Article

Intelligent Bio-Latticed Cryptography: A Quantum-Proof Efficient Proposal

Ohood Saud Althobaiti 1,2,*, Toktam Mahmoodi 1 and Mischa Dohler 1,3

1 Department of Engineering, King’s College London, London WC2R 2LS, UK
2 Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
3 Advanced Technology Group Ericsson Inc., Silicon Valley, NC 94087, USA

* Correspondence: ohood.althobaiti@kcl.ac.uk or ohood.s@tu.edu.sa

Abstract: The emergence of the Internet of Things (IoT) and the tactile internet presents high-quality connectivity strengthened by next-generation networking to cover a vast array of smart systems. Quantum computing is another powerful enabler of the next technological revolution, which will improve the world tremendously, and it will continue to grow to cover an extensive array of important functions, in addition to it receiving recently great interest in the scientific scene. Because quantum computers have the potential to overcome various issues related to traditional computing, major worldwide technical corporations are investing competitively in them. However, along with its novel potential, quantum computing is introducing threats to cybersecurity algorithms, as quantum computers are able to decipher many complex mathematical problems that classical computers cannot. This research paper proposes a robust and performance-effective lattice-driven cryptosystem in the context of face recognition that provides lightweight intelligent bio-latticed cryptography, which will aid in overcoming the cybersecurity challenges of smart world applications in the pre- and post-quantum era and with sixth-generation (6G) networks. Since facial features are symmetrically used to generate encryption keys on the fly without sending or storing private data, our proposal has the valuable attribute of dramatically combining symmetric and asymmetric cryptography operations in the proposed cryptosystem. Implementation-based evaluation results prove that the proposed protocol maintains high-performance in the context of delay, energy consumption, throughput and stability on cellular network topology in classical Narrowband-Internet of Things (NB-IoT) mode.

Keywords: cybersecurity; cryptography; Internet of Things; lattices; face recognition; biometric encryption; post-quantum era; artificial intelligence; cellular networks; symmetric and asymmetric operations

1. Introduction

Recent developments in quantum computing are certain to lead to the widespread use of sophisticated quantum computers. The “bit” is the smallest unit of data storage in conventional computing, and it can store either zero or one, while the “qubit” is the smallest unit of storage in quantum computing and can store zero, one, or both values simultaneously (i.e., $|\psi\rangle = |C_0\rangle|0\rangle + |C_1\rangle|1\rangle$). “Superposition” is the term used to describe this simultaneous characteristic. This should cause serious concern, as most current cybersecurity schemes have been proven to be compromised by the inclusion of quantum computing. In other words, the security of wireless networking is a serious problem in the quantum IoT and sixth generation (6G) networking. Over the preceding decades, public key encryption had gained trust due to its resistance to being cracked. Unfortunately, that has changed since 1994, specifically with the discovery by the scientist Peter Shor [1] that the enormous processing capabilities of quantum computers will, in the future, enable them to break encryption keys. Thus, creating quantum-resistant practical advanced cryptographic techniques is essential. Therefore, this research presents a practical lattice-driven...
Cryptographic prototype in terms of face biometrics that offers intelligent bio-latticed cryptography that can overcome the cybersecurity challenges of the smart world in the pre- and post-quantum computing era. Cryptography based on lattice problem theory is considered an appropriate alternative cryptographic method for the IoT in the post-quantum world because it uses short keys with high effectiveness [2–5]. The emergence of the IoT has had a positive effect on the submission of requests to data warehouses and access to internet services, as the IoT is one of the 21st century’s most revolutionising developments. Moreover, it has led to the appearance of the industrial IoT (IloT) and the tactile internet, which is an embodiment of critical iIoT. Interest in face recognition for security purposes is growing rapidly due to the technology’s flexibility, high accuracy in identification verification, and its prolific use in IoT applications such as smart cities. Because of its respected reputation in the biometrics world, face recognition technology requires a secure environment.

In this paper, an enhanced artificial neural network based on the Gabor and Kalman filters, Karhunen–Loève algorithm, Principal Component Analysis (PCA), and genetic optimisation algorithm is employed to classify extracted facial features. This will improve the accuracy of the proposed scheme. Filter algorithms minimise redundant information and noise by optimising image models. Gabor functions, which are linear filters, have gained significant interest in the image processing field because they attempt to operate based on some principles of human vision. In computer vision, optimal localisation characteristics can be possessed in frequency and spatial domains using two-dimensional Gabor filters. Gabor filters are used to represent the local structural information of an image, such as spatial location, smoothness, spatial scale, orientation of edges, and direction selectivity [6]. This means that the Gabor function is appropriate for issues of texture segmentation and edge detection, and helps maintain the maximum amount of facial texture information possible. The Kalman filter (linear quadratic estimation) has had increasing significance in computer vision as an optimal recursive mathematical–statistical function used to process data, such as by estimating unknown variables [7–9].

One of the most common approaches to pattern recognition is PCA, which is an eigenface technique [10]. This method is easy, practical, and provides satisfactory results [11]. Therefore, our proposal uses statistical PCA (eigenface) to extract facial features. PCA is used to improve the performance of supervised neural network learning and reduce the dimensions of a face image, hence decreasing the amount of memory storage space necessary. In this prototype, the feature extraction process involves the following:

- Normalising data by Gaussian normal distribution. Gaussian distribution is a normal unique probability distribution that is preferred for describing random systems because numerous random processes that occur in nature act as normal distributions. The central limit theorem declares that for any distribution, the sum of random variables tends to fall within normal distribution under moderate circumstances. Thus, normal distribution has flexible mathematical attributes [7];
- Calculating a covariance matrix;
- Deriving eigenvalue and eigenvectors based on the covariance matrix;
- Picking eigenvector dimension \( k \);
- Computing the Karhunen–Loève transformation into \( k \).

In real-life scenarios, no single approach is perfectly efficient in all instances. Accordingly, it is necessary to integrate a combination of approaches to improve the performance of the architecture. For example, although machine learning has recently become popular in numerous essential applications, it requires a large amount of data [12], whereas genetic algorithms do not necessitate a large amount of data. Additionally, the majority of high-performing convolutional neural networks are intended to run on high-end graphics processing units with large memory and computing capability. This leads to the limited use of convolutional neural networks in resource-constrained devices such as those used in the IoT [13]. In addition, the accuracy of artificial neural networks increases with an increase in hidden layers. The number of artificial neurons must be large enough to express problems and identify potential hidden patterns. Therefore, there is a trade-off between
the complexity and performance of a neural network. To resolve these issues, we use a genetic algorithm to optimise the fitness of a neural network, use filters to reduce redundant information and estimate unknown variables, and use a pattern recognition method and the Karhunen–Loève algorithm to mitigate the dependency on neural networks.

Javadi et al. [14] state that using genetic algorithms to optimise complicated systems might cause the need for significant computing effort because of the repeated re-evaluation process of the objective functions and the characteristics of the search based on population. As a result, they presented a hybrid optimisation approach based on a combination of a back-propagation neural network and a conventional genetic algorithm. This back-propagation neural network is employed to enhance genetic algorithm convergence during the search process for an optimal outcome. Their suggested computational method’s efficiency is demonstrated through the use of a number of test scenarios. In [15], the authors adopt an improved genetic algorithm called the generalised genetic algorithm to find optimal sensor placement. This solves the problem of the optimal sensor placement procedure, which performs the important function of health monitoring for large-scale complicated structures [15].

According to Shiffman [16], using genetic algorithms with a large population will provide more variation, thus generating a more accurate output. Consequently, to increase the accuracy of the genetic algorithm, we initialise the neural network with a population of M components that each involves DNA generated based on PCA. The genetic algorithm performs three actions: selection, reproduction, and replacement. The fitness of each population component is evaluated to form a mating pool in the selection phase. However, there are ways to obtain more variation in this phase, such as using \(2^{\text{number of correct characters}}\), which is especially useful when there is not enough variation during the population-creation stage [16]. The reproduction phase includes the following sub-steps: choosing two parents that have a high probability based on their respective fitness, merging the parents’ DNA to produce a child (crossover), mutating the DNA of the child according to a given probability, and adding the new child to the updated population. Finally, the old population is replaced with the updated population.

Main contributions for intelligent bio-latticed cryptographic proposal:

- While humanity is benefitted by the information technology revolution, which derives its power from information to transfer knowledge and share resources, many exploit this revolution for malicious purposes such as attacking, eavesdropping, fraud, etc. According to PwC’s survey 2022 [17], cybercrimes have topped the list of external fraud threats faced by businesses worldwide. The survey included 1296 chief executive officers belonging to 53 countries in the world, and nearly half of these corporations (46%) admitted that they had been subjected to cyber-attack, fraud, or financial crimes due to the high rate of cybercrimes and fraud around the world since the emergence of COVID-19. Moreover, [17] stated that cyber-attacks pose more risk to organisations than before, as fraud and cyber-attacks have become more sophisticated. One in five global businesses, whose revenues exceed $10 billion, have been exposed to a fraud case that cost more than $50 million. More than a third of corporations (38%) with revenues of less than USD 100 million reported having experienced some form of cybercrime and 22% of these corporations were affected by more than USD 1 million. Consequently, to counter this dangerous phenomenon, we propose intelligent performance-efficient lattice-driven cryptography using biometrics.

- The main benefit of combining lattice theory and biometrics is that doing so eliminates the need to save or send biometric templates, private keys, or any secret information, which solves some public key infrastructure problems, such as public keys distribution challenges and key expiration issues, thereby preserving privacy, improving cybersecurity in a post-quantum era, and minimising the risk of information leakage online or offline.

- The proposed cryptography resists quantum attacks such as Shor’s quantum algorithm. At the same time, it inherits neither the shortcomings of the quantum computer, such
the large gap between the implementation of real devices and physical quantum theory, nor the defects of quantum cryptography, such as a vulnerability to side-channel attacks, source flaws, laser damage, Trojan horses, injection-locking lasers, and timing attacks. Since the first quantum cryptosystems—represented by quantum key distribution systems—were made available, many adversaries have attempted to hack them with unsettling success. Fierce attacks have focused on exploiting flaws in the equipment used to transmit quantum information. Consequently, adversaries have demonstrated that the equipment is not perfect, even though the laws of quantum physics imply perfect security and privacy. Furthermore, one of the most significant drawbacks of quantum computing and quantum cryptography is the limited distance that must be considered for transmitting photons, which often should not exceed tens of kilometres. This is due to the probability that the polarisation of photons may change or even disappear completely as a result of consecutive collisions with other particles while travelling long distances. However, this problem can be solved by adding spaced quantum repeaters at uniform intervals that amplify optical signals and maintain quantum randomness for thousands of kilometres.

- Enhancement of cybersecurity allows the private keys created from biometric encryption to be stronger, more complex, and less vulnerable to cybersecurity attacks. Traditional/classical biometric systems are susceptible to various attacks, such as manipulations, impersonation attacks, stolen verifier attacks, device compromise attacks, replay attacks, denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attacks, integrity threats, privacy threats, confidentiality concerns, and insider attacks. The use of the proposed advanced algorithm eliminates these vulnerabilities. It also enhances accuracy and performance by using artificial intelligence (AI), such as machine learning (artificial neural networks) and genetic algorithms.

To this end, the research paper is systematised as follows. An overview of the biometric principles that are used in the technical biometric systems is provided in Section 2. Section 3 presents a glance at the resulting combination of biometrics and asymmetric encryption, and mentions the most important related works. In Section 4, we suggest a powerful and performance-effective cryptosystem based on mathematical lattice problem theory and face verification. Section 5 examines the performance of the proposed cryptosystem required for IoT in terms of the pre- and post-quantum smart world, notably in terms of delay, energy consumption, throughput, and stability period. Security proof of the proposed lattice-driven encryption scheme is demonstrated in Section 6. In Section 7, our concluding remarks are offered.

2. Biometrics

Body characteristics such as the face [18,19], fingerprints [20,21], and iris [19,22] have been used to recognise and verify people for different purposes in police departments, hospitals, etc. These unique human identification data are called biometrics. The word biometric is a combination of ‘bios’ (Greek for life) and ‘metrikos’ (Greek for measure). The biometric technique recognises patterns that capture details such as the face, gait, fingerprint, iris, or voice, and it extracts certain characteristics for either identification or verification [23]. Currently, many biometric applications are used in the government sector, for things such as national ID cards, social security, and welfare schemes; in forensic areas, such as corpse identification, criminal investigation, and parenthood determination; and for commercial purposes, such as data security, network login, cellular phones, and medical record management [24]. Since a user cannot forget or lose biometric data, the biometric system is more reliable than other systems.

As shown in Figure 1, a general biometric system involves the following basic components [25,26]:

1. An enrolment module acquires the data related to biometrics;
2. A feature-extraction module extracts the required set of characteristics from the collected biometric data;
3. A matching module compares the extracted features with the features in existing data;  
4. A decision-making module checks whether the identity of the user exists and whether it is accepted or rejected.

There are several requirements for human physiological or behavioural characteristics to be biometric characteristics. Some of the important requirements are as follows [25,26]:  
1. Universality: each person must have it;  
2. Uniqueness: there should be sufficient and significant differences between the characteristics of any two persons;  
3. Longevity: it must be adequately invariant over a certain period.

![Figure 1. An overview of a biometric system.](image)

3. Merits of Combining Biometrics and Asymmetric Encryption

Biometric encryption is the secure binding of a cryptographic key and biometric data in such a way that another party cannot retrieve the key or the biometric data [27]. Biometric encryption has the potential to improve security and privacy. Some of the main uses and advantages of biometric encryption [27] are summarised below.

3.1. Management of Public and Private Keys

In biometric encryption, there is no need to save or send private keys or any secret information, such as biometrics. This can solve challenges to the management of public and private keys and improve cybersecurity [27–31]. Thus, biometric encryption improves public key infrastructure (PKI), since the traditional building of a PKI is very expensive in complexity and cost. However, PKI-based architecture used for communication systems is an important issue for the European Infrastructure Public–Private Partnership (5G PPP).

3.2. No Storage of Biometric Data

The leaking or misuse of biometric information or data from storage is a major concern in biometric applications. Furthermore, biometric information is personally identifiable information (PII), and it is susceptible to privacy leaks and identity theft. The best way to preserve privacy is not to collect any PII at all. Biometric encryption addresses these
concerns and threats by encrypting biometric data and giving users full control over the use of their own biometrics [27]. This also enhances trust and confidence in biometric systems.

3.3. Cancellation and Revocation in Biometric Systems

Because biometric encryptions of the same data with different keys are always different, an individual can use the same biometrics for multiple accounts without fear that the accounts will be linked. Even if one of these accounts is compromised, there is a strong probability that other accounts will remain safe.

In a traditional biometric system, if the biometric data of an individual are compromised, it is not possible to replace them, as a person’s new biometric is always the same as their old biometric. Biometric encryption allows the system to cancel or revoke someone’s encrypted biometric and replace it with a newly generated encrypted biometric of the same person [27].

3.4. Security against Known Vulnerabilities in Biometric Systems

Account identities created from biometric encryption are much stronger, more complex and less vulnerable to security attacks. Traditional biometric systems have various vulnerabilities, such as substitution attack, manipulation, masquerading, trojan horse attacks and overriding decision response. Using biometric encryption safeguards the system from all these vulnerabilities [27].

3.5. Security and Privacy of Personal Data

Biometric encryption is easy to use and convenient to implement for any application. Therefore, users can encrypt their personal or sensitive data using biometric encryption [27]. This can be considered an asset. This technology is very powerful, as it can be easily scalable and feasible for anyone to use.

3.6. Public Acceptance Based on Embedded Privacy and Security

The components that play the most important roles in the successful deployment of any system involving personal data are public confidence and trust. A single data breach in such a system can significantly reduce public confidence, and could set the whole industry back for decades. Policies related to data governance are useful for gaining public trust, but a system with embedded privacy, security, and trust is always preferred and better. Biometric encryption directly embeds privacy and security into the system, so it can easily gain public trust [27].

Biometric encryption gives control of biometric data exclusively to the individual in such a way that it minimises the risk of any privacy leakage and it maximises the utility of the system [27]. This will encourage greater use and acceptance of biometrics.

3.7. Making Biometric Systems Scalable

Biometric encryption provides a strong reason for authorities that desire privacy and protection to adopt biometric encryption technologies for use in authenticating or verifying the identity of an individual, and not only for purposes of identification. It also allows biometrics to be used to link the holder of a token or card in a positive way by allowing local storage systems [27].

It is not clear whether biometric technology is sufficiently accurate to allow real-time comparisons of samples of several million or more. This is a concern in biometric applications for large systems. However, many one-to-many public biometric applications for large systems have been presented, and they are functioning well [27].

Most biometric applications use biometric data for authentication, not identification. However, even for authentication, the data must be transmitted to a database for comparison. From a privacy point of view, it is always risky to send biometric data to a centralised database. Some (multimodal) biometric technologies collect and compare the solutions of more than one biometric. The main reason for using a multimodal approach is the insuf-
ciency of the speed of current biometrics. Therefore, collecting more and more data from biometrics and other personal data appears to be a technical solution for the authentication used in biometrics. However, collecting more biometric data makes the system susceptible to possible privacy leakage and identity theft. Biometric encryption can be used with a multimodal database to preserve the privacy of individuals. Thus, this makes a biometric system scalable [27].

4. Lightweight Intelligent Bio-Latticed Cryptography

An overview of proposed intelligent bio-latticed cryptography is depicted in Figure 2. We develop the lattice-based cryptography (shortest vector problem (SVP)) [32–38] as follows:

We define a square lattice (right-isosceles-triangular) \( \mathcal{L} \) over Galois field \( F_{p^n} \) such that \( \mathcal{L} \subset F_{p^n}^{i \times j} \) good prime unique Galois polynomial entropies with dimensions \( i \) and \( j \) and order \( p^n \) for any integer \( n \) and prime \( p \).

A message (i.e., plain text) \( \text{Msg} \in \mathcal{L} \), where \( \mathcal{L} \) is square lattice (right-isosceles-triangular). An example of a square lattice \( \mathcal{L} \) is displayed in Figure 3.

Select \( \beta, \alpha \in \mathcal{L} \subset F_{p^n} \) good Galois entropies.

Select matrices \( \Lambda, \Gamma, \Upsilon \in \mathcal{L} \subset F_{i \times j}^{p^n} \) good Galois polynomial entropy (\( i \times j \) is 2-dimensional of \( \mathcal{L} \)).

1. Key generation:

\[
S_1 = \text{shift}_a \left( \text{shuffle}_H \left( \text{h(corrected facial features)} \oplus \Upsilon \right) \right)
\]

where \( h \) is a one-way hash function [39] and \( \text{shuffle}_H \) is a Henon shuffling map. Because biometric data is naturally changeable, while the symmetrical cryptography process requires exact data to operate properly, the representation of biometrics must be corrected symmetrically before it can be employed. To stabilise the biometric matrix, error-correction principles are symmetrically applied [30,40,41]. Further detailed information concerning the principles of the process of data correction can be found in [30,40,41].

\[
S_2 = \Lambda \oplus \Gamma \oplus S_1
\]

Secret key (private key): \((S_1, S_2)\)

\[
PK = S_1^{-1} \cdot S_2^T
\]

where \( T \) refers to the matrix transpose operation.

Public key: \((\beta, PK)\)

2. Encryption:

\[
\text{Enc}_0 = \text{Shuffle}[\text{Shift}_\beta[M_{\text{msg}}(\text{mod}\beta) \oplus \beta]]
\]

\[
\text{Enc}_1 = \text{Enc}_0 \cdot PK
\]

\[
\text{Enc} = T_s \| \text{Enc}_1
\]

where \( T_s \) is the current time of the transmitter’s device (the sender picks up timestamp \( T_s \)) and \( \| \) denotes a concatenation operation.

3. Decryption:

\[
M_{\text{msg}} = \left[ \left[ (\text{Enc} \oplus \beta) \text{mod}\beta \right] \cdot S_1 \right] \cdot \left[ \left( S_2^T S_2 \right)^{-1} S_2^T \right]
\]

When the receiver obtains the encrypted message at time \( T_r \), this message is decrypted via the secret key \((S_1, S_2)\) and then tested for the timestamp freshness \( T_s \). If \( (T_r - T_s) > \Delta T \), the receiver will reject this message, since it is expired; i.e., it is significantly vulnerable to reply attack, where \( \Delta T \) indicates the expected time interval for the communication delay in the wireless networks. Conversely, if \( (T_r - T_s) \leq \Delta T \), the receiver will accept this message.
Figure 2. Intelligent bio-latticed cryptography.

Figure 3. Square lattice (right-isosceles-triangular) [42].
5. Implementation-Based Evaluation Results

Here, we provide a simulation-based analysis of the average performance of the proposed intelligent bio-latticed cryptography to make sure that it operates efficiently without degrading the performance of the NB-IoT network. All experiments are executed by our open-sourced simulator [43], which is publicly available on the MDPI website (https://www.mdpi.com/1424-8220/21/5/1824/htm#app1-sensors-21-01824) (access date: 1 November 2022) and on GitHub (https://github.com/Ohood-Althobaiti/NB-IoTD2DSimulation-AnOpen-SourcedFramework (access date: 1 November 2022)), to compute performance metrics (i.e., delay, energy consumption, throughput, and stability period) on cellular network topology in classical mode, adapting the simulator to include various heterogeneous devices beyond sensors. For brevity, interested readers are directed to [43] for further detailed information concerning our open-source simulator. Furthermore, the resources [11,40,41,44–48] are used to implement the face verification phase in the proposed prototype.

We suppose, in this research, the following features for the heterogeneous conventional cellular network displayed in Figure 4.

- An 80 km² classical attocell network topology in an urban macrocell scenario such as a smart city;
- Five cells; each cell ($R_{cell}$) is 2 km;
- 24 Base Stations (BSs). $R_{cell}$ is a hexagon bordered by BSs placed at the vertices, with another BS placed at the centre;
- The number of devices is 250, and these are positioned randomly in 2-dimensional space;
- In traditional cellular communications, all the devices transmit uplink/downlink requests at the same time to the BS. In other words, all transmissions between cellular devices must be accomplished through the BS without considering if Device-to-Device (D2D) communication is within two cellular devices’ reach;
- The initial energy for a cell device ($E_o$) is 5000–10,000 Joules.

![Figure 4. Secure heterogeneous cellular network in traditional mode with quantum-resistant intelligent bio-latticed cryptography.](image-url)
Figure 5 depicts a comparison of the amount of time passed in two different scenarios in an urban macrocell; the first scenario is a secure NB-IoT network (using the suggested cryptosystem) and the second scenario is an unsecure NB-IoT network (without giving any thought to security). Both of these scenarios take place until most cell devices in NB-IoT networking are dead, i.e., depleted batteries (around 300 rounds). Plain communications were sent in the insecure NB-IoT attocell, regardless of whether or not eavesdroppers or adversaries were present in the public network. All communication and processing expenses in the secure NB-IoT attocell design were taken into account. Operation and transmission costs in the presence of the proposed scheme are 16.5698 min, compared to 15.0786 min without any cybersecurity measures, i.e., exposed NB-IoT. This shows that the suggested scheme only adds 1.4912 min to the total time. Consequently, a delay of this magnitude is trivial in comparison to constructing an NB-IoT attocell network that is secure.

The stability period is the amount of time that elapses between the start of network activity and the depletion of a device’s battery (dead) in the network [49]. Figure 6 compares the stability durations of NB-IoT networks that are both secure and insecure. The insecure NB-IoT attocell has a stability duration of 98 rounds, while the secure NB-IoT attocell has a stability period of 87 rounds. As a result, the intervals between stability durations in the two scenarios are quite close together.

![Figure 5. Comparison of elapsed times in minutes.](chart)

Figure 7 compares the delay times at BS number 9 for the insecure and secure NB-IoT networks in seconds, which are 2.1 and 2.8, respectively. In the secure NB-IoT network, however, there is no considerable delay.

A comparison of the number of packets transmitted from each cell device to the BS (throughput/data rates) for secure and exposed NB-IoT attocell is depicted in Figures 8 and 9. In light of the suggested cryptosystem, the number of packets (throughput) remains high.

Figures 10–12 illustrate the comparison of the energy consumption profiles of cell devices no. 101, 100, and 13, respectively, in both scenarios. Therefore, the battery health and charge levels of a cell device are handled effectively, as can be shown in these examples. This means that, in the presence of the proposed cryptosystem, there is no major overhead expense besides preventing adversarial assaults on IoT networks.
Figure 6. Stability periods for secure and insecure NB-IoT attocells.

Figure 7. Delay time comparisons at BS no. 9 with and without encryption.
Figure 8. Comparison of numbers of packets.

Figure 9. Comparison of throughput.
Figure 10. Comparison of the power consumption of cell device no. 101.

Figure 11. Comparison of the power consumption of cell device no. 100.
6. Security Proof of the Proposed Lattice-Driven Encryption Scheme

Lemma 1. The Proposed Lattice-Driven Encryption Scheme Implies $P \neq NP$.

Proof. Let us consider $\mathcal{L}$ to be an $i \times j$-dimensional square lattice (right-isosceles-triangular) that equals a set of vectors such that $\{\sum_{m=1}^{i \times j} b_m v_m | b_m, v_m \in \mathbb{F}_{p^i \times j} \}$ good prime unique Galois polynomial entropies. In shortest vector problem (SVP), the goal is to find the shortest vector (non-zero lattice point) for the given basis vectors $v_1, v_2, v_3, \ldots, v_n$ in the Euclidean norm. In the closest vector problem (CVP), the goal is to find the point closest to the given vector. For example, if $v_1, v_2, v_3, \ldots, v_n$ were the given basis vectors and $v$ was a given target vector, our objective would be to determine the closest lattice point (non-zero vector) within the Euclidean norm closest to the given target vector $v$.

As we maintained previously in [5], proof by assuming the opposite (proof by contradiction) is used to establish the validity of the security of lattice-based algorithms, such as SVP or CVP are NP-hard [50–52] against different quantum attacks. In other words, assuming the proposition to be false leads to a contradiction. By considering the NP-hard factoring problem to describe the problem of factoring for a given string $s$, we must have a polynomial-time algorithm that determines whether the given string $s$ equals solution $P$ or not. At present, in cryptography, we do not have proof that $P$ is NP. Therefore, we consider that $P \neq NP$ [53–55]. Furthermore, we discuss the relationship between the proposed lattice-driven cryptosystem and complexity theory in the context of the NP-hard problem to investigate whether they follow $P \neq NP$, since computational complexity is efficiently used to achieve encryption systems.

The two fields of complexity theory and cryptography science share some main objectives. In complexity theory, one of the main objectives is to find mathematical problems that cannot be calculated in polynomial time, and in cybersecurity science, one of the main goals is to design schemes that cannot be cracked in polynomial time. Both of these objectives are important. It is obvious that they are quite compatible with one another (i.e., complexity-associated cryptography) [56]. Raouf N. Gorgui-Naguib [57] discussed the relationship between the theory of nondeterministic polynomial completeness (NP-completeness) and computational complexity theory, thus defining complexity theory as an assemblage of findings in the field of computer science that aims to quantify this assertion: “problem A is more difficult than problem B”.

Figure 12. Comparison of the energy consumerism of cell device No. 13.
Moreover, Salil Vadhan [56] defined computational complexity theory as follows: the analysis of the minimum resources (hardware and software) that are required to solve computational tasks. It especially seeks to differentiate between problems that can be solved using effective methods (referred to as “easy” problems) and those that cannot be solved in any method or form (referred to as “hard” problems). As a result, complexity theory serves as the basis for cryptography, the focus of which is on the development of cryptographic algorithms that are “simple to use” while being “hard to crack”.

According to Raouf N. Gorgui-Naguib [57], the NP-completeness problem is a type of problem that falls under the umbrella of NP problems. For the purpose of defining this category, the satisfiability problem will be defined first, as it is a common problem in the field of computational complexity. There is an algorithm that can, in polynomial time, minimise any specific problem in type NP to the satisfiability problem. This method can do so for every problem in category NP. If the satisfiability problem can be decoded with an algorithm that takes polynomial time, then every problem that falls under the NP umbrella also falls under the P umbrella. On the other hand, if any problem in the NP class is impossible to solve, then the satisfiability problem itself must likewise be unsolvable. Such problems are known as NP-completeness problems, which have intractability features. This means that for a problem \( P_o \)

\[
\begin{cases}
\in P \text{ class} & \text{if } P_o \text{ is solvable in polynomial time deterministically} \\
\in NP - \text{completeness } (NP - \text{hardness}) & \text{if } P_o \text{ is unsolvable}
\end{cases}
\]

Woeginger [58] argues that, logically, it cannot be anticipated to discover polynomial-running time techniques for NP-completeness problems. Given the widespread acceptance of the hypothesis \( P \neq NP \), proof of NP-hard proves that a certain problem cannot be solved using an algorithm that runs in polynomial time. A number of studies have been conducted [59] to investigate the impossibility of approximating the NP-hardness problem for CVP and SVP within the terms of the polynomial factors. The problem of the approximation relevant to the closest vector and the SVPs in the context of the promise problem was investigated in [60,61].

Decision problems with a yes/no answer are the norm when addressing difficulties of nondeterministic polynomial-running time in terms of hardness [57]. If a decision problem can be solved in polynomial running time employing a deterministic Turing machine, then it belongs to the computational complexity category P. On contrary, a decision problem is considered to belong to type NP if it can be computed using a non-deterministic machine in polynomial running time [57].

Khot discussed the hardness of approximating the shortest vector problem (SVP) in lattices and in high \( \ell_p \) norms in [62,63], respectively. He showed that under the assumption \( NP \notin RP \) (random polynomial time), there is no method with a polynomial-running time that can approximate the SVP in \( \ell_p \) norm within a constant coefficient. First, he introduced a randomised reduction of the CVP into the SVP, which obtains certain hard constant factors. The BCH codes were the basis for this reduction. Thus, the SVP instances that are formed as a result of the reduction have good behaviour under the augmented tensor (vector/matrix) product, which is a new tensor product that they have introduced. This is one of its advantages. As a result, it can increase the hardness degree to \( 2^{(\log n)/2 - \epsilon} \).

Khot [62] stated that the NP-hardness of SVP in norm \( \ell_{\infty} \) was proven by van Emde Boas [64], who also hypothesised that it holds for any \( \ell_p \) norm. Additionally, he declared that an alternative public key cryptographic algorithm based on the \( n^{1.5} \)-hard problem of SVP was presented by Regev [65], and all these findings suppose the hardness of a variant named unique-SVP. Since proving that SVP approximation in \( n^{1.5} \) is an NP-hard problem is theoretically possible, this could also involve the primitives of cryptography that are dependent on the assumption \( P \neq NP \) [62]. Moreover, demonstrating the NP-hardness of factor \( n \) could entail that \( NP = coNP \), which would lead to the collapse of the polynomial
hierarchy. Then, research conducted by Aharonov and Regev [66] illustrated that factor $\sqrt{n}$ for SVP could entail that $NP = coNP$, i.e., NP-hardness [62].

By aiming to develop techniques that render any cryptanalytic operation intractable, cryptography draws from computational complexity theory and, in particular, from the notion of NP-completeness/NP-hardness [57]. It is important to note, however, that existing attack techniques in the literature do not address the lattice problem with $i \times j$ dimensions in any case. However, the adversarial techniques depend mainly on the encrypted message itself, as well as information available publicly to retrieve the related transmitted plaintext. Consequently, we use mathematical and cryptographic preliminaries such as Galois field $F^{i \times j}$, XOR, entropy, etc. to increase the complexity of the proposed lattice-driven encryption scheme, thus reflecting complexity theory’s requirement and ensuring that the proposed lattice-driven cryptosystem implies $P \neq NP$ while maintaining its optimised performance.

**Lemma 2.** The proposed lattice-driven encryption scheme resists replay attacks.

**Proof.** A replay attack is impossible as a general rule if the data that was acquired is either time-sensitive or cannot be reused [67]. Whenever an adversary is present in the channel between the sender and the receiver device, the adversary obtains unreadable data and expired packets, neither of which can be used again. Therefore, the timestamps $T_s$ and $T_r$ are used in the proposed lattice-driven cryptosystem to abort any attempted replay attacks. If an attacker exploits the communication to replay the old packet, the attacker cannot succeed in the proof process where $(T_r - T_s) > \Delta T$; thus, this packet is aborted because it is expired. $\Delta T$ denotes the expected time interval for the communication delay in the wireless network, $T_s$ refers to the current time of the sender’s node, and $T_r$ refers to the message reception time at the receiver’s device.

**Lemma 3.** The proposed lattice-driven cryptosystem follows the functional requirement of security by using mathematical and cryptographic preliminaries such as Galois field $F^{i \times j}$, XOR, entropy, etc., thereby reflecting the perspectives of computational complexity and cybersecurity.

1. **Biometric templates blended with encryption keys can improve online cybersecurity while simultaneously preserving users’ privacy.**

   **Proof.** In the lightweight intelligent bio-latticed cryptosystem, the one-way hash function of a corrected facial image is XORed with $Y$ matrix $\in F^{i \times j}_{2^n}$ 2-dimension good Galois polynomial entropy to regenerate the private key $(S_1, S_2)$ on-the-fly without transmitting or holding any secret data that may be compromised and breach the privacy of users. In biometric encryption, there is no requirement to memorise either facial images or templates of these images, which addresses the classic flaw of biometric methods. Additionally, an adversary cannot retrieve an encryption parameter $Y$, a facial image, or a facial template after binding them and then discarding them. This leads to the dramatic enhancement of security features, such as generating a robust biometric-based lattice private key $(S_1, S_2)$ on-the-fly and at the same time maintaining the performance of restricted-resource devices, since this private key has more security than typical passwords and less storage space than biometric facial data. Additionally, the key generating process is characterised by its low computational requirements and lightweight operations.

2. **Lightweight intelligent bio-latticed cryptography and Galois field $F^{i \times j}_{2^n}$.**

   **Proof.** A finite field, which is commonly referred to as a Galois field, is a set of numbers to perform mathematical operations such as addition, multiplication, subtraction, and division that always produces a result contained within the same set of numbers. Cryptography benefits from this, since a restricted set of very large numbers can be used [68]. The proposed bio-lattice cryptography uses Galois field theory, which has many applications in cryptography. Some of the main reasons for this are that it is
possible for arithmetic operations to scramble data quickly and efficaciously when the data is represented as a vector in a Galois Field, and subtraction and multiplication in a Galois Field need extra operations/steps, unlike in Euclidean space [69].

In the proposed bio-lattice cryptography, $\mathbb{F}_{2^{63}}^{i \times j}$ is used, since manipulating the bytes is required. $\mathbb{F}_{2^{63}}^{i \times j}$ has an array of elements that together represent all of the various potential values that may be assigned to a byte. Because the Galois field’s addition and multiplication operations are closed, it is easy to perform arithmetic operations on any two bytes to yield a new byte belonging to the array of that field, making it ideal for manipulating bytes [70]. Furthermore, multiplications in $\mathbb{F}_{2^{63}}$ can be optimised securely for applications in cryptography when the $P^n$ is smaller than the bits of the device (i.e., $P^n < 64$, on standard desktops or smartphones) [71].

The National Institute of Standards and Technology (NIST) has issued a request for standardization of Post-Quantum Cryptography (PQC) [72] because of the growing awareness of the need for PQC in light of the impending arrival of quantum computing. According to Danger et al. [71], code-based encryption, along with multivariate and lattice-based cryptosystems, is one of the primary competitors for this challenge, because of its inherent resistance to quantum cyberattacks. Despite being nearly as age-old as RSA and Diffie–Hellman, the original McEliece cryptography has never been widely employed, mostly because of its large key sizes [71]. There are numerous cryptosystems defined on $\mathbb{F}_{2^{N}}$ that were recognised as candidates for the first round of the NIST PQC competition [71]. The carry-less feature of addition in $\mathbb{F}_{2^{N}}$ makes arithmetic operations in this setting notably desirable. Consequently, many cryptographic approaches use it, since it provides efficiency in both hardware and software implementations because there is no carry and, thus, there are no lengthy delays [71]. In addition, Danger et al. [71] present a case study in which they assess several implementations of $\mathbb{F}_{2^{N}}$ multiplication with regard to both their level of safety and how well they perform. They claim in their conclusion that their findings are applicable to accelerate and secure implementations of the other PQC outlined in their research, in addition to symmetric ciphers such as AES that operate on finite fields $\mathbb{F}_{2^{N}}$.

Moreover, in the implementation of any cryptographic application, the size of the employed finite fields and the conditions imposed on the field parameters are determined by security concerns [73]. Therefore, the proposed intelligent bio-lattice cryptography devotes a square lattice (right-isosceles-triangular) $L$ over Galois field $\mathbb{F}_{p^n}$ such that $L \subset \mathbb{F}_{p^n}$, good prime unique Galois polynomial entropies with dimensions $i$ and $j$ and order $p^n$ for any integer $n$ and prime $p$.

3. **Entropic randomness, shifting, shuffling, XOR, and proposed lattice-driven cryptosystem.**

**Proof.** Random entropies are essential for assuring the security of sensitive information stored electronically [74,75]. Furthermore, a MATLAB-based shuffling package was developed to enhance a cryptosystem in [76]. This research paper included suggestions to enhance cryptography and make it invulnerable to data leaks using random shuffling. Hence, in the proposed cryptosystem, entropic randomness distribution, shifting, shuffling, and XORing are all used to make it difficult for an adversary without the appropriate private key to extrapolate anything valuable about the message (plaintext) from the encrypted message (corresponding ciphertext), strengthening proposed cryptosystem’s ability to resist data leaks and preserve privacy and making it more secure.

Reyzin summarised essential entropy concepts used to study cryptographic architectures in [77], since the capability of assigning a random variable’s value in a single try is often used as a significant metric of its quality, especially in applications related to cybersecurity. Moreover, he defined this capability as follows:
A random variable $A$ has min-entropy $b$, indicated by $H_\infty(A) = b$, if $\max_a \Pr[A = a] = 2^{-b}$.

Extractors of randomness have been expressed in terms of their compatibility with any distribution having a min-entropy $[77,78]$. Furthermore, the outputs from robust extractors are almost uniform, regardless of the seed, and tend to maximal min-entropy, as these extractors are able to generate outputs with a high possibility over the seed selection [77].

Similar to cryptography literature employing shuffling to prevent information leaks from encoded correspondences [76], Henon shuffling maps are used in the proposed lattice-driven cryptosystem. Using a random shuffling package, the researcher in [76] improved the security and efficacy of the Goldreich–Goldwasser–Halevi (GGH) public-key scheme. She proposed enhanced functions of GGH encryption and decryption principally relying on MATLAB-based shuffling to prevent sensitive information from leaking in images. In [32], public-key cryptography established on the closest vector problem was presented by Goldreich, Goldwasser, and Halevi to be an NP-hard lattice problem at the Crypto ’97 conference. Unfortunately, later at the Crypto ’99 conference, in [79], Phong Nguyen analysed the GGH cryptography and demonstrated that there are serious shortcomings including: any encrypted message can leak sensitive data concerning the plain message, and the difficulty of decryption can be reduced to a particular closest vector problem, which will significantly be easier than the general problem.

To this end, in order to demonstrate that the suggested lattice-driven encryption scheme satisfies the necessary standards for cybersecurity in the pre- and post-quantum world, we have conducted an analysis of each of the main security preliminaries, as illustrated above.

Reducing a Vector Module to a Lattice-Based Problem

According to [80], when attempting to solve several types of lattice problems, it is necessary to take into account the connection that exists between a vector denoted by $v \in \mathbb{Z}_{P}^{i \times j}$ and a lattice denoted by $L_B$. For computational purposes, given the basis matrix $B$ to represent the lattice $L_B$, one is essentially only concerned with the relationship that exists between the vector $v$ and the basis $B$ when it is translated to the neighbourhood of $v$. Because the domain of the lattice is infinite, this relationship can be simplified by translating the vector $v$ to the origin’s neighbourhood while maintaining relatively the same location inside the lattice. This will retain the same relationship between the vector and the lattice. A lattice modulo reduction is a term for this translation of the vector $v$.

Algorithm 1 depicts the reduction of the proposed lattice-based scheme.

However, to ensure that the reduction of the proposed lattice-based algorithm has good security, that its reduction security is equivalent to SVP reduction security, which is secure against the solution algorithms for SVP such as Lenstra–Lenstra–Lovász (LLL) or Block Korkine–Zolotarev (BKZ), and that it retains required computational complexity, in intelligent bio-latticed cryptography we use facial biometric features to generate the private key, as they constitute live-body identification and difficult to manipulate or impersonate, thus resulting in a high level of security. Accordingly, the proposed lattice-based algorithm is reducible to NP-hard.
Algorithm 1: Reduction of the proposed lattice-based scheme

INPUT: Basis $H \in \mathbb{F}_{p^n}^{i \times j}$ of Hermite Normal Form, $v \in \mathbb{F}_{p^n}^{i \times j}$

OUTPUT: $b \in \mathbb{F}_{p^n}^{i \times j}$

Start

$b \leftarrow v$

for $y \leftarrow j$ to 1 do

for $x \leftarrow i$ to 1 do

$c_{x,y} \leftarrow b_{x,y} \div h_{x,y}$

$b \leftarrow b - c_{x,y} \times b_{x,y}$

end

end

return $b$

End

7. Conclusions and Future Work

The IoT, while providing infrastructure to foster digitalisation in different areas, can also introduce harmful attacks, especially in a post-quantum society. Quantum computers’ dependence on quantum physical laws makes them have extremely powerful processing capabilities that can decrypt secure data, such as government secrets, bank records, and passwords of Internet users. This means that if these quantum computers are harnessed for criminal purposes, current encryption techniques will not be able to resist them. This is prompting governments, companies, and cryptographic experts around the world to develop encryption techniques that are resistant to attacks from such computers. This study focuses on modern scientific methods for developing cybersecurity for the IoT and the tactile internet, and preserving user privacy in smart cities in the quantum computing era using AI, biometric identification techniques, and lattice theory. The efficiency of the proposed protocol at mitigating the quantum threats while maintaining IoT performance is also assessed. As an important future work, we will compute the performance metrics of our proposal on real cellular network topology in traditional mode using heterogeneous devices such as cell phones. We will also compare our proposal with some of the existing lattice-based cryptosystems in the context of elapsed time for key generation, message encryption, and message decryption. Furthermore, we will empirically examine the influence of the parameters to find the best optimisation between the security level and performance, notably through a comparative study including lattice literature-based selected parameters and corresponding security levels, since these parameters of the cryptographic scheme are related to the hardness of the SVP.

Author Contributions: Writing–original draft, O.S.A.; Writing–review & editing, O.S.A., T.M. and M.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The first author would like to thank Taif University and the Royal Embassy of Saudi Arabia Cultural Bureau for sponsoring her Ph.D. study.

Conflicts of Interest: The authors declare no conflict of interest.
Abbreviations

The following abbreviations are used in this manuscript:

- **PKI**: Public Key Infrastructure
- **6G**: Sixth-generation Networks
- **NB-IoT**: Narrowband-Internet of Things
- **IoT**: Internet of Things
- **5G PPP**: European Infrastructure Public Private Partnership
- **LEACH**: Low Energy Adaptive ClusteringHierarchy
- **BS**: Base Station
- **Msg**: Message
- **AI**: Artificial Intelligence
- **DoS**: Denial-of-Service attack
- **DDoS**: Distributed Denial-of-Service attack
- **PCA**: Principal Component Analysis
- **iIoT**: Industrial Internet of Things
- **NP**: Nondeterministic Polynomial-type
- **NP-hardness**: Nondeterministic Polynomial-time hardness
- **SVP**: Shortest Vector Problem
- **CVP**: Closest Vector Problem
- **RP**: Random Polynomial time
- **LLL**: Lenstra–Lenstra–Lovász
- **BKZ**: Block Korkine–Zolotarev

References
