether they become block proposer, but do not know who actually is elected as the block proposer. However, each node can verify the legitimacy of real block proposer independently. Such design can greatly reduce resource cost of block proposer election phase and the corruption risk of adversary. What's more, We adopt threshold BLS(Boneh-Lynn-Shacham) signature scheme to decouple block proposer phase and block verification and finalization phase. In this way, block finalization can be achieved by any node that obtain sufficient votes, and not only rely on correct block proposer. Such design can improve the stability and efficiency of consensus process, and reduce the risk of failure consensus due to fault node or instable wireless channel.

We make the following main contributions:

* + We propose a stable wireless blockchain consensus protocol that combines verifiable random election scheme and threshold BLS signature scheme. Our protocol can ensure blockchain system stably generate block and reach consensus in unreliable and unstable wireless networks.
  + We define node stability by the lifetime and the number of recent generated blocks of node. According to the stability of consensus nodes, our protocol can elect a quality node as block proposer randomly and verifiably. This way can reduce the corruption risk of adversary and improve the chance of generating valid block.
  + We use threshold BLS signature scheme to decouple block proposer with consensus process to improve the robustness of stable wireless blockchain consensus protocol. In this way, even block proposer fails after broadcasting a valid block, block finalization can be completed through a round of partial signatures exchanges. What's more, our protocol satisfies strong consistency that can efficiently avoid blockchain forks.
  + When adversary controls less than 50% of voting power, our protocol guarantees persistence and liveness to wireless blockchain system.
  + Finally, massive simulation studies are supported our theoretical analysis.

The rest of this paper is composed as follows. Section 2 introduces the most related works on state-of-art blockchain protocols, wireless consensus algorithms and threshold BLS signature scheme. The models and assumption of this paper is presented in Section 3. In section 4, we discuss the details of the stable wireless blockchain consensus protocol. Security analysis and performance analysis of our protocol is discussed in section 5. We report the result of our simulation in section 6 and give the conclusion of this paper in section 7.

# Related Work

## 2.1 Blockchain Consensus Protocols

We divide the current blockchain consensus protocols into resource-proof-based consensus protocols and communication-based consensus protocols. We will briefly introduce blockchain consensus protocols category in this section, more detailed and comprehensive overview of blockchain consensus protocols has been introduced in [13].

Resource-proof-based consensus protocols require participants compete for block proposal right in each round through physical resources (e.g. computational power, memory, etc.) or virtual resources (e.g. shares, reputation, wealth, etc.). The most classical proof-of-physical-resources is Proof of Work [4] that adopted by Bitcoin and Ethereum. Consensus nodes win the block proposal chance by solving a computational puzzle. However, PoW consensus algorithm cannot provide instant consensus finality of blockchain protocol [14]. Actually, multi-blocks confirmation can guarantee probabilistic consistency of PoW-based blockchain consensus protocol if adversary controls computing power is less than 50% of total power. Therefore, the block-confirmation latency of PoW-based blockchain protocol is large, and transaction throughput is limitation. In addition, other physical-resource-proof-based consensus protocols include Proof of Space [15], in which consensus nodes compete for block proposal right through occupied memory or disk space; and Proof of Burn[16], consensus nodes obtain block proposal chance by burning another “coin”, such as Bitcoin. Physical-resource-proof-based consensus protocols require consensus nodes win block proposal chance by consuming huge physical resources, which lead to the waste of resources. As an alternative to physical-resource-proof-based consensus protocol, virtual-resource-proof-based consensus protocols can avoid large resources overhead. Proof-of-Stake (PoS) [5] is a typical consensus algorithm for virtual-resource-proof-based blockchain consensus protocols. Consensus nodes is elected as block proposer according to their stakes. The more stakes of nodes, the large probability to be block proposer. Casper [17] is a hybrid consensus of PoW and PoS, aiming to replace the PoW consensus algorithm with PoS consensus algorithm in Ethereum. Besides, proof-of-Reputation [18] is also a virtual-resource-proof-based consensus protocol. Consensus nodes with enough reputation can obtain the right to generate a new block. Virtual-resource-proof-based consensus protocols do not consume physical resources, and is friendly to environment. Therefore, more and more blockchain consensus protocols would like to use proof-of-virtual-resource as consensus algorithm.

