UDC 004.056:004.774:621.9.048.5
DOI https://doi.org/10.32689/maup.it.2025.2.25

Inna ROZLOMII
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Information Security and Computer Engineering,
Cherkasy State Technological University, inna-roz@ukr.net
***ORCID:** 0000-0001-5065-9004*

Serhii NAUMENKO
Lecturer at the Department of Information Technologies,
Bohdan Khmelnytsky National University of Cherkasy, naumenko.serhii1122@vu.cdu.edu.ua
***ORCID:** 0000-0002-6337-1605*

Volodymyr SYMONYUK
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Automation and Computer-Integrated Technologies,
Lutsk National Technical University, v.symonyuk@lntu.edu.ua
***ORCID:** 0000-0002-7624-4760*

Vitalii PTASHENCHUK
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Automation and Computer-Integrated Technologies,
Lutsk National Technical University, v.ptashenchuk@lntu.edu.ua
***ORCID:** 0000-0003-1570-7570*

Vitalii ZAZHOMA
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Information Systems and Organization of Civil Protection Measures,
National University of Civil Protection of Ukraine, zazhoma_vitalii@nuczu.edu.ua
***ORCID:** 0000-0003-2083-2472*

SIMPLIFIED CRYPTOGRAPHY FOR SECURE VIBRATION PARAMETERS IN POST-PROCESSING OF 3D-PRINTED PARTS

***Abstract**. In modern manufacturing, 3D printing technologies are gaining increasing popularity due to their ability to rapidly create complex and customized parts. However, to achieve high quality and meet industrial standards, 3D-printed parts require post-processing. Vibration containers are widely used for grinding, polishing, and other processing methods, improving the appearance and mechanical properties of products. This highlights the need to protect data generated during the vibration process, which is transmitted to central servers for analysis and management.*

***The aim** of this study is to develop a framework for a secure post-processing system for 3D-printed parts, which includes an encryption module based on lightweight ciphers to protect vibration parameters and other operational data.*

***Methodology.** This article proposes the use of lightweight cryptography to ensure the security of vibration parameters in the post-processing of parts printed using 3D printing methods. Lightweight cryptography allows for efficient data encryption with minimal resource consumption, which is critical for systems with limited computational capabilities. The paper discusses various post-processing methods – such as mechanical grinding and polishing – and their impact on the surface quality and compliance with standards. The cryptographic protocols used to protect data during its transmission from vibration containers to central servers are described in detail.*

***The results** can contribute to the advancement of 3D printing technologies and the creation of new post-processing methods that meet contemporary requirements for quality and information security.*

***Scientific novelty.** The use of the SPECK cipher has proven to be the optimal solution for resource-constrained systems, as it provides high encryption speed with low energy consumption, which is critical for microcontrollers and embedded systems used in post-processing operations.*

***Conclusion.** The proposed solutions provide reliable protection against unauthorized access and manipulation, improving overall manufacturing security and efficiency. Special attention is given to the integration of cryptographic methods into monitoring and control systems for vibration processes, ensuring high accuracy and reliability in data processing.*

***Key words:** 3D printing, post-processing, vibration containers, lightweight cryptography, data encryption, mechanical grinding, polishing.*

Інна РОЗЛОМІЙ, Сергій НАУМЕНКО, Володимир СИМОНЮК, Віталій ПТАШЕНЧУК, Віталій ЗАЖОМА.

ПОЛЕГШЕНА КРИПТОГРАФІЯ ДЛЯ БЕЗПЕКИ ПАРАМЕТРІВ ВІБРАЦІЇ В ПОСТОБРОБЦІ 3D-ДРУКОВАНИХ ДЕТАЛЕЙ

Анотація. *У сучасному виробництві технології 3D-друку набувають все більшої популярності завдяки можливості швидкого створення складних та індивідуальних деталей. Однак, для досягнення високої якості та відповідності промисловим стандартам, 3D-друковані деталі потребують постобробки. Вібраційні контейнери широко використовуються для шліфування, полірування та інших методів обробки, покращуючи зовнішній вигляд і механічні властивості виробів. При цьому виникає потреба у захисті даних, які генеруються під час процесу вібрації та передаються на центральні сервери для аналізу та управління.*

Метою *цього дослідження є розробка структури захищеної системи постобробки деталей, надрукованих методом 3D-друку, яка включає модуль шифрування на основі полегшених шифрів для забезпечення захисту параметрів вібрації та інших операційних даних.*

