УДК 004.056.55

В. Р. Караван

Ю. В. Баришев

ЗАХИСТ ПРИВАТНИХ ПОВІДОМЛЕНЬ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА ПСЕВДОНЕДЕТЕРМІНОВАНОГО ШИФРУВАННЯ

Вінницький національний технічний університет

Анотація

Проаналізовано відомі систем обміну повідомленнями та спроектовано структуру власної системи захисту обміну повідомленнями на основі технології смарт-контрактів із застосуванням методу псевдонедетермінованого шифрування. Смарт-контракт розгорнуто у блокчейні Ethereum.

Ключові слова: шифрування, потокові шифри, криптографія, блокчейн, смарт-контракти.

Abstract

The analysis of known messaging systems was performed and designed the structure of own secure messaging system based on smart-contract technology using the pseudonondeterministic ciphering method. Smart contract is deployed in the Ethereum blockchain.

Keywords: ciphering, stream ciphers, cryptography, blockchain, smart-contracts.

Вступ

Використовуючи електронне спілкування, потрібно бути готовим до певних загроз. Це може бути, наприклад, перехоплення повідомлень, зміна їх вмісту, обмеження доступу до сервісу обміну повідомленнями тощо. Для вирішення даних задач пропонується використати технологію смарт-контрактів, що розгортаються у блокчейні. Вона дозволить прослідковувати створення, зміну та видалення даних, що роблять користувачі. Але дані у блокчейні зберігаються у відкритому вигляді, що дозволить будь-кому прочитати їх. Для вирішення цієї проблеми, а також загрози перехоплення повідомлень, пропонується застосувати шифрування.

Метою дослідження є підвищення захисту систем обміну повідомленнями. Для її досягненнях[1]:

- проаналізовано відомі системи обміну повідомленнями;
- розроблено підхід до реалізації захищеного обміну;
- розроблено структуру пристрою, що реалізує підхід.

Аналіз відомих систем обміну повідомленнями

Найбільш поширеним методом листування є електронна пошта. Перехоплення поштового трафіку

можна здійснювати двома способами. Перший – інтеграція контролюючого модуля в програмне забезпечення поштового сервера. Цей спосіб дозволяє гарантовано перевіряти всі листи, що проходять через сервер, а також заблокувати або затримати відсилання листа. Другий спосіб контролю за поштою – автономний моніторинг поштового трафіку. При цьому контролюється абсолютно весь поштовий трафік, в тому числі і листи, відправлені на чужі поштові сервери [2]. За останні декілька років, особливої популярності набули месенджери. Значна частина застосунків для листування безпосередньо належить корпораціям, які хочуть зібрати якомога більше даних про користувачів. Крім того, традиційна модель месенджерів передбачає централізацію, що дозволяє обмежувати кінцевих користувачів у доступі до інструменту комунікації [3].

Як видно з результатів дослідження, всі відомі системи обміну повідомленнями мають низку загроз, які можуть призвести до розкриття вмісту повідомлень користувачів стороннім особам. Відповідно актуально розробити нову систему, яка усуне вищезазначені недоліки.

Система захисту обміну повідомленнями

Система захисту обміну повідомленнями буде реалізована за допомогою технології смарт-контрактів. Розумні контракти найкраще працюють на базі проекту Ethereum [4]. Але оскільки дані у блокчейні зберігають у відкритому вигляді, має сенс шифрування, яке буде застосоване до даних перед тим, як вони записуватимуться до блокчейну. Але всі сучасні шифри в повній або частковій мірі вже були зламані зловмисниками, а також потребують суттєвої алгоритмічної складності для реалізації, що у випадку смарт-контракту – збільшуватиме вартість користування, тому доцільно забезпечити захист за рахунок псевдонедетермінованого потокового шифрування, розглянутого у [5].

Ідея шифру полягає у реалізації концепції псевдонедетермінованої криптографії [6, 7]. Зокрема це втілиться у використанні різних операцій для накладання гами. Запропонований метод реалізований на базі шести регістрів зсуву з лінійним зворотним зв'язком. РЗЛЗЗ 1_1 та 1_2 використовуються для визначення стану РЗЛЗЗ 2_1 та 2_2, які є входами мультиплексора. РЗЛЗЗ Select, в свою чергу, керує даними входами. А РЗЛЗЗ Operation використовується в процесі накладання гами. Тобто він визначає який операційний пристрій буде застосовано: XOR або інверсний XOR [5]. На виході отримується послідовність бітів, які, в свою чергу, формують шифротекст. Структуру пристрою, що реалізує даний підхід наведено на рисунку 1.

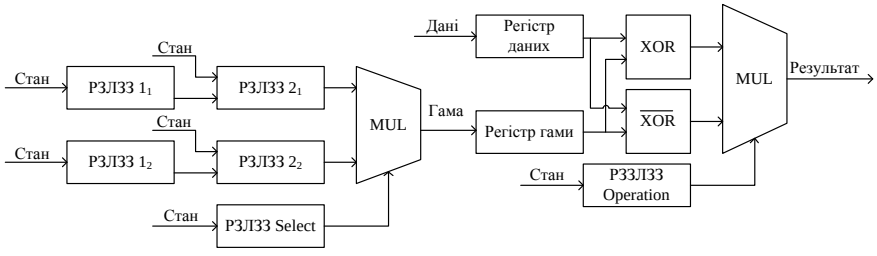

Рисунок 1 – Схема пристрою шифрування

Стійкість запропонованого шифру полягає у тому, що зловмисник не може дослідити характер гами, а також не знає, яка з вбудованих операцій була виконана.

Висновки

Аналіз показав необхідність захисту сучасних систем обміну повідомленнями. Необхідність полягає в запобіганні таких основних загроз, як перехоплення повідомлень та зміна їх вмісту. Для вирішення проблеми перехоплення було використано власний алгоритм псевдонедетермінованого потокового шифрування, так як більшість сучасних рішень вже давно були досліджені та зламані зловмисниками. Для вирішення проблеми зміни вмісту повідомлення, систему обміну було реалізовано на основі технології смарт-контрактів у блокчейні Ethereum.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азарова, А. О., Карпінець, В. В. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 – «Менеджмент» та 6.170103 – «Управління інформаційною безпекою» Вінниця, 2013. 44 с.
2. Перехват электронной почты URL: http://www.comprice.ru/articles/detail.php?ID=40699 (дата звернення: 04.02.2019).
3. Безопасность мессенджеров URL: https://habr.com/post/413695/ (дата звернення: 04.02.2019).
4. Ethereum : URL: https://ethereum.org/ (дата звернення: 02.02.2019).
5. Караван В. Р. Метод псевдонедетермінованого шифрування. *XLVII Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії*, 2018. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2018/paper/view/5172/4543 (дата звернення: 04.02.2019).
6. Luzhetsky V., Baryshev Y. The Generalized Construction of pseudonondeterministic hashing. *Computing*, 2012, Vol. 11 (Issue 3), P. 302-308.
7. Лужецький В. А., Баришев Ю. В. Концепція псевдонедетермінованого хешування. *Системи управління, навігації та зв'язку*, 2010, №3, С. 94-98.

Караван Владислав Русланович — студент, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: vlad30.96.12@gmail.com

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, email: yuriy.baryshev@gmail.com

Karavan Vladislav — student, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vlad30.96.12@gmail.com

Baryshev Yurii — Cand. Sc. (Eng), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, yuriy.baryshev@gmail.com