In communication-based blockchain consensus protocols, all consensus nodes reach consensus on block proposal by exchanging messages and performing local computation. Most of them can tolerate Byzantine fault and provide strong consistency. The most classical communication-based consensus protocol is practical Byzantine fault tolerant consensus (PBFT) protocol [19]. A block proposer is elected from all consensus nodes to generate a new block. Besides, the block proposer is also responsible for communicating with other nodes to reach agreement on block proposal. The malicious cost of adversary in communication-based consensus protocol can be reduced for consensus nodes do not equity mortgage or resource consumption. However, the cooperation mechanism of communication-based consensus protocol can eliminate the influence of malicious behavior and ensure blockchain system security. Some protocols are proposed to improve consensus performance to overcome low scalability. In NEO[20], delegated Byzantine fault tolerant consensus protocol delegates partial nodes to increase consensus performance. These delegated nodes can reach consensus by voting on generated block. In Zyzzyva[21], the modified BFT consensus algorithm SBFT employs threshold signatures to reduce communication cost of consensus process. However, it still requires two-rounds communications to aggregate signatures and terminate block confirmation. In addition, Tendermint consensus algorithm of Cosmos[22] adopts leader rotation mechanism to avoid adversary corruption and use gossip to improve the scalability of transaction propagation. Algorand consensus protocol [23] combines Byzantine agreement protocol and VRF committee election scheme to ensure the security and scalability of blockchain consensus process. Most communication-based consensus protocols rely on the correctness of leader. All consensus nodes should change view when the leader fails and consensus process is interrupted. Besides, communication-based blockchain consensus protocol usually require reliable message transmission model, and make use of all-to-all broadcast communications. Therefore, this blockchain consensus protocol is more suitable for small network size scenarios.

## 2.2 Consensus Protocols for Wireless Networks

We briefly introduce the exist studies on wireless consensus protocols in this subsection.

Many consensus algorithms are proposed to improve consensus efficiency in wireless networks. Leverage the natural superposition property of wireless multiple-access channels, M. Zheng et al. [24] propose fast average consensus in clustered wireless sensor networks to achieve consensus within low times. In order to efficiently achieve a global consensus among nodes in clustered wireless network with respect to arbitrary initial states, M. Goldenbau et al. [25] present an iterative gossip algorithm that based on the superposition property of wireless channel. C. Newport and P. Robinson [26] propose fault-tolerant distributed consensus algorithms to solve consensus problem of wireless systems through abstract MAC layer model. These consensus algorithms can guarantee termination with high probability even there are any number of failures and no advanced information of network. To achieve finite-time max-consensus in a multiagent system, F. Molinari et al. [27] present a switching consensus protocol according to the superposition property of fading wireless channel. Max-consensus can be achieved under this protocol within finite number of iterations. H. Moniz et al. [28] propose an asynchronous Byzantine consensus protocol for resource-constrained wireless ad hoc networks. Even some messages are lost dynamically, the protocol can efficiently achieve consensus.

In recent years, some studies combine wireless consensus algorithms with blockchain to design blockchain consensus protocols that are more suitable for wireless networks. According to the nature property of wireless broadcast communication, Z. Jiang et al. [8] propose a Sybil-proof-based Byzantine fault-tolerant consensus protocol, which can realize real-time consensus in wireless networks. Some studies increase consensus efficiency by making full use of wireless broadcast operation. Q. Xu et al. [9] propose an efficient and fair Proof-of-Communication consensus protocol in wireless blockchain system. And Y. Zou et al. [10] propose a fast consensus protocol that can achieve k-times consensus in unreliable and multi-access wireless environment. Besides, to overcome the interference of wireless broadcast communication, M. Xu et al. propose BLOWN that based on a Proof-of-Channel consensus algorithm under adversarial SINR model [11]. In addition, M.Xu et al. design a fast fault-tolerant wireless blockchain protocol wChain, which can quickly aggregate data and reach consensus in multi-hop wireless communication networks [12].

## 2.3 Threshold Signature Scheme

Blockchain consensus protocols that adopt threshold signature scheme [29] can achieve consensus quickly and steadily in wireless networks with unreliable and unstable communication channels. Threshold signature scheme allows a group of parties to constructing a signature without learning information about private key. In a -threshold signature scheme, parties hold distinct key shares and any subset of distinct parties can issue a valid signature, where as any subset or fewer parties can't. In blockchain consensus protocols, all consensus nodes generate partial signature of consensus result by their private key and broadcast it to other nodes. unique complete signature will be recovered when any node collects enough distinct partial signatures of consensus result. Each node can confirm consensus result by verifying the recovery complete signature. In this way, even some message loss or nodes fail, the consensus can be reached in blockchain system efficiently.