Методологія. *У цій статті пропонується використання полегшеної криптографії для забезпечення безпеки параметрів вібрації в процесі постобробки деталей, надрукованих методом 3D-друку. Полегшена криптографія дозволяє ефективно шифрувати дані з мінімальними витратами ресурсів, що є критичним для систем з обмеженими обчислювальними можливостями. Розглядаються різні методи постобробки, включаючи механічне шліфування та полірування, а також їх вплив на якість поверхні та відповідність стандартам. Детально описуються криптографічні протоколи, які використовуються для захисту даних під час їх передачі від вібраційних контейнерів до центральних серверів.*

Результати *можуть бути використані для подальшого вдосконалення технологій 3D-друку та розробки нових методів постобробки, що відповідають сучасним вимогам до якості та інформаційної безпеки.*

Наукова новизна. *Використання шифру SPECK виявилося оптимальним рішенням для систем з обмеженими ресурсами, оскільки він забезпечує високу швидкість шифрування при низькому енергоспоживанні, що є критично важливим для мікроконтролерів та вбудованих систем, які використовуються в процесах постобробки.*

Висновки. *Запропоновані рішення забезпечують надійний захист від несанкціонованого доступу та маніпуляцій, підвищуючи загальну безпеку та ефективність виробничих процесів. Особлива увага приділяється інтеграції криптографічних методів у системи моніторингу та контролю вібраційних процесів, що дозволяє забезпечити високу точність та надійність обробки даних.*

Ключові слова: *3D-друк, постобробка, вібраційні контейнери, полегшена криптографія, шифрування даних, механічне шліфування, полірування.*

Introduction. A prominent trend in modern manufacturing is the implementation of technologies related to 3D printing, which enables the creation of parts with various levels of complexity at high speed and precision [5]. Additionally, 3D printing technology often requires an additional stage to produce of high-quality printed parts, known as post-processing [16].

An important aspect of the 3D printing process is post-processing, as it enhances the quality, appearance, and mechanical properties of printed parts [3, 5]. Different 3D printing technologies, such as stereolithography (SLA), fused deposition modeling (FDM), and selective laser sintering (SLS), require specialized post-processing methods to address various issues, such as layer lines, support marks, and rough surfaces. Resolving these issues enables printing parts that meet industry standards and achieve the desired functionality and aesthetics.

According to research [1], the 3D printing market continues to grow across various sectors. For example, in the medical field, 3D printing is actively used to create prosthetics, implants, and surgical instruments, contributing to its rapid growth. In the aerospace industry, 3D printing is used to produce complex and lightweight components, driving significant growth in this segment. The automotive industry utilizes 3D printing for prototyping and small-scale production of parts, allowing for a substantial reduction in production time and costs. Figure 1 shows a graph depicting the growth in the number of 3D-printed parts across various sectors, including aerospace, automotive, medical industries, and consumer goods, based on real data [1].

As shown, all sectors demonstrate significant growth in the number of manufactured parts, particularly in the automotive and medical industries. 3D printing is becoming increasingly popular due to its ability to create complex and customized parts [4, 18]. The quality and appearance of a 3D-printed object often depend on the technology and post-processing stages [7]. Post-processing technology not only improves the aesthetics of the printed part but can also enhance its mechanical properties according to technical requirements [9].

Post-processing plays an important role in ensuring that 3D-printed parts meet the necessary quality and aesthetic standards. For instance, the SLS 3D printing process may result in visible layer lines on the surface of a part, which can diminish its overall aesthetic quality. A rough surface texture is also a common issue with parts printed on a 3D printer. However, post-processing methods such as grinding, polishing, and painting can effectively eliminate or minimize these defects [7].

In industries such as aerospace, automotive, and medical, there are often strict regulations and standards regarding the quality, performance, and appearance of parts [9]. For example, manufacturers typically use ASME Y14.36 or ISO 21920-1 to specify surface texture. Post-processing technologies, such as grinding, polishing, smoothing, and coating, help ensure that 3D-printed parts comply with these standards, making them suitable and attractive for a variety of applications [6].

