помилкових сповіщень може зменшитися приблизно на 60%, а розслідування інцидентів може стати приблизно на 40% швидшим [5]. Але варто підкреслити, що ці числа треба сприймати обережно, бо вони взяті з вторинних джерел, а не з контрольованого експерименту.

Для оцінювання таких систем доцільно не обмежуватися ROC-AUC. У безпекових даних шкідливий трафік часто становить менше ніж 0,1% від усього трафіку, тому ROC-AUC може приховати велику кількість зайвих сповіщень. Криві Precision-Recall та показник Average Precision краще показують, скільки сповіщень справді є корисними [6]. Для систем реального часу пропонується Numenta Anomaly Benchmark, бо він враховує, наскільки рано система помітила аномалію [7].

Висновки. У дослідженні запропоновано гібридну модель захисту вебзастосунків з двома шарами. Foundation дає базовий і зрозумілий захист за OWASP Top 10:2025, а Amplifier підсилює його трьома методами ШІ: HTTP2vec, графовими нейронними мережами та Kitsune. Головна ідея моделі проста: ШІ не замінює традиційний захист, а робить його сильнішим. Подальша робота має включати перевірку моделі в контрольованому середовищі, створення кращих відкритих наборів даних, навчання моделей без передавання чутливого трафіку та тестування стійкості ШІ до навмисного обходу.

1. OWASP Foundation. OWASP Top 10:2025. 2025. URL: https://owasp.org/Top10/2025/
2. Gniewkowski M. et al. HTTP2vec: Embedding of HTTP requests for detection of anomalous traffic. arXiv, 2021.
3. Bilot T., Legay A., Rønne P. B. Graph neural networks for intrusion detection: A survey // IEEE Access. 2023. Vol. 11. P. 45589-45612.
4. Mirsky Y. et al. Kitsune: An ensemble of autoencoders for online network intrusion detection // Proc. NDSS 2018.
5. Dilmegani C. Top 13 AI cybersecurity use cases with real examples in 2025. AIMultiple Research. 2025.
6. Saito T., Rehmsmeier M. The Precision-Recall plot is more informative than the ROC plot // PLOS ONE. 2015. Vol. 10(3). e0118432.
7. Lavin A., Ahmad S. Evaluating real-time anomaly detection algorithms - the Numenta Anomaly Benchmark // IEEE ICMLA. 2015. P. 38-44.

Fast squaring of multiword numbers using Mersenne modules

UDK 519.67

Andrii Tereshchenko[1], Valeriy Zadiraka[2]

V.M. Glushkov Institute of Cybernetics, [1]teramidi@ukr.net, [2]zvk140@ukr.net

In the era of post-quantum computing, it is necessary to increase the length of keys to increase cryptographic strength, which affects the performance of hardware-software cryptographic complexes. The performance of such complexes depends to a greater extent on the performance of the square operation [1] by modulus.

The multiword operation of squaring by Mersenne modulus is considered, which is one of the steps of the algorithm for implementing the multiword operation of

squaring based on the Mersenne transform. The operation of squaring by Mersenne modulus is performed element by element for each value of the result of the calculation of the direct Mersenne transform similarly to the Schönhage-Strassen algorithm [2].

A new algorithm for multiplication modulo a Mersenne prime is considered based on two half-length multiplications, instead of three multiplications, as in the Karatsuba method [3].

Lemma 1. The operation of squaring $\left\langle A^2 \right\rangle_{M_p}$ a number $A = A_1 \cdot 2^{p_0} + A_0$ of length p bits modulo a Mersenne prime $M_p = 2^p - 1$ can be implemented based on two operations of multiplication of numbers of length $p_0 = (p+1)/2$ and $p_1 = p_0 - 1$ bits.

Proof. The square of a number modulo $\left\langle A^2 \right\rangle_{M_p}$ can be represented in the form $\left\langle (A_1 \cdot 2^{p_0} + A_0)^2 \right\rangle_{M_p} = \left\langle A_1^2 \cdot 2^{2p_0} + 2 \cdot A_1 \cdot A_0 \cdot 2^{p_0} + A_0^2 \right\rangle_{M_p}$. Given that $\left\langle 2^{2p_0} \right\rangle_{M_p} = \left\langle 2^{p+1} \right\rangle_{M_p} = 2,$ the previous expression can be written in the form $\left\langle A^2 \right\rangle_{M_p} = \left\langle A_1^2 \cdot 2^{2p_0} + 2 \cdot A_1 \cdot A_0 \cdot 2^{p_0} + A_0^2 \right\rangle_{M_p}$. Let's add $3 \cdot A_1 \cdot A_0 - 3 \cdot A_1 \cdot A_0$ to the expression and get:

$$\left\langle A^2 \right\rangle_{M_p} = \left\langle A_1^2 \cdot 2^{2p_0} + 2 \cdot A_1 \cdot A_0 \cdot 2^{p_0} + A_0^2 + 3 \cdot A_1 \cdot A_0 - 3 \cdot A_1 \cdot A_0 \right\rangle_{M_p}.$$

We will use $M_0 = (2 \cdot A_1 + A_0) \cdot (A_1 + A_0),\ M_1 = A_1 \cdot A_0$ for replacement and get finally $\left\langle A^2 \right\rangle_{M_p} = \left\langle M_0 + 2 \cdot M_1 \cdot 2^{p_0} - 3 \cdot M_1 \right\rangle_{M_p}$.

