Multisignature with double threshold condition in the blockchain and its application to and strong keys generating

Ruslan Skuratovskii[1], Anastasia Afanasieva[2], Alexandr Kalenyk[3]

National Aviation University, [1]ORCID: 0000-0002-5692-6123.
[1]ruslcomp@gmail.com, ruslan.skuratovskii@nau.edu.ua
[2]anastasia.afanasieva.bit@stud.nau.edu.ua, [3]oleksandr.kalenyk.bit@stud.nau.edu.ua

Abstract*. Improving the reliability of account protection in the blockchain is one of the most important goals of the entire cryptographic arsenal used in the blockchain and cryptocurrency exchange. We propose a new threshold multisignature scheme with a double boundary condition. Access to funds stored on a multisig wallet is possible only when two or more signatures are provided at the same time.*

Keywords*— multisignature (t,n) with threshold in blockchain, non-commutative cryptography, CSP and CDH problems; Miller-Moreno p-group, generalization of CDH problem, conjugacy problem, multisignature in blockchain.*

A simple analogy is a safe deposit box or safe with two locks and two keys. Maria holds one key, Juan holds the other. They can open the cell only if they present both keys at the same time. Individually, they cannot open a cell without the approval of the other [1].

Thus, multisig wallets provide an additional layer of security. With this technology, users can avoid the problems often encountered with single-key wallets, single point of failure, and vulnerable to attacks from cybercriminals who are constantly developing new phishing techniques.

Since multisig wallets require more than one signature to move funds, they are also suitable for businesses and corporations looking to store funds in shared wallets.

Definition. Multisignature is a technology for signing transactions with multiple private keys to increase security and privacy during the approval process for sending transactions.

A multisignature is a kind of threshold signature, implemented as a check of conditions specified in the basic scripting language of the cryptocurrency. Multisignature technology has become widespread in the

world of cryptocurrencies [2].

Definition. A token is a digital certificate that guarantees the company's obligations to its owner, an analogue of shares on the stock exchange in the world of cryptocurrencies [3].

Definition. Threshold signature is a variant of an electronic signature, for the imposition of which the cooperation of at least ***t*** members of a group of ***n*** participants is required, denoted as. S_n . In essence, it is a special case of the threshold division of a secret according to the scheme (***t***, ***n***), when the private key is split into ***n*** parts, and any ***t*** parts are enough to recover it. The public key is used in the usual way. Generation, sharing of a key and distribution of its fragments requires a group manager (dealer).

Multisignature technology has become widespread in the world of cryptocurrencies. A token is a digital certificate that guarantees the company's obligations to its owner, an analogue of shares on the stock exchange in the world of cryptocurrencies Threshold signature - a variant of an electronic signature, for the imposition of which the cooperation of at least t members of a group of n participants is required, denoted as S_n. In essence, it is a special case of the threshold division of a secret according to the (*t, n*) scheme, when the private key is divided into n parts, and any *t* parts are sufficient to restore it (these *t* persons we call as *significants*). The public key is used in the usual way. Generation, sharing of a key and distribution of its fragments requires a group manager (dealer).

Note that such a group can be, in particular, a manning pool consisting of ***n*** members.

Since the idea of public key cryptography (PKC) was introduced by Diffie and Hellman [2, 4] in 1976, many PKC schemes have been proposed and broken. For instance Diffie Hellman key exchange protocol is vulnerable to man in the middle attack during key exchange steps. To prevent these attacks we propose to use block chain and divide on domains blockchain using proof of stake (PoS). The automatic generation of unique one-time keys prevents the connectivity of transactions and is

possibly due to the optimization of the key exchange using the Diffie-Hellman method.

Any subset of nodes had to have a unique multisignature key. Multisignature is a technology for signing transactions with multiple private keys to increase the level of security and privacy during the approval process for sending transactions. A multisignature is a kind of threshold signature, implemented as a check of conditions specified in the basic scripting language of the cryptocurrency.

Let's denote $m_i(n)$ – the number of tokens in the wallet of the i-th account belonging to a subset S_n of the n accounts from the blockchain which use (PoS). Note that one participant can have several accounts, therefore, we consider double indexing $m_{ij}(n)$ where i – denotes a wallet in the blockchain network and j is the owner of the wallet. More generally, cryptocurrency can be used instead of tokens. It is convenient to express the value of a token in cryptocurrency as in monetary terms.

Note that such a group can be in particular a manning pool consisting of n participants. Let us denote by $m_{ij}(n)$ the number of tokens in the wallet of the *i*-th account belonging to the subset S_n of *n* accounts from the blockchain. Note that one participant can have several accounts, so we consider double indexing $m_{ij}(n)$ where a number of wallet in the blockchain network denoted by *i* and j is the owner of the wallet. More generally, cryptocurrency can be used instead of tokens. It is convenient to express the value of a token in cryptocurrency as in monetary terms.

