cryptography

MDPI

Article

New Method of Prime Factorisation-Based Attacks on RSA Authentication in IoT

Sitalakshmi Venkatraman * and Anthony Overmars

School of Engineering, Construction & Design, Melbourne Polytechnic, Victoria 3181, Australia

* Correspondence: SitaVenkat@melbournepolytechnic.edu.au; Tel.: +61-3-9269-1171

Received: 30 June 2019; Accepted: 12 August 2019; Published: 15 August 2019

check for updates

Abstract: The potential benefits of the Internet of Things (IoT) are hampered by malicious interventions of attackers when the fundamental security requirements such as authentication and authorization are not sufficiently met and existing measures are unable to protect the IoT environment from data breaches. With the spectrum of IoT application domains increasing to include mobile health, smart homes and smart cities in everyday life, the consequences of an attack in the IoT network connecting billions of devices will become critical. Due to the challenges in applying existing cryptographic standards to resource constrained IoT devices, new security solutions being proposed come with a tradeoff between security and performance. While much research has focused on developing lightweight cryptographic solutions that predominantly adopt RSA (Rivest–Shamir–Adleman) authentication methods, there is a need to identify the limitations in the usage of such measures. This research paper discusses the importance of a better understanding of RSA-based lightweight cryptography and the associated vulnerabilities of the cryptographic keys that are generated using semi-primes. In this paper, we employ mathematical operations on the sum of four squares to obtain one of the prime factors of a semi-prime that could lead to the attack of the RSA keys. We consider the even sum of squares and show how a modified binary greatest common divisor (GCD) can be used to quickly recover one of the factors of a semi-prime. The method presented in this paper only uses binary arithmetic shifts that are more suitable for the resource-constrained IoT landscape. This is a further improvement on previous work based on Euler's method which is demonstrated using an illustration that allows for the faster testing of multiple sums of squares solutions more quickly.

Keywords: Internet of Things; IoT; security; cryptography; RSA keys; semi-prime; prime factorization; binary GCD; crypto attacks

1. Introduction

With the development of a variety of technologies such as sensors, actuators, controllers, mobile devices and cloud computing, the Internet of Things (IoT) is evolving to be a large network of networks connecting smart devices that are exponentially growing in the physical world [1]. By seamlessly interconnecting humans with such an intelligent physical world, the IoT brings about benefits in various domains such as public health, transportation, agriculture, energy management, and waste management that can lead to smart cities and homes [2,3]. While such smart devices have capabilities to collect and analyze huge data for decision-making, security is a major concern, as IoT attacks by perpetuators with malicious interventions are on the rise. Hence, secure authentication and authorization form a supreme requirement in an IoT system, as a malicious unauthenticated device could lead to severe damages to individuals and organisations [4,5]. More than the connectivity challenges for billions of devices to interact with humans and communicate with each other, with the IoT being exploited to become an attack tool, security challenges are becoming top priority in the recent research agenda [6,7]. In addition, due to the inherent resource limitations of IoT devices, traditional communication protocols and security schemes are either infeasible or ineffective. Recently, a security weakness discovered in a pacemaker device became a threat for a patient using it because the hacker of the device could take control of the patient's heart-beat. The impact of such a security breach can be life-threatening, and, hence, the US Food and Drug Administration (FDA) has recalled 500,000 pacemakers with identified security gaps [8].

The success of IoT-enabled technologies in the development of smart cities, smart homes and intelligent mobile-health systems depends on the robustness in IoT authentication and secure data transmission between the IoT nodes and servers [9,10]. The aim of IoT security solutions is to prevent the leakage of private information and harmful actuating activities. However, IoT devices suffer from security limitations due to their resource constrained attributes [11] such as:

- Power and energy consumption.
- Communication bandwidth.
- Memory capacity (e.g., RAM (Random-access memory), Flash).
- Size and complexity (e.g., display, storage, gate count, I/O (Input/output) pin count).
- Lack of user interface.
- Short device lifetime.

Due to the inherent limitations of the IoT devices, they are susceptible to be captured by an adversary, since traditional authentication schemes are infeasible and cannot be practically deployed in resource constrained IoT environment. Existing solutions such as public-key-based authentication, identity-based authentication, encryption, and digital signature require suitable adaptation depending on the security needs of the IoT device application [12,13]. The RSA (Rivest–Shamir–Adleman), named after its inventors, is well known among all the public key algorithms due the difficulty in finding its public and private keys that consist of prime factors of a large number (semi-prime) [14,15]. However, due to the specific requirements of IoT devices, such traditional authentication schemes that are designed for high processing and large memory devices cannot be easily re-designed to suit the resource constrained IoT nodes. Hence, the need for lightweight security solutions has been realized for ensuring the security requirements of an IoT network. In particular, authentication is considered as a key requirement, since trusted access to the IoT device is crucial for the well-functioning of the network. Further, many existing solutions for IoT security are cloud-based and are susceptible to internet prone vulnerabilities [16]. The entire IoT network could be brought down by a malicious attack or even a single compromised node [17,18]. While the emergence of lightweight authentication schemes or cryptography is on the rise, researchers are still at the first step of evaluating the proposed authentication protocols in terms of their strengths and weaknesses [19]. Overall, the main challenges identified are heterogeneity, scalability, and inter-operability as new IoT devices and network protocols are introduced in open environments.

