КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1181
УДК 004.056.5:004.738.5:004.75

Шлапак Вікторія Олексіївна
студентка кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка», м. Львів, Україна
ORCID: 0009-0009-0185-7632
viktoriia.shlapak.kb.2022@lpnu.ua

Семенюк Сергій Анатолійович
к.ф.-м.н., доцент кафедри безпеки інформаційних систем
Національного університету «Львівська політехніка», м. Львів, Україна
ORCID: 0000-0002-8143-5887
serhii.a.semenyuk@lpnu.ua

БЕЗПЕЧНА АВТОРИЗАЦІЯ БАНКІВСЬКИХ ТРАНЗАКЦІЙ НА ОСНОВІ СХЕМИ ШНОРА

Анотація. Метод безпечної авторизації банківських транзакцій на основі схеми Шнора представляє криптографічний підхід до підтвердження автентичності користувача із застосуванням протоколів доведення з нульовим розголошенням (Zero Knowledge Proof, ZKP). Запропонований підхід орієнтований на мінімізацію ризиків компрометації конфіденційних даних під час виконання транзакцій у відкритих або частково довірених середовищах. Основою методу є використання протоколу ідентифікації Шнора, що має в основі складність задачі дискретного логарифмування і дає змогу здійснювати перевірку автентичності без передачі секретного ключа користувача. Модель авторизації включає процес взаємодії між трьома складовими транзакції, а саме: клієнтом, захищеним середовищем виконання транзакції та банківською стороною. Протокол включає у себе послідовність етапів: спочатку відбувається генерація початкових параметрів (p, g), далі формується значення публічного ключа (y), на його основі створюється доказ (t), на стороні банку генерується виклик (e) та подальше обчислення значення параметру s, з подальшою перевіркою коректності співвідношення на стороною банку. Особливістю є відсутність передачі приватного ключа та використання випадкових значень, що унеможливлює відновлення секретних параметрів навіть при перехопленні частини даних. У межах дослідження реалізовано моделювання атак типу MITM та replay-атак з метою оцінки стійкості запропонованого підходу. У випадку атаки «людина посередині» показано, що модифікація параметра t призводить до порушення перевірочного співвідношення, що унеможливлює успішну авторизацію транзакції. Для протидії replay-атакам у модель інтегровано механізм часових міток (TS) та унікальності параметрів транзакції, що виключає можливість повторного використання перехоплених даних. Побудована модель базується на криптографічній стійкості, зменшення впливу вразливості середовища виконання транзакції та забезпечення основних принципів цифрової безпеки, а саме цілісності, конфіденційності та автентичності даних. Запропонований метод демонструє ефективність у сценаріях, де рівень загроз є високим.

Ключові слова: банківська транзакція, схема Шнора, доказ з нульовим розголошенням, MITM атака, replay атака.

ВСТУП

У сучасному цифровому світі, кількість фінансових транзакцій невпинно зростає. Тому забезпечення безпеки проведення процесів банківських транзакцій та автентифікації їх користувачів набуває все більш критичного значення. Звичні методи забезпечення захисту, які передають конфіденційні дані є вразливими до типових атак, наприклад, до replay-атак та MITM.

Одним із варіантів вирішення цієї проблеми, це використання криптографічних протоколів, які в своїй основі дотримуються принципу нульового розголошення (Zero-Knowledge Proofs). Такі протоколи дають змогу підтвердити автентичність користувача, без необхідності розкриття його конфіденційних даних. Одним з прикладів є схема Шнора, яка базується на складності виконання дискретного логарифмування, чим забезпечується високий рівень криптостійкості.

Постановка проблеми. Традиційні методи є вразливими до більшості нових атак, зокрема до атаки типу MITM («людина посередині») та атак типу replay («атака повторного використання»). Тому актуальним є дослідження та проєктування авторизації банківських транзакцій побудованих на нульовому знання, в основі схеми якої лежить схема Шнора, а також визначення процесу та алгоритму захисту від атак.