BLS signature scheme [30] utilizes cyclic group and bilinear mapping to construct aggregate signature, which used in multi-party signature and verification. The BLS signature scheme consists of signature generation algorithm and signature verification algorithm. Let be a cyclic group with prime order and generator .And let be a secure hash function. Tuple is considered as global information. Each party has a key pair , where is private key that can be used to compute public key. Signature of message can be computed as, where can ensure the integrity of message Verifiers verify the validity of signature by checking whether is valid.

Threshold BLS signature (TSS) scheme [29] is derived from BLS signature scheme, and work in a non-interactive way. The partial signature generation of TSS is similar to BLS signature scheme, and the recovery of complete signature can be finished without interaction. Threshold BLS signature scheme includes key generation algorithm, signature generation algorithm and verification algorithm. The key generation algorithm adopts distributed key generation protocol [31] to distribute key pair , public keys and the aggregated main public key to participants. And the aggregated main public key is used to verify the validation of complete signature. Let and be the order and generator of cyclic group respectively. Tuple is global information of threshold BLS signature scheme. Discrete log-based distributed key generation protocol is a common key generation algorithm of threshold BLS signature scheme. The key generate protocol will randomly select a special value of -degree polynomial to generate main complete public key that usually used to verify complete signature. And then, each node will use a random value of the polynomial to generate a private-public key pair . A node can recover the unique value if it collects enough secret shares . Signature generation algorithm contains a partial signature generation protocol and a complete signature recovery protocol. Among them, the partial signature generation protocol will generate partial signature of each node; the complete signature recovery protocol will recover unique complete signature, i.e. a Lagrange interpolation polynomial of partial signatures. Besides, the verification algorithm of BLS threshold signature scheme uses the main public key to verify the validation of the complete signature.

Stable wireless blockchain consensus protocol uses the -BLS threshold signature scheme to guarantee the stability and efficiency of consensus process in wireless blockchain system. Since signature aggregation can be executed by consensus nodes, complete signature will be recovered even if some nodes fail to aggregate enough partial signature. Our protocol decreases the risk of single point failure by decoupling block proposer with consensus process. This design greatly improves the stability of wireless blockchain consensus protocol. In addition, consensus process can be finished after one round communication, our consensus protocol decreases the communication complexity significantly.

# Models And Assumptions

In this section, we introduce the models and assumptions in this paper.

## 3.1 Blockchain Basics

In wireless blockchain system, we assume that each node locally maintains a blockchain, which is a hash-chain of blocks. Each block will contain a set of transactions, which can be modeled as a coin exchange process.

## 3.2 Network Model

对于大型无线多跳网络，由于巨大的通信开销和交易的多样性，采用单一委员会的机制完全无法满足性能的需求。为了提高交易处理效率，降低区块确认延时，需要设计一个适用于大型组网的区块链共识算法。

## 3.3 Interference Model

由于大规模无线多跳网络通信都非常复杂，需要的通信资源都非常地巨大，因此可以根据节点的特性（位置、功能等），将节点分片降低节点之间的通信能耗。对于分片的无线多跳网络中的共识算法将面临新的问题，需要相应的解决方案。

区块奖励和交易费用将会平均分发给委员会成员。如果节点在未到活动时间结束之前离开系统，则会扣除部分押金，如果发现有节点作恶，也会扣除押金，从而降低节点离线和作恶的机会。

## 3.4 Adversary

仿真验证区块链的性能：吞吐量和确认延时。仿真设置参数：节点数量、网络分区设置、带宽大小，区块大小等。

# The Stable Consensus Protocol

## 4.1 Overall Architecture

【简单描述区块链模型】

【简单描述区块生成过程】

【重点剖析与研究问题紧密相关的几个部分】

## 4.2 The Stable Consensus Protocol

### 4.2.1 Protocol Basic Setup

对于无线多跳网络环境下的区块链，通常会随着节点数量的增加而降低性能，且具有区块链分叉的危险。为了提高区块链的扩展性，加快交易处理效率，采用DAG区块链不经能够允许分叉，随着节点数量的增加还能降低交易的确认时延。