Recently, IoT devices are being embedded with several lightweight block ciphers, which has resulted in the need to ensure the security of the secret/sensitive cryptographic keys within the device throughout its life cycle [20,21]. Today, RSA is adopted for several purposes such as key exchange, digital signatures, or even the encryption of small blocks of data (block ciphers) [12]. The key-pair of RSA that uses a variable size encryption block and a variable size key is derived from a very large number (a semi-prime). If this large number is known, determining the two prime factors is computationally difficult. This property can be used as a secure communications channel in the IoT to openly publish the "public" key to anyone wishing to send a secure message, since someone who knows the prime factors can only decrypt the message. Such a secure communication channel can be used to share keys for lightweight cryptographic algorithms that are still very robust but require less computing power than the public key cryptosystems [22]. Hence, many algorithms to factor large numbers for attacking schemes such as RSA are gaining attention [23–25]. This motivates our research to identify the limitations of RSA-based lightweight block ciphers for IoT authentication requirements. A device could be active for several years since it is manufactured, and, during its life span, it is important to identify its safety zone before it can be physically accessible by attackers. To address this problem, we analyze the level of resistance of RSA against malicious attacks by proposing a new method of factorization of semi-primes and determining its practical implementation feasibility.

In this paper, we first present a review of RSA-based IoT authentication schemes. Next, we discuss the attacking techniques adopted in the four layers of IoT architecture and how our research fits in. Finally, we propose a new method to perform resource-efficient semi-prime factorization that could lead to RSA attacks using practical illustrations. Then, we provide mathematical proof of its improvement over previous work before concluding the paper with future research directions.

2. RSA-Based Authentication Schemes for the IoT

The aim of a cryptosystem is to encrypt a message before it is transmitted so that only the authenticated user who has the right key to decrypt would be able to read the message while preserving its confidentiality and integrity throughout the transmission process. Several cryptosystems are widely used in computer networks with a common goal to protect private communications. A number of ciphers have been developed, such as the Data Encryption Standard (DES), Ron Rivest, Adi Shamir and Leonard Adleman (RSA) [26]. RSA is one of the widely used public-key cryptosystems, and it is based on the practical difficulty of finding the factors of a semiprime number. In general, a key pair consisting of the public key and the private key can be easily generated for encryption and decryption. While the public key is publicly made available, the private key is maintained as a secret. The public key is generally used for two main purposes: (i) For the public-key encryption of a message into a cipher text that can be decrypted only with the corresponding private key, and (ii) for exchanging digital signatures, wherein a cipher text generated with the private key can be decrypted by anyone who has access to the public key. Therefore, RSA-based security schemes are popularly used to protect confidential information and communications while also authenticating the senders and receivers of the information to be securely shared. However, the security strength of RSA depends on the difficulty to determine a private key from its public key, and, therefore, deciding on the length of the private key plays an important factor for securing the system from attacks that can decode the message [27]. A large key size of RSA increases the level of security but slows down the algorithm due to expensive computation costs. RSA encryption is an expensive operation; in the IoT, however, it is commonly used to pass encrypted shared keys for symmetric key cryptography,

It has become a clear requirement in the IoT landscape that calls for a lightweight key distribution method using the public key to securely communicate between nodes and the IoT infrastructure in order to reduce computational costs. Encryption algorithms such as the Advanced Encryption Standard (AES) established by the U.S. National Institute of Standards and Technology (NIST), RSA, and elliptical curve cryptography (ECC) cannot be deployed to an IoT device. Due to these limitations, the internet engineering task force (IETF) has considered the application of a Transport Layer Security (TLS), a Datagram Transport Layer Security (DTLS) and internet protocol security (IPSec) in IP-based networks [28]. The use of a DTLS to constrained application protocol (CoAP) is considered to be the key protocol in the IoT [29].

In recent years, NIST- approved cryptography algorithms have been adapted to fit into the limited resources of constrained IoT environments. However, their performance may not be acceptable, and NIST has described plans for the standardization of lightweight cryptographic algorithms [30]. Hence, the performance and security challenges in the IoT, such as storage cost and key management, form the prime motivation for recent research studies. Several lightweight authentication protocols as well as methods to include a one-time signature for multicast authentication have been proposed for smart grids [31–33]. Two-way IoT authentication schemes based on RSA with the use of the Trusted Platform Module (TPM) have been enhanced using the Datagram Transport Layer Security (DTLS) protocol with the exchange of certificates based on RSA [34]. A mutual authentication scheme was also proposed [35,36]. It consists of two stages: In the enrollment stage, every node is identified within the system; in the authentication stage, a number of handshake messages are exchanged between the end device and the server, resulting in a session key used for the secure communication. Recent research studies have proposed different protocols for different purposes: Diffie–Hellman for key agreement protocol, RSA and Advanced Encryption Standard (AES) for achieving message confidentiality, and hash-based message authentication code (HMAC) for maintaining message integrity. Even though traditional public key infrastructure (PKI) is not considered suitable for the IoT due to computation and communication costs, recent studies have proposed a lightweight PKI within IoT use cases, including efficient message transmission to ensure privacy and security [37,38]. Such novel schemes using customized data encapsulation could reduce both computation and communication overhead, thereby making RSA encryption viable for the IoT.