Multiplications by 2 and 3 are not considered, as they can be replaced by addition operations. Multiplication by 2^{p_0} can be replaced by a bitwise cyclic shift to the left (towards the most significant bits).

The lemma is proven.

Similarly, it can be shown that in the case of dividing a multiword number into three sections, squaring modulo a Mersenne number can be performed based on three squaring operations and two multiplication operations of numbers of lengths that are a third of the original length of the number.

Lemma 2. The operation of squaring $\left\langle A^2 \right\rangle_{M_p}$ a number $A = A_2 \cdot 2^{p_1 + p_0} + A_1 \cdot 2^{p_0} + A_0$ of length p bits modulo a Mersenne number $M_p = 2^p - 1$ can be implemented based on three operations of squaring and two

operations of multiplying numbers of length $p_0 = p_1 = (p+1)/3$ and $p_2 = p_0 - 1$ bits.

$$\left\langle A^2 \right\rangle_{M_p} = \left\langle R_2 \cdot 2^{p_0+p_1} + R_1 \cdot 2^{p_0} + R_0 \right\rangle_{M_p}, \text{ where}$$

$$M_0 = (A_0 + (A_1 + A_2))^2, \quad R_0 = \frac{M_0 + M_1}{2} - M_2,$$
$$M_1 = (A_0 - (A_1 + A_2))^2,$$
$$M_2 = (A_1 - A_2)^2, \quad R_1 = \frac{M_0 - M_1}{2} - M_3,$$
$$M_3 = 2 \cdot (A_0 - A_2) \cdot A_2, \quad R_2 = \frac{M_0 - M_1}{2} - M_4.$$
$$M_3 = (2 \cdot A_0 - A_1) \cdot A_1.$$

For verification:

$$R_0 = (A_0)^2 + 4 \cdot A_1 \cdot A_2,$$
$$R_1 = 2 \cdot (A_2)^2 + 2 \cdot A_0 \cdot A_1,$$
$$R_2 = (A_1)^2 + 2 \cdot A_0 \cdot A_2.$$

Similarly to Lemma 1, multiplication and division by 2, multiplication by 2^{p_0} and $2^{p_0+p_1}$ can be disregarded in the total number of multiplication operations.

The algorithm for squaring a Mersenne number modulo by dividing the number into two sections (Lemma 1) is 33% more efficient than the Karatsuba method. The algorithm for squaring a Mersenne number modulo by dividing the number into three sections (Lemma 2) allows us to calculate the squaring operation by using three smaller-length squaring operations out of the five required multiplication operations. Squaring smaller-length numbers based on the fast Fourier transform is one of the reserves for optimizing the implementation of the multiword multiplication operation.

1. Zadiraka, V.K., Tereshchenko, A.M. An Efficient Algorithm for Squaring Multi–Word Numbers. *Cybern Syst Anal*, 61, 521-526 (2025).
2. Schönhage A., Strassen V. Schnelle Multiplikation großer Zahlen. *Computing*. – 1971. – № 7. – P. 281–292.
3. Karatsuba, A. A.; Ofman, Y. P. (1962). Multiplication of Many-Digital Numbers by Automatic Computers. Proceedings of the USSR Academy of Sciences (in Russian). 145: 293–294.

Система виявлення інформаційно-фінансових атак на криптовалютних ринках із застосуванням показника поглинання імпульсу

УДК 004.056.5:004.42:336.74

Ігор Цапро[1], Оксана Золотухіна[2]

Державний університет інформаційно-комунікаційних технологій,
[1]tsapro.ihor.work@gmail.com, [2]o.zolotukhina@duikt.edu.ua

Постановка проблеми. Стрімкий розвиток цифрових фінансових платформ, криптовалютних бірж та децентралізованих фінансових сервісів супроводжується збільшенням кількості кіберфінансових загроз, серед яких особливу небезпеку становлять координовані інформаційно-фінансові атаки: алгоритмічні маніпуляції ліквідністю, spoofing, wash trading та приховане накопичення позицій великими учасниками ринку [1]. Особливість таких атак