МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний технологічний університет
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

21-22 квітня 2022 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 21-22 квітня 2022 р**.** - Одеса, Видавництво ОНТУ, 2022 р. – 251 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова - д.т.н., проф., **Єгоров Б.В.**, ректор ОНТУ

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНТУ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНТУ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м.Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц., Київський національний університет імені Тараса Шевченка

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНТУ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНТУ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНТУ,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ “Львівська політехніка”,
Жуков І.А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською та англійською мовами.
Редактор збірника Котлик С.В.

ЗМІСТ

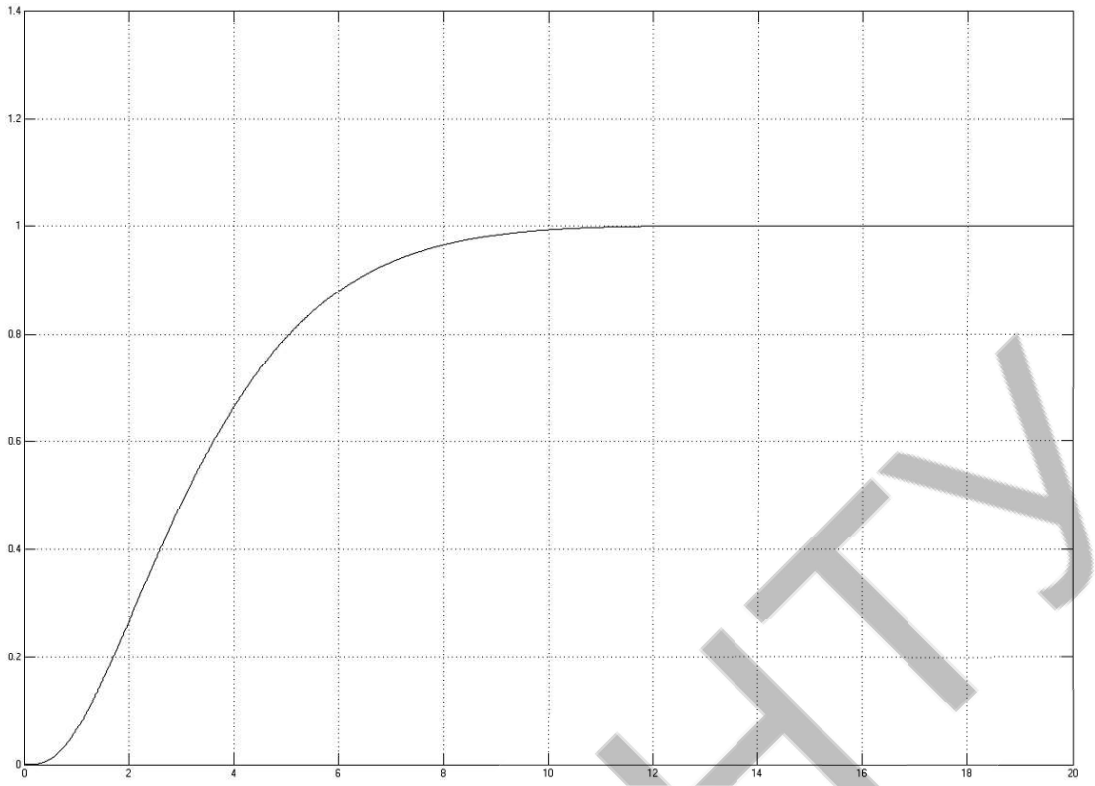

Figure 1 – Transient process of closed-circuit ACS with integrated correcting component

UDC 003.26

CUMULATIVE DISCRETE LOGARITHM ZERO-KNOWLEDGE PROOF

K. VOLKOV (kyrylo-volkov@stud.onu.edu.ua), I. MAZUROK (igor@mazurok.com),
Y. LEONCHYK (leonchik@ukr.net), O. ANTONENKO (asantonenko@gmail.com)
Odesa I. I. Mechnikov National University

Keywords: zero-knowledge proof, cryptographic, elliptic curve, blockchain

Introduction. Currently cryptographic algorithms are widely used in many areas of information technology. The most used of its achievements are encryption and digital signature algorithms, zero-knowledge proofs and so on. The last ones have become especially popular due to rapid development of blockchain technology [1].

Intuitively (not formally) the idea of zero-knowledge proof is to provide person A with the possibility to prove to person B some knowledge K in such a way that from the one hand B becomes sure that knows the value K, and from the other hand B does not gain any additional knowledge. Such schemes are widely used in decentralized networks. For example, Ethereum uses them as one of the main components for the Sharding concept implementation.

Discrete Logarithm Zero Knowledge Proof. The discrete logarithm zero-knowledge proof most applicable in applied tasks proof.

Let G to be a cyclic group with generator g such that the finding the discrete logarithm in this group is computationally difficult. The standard problem of discrete logarithm zero-knowledge proof is formulated as following for given value $y \in G$ prove knowledge of such value x that $y = g^x$.

In the [2] the following scheme of the proof is given. In order to generate the proof the prover Peggy:

1.Generates random value v and computes $t = g^v$.

2.Computes $c = hash(g, y, t), i = \overline{1, n}$

3.Peggy computes $r = v - cx$

4.The proof is the pair (t, r).