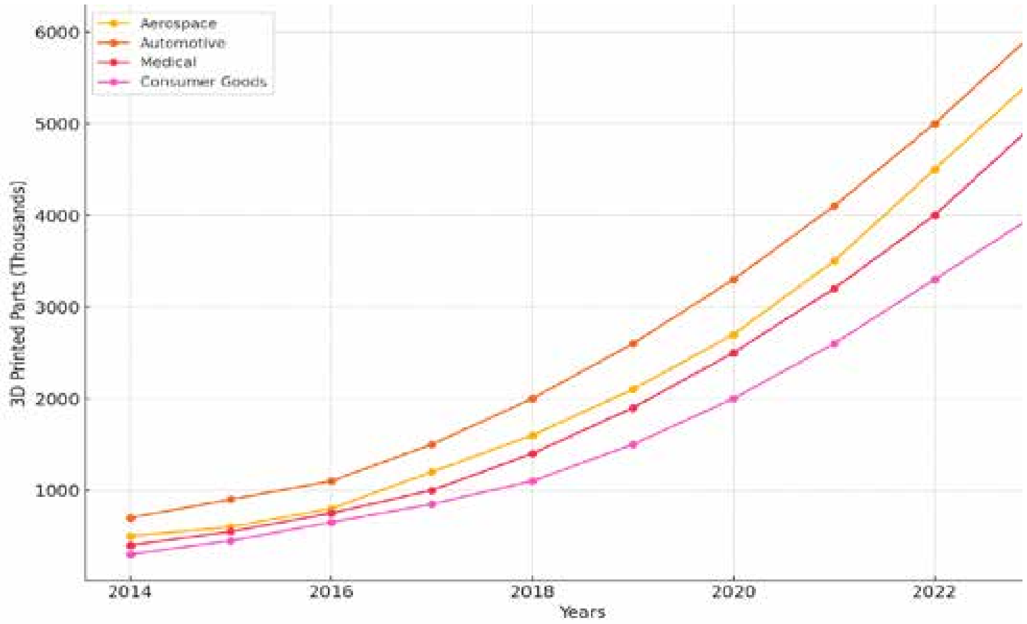

Fig. 1. Growth in the Number of 3D-Printed Parts Across Various Sectors

In addition to improving the quality and appearance of parts, protecting the information generated during the post-processing process is also crucial. Vibration parameters and other information should be encrypted before being transmitted to the central server for analysis and management. This ensures data security and prevents unauthorized access.

The aim of this study is to develop a framework for a secure post-processing system for 3D-printed parts, which includes an encryption module based on lightweight ciphers to protect vibration parameters and other operational data.

Related Works. The scientific community's interest in 3D printing technologies and post-processing methods for printed parts has significantly increased in recent years. In particular, several authors in their studies [6, 7] have analyzed various post-processing methods to improve the surface quality of 3D-printed parts, including grinding and polishing. They found that the application of mechanical grinding can significantly reduce surface roughness and enhance the overall aesthetics of the parts.

In the study [12], an analysis was conducted on the impact of different vibration modes on the quality of parts processed using abrasive vibration methods. The authors discovered that optimizing vibration parameters can greatly improve the efficiency of grinding and polishing.

The importance of cryptographic data protection in industrial applications is also a subject of research for many scientists. In [15], modern methods of lightweight cryptography that can be applied to protect information in IoT devices are discussed. The authors propose the use of efficient cryptographic protocols to protect transmitted data in resource-constrained systems. In [8], the application of cryptographic methods for data protection in industrial systems, including vibration technologies, is explored.

However, the integration of cryptographic methods into the post-processing of 3D-printed parts, particularly the protection of vibration parameters during grinding and polishing, remains underexplored. An important aspect is the development of effective methods for encrypting data generated by vibration containers and transmitting it to central servers for further analysis and management. This would ensure a high level of data security and improve the overall efficiency of manufacturing processes.

Therefore, there is a need for further research aimed at integrating cryptographic protocols into the post-processing of 3D-printed parts, particularly the development of methods to protect vibration parameters and other critical data.

Research Methodology. The research methodology is based on the use of various materials and methods for post-processing 3D-printed parts, as well as the development of data protection methods using lightweight cryptography. The main stages of the research include sample preparation, post-processing, data collection and analysis, and ensuring data security.

The study utilizes samples printed using SLA, FDM and SLS technologies. Each sample undergoes different post-processing methods, such as grinding, polishing, and painting, to determine the optimal processing parameters. The samples are made from various materials, including photopolymers, thermoplastics, and metal powders.