We introduce a double threshold signature condition according to the scheme (***t***, ***n***), where different *t* participants have rights to make sign (persons entitled to sign or *significants*) from S_n satisfying the inequality

$$\sum_{i=1}^{t} m_{ij}(n) \geq S(n) \tag{1}$$

Where t is minimal number of *significants* which is enough to make multisignature if they satisfy condition (1), where $j \in S_n$ that is, participant j really belongs to the group S_n from n persons. The $S(n)$ this is the boundary

number of tokens (or their value in the specified crypto currency) that persons must have in order to be eligible for multisignature.

Access to funds stored on a multisignature wallet is possible only when two or more signatures are provided at the same time. At its core, a user's account can be identified with his wallet. But one person can have several accounts (for example, this happens during a CB-attack). Therefore, if person j proves that she has in the aggregate at least the threshold amount necessary to satisfy the inequality of the threshold amount for multisignature, then the sums of tokens or currency equivalents on all her wallets are summed up and included in the total amount of the group S_n. To install accounts on a node, each of the participants can use the BIP 39 algorithm. Even on one node, one person can have several accounts. Therefore, we will summarize each wallet j -th the participant indexing it by its index i and then we summarize the amounts available to different participants in the external amount by j. Then we construct **multisignature with scheme** (t,n), where t is minimal number of significan, number of wallets of participant j denoted by $k(j)$ and $m_{ij}(n)$ is sum of taken in i -th wallet of j -th participant of blochain

$$\sum_{j=1}^{t}\sum_{i=1}^{k(j)} m_{ij}(n) \geq S(n)$$

The method of proving that j -th a person has a certain amount in the wallet can be a simple contract, where the money is transferred back to the same j -th user. Thus, the j -th participant shows in the contract that he has this amount explicitly, but then transfers it back to himself (possibly by paying for the transaction). In most cases, for example, in the Effirium currency, the amount in the wallet is visible inside the blockchain. In addition, such an amount can be counted as the sum of incoming money from records inside blockchain transactions and the amount of outgoing spending from this wallet visible in blockchain transactions. Thus, in any case, the total amount of tokens or currency of the j -th participant can be calculated without cost.

We will divide the entire blockchain into domains, each of which has its own digital signature. Only those domain entities whose wallets have the number of tokens in excess of a percentage of the critical number of tokens of the entire blockchain domain have the right to sign. The persons who has the authority to sign in the i-th domain will be denoted by S_i. If a domain member does not have a number of tokens that exceed the percentage of critical tokens of the entire domain i, it can apply for the right to sign to the authorized person of his domain S. It should be noted that S_n can be located at the intersection of domains, then the process of transferring the key is simplified due to the fact that an authorized person acts as a surety of two parties at once.

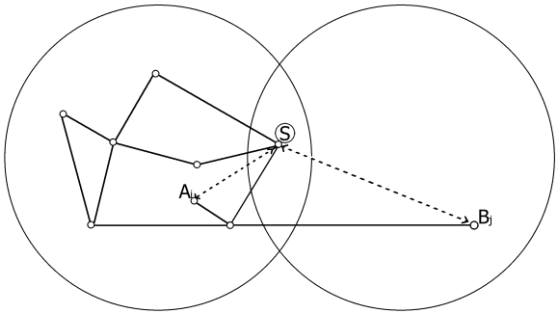

Fig. 1 Location of information exchange participants, with S at the intersection

We consider this case that is specified at Fig. 1. Suppose that *S*, as shown in the figure, is at an intersection, A located in *i*-th domain intends to transfer the secret key a, to person *B* in domain j, then A encrypts the component of new secret key k wich *A* and *B* going to construct, with using the conjugating by secret key x and sends it for signature to authorized persons *S*, in turn, returns the message with signature. Then the process of transferring the key to side *B* takes place. Side *B*

receives the message and sends it for verification to S, and only then encrypts the received message with its key.

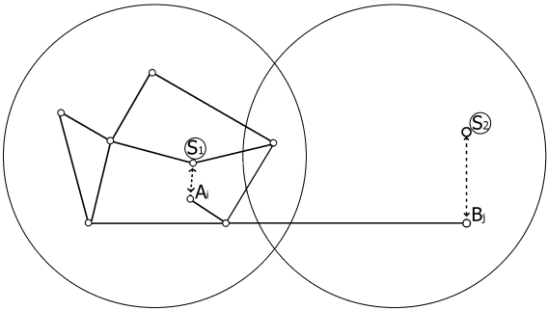

Fig. 2 Location of information exchange participants, without S at the intersection

In the second case that is specified at Fig. 2, at the intersection of domains there is no person with the authority to sign S, then we denote the person with the authority to sign in the domain in which A is located as S_1, in the case of side B, as S_2, respectively. It is worth noting that the parties S_1 and S_2 must have a part of the digital signature of the neighboring domain, or the ability to exchange with a secure transmission channel. Then A, as in the first case, encrypts the message and transmits it to S_1, then, S_1 returns the tuple [$x^{-1}ax$, $Sign(x^{-1}ax)$]. After the transfer now side B sends the not signed message to S_2 for identification.

