УДК 004.056

В. І. Селезньов

МЕТОД АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІЗ НУЛЬОВИМ ЗНАННЯМ

Вінницький національний технічний університет;

Анотація

Проаналізовано відомі методи автентифікації з нульовим знанням. Запропоновано новий метод автентифікації користувачів із нульовим знанням, що дозволяє підвищити стійкість односторонньої автентифікації за рахунок внесення модифікацій у процес автентифікації.

Ключові слова: автентифікація користувача, криптографічний протокол, алгоритм, доведення з нульовим знанням.

Abstract

The analysis of known zero knowledge authentication methods was performed. A new zero knowledge authentication method was proposed to increase stability of one-sided authentication by making modifications to the authentication process.

Keywords: user authentication, cryptographic protocol, algorithm, zero knowledge proof.

Вступ

Від реалізація процесу автентифікації може залежати безпека не лише користувача, а й усієї системи. Не всі сучасні засоби автентифікації забезпечують достатній рівень захищеності при автентифікації користувача. Серед сучасних засобів автентифікації використання доведення з нульовим розголошенням дозволяє усунути велику кількість відомих атак на процес автентифікації за рахунок відсутності розкриття будь-якої інформації про секретні дані [1].

Актуальність розробки методу автентифікації користувачів із нульовим знанням полягає у необхідності підвищення стійкості, шляхом внесення модифікацій у процес автентифікації.

Об’єктом дослідження є процес автентифікації користувачів. Предметом дослідження є засоби та методи автентифікації користувачів. Метою дослідження є покращення захищеності автентифікації користувачів із нульовим знанням шляхом внесення модифікацій у процес автентифікації. Для досягнення мети необхідно:

- проаналізувати відомі методи автентифікації з нульовим знанням;
- виконати порівняння методів автентифікації з нульовим знанням
- розробити метод автентифікації з нульовим знанням.

Аналіз протоколів автентифікації з нульовим знанням

У протоколах автентифікації з нульовим знанням користувач, що проходить автентифікацію (Петті) повинен довести стороні сервера (Віктору), що він володіє секретною інформацією без розкриття секрету при цьому. Тобто при виконанні процесу автентифікації відбувається нульовий розголос секрету Петті.

На сьогодні класичними протоколами автентифікації з нульовим знанням є протокол Шнорра, протокол Фіата-Шаміра протокол на основі задачі про ізоморфізм графів з різними модифікаціями. Серед сучасних протоколів доведення з нульовим розголошенням представлені протоколи zk-SNARK, zk–STARK та Bulletproofs.

Протокол Шнорра застосовує проблему дискретного логарифмування для процесу автентифікації. Спочатку відкритий ключ Петті обчислюється з секретного ключа x за формулою $y = \alpha^x \bmod p$, де p – достатньо велике випадкове число; α – випадкове число великого простого порядку $q < p$. Процес

автентифікації складається з декількох раундів, які, в свою чергу, складаються з трьох основних кроків:

Петті обирає випадкове число $k(k < q)$, обраховує значення $R = \alpha^k \bmod p$ та передає Віктору.

Віктор формує випадковий біт r та передає Петті.

Петті обчислює $w = k + rx \bmod p$ та відсилає Віктору. Віктор виконує перевірку співвідношення:

$$Ry^r \equiv \alpha^w \bmod p \tag{1.1}$$

У разі істини співвідношення Петті успішно проходить автентифікацію.

Протокол Фіата-Шаміра заснований на складності добування квадратного кореня за складеним модулем, але має подібну структуру до протоколу Шнорра [2].

Перед процесом автентифікації обирається секретний ключ, модуль та відкритий ключ, що обчислюється шляхом піднесення секретного ключа до квадрату за модулем.

Процес автентифікації розпочинається з вибору Петті випадкового числа, піднесення його до квадрату за обраним модулем та передачі результату Віктору. Віктор випадковим чином формує число 0 або 1 і передає його Петті. Петті виконує обчислення піднесення секретного ключа до степені отриманого від Віктора, виконує множення результату на випадкове число, яке вона сформувала раніше, за відповідним модулем. Результат обчислення надсилається до Віктора. Віктор виконує перевірку результату шляхом його піднесення до квадрату за відповідним модулем та порівнянням з власним результатом, отриманим на основі відкритого ключа та випадкового числа Петті. У разі ідентичності результатів, Петті успішно проходить раунд автентифікації [3].

Протокол zk-SNARK використовується у багатьох сучасних криптовалютах. zk-SNARK є представником неінтерактивних протоколів з нульовим знанням. Якщо розглядати з сторони конфіденційності, то дана форма є більш безпечною, оскільки відсутність взаємодії сторонами дає більшу впевненість в тому, що витоку інформації під час взаємодії не відбудеться. zk-SNARK складається з трьох ефективних алгоритмів (G, P, V).

