МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ
(зимовий форум)

Одеса, Україна, 14 листопада 2025 р.

Одеса
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL UNIVERSITY

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025)

Odesa, Ukraine, November 14, 2025

Conference Proceedings
(winter forum)

Odesa
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025)

Одеса, Україна, 14 листопада 2025 р.

Матеріали конференції
(зимовий форум)

Одеса
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings (winter forum). Odesa : International university, 2025, 101 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції (зимовий форум). Одеса : Міжнародний університет, 2025, 101 с.

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.
ЙОНА Л.Г. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.
ПЕДЯШ В.В. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КУЧАЙ О.В. - д.п.н., проф., Національний університет біоресурсів і природокористування України.
ЖИГУЛІН О.А. – д.е.н., проф., Міжнародний університет, Одеса, Україна
ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

ЗМІСТ

4. UKR.NET. Система електронних платежів НБУ обробила 483 млн операцій за рік: які платежі найпопулярніші. – Режим доступу: https://www.ukr.net/news/details/economics/109008745.html (дата звернення: 06.11.2025).

5. Академічні візії. Стан і тенденції розвитку ринку електронних платежів в Україні. – Режим доступу: https://academy-vision.org/index.php/av/article/download/1799/1666/1706 (дата звернення: 06.11.2025).

UDC 004.056.55

Onatskyi Oleksii,
Candidate of technical sciences, associate professor,
International Humanitarian University, Odessa, Ukraine
onatsky@meta.ua
Zharova Oksana,
Candidate of physical and mathematical sciences, associate professor,
Odessa polytechnic state university, Odessa, Ukraine
Ksenia.gds@gmail.com

COMPARATIVE ANALYSIS OF HOMOMORPHIC PROPERTIES OF ASYMMETRIC CRYPTOSYSTEMS RSA AND PAILLIER

Abstract. *This study conducts a comparative analysis of homomorphic properties in RSA and Paillier cryptosystems. With growing demands for secure cloud computing and IoT applications, homomorphic encryption enables operations on encrypted data without decryption. The research implements both systems in Python, analyzing their mathematical foundations and performance. Results show RSA multiplicative homomorphism poses security risks, while Paillier additive homomorphism, though computationally heavier, provides secure privacy-preserving operations. Paillier excels in electronic voting and secure data analytics, whereas RSA remains optimal for traditional encryption. The findings guide cryptosystem selection based on specific security and functionality requirements in modern applications.*

Modern requirements for data processing, particularly in cloud computing schemes, Internet of Things, and secure voting systems, highlight the problem of information confidentiality. Classical cryptosystems require data decryption to perform any operations on them, which creates risks of data leakage. The solution to this problem is homomorphic encryption – a class of cryptographic schemes that allows performing mathematical operations on ciphertexts, obtaining a result that, after decryption, corresponds to the result of the same operations performed on plaintexts. The RSA cryptosystem, although not designed as fully homomorphic, demonstrates homomorphic properties regarding the multiplication operation. In contrast, the Paillier cryptosystem was specifically designed with powerful homomorphic properties regarding addition, making it a key tool for many practical applications. Thus, the relevance of the research lies in comparing the classical RSA cryptosystem and the homomorphic Paillier cryptosystem to determine their advantages, disadvantages, and possible directions of practical application. To conduct a comparative analysis of the functioning algorithms and implementation features of RSA and Paillier cryptosystems, mathematical foundations, areas of effective application and computational complexity, as well as comparing their characteristics from the perspective of security, efficiency, and homomorphic encryption capabilities.

The RSA cryptosystem was developed in 1977 by R. Rivest, A. Shamir, and L. Adleman [1, 2]. It is based on a one-way function – the product of two large prime numbers, whose factorization is a computationally complex task. For the RSA algorithm $\left[E(m_1)E(m_2)\right] \bmod n = E(m_1 m_2) \bmod n$, which demonstrates multiplicative homomorphism, where $E(m_1)$ and $E(m_2)$ – ciphertexts of two messages.

