IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN IDENTITY BASED ENCRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY AND PERMISSIONED BLOCKCHAIN FOR PROTECTING DATA PRIVACY

Dr. Kondapalli Venkata Ramana, CH. Lakshmi Narayana, Pothula Ushasri

Associate Professor, Department of CSSE AUCE (A), Andhra University, Visakhapatnam
Research Scholar, Department of CSSE AUCE (A), Andhra University, Visakhapatnam
PG Student, Department of CSSE AUCE (A), Andhra University, Visakhapatnam

Abstract: Governments, financial institutions, and high-tech companies have recently focused heavily on blockchain, a developing decentralized architecture and distributed public ledger technology that underpins Bitcoin. Blockchain is thought to increase productivity, save costs, and improve data security, but there are still significant privacy concerns that could prevent blockchain from being widely used. In this research, we introduce a practical technique that significantly enhances data privacy for non-transaction applications by incorporating the Identity-Based encryption system using Elliptic curve cryptography (ECC), solidity and ethereum. Analysis demonstrates that our concept is functional, effective, and practicable in many applications for non-transactional scenarios, and that it has a high security level that can avoid both disguise and passive assaults.

Index Terms- Blockchain, Decentralized Architecture, Identity-Based encryption system, ECC, Solidarity, Ethereum.

1. Introduction

Blockchain is a distributed public ledger system that operates on a peer-to-peer network and is distinguished by its decentralization and lack of trust. It is gaining popularity across a variety of industries and use cases. A distributed network of peer p applying transactions that have been verified by a consensus procedure and arranged into blocks with a hash that links each block to the one before it, these nodes each keep a copy of the ledge. The fundamental design of blockchain .A distributed ledger that keeps track of all network transactions serves as the brain of a blockchain network. It is simple to verify that data has not been altered after the event thanks to this immutability attribute. The blockchain's earliest and most well-known application is the Bitcoin money, but Ethereum took a different tack by including many of Bitcoin's fundamental traits while also including smart contracts to build a platform for distributed applications. A category of public permissionless blockchain technology includes Bitcoin and Ethereum. In essence, these are public networks that are accessible to everyone and allow for anonymous communication. Almost anyone can participate in a permissionless blockchain, and each participant is anonymous. Permissionless blockchains often use a "mined" native coin or transaction fees to give economic incentive to balance the extraordinarily high costs of participation in order to overcome the lack of trust in a form of byzantine fault tolerant consensus based on “proof of work”.

2 Literature Survey

2.1 Identity based key management system

Shamir (1) presented a novel solution to the problem of Secret sharing among nodes. He devised an ideaof sharing Secret data D by dividing among n nodes in n pieces in such a way that it can be reconstructed by any t pieces. Even Knowledge of t – 1 will not be able to reconstruct the data D. Shamir called it as (t, n) threshold scheme. He used Polynomial interpolation and divided secret D into n pieces and each piece is the value of the polynomial at that point. Thus any t pieces can reconstruct D using Lagrange interpolation. He suggested for modular arithmetic and not real arithmetic. This scheme was later on used by many researchers for construction distributed PKG to enhance security. Various identity based key management scheme are available in the literature. Key management includes generation of the key and distributing

the same safely and later on safekeeping and renewal of generated keys. A comparative study of some of the important schemes is presented here.

2.1.1 Khalili-Katz-Arbaugh's Id based key management

This scheme emphasized on key distribution and threshold cryptography. It introduced the concept of distributed PKG. A set of n nodes required to perform the function of PKG. Such nodes are known asthreshold PKG. The master Private key is provided to all nodes of a network in such a way that no ansy node can generate a master private key on its own but at least t nodes are required to complete this function. It is known as (t, n) threshold scheme. Node's identity is its public key. It assumed that nodeidentity is recorded into hardware and can't be altered. Private Key is generated by at least t nodescollectively. Each of these t nodes shall provide a part of node's private key on successful authentication. A node combines these parts and gets its private key.

.