Аналіз останніх досліджень і публікацій. У сучасних дослідженнях публікацій, велика увага приділяється саме впровадженню криптографічних протоколів, для безпечної авторизації користувачів у фінансових системах. У роботах [1] і [2] розглядається протокол Шнора, що має в своїй основі задачу дискретного логарифмування, та використовується для побудови протоколів доведення з нульовим розголошенням. Ці протоколи дають змогу довести, що сторона володіє секретним параметром, без розкриття його вмісту, що підвищує рівень захищеності даних користувачів. Теоретичну основу доведень з нульовим розголошенням заклали Goldwasser, Micali та Rackoff [3], довівши можливість інтерактивного доведення знання без розкриття інформації. Безпека схем цифрового підпису та сліпого підпису на основі ZKP детально проаналізована у роботі Pointcheval і Stern [4], де формально доведена стійкість схеми Шнора до атак на видавання себе за іншу особу. Питання захисту від атак типу MITM в мережевих протоколах розглядається у роботі Conti, Dragoni та Lesyk [5]. Сучасний стан та тенденції застосування ZKP у фінансових технологіях висвітлено у роботі Ben-Sasson et al. [6], де показано перспективність протоколів нульового розголошення для побудови масштабованих та приватних платіжних систем.

МЕТОДИКА ДОСЛІДЖЕННЯ

Дослідження проводилося у кілька етапів. На першому етапі здійснено теоретичний аналіз протоколу ідентифікації Шнора та його властивостей у контексті захисту банківських транзакцій. На другому етапі розроблено модель авторизації та проведено моделювання сценаріїв атак типу MITM та replay за допомогою мови програмування Python 3.11. Для реалізації криптографічних операцій використовувалися бібліотеки hashlib (для обчислення хеш-функцій) та secrets (для генерації криптографічно стійких випадкових чисел). Параметри тестового середовища: просте число p (512 біт), генератор групи g, випадкові значення r генерувалися в межах [1, p-2]. Часова мітка TS формувалася як Unix-час з точністю до секунди з допустимим вікном відтворення не більше 30 секунд. Критеріями оцінки стійкості слугували: коректність перевірки доказу в штатному режимі, здатність системи відхиляти модифіковані параметри (атака MITM) та застарілі докази (replay-атака), а також відсутність витоку інформації про приватний ключ у будь-якому з повідомлень протоколу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У процесі проведення банківської транзакції основними його учасниками є клієнт, середовище проведення транзакції та банк. Вразливим місцем цієї транзакції є середовище виконання транзакції, оскільки його можна скомпрометувати. Метою створення моделі загрози є визначення потенційних напрямків атаки, що можуть порушити основні аспекти безпеки авторизації банківської транзакції, а саме цілісність, автентичність та конфіденційність даних.

Для побудови безпечного протоколу авторизації використовується Zero–Knowledge Proofs схема Шнора [1], яка базується на властивостях дискретного логарифмування. Важливо зазначити що використовується випадкове значення r, а виклик e формується як хеш від параметрів протоколу даних транзакції.

Основними етапами авторизації на основі схеми Шнора є формуванні доказу, виклику доказу та відповіді банку. Процес відображено на рис. 1 у якому були відображені такі дії:

1 – передача клієнту значень p і g;

2 – передача банку значення параметрів даних транзакції та TS що буде часовою міткою;

3 – передача банку значення публічного ключа y;

4 – передача обчисленого значення t, як початок створення доказу;

5 – надсилання значення e клієнту. Включення значення публічного ключа y в значення хеш-функції є критичним, задля запобіганням подальших атакам, де зловмисник може спробувати використати доказ, який був наданий клієнтом для іншого ключа.

6 – надсилання вирахуваного значення s.

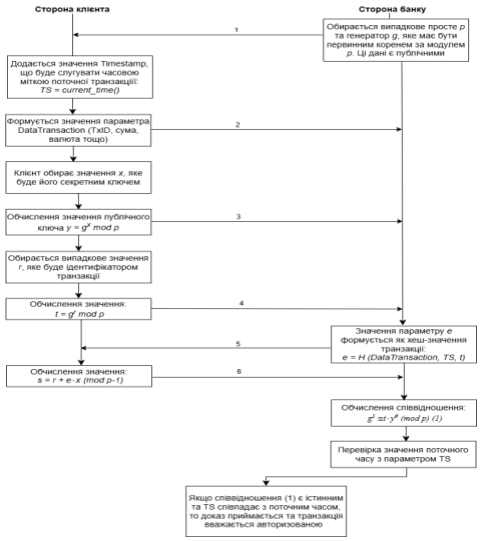

Рис. 1. Процес авторизації банківських транзакцій на основі схеми Шнора

Згідно схеми Шнора, під час авторизації банківської транзакції жодна сторона протоколу не повинна розкривати приватний ключ користувача *x*, випадкове число *r*, яке використовується під час процесу доказу, а також проміжні обчислення, які зможуть спростити процес відновлення секретного параметру *x*, та значення всіх параметрів проведеної процедури, задля уникнення його повторного використання.