We consider non-commutative generalization of CDH problem [8] on base of metacyclic group *G* of Miller-Moreno type (minimal non-abelian group). We show that conjugacy problem in this group is intractable. For preventing attacks of decomposition or man in the middle attack [7, 9, 10] both key exchange protocol [7] participants send to network arbitrator (*o*) hash $h(\beta)$ and a hash of conjugated element $h(\beta^g)$ [4] by an private key element β. key exchange protocol with using signature

To avoid well known Man-in-the-Middle Attack [7, 11,12] we use multisignature with double threshold condition in blockchain.

Our goal is the obtaining an efficient algorithm for conjugated elements computation in the case we want to develop a key exchange algorithm on the basis of non-commutative DH problem [3]. Because of the relation in metacyclic group, which determine the homomorphism $\varphi:\langle b\rangle\rightarrow \mathrm{Aut}(\langle a\rangle)$ to the automorphism group of the $A=\langle a\rangle$, a formula to find a conjugated element is obtained. By applying this formula, we are able effectively compute the element conjugated to a^i by means of raising to the $1+p^{(m-1)}$-th power by modulo p^m, where $m>1$.

Thus, our protocol it not vulnerable for the attack of the man in the middle by solving the decomposition problem [10] of key exchange.

References:

[1] Funds stored on a multisig wallet is possible only when two or more signatures are provided at the same time. [Electronic resource] / According to the general edition «Multisignature» Access mode: https://www.okex.com/academy/ru/%D0%BC%D1%83%D0%BB%D1%8C%D1%82%D0%B8%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C

[2] Multisignature is a technology for signing transactions with multiple private keys to increase security and privacy during the approval process for sending transactions. [Electronic resource] / According to the general edition «What is multisignature? What is a ring signature?» Access mode: https://forklog.com/chto-takoe-multipodpis/

[3] A token is a digital certificate that guarantees the company's obligations to its owner, an analogue of shares on the stock exchange in the world of cryptocurrencies. [Electronic resource] / According to the general edition Karpova K. Access mode: https://secretmag.ru/enciklopediya/chto-takoe-token-obyasnyaem-prostymi-slovami.htm

[4] Skuratovskii, R. V. Employment of Minimal Generating Sets and Structure of Sylow 2-Subgroups Alternating Groups in Block Ciphers. Advances in Computer Communication and Computational Sciences, Springer, pp. 351–364, 2019.

[5] Skuratovskii, R. V. A Multi Agent-Based System for Securing University Campus: Design and Architecture - IEEE Conference Publication. 2019-12-17. doi:10.1109/ISMS.2010.25.

[6] Skuratovskii, R. V. The timer compression of data and information.Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020, pp. 455–459.

[7] Skuratovskii, R. An Application of Metacyclic and Miller-Moreno p-Groups to Generalization of Diffie-Hellman Protocol. Advances in Intelligent Systems and Computing, 2021, 1290, pp. 869–876.

[8] Gu, L., Zheng, S.: Conjugacy systems based on nonabelian factorization problems and their applications cryptography, J. Appl. Math. 6 pp. 1–10, 2014.

[9] Gu, L. Wang, L., Ota, K., Dong, M., Cao Z. and Yang, Y.: New public key cryptosystems based on non-abelian factorization problems, Secur. Commun. Netw. 6 (7), pp. 912–922, 2013.

[10] Bohli, J.-M., Glas B., and Steinwandt, R.: Towards provable secure group key agreement building on group theory, Cryptology ePrint Archive: Report 2006/079, 2006.

[11] Ruslan Skuratovskii, Alexandr Kalenyk. Blockchain and key distribution problemThe 11th International Scientific Conference «ITSec» October, 1-6, 2021

[12] Bharat Bhushan; G. Sahoo; Amit Kumar. Man-in-the-middle attack in wireless and computer networking. 3rd International Conference on Advances in Computing,Communication Automation (ICACCA). DOI: 10.1109/ICACCAF.2017.8344724

[13] Skuratovskii, R., Osadchyy, V., Williams, A. An application of metacyclic and Miller Moreno *p*-groups to establishment protocol WSEAS Transactions on Mathematicsthis link is disabled, 2020, 19, pp. 384–390.

[14] Skuratovskii, R., Osadchyy, V., Williams, A. An application of miller moreno groups to establishment protocol non commutative cryptography. Advances in Intelligent Systems and Computingthis link is disabled, 2021, 1290, pp. 869–876.

[15] Skuratovskii, R., Osadchyy, V. Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020this link is disabled, 2020, pp. 126–130, 9210334