sustainability

MDPI

Article

Biometrics-Based RSA Cryptosystem for Securing Real-Time Communication

Xiaolong Liu [1], Wei-Bin Lee [2,*], Quy-Anh Bui [2], Chia-Chen Lin [3,*] and Hsiao-Ling Wu [2]

[1] College of Computer and Information Sciences, Fujian Agriculture and Forestry University, Fuzhou 350002, China; xlliu@fafu.edu.cn
[2] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan; quanganhit@gmail.com (Q.-A.B.); wuhsiaoling590@gmail.com (H.-L.W.)
[3] Computer Science and Information Management, Providence University, Taichung 43301, Taiwan
* Correspondence: wblee@fcu.edu.tw (W.-B.L.); mhlin3@pu.edu.tw (C.-C.L.)

Received: 12 September 2018; Accepted: 3 October 2018; Published: 9 October 2018

Abstract: Real-time online communication technology has become increasingly important in modern business applications. It allows people to easily connect with business partners over the Internet through the camera lens on digital devices. However, despite the fact that users can identify and confirm the identity of the person in front of the camera, they cannot verify the authenticity of messages between communication partners. It is because the tunnel for the video is not the same as the tunnel that delivers the messages. To protect confidential messages, it is essential to establish a secure communication channel between users. This paper proposes a biometrics-based RSA cryptosystem to secure real-time communication in business. The idea put forward is to generate a cryptographic public key based on a user's biometric information without using Public Key Infrastructure (PKI) and establish a secured channel in a public network. In such a way, the key must be verified with the user's biometrics online. Since the key is derived from the user's biometrics, it is strongly user-dependent and works well to convince others of the authenticity of the owner. Additionally, the derived biometric key is self-certified with the user's biometrics, which means the cost of certificate storage, delivery and revocation can be significantly reduced.

Keywords: real-time communication; RSA cryptosystem; Public Key Infrastructure; identity authentication; secure business

1. Introduction

In the day-to-day workings of developed economies, this decade has already witnessed an extraordinary evolution in the technology of E-Commerce. Over the past decade, communication technology has become increasingly important in modern business applications. New electronic communications have made real-time online communication very common in E-Commerce, such as video conferencing, smart space and collaborative business [1–3]. Real-time online communication offers people a convenient communication channel and now people can easily contact others on the Internet anywhere and anytime [4]. Moreover, most people now have digital devices, which makes it even more convenient to connect with others. Most of these devices provide a camera that enables users to see the communication partners through camera lens. Nowadays, real-time online communication is a kind of face-to-face communication accompany message exchanging. For some real-time video communication situations, confidential and sensitive messages are usually conveyed between partners at the same time. For examples: in telemedicine [5], doctors diagnose patients' problem in real time video communication and the confidential medical information are exchanged simultaneously; in remote collaboration [6], valuable business information and documents are transmitted during

remote interaction. However, the communication tunnel for the transported video signal is different than the tunnel of the conveyed message and it is not possible to verify the authenticity of conveyed message via the video of the communication partner. Although users can confirm the communication partners from the live video feed, they cannot verify whether the messages sent by the communication partners have been modified or eavesdropped by a malicious adversary. Therefore, it is essential to establish secure message communication channel for real time online communication.

The main technology to protect the security communication, in particular the confidentiality and integrity of the message, is key establishment [7]. In other words, the message communication between partners should be established through a secured channel. The content of the communication can be protected with encryption if a session key is shared between communication partners [8,9]. An RSA cryptosystem [10] can be used to share a session key between communication partners. The sender who wants to communicate with the receiver will use the session key to encrypt the message. After the sender uses the receiver's public key to encrypt the session key, the sender sends the encrypted message using secret-key cryptography and an encrypted session key using public key cryptography to the receiver. A wide variety of RSA-based public key encryption schemes have been proposed for secure communication [11–14]. However, RSA-based cryptosystems will have no legal value if there is no reliable public key authentication. A malicious adversary may impersonate the receiver by claiming that the public key is the receiver's. To avoid this situation, the core problem for information security and cryptography is that all of the security functions based on public key cryptography are eligible only if the owner of the key is verified.

Public key infrastructure (PKI) has been adopted for several decades to solve this problem [15]. PKI is a complex distributed system that can prove the relationship between the public key and identity of the users [16]. With PKI, digital certificates are often issued by an independent Certificate Authority (CA) that then acts as a third-party reference for the identity of the owner. With the guarantee from CA, the authenticity of the public key is assured by the verifier [17]. PKI uses certificates to