The research methodology includes the following stages:

1. Sample preparation. In the first stage, samples are printed using three different 3D printing technologies: SLA, FDM, and SLS [13]. The initial surface parameters for each sample are determined, including surface roughness, visible layer lines, and other defects.

2. Sample post-processing. In the second stage, the samples undergo various post-processing methods, including mechanical grinding, polishing, and painting. Different abrasive materials and polishing pastes are used for each method. The vibration modes for the containers in which the processing takes place are optimized to achieve the best results.

3. Data collection and analysis. After the post-processing is completed, the surface quality of the samples is analyzed. Parameters such as roughness, visibility of layer lines, and overall aesthetic appearance are evaluated. Data is collected using specialized equipment, including profilometers and optical microscopes.

4. Data protection. An important aspect of the research is ensuring the security of the data generated during the post-processing process. Lightweight cryptography methods are used to effectively encrypt the data with minimal resource expenditure. The data is encrypted before being transmitted to central servers for further analysis and management.

5. Integration of cryptographic protocols. In the final stage, cryptographic protocols are developed and implemented to protect the data during transmission from the vibration containers to the central servers. The choice of encryption methods is based on their efficiency and ability to integrate into monitoring and control systems for vibration processes.

This research methodology ensures high quality of 3D-printed parts and reliable protection of data generated during post-processing. The results of the study can be used to improve 3D printing technologies and develop new post-processing methods that meet modern quality and security standards.

Vibration Processing Techniques. To ensure high quality of 3D-printed parts, several post-processing methods are used, including grinding, polishing, and painting. Grinding and polishing help to remove surface roughness and visible layer lines that form during printing [6]. Various abrasive materials and polishing pastes are employed to achieve the desired level of smoothness and aesthetic appearance.

An important aspect of post-processing is selecting the correct vibration modes for the containers in which the parts are processed [12]. Optimal vibration modes help to improve the quality of grinding and polishing by ensuring even surface treatment of the parts. Mechanical grinding and polishing are most effective when processing multiple parts simultaneously, as this is economically advantageous. However, considering certain design features of the parts being processed, their size, production scale, and other technical, organizational, and economic factors of the technological process, it may also be feasible to process one or more parts at a time.

Processing occurs in a specialized vibratory bowl filled with processing media [15]. For simultaneous processing of a large number of parts, bowls with ring-shaped, parabolic, or toroidal geometry (Fig. 2: a, b, c), and other rounded forms are preferred.

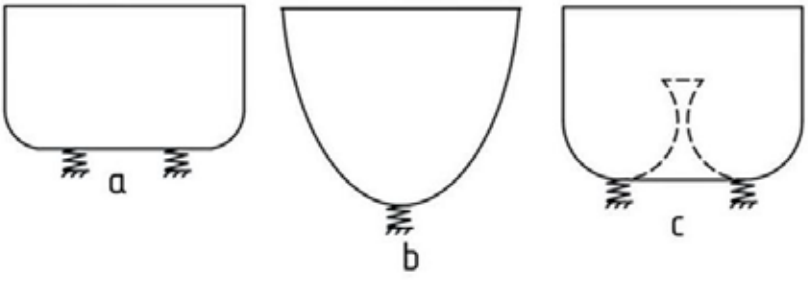

Fig. 2. Diagrams of the Most Common Shapes of Vibratory Bowls

To process a part of the surface of the components, it is necessary to protect the unprocessed part with certain means or special fixtures (Fig. 3).

The processing media in the vibratory bowl can include various types of abrasive materials or their mixtures combined with softening agents and liquid solutions. The selection and application of these media depend on numerous technical, economic, scientific, research, and other factors.

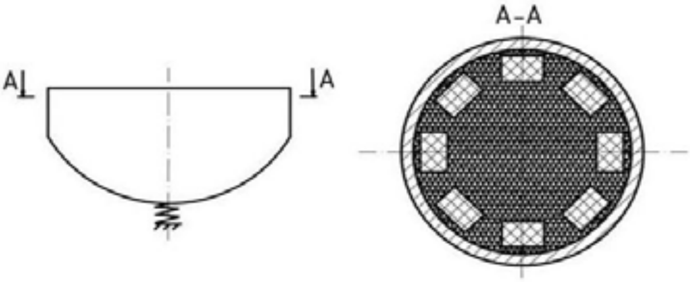

Fig. 3. Diagram of Part Placement with Fixtures in a Vibratory Bowl with Processing Media

Structure of a Secured Post-Processing System for 3D-Printed Parts. During the post-processing of 3D-printed parts, there is a need to protect the data generated by vibratory containers and transmitted to central servers for further analysis and management. Lightweight cryptography methods are used to effectively encrypt the data with minimal resource expenditure.