3. IoT Authentication Issues and Attacks

There are several IoT authentication challenges and issues that need to be understood before employing the right security solution that can dynamically vary with the situation [21,35]. Based on certain critical situations such as IoT health applications, frequent authorization and authentication are necessary and could dynamically vary, potentially resulting in changes to the authorization of IoT devices [2]. To address these issues, automated mutual authentication without user intervention is required in supporting users from remembering passwords for a large number of devices [39]. Additionally, due to the dynamic changes to the network environment under which the devices operate, unstable connectivity warrants adding and removing mobile devices from authentication/authorization systems which should be trusted and manageable in the IoT network. Various considerations for resource-constrained devices and scalability in IoT network architecture are essential [40,41]. In certain critical situations, the availability of IoT devices is as important as information protection and privacy. Hence, the availability of IoT authentication and authorization services should not be hampered by network attacks or internet disruptions. IoT security solutions should be easily deployable and manageable in local networks without having to depend too much on remote systems so that scalability within heterogeneous IoT networks could be achieved while protecting from various security risks.

Today, organisations are required to defend against cloud, mobile and IoT security attacks, in addition to risks caused by third-party users [42]. They need to identify and monitor the IoT devices connected to their networks as well as the IoT activities that require business information access and storage. Hence, there are serious security and privacy challenges that need to be addressed in order to make the IoT environment secure in an organisation. It is important to consciously understand that IoT devices are also required to be treated as entities similar to the users for operating within the organisation's network. The level of authorization/authentication should be determined for every IoT device so that customized security solutions are applied. Many attacks take place after launching the IoT authentication schemes without understanding what data are collected or shared by the devices, how sensitive they are, and who are authorized to share them while determining the device storage, access and decommissioning requirements. Some attacks are due to incomplete firmware updates [43,44]. Hence, it is also important to understand the attack techniques employed in the IoT environment in order to employ suitable IoT security measures.

The main types of IoT attacks are: (i) denial of service (DoS) attacks that can block the availability of IoT system or services so that the resources are completely exhausted; (ii) physical attacks that can tamper the device components bringing risks to the IoT systems; (iii) eavesdropping that can compromise confidentiality when there is unauthorized access of IoT end-nodes due to impersonation or man-in-the-middle (MITM) of a malicious entity in the IoT network [24]. In an MITM attack, the malicious user replaces the exchanged keys in the public key cryptosystem with its own key to establish a secure channel to gain access to private messages; (iv) access attacks that allow unauthorized entities to gain access to IoT systems or devices; and (v) other attacks, such as channel side attacks, firmware attacks, RAM attacks and ransomware. A knowledge of these attacks helps IoT system developers to employ security primitives, schemes and protocols to be customized to lightweight cryptography. Probabilistic key sharing mechanisms should include the pre-distribution of keys, shared-key discovery of its neighbours, and assigning them with path-keys [45]. Various policies should also be established for node-to-node authentication, key revocation and disabling of sensors when node-capture is detected.

The right IoT authentication schemes in each of the four layers of the IoT architecture, which is based on the Open Systems Interconnection (OSI) model, are selected depending on the security requirements for each of the four layers [10]. The users communicate with the IoT devices through an interface that is present within the application layer [7]. The security in this application layer depends on the application requirements and data sharing issues related to access control, data privacy and integrity are some of the important challenges to be addressed. In this layer, the security solution should take care of IoT authentication and key agreement, as well as policies around user password management and awareness training. The next layer, namely the network layer, is responsible for the secure data transmission in the IoT network via various wireless technologies such as Bluetooth, infrared, internet, and Wi-Fi as well as a wired connection to a local area network (LAN). Common security problems due to DoS, MITM, eavesdropping, etc., are applicable in this network layer, and due to the mobility of the nodes in an IoT network, this layer is more vulnerable to attacks. Illegal nodes joining and leaving the network without prior authentication could contribute to the major security problem in the network layer. The support layer works with both the application layer and the network layer, and it makes use of cloud computing and smart grids for various computation intensive processing and intelligence. This layer supports with massive data processing and hence can be used for generating keys for IoT authentication methods such as RSA. However, this layer is also susceptible to RSA and other authentication scheme attacks. The final layer, namely the perception/recognition layer uses wireless data communication to automatically identify physical devices using technologies such as radio frequency identification (RFID), Global Positioning System (GPS), Zigbee, Smart card and sensor networks [22]. The data transmitted through wireless sensor networks are also vulnerable to sensor attacks such as node-capture, DoS and fake nodes. Due to the limitations of memory, power and bandwidth, this layer requires lightweight security measures for practical implementations.