Генерування ключів G отримує на вхід секретний параметр λ та програму C і генерує два загальнодоступні ключі, p_k ключ для доведення та v_k ключ для верифікації. Дані ключі є публічними і генеруються лише один раз для заданої програми.

Алгоритм побудови доведення P отримує на вхід ключ доведення p_k, публічний параметр x та секретний параметр w. Алгоритм генерує доведення $\pi = P(p_k, x, w)$.

Завдяки своїй структурі та особливостям алгоритму протокол є достатньо стійким до переважної більшості сучасних атак. Окрім того zk-SNARK має одні з найкращих показників швидкодії та невеликий обсяг даних, що передається при автентифікації. Головним недоліком zk-SNARK є потреба у етапі налаштування перед виконанням автентифікації [4].

На відміну від zk-SNARK, zk-STARK не вимагає попереднього налаштування і розкриття інформації третій стороні. Протокол zk-STARK використовує нову технологію інтерактивного доведення з оракулом або IOP (Interactive Oracle Proofs).

Нехай, Петті хоче довести Віктору, що вона володіє деякими даними, які задовольняють якийсь функції. Тоді вона представляє ці дані у вигляді дерева Меркле і відправляє геш кореня дерева Віктору. Віктор тоді вибирає випадковим чином якусь кількість точок і просить для цих точок надіслати гілки дерева Меркле. Петті обчислює і відправляє необхідні дані. Віктор перевіряє, що ці отримані гілки відповідають тим, які належать початковому кореню дерева. Віктор також перевіряє, що в цих точках значення задовольняють деякій функції перевірки. Зазначений трьох-кроковий алгоритм може бути перероблений в неінтерактивному доведенні, де Петті відправляє лише одне повідомлення, яке може бути перевірено будь-яким учасником [5, 6].

Bulletproofs – новий неінтерактивний протокол з нульовим знанням, що не потребує попереднього довіреного налаштування та використовує короткі доведення.

Bulletproofs придатний для доведення тверджень щодо фіксованих значень, таких як докази діапазонів, арифметичні схеми тощо. Протокол базується на дискретному логарифмічному припущенні та є неінтерактивним за допомогою евристики Фіата-Шаміра. Основним алгоритмом Bulletproofs є внутрішній алгоритм продукту, представлений Гротом. Алгоритм перевіряє знання двох зв'язаних векторів зобов'язання Педерсена, що відповідають вказаному внутрішньому зв'язку [7].

Bulletproofs спиратися на методику, описану в [7], що дозволяє збільшити ефективність внутріш-

ньої взаємодії при виконанні доведення та зменшує загальну складність комунікацій до $2\log_2(n)$, де n – розмір двох векторів зобов'язань. Протокол Bulletproofs реалізує проведення доведення приналежності до короткого та агрегованого діапазону, використовуючи поліноми. Докази діапазону - це доведення того, що таємне значення (секрет) належить до певного інтервалу. Докази діапазону не дають жодної інформації про секрет, крім того, що він належить інтервалу.

У порівнянні із zk-SNARK та zk-STARK протокол Bulletproofs значно повільніший та потребує значного часу як на роботу на доведення Петґі, так і на перевірку доведення Віктором [8, 9].

Порівняння протоколів автентифікації з нульовим знанням здійснено на основі властивостей, якими володіють протоколи. Серед переліку властивостей час виконання протоколів, потреба у початкових налаштуваннях, обсяг даних, що передається при використанні протоколу з стандартними параметрами, стійкість до деяких атак та особливості структури. Результати порівняння протоколів автентифікації показано в таблиці 1.

Таблиця 1 – Порівняння протоколів автентифікації з нульовим знанням

№	Властивість	протокол автентифікації				
		Протокол Фіата-Шаміра	Протокол Шнорра	zk-SNARK	zk-STARK	Bulletproofs
1	Потреба у «trusted setup»	+	+	+	-	-
2	Час підтвердження «verification time»	12мс	13мс	10мс-20мс	10 мс	1 сек
3	Час доведення «proof time»	від 2 до 4 сек	від 2 до 4 сек	до 4 сек	до 2 сек	більше 10 сек
4	Розмір даних, що передаються	~135KB	~80KB	288B	45KB-200KB	1.3KB-10KB
5	Перевіряє автентичність двох сторін	-	-	-	-	+
6	Стійкість до атаки за обраним шифр-текстом	+	+	+	+	+
7	Стійкість до атаки «маскарад»	+	+	+	+	+
8	Стійкість до пост квантових атак	-	-	-	+	-
9	Побудований на основі дерев Меркла	-	-	+	+	-