The Paillier cryptosystem, proposed by Pascal Paillier in 1999 [3, 4], is based on the complexity of computing the *n*-residue function modulo n^2. It is distinguished by a unique property – additive homomorphism, which means the ability to perform addition operations on encrypted data without their decryption. For the Paillier algorithm

$$\left[E(m_1)E(m_2)\right] \bmod n^2 = E(m_1 + m_2) \bmod n^2,\ E(m_1)^k \bmod n^2 = E(k\,m_1) \bmod n^2,$$

which demonstrates additive homomorphism.

The research used methods of theoretical analysis and mathematical modeling. To practically confirm the properties of RSA and Paillier algorithms, tools of the Python programming environment were applied, particularly the SymPy library (a library for symbolic mathematical computations in Python). Models of key generation, message encryption and decryption processes were implemented, and the homomorphism of RSA and Paillier cryptosystems was verified. The comparison was carried out according to the following criteria: length of cryptographic keys; execution time of encryption/decryption operations; support of homomorphic properties. RSA and Paillier algorithms include three main stages: key generation, encryption, and decryption [1, 2].

The result of executing the program code is shown in Fig. 1 – 5.

```
================================================================================================
         COMPARATIVE ANALYSIS OF RSA AND PAILLIER CRYPTOSYSTEMS
================================================================================================
1. DATA INPUT:
------------------------------------------------------------------------------------------------
Choose input data type (1 - numbers, 2 - text): 1
Enter first number: 23
Enter second number: 61
Enter key length (bits) [512]: 100

2. KEY GENERATION:
------------------------------------------------------------------------------------------------
RSA Keys:
  Public key  (e, n): (65537, 27014142956232615339005549221171725665041592692410806475022 9)
  Private key (d, n): (834203923200994353160496063499770843386971402295122451438 73,
                       27014142956232615339005549221171725665041592692410806475022 9)
  Private key  (hex): d=D4A2588B1F92347E1306DA5A1967A6899987014E1C2E9E941

Paillier Keys:
  Public key  (n, g): (396715656050536708961692760932240264459811676959572130477 3,
                       396715656050536708961692760932240264459811676959572130477 4)

  Private key (lambda, mu, n): (396715656050536708961692760820239570730132880202535507408 0,
                                322314338574677341862113083927991935756671663459037375237 6,
                                396715656050536708961692760932240264459811676959572130477 3)
  Private key (hex): lambda=A1CB0C0DE8896998F378C1BE620350B6386843A9522BDA20
                     mu=83732FE5A134A47B0702C92166412F7A3CDF718A0C342E38
```

Figure 1 – Data input. Key generation for RSA and Paillier cryptosystems

```
3. ENCRYPTION:
--------------------------------------------------------------------------------------------------------------------------------
RSA Encryption (numbers):
  23 -> 23528604538132694558777972856237631012776062230234317743046 3
  23 (hex) -> 257BB4EEDF531559E60EA5D99C6DB483DC4CEDEA47B43BE5BF
  61 -> 60118280450905581787621741506285336529404368764732344974376
  61 (hex) -> 993D0226BACD536BF61EE93319EB9E82CDC3AE0ED478D3C28
  Encryption time: 0.98 ms, 0.86 ms

Paillier Encryption (numbers):
  23 -> 689538271885994908640018964742325375730079051093853378951245267848297084087984295120735052980531157901874159134829
  Random r for 23: 366639550376363308255788490635923281439576145978178842480
  Random r (hex): EF3E54066E4753B8265ABC5B7F100A254CD4DE9CD3AAF70
  61 -> 14366884597946863884553412288404164048237776602422903238666244388382242653257796932282030553936891457107183687513690
  Random r for 61: 13819614842304427948487875976888703415114503451130530868 1
  Random r (hex): 5A2D5C9E01A20451474195F7E04D96B5CFC0BFE82C27A09
  Encryption time: 34.65 ms, 34.38 ms
```

Figure 2 – Encryption for RSA and Paillier cryptosystems

```
4. DECRYPTION:
--------------------------------------------------------------------------------------------------------------------------------
RSA Decryption (numbers):
  23528604538132694558777972856237631012776062230234317743046 3 -> 23
  257BB4EEDF531559E60EA5D99C6DB483DC4CEDEA47B43BE5BF -> 23
  60118280450905581787621741506285336529404368764732344974376 -> 61
  993D0226BACD536BF61EE93319EB9E82CDC3AE0ED478D3C28 -> 61
  Decryption time: 18.96 ms, 18.77 ms

Paillier Decryption (numbers):
  689538271885994908640018964742325375730079051093853378951245267848297084087984295120735052980531157901874159134829 -> 23
  14366884597946863884553412288404164048237776602422903238666244388382242653257796932282030553936891457107183687513690 -> 61
  Decryption time: 33.88 ms, 33.49 ms
```