Overall, all the four layers of an IoT architecture are faced with IoT authentication issues, and the attack surface of the modern enterprise is expanding requiring a layer-based approach for ensuring message authentication and integrity in the IoT environment. The security scheme should be enforced during the entire life cycle of the device, including secure boot and access control. In the secure boot process, the cryptography allows an electronic device to start executing authenticated and trusted schemes of public-key-based signature verification such as lightweight RSA to operate [46,47]. However, the nodes still need protection from various run-time threats and attacks that require appropriate access control schemes. Different forms of resources and roles in the IoT should be authorized using public key cryptography schemes to verify the integrity and authenticity of data. The digital signature ensures message integrity and authenticity. While message integrity is guaranteed by message digest or a secure hash algorithm, the authenticity is guaranteed by the public-key-based signature scheme consisting of key pairs (with a private key stored secretly and one public key available publicly to anyone). These keys are semi-primes and for RSA-based lightweight cryptography, the security strength depends on how quickly the factorization of semi-primes can be computed. Popular methods using the sum of four squares can generate many correct solutions; however, only one of these leads to the factorization of semi-primes. The aim of this paper is to propose a new correct factorisation method that could be employed for breaking RSA-based lightweight keys. Hence, to determine the limitations of RSA authentication in the IoT, in the next section, we propose a semi-prime factorization method using illustrations of breaking the lightweight cryptographic keys and also mathematically prove its efficiency.

4. Proposed Semi-Prime Factorisation Method Using Illustrations

Lightweight cryptography, a subfield of cryptography, aims to provide security solutions tailored to resource-constrained devices. A significant amount of work has been done by the academic community to introduce new lightweight algorithms and protocols. These complex cryptographic algorithms involve a great deal of mathematics at the core that can even be buried inside the electronic devices within the IoT. While mathematics is used to create difficult-to-break cryptographic functions, it has been proven that mathematics could also be used to break cryptographic keys, provided we can determine the two prime factors computationally fast enough. This forms the prime motivation to propose a fast semi-prime factorisation method using mathematical operations [48–50]. Currently, the RSA encryption algorithm is one of the most secure methods to transmit messages over the internet. The RSA cryptosystem uses a public key and a private key, and these keys are semi-primes. For RSA-based lightweight cryptography, these key lengths have limitations and are vulnerable to factorisation attacks. Existing literature shows that a semi-prime can be expressed as a sum of four squares and that fast factorisation methods exist [51,52]. We identify the limitations of the four squares method using illustrations in Case 1 and 2.

The four squares method generates many solutions of four squares; however, only one solution exists that will provide a factorization. Therefore, a fast method for testing a sum of four squares to determine its suitability as the correct factorization solution should be done as efficiently (quickly) as possible. We propose an enhanced method in this work and demonstrate the implementation using illustrated examples and verify its efficiency mathematically. By comparing three cases, the efficiency of our proposed method is demonstrated using an illustration in Case 3.

Case 1. Consider a semi-prime, N = 169, which could be used to generate a lightweight cryptographic key in an RSA algorithm. This semi-prime can be expressed as the sum of four squares:

$$169 = 13^2 = \left(2^2 + 3^2\right)\left(2^2 + 3^2\right) = 4^2 + 6^2 + 6^2 + 9^2 = 4^2 + 4^2 + 4^2 + 11^2$$

The Brahmagupta–Fibonacci identity expresses the product of two sums of two squares as a sum of two squares in two different ways as follows:

$$N = p_1 p_2 = \left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ad - bc)^2$$

Applying the Brahmagupta–Fibonacci identity from above, we get

$$4^2 + 6^2 + 6^2 + 9^2 = (9 - 4)^2 + (6 + 6)^2 = 5^2 + 12^2 = (9 + 4)^2 + (6 - 6)^2 = 13^2 + 0^2 = 13^2$$

$$4^2 + 4^2 + 4^2 + 11^2 \neq (11 - 4)^2 + (4 + 4)^2 = 7^2 + 8^2 = 113 \neq 169$$

$$4^2 + 4^2 + 4^2 + 11^2 \neq (11 + 4)^2 + (4 - 4)^2 = 15 + 0^2 = 225 \neq 169$$

Case 2. Consider a semi-prime, N = 377, which could be used to generate a lightweight cryptographic key in an RSA algorithm. This semi-prime can be expressed as the sum of four squares:

$$377 = (13)(29) = \left(2^2 + 3^2\right)\left(2^2 + 5^2\right) = 4^2 + 6^2 + 10^2 + 15^2$$

Applying the Brahmagupta–Fibonacci identity provides the two sums of squares.

$$377 = 4^2 + 6^2 + 10^2 + 15^2 = (15 - 4)^2 + (10 + 6)^2 = 11^2 + 16^2 = (15 + 4)^2 + (10 - 6)^2 = 19^2 + 4^2$$

$$377 = 4^2 + 19^2 = 11^2 + 16^2$$

Once the two sums of two squares are known, the prime factors can be found using a modified Euler factorisation.

$$\Delta e = 16 - 4 = 12, \Delta o = 19 - 11 = 8, g = \gcd(8, 12) = 4, p_1 = \left(\frac{8}{4}\right)^2 + \left(\frac{12}{4}\right)^2 = 13$$

However, in this case, there are nine sums of four squares.

$$(1,4,6,18),(1,6,12,14),(2,2,12,15),(2,6,9,16),(4,6,6,17),(4,6,10,15),(5,8,12,12),(6,6,7,16),(6,8,9,14)$$

Only one of these is applicable to the Brahmagupta–Fibonacci identity, providing the two sum of two squares.

A faster method, using a modified binary greatest common divisor, quickly validates a sum of four squares.

$$(4,6,10,15) = 15, 2(5,2,3) \Rightarrow (5,2),(2,3) \Rightarrow \left(2^2+5^2\right)\left(2^2+3^2\right) = (29)(13) = 377$$

This requires sums of four squares to be found until the correct sum of four squares is factored.