### 4.2.2 Distributed Randomness Generation Mechanism

1. 带宽：原因？【由于无线通信协议MAC（例如CSMA/CA）的限制，导致区块传输受限，影响最终一致性的达成】方案？【保持无线通讯协议，使用类PoS的共识算法（打包区块不消耗算力），通过减少区块的大小，提到区块传输的成功率；】
2. 分叉：原因

### 4.2.3 Block Proposer Election and proposal Process

### 4.2.4 Block Verification and Finalization Process

### 4.2.5 Protocol Operation Under Faults

#### (1) Sibil Attack

#### (2) Jamming Attack

## 4.3 Reward and Punishment Mechanism

DAG区块链由于允许分叉，因此需要主链机制来为交易分配一个主链序，从而防止交易双花。此外还需要一个交易确认机制使得交易能够在交易流小的情况下也能够最终被确认。

### 4.3.1 Reward Mechanism

### 4.3.2 Punishment Mechanism

共识算法包括见证委员会选举机制、一致性协议、见证委员会重置。

1. 根据节点的稳定度选举出见证委员会成员，随后根据节点的位置、网络延时等作为委员会首领选举的影响因素，给出选举函数，并通过实验得到相应的权重系数。
2. 采用基于可验证随机函数和门限签名一致性协议，需要了解这两种机制的原理，并且根据一致性协议的执行流程设计出相应的功能函数，并给出伪代码。
3. 主链可以采用见证委员会交易来确定。合理的实际主链机制，给出相应的主链号。给出主链的选择原则，并一一讨论。

# Protocol Analysis

## 5.1 Security Analysis

### 5.1.1 Persistence Analysis

### 5.1.2 Liveness Analysis

### 5.1.3 Sybil Attack Analysis

### 5.1.4 Jamming Attack Analysis

## 5.2 Performance Analysis

## 5.2.1 Computational Cost Analysis

## 5.2.2 Communication Cost Analysis

## 5.2.3 Stability Analysis

# Simulation Result

区块确认可以采用门限签名，避免节点之间二次通信。对于门限签名机制需要了解，并且看能否进习性改进使得这个机制具有动态自适应的功能，可以很好的用于我们的场景中。

## 6.1 Weight Coefficient

## 6.2 Block Size

## 6.3 Number of Nodes

## 6.4 Bandwidth

## 6.5 Sybil Attack

## 6.6 Jamming Attack

# Conclusion and Future Research

# References:

[1] J. Xu, S. Wang, A. Zhou and F. Yang, "Edgence: A blockchain-enabled edge-computing platform for intelligent IoT-based dApps," in China Communications, vol. 17, no. 4, pp. 78-87, April 2020, doi: 10.23919/JCC.2020.04.008.

[2] T. Maksymyuk, J. Gazda, L. Han and M. Jo, "Blockchain-Based Intelligent Network Management for 5G and Beyond," 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019, pp. 36-39, doi: 10.1109/AIACT.2019.8847762.

[3] R. Jabbar, N. Fetais, M. Kharbeche, M. Krichen, K. Barkaoui and M. Shinoy, "Blockchain for the Internet of Vehicles: How to Use Blockchain to Secure Vehicle-to-Everything (V2X) Communication and Payment?," in IEEE Sensors Journal, vol. 21, no. 14, pp. 15807-15823, 15 July15, 2021, doi: 10.1109/JSEN.2021.3062219.

[4] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, 2008.

[5] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” in *Annual* *International Cryptology Conference*. Springer, 2017, pp. 357–388.

[6] M. Castro, B. Liskov. Practical Byzantine fault tolerance[C]. Proceedings of the 3rd Symposium on Operating Systems Design and Implementation(OSDI), 1999: 173-186.

[7] Z. Jiao, B. Zhang, L. Zhang, M. Liu, W. Gong and C. Li. A Blockchain-Based Computing Architecture for Mobile Ad Hoc Cloud, in IEEE Network, vol. 34, no. 4, pp. 140-149, July/August 2020.

[8] Z. Jiang, Z. Cao, B. Krishnamachari, S. Zhou and Z. Niu, "SENATE: A Permissionless Byzantine Consensus Protocol in Wireless Networks for Real-Time Internet-of-Things Applications," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6576-6588, July 2020.

[9] Q. Xu, Y. Zou, D. Yu, M. Xu, S. Shen, F. Li. Consensus in Wireless Blockchain System, in WASA, 2020.