Figure 3 – Decryption for RSA and Paillier cryptosystems

```
5. HOMOMORPHIC OPERATIONS:
--------------------------------------------------------------------------------------------------------------------------------
RSA Homomorphic Multiplication:
  Enc(23) * Enc(61) = Enc(1403)
  Result ciphertext: 11957331675345133245529837276036806453223004797413637 1499570
  Result ciphertext (hex): 130C93AD498C88BF80D11C52B5FE1B94610ABA57DFD52C5232
  Decrypted result: 1403
  Expected result: 1403
  Validation: ✅

Paillier Homomorphic Addition:
  Enc(23) + Enc(61) = Enc(84)
  Result ciphertext: 654576960331059033737808714752134674381841175918416665633467911425353165329474741625108675308475476657787779227460 0
  Decrypted result: 84
  Expected result: 84
  Validation: ✅

Paillier Homomorphic Multiplication by Constant (3):
  3 * Enc(23) = Enc(69)
  Result ciphertext: 17961821872494793541805248670643971922344699476899913870776638341085624747320997105066462062237617161142920764708 34
  Decrypted result: 69
  Expected result: 69
  Validation: ✅

6. BENCHMARKING (100 iterations):
--------------------------------------------------------------------------------------------------------------------------------
  RSA Encryption: 0.80 ms
  RSA Decryption: 19.93 ms
  Paillier Encryption: 49.77 ms
  Paillier Decryption: 33.74 ms

  Fastest operation: RSA Encryption (0.80 ms)

  Speed ratio: Paillier ≈ 62.0 times slower than RSA
```

Figure 4 – Homomorphic operations for RSA and Paillier cryptosystems

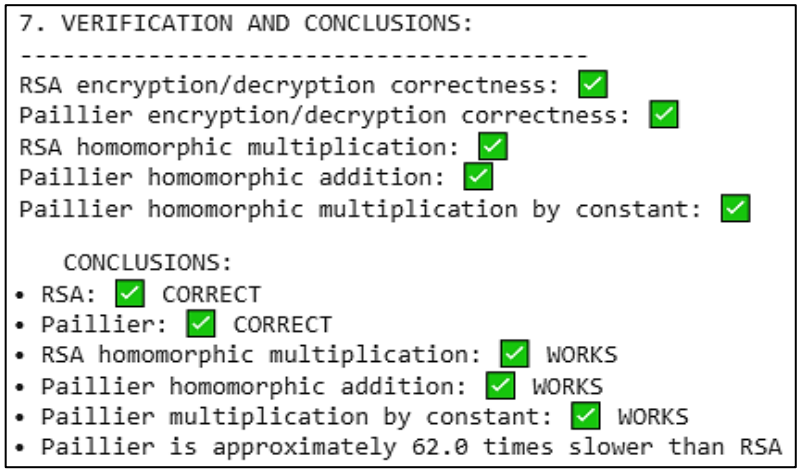

Figure 5 – Verification and conclusions for RSA and Paillier cryptosystems

Homomorphic properties. The RSA cryptosystem demonstrates multiplicative homomorphism. However, this property makes it vulnerable to chosen-ciphertext attacks, which requires special padding schemes (for example, OAEP – Optimal Asymmetric Encryption Padding) for practical use, which, in turn, destroy homomorphism. Thus, it is not suitable for performing operations on encrypted data. The Paillier cryptosystem possesses additive homomorphism, which is secure and intentionally built into the system design, but requires more memory and time to perform operations.

Mathematical foundations. RSA security is based on the complexity of solving the factorization problem of large numbers. Paillier security is based on the complexity of solving the decisional composite residuosity problem modulo n^2, which is considered more complex.

Computational complexity. Encryption and decryption operations in Paillier are more computationally complex due to working with modulus n^2, while RSA uses modulus n.