Case 3. Consider a semi-prime used to generate a lightweight cryptographic key in an RSA algorithm: $N = 1445897$.

This semi-prime can be expressed as the sum of four squares:

$$1445897 = 120^2 + 224^2 + 555^2 + 1036^2(120,224,555,1036)$$

Consider the odd square and re-order the squares:

$$(120,224,555,1036) = (555,120,224,1036)$$

Divide the remaining even squares by two until an odd square results and factor this out.

$$(555,120,224,1036) = (555,4(30,56,259))$$

Consider the odd square and re-order the squares:

$$(555,4(30,56,259)) = (555,4(259,30,56)$$

Divide the remaining even squares by two until an odd square results and factor this out.

$$(555,4(30,56,259)) = (555,4(259,2(15,28))$$

This is considered to be the solution, and the remaining odd/even pair is a factor of the semi-prime.

$$1445897 = (555,4(259,2(15,28)) \Rightarrow p_1 = 15^2 + 28^2 = 1009$$

The solution can be tested by a division.

$$p_2 = \frac{1445897}{1009} = 1433$$

4.1. Proposed Factorisation Implementation Using Binary Greatest Common Divisor (GCD)

We adopted Stein's binary greatest common divisor (GCD) algorithm that computes the greatest common divisor of two nonnegative integers using simpler arithmetic shifts, comparisons, and subtraction operations that provide much faster computations [53]. For the purpose of illustration, let us consider the semi-prime given below.

Consider the semi-prime, $N = 1445897 = (555,4(259,2(15,28))$

The implementation of our proposed factorisation method using the GCD function is provided here.

1. Test least significant bit (LSB)				
555	1000101011_2	1000101001 | 1	*Delete*	
2. Shift right until LSB set				
1036	10000001100_2	100000011 | 00	*Delete*	
3. Shift right until LSB set				
224	11100000_2	11100 | 000	11100_2	28_D
120	1111000_2	1111 | 000	1111_2	15_D
4. Sum squares				
28^2	15^2	$p_1 = 1009$		
5. Division				
$\frac{1445897}{1009}$		$p_2 = 1433$		

$$555 = 1000101011_2 = 10001010 \mid 0111036 = 10000001100_2 = 10000001 \mid 100$$

$$224 = 11100000_2 = 11100 \mid 000 \Rightarrow 11100_2 = 28_D$$

$$120 = 1111000_2 = 1111 \mid 000 \Rightarrow 1111_2 = 15_D$$

$$28^2 + 15^2 = 1009, p_1 = 1009, p_2 = \frac{1445897}{1009} = 1433$$

The above example, whilst illustrating the basic principle, is a special case, as one of the factors of the two squares is a higher power of 2^n than the other, such that $1433 = 8^2 + 37^2$.

The factor $8 = 1000_2 = 2^3 and 28 = 11100_2 = 2^4 + 2^3 + 2^2$ is such that $2^2 < 2^3$, so the shift right leaves a unique factor.

Consider the semi-prime, 6401.

This can be expressed as $6401 = 2^2 + 12^2 + 13^2 + 78^2 = (2, 12, 13, 78) = (13, 2(1, 6, 39))$.

This cannot be reduced further and has three terms (not two). However, upon quick inspection $p_1 = 1^2 + 6^2 = (1, 6) = 37$ and $p_2 = 157$.

Note that the $\mathrm{GCD}(1, 6) = 1 \Rightarrow \left(\frac{1}{1}, \frac{6}{1}\right) = (1, 6) = 37$ and $\gcd(6, 39) = 3 \Rightarrow \left(\frac{6}{3}, \frac{39}{3}\right) = (2, 13) = 173$. Consider the semi-prime, 5809.

$$5809 = (6, 11, 36, 66) = (11, 2(3, 18, 33)).$$

$$\mathrm{GCD}(3, 18) = 3 \Rightarrow \left(\frac{3}{3}, \frac{18}{3}\right) = (1, 6) \Rightarrow p_1 = 37,\ GCD = 3 \Rightarrow \left(\frac{18}{3}, \frac{33}{3}\right) = (6, 11) = 157.$$

Note that, to factorize the semi-prime, only one of the GCD functions needs to be determined.

This, in essence demonstrated the working of our proposed semi-prime factorisation method using binary GCD.

4.2. Mathematical Proof for Efficiency

Revisiting the RSA algorithm, we have N to be a product of two prime numbers ($N = p_1 p_2$) and a semi-prime [54,55]. Previous research [52,56] showed that one of the primes p_2 can be derived as follows:

$$N = p_1 p_2 = \left(a^2 + b^2\right)\left(c^2 + d^2\right)$$

If this specific sum of four squares is known, then

$$N = (ac)^2 + (bc)^2 + (ad)^2 + (bd)^2 = (ad \pm bc)^2 + (bd \mp ac)^2$$

Then by considering the parity

$$N = (ad + bc)^2 + (bd - ac)^2 = (ad - bc)^2 + (bd + ac)^2 = odd_1^2 + even_1^2 = odd_2^2 + even_2^2$$
$$\Delta o = odd_1 - odd_2, \Delta e = even_1 - even_2, g = \mathrm{GCD}(\Delta o, \Delta e)$$