Vibration parameters and other information must be encrypted before transmission to the central server for analysis and management. This ensures the confidentiality and integrity of the transmitted data and prevents unauthorized access and modification.

Data transmission and processing in the 3D-printed parts post-processing system occur in several stages, each of which is crucial for ensuring the security and quality of the finished products [8]. As shown in the structural diagram, data collected by sensors is processed by a local controller for preliminary processing, then encrypted and transmitted via a secure communication channel to the central server. On the server, the data is decrypted and analyzed to detect potential defects or deviations, allowing for timely corrective actions. This process ensures data confidentiality and enhances production efficiency.

Figure 4 presents the structural diagram of the 3D-printed parts post-processing system, which includes an integrated encryption module to ensure data transmission security.

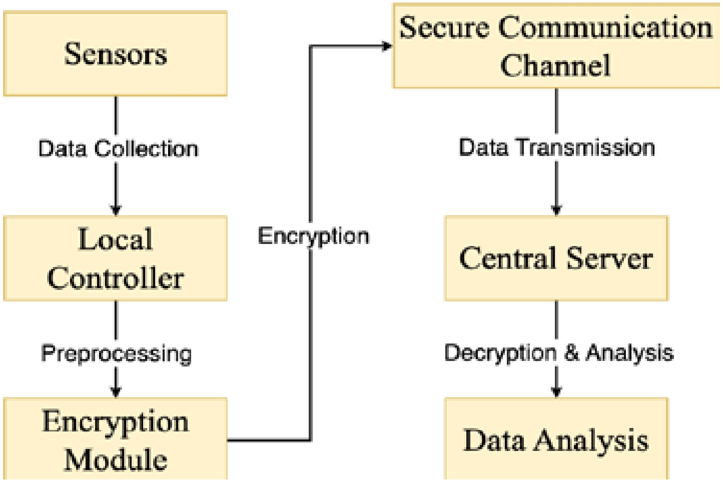

Fig. 4. Structural Scheme of the Secured 3D-Printed Parts Post-Processing System

The post-processing of 3D-printed parts involves the following stages:

1. Sensors collect vibration parameters and other necessary data during the post-processing process.
2. A local controller receives data from the sensors and performs preliminary processing, filtering, and aggregation of the data.
3. After preliminary processing, the data is transmitted to the encryption module, where it is encrypted to ensure security.
4. The encrypted data is transmitted via a secure communication channel to the central server.
5. On the central server, the data is decrypted and further analyzed.
6. The data analysis process allows for the detection of potential defects or deviations, after which necessary corrective actions can be taken.

Upon completing all stages of post-processing, the system not only ensures high quality of the 3D-printed parts but also guarantees the security and confidentiality of technological data. With the integration of the encryption module, the collected data is protected from unauthorized access, preserving the integrity of the information during transmission and subsequent processing on the central server. This enhances the reliability of the entire post-processing process and minimizes risks associated with information leakage or external threats.

Integration of Cryptographic Protocols. Cryptographic protocols provide robust protection against unauthorized access and tampering, which is critical for systems with limited computational capabilities. The use of lightweight encryption algorithms ensures data security without significantly impacting system performance. A key aspect is the integration of these protocols into vibration process monitoring and control systems, enabling high accuracy and reliability in data processing.

Encrypting data is essential for protecting sensitive information from cyberattacks [13]. Vibration parameters and other data collected during the post-processing of 3D-printed parts may contain confidential technological information that needs to be protected from competitors and malicious actors. Encryption ensures that even if the data is intercepted, it remains inaccessible to unauthorized parties.

In post-processing 3D-printed parts, devices with limited resources, such as microcontrollers or embedded systems, are often used. Lightweight ciphers, unlike traditional ones, are specifically designed to operate under conditions of limited computational power and energy consumption. They provide the necessary level of security while not overburdening the system or affecting performance.