2.1.2 Deng-Mukharji-Agrawal's scheme

This scheme is divided into two parts:

- Private key generation in distributed way
- Identity based authentication

In the first phase, the master key is generated for key generator nodes. Each node's public and private key is calculated and sent in a secure way. In the second phase, identity based authentication is provided. Authentication is ascertained end to end. On successful authentication, a secret key is exchanged between nodes and communication takes place using such shared key. The scheme uses IP Address as identity. In this scheme during key generation phase, network's master key is generated. Also, each node is provided with a pair of public and private keys. End to end authentication is provided through the presented authentication scheme which is based on node's identity. Also, the communication among nodes is confidential. On successful authentication only, a session key is exchanged and future communication takes place using this session key.

2.1.3 IDAKE - Identity based authentication and key exchange

There are two main variants of this scheme: Basic IDAKE and fully self-organized IDAKE. It uses symmetric cryptography and pairing based keys. The trusted Third party initializes all devices before they join the network. The public key is Qi = H1 (Idi || 'expiry date'). They are first to introduce key revocation and key renewing mechanisms for IBC schemes. Both the variants employ pairing based keys and symmetric cryptography. The scheme is divided into following six sub-algorithms:

Setup generates a long-term private key of PKG and public parameters of the network.

Extract generates participating nodes' public key – as identity and computes private key.

Distribute, the private key is provided to nodes, when two nodes want to communicate.

Compute algorithm provides a symmetric paired key which will be used for encryption of data.

Key Renewal will play its part when a key's lifetime is expired or it is revoked during operation.

Key Revocation is activated when a node is found to be compromised. Various rule-based observations are carried out like neighborhood watch and accusation scheme to perform this operation. In basic mode, PKG performs pre-initialization activities like the setup, extract, and distribution of keys algorithm. In the second mode that is running system phase, nodes themselves perform various activities like computation of shared keys, key renewal, and key revocation.

2.1.4 Identity Based key management scheme – IKM

This scheme is a combination of threshold cryptography and key management using identity. It Proves IKM has advantages over Certificate based cryptographic scheme. Public and private keys of the nodes are formed using their identity and a network-wide common element.

PKG issues a random number salt to each node with an efficient hash function h such as SHA-1. Use of common network element facilitates fast and efficient key update through a broadcast message. On the other hand, ID-basedelement helps in maintaining the secrecy of nodes.

The key pre-distribution happens in network initialization where PKG provides keying material and system parameters to each node. PKG also hand over it's working to a set of distributed PKGs, which are called d-PKGs. The private key is computed by (t,n) threshold cryptography. For key revocation, during normal network operation mode, each node monitors another node for any malicious activity. If any suspected activity is observed then that node sends a signed message to d-PKG. A node is declared malicious when a number of accusations reported at d-PKG against it reach its defined revocation threshold limit. In this scheme, nodes update their public and private keys at defined intervals. A revoked node is not able to renew its key on its own and hence gets separated from the network.

3 Implementation Study

To meet the needs of enhancing the data privacy in blockchain, it is necessary to use encryption technology to transform the plaintext to the ciphertext, and the encryption algorithm should be carefully designed to avoid broking the process of consensus. However, for non-transaction case, all operations in consensus don't involve mathematical operations. Therefore, as long as solving the key management problem, we can make sure that sensitive data encrypted while recording on the blockchain. In this section, we construct a simple ID-based encryption privacy protection scheme, which can be well applied to non- transaction scenarios in permissioned blockchain. ID-based Encryption. In 1984, Shamir [4] asked for

a public key encryption scheme in which the public key can be an arbitrary string and the private key can be generated by the trusted third party PKG (Private Key Generator)

DISADVANTAGES:

1. LESS ACCURACY
2. LOW EFFICIENCY

3.1 Proposed Methodology

In the proposed system, the master key is of the most importance. Once the master key is compromised, the entire system is destroyed. As a result, it should be carefully saved. In many systems, the master key is managed by a single PKG, which brings problems of centralization and security. At this point, a threshold secret sharing scheme can be used. By constructing a (t, n) threshold scheme, the master key is controlled by a multi-trusted PKG instead of a single PKG, thus any single PKG cannot recover the master key, which solves the problem of centralization and security here we implement private key generation using ECC cryptography

Advantages:

1. HIGH ACCURACY
2. HIGH EFFICIENCY

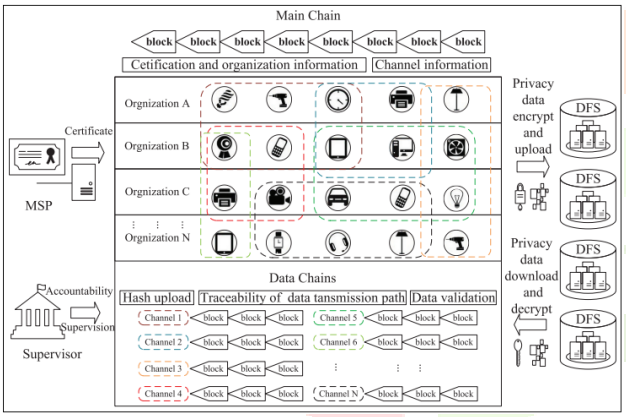

Fig1: System Architecture

4. Methodology and Algorithm

MODULES:

4.1 **Block chain generator**: - by using we generate the block chain here it will generate the 10 block chain users and 10 block chain private keys after that we use the master key to connect to the solidarity to store the data in the form of blocks

4.2 **User login:** - user has to first register and after registration the user can upload a document and message where these data will be stored in the block chain and the image will be only visible to the user after the validation of the ECC private key is validated and then the user can view the information which was shared to the user only the permissible users can see the data.

4.3 Ethereum Implementation

4.3.1 Bitcoin signalled the emergence of a radically new form of digital money that operates outside the control of any government or corporation.

4.3.2 With time, people began to realize that one of the underlying innovations of bitcoin, the blockchain, could be utilized for other purposes.

4.3.3 Ethereum proposed to utilize blockchain technology not only for maintaining a decentralized payment network but also for storing computer code that can be used to power tamper-proof decentralized financial contracts and applications. Ethereum applications and contracts are powered by ether, the Ethereum network's currency.

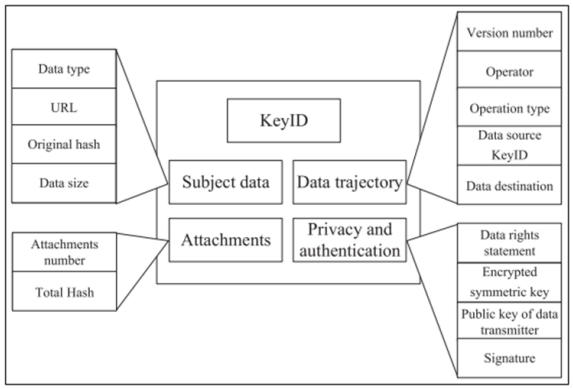

Fig 2: - process structure

We suggest a version-based, fine-grained, and privacy-protected data structure with five sections, as illustrated in Figures 2 and 3. These sections are KeyID, Subject data, Attachments, Data trajectory, and Privacy and authentication. For each data transmission activity on the blockchain, the KeyID component represents the specific identifying code. The transmitted data's metadata are contained in the Subject data portion. The information about attachment files is kept with the primary data in the Attachments portion.

4.4 ECC Algorithm: -

Elliptic Curve Cryptography (ECC) is a contemporary family of public-key cryptosystems that is based on the algebraic structures of elliptic curves over finite fields and on the challenge of the Elliptic Curve Discrete Logarithm Problem (ECDLP).

ECC implements encryption, signatures, and key exchange, which are the three main asymmetric cryptosystem features.

Since ECC utilises fewer keys and signatures than RSA for the same level of security and offers very quick key generation, quick key agreement, and quick signatures, it is seen as the logical modern replacement for the RSA cryptosystem.

Step 1: -The private keys in the ECC are integers (in the range of the curve's field size, typically 256-bit integers). Example of 256-bit ECC private key (hex encoded, 32 bytes, 64 hex digits) is: 0x51897b64e85c3f714bba707e867914295a1377a7463a9dae8ea6a8b914246319.

Step 2: - The key generation in the ECC cryptography is as simple as securely generating a random integer in certain range, so it is extremely fast. Any number within the range is valid ECC private key.