It can be shown that one of the primes, p_2 can be represented as:

$$p_2 = \left(\frac{\Delta o}{g}\right)^2 + \left(\frac{\Delta e}{g}\right)^2, p_1 = \frac{N}{p_2}.$$

If $N = (ac, bc, ad, bd)$ are known, this can be summarised by the following steps:
Definition: $odd_n o_n, even_n e_n$

1. $(ad + bc)^2 + (bd - ac)^2 = (ad - bc)^2 + (bd + ac)^2 = o_1^2 + e_1^2 = o_2^2 + e_2^2$
2. $\Delta o = o_1 - o_2, \Delta e = e_1 - e_2, g = \text{GCD}(\Delta o, \Delta e)$
3. $p_2 = \left(\frac{\Delta o}{g}\right)^2 + \left(\frac{\Delta e}{g}\right)^2, p_1 = \frac{N}{p_2}$

By performing a comparative analysis of Cases 2 and 3 described above, the new method can be summarised as follows:

1. $N = (a, b, c, d) = (o_1, e_2, e_3, e_4) = (o_1, 2^m(o_2, e_5, e_6))$
2. $g = \text{GCD}(o_2, e_5)$
3. $p_2 = \left(\frac{o_2}{g}\right)^2 + \left(\frac{e_5}{g}\right)^2, p_1 = \frac{N}{p_2}$

OR best case scenario

1. $N = (a, b, c, d) = (o_1, e_2, e_3, e_4) = (o_1, 2^m(o_2, 2^n(o_3, e_5))$
2. $p_2 = (o_3)^2 + (e_5)^2,\ p_1 = \frac{N}{p_2}$

In general, the number of operations of a factorisation algorithm determines its computational complexity [57]. RSA encryption keys are developed and used in practical deployments, since existing algorithms are not able to solve the factorisation problem in polynomial time [58]. It is clear from the above mathematical proof that our new method is significantly faster by testing possible sum of squares as solutions to $N = p_1 p_2$, and this could lead to possible RSA key attacks in the IoT.

5. Conclusions and Future Work

This paper presented the importance of security requirements in the IoT and the applicability of RSA-based lightweight cryptography. A review of recent works related to RSA authentication in the IoT environment was provided. We identified the IoT authentication issues and attacks possible at the four layers of IoT architecture by identifying the associated vulnerabilities of the cryptographic keys that are generated using semi-primes. We proposed a semi-prime factorisation method of lightweight RSA keys by employing simple mathematical operations such as modified binary greatest common divisor and binary arithmetic shifts that are more suitable for the resource-constrained IoT context. We demonstrated the implementation steps using suitable semi-prime examples and proved its efficiency mathematically. This ongoing research provides scope for addressing the open issues and in identifying limitations of IoT authentication schemes for IoT networks and applications. Future work would involve further mathematical investigations by considering a hybrid factorization method using Lebesgue's identity along with Fermat's factorization in order to arrive at a reduction in the sum of four squares.

Author Contributions: Conceptualization, S.V. and A.O.; methodology, S.V. and A.O.; validation, A.O.; resources, S.V.; data curation, A.O.; writing—original draft preparation, S.V. and A.O.; writing—review and editing, S.V.

Funding: This research received no external funding.