Encryption algorithms in such systems are implemented both in hardware and software [17]. Hardware modules, such as specialized chips or embedded cryptographic processors, can provide high encryption and decryption speeds with minimal energy consumption. This is especially important for devices that run on batteries or have limited energy resources. On the other hand, software implementation of encryption algorithms allows for greater flexibility in adapting to the specific requirements of the system [2].

In both cases, the main goal is to ensure data security without significantly impacting system performance. This enables secure data processing in low-resource systems.

In environments with limited computational resources, such as post-processing of 3D-printed parts, it is crucial to choose cryptographic algorithms that are both lightweight and effective. Several low-resource ciphers have been developed specifically for such applications, providing a balance between security and performance.

In such systems, it is important to encrypt not only vibration parameters but also other critical data generated during the post-processing of 3D-printed parts. This includes temperature readings, the speed and direction of material movement, equipment technological parameters, configuration files and programs that define system operating modes, and the results of surface quality measurements, including roughness and layer line visibility. Additionally, data on energy consumption during processing also needs to be encrypted to prevent unauthorized access to confidential information that may contain important technological details.

The application of cryptographic algorithms in post-processing systems for 3D-printed parts is a crucial step in ensuring information security. Given the limited computational resources and energy consumption of such systems, special attention must be paid to selecting ciphers that can provide reliable data protection without overburdening the system. Some of these ciphers include SPECK, SIMON, and PRESENT, which have been specifically designed for efficient operation in resource-constrained environments [14]. They provide a high level of security with minimal energy consumption, making them an ideal choice for use in embedded systems and microcontrollers used in post-processing operations.

SPECK is a lightweight block cipher optimized for software implementations in resource-constrained environments, such as post-processing systems for 3D-printed parts [11]. Due to its simple structure and flexibility, SPECK provides high encryption speed with minimal computational resource consumption, making it an ideal choice for data protection in devices that operate on batteries or have limited energy and computational capabilities. It employs a key schedule (1). In this study, the SPECK64/96 configuration was selected, which operates on a 64-bit data block and uses a 96-bit key. This configuration offers an excellent trade-off between security level and efficiency in constrained environments.

$$\mathrm{K_i} = \left(\mathrm{K_{(i-1)}} \oplus \mathrm{F_{(i-1)}}\left(\mathrm{K_{(i-2)}}, \mathrm{K_{(i-3)}}\right)\right) \tag{1}$$

where $F_{i-1}\left(K_{i-2}, K_{i-3}\right)$ is a round function that combines keys from previous rounds.

The encryption round function is represented by the expression (2).

$$F\left(x, y\right) = \left(\left(x \gg 8\right) + y\right) \oplus K_i \tag{2}$$

This function shifts the value of x 8 bits to the right, adds it to y, and the result is XOR-ed with the key K_i.

SPECK is characterized by low energy consumption and high data processing speed, making it ideal for use in battery-powered devices. Cryptanalysis studies have demonstrated that SPECK64/96 offers sufficient resistance against differential and linear attacks in non-critical embedded systems.

SIMON is a lightweight block cipher designed for hardware implementations with minimal requirements for logic elements and power consumption. It provides high efficiency and flexibility in various embedded systems, particularly where computational resources are limited. SIMON supports multiple block and key sizes, allowing it to be adapted to specific security and performance requirements. SIMON is particularly well-suited for hardware implementations, offering low logic element count and energy consumption, making it ideal for battery-powered devices in post-processing systems. The cipher uses a key schedule (3).

$$\mathrm{K}_{(i+1)} = \mathrm{K}_i \oplus \left(\mathrm{K}_{(i-1)} \oplus \mathrm{RotateLeft}\left(\mathrm{K}_{(i-2)}, 8\right)\right) \tag{3}$$

Here, the next round key is obtained by XOR-ing the current key with the result of rotating the key from two rounds ago by 8 bits and then XOR-ing it with the previous key.

The encryption round function is represented by the expression (4).

$$F(x) = \left((x \gg 1) \wedge (x \gg 8)\right) \oplus (x \gg 2) \tag{4}$$

This function processes the value of x by shifting it 1 and 8 bits to the right and applying the AND operation. Then the result is XOR-ed with x shifted by 2 bits to the right. The compact design of SIMON ensures its efficient integration into embedded systems with minimal impact on overall performance.