Step 3: - The public keys in the ECC are EC points - pairs of integer coordinates $\{x, y\}$, laying on the curve. Due to their special properties, EC points can be compressed to just one coordinate + 1 bit (odd or even). Thus, the compressed public key, corresponding to a 256-bit ECC private key, is a 257-bit integer. Example of ECC public key (corresponding to the above private key, encoded in the Ethereum format, as hex with prefix 02 or 03) is: 0x02f54ba86dc1ccb5bed0224d23f01ed87e4a443c47fc690d7797a13d41d2340e1a. In this format the public key actually takes 33 bytes (66 hex digits), which can be optimized to exactly 257 bits.

All algebraic operations within the field (like point addition and multiplication) result in another point within the field. The elliptic curve equation over the finite field **𝔽p** takes the following modular form:

$$y2 \equiv x3 + \_a\_x + b \pmod{p} \quad \text{-eq1}$$

Respectively, the "Bitcoin curve" secp256k1 takes the form:

$$y2 \equiv x3 + 7 \pmod{p} \quad \text{-eq2}$$

Unlike **RSA**, which uses for its key space the **integers** in the range [0...p-1] (the field $\mathbb{Z}p$), the **ECC** uses the **points** $\{x, y\}$ within the Galois field **𝔽p** (where x and y are integers in the range [0...p-1]). An **elliptic curve over the finite field 𝔽p** consists of:

- a set of integer coordinates $\{x, y\}$, such that $0 \le x, y < p$
- staying on the elliptic curve: $\_y\_2 \equiv x3 + \_a\_x + b \pmod{p}$

Example of elliptic curve over the finite field **𝔽17**:

- $y2 \equiv x3 + 7 \pmod{17}$

This elliptic curve over **𝔽17** looks like this:

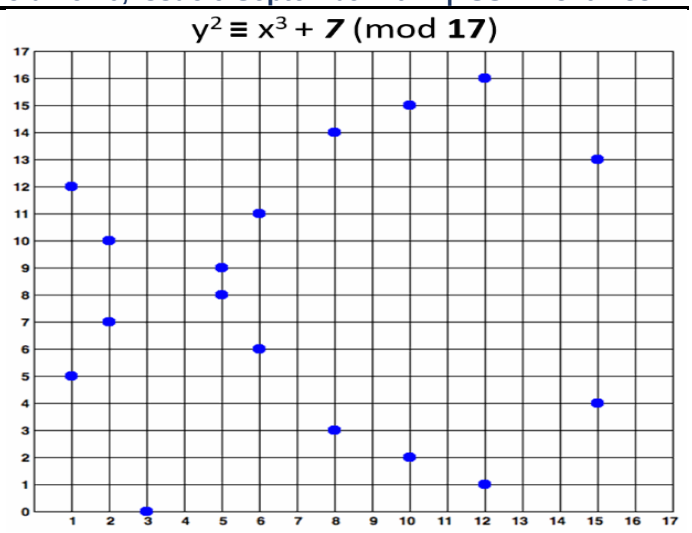

Fig 3:- Note that the elliptic curve over finite field y2 ≡ x3 + **7** (mod **17**) consists of the **blue points** at the above figure, i.e. in practice the "*elliptic curves*" used in cryptography are "*sets of points in square matrix*", not classical "*curves*".