Areas of application. Due to its additive homomorphism, the Paillier system has found wide application in:

– electronic voting (vote counting without decryption);

– secure cloud computing (finding data sums);

– machine learning with privacy preservation (calculating averages, sums of squares, etc.);

– secure medical research;

– electronic payment order systems.

The multiplicative homomorphism of RSA has more limited applications, for example, for building blind signature protocols.

Conclusions. The conducted comparative analysis leads to the conclusion that although both RSA and Paillier, have homomorphic properties, they are fundamentally different in their nature and practical value. The RSA cryptosystem, being the first widely known asymmetric system, has limited and potentially dangerous multiplicative homomorphism. The RSA cryptosystem remains one of the most reliable and widespread asymmetric encryption algorithms, which is effectively used for data protection and implementation of digital signatures. In contrast, the Paillier cryptosystem is a specialized and secure tool that implements additive homomorphism, making it indispensable for modern applications where operations need to be performed on encrypted data without their disclosure. Consequently, the selection of an appropriate cryptosystem is contingent upon the specific requirements of the intended application: RSA remains the standard for ensuring confidentiality and authentication, while Paillier is the optimal choice for implementing homomorphic computations, particularly for addition, which is important in tasks of analyzing confidential data in cloud environments, electronic voting, financial services, and user privacy protection. Further research should be directed towards optimizing homomorphic algorithms, reducing their computational complexity and integration with post-quantum protection methods, opening new opportunities for creating secure, efficient, and confidential information technologies of the future.

References:

1. Онацький О. В., Йона Л. Г. Белова Ю. В. Криптографічний захист інформації: навчальний посібник з дисципліни «Криптографічний захист інформації». Держ. ун-т інтелект. технологій і зв'язку. – Одеса: Астропринт, 2023. 252 с.

2. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика: монографія. – Харків: Видавництво «Форт», 2012. 880 с.

3. Paillier P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes // Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol. (EUROCRYPT), Prague. Czech Republic, May 1999, Pp. 223-238.

4. The Paillier's Cryptosystem and Some Variants. [Electronic resource] – Mode of access: https://scispace.com/pdf/the-paillier-s-cryptosystem-and-some-variants-revisited-186lebbhcg.pdf

Ковальчук Д. А.
здобувач вищої освіти третього (освітньо-наукового рівня)
спеціальності 125 Кібербезпека
denys.kovalchuk1@gmail.com
Науковий керівник: Йона Л. Г.
Кандидат технічних наук,
Доцент кафедри Комп'ютерної інженерії та інноваційних технологій
Міжнародного університету м. Одеса, Україна

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК СКЛАДОВА ГІБРИДНИХ КІБЕРОПЕРАЦІЙ: СУЧАСНІ ТЕНДЕНЦІЇ ТА ВИКЛИКИ БЕЗПЕКИ

***Анотація**. У тезах розглянуто соціальну інженерію як один із ключових інструментів гібридних кібероперацій, що поєднує технічні та психологічні засоби впливу. Проаналізовано сучасні тенденції розвитку соціально-інженерних методів, їх роль у дестабілізації інформаційного простору та підриві довіри до цифрових систем. Визначено основні канали поширення таких атак, а також виклики, що постають перед системами кібербезпеки держави, бізнесу та суспільства. Запропоновано напрями підвищення рівня кіберстійкості та соціальної відповідальності користувачів.*

Вступ

Сучасні гібридні конфлікти характеризуються поєднанням традиційних та кіберінструментів впливу, серед яких соціальна інженерія посідає особливе місце. На відміну від класичних технічних атак, соціально-інженерні операції спрямовані на маніпулювання людською поведінкою, емоціями та когнітивними особливостями. Це робить їх надзвичайно ефективними, адже навіть найзахищеніші інформаційні системи залишаються вразливими через «людський фактор».

В умовах війни, яку веде Російська Федерація проти України, соціальна інженерія використовується не лише для викрадення даних чи фінансових ресурсів, але й як засіб інформаційно-психологічного тиску на населення, деморалізації та дезінформації. З огляду на це, дослідження соціальної інженерії як складової гібридних кібероперацій набуває стратегічного значення для національної безпеки.