В результаті дослідження та порівняння методів автентифікації з нульовим знанням з'ясовано, що високі показники захищеності мають усі розглянуті методи, однак Bulletproofs має найгірші показники швидкості, а zk-SNARK та zk-STARK побудовані на основі дерев Меркла, що доцільно для систем з подібною структурою даних. Отже, для подальшого дослідження та моделювання протоколу автентифікації користувачів із нульовим знанням за основу варто взяти протоколи Шнорра та Фіата-Шаміра, що забезпечують оптимальні показники швидкості та безпеки автентифікації.

Результати розробки

Розглянутий у [2, 3] підхід до автентифікації з нульовим розголошенням секрету поєднує для відомих протоколи автентифікації користувачів із нульовим знанням: протокол Шнорра та протокол Фіата-Шаміра. За описаним підходом два протоколи мають подібну структуру, що дозволяє уніфікувати вхідні та вихідні дані для застосування кожним із протоколів. Однак одночасне використання двох протоколів, хоч на перший погляд і дозволяє збільшити стійкість системи, однак має низку недоліків, наприклад збільшення обсягу даних, що передаються при автентифікації, збільшення часу автентифікації удвічі. Крім того, одночасне використання двох стійких протоколів автентифікації за стійкістю відповідатиме використанню одного з протоколів, але зі збільшенням кількості раундів удвічі.

Оскільки два відомих методи автентифікації з нульовим знанням базуються на різних математичних проблемах: дискретного логарифмування для протоколу Шнорра та складності добування квадратного модуля за складеним модулем, що включає два великих простих множники, які зберігаються в секреті,- для протоколу Фіата-Шаміра, то з міркувань безпеки доцільно під час автентифікації вико-

ристати вибір одного із зазначених протоколів. При кожній новій автентифікації користувачів вибір протоколу для автентифікації повинен бути псевдовипадковим. Тоді у разі атаки на протокол автентифікації зловмиснику спочатку потрібно буде дізнатися, за обчисленнями якого саме з протоколів, Шнорра чи Фіата-Шаміра користувач проходить автентифікацію.

Під час процесу автентифікації користувач повинен узгодити з сервером початкові дані при автентифікації, що дозволять узгодити обраний протокол автентифікації. Для псевдовипадкового вибору протоколу використано регістр зсуву з лінійним зворотнім зв'язком РЗЛЗЗ [10]. Регістр зсуву при кожній наступній автентифікації користувача надаватиме старший біт послідовності регістру, який приймає два можливих значення, що відповідають протоколу, за яким відбуватимуться подальші обчислення. Для забезпечення синхронізації взаємодії між користувачем, що проходить автентифікацію та сервером початковий стан регістр зсуву з лінійним зворотнім зв'язком для користувача та сервера повинен бути однаковим, тобто його необхідно узгодити між двома учасниками взаємодії.

Для здійснення встановлення початкового стану регістра зсуву з лінійним зворотнім використано додатковий програмний токен [11]. Токен надається кожному користувачу сервером та надає користувачу відповідне значення початкового стану, що передається у зашифрованому вигляді. Таким чином кожен новий процес автентифікації для користувача можливий лише за наявності токену користувача. Процес автентифікації користувача за таким методом зображено на рисунку 1.

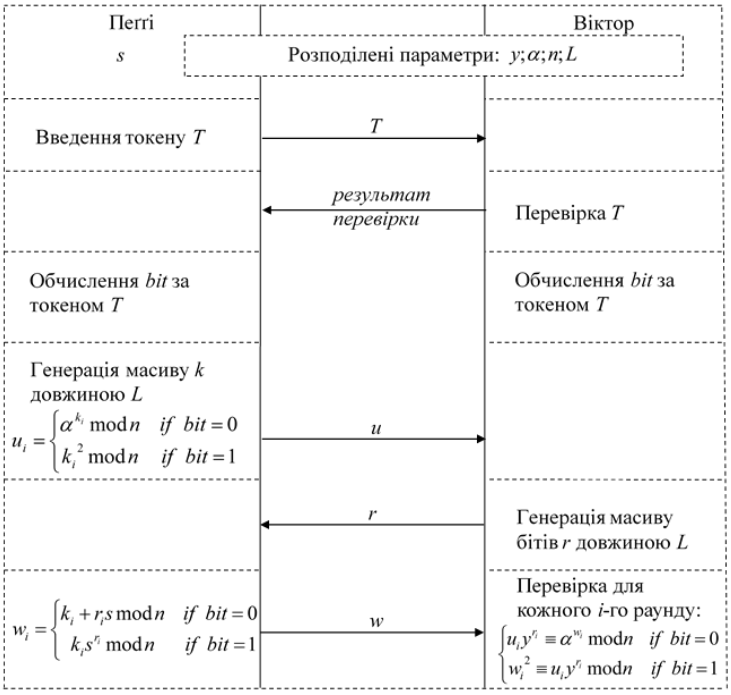

Рисунок 1 – Процес автентифікації користувача

Запропонований метод автентифікації з нульовим знанням передбачає зменшення кількості раундів у порівнянні з оригінальними протоколами, а також у протоколі суттєво покращується стійкість при автентифікації.