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

References

1. Rajakumari, S.; Azhagumeena, S.; Devi, A.B.; Ananthi, M. Upgraded living think-IoT and big data. In Proceedings of the 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 23–24 February 2017.
2. Dineshkumar, P.; SenthilKumar, R.; Sujatha, K.; Ponmagal, R.; Rajavarman, V. Big data analytics of IoT based Health care monitoring system. In Proceedings of the 2016 IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics Engineering (UPCON), Varanasi, India, 9–11 December 2016.
3. Liu, R.; Wang, J. Internet of Things: Application and Prospect. In *MATEC Web of Conferences*; Zhao, L., Xavior, A., Cai, J., You, L., Eds.; EDP Sciences France: Les Ulis, France, 2017; Volume 100, p. 02034.
4. Sen, S.; Koo, J.; Bagchi, S. TRIFECTA: Security, Energy Efficiency, and Communication Capacity Comparison for Wireless IoT Devices. *IEEE Internet Comput.* **2018**, *22*, 74–81. [CrossRef]
5. McAfee. *McAfee Labs Threats Report*; Technical Report; McAfee: Santa Clara, CA, USA, 2017.
6. Wu, M.; Lu, T.J.; Ling, F.Y.; Sun, J.; Du, H.Y. Research on the architecture of Internet of Things. In Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China, 20–22 August 2010.
7. Nastase, L. Security in the Internet of Things: A Survey on Application Layer Protocols. In Proceedings of the 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 29–31 May 2017; pp. 659–666.
8. Hern, A. Hacking Risk Leads to Recall of 500,000 Pacemakers due to Patient Death Fears. The Guardian. 31 August 2017. Available online: https://www.google.com.hk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwjxjfnGs4TkAhWCfXAKHYvMAmIQFjACegQIARAB&url=https%3A%2F%2Fwww.theguardian.com%2Ftechnology%2F2017%2Faug%2F31%2Fhacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update&usg=AOvVaw1iTl1YppU9tgAM6Ex9rfHO (accessed on 14 August 2019).
9. Husamuddin, M.; Qayyum, M. Internet of Things: A study on security and privacy threats. In Proceedings of the 2017 2nd International Conferenceon Anti-CyberCrimes (ICACC), Abha, Saudi Arabia, 26–27 March 2017.
10. El Mouaatamid, O.; Lahmer, M.; Belkasmi, M. Internet of Things Security: Layered classification of attacks and possible Countermeasures. *Electron. J. Inf. Technol.* **2016**, *9*, 24–37.
11. Trappe, W.; Howard, R.; Moore, R.S. Low-energy security: Limits and opportunities in the Internet of things. *IEEE Secur. Privacy* **2015**, *13*, 14–21. [CrossRef]
12. Suárez-Albela, M.; Fraga-Lamas, P.; Fernández-Caramés, T.M. A Practical Evaluation on RSA and ECC-Based Cipher Suites for IoT High-Security Energy-Efficient Fog and Mist Computing Devices. *Sensors* **2018**, *18*, 3868. [CrossRef] [PubMed]
13. Gope, P.; Hwang, T. A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. *IEEE Trans. Ind. Electron.* **2016**, *63*, 7124–7132. [CrossRef]
14. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
15. Sun, H.M.; Wu, M.E.; Ting, W.C.; Hinek, M.J. Dual RSA and its Security Analysis. *IEEE Trans. Inf. Theory* **2007**, *53*, 2922–2933.
16. Zhou, L.; Li, X.; Yeh, K.H.; Su, C.; Chiu, W. Lightweight IoT-based authentication scheme in cloud computing circumstance. Future Gen. *Comput. Syst.* **2019**, *91*, 244–251.
17. Pammu, A.A.; Chong, K.S.; Ho, W.G.; Gwee, B.H. Interceptive side channel attack on AES-128 wireless communications for IoT applications. In Proceedings of the 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Jeju, Korea, 25–28 October 2016.
18. Choi, J.; Kim, Y. An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system. In Proceedings of the 2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), Jeju, Korea, 13–16 December 2016.
19. El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* **2019**, *19*, 1141. [CrossRef]
20. Abomhara, M.; Koien, G.M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *J. Cyber Secur. Mobil.* **2015**, *4*, 65–88. [CrossRef]

21. Wen, Q.; Dong, X.; Zhang, R. Application of dynamic variable cipher security certificate in Internet of Things. In Proceedings of the 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, Hangzhou, China, 30 October–1 November 2012.
22. Ye, N.; Zhu, Y.; Wang, R.C.; Malekian, R.; Qiao-min, L. An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things. *Appl. Math. Inf. Sci.* **2014**, *8*, 1617–1624. [CrossRef]
23. Aboud, S.J. An efficient method for attack RSA scheme. In Proceedings of the ICADIWT 2nd International Conference, London, UK, 4–6 August 2009; pp. 587–591.
24. Cekerevac, Z.; Dvorak, Z.; Prigoda, L.; Cekerevac, P. Man in the Middle Attacks and the Internet of Things—Security and economic risks. *FBIM Trans.* **2017**, *5*, 25–35. [CrossRef]
25. Haddad, Z.J.; Taha, S.; Saroit, I.A. Anonymous authentication and location privacy preserving schemes for LTE-A networks. *Egypt. Inform. J.* **2017**, *18*, 193–203. [CrossRef]
26. Schneier, B. *Applied Cryptography*, 2nd ed.; John Wiley & Sons, Inc.: New York, NY, USA, 1996.
27. Da Silva, J.C.L. Factoring Semi primes and Possible Implications. In Proceedings of the 26th IEEE Convention in Israel, Eliat, Israel, 17–20 November 2010; pp. 182–183.
28. Raza, S.; Voigt, T.; Jutvik, V. Lightweight ikev2: A key management solution for both the compressed IPsec and the IEEE 802.15. 4 security. In Proceedings of the IETF Workshop on Smart Object Security, Paris, France, 23 March 2012.
29. Raza, S.; Shafagh, H.; Hewage, K.; Hummen, R.; Voigt, T. Lithe: Lightweight secure CoAP for the internet of things. *IEEE Sens. J.* **2013**, *13*, 3711–3720. [CrossRef]
30. Barker, E. Recommendation for Key Management —Part 1: General, NIST Special Publication 800-57: Part 1 (Revision 4). January 2016. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf (accessed on 14 August 2019).
31. Mahmood, K.; Chaudhry, S.A.; Naqvi, H.; Shon, T.; Ahmad, H.F. A lightweight message authentication scheme for Smart Grid communications in power sector. *Comput. Electr. Eng.* **2016**, *52*, 114–124. [CrossRef]
32. Chim, T.W.; Yiu, S.M.; Li, V.O.; Hui, L.C.; Zhong, J. PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid. *IEEE Trans. Dependable Secur. Comput.* **2015**, *12*, 85–97.
33. Li, Q.; Cao, G. Multicast Authentication in the Smart Grid with One-Time Signature. *IEEE Trans. Smart Grid* **2011**, *2*, 686–696. [CrossRef]
34. Kothmayr, T.; Schmitt, C.; Hu, W.; Brünig, M.; Carle, G. DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Netw.* **2013**, *11*, 2710–2723. [CrossRef]
35. Huth, C.; Zibuschka, J.; Duplys, P.; Guneysu, T. Securing systems on the Internet of Things via physical properties of devices and communications. In Proceedings of the 2015 Annual IEEE Systems Conference (SysCon) Proceedings, Vancouver, BC, Canada, 13–16 April 2015.
36. Schmitt, C.; Noack, M.; Stiller, B. *TinyTO: Two-way authentication for constrained devices in the Internet of Things. Internet of Things*; Elsevier: Amsterdam, The Netherlands, 2016; pp. 239–258.
37. Hong, N. A Security Framework for the Internet of Things Based on Public Key Infrastructure. *Adv. Mater. Res.* **2013**, *671–674*, 3223–3226. [CrossRef]
38. Zhao, Y.L. Research on Data Security Technology in Internet of Things. *Appl. Mech. Mater.* **2013**, *433–435*, 1752–1755. [CrossRef]
39. Armando, A.; Basin, D.; Boichut, Y.; Chevalier, Y.; Compagna, L.; Cuellar, J.; Drielsma, P.H.; Heám, P.C.; Kouchnarenko, O.; Mantovani, J.; et al. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In *Computer Aided Verification*; Etessami, K., Rajamani, S.K., Eds.; Springer: Berlin/Heidelberg, Germany, 2005; pp. 281–285.
40. Tangade, S.; Manvi, S.S. Scalable and privacy-preserving authentication protocol for secure vehicular communications. In Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bangalore, India, 6–9 November 2016.
41. Chung, Y.; Choi, S.; Lee, Y.; Park, N.; Won, D. An Enhanced Lightweight Anonymous Authentication Scheme for a Scalable Localization Roaming Service in Wireless Sensor Networks. *Sensors* **2016**, *16*, 1653. [CrossRef] [PubMed]
42. Ahmed, M.E.; Kim, H. DDoS Attack Mitigation in Internet of Things Using Software Defined Networking. In Proceedings of the 2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService), San Francisco, CA, USA, 6–9 April 2017.