Однією із основних можливих загроз може бути атака типу MITM («людина посередині») [4] де зловмисник перехоплює або модифікує дані, які передаються між клієнтом та банком. Під час реалізації зловмисної схеми атаки типу MITM (рис. 2), будемо вважати, що значення публічного ключа *y* було передано іншим захищеним каналом зв'язку, тобто фактично зловмисник не має доступу до цього значення. Потрібно врахувати, що значення *e* буде обчислюватися на двох сторонах транзакції незалежно.

Отже атака типу MITM почне свою дію з перехоплення обчисленого користувачем параметра *t*, і зловмисник замінить його на своє значення *t'*. Також, оскільки значення параметра *e* було обчислено двома сторонами, то після модифікації зловмисником значення *t* значення *e* будуть відрізнятися. Далі створення процедури доказу вже буде відбуватися зловмисником на основі змінених даних. У кінці співвідношення не буде правильним, оскільки значення публічного ключа не було перехоплено, а тільки деякі значення співвідношення (1) було модифіковано. Тому під час перевірки на стороні банку співвідношення не буде істинним. Таким чином доказ не буде істинним, а отже транзакція не буде авторизованою.

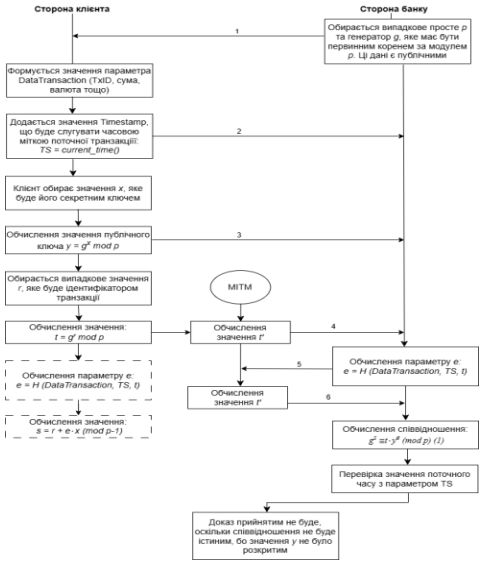

Рис. 2. Схема авторизації з реалізацією атаки типу MITM

Далі розглянемо сценарій атаки типу replay. Суть атаки полягає у тому, що зловмисник перехоплює справжню передачу даних між сторонами транзакції (сторона банку та клієнта). Інформація, яка була захоплена, буде зберігатися для подальшого використання.

Атака типу replay (рис. 3) почне свою дію з перехоплення параметрів транзакції, після її завершення, а саме DataTransaction, TS, t, s. Далі вже зловмисник маскується під клієнта та відправить отримані параметри транзакції другій стороні. У свою чергу на стороні банку було додано пункт перевірки значення параметра TS, що є часовою міткою, для перевірки дійсності та автентичності даних. Отже доказ не буде істинним, тому транзакція не буде авторизованою.