Висновки

На основі результатів порівняння сучасних протоколів автентифікації користувачів із нульовим знанням було визначено, що більшість з них забезпечують стійкість при великій кількості раундів та розраховані для використання в системах особливої структури, що породжує необхідність модифікації досліджених методів для забезпечення високого рівня захищеності при автентифікації. Модифікований метод автентифікації користувачів із нульовим знанням, який на відміну від відомих методів використовує псевдовипадковий вибір способу реалізації раунду автентифікації з нульовим знанням, що дозволяє вдвічі підвищити рівень захищеності при автентифікації за рахунок необхідності початкового «вгадування» зловмисником способу реалізації раунду автентифікації. Використання модифікованого методу суттєво підвищує складність реалізації модуля, однак це не є суттєвим при програмній реалізації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Баришев, Ю. В. Кривешко К. І. Метод автентифікації користувачів комп`ютерної мережі з прив`язкою до параметрів робочої станції / Тези доповідей Третьої Міжнародної науково-практичної конференції «Інформаційні технології та коп‘ютерна інженерія», м. Вінниця, 29-31 травня 2012 р. – Вінниця : ВНТУ, 2012. – С. 187-188.

2. Селезньов В. І. Баришев Ю. В. Протокол автентифікації з нульовим знанням / XLIX науково-технічної конференції підрозділів ВНТУ: Матеріали доповідей, Вінниця, 27-28 квітня 2020 р. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2020/paper/view/9299 (дата звернення 22.12.2021).

3. Селезньов В. І. Модуль автентифікації користувачів / Всеукраїнська науково-практична інтернет-конференція Молодь в науці: дослідження, проблеми, перспективи (МН-2021): Матеріали доповідей, Вінниця, URL: https://publish.vntu.edu.ua /index.php/mn/mn2021/paper/view/11169 (дата звернення 22.12.2021).

4. Ben-Sasson E., Chiesa A., Tromer E. Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture. 2015. URL: https://eprint.iacr.org/2013/879.pdf (дата звернення: 21.09.2021)

5. Ben-Sasson E., Bentov I., Horesh Y. Scalable, transparent, and post-quantum secure computational integrity. 2018. URL: https://eprint.iacr.org/2018/046.pdf (дата звернення: 21.09.2021)

6. Ben-Sasson E., Chiesa A., Spooner N. Interactive Oracle Proofs. 2016. URL: https://eprint.iacr.org/2016/116.pdf (дата звернення: 22.09.2021)

7. Bulletproofs: веб-сайт. URL: https://sikoba.com/docs/SKOR_DK _Bulletproofs_ 201905.pdf (дата звернення: 25.09.2021)

8. Awesome zero knowledge proofs (zkp): веб-сайт. URL: https://github.com/matter-labs/awesome-zero-knowledge-proofs (дата звернення: 25.09.2021)

9. Zero-Knowledge Proofs: STARKs vs SNARKs: веб-сайт. URL: https://consensys.net/blog/blockchain-explained/zero-knowledge-proofs-starks-vs-snar ks/ (дата звернення: 25.09.2021)

10. Баришев Ю. В. Метод автентифікації віддалених користувачів для мережевих сервісів / Ю. В. Баришев, В. А. Каплун. Інформаційні технології та комп'ютерна інженерія: наук.-техн. журнал. – 2014. – Том 30. – № 2. – с. 13-17.

11. Ісхаков, А. Ю., Мещеряков Р.В., Ходашінскій І.А. Двухфакторная аутентифікація на основі программного токена Питання захисту інформації. 2013. № 3. С. 23-28.

Селезньов Віталій Ігорович — студент групи 1БС-20м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: seleznov.vitalii@kaskadb.com.ua

Науковий керівник – ***Баришев Юрій Володимирович*** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua

Seleznov Vitalii — Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : seleznov.vitalii@kaskadb.com.ua

Scientific supervisor – ***Baryshev Yurii*** — PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, yuriy.baryshev@vntu.edu.ua