PRESENT is a lightweight block cipher designed for use in resource-constrained environments, such as embedded systems and microcontrollers. It operates with a fixed block length of 64 bits and a key of either 80 or 128 bits. PRESENT is particularly effective in environments where memory and computational power are severely limited [10]. PRESENT uses a key schedule (5).

$$K_i = SubBytes\left(RotateLeft\left(K_{(i-1)}, 61\right)\right) \oplus i \tag{5}$$

The key is processed by the SubBytes, function, which is applied to the key, then rotated 61 bits to the right, and the result is XOR-ed with the round number *i*.

The round function for encryption is represented by expression (6).

$$F(x) = SBox(x) \oplus Perm(x) \tag{6}$$

In this function, the value x is first passed through the SBox (substitution table), and then the result is XOR-ed with the permuted value of x.

Given the need for high processing speed and flexibility in software implementations, which are characteristic of post-processing systems for 3D-printed parts, the SPECK cipher is the most suitable for protecting vibration parameters and other operational data. SPECK provides the necessary level of security with minimal impact on computational resources, which is critical for such systems.

Results and Discussion. As a result of the research, a post-processing system for 3D-printed parts with an integrated encryption module has been proposed. The post-processing system includes vibration containers equipped with sensors that measure vibration parameters and other technological indicators during the processing of 3D-printed parts. The collected data is sent to a local controller, where it undergoes preprocessing, including filtering and aggregation. The data is then encrypted before being transmitted to a central server for further analysis.

The integrated encryption module is implemented as a separate component at the preprocessing stage. This stage handles the data generated during vibration processing. The main function of the module is to protect confidential technological information from unauthorized access during its transmission to the central server for further analysis. The encryption module is integrated into the local controller, which receives data from the sensors in the vibration containers. In this research, the encryption module was implemented on a resource-constrained microcontroller platform, specifically the **STM32F103** based on ARM Cortex-M3 architecture. This controller is widely used in industrial applications due to its low power consumption and real-time processing capabilities. The SPECK cipher was embedded into the firmware using a lightweight cryptographic library optimized for this microcontroller. Several lightweight cryptographic algorithms were considered for encrypting the data. Among them, SPECK was selected due to its optimal balance of software implementation efficiency, encryption speed, and minimal RAM/ROM footprint, making it highly suitable for microcontrollers commonly used in post-processing control systems. Its performance was benchmarked against SIMON and PRESENT in terms of energy efficiency and throughput, where SPECK showed a favorable trade-off for systems without hardware acceleration. It provides high encryption speed, low energy consumption, and minimal computational resource requirements, which is critical for systems with limited capabilities, such as microcontrollers used in post-processing of 3D-printed parts. SPECK effectively protects confidential technological data without impacting the overall system performance, making it an ideal solution for such conditions.

Conclusion. As a result of the conducted research, a structure for a secure post-processing system for 3D-printed parts has been developed, which includes an integrated encryption module based on lightweight cryptographic algorithms. The proposed system ensures high surface processing quality by optimizing vibration process parameters and effectively encrypting data generated during post-processing. The use of the SPECK cipher has proven to be the optimal solution for resource-constrained systems, as it provides high encryption speed with low energy consumption, which is critical for microcontrollers and embedded systems used in post-processing operations. The results can contribute to the advancement of 3D printing technologies and the creation of new post-processing methods that meet contemporary requirements for quality and information security.

Bibliography:

1. Fortune Business Insights. (n.d.). 3D printing market size, share & COVID-19 impact analysis. URL: https://www.fortunebusinessinsights.com/industry-reports/3d-printing-market-101902 (February 10, 2025)

2. Hozdić E. Characterization and Comparative Analysis of Mechanical Parameters of FDM-and SLA-Printed ABS Materials. *Applied Sciences.* 2024. № 14(2). P. 649. https://doi.org/10.3390/app14020649

3. Huang J., Qin Q., Wang J. A review of stereolithography: Processes and systems. *Processes.* 2020. № 8(9). P. 1138. https://doi.org/10.3390/pr8091138

4. Kafle A., Luis E., Silwal R., Pan H. M., Shrestha P. L., Bastola A. K. 3D/4D printing of polymers: fused deposition modelling (FDM), selective laser sintering (SLS), and stereolithography (SLA). *Polymer.* 2021. № 13(18). P. 3101. https://doi.org/10.3390/polym13183101