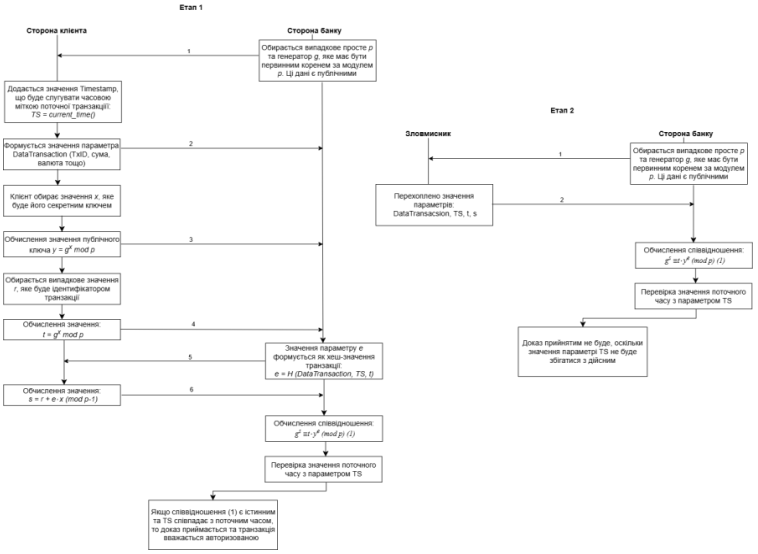

Рис. 3. Схема авторизації з реалізації replay-атаки

ОБГОВОРЕННЯ

Отримані результати підтверджують принципову відмінність підходу на основі ZKP від традиційних методів ідентифікації, зокрема парольної автентифікації та схем на основі одноразових кодів (OTP). На відміну від цих підходів, схема Шнора не передає жодного секретного параметра між сторонами, що усуває цілий клас загроз, пов'язаних із перехопленням облікових даних. Порівняно з PKI-рішеннями, де компрометація закритого ключа може призвести до тривалого несанкціонованого доступу, ZKP-підхід обмежує ризик окремою транзакцією завдяки використанню унікальних одноразових параметрів r та TS.

Стійкість до MITM-атак забезпечується не лише математичними властивостями схеми Шнора, а й архітектурним рішенням щодо передачі публічного ключа окремим захищеним каналом. Це означає, що навіть при повній компрометації середовища виконання транзакції зловмисник не здатен сформувати коректний доказ без знання приватного ключа x. Дане спостереження має важливе практичне значення: воно вказує на можливість розгортання протоколу у відкритих або ненадійних мережах за умови одноразового захищеного обміну публічним ключем.

Механізм часових міток для протидії replay-атакам є типовим підходом у криптографічних протоколах, однак його ефективність залежить від синхронізації годинників між сторонами транзакції. У реальних умовах банківської системи це завдання вирішується засобами NTP-серверів, що є стандартною практикою. Важливо зазначити, що TS у запропонованій моделі є частиною підписаного доказу, тому його підміна зловмисником виявляється при перевірці, що робить цей механізм стійким навіть за часткової компрометації мережевого рівня.

Застосування протоколів ZKP вимагає додаткових обчислювальних ресурсів порівняно з традиційними підходами до ідентифікації. Однак у контексті фінансових транзакцій, де вартість компрометації суттєво перевищує вартість обчислень, такий обмін є виправданим. Запропонована модель демонструє, що навіть при додатковому обчислювальному навантаженні ключові властивості безпеки (цілісність, конфіденційність та ідентифікація) зберігаються у повному обсязі.

Таким чином, запропонований підхід є особливо доцільним у сценаріях з підвищеними вимогами до захисту персональних і фінансових даних, де важливим є не лише підтвердження ідентичності користувача, а й забезпечення того, що сам процес ідентифікації не стає джерелом витоку.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті дослідження було проаналізовано доцільність застосування схеми Шнора на основі протоколу доведення з нульовим розголошенням для забезпечення безпечної авторизації банківських транзакцій. Запропонований підхід забезпечує верифікацію автентичності клієнта без передачі приватного ключа, що принципово відрізняє його від традиційних методів автентифікації та забезпечує якісно вищий рівень захисту конфіденційних даних у середовищах із частковою довірою.

Змодельовано два ключові сценарії атак: атака типу MITM та replay-атака. У сценарії MITM показано, що будь-яке несанкціоноване втручання у значення параметра t спричиняє порушення перевірочного співвідношення на стороні банку, що унеможливлює успішну авторизацію транзакції. Це підтверджує математичну стійкість схеми Шнора до атак на цілісність даних. У сценарії replay-атаки продемонстровано, що інтеграція механізму часових міток (TS) ефективно запобігає повторному використанню перехоплених параметрів, оскільки застарілий доказ відхиляється банківською стороною під час перевірки актуальності транзакції.