[10] Y. Zou, M. Xu, J. Yu, F. Zhao and X. Cheng, "A Fast Consensus for Permissioned Wireless Blockchains," in IEEE Internet of Things Journal, 2021.

[11] M. Xu, F. Zhao, Y. Zou, C. Liu, X. Cheng, F. Dressler. BLOWN:A Blockchain Protocol for Single-Hop Wireless Networks under Adversarial SINR, in CoRR abs/2103.08361, 2021.

[12] M. Xu, C. Liu, Y. Zou, F. Zhao, J. Yu and X. Cheng, "wChain: A Fast Fault-Tolerant Blockchain Protocol for Multihop Wireless Networks," in IEEE Transactions on Wireless Communications, vol. 20, no. 10, pp. 6915-6926, Oct. 2021, doi: 10.1109/TWC.2021.3078639.

[13] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, “A survey of distributed consensus protocols for blockchain networks,” IEEE Commun.Surv. Tutorials, vol. 22, no. 2, pp. 1432–1465, 2020.

[14] M. Vukolic, ‘‘The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication,’’ in Proc. Int. Workshop Open Problems Netw. Secur., 2015, pp. 112–125.

[15] Burstcoin official website. https://www.burst-coin.org/. May. 2019.

[16] B. Wiki. Proof of burn. [Online]. Available: https://en.bitcoin.it/wiki/Proof\_of\_burn

[17] V. Buterin and V. Griffith, ‘‘Casper the friendly finality gadget,’’ 2017, arXiv:1710.09437. [Online]. Available: https://arxiv.org/abs/1710.09437

[18] Proof of Reputation: A Reputation-Based Consensus Protocol for Peer-to-Peer Network. https://link.springer.com/content/pdf/10.1007%2F978-3-319-91458-9\_41.pdf. Jan. 2019.

[19] Fabric official website. https://get.fabric.io/. Jan. 2019.

[20] Open Network for the Smart Economy. Accessed: Mar. 20, 2018. [Online]. Available: <https://neo.org/>

[21] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong, ‘‘Zyzzyva: Speculative byzantine fault tolerance,’’ ACM Trans. Comput. Syst., vol. 27, no. 4, pp. 1–39, 2010.

[22] J. Kwon. Tendermint: Consensus without mining.

https://tendermint.com/static/docs/tendermint.pdf (21 August 2021, date last accessed).

[23] Y.Gilad, R. Hemo, S. Micali, et al. Algorand: Scaling Byzantine agreements for cryptocurrencies[C]. In: Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, October 28–31, 2017: 51–68.

[24] M. Zheng, M. Goldenbaum, S. Stańczak and H. Yu, "Fast average consensus in clustered wireless sensor networks by superposition gossiping," 2012 IEEE Wireless Communications and Networking Conference (WCNC), 2012, pp. 1982-1987, doi: 10.1109/WCNC.2012.6214113.

[25] M. Goldenbaum, H. Boche and S. Stańczak, "Nomographic gossiping for f-consensus", Proc. 10th Int. Symp. Model. Optimiz. Mobile Ad Hoc Wireless Netw., pp. 130-137, 2012.

[26] C. Newport and P. Robinson, “Fault-tolerant consensus with an  
abstract mac layer,” arXiv preprint arXiv:1810.02848, 2018.

[27] F. Molinari, N. Agrawal, S. Stańczak and J. Raisch, "Max-Consensus Over Fading Wireless Channels," in IEEE Transactions on Control of Network Systems, vol. 8, no. 2, pp. 791-802, June 2021.

[28] H. Moniz, N. F. Neves and M. Correia, "Byzantine Fault-Tolerant Consensus in Wireless Ad Hoc Networks," in IEEE Transactions on Mobile Computing, vol. 12, no. 12, pp. 2441-2454, Dec. 2013, doi: 10.1109/TMC.2012.225.

[29] A. Boldyreva. "Threshold signatures, multi signatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme," in Proc. 6th Int. Workshop Theory Pract. Public Key Cryptogr., 2003, pp. 31–46.

[30] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing[C]". International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2001:514-532.

[31] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. "Secure distributed key generation for discrete-log based cryptosystems," in Proc.Int. Conf. Theory Appl. Cryptograph. Techn., vol. 1592, Aug. 2010,pp. 295–310.