43. Na, S.; Hwang, D.; Shin, W.; Kim, K.H. Scenario and countermeasure for replay attack using join request messages in LoRaWAN. In Proceedings of the 2017 International Conference on Information Networking (ICOIN), Da Nang, Vietnam, 11–13 January 2017.
44. Anirudh, M.; Thileeban, S.A.; Nallathambi, D.J. Use of honeypots for mitigating DoS attacks targeted on IoT networks. In Proceedings of the 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 10–11 January 2017.
45. Bamasag, O.O.; Youcef-Toumi, K. Towards continuous authentication in Internet of things based on secret sharing scheme. In Proceedings of the WESS'15: Workshop on Embedded Systems Security, Amsterdam, The Netherlands, 4–9 October 2015.
46. Neto, A.L.M.; Souza, A.L.F.; Cunha, I.; Nogueira, M.; Nunes, I.O.; Cotta, L.; Gentille, N.; Loureiro, A.A.F.; Aranha, D.F.; Patil, H.K.; et al. AoT: Authentication and Access Control for the Entire IoT Device Life-Cycle. In Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM (ACM SenSys 2016), New York, NY, USA, 14–16 November 2016; pp. 1–15.
47. Wiener, M. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory* **1990**, *160*, 553–558. [CrossRef]
48. Weisstein, E.W. *Semiprime*; Wolfram Research, Inc.: Champaign, IL, USA, 2003.
49. Kaddoura, I.; Abdul-Nabi, S.; Al-Akhrass, K. New Formulas for Semi-Primes. Testing, Counting and Identification of the nth and next Semi-Primes. *arXiv* **2016**, arXiv:1608.05405.
50. Kostopoulos, G. An Original Numerical Factorization Algorithm. *J. Inf. Assur. Cyber Secur.* **2016**, *2016*, 775081. [CrossRef]
51. Pollard, J. Theorems on factorization and primality testing. *Proc. Camb. Philos. Soc.* **1974**, *76*, 521–528. [CrossRef]
52. Overmars, A.; Venkatraman, S. A Fast Factorisation of Semi-Primes Using Sum of Squares. *Math. Comput. Appl.* **2019**, *24*, 62. [CrossRef]
53. Stein, J. Computational problems associated with Racah algebra. *J. Comput. Phys.* **1967**, *1*, 397–405. [CrossRef]
54. Ambedkar, B.R.; Bedi, S.S. A New Factorization Method to Factorize RSA Public Key Encryption. *Int. J. Comput. Sci. Issues (IJCSI)* **2011**, *8*, 242–247.
55. Yan, S.Y. Factoring Based Cryptography. In *Cyber Cryptography: Applicable Cryptography for Cyberspace Security*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 217–286.
56. Overmars, A.; Ntogramatzidis, L.; Venkatraman, S. A new approach to generate all Pythagorean triples. *AIMS Math.* **2019**, *4*, 242–253. [CrossRef]
57. Karatsuba, A. The complexity of computations. *Proc. Steklov Inst. Math.* **1995**, *211*, 169–183.
58. Traversa, F.L.; di Ventra, M. Polynomial-time solution of prime factorization and NP-complete problems with digital memcomputing machines. *Chaos Interdiscip. J. Nonlinear Sci.* **2017**, *27*, 023107. [CrossRef] [PubMed]