Практична цінність запропонованого рішення полягає у можливості його застосування у банківських системах з мінімальними змінами до наявної інфраструктури. Використання стандартизованого протоколу Шнора (RFC 8235) гарантує сумісність з існуючими криптографічними бібліотеками та полегшує процес інтеграції. Разом з тим слід зазначити, що застосування ZKP-протоколів вимагає додаткових обчислювальних ресурсів порівняно з традиційними методами, що є компромісом між рівнем безпеки та ефективністю виконання транзакцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Internet Engineering Task Force (IETF). (2017). *Schnorr non-interactive zero-knowledge proof* (RFC 8235). https://datatracker.ietf.org/doc/html/rfc8235
2. Bellare, M., & Palacio, A. (2002). GQ and Schnorr identification schemes:Proofs of security against impersonation under active and concurrent attacks.In *Advances in cryptology – CRYPTO 2002* (Lecture Notes in Computer Science, Vol. 2442, pp. 162-177).Springer. https://doi.org/10.1007/3-540-45708-9_11
3. Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on Computing, 18*(1), 186-208. https://doi.org/10.1137/0218012
4. Pointcheval, D., & Stern, J. (2000). Security arguments for digital signatures and blind signatures. *Journal of Cryptology, 13*(3), 361-396. https://doi.org/10.1007/s001450010003
5. Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. *IEEE Communications Surveys & Tutorials, 18*(3), 2027-2051. https://doi.org/10.1109/COMST.2016.2548426
6. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 459-474). IEEE. https://doi.org/10.1109/SP.2014.36

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Viktoriia Shlapak
A student of the Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0009-0185-7632
viktoriia.shlapak.kb.2022@lpnu.ua

Serhiy Semenyuk
PhD, Associate Professor of the Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-8143-5887
serhii.a.semenyuk@lpnu.ua

SECURE AUTHORIZATION OF BANKING TRANSACTIONS BASED ON THE SCHNORR SCHEME

Abstract. The method of secure authorization of banking transaction based on the Schnorr scheme represents a cryptographic approach to verifying user authenticity using Zero-Knowledge Proof (ZKP) protocols. The proposed approach is focused at minimizing the risks of compromising confidential data during the execution of transaction in open or partially trusted environments. The method is based on the Schnorr identification protocol, which relies on the computational hardness of the discrete logarithm problem and enables authentication without transmitting the user's secret key. The authorization model includes the interaction process between three components of the transaction, namely the client, the transaction execution environment, and the banking side. The transaction execution environment is considered to be critical and untrusted component. The protocol consists of a sequence of stages: first, the initial parameters (p, g) are generated; then the public key value (y) is formed; based on it, a proof value (t) is created; on the bank`s side, a challenge (e) is generated followed by the computation of the parameter *s*, and subsequently the correctness of the verification relation is checked by the bank. A distinctive feature of the approach is the absence of private key transmission and the use of random values, which prevents the recovery of secret parameters even if part of the data is intercepted. Within the scope of the study, simulations of Man-in-the-Middle (MITM) and replay attacks were performed in older to evaluate the robustness of the proposed approach. In the case of a Man-in-the-Middle attack, it is shown that modification of the parameter *t* leads to a violation of the verification relation, making successful transaction authorization impossible. To counter replay attacks, a timestamp (TS) mechanism and transaction parameter uniqueness were integrated into the model, eliminating the possibility of reusing intercepted data. The constructed model is based on cryptographic strength, reduction of the impact of vulnerabilities in the transaction execution environment, and ensuring the fundamental principles of digital security, namely data integrity, confidentiality, and authenticity. The proposed method demonstrates its effectiveness in scenario with a high level of threats, such as in the financial sector, where transaction protection is a critical component.

Keywords: banking transaction, Schnorr scheme, zero-knowledge proof, Man-in-the-Middle attack, replay attack.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Internet Engineering Task Force (IETF). (2017). *Schnorr non-interactive zero-knowledge proof* (RFC 8235). https://datatracker.ietf.org/doc/html/rfc8235
2. Bellare, M., & Palacio, A. (2002). GQ and Schnorr identification schemes:Proofs of security against impersonation under active and concurrent attacks.In *Advances in cryptology – CRYPTO 2002* (Lecture Notes in Computer Science, Vol. 2442, pp. 162-177).Springer. https://doi.org/10.1007/3-540-45708-9_11
3. Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, *18*(1), 186-208. https://doi.org/10.1137/0218012
4. Pointcheval, D., & Stern, J. (2000). Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, *13*(3), 361-396. https://doi.org/10.1007/s001450010003

5. Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. *IEEE Communications Surveys & Tutorials, 18*(3), 2027-2051. https://doi.org/10.1109/COMST.2016.2548426
6. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 459-474). IEEE. https://doi.org/10.1109/SP.2014.36

Отримано редакцією журналу / Received: 02.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 25.06.26