5 Results and Evolution Metrices

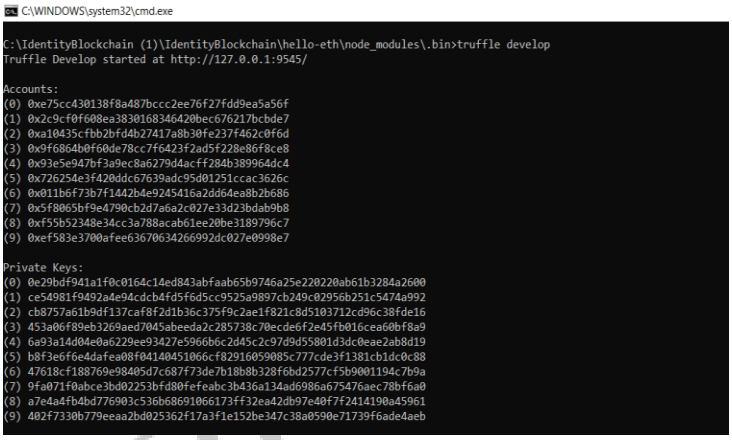

Fig 3: Block chain private keys generated using Ethereum

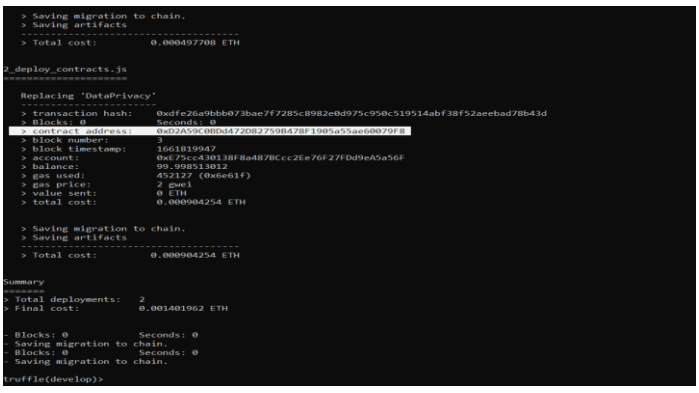

Fig 4: Contract Address

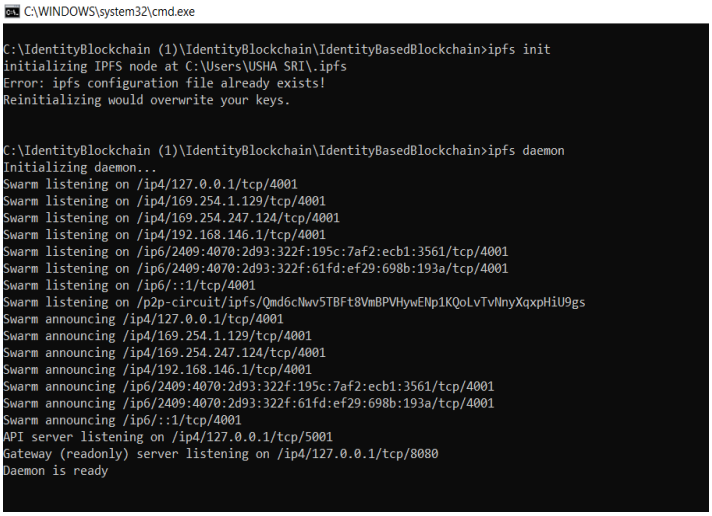

Fig 4: IPFS Server Started

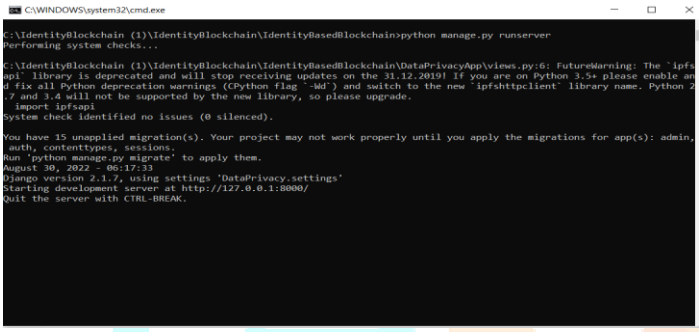

Fig 5: Django Server Started

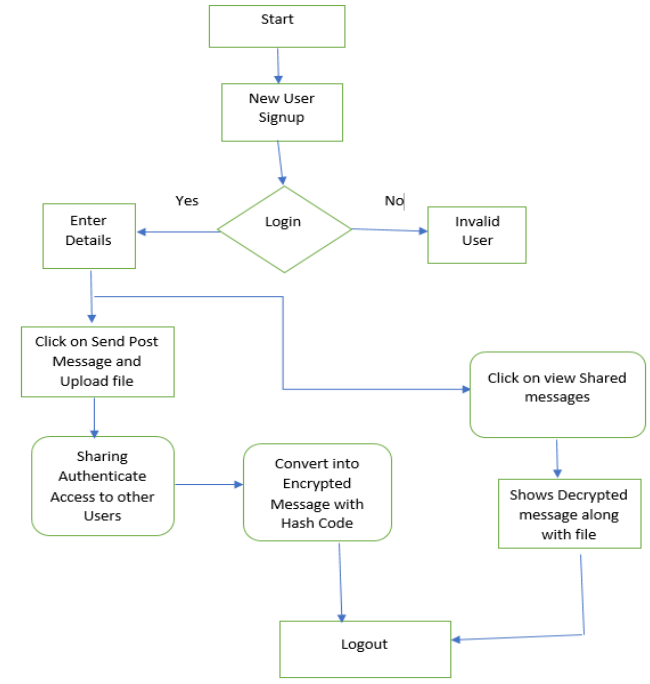

Fig 6: Flow Process

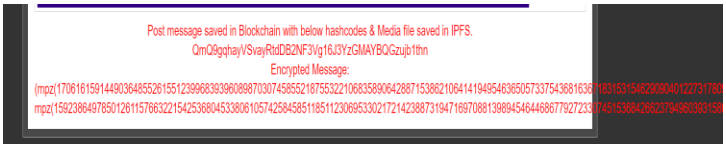

Fig 7: Encrypted Message with Hash Code

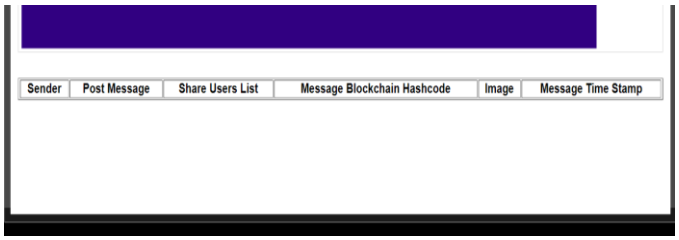

Fig 8: Unauthorized user has no access to decrypt

6 Conclusion

To further demonstrate the privacy, we have suggested an enhanced delicately scheme on top of non-transactional circumstances in permissioned blockchain. Without the use of cutting-edge technologies like ring signature, homomorphic encryption, or zero-knowledge proofs, our approach may conceal the information by converting the plaintext into the ciphertext. Our approach not only eliminates the challenging certificate issuing and management seen in the conventional PKI system, but it also offers a high level of security that can thwart passive and disguised attacks and is functional, efficient, and useful for applications. This system offers an innovative method for maintaining sensitive transaction confidentiality in numerous applications for non-transactional contexts.

7 References

[1] The Linux Foundation Helps Hyperledger Build the Most Vibrant Open Source Ecosystem for Blockchain. http://www.linuxfoundation.org/.