5. Karakurt I., Lin L. 3D printing technologies: techniques, materials, and post-processing. *Current Opinion in Chemical Engineering.* 2020. № 28. P. 134–143. https://doi.org/10.1016/j.coche.2020.04.001

6. Kopar M., Yildiz A. R. Experimental investigation of mechanical properties of PLA, ABS, and PETG 3-d printing materials using fused deposition modeling technique. *Materials Testing.* 2023. № 65(12). P. 1795–1804. https://doi.org/10.1515/mt-2023-0202

7. Kristiawan R. B., Imaduddin F., Ariawan D., Ubaidillah Arifin, Z. A review on the fused deposition modeling (FDM) 3D printing: Filament processing, materials, and printing parameters. *Open Engineering.* 2021. № 11(1). P. 639–649. https://doi.org/10.1515/eng-2021-0063

8. Lim J. X. Y., Pham Q. C. Automated post-processing of 3D-printed parts: artificial powdering for deep classification and localisation. *Virtual and Physical Prototyping.* 2021. № 16(1). P. 1–14. https://doi.org/10.1080/17452759.2021.1927762

9. Pavlenko P., Teslia I., Khlevna I., Yehorchenkov O., Yehorchenkova N., Kataieva Y., Khlevnyi A., Veretelnyk V., Latysheva T., Kubiavka L. Development of a concept of combined project-production activities planning using digital twins. *Eastern-European Journal of Enterprise Technologies.* 2024. № 5 (131(3)). P. 6–17. https://doi.org/10.15587/1729-4061.2024.311751

10. Rashidi B. Flexible structures of lightweight block ciphers PRESENT, SIMON and LED. *IET Circuits, Devices & Systems.* 2020. № 14(3). P. 369–380. https://doi.org/10.1049/iet-cds.2019.0363

11. Rashidi B. High-throughput and flexible ASIC implementations of SIMON and SPECK lightweight block ciphers. *International Journal of Circuit Theory and Applications.* 2019. № 47(8). P. 1254–1268. https://doi.org/10.1002/cta.2645

12. Raza A., Markovic N., Wolf T., Romahn P., Zinn A. H., Kolossa D. Glass Container Fill Level Measurement via Vibration on a Low-Power Embedded System. In *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS),* July 2023, pp. 1–6.

13. Rozlomii I., Yarmilko A., Naumenko S. Analysis of Information Security Issues in Balancing Multiple Independent Containers on a Single Server. *CEUR Workshop Proceedings.* 2023.Vol. 3628. P. 450–461. URL: https://ceur-ws.org/Vol-3628/paper26.pdf

14. Rozlomii I., Yarmilko A., Naumenko S. Data security of IoT devices with limited resources: challenges and potential solutions. *CEUR Workshop Proceedings.* 2024. Vol. 3666. P. 85–96. URL: https://ceur-ws.org/Vol-3666/paper13.pdf

15. Symoniuk V., Denysiuk V., Lapchenko Y., Kaidyk O., Ptachenchuk V. About Trimming Processes of Parts in the Shock-Impulse Load of Vibrobunker. In *Grabchenko's International Conference on Advanced Manufacturing Processes,* September 2019. Cham: Springer International Publishing, 2019, pp. 321–330.

16. Symonyuk V. P., Ptashenchuk V. V., Tymoshchuk A. A. To analysis of the technical state of the equipment for manufacturing parts using 3D printing. *Promising technologies and devices.* 2022. № 21. P. 113–118.

17. Voievodin Y., Rozlomii I. Application Security Optimization in Container Orchestration Systems Through Strategic Scheduler Decisions. *CEUR Workshop Proceedings.* 2024. Vol. 3654. P. 471–478. URL: https://ceur-ws.org/Vol-3654/short16.pdf

18. Xu X., Goyanes A., Trenfield S. J., Diaz-Gomez L., Alvarez-Lorenzo C., Gaisford S., Basit A. W. Stereolithography (SLA) 3D printing of a bladder device for intravesical drug delivery. *Mater Sci Eng C Mater Biol Appl.* 2021 Jan; 120:111773. https://doi.org/10.1016/j.msec.2020.111773. Epub 2020 Dec 4. PMID: 33545904.

Дата надходження статті: 01.07.2025
Дата прийняття статті: 11.07.2025
Опубліковано: 23.09.2025