In order to verify the proof verifier Victor

1.Computes $c = hash(g, y, t), i = \overline{1, n}$

2.Checks the next equality: $t = g^r y^c$

Cumulative Discrete Logarithm Zero Knowledge Proof. The described scheme of the discrete zero-knowledge proof has a significant drawback: in order to sequentially proof knowledge of n values it is necessary to generate n proofs that can very expensive from the memory point of view. Such a problem is especially important in blockchain. From the other hand based on applied tasks, a convenient tool should allow proving knowledge of values $x_1, \dots, x_{t_n}$ for some increasing sequence $t_1, \dots, t_m, \dots$ with the following asymptotic complexity:

	Individual Proof	m Proofs
Time	$O(t_m - t_{m-1})$	$O(t_m)$
Memory	$O(1)$	$O(m)$

In order to satisfy all the requirements we offer the scheme of Cumulative Discrete Logarithm Zero-Knowledge Proof that consists of two parts.

Main Proof

Cumulative Proof Generation. Let Peggy has already generated the Proof for values $x_1, \dots, x_{t_{m-1}}$ and now she would like to prove Victor that she possesses values $x_1, \dots, x_{z_m}$ that are discrete logarithms of values $y_1, \dots y_{z_m}$ base g. In order to generate the Main Proof Peggy

1) computes $c_i = hash(g, y_i)$, $i = \overline{z_{m-1} + 1, z_m}$

2) randomly picks $v \in Z_l$, where l is the size of the group G.

3) computes $t_{z_m} = g^v$.

4) computes $r_{z_m} = v - c_1 x_1 - \dots - c_{z_m} x_{z_m} mod l$

The tuple $b = \left(t_{z_m}, r_{z_m}\right)$ is called Main Proof.

Safety Proof

The Safety Proof serves for the avoidance of fraudulent generation of the Main Proof. It allows proving that Peggy truly knows the value of the discrete logarithm of $t_{t_{z_m}}$ using standard discrete logarithm zero-knowledge proof.

In order to generate Safety Proof Peggy:

1) randomly picks $w \in Z_l$;

2) computes $f = g^w$;

3) computes $d = hash\left(f, t_{z_m}, P\right)$;

4)computes $k = w - dv mod l$.

The tuple $q = (f, k)$ is called Safety Proof.

Cumulative Proof Verification. The Verification of the Cumulative Proof for values $x_1, \dots x_{t_m}$ consists of two parts: Safety Proof Verification and Main Proof Verification.

Safety Proof Verification

In order to verify whether the Safety Proof is valid, Victor:

1) computes $d = hash\left(f, t_{t_{z_m}}, P\right)$;

2) verifies the equality: $f = g^k t_{t_{z_m}}^d$.

If the equality is true, then Victor goes to Main Proof Verification else the entire Proof is invalid.

In order to verify whether the Main Proof is valid, Victor:

1) computes $c_i = hash(g, y_i), i = \overline{z_{m-1}+1, z_m}$;

2) verifies the equality $t_{z_m} t_{z_{m-1}}^{-1} = g^{r_{z_m} - t_{z_{m-1}}} y_{z_{m-1}+1}^{c_{z_{m-1}+1}} \cdot \ldots \cdot y_{z_m}^{c_{z_m}}$

If the equality is true then the entire Cumulative Proof is considered as a valid one.

Conclusion. In the work a new cryptographic algorithm called cumulative discrete zero-knowledge proof was offered. It allows proving the knowledge of sequence of values effectively from the point of time and memory complexity and possesses Completeness, Soundness and Zero-Knowledge properties.

Literature.

1. Ben-Sasson, E., Chiesa, A., Tromer, E. & Virza, M. "Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture". *SEC'14: Proceedings of the 23rd USENIX Conference on Security Symposium.* 2014. p. 781–796.

2. Bernhard, D., Pereira, O. & Warinschi, B. "How Not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios". *Advances in Cryptology – ASIACRYPT*. 2012. p. 626-643. DOI: https://doi.org/10.1007/978-3-642-34961-4_38.

UDC 669.184:004.942

COMPUTER SYSTEM OF THE THERMAL MODE OF THE TOP CONVERTER LANCE

ZHULKOVSKYI O.O., ZHULKOVSKA I.I.,
PANTEIKOV S.P, MUZYCHKA K.O. (olalzh@ukr.net)
Dniprovsky State Technical University

A computer information-modeling forecasting system of the thermal mode of the top lance barrel of the oxygen converter has been developed in order to fulfill the urgent and economically feasible task of determining the compliance of the input technological parameters with certain safety criteria for conducting of converter melting, on the basis of mathematical modeling and object-oriented programming.

Nowadays, safe and stable converter melting is fulfilled due to permanent monitoring of the technological process and its adjustment. It requires continuous or discrete information about the parameters of the steelmaking pool and, first of all, about the carbon content and the temperature of the metal. Knowledge of these parameters allows you to make the necessary adjustments during the melting. Moreover, it gives high accuracy of the obtained (final) results of the converter processing.

Thus, the development of forecasting systems, which allow you to determine the compliance of the input technological parameters with certain safety criteria for conducting converter melting, is an actual and economically feasible task.

The presence of forecasting systems of the thermal mode of the top blowing lance barrel during the melting in an oxygen converter means providing a rational temperature regime for the blowing devices throughout the entire operation period to increase their service life, exploitation and trouble-free operation period. This is especially urgent for the conditions of the mining and metallurgical industry of Ukraine, where many converter shops are equipped with outdated designs of top water-cooled lances, which do not fulfil the technical and technological requirements and have welded lance heads with a low service life [1].

What is more, such forecasting computer systems make it possible to determine the optimal design and technological parameters of the used lancers (gaps for coolant supply, pipe thickness and material, water flow and temperature etc.) on the stage of the development of the top blow device.

XXII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

21-22 квітня 2022 р

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.