information

Article

Improved Spacecraft Authentication Method for Satellite Internet System Using Residue Codes

Alexandr Anatolyevich Olenev [1], Igor Anatolyevich Kalmykov [2,*], Vladimir Petrovich Pashintsev [2], Nikita Konstantinovich Chistousov [2], Daniil Vyacheslavovich Dukhovnyj [2] and Natalya Igorevna Kalmykova [2]

[1] Stavropol State Pedagogical Institute, 417 Lenina Str., 355009 Stavropol, Russia; olenevalexandr@gmail.com
[2] Department of Information Security of Automated Systems, North-Caucasus Federal University Stavropol, 1 Pushkina Str., 355017 Stavropol, Russia; pashintsevp@mail.ru (V.P.P.); chistousov.nik@yandex.ru (N.K.C.); dduhovny26@gmail.com (D.V.D.); kia545@yandex.ru (N.I.K.)
* Correspondence: kia762@yandex.ru

Abstract: Low-orbit satellite internet (LOSI) expands the scope of the Industrial Internet of Things (IIoT) in the oil and gas industry (OGI) to include areas of the Far North. However, due to the large length of the communication channel, the number of threats and attacks increases. A special place among them is occupied by relay spoofing interference. In this case, an intruder satellite intercepts the control signal coming from the satellite (SC), delays it, and then imposes it on the receiver located on the unattended OGI object. This can lead to a disruption of the facility and even cause an environmental disaster. To prevent a spoofing attack, a satellite authentication method has been developed that uses a zero-knowledge authentication protocol (ZKAP). These protocols have high cryptographic strength without the use of encryption. However, they have a significant drawback. This is their low authentication speed, which is caused by calculations over a large module Q (128 bits or more). It is possible to reduce the time of determining the status of an SC by switching to parallel computing. To solve this problem, the paper proposes to use residue codes (RC). Addition, subtraction, and multiplication operations are performed in parallel in RC. Thus, a correct choice of a set of modules of RC allows for providing an operating range of calculations not less than the number Q. Therefore, the development of a spacecraft authentication method for the satellite internet system using RC that allows for reducing the authentication time is an urgent task.

Keywords: Industrial Internet of Things (IIoT); low-orbit satellite internet systems; spoofing interference; zero-knowledge authentication protocols; residue codes

check for updates

Citation: Olenev, A.A.; Kalmykov, I.A.; Pashintsev, V.P.; Chistousov, N.K.; Dukhovnyj, D.V.; Kalmykova, N.I. Improved Spacecraft Authentication Method for Satellite Internet System Using Residue Codes. *Information* **2023**, *14*, 407. https://doi.org/10.3390/info14070407

Academic Editors: Stefano Caputo, Lorenzo Biotti and Lorenzo Mucchi

Received: 25 June 2023
Revised: 12 July 2023
Accepted: 14 July 2023
Published: 15 July 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The Internet of Things (IoT) is a technology that integrates devices into a computer network to solve problems of collecting, analyzing, processing, and transmitting data to other objects through software, applications, or technical devices [1]. The use of the concept of IoT can significantly improve many areas of human lives and help to create a more comfortable, smarter, and safer world. In addition, the IoT acts as a driver and basis for the realization of scientific and technological breakthroughs in almost all areas of modern society. Therefore, there is currently a large-scale increase in the number of connected IoT devices. The number of connections was in the range of 17 billion in 2022 [1], and their number will exceed 41 billion by 2027. The economic profits from the introduction of IoT technology could increase to USD 11.1 trillion by 2025 [2].

Along with the consumer segment of the Internet of Things, the Industrial IoT (IIoT) segment is rapidly developing. Interest in IIoT technology is determined by a number of its advantages [3,4]. Firstly, switching to IIoT technology helps to reduce costs caused by equipment downtime due to failures and malfunctions. This is achieved by the fast processing of data coming from sensors, which allows using new methods of forecasting

and preventing emergency situations in production. Secondly, thanks to IIoT technology, it is possible to increase the productivity of enterprise personnel, reducing the time it takes to work out and make more effective decisions. Thirdly, the Industrial Internet of Things helps to reduce production costs through more efficient use of energy. Finally, IIoT technology can improve workplace safety and reduce the negative impact of production on the environment.

A qualitative leap in the expansion of IIoT applications is the use of low-orbit satellite internet (LOSI). The use of LOSI makes it possible to expand the geography of the IIoT to a significant extent, ensuring its effective application even in areas of the Arctic Ocean. However, the transition from 4G and 5G wireless technology to LOSI leads to a dramatic increase in IIoT cybersecurity challenges. This is due to the fact that the LOSI data channel has a fairly long length. This entails an increase in the number of threats and attacks on the communication channel. A special place among the destructive impacts on the LOSI from an intruder satellite is occupied by relay spoofing interference. During the execution of this attack, the intruder satellite first intercepts the signal, which the LOSI satellite transmits to the unattended control point of hydrocarbon production and transportation. Then, it imposes this signal to the receiver, which is located at the unattended facility. Since the parameters of the imposed signal are fully consistent, the receiver perceives it as a "friendly signal" and passes the control command for execution. As a result, the equipment of the unattended hydrocarbon production and transportation control point can go into abnormal mode and even go out of order. Under certain conditions, this can lead to an environmental disaster.

The paper presents the developed method of spacecraft authentication, which provides imitation resistance of low-orbit satellite internet to relay spoofing interference. The use of this method does not allow an intruder satellite to execute a spoofing attack on the LOSI, as the authentication of this satellite is carried out before the communication session. The communication session will be provided only when the satellite is a "friend". The paper proposes the joint use of zero-knowledge authentication protocols (ZKAP) and residue codes (RC) to improve the imitation resistance of the LOSI to spoofing interference. The originality of this method is based on the integration of cryptography methods and methods of constructions of parallel arithmetic codes. The use of authentication protocols with zero-knowledge proof allows to provide high resistance to the brute-force selection of the responder signal, and the use of RC leads to a reduction in time costs for determining the status of the satellite due to paralleling the calculations at the level of arithmetic operations. In this case, the use of RC allows us to achieve this result without reducing the level of cryptographic strength of the protocol due to the correct choice of a set of code modules.

2. IIoT Technology in the Oil and Gas Industry

The expansion of IIoT technology has affected one of the most promising and high-tech areas, the oil and gas industry. Let us look at the main areas of development of this technology. As in other industrial areas, the application of IIoT technology is primarily aimed at increasing the efficiency of process control. The underlying application areas of IIoT, with sources that highlight issues that can be solved with this technology, are shown in Table 1.

Table 1. Basic applications of IIoT in the oil and gas industry.

	Application Area	Sources
1	Production automation	1. Construction and operation of automated drilling rigs [5,6]. 2. Automation of obsolete drilling rigs [7,8]. 3. Automation of the process of injecting solutions into wells [9,10].

Table 1. *Cont.*

	Application Area	Sources
2	Monitoring and control of technological processes	1. Monitoring of the operation of pumping station equipment [11,12]. 2. Increase in the level of technological safety using intelligent video surveillance cameras [13,14]. 3. Pipelines' protection from unauthorized access using intelligent sensor networks [15].
3	Improvement of labor safety at enterprises	1. Personal protective equipment with sensors supporting the Internet of Things technology [16,17]. 2. Use of IIoT technology to monitor the health status of personnel [18–20].
4	Development and use of digital twins	1. Creation of digital twins of hydrocarbon deposits [21–23]. 2. Creation and use of a digital twin of a drilling rig in training [24].
5	Transportation logistics	1. Application of IIoT in solving logistics problems at oil and gas enterprises [25,26].

The emergence of low-orbit satellite internet (LOSI) will provide a qualitative leap in the expansion of applications of IIoT technology in the oil and gas industry [27]. This is due to the fact that only with the help of low-orbit satellites it is possible to provide high-speed and reliable communication with subscribers located anywhere on Earth. LOSI can provide subscribers with broadband high-speed internet access with minimal signal time delay [28–30].

The promising use of LOSI and IIoT in the oil and gas industry is determined by the presence of large oil and gas deposits located on the Arctic Ocean shelf. According to scientists, these fields have a high potential for use, as they contain more than 20% of the total hydrocarbon reserves [31]. The efficient development of oil and gas resources in the Arctic region will increase the economic potential of the northern regions and countries of the region, as well as contribute to the development of their modern infrastructure.

One of the main constraints for the widespread development of such hydrocarbon deposits is difficult natural conditions. The Arctic Ocean is covered with ice seven months of the year, the temperature drops to minus 46 degrees Celsius, and the wind speed reaches 20 m per second. In addition, hydrocarbon fields are located in sparsely populated and hard-to-reach areas of the Far North. It is possible to minimize these negative factors and reduce the cost of production through the use of automated systems of remote control of oil and gas fields (ASRCOGF) [32]. The facilities involved in the production and transportation of hydrocarbons are unattended in such systems. In this case, only LOSI can be used to organize reliable and up-to-date data exchange between IIoT devices located at such facilities and the operations support center. Since the orbit of the satellites does not exceed 1500 km, the constellation of modern LOSI Starlink contains more than 2100 satellites [33,34].

The expansion of the number of countries and corporations planning to develop hydrocarbon deposits on the Arctic Ocean shelf leads to an increase in constellations of low-orbit satellites. In this case, there may be a situation of an effective attack of malicious satellites on the communication system used in IIoT technology. As a result, there may be disruptions in the technological processes of hydrocarbon production and transportation. This can lead to an environmental disaster, the consequences of which will have a negative impact on the ecosystem of the Far North.