[2] S. Omohundro. Cryptocurrencies, smart contracts, and artificial intelli- gence. AI Matters, 1(2):19C21, Dec. 2014.

[3] D. D. Detwiler. One nations move to increase food safety with blockchain. https://www.ibm.com/blogs/blockchain/2018/02/one-nations-move-to-increase-food-safety-with-blockchain/,2018. [Online; accessed 1-May-2018].

[4] Shamir, A. Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47C53. Springer, Heidelberg (1985)

[5] Boneh, D., Franklin, M. Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213C229. Springer, Berlin, Ger- many (2001)

[6] Boneh, D., Boyen, X. Efficient selective-ID secure identity based en- cryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223C238. Springer, Berlin, Germany (2004)

[7] Boneh, D., Boyen, X. Secure identity based encryption without random oracles. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, Springer, Berlin, Germany (2004).

[8] Gentry, C. Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445C464. Springer, Berlin, Germany (2006).

[9] Labs, Shen Noether Mrl. Ring confidential transactions. 2016.

[10] R. S. Wahby, I. Tzialla, A. Shelat, J. Thaler and M. Walfish. Doubly- Efficient zkSNARKs Without Trusted Setup. 2018 IEEE

Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 926-943.

[11] B. Bnz J. Bootle D. Boneh A. Poelstra P. Wuille G. Maxwell. Bullet- proofs: Efficient range proofs for confidential transactions", IEEE S&P May 2018.

[12] A. Chiesa E. Tromer M. Virza. Cluster computing in zero knowledge, EUROCRYPT Apr. 2015.