The conducted research has shown that the most possible destructive impact on LOSI by an intruder satellite would be the imposition of relay spoofing interference. It is possible to provide an effective counteraction to such interference by increasing the imitation resistance of the LOSI system (LOSIS) on the basis of the application of the satellite identification system. The interrogator is installed on an unattended fortification object. The responder is placed on board the satellite. The use of a "friend-or-foe" identification system in the LOSIS allows the satellite to be authenticated before starting a communication session.

If the satellite turns out to be a "friend," it will be given a communication session with an unattended control object. If the satellite turns out to be a "foe," it will be denied a session. As a result, an intruder satellite will not be able to impose a relay spoofing interference.

Obviously, the faster a spacecraft is authenticated, the less time an intruder satellite will have to guess the correct transponder signal. This, in turn, will reduce the probability of imposition of a relay spoofing interference to the control object. To solve this problem, it is proposed to use residue codes (RC).

The novelty of this approach is that the solution is at the junction of two scientific fields—the theory of design of cryptographic authentication protocols and the theory of parallel computing. The use of authentication protocols with zero-knowledge proof allows to provide high resistance to the brute-force selection of the responder signal, and the use of RC leads to a reduction in time costs for determining the status of the satellite due to paralleling the calculations at the level of arithmetic operations. In this case, the use of RC allows us to achieve this result without reducing the level of cryptographic strength of the protocol due to the correct choice of a set of code bases.

The purpose of the article is to reduce the time required to identify the satellite due to the joint use of the zero-knowledge authentication protocol and residue codes. The developed authentication method will increase the imitation resistance of the LOSI to relay spoofing interference imposed by an intruder satellite.

The structure of the paper is as follows. Section 3 analyzes attacks on the LOSI and methods to counter them. Section 4 discusses cryptographic authentication methods that can be applied to the satellite identification system. Section 5 presents the implementation of a zero-knowledge authentication protocol using residue codes. Section 6 presents the results and discussion of the performed tests. Section 7 presents conclusions and prospects for the development of this scientific direction.

3. Analysis of Destructive Impacts on the LOSIS and Ways to Prevent Them

Based on the fact that most of the facilities and enterprises of the oil and gas industry are located in remote and sparsely populated areas of the Far North, low-orbit satellite communication systems are used to ensure the uninterrupted exchange of information with such facilities. This means that low-orbit satellites' orbits do not exceed 1500 km and they are within the receiver's visibility range for not more than 15 min. That is why there are more than 2000 satellites in the Starlink constellation now [35]. Such a system allows to ensure uninterrupted delivery of information from anywhere, including beyond the Arctic Circle.

The use of the new satellite communication system for data transmission has led to the following contradiction. On the one hand, the use of low-orbit satellite internet allows to greatly expand the scope of IIoT technologies in the oil and gas sector, which contributes to a reduction in production costs and additional profits. On the other hand, due to the large length of LOSIS communication channels, new vulnerabilities and attacks arise, the implementation of which can lead to significant economic losses. Let us consider the main destructive impacts on the LOSIS channel and ways to prevent them.

One of the first destructive impacts is the control of LOSIS channel traffic. To counter attacks that perform statistical analysis of traffic, methods for preserving traffic flow confidentiality (TFC) are used [36,37].

Refs. [36,37] present the results of research on countermeasures against traffic analysis attacks. To counter traffic analysis attacks, it is proposed to use the method of forced traffic filling. The main disadvantage of this method is a decrease in the data transfer rate due to the transmitting of "false" packets.

An attack on the confidentiality of information transmitted via the satellite channel is also among the destructive impacts. One of the often proposed ways to improve the security of the LOSIS is encryption.

Since most IIoT systems have small embedded computing resources, it is advisable to use lightweight cryptography to counter a privacy attack. The lightweight cryptography standard [38] proposes to use three block ciphers to protect data from unauthorized access. The first one is the PRESENT block cipher. It is a classic SP-net (Substitution Permutation Network) with a 64-bit information block. The recommended key length is 80 or 128 bits. The number of encryption rounds is 32. The second block cipher is CLEFIA. It uses a generalized Feistel scheme, in which a 128-bit information block is split into 4 subblocks. The recommended key length is 128, 192, or 256 bits. Depending on the key length, the algorithm has 18, 22, or 26 encryption cycles, respectively.

The third block cipher is LEA. It has an input plaintext block size of 128 bits. The recommended key lengths are 128, 192, or 256 bits. Depending on the key length, the LEA cipher has 24, 28, or 32 encryption cycles, respectively.

Stream lightweight ciphers are presented in the standard [39]. This standard recommends the use of two stream ciphers. This standard includes the Enocoro byte-oriented stream cipher (Enocoro-80 and Enocoro-128v2), operating with 80-bit and 128-bit keys respectively. The standard [39] recommends the Trivium cryptographic algorithm as the second stream cipher. This is a hardware-oriented cipher that uses an 80-bit key.

Data integrity attacks can also be used as a destructive impact in modern LOSIS. One way to prevent such an attack is the use of electronic digital signatures (EDSs) in modern IIoT ecosystems.

It should be noted that EDSs also allow for effective authentication of the message source. Using EDSs, the ASRCOGF's decision-making center will be able to unambiguously identify the IIoT device from which the information comes. Different types of digital signatures can be used for this purpose:

- Joint signature [40];
- Group signature [41];
- Circular signature [42];
- Blind signature [43];
- Proxy signature [44].

ISO/IEC 29192-4:2013 offers three simplified asymmetric cryptographic transformations for EDS calculation:

- One-way authentication based on discrete logarithms on elliptic curves;
- Authenticated lightweight key exchange (ALIKE) scheme for one-way authentication and session key establishment;
- Identity-based signature mechanism.

As satellite constellations increase and space information networks (SINs) expand, the problem of satellite authentication becomes more and more urgent. It is known that secret key encryption systems have higher performance than public key infrastructure (PKI) systems. The disadvantage of this approach is the need to periodically change secret keys. When the next secret key is delivered to the satellite, it may be intercepted by an intruder. As a result, the whole system will be compromised. The generation of session secret keys directly on board the satellite and the control object allows for eliminating this disadvantage. For this purpose, a primary secret key obtained from the network control center (NCC) is used. This approach is shown in [45].

The feasibility of using generated secret session keys for authentication in SINs is discussed in [46]. The authors point out that when the session key is intercepted, the attacker will be able to guess the correct responder signal only in the current session. A similar approach is discussed in [47]. A third-party network control center (NCC) is used in this authentication protocol. In this case, the shared session key is generated at the NCC and delivered to the subscribers.

The principles of operation of tripartite authentication protocols in space information networks are discussed in [48–50]. The tripartite protocols presented in [48,49] have a drawback. These protocols use password authentication for legitimacy verification, which has low cryptographic strength. In [50], a third party, which is a global offline trusted third party (TTP), is used to generate public and secret keys for each NCC. With the help of these keys, NCCs perform authentication.

The analysis of the works has shown that despite the different approaches to authentication in SINs, their implementation will require significant financial costs. This is due to the fact that the majority of unattended hydrocarbon production and transportation facilities are located in sparsely populated and remote areas of the Far North.

Since low-orbit satellite communications systems use a radio channel to transmit data, it is obvious that an intruder satellite can try to block this channel with active and passive interferences [51–53]. However, given the peculiarities of the power supply of low-orbit satellites, we can conclude that the intruder satellite does not have enough energy coming from the solar panels to effectively block the signal transmission through the radio channel. Therefore, the most likely destructive impact on the LOSIS is the imposition of relay spoofing interference [54,55]. To impose a relay spoofing interference, an intruder satellite must do the following. Firstly, it needs to intercept the signal that comes from the satellite to the target. Secondly, it has to transmit the intercepted signal in the direction of the receiver. Since the parameters of the imposed signal coincide with the parameters of the "friend" signal, the receiver transmits the control command to the subscriber terminal, which controls the object. As a result, the technological process performed by the unattended object is violated. This, in turn, can lead to a man-made disaster.

It is possible to reduce the effectiveness of relay spoofing interference by using a satellite identification system. This system performs satellite authentication before the communication session. A communication session will be granted only when the satellite confirms its "friend" status. Thus, an intruder satellite will not be able to transmit a spoofing jam to the receiver. Obviously, the effectiveness of the "friend-or-foe" identification system depends largely on the authentication protocol. At the same time, the protocol must have sufficient imitation resistance to signal guessing and must not require large time costs for satellite authentication.

4. Analysis of Cryptographic Authentication Methods

The many authentication protocols in use can be divided into three groups [56,57]. The first group includes password authentication protocols. In these protocols, the prover (P) and the verifier (V) know the secret (password). Both reusable and one-time secret passwords can be used to authenticate the prover. A description of password authentication methods is presented in sufficient detail in [57]. The advantage of these protocols is the small time and hardware costs to perform authentication. Because of this, password authentication methods have found widespread use. However, password authentication protocols have the disadvantage that the prover and verifier must have a list of secret passwords to determine the status of the prover. In addition, they have relatively low resistance to "protocol participant spoofing" attacks.

The second group includes challenge–response authentication protocols [56,57]. In the authentication process, the prover must provide a response to the verifier's challenge that depends simultaneously on the secret and the given challenge. At the same time, the challenge must change periodically. Usually, random numbers are used as challenges. These authentication protocols have a higher cryptographic resistance to attacks. This is achieved by using symmetric and asymmetric encryption methods in the authentication process.

The main disadvantage of the authentication protocols of the second group is the use of secret keys, which must be periodically delivered to the spacecraft. As a result of their interception, an intruder can break into the authentication system [56].

The third group is zero-knowledge authentication protocols (ZKAP). The main feature of these protocols is the ability to handle the identification of the prover without the use of encryption systems. At the same time, the protocols provide high resistance to the process of guessing correct responses for challenges from the verifier [56,57].

The distinguishing feature of these authentication protocols from those previously discussed is that the secret is known only to the prover (P). The protocols are designed in such a way that as a result of the challenge–response exchange, the verifier can be sure that the prover possesses the secret. However, the secret itself remains unknown to him.

The high cryptographic strength of ZKAP protocols is achieved in either of two ways. The first one is performing calculations modulo large prime number Q or the product of two prime numbers q and r. The second way is based on the fact that some ZKAP protocols require performing several authentication rounds. The iterative nature of the protocol execution allows to provide the required value of the probability of authenticating an intruder.

Due to their advantages, zero-knowledge authentication protocols have found applications in a wide variety of fields. These include:

- IoT (IIoT) [58–60];
- Systems of automatic identification of objects using RFID tags [61–63];
- Vehicular ad-hoc networks (VANET) [64–66].

Let us consider the main zero-knowledge authentication protocols. FS ZKAP is presented in [56,67]. The authors of the protocol are Fiat et al. High cryptographic strength is achieved by using the product of two large prime numbers and performing at least 20 authentication rounds. Let us consider the protocol's preliminary stage and one authentication round.

The generation of public and secret protocol keys, as well as their delivery to the prover and the verifier, is handled at the preliminary stage of the protocol. The Key Distribution Center (KDC) is used for this purpose.

The preliminary stage.

1. KDC chooses two large prime numbers, q and r, and then calculates their product:

$$Q = q \cdot r. \tag{1}$$

2. KDC generates a prime number M, which is the prover's secret key, where

$$M < Q, \quad \gcd(M, Q) = 1. \tag{2}$$

3. KDC finds the number H, which satisfies the following conditions:

$$H = M^2 \mathrm{mod} Q, \tag{3}$$

$$H \cdot H^{-1} \equiv 1 \mathrm{mod} Q. \tag{4}$$

4. KDC delivers the secret key M to the prover and the public key (Q, H) to the verifier.

The authentication stage (one round).

5. The prover P chooses a random number S that satisfies the condition $1 < S < M - 1$ and performs the following calculation:

$$E \equiv S^2 \mathrm{mod} Q. \tag{5}$$

Then, the prover P sends the number E to the verifier.

6. The verifier V chooses a random number B from the condition $B \in \{0, 1\}$, which is passed to the prover P.

7. Given the number B, the prover P performs the following calculation:

$$Y = SM^B \mathrm{mod} Q. \quad (6)$$

The result of the calculations is passed to the verifier.

8. After receiving the response, the verifier performs the following calculation:

$$L = (Y^2 H) \mathrm{mod} Q. \quad (7)$$

The prover P will be considered a "friend" at this stage of authentication only if the following condition is satisfied:

$$L \equiv E \mathrm{mod} Q. \quad (8)$$

Since the verifier's challenge can only take values $B \in \{0, 1\}$, this authentication stage is performed several times. Therefore, if the number of rounds is $D = 30$, the probability of authenticating an intruder will be $P = 1/2^D = 1/2^{30} = 9.31 \times 10^{-10}$. Obviously, this protocol has a significant time cost for authenticating the prover because of the large number of rounds. Therefore, it is not reasonable to use it in the satellite authentication system.

FFS ZKAP reduces the time cost of authentication [56,68]. The authors of the protocol are Feige et al. This protocol has fewer authentication rounds than FS ZKAP. This is achieved by increasing the size of the challenge generated by the verifier. So, if the challenge contains five numbers $B = \{B_1, B_2, B_3, B_4, B_5\}$, i.e., $C = 5$, then it is sufficient to perform $M = 6$ rounds to achieve the probability of authenticating an intruder equal to $P = 9.31 \times 10^{-10}$. In other words, we have $P = 1/2^{MC} = 1/2^{30} = 9.31 \times 10^{-10}$. However, despite reducing the time cost of the prover's authentication, this protocol is not feasible to use in a satellite identification system.

Non-iterative ZKAP can reduce time costs. These protocols use only one round of authentication. Refs. [56,57] show an authentication protocol, which is a modification of the Schnorr algorithm for electronic digital signature generation. Ref. [69] shows the prospects of using this authentication protocol in RFID within the Internet of Things in healthcare in COVID-19 conditions. The use of the Schnorr protocol for agent authentication in a multi-agent system is considered in [70]. The use of AVISPA software product has confirmed the effectiveness of this protocol.

The principles of the Okamoto authentication protocol are shown in [71]. The advantage of this protocol is the ability to provide resistance to participants' keys compromises through the use of redundancy in the key set. Due to this property, it is proposed in [72] to use the Okamoto authentication protocol when performing Diffie–Hellman key exchange to reduce the effectiveness of "man in the middle" attacks.

GQ ZKAP based on the RSA scheme is described in [73]. The authors of this protocol are Guillou et al. The application of the GQ protocol for smart card authentication is shown in [74]. The possibility of using the GQ protocol in a zero-knowledge identity verification scheme based on visual images is shown in [75].

However, these authentication protocols have one drawback. Their implementation requires the use of both public and secret keys. Secret keys are delivered to all provers, which are placed on board LOSIS satellites. Public keys are transmitted to verifiers, which are placed on unattended hydrocarbon production and transportation facilities. Thus, if the secret keys are intercepted when they are being changed, an intruder can easily mimic the prover's signal. As a result, he will be provided with a communication session and will be able to impose a relay spoofing interference.

The keyless zero-knowledge authentication protocol eliminates this drawback [76]. This protocol uses the prover's true and distorted statuses and three responses to the verifier's challenge in order to authenticate the prover. The protocol also uses session keys *V(k)* (where *k* is the session number) to increase the resistance to answer guessing. In addition, this protocol has a mechanism that allows us to determine the fact of re-use of the session key *V(k)* by the parameter *E(k)*. All calculations are performed modulo large prime number Q. Let us consider this zero-knowledge authentication protocol.

The preliminary stage.

1. This protocol uses the following secret parameters:

- The prover's secret key G, where $G < Q$;
- The satellite's session key $V(k)$;
- $E(k)$, i.e., the number by which the decision-making center will be able to establish the fact of re-use of the session key $V(k)$.

The following condition is satisfied for these parameters:

$$\{G, \Delta V(k), \Delta E(k)\} < \phi(Q), \tag{9}$$

where $\phi(Q)$ is the value of the Euler totient function at Q.

Secret parameters are kept by the prover.

2. The prover calculates his true status:

$$A(k) = (u^G u^{V(k)} u^{E(k)}) \mathrm{mod} Q, \tag{10}$$

where u is the generator of a multiplicative group modulo Q; $k = 1, 2, \ldots$ is the session number.

3. The prover generates random numbers $\Delta G(k)$, $\Delta V(k)$, $\Delta E(k)$, which satisfy the following condition:

$$\{\Delta G(k), \Delta V(k), \Delta E(k)\} < \phi(Q), \tag{11}$$

Using these numbers, the prover calculates distorted secret parameters:

$$\begin{array}{l} G'''(k) = G + \Delta G(k) \mathrm{mod} \phi(Q), \\ V'''(k) = V(k) + \Delta V(k) \mathrm{mod} \phi(Q), \\ E'''(k) = E(k) + \Delta E(k) \mathrm{mod} \phi(Q), \end{array} \tag{12}$$

where $k = 1, 2, \ldots$.

4. The prover calculates his distorted status:

$$A'''(k) = (u^{G'''(k)} u^{V'''(k)} u^{E'''(k)}) \mathrm{mod} Q, \tag{13}$$

where $k = 1, 2, \ldots$.

This ends the first part of the keyless ZKAP. The second part of the protocol performs the prover authentication procedure.

The authentication stage.

5. The verifier generates a random number, which satisfies the following condition:

$$B(k) < \phi(Q). \tag{14}$$

This number is the challenge. The challenge is given to the prover.

6. The prover receives the challenge $B(k)$ and proceeds to calculate three responses:

$$W^1(k) = (G'''(k) - B(k)G) \mathrm{mod} \phi(Q), \tag{15}$$

$$W^2(k) = (V'''(k) - B(k)V(k)) \mathrm{mod} \phi(Q), \tag{16}$$

$$W^3(k) = (E'''(k) - B(k)E(k)) \mathrm{mod} \phi(Q). \tag{17}$$

The prover sends the following signal to the verifier:

$$\left\{ (A(k)) || (A'''(k)) || \left(W^1(k)\right) || \left(W^2(k)\right) || \left(W^3(k)\right) \right\}. \tag{18}$$

7. Given the number B, the prover P performs the following calculation:

$$X(k) = (A(k))^{B(k)} u^{W^1(k)} u^{W^2(k)} u^{W^3(k)} \mathrm{mod} Q. \quad (19)$$

The result of (19) is compared to the distorted status of the prover. If they match, the prover is authenticated as a "friend".

The advantage of this protocol is that it requires fewer operations during the authentication stage compared to ZKAPs presented above.

However, this protocol has disadvantages. This is due to the use of a large number Q for the authentication process of the prover. Using a large number increases the imitation resistance of the authentication system. However, it also increases the computational complexity when executing the protocol. It is known that the larger the size of the operands, the more time it takes to perform a multiplicative operation. Therefore, multiplication by a large modulo will increase the time to determine the status of the prover. However, this operation is an essential one in the considered protocol. As a result, it also increases the time during which an intruder can guess correct responses to the given challenge. This leads to an increase in the probability of authenticating an intruder. Therefore, it is necessary to reduce the time required to execute the authentication protocol.

The most simple solution is to reduce the size of Q. Obviously, decreasing the size of module Q, on the one hand, will reduce the time spent on protocol execution, which will lead to a decrease in the probability of the intruder guessing correct responses of the prover. On the other hand, such a decrease in the size of module Q increases the probability of authenticating an intruder by reducing the number of possible responses to the given challenge.

It is possible to solve this contradiction by transitioning to parallel computations in the zero-knowledge authentication protocol. Parallelization of arithmetic operations is provided by residue codes.

5. Implementation of the Satellite Authentication Method Using Residue Codes

The principles of construction of residue code are defined from the name of the code itself. RC consists of modules, which can be either integers $p_1, p_2, \ldots, p_n$ [77–79] or irreducible polynomials $p_1(x), p_2(x), \ldots, p_n(x)$ [77,80]. Since RCs are arithmetic codes, they perform addition, subtraction, and multiplication operations modulo the modules of the code. In this article, residue codes with prime numbers $p_1, p_2, \ldots, p_n$ will be considered.

Let us consider the principles of construction of RC. In order to do this, the modules are chosen, for which the greatest common divisor is equal to one. After that, the modules are placed in the following order:

$$p_1 < p_2 < \ldots < p_n, \quad (20)$$

where $\underset{i \neq j}{\gcd}(p_i, p_j) = 1$.

The product of the chosen modules determines the operating range of the RC:

$$P_n = \prod_{i=1}^{n} p_i. \quad (21)$$

To obtain an RC code combination, you must choose an integer Y, the value of which does not exceed the operating range, and then determine residues of its division by RCs modules. As a result, we get a tuple of residues

$$Y = (y_1, y_2, \ldots, y_{n-1}, y_n), \quad (22)$$

where $Y < P_n; y_i \equiv Y \mathrm{mod} p_i; i = 1, \ldots, n$.

Since RCs are arithmetic codes, they can be used to effectively perform modular operations, which include addition, subtraction, and multiplication. In this case, the following equations are valid for two numbers Y and A:

$$A + Y = |a_1 + y_1|_{p_1}^+, |a_2 + y_2|_{p_2}^+, \ldots, |a_n + y_n|_{p_n}^+, \tag{23}$$

$$A - Y = |a_1 - y_1|_{p_1}^+, |a_2 - y_2|_{p_2}^+, \ldots, |a_n - y_n|_{p_n}^+, \tag{24}$$

$$A \cdot Y = |a_1 \cdot y_1|_{p_1}^+, |a_2 \cdot y_2|_{p_2}^+, \ldots, |a_n \cdot y_n|_{p_n}^+, \tag{25}$$

where $A < P_n$; $a_i \equiv A \bmod p_i$; $i = 1, \ldots, n$.

Expressions (23)–(25) clearly show the advantages of RCs. Firstly, these operations are performed in parallel. Secondly, there are no transfers between the modules of RC during calculations. Thirdly, operands y_i, a_i (where $i = 1, \ldots, n$) have less size than integers Y and A. Summing up, it can be concluded that the RC supports parallel computations. At the same time, there is an opportunity to replace the execution of modular operations with the selection of results from the LUT-tables due to the small size of the operands. Thus, using RC, it is possible to increase the speed of performing additive and multiplicative operations.

The analysis carried out in Section 4 showed that zero-knowledge authentication protocols use exactly such operations. Taking this into account, it is possible to put forward the following hypothesis. Implementation of zero-knowledge authentication protocols using RC will reduce the time for identification of the prover.

In addition, RC will allow to provide cryptographic strength not lower than the single-module authentication protocols. For this purpose, it is necessary to choose RC's modules in a way that the following condition is satisfied:

$$Q < P_n. \tag{26}$$

Then, according to the isomorphism of the Chinese remainder theorem, the calculations that are performed on large modulo Q can be implemented using RC.

These hypotheses were the basis for the developed authentication method, which is an integration of the keyless zero-knowledge authentication protocol and RC.

The limitations of this method are determined by the choice of bases of the residue code. A number of works [77–79] propose to use pairwise coprime numbers of the form $2^n - 1$, 2^n, $2^n + 1$ as RC's modules. This choice of bases allows us to reduce time and hardware costs to perform the direct conversion (from positional code to RC) and the reverse conversion (from RC to positional code). In the developed authentication method, such bases cannot be used. This is due to the fact that generating elements are used during the calculation of the true and distorted digests, as well as the verification of the signal of the prover. Therefore, it is necessary to choose only prime numbers as RC's modules. Let us consider the developed authentication method.

In the preliminary stage of the developed zero-knowledge authentication protocol using RC, the Certificate Authority (CA) generates secret parameters, which are then passed to the prover and the verifier. Let us take a look at this stage.

The preliminary stage.

1. The CA chooses the modules of the RC, which are prime numbers. The choice of modules is determined by the size of the prover's signal, which includes the true status, the distorted status, and three responses to the given challenge, all calculated modulo the prime number Q. A generator u_i is determined for each i-th module of RC:

$$\text{CA}: \ p_1 < p_2 < \ldots < p_n, \tag{27}$$

$$\text{CA}: \ P_n = \prod_{i=1}^{n} p_i, \tag{28}$$

$$\text{CA}: \ \log_2 P_n > \log_2 Q, \tag{29}$$

$$\text{CA}: \ u_i < p_i, \tag{30}$$

where P_n is the operating range of RC; $\log_2 Q = L/5$; L is the bit depth of the prover's signal.

2. The CA presents the secret parameters of the authentication method in RC with the chosen modules:

$$G = (G_1, G_2, \ldots, G_n), \tag{31}$$

$$V(k) = (V_1(k), V_2(k), \ldots, V_n(k)), \tag{32}$$

$$E(k) = (E_1(k), E_2(k), \ldots, E_n(k)), \tag{33}$$

where G is the satellite's secret key; *V(k)* is the satellite's session key; *E(k)* is the number by which the decision-making center will be able to establish the fact of re-use of the session key; $\{G, V(k), E(k)\} < P_n - 2$; $G_i = G \bmod p_i$; $V_i(k) = V(k) \bmod p_i$; $E_i(k) = E(k) \bmod p_i$; $k = 1, 2, \ldots$ is the serial number of the authentication session.

3. The secret parameters presented in RC are written into the memory of the prover on board the satellite and the verifier located at the unattended control facility.

The main stage of the method.

The developed authentication method consists of two parts. Its first part is used to calculate the true and distorted statuses of the SC, which are used in the process of checking the satellite status.

4. The responder, using his secret parameters, calculates the true status of the SC for the k-th authentication session:

$$\begin{aligned} A_1(k) &= (u_1^{G_1} u_1^{V_1(k)} u_1^{E_1(k)}) \bmod p_1, \\ &\vdots \\ A_n(k) &= (u_n^{G_n} u_n^{V_n(k)} u_n^{E_n(k)}) \bmod p_n, \end{aligned} \tag{34}$$

where u_i is the generator of a multiplicative group modulo p_i; $i = 1, \ldots, n$.

Since calculations in RC occur in parallel on the modules, generators may not coincide.

5. The prover proceeds to distort the secret parameters before calculating the distorted status. To do this, he chooses three random numbers $\Delta G(k)$, $\Delta V(k)$, $\Delta E(k)$ for which the following condition is satisfied:

$$\{\Delta G(k), \Delta V(k), \Delta E(k)\} < \prod_{i=1}^{n} \phi(p_i) - 1, \tag{35}$$

where $\phi(p_i)$ is the value of the Euler totient function at p_i; $i = 1, \ldots, n$.

Using these numbers, the prover calculates distorted secret parameters:

$$\begin{aligned} G_i'''(k) &= G_i + \Delta G_i(k) \mathrm{mod} \phi(p_i), \\ V_i'''(k) &= V_i(k) + \Delta V_i(k) \mathrm{mod} \phi(p_i), \\ E_i'''(k) &= E_i(k) + \Delta E_i(k) \mathrm{mod} \phi(p_i), \end{aligned} \tag{36}$$

where $\Delta G_i(k) \equiv \Delta G(k) \mathrm{mod} p_i; \Delta V_i(k) \equiv \Delta V(k) \mathrm{mod} p_i; \Delta E_i(k) \equiv \Delta E(k) \mathrm{mod} p_i; i = 1, \ldots, n.$

6. The prover proceeds to calculate the distorted status of the SC using the distorted secret parameters:

$$\begin{aligned} A_1'''(k) &= (u_1^{G_1'''(k)} u_1^{V_1'''(k)} u_1^{E_1'''(k))}) \mathrm{mod} p_1, \\ &\vdots \\ A_n'''(k) &= (u_n^{G_n'''(k)} u_n^{V_n'''(k)} u_n^{E_n'''(k))}) \mathrm{mod} p_n. \end{aligned} \tag{37}$$

This ends the first part of the developed authentication method. The second part of the developed method performs the satellite authentication procedure.

7. After the satellite appears in the line of sight of the verifier, the latter generates the RC code combination:

$$B(k) = (B_1(k), B_2(k), \ldots, B_n(k)) \tag{38}$$

where $B_i(k) < p_i; i = 1, \ldots, n$.

This code combination plays the role of the challenge. This challenge is transmitted to the prover.

8. The prover proceeds to calculate three responses to the given challenge $B(k) = (B_1(k), B_2(k), \ldots, B_n(k))$:

$$W_i^1(k) = (G_i'''(k) - B_i(k) G_i) \mathrm{mod} \phi(p_i), \tag{39}$$

$$W_i^2(k) = (V_i'''(k) - B_i(k) V_i(k)) \mathrm{mod} \phi(p_i), \tag{40}$$

$$W_i^3(k) = (E_i'''(k) - B_i(k) E_i(k)) \mathrm{mod} \phi(p_i), \tag{41}$$

where $i = 1, \ldots, n$.

The prover transmits his responses to the verifier:

$$\left\{ (A_i(k)) \,||\, (A_i'''(k)) || \left(W_i^1(k) \right) || \left(W_i^2(k) \right) || \left(W_i^3(k) \right) \right\} \tag{42}$$

9. After receiving the prover's signal, the verifier proceeds to its verification:

$$\begin{aligned} X_1(k) &= \left(A_1(k) \right)^{B_1(k)} u^{W_1^1(k)} u^{W_1^2(k)} u^{W_1^3(k)} \mathrm{mod} p_1, \\ &\vdots \\ X_n(k) &= (A_n(k))^{B_n(k)} u^{W_n^1(k)} u^{W_n^2(k)} u^{W_n^3(k)} \mathrm{mod} p_n. \end{aligned} \tag{43}$$

The result of (43) is compared to the distorted status of the SC. If the following equation holds:

$$(X_1(k), X_2(k), \ldots, X_n(k)) = (A_1'''(k), A_2'''(k), \ldots, A_n'''(k)). \tag{44}$$

then the SC is authenticated as a "friend" and is given a session with the unattended control object. Figure 1 shows how this authentication method works.

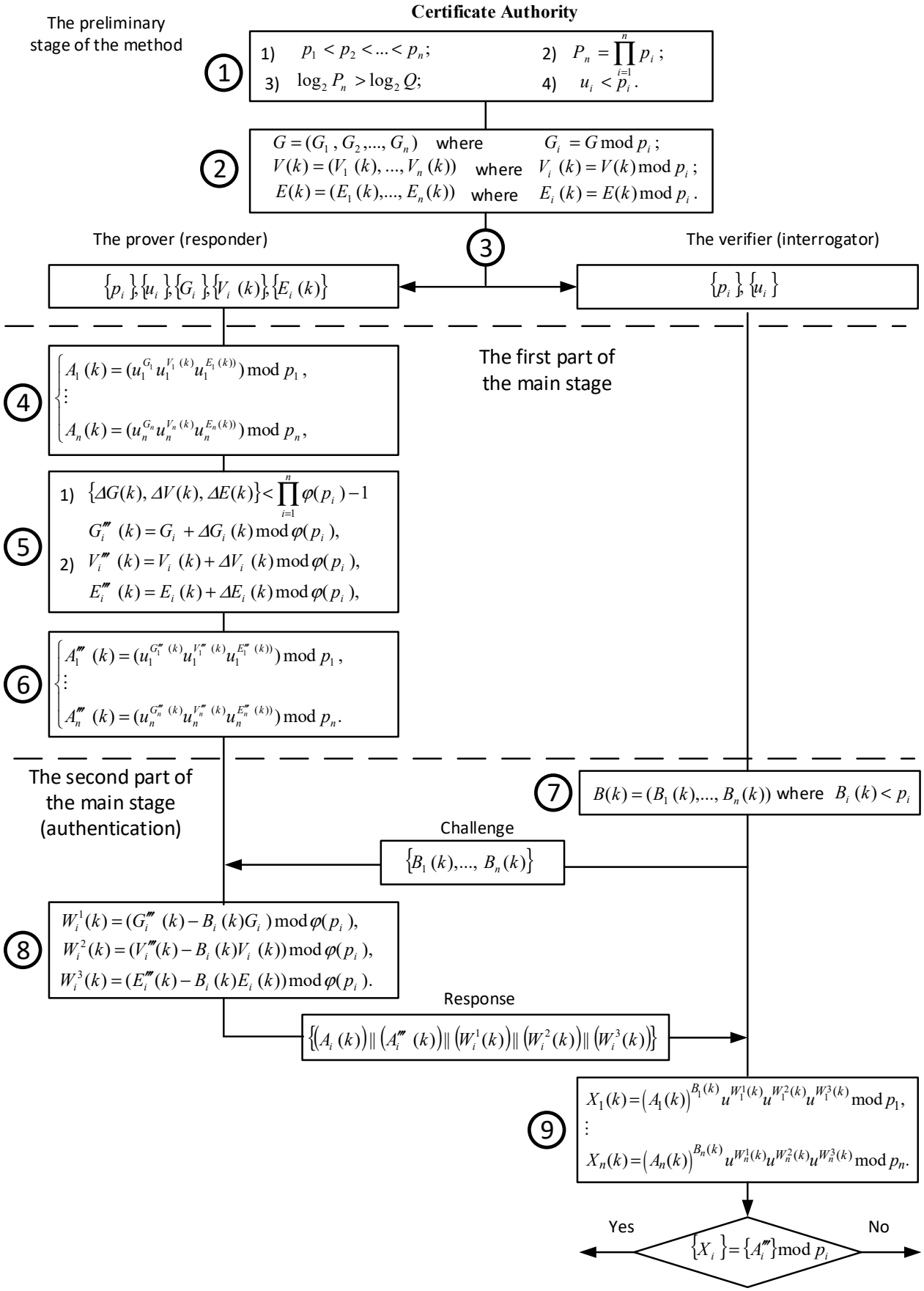

Figure 1. The developed authentication method.

6. Research Results and Discussion of the Performed Tests

An FPGA Kintex UltraScale (xcku3p-ffva676-1-e) was used to carry out a comparative analysis of the time cost of executing FS protocol in the single-module and RC implementations, the single-module keyless protocol, and the developed authentication method implemented using RC. CAD Xilinx Vivado-HLS 2018 was used to obtain the time cost of authentication.

The setup is as follows:

1. The size of the prover's signal is 160 bits;
2. FS protocol is performed for 20 rounds;
3. The modular exponentiation operation is based on the Montgomery algorithm;
4. The time of transmission of signals over the communication channel is not taken into account.

Let us consider the implementation of zero-knowledge authentication protocols without the use of RC. Therefore, the time cost of FS protocol implementation for a given setup is 21.134 μs.

Let us consider the implementation of zero-knowledge authentication protocols using RC. To fulfill Condition (26), a set of modules was chosen, which consists of 10 prime numbers. They are presented in Table 2. The maximum size of the module from this set is 18 bits.

Table 2. A set of RC's modules for FS protocol.

p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}
131	131063	131071	131101	131111	131113	131129	131143	131149	131171

The studies of the prototype showed that the use of residue codes for performing the authentication of the prover provided a reduction in the time cost for the satellite identification without reducing the cryptographic strength. This is achieved by performing parallel calculations on RC's modules. When implementing FS protocol using RC, the satellite authentication time is 4957 ns. Thus, the use of RC reduced the time of satellite identification by 4.26 times compared with the single-module protocol.

Let us consider the implementation of the single-module keyless protocol and the developed authentication method implemented using RC. The setup is as follows. The size of the prover's signal is 160 bits. Taking into account that this signal contains true and distorted statuses and three responses, the size of Q is 32 bits. Therefore, we choose a prime number Q = 4294967291.

It is known that the execution time of multiplicative operations is proportional to the size of operands. Therefore, three sets of modules will be chosen.

The first set of RC's modules contains one 17-bit number and one 16-bit number: $p_1 = 65029$, $p_2 = 66047$. Then, the operating range is equal to $P_2 = 4294970363$. Thus, Condition (26) is satisfied.

The second set of RC's modules contains three 11-bit numbers: $p_1 = 2053$, $p_2 = 2063$, $p_3 = 2069$. Then the operating range is equal to $P_3 = 8762916391$. Thus, Condition (26) is satisfied.

The third set of RC's modules contains one 9-bit and three 8-bit numbers: $p_1 = 149$, $p_2 = 251$, $p_3 = 241$, $p_4 = 509$. Then the operating range is equal to $P_4 = 4587697931$. Thus, Condition (26) is satisfied.

The fourth set of RC's modules contains six 6-bit numbers: $p_1 = 37$, $p_2 = 41$, $p_3 = 43$, $p_4 = 47$, $p_5 = 53$, $p_6 = 59$. Then the operating range is equal to $P_6 = 9586934839$. Thus, Condition (26) is satisfied.

The issues of optimal selection of RC's modules are not considered in this article. The choice of RC's modules was determined only by Condition (26). Obviously, the optimal set of modules should provide such an operating range for which Condition (26) is satisfied,

and the value P_n is as close as possible to the number Q. It will allow to reduce hardware costs for implementation of the satellite authentication system.

Let us carry out a comparative analysis of the first parts of the developed method and the single-module keyless protocol. The following operations are performed during their execution: calculation of the true status, distortion of secret parameters, and calculation of the distorted status. Table 3 shows the execution costs of the first part of the method and authentication protocol.

Table 3. The costs of executing the first parts of the developed method and authentication protocol.

RC's Modules	DSP [1]	FF [2]	LUT [3]	Time Cost, ns
Single-module protocol (32-bit)	29	679	1585	1803
The first set (17-bit)	21	605	1461	1395
The second set (11-bit)	13	562	1362	968
The third set (9-bit)	5	519	1310	825
The fourth set (6-bit)	2	495	1274	540

[1] Digital signal processing elements. [2] Flip-flop triggers. [3] Lookup tables.

Based on the analysis of the data shown in Table 3, the following conclusions can be made. The hypothesis about the joint use of ZKAP and RC has been confirmed. Parallel execution of modular operations allowed to reduce time costs of satellite authentication in comparison with the prototype. Thus, when the first set of RC's modules is used, the execution time of the first part of the authentication method is 1395 ns, which is reduced by 1.29 times compared to the single-module protocol. Reduction of the size of RC's modules has a positive effect on the time cost. Thus, when the second set of RC's modules is used, the execution time of the first part of the developed method is 968 ns, which is 1.86 times less than for the single-module protocol. When the developed method is implemented using the third set of RC's modules, the execution time of the first part is 825 ns, which is 2.18 times less than for the single-module protocol. The transition to 6-bit RC's modules (the fourth set) allows us to reduce the execution time of the first part of the developed method to 540 ns, which is 3.33 times less than for the single-module protocol [76].

Let's carry out a comparative analysis of the second part of the developed method and the single-module keyless protocol. The following operations are performed during their execution: calculation of three responses to a given challenge and verification of these responses. The calculation of the responses is performed in parallel. Table 4 shows the cost of the second part of the method and the authentication protocol.

Table 4. The costs of executing the second parts of the developed method and authentication protocol.

RC's Modules	DSP	FF	LUT	Time Cost, ns
Single-module protocol (32-bit)	68	2446	4100	2109
The first set (17-bit)	36	2223	3671	1615
The second set (11-bit)	18	2182	3490	1334
The third set (9-bit)	11	2154	3403	1185
The fourth set (6-bit)	5	2128	3366	1060

Based on the analysis of the data shown in Table 4, the following conclusions can be made. When the first set of RC's modules is used, the execution time of the second part of the authentication method is 1615 ns, which is reduced by 1.30 times compared to the single-module protocol. As with the execution of the second part of the developed authentication method, the decrease in the size of RC's modules has a positive effect on the time cost. Thus, when the second set of RC's modules is used, the execution time of the second part of the developed method is 1334 ns, which is 1.58 times less than for the single-module protocol. When the developed method is implemented using the third set of RC's modules, the execution time of the second part is 1185 ns, which is 1.77 times less than for the single-module protocol. The transition to 6-bit RC's modules (the fourth set) allows

us to reduce the execution time of the second part of the developed method to 1060 ns, which is 1.98 times less than for the single-module protocol [76].

Let's carry out a comparative analysis of the developed authentication method with the previously used zero-knowledge protocols in IIoT. Figure 2 shows the time cost of authentication using FFS protocol, single-module keyless protocol, and the developed zero-knowledge method with four sets of RC's modules.

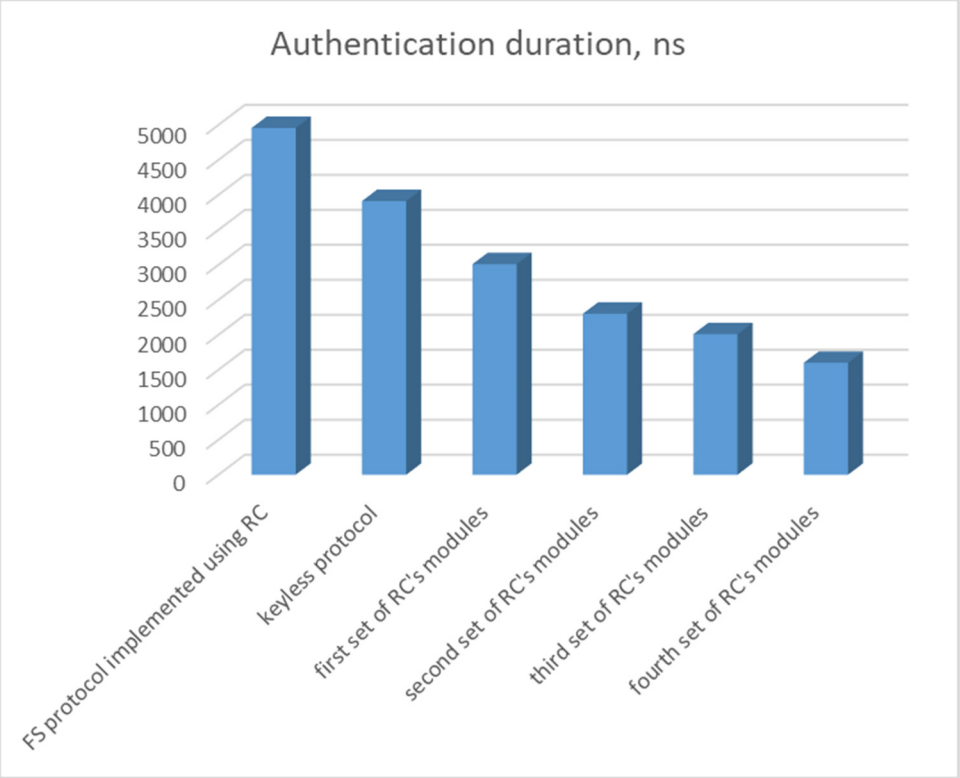

Figure 2. Time costs for authentication of the prover.

Figure 2 shows that the use of parallel computing based on RC allows to reduce the time cost of satellite authentication. Thus, implementing FS zero-knowledge authentication protocol allows to carry out authentication for 4957 ns. Authentication time is 3912 ns when a single-module zero-knowledge authentication protocol is used. There is a decrease in the time cost of satellite identification when the developed authentication method is used. The use of the first set of RC's modules reduces the authentication time to 3010 ns, which is 1.29 times less than in the case of using the single-module protocol. The use of the second set of RC's modules reduces the authentication time to 2302 ns, which is 1.69 times less than in the case of using the single-module protocol. The use of the third set of RC's modules reduces the authentication time to 2010 ns, which is 1.94 times less than in the case of using the single-module protocol. The use of the fourth set of RC's modules the authentication time to 1600 ns, which is 2.44 times less than in the case of using the single-module protocol.

Thus, the obtained research results showed that the implementation of the zero-knowledge authentication protocol using residue codes allows to reduce the time cost of satellite identification. It should be noted that the efficiency of the developed method will only increase with an increase in the size of the prover's signal. In this case, the correct choice of a set of RC's modules will allow to provide cryptographic strength of the developed method not less than the single-module authentication protocol. It is obvious that the application of the developed method leads to a reduction in time costs for authentication. As a result, the time interval for an intruder to guess the correct prover's signal is reduced. In this case, the probability of an intruder satellite imposing the

intercepted and delayed satellite signal is reduced. This will provide increased imitation resistance of low-orbit satellite internet to relay spoofing interference.

7. Conclusions

The emergence of low-orbit satellite internet (LOSI) was a qualitative leap in the expansion of IIoT technology applications in the oil and gas industry. The promising use of LOSI and IIoT is determined by the presence of large oil and gas deposits located on the Arctic Ocean shelf. ASRCOGFs are used for the effective development of these fields. Since the fields are located in hard-to-reach areas with difficult climatic conditions, most of the hydrocarbon production and transportation facilities will be unattended. Therefore, the efficiency of ASRCOGF's operation is largely determined by reliable and timely data exchange via LOSI. The expansion of the number of countries and corporations planning to develop hydrocarbon fields on the Arctic Ocean shelf leads to an increase in low-orbit satellite constellations. In this case, there may be a situation of effective attack of intruder satellites on the communication system used in IIoT technology. Studies have shown that LOSIS is susceptible to spoofing attacks. To prevent the possibility of relay spoofing interference, the article proposed the use of a satellite identification system. This system performs satellite authentication before starting a communication session. The session will be granted only if the satellite obtains "friend" status. In order to improve the efficiency of the satellite identification system, an analysis of cryptographic authentication protocols was carried out, which showed the promise of using zero-knowledge authentication protocols. Despite having high cryptographic strength, these protocols have a significant disadvantage—a large time cost for the authentication of the prover. To eliminate this disadvantage, the article proposed a method of authentication with zero-knowledge proof implemented using RC. The use of RC will reduce the authentication time by paralleling the calculations, which are performed independently on RC's modules. In this case, the choice of the correct set of RC's modules allows to provide cryptographic strength of the authentication method comparable to the single-module authentication protocol. The article presented a description of the developed zero-knowledge authentication method implemented using RC. A Kintex UltraScale FPGA (xcku3p-ffva676-1-e) was used to perform a comparative analysis to evaluate the effectiveness of the developed method. Analysis of the results of circuit modeling showed the prospects of using RC for satellite authentication. Thus, when a set of 6-bit RC's modules was used, the authentication time was reduced by 2.44 times compared to the single-module protocol [76]. At the same time, the efficiency of the developed method will only increase with an increase in the size of the prover's signal.

There are several prospective directions for the development of this scientific direction. Firstly, the independence of the computations performed on the MRRC's modules and the lack of data exchange between them are the basis for the construction of redundant RC. With the help of these codes, it is possible to detect and correct errors arising in the process of system functioning due to failures and malfunctions. That is, it is possible to increase the fault tolerance of the satellite authentication system at a lower hardware cost in comparison with the "2 of 3" method of structural redundancy. Secondly, redundant RCs can be used as error correction codes. In this case, it will be possible to give up the use of cascade codes, which will also reduce hardware costs for the implementation of the satellite authentication system.

Author Contributions: Conceptualization, I.A.K.; Data curation, I.A.K., A.A.O. and V.P.P.; Formal analysis, I.A.K.; Investigation, I.A.K., A.A.O. and N.K.C.; Methodology, I.A.K. and V.P.P.; Project administration, I.A.K.; Software, N.K.C. and D.V.D.; Supervision, I.A.K.; Validation, D.V.D. and N.I.K.; Visualization, D.V.D. and N.I.K.; Writing—original draft, I.A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Russian Science Foundation, grant number 23-21-00036, https://rscf.ru/en/project/23-21-00036/ (accessed on 15 June 2023).

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

References

1. Insider. What Is the Internet of Things? What IoT Means and How It Works. Available online: https://www.insiderintelligence.com/insights/internet-of-things-definition/ (accessed on 15 June 2023).
2. By 2025, Internet of Things Applications Could Have $11 Trillion Impact. Available online: https://www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact (accessed on 19 June 2023).
3. Khana, W.Z.; Rehmanb, M.H.; Zangoti, H.M. Industrial internet of things: Recent advances, enabling technologies and open challenges. *Comput. Electr. Eng.* **2020**, *81*, 106522. [CrossRef]
4. Zhu, C.; Rodrigues, J.J.P.C.; Leung, V.C.M.; Shu, L.; Yang, L.T. Trust-based communication for the industrial internet of things. *IEEE Commun. Mag.* **2018**, *56*, 16–22. [CrossRef]
5. Mahdavi, M. Ushering in a new era of oilfield innovation with the Internet of Things. *J. Pet. Technol.* **2017**, *69*, 14–15. [CrossRef]
6. Konovalov, S. Addressing O & G big data challenges at the remote edge. In Proceedings of the SPE Digital Energy Conference and Exhibition 2015, The Woodlands, TX, USA, 3–5 March 2015; p. 5.
7. Ziatdinov, S.; Philip, T.T. Step Change Transformation of Legacy Rigs to Autonomous Drilling Rigs. In Proceedings of the Abu Dhabi International Petroleum Exhibition & Conference, Abu Dhabi, United Arab Emirates, 15–18 November 2021. [CrossRef]
8. Gul, S.; van Oort, E. A machine learning approach to filtrate loss determination and test automation for drilling and completion fluids. *J. Pet. Sci. Eng.* **2020**, *186*, 106727. [CrossRef]
9. Geng, H. *IoT Revolution in Oil and Gas Industry*; Wiley: New York, NY, USA, 2017; pp. 513–520. [CrossRef]
10. Gomez, E.; Ombe, E.; Goodkey, B.; Carvalho, R. Drilling Automation: The Step Forward for Improving Safety, Consistency, and Performance in Onshore Gas Drilling. In Proceedings of the SPE Middle East Oil & Gas Show and Conference, Sanabis, Bahrain, 28 November–1 December 2021. [CrossRef]
11. Gharibi, W.; Aalsalem, M.; Khan, W.Z.; Armi, N.; Ghribi, W. Monitoring gas and oil fields with reliable wireless sensing and Internet of Things. In Proceedings of the 2017 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), Jakarta, Indonesia, 23–24 October 2017; pp. 188–191.
12. Zhou, B.; Wang, Y.; Liu, W.; Liu, B. Identification of working condition from sucker-ROD pumping wells based on multi-view cotraining and hessian regularization of SVM. In Proceedings of the 14th IEEE International Conference on Signal Processing (ICSP), Beijing, China, 12–16 August 2018; pp. 969–973.
13. Sequera, N. Deployment of smart ultrasonic sensors for internal corrosion monitoring using Internet of Things. In Proceedings of the Annual Conference of the Australasian Corrosion Association, Sydney, Australia, 12–15 November 2017.
14. Gulve, S.P.; Khoje, S.A.; Pardeshi, P. Implementation of IoT-based smart video surveillance system. In *Computational Intelligence in Data Mining*; Springer: Singapore, 2017; pp. 771–780.
15. Sun, J.; Zhang, Z.; Sun, X. The intelligent crude oil anti-theft system based on IoT under different scenarios. *Procedia Comput. Sci.* **2016**, *96*, 1581–1588. [CrossRef]
16. Syreyshchikova, N.V.; Pimenov, D.Y. The State of Occupational Health and Safety Management Frameworks (OHSMF) and Occupational Injuries and Accidents in the Ghanaian Oil and Gas Industry: Assessing the Mediating Role of Safety Knowledge. *Procedia Manuf.* **2019**, *32*, 278–285. [CrossRef]
17. Baudoin, C.R. Deploying the industrial Internet in oil & gas: Challenges and opportunities. In Proceedings of the SPE Intelligent Energy International Conference and Exhibition, Aberdeen, UK, 6–8 September 2016; p. 11. [CrossRef]
18. Klein, L.; Ramachandran, M.; van Kessel, T.; Nair, D.; Hinds, N.; Hamann, H.; Sosa, N. Wireless sensor networks for fugitive methane emissions monitoring in oil and gas industry. In Proceedings of the IEEE International Congress on Internet of Things (ICIOT), San Francisco, CA, USA, 2–7 July 2018; pp. 41–48.
19. Bragattoa, P.; Faramondib, L.; Faillab, F.; Gnonic, M.G. Potential and limits of IoT for hazardous job in process industries. *Chem. Eng. Trans.* **2018**, *67*, 865–869.
20. Lipnicki, P.; Lewandowski, D.; Pareschi, D.; Pakos, W.; Ragaini, E. Future of IoTSP–IT and OT integration. In Proceedings of the IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, Spain, 6–8 August 2018; pp. 203–207.
21. Poddar, T. Digital twin bridging intelligence among man, machine, and environment. In Proceedings of the Offshore Technology Conference Asia, Kuala Lumpur, Malaysia, 19–23 March 2018; p. 4. [CrossRef]
22. Sharma, P.; Knezevic, D.; Huynh, P.; Malinowski, G. RB-FEA based digital twin for structural integrity assessment of offshore structures. In Proceedings of the Offshore Technology Conference, Houston, TX, USA, 30 April–3 May 2018; p. 6. [CrossRef]
23. Mohr, J.-P. *Digital Twins for the Oil and Gas Industry*; Hashplay, Inc.: San Francisco, CA, USA, 2018. [CrossRef]
24. Said, M.M.; Pilgrim, R.; Rideout, G.; But, S. Theoretical Development of a Digital-Twin Based Automation System for Oil Well Drilling Rigs. In Proceedings of the SPE Canadian Energy Technology Conference, Calgary, AB, Canada, 16–17 March 2022. [CrossRef]

25. Wang, G.; Saputra, J.F.G. Terminal automation system: Automation solution in the oil and gas industry. In Proceedings of the Indonesian Association for Pattern Recognition International Conference (INAPR), Jakarta, Indonesia, 7–8 September 2018; pp. 296–301.
26. Slaughter, A.; Bean, G.; Mittal, A. *Connected Barrels: Transforming Oil and Gas Strategies with the Internet of Things*; Accenture: Dublin, Ireland, 2015.
27. Qu, Z.; Zhang, G.; Cao, H.; Xie, J. LEO satellite constellation for internet of things. *IEEE Access* **2017**, *5*, 18391–18401. [CrossRef]
28. Marchese, M.; Moheddine, A.; Patrone, F. IoT and UAV Integration in 5G Hybrid Terrestrial-Satellite Networks. *Sensors* **2019**, *19*, 3704. [CrossRef]
29. Qian, Y.; Ma, L.; Liang, X. The Performance of Chirp Signal Used in LEO Satellite Internet of Things. *IEEE Commun. Lett.* **2019**, *23*, 1319–1322. [CrossRef]
30. Qian, Y.; Ma, L.; Liang, X. Symmetry chirp spread spectrum modulation used in LEO satellite Internet of Things. *IEEE Commun. Lett.* **2018**, *22*, 2230–2233. [CrossRef]
31. National Petroleum Council. Arctic Potential: Realizing the Promise of U.S. Arctic Oil and Gas Resources. Available online: https://www.npcarcticreport.org (accessed on 20 June 2023).
32. Schlumberger Limited (SLB). Available online: https://www.slb.com (accessed on 20 June 2023).
33. Kalyani, P. Internet from Sky: Starlink. *Proc. IEEE* **2021**, *8*, 2394–8124.
34. Oughton, E.J. A Techno-Economic Framework for Satellite Networks Applied to Low Earth Orbit Constellations Assessing Starlink, OneWeb and Kuiper. *IEEE Access* **2021**, *9*, 141611–141622.
35. HS, S.; Supreeth, M. Starlink Satellite Internet Service. *Int. J. Res. Publ. Rev.* **2022**, *3*, 4501–4504.
36. Fu, X.; Graham, B.; Bettati, R.; Zhao, W.; Xuan, D. Analytical and Empirical Analysis of Countermeasures to Traffic Analysis Attacks. In Proceedings of the International Conference on Parallel Processing, Kaohsiung, Taiwan, 6–9 October 2003; pp. 483–492.
37. Kiraly, C.; Bianchi, G. Traffic Masking in IPsec: Architecture and Implementation. In Proceedings of the 16th IST Mobile and Wireless Communications Summit, Budapest, Hungary, 1–5 July 2007. [CrossRef]
38. *ISO/IEC 29192-2:2019*; Lightweight Cryptography—Part 2: Block Ciphers. ISO: Geneva, Switzerland, 2012.
39. *ISO/IEC 29192-3:2019(E)*; Security Techniques—Lightweight cryptography—Part 3: Stream Ciphers. ISO: Geneva, Switzerland, 2012.
40. Choon, J.C.; Hee Cheon, J. *An Identity-Based Signature from Gap Diffie-Hellman Groups*; Desmedt, Y.G., Ed.; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2567, pp. 18–30.
41. Fang, W.D.; Chen, W.; Zhang, W.X.; Pei, J.; Gao, W.; Wang, G. Digital signature scheme for information non-repudiation in blockchain: A state-of-the-art review. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 56. [CrossRef]
42. Huang, K.; Zhang, X.; Mu, Y.; Rezaeibagha, F.; Du, X. Scalable and redactable blockchain with update and anonymity. *Inf. Sci.* **2021**, *546*, 25–41. [CrossRef]
43. Li, C.; Tian, Y.; Chen, X.; Li, J. An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems. *Inf. Sci.* **2020**, *546*, 253–264. [CrossRef]
44. Manzoor, A.; Braeken, A.; Kanhere, S.S.; Ylianttila, M.; Liyanage, M. Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. *J. Netw. Comput. Appl.* **2020**, *176*, 102917. [CrossRef]
45. Hwang, M.-S.; Yang, C.-C.; Shiu, C.-Y. An authentication scheme for mobile satellite communication systems. *ACM Oper. Syst.* **2003**, *37*, 42–47. [CrossRef]
46. Murtaza, A.; Xu, T.; Pirzada, J.; Liu, J. A Lightweight Authentication and Key Sharing Protocol for Satellite Communication. *Int. J. Comput. Commun. Eng.* **2020**, *9*, 46–53. [CrossRef]
47. Zhang, Y.; Zhai, Z. An efficient and provably secure key agreement scheme for satellite communication systems. *PLoS ONE* **2021**, *16*, e0250205. [CrossRef] [PubMed]
48. Chang, C.-C.; Cheng, T.-F.; Wu, H.-L. An authentication and key agreement protocol for satellite communications. *Int. J. Commun. Syst.* **2014**, *27*, 1994–2006. [CrossRef]
49. Farash, M.S.; Attari, M.A. An efficient client–client password-based authentication scheme with provable security. *J. Supercomput.* **2014**, *70*, 1002–1022. [CrossRef]
50. Yang, Q.; Xue, K.; Xu, J.; Wang, J.; Li, F.; Yu, N. Anfra: Anonymous and fast roaming authentication for space information network. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 486–497. [CrossRef]
51. Li, L.; Kou, X.; Yin, H.; Chen, K. Design of a high-speed anti-blocking wideband receiver front-end. In Proceedings of the 2020 International Conference on Microwave and Millimeter Wave Technology (ICMMT), Shanghai, China, 20–23 September 2020. [CrossRef]
52. Sineglazov, V.M.; Tkachenko, O.Y. Intellectual two-level system of electronic warfare with UAVs. *Electron. Control. Syst.* **2015**, *4*, 22–26. [CrossRef]
53. Basholli, F. Electronic interference and protection from it. In Proceedings of the 5th Advanced Engineering Days (AED), Mersin, Türkiye, 3 December 2022; pp. 74–76.
54. Bose, S.C. GPS Spoofing Detection by Neural Network Machine Learning. *IEEE Aerosp. Electron. Syst. Mag.* **2021**, *37*, 18–31. [CrossRef]
55. Shuai, H.; Yu, Z.; Meng, W.; Cheng, L. GPS anti-spoofing technology based on RELAX algorithm in smart grid. In Proceedings of the 10th International Conference on Communications and Networking in China (ChinaCom), Shanghai, China, 15–17 August 2015.

56. Gregg, M.; Schneier, B. *Security Practitioner and Cryptography Handbook and Study Guide Set*; Wiley: New York, NY, USA, 2014; 1344p.
57. Schneier, B. *Applied Cryptography: Protocols, Algorithms and Source Code in C*; Wiley: New York, NY, USA, 2017; 784p.
58. Kang, J.; Park, G.; Park, J.H. Design of secure authentication scheme between devices based on zero-knowledge proofs in home automation service environments. *J. Supercomput.* **2016**, *72*, 4319–4336. [CrossRef]
59. Xiong, C. *Secured System Architecture for the Internet of Things Using a Two Factor Authentication Protocol*; University of Ottawa: Ottawa, ON, Canada, 2020; 144p.
60. Soewito, B.; Marcellinus, Y. IoT security system with modified Zero Knowledge Proof algorithm for authentication. *Egypt. Inform. J.* **2021**, *22*, 269–276. [CrossRef]
61. Song, J.; Harn, P.-W.; Sakai, K. An RFID Zero-Knowledge Authentication Protocol Based on Quadratic Residues. *IEEE Internet Things J.* **2022**, *9*, 12813–12824. [CrossRef]
62. Liu, H.; Ning, H. Zero-Knowledge Authentication Protocol Based on Alternative Mode in RFID Systems. *IEEE Sens. J.* **2011**, *11*, 3235–3245. [CrossRef]
63. Debiao, H.; Sherali, Z. An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography. *IEEE Internet Things J.* **2014**, *2*, 72–83.
64. Chistousov, N.K.; Kalmykov, I.A.; Dukhovnyj, D.V.; Kalmykov, M.I.; Olenev, A.A. Adaptive Authentication Protocol Based on Zero-Knowledge Proof. *Algorithms* **2022**, *15*, 50. [CrossRef]
65. Kang, J.; Elmehdwi, Y.; Lin, D. SLIM: Secure and Lightweight Identity Management in VANETs with Minimum Infrastructure Reliance. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Singapore, 8–10 August 2018; Volume 238, pp. 823–837.
66. Hegde, N.; Manvi, S.S. MFZKAP: Multi Factor Zero Knowledge Proof Authentication for Secure Service in Vehicular Cloud Computing. In Proceedings of the 2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP), Gangtok, India, 25–28 February 2019; pp. 1–6.
67. Fiat, A.; Shamir, A. How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Advances in Cryptology—CRYPTO' 86*; Springer: Berlin/Heidelberg, Germany, 2000; pp. 186–194. [CrossRef]
68. Feige, U.; Shamir, A. Witness indistinguishable and witness hiding protocols. In Proceedings of the 22nd annual ACM symposium on Theory of Computing, Baltimore, MD, USA, 13–17 May 1990. [CrossRef]
69. Mohd, S.; Singh, K.; Bajuri, M.Y. A Secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario. *Sustain. Cities Soc.* **2021**, *75*, 103354.
70. Hanaoui, S.; Laassiri, J.; Berguig, Y. MULTI-AGENT Identity Combined Key Signature Authentication Protocol Based Schnorr Signature with Provable Security under AVISPA. *Int. J. Adv. Trends Comput. Sci. Eng.* **2020**, *9*, 5.
71. Okamoto, E.; Tanaka, K. Key Distribution System Based on Identification Information. *IEEE J. Sel. Areas Commun.* **1989**, *7*, 481–485. [CrossRef]
72. Gennaro, R.; Krawczyk, H.; Rabin, T. Okamoto-Tanaka Revisited: Fully Authenticated Diffie-Hellman with Minimal Overhead. In *Applied Cryptography and Network Security*; Zhou, J., Yung, M., Eds.; ACNS 2010. Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6123. [CrossRef]
73. Guillou, L.C.; Quisquater, J.J. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory. In *Advances in Cryptology—EUROCRYPT '88. EUROCRYPT 1988*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1988; Volume 330. [CrossRef]
74. Guillou, L.C.; Ugon, M.; Quisquater, J.-J. Cryptographic authentication protocols for smart cards. *Comput. Netw.* **2001**, *36*, 437–451. [CrossRef]
75. Sahl, A.N.; Samsudin, A.; Letchmunan, S. Visual Zero-Knowledge Proof of Identity Scheme by Using Color Images. *Middle-East J. Sci. Res.* **2014**, *21*, 1188–1196. [CrossRef]
76. Kalmykov, I.A.; Olenev, A.A.; Kalmykova, N.I.; Dukhovnyj, D.V. Using Adaptive Zero-Knowledge Authentication Protocol in VANET Automotive Network. *Information* **2023**, *14*, 27. [CrossRef]
77. Mohan, A. Residue Number Systems. In *Theory and Applications*; Springer International Publishing: Cham, Switzerland, 2016; 351p.
78. Mohan, P.V. Residue Number Systems. In *Algorithms and Architectures*; Springer: New York, NY, USA, 2002; 253p.
79. Omondi, A.; Premkumar, B. *Residue Number Systems: Theory and Implementation*; Imperial College Press: London, UK, 2007; 293p.
80. Kalmykov, I.A.; Pashintsev, V.P.; Tyncherov, K.T.; Olenev, A.A.; Chistousov, N.K. Error-Correction Coding Using Polynomial Residue Number System. *Appl. Sci.* **2022**, *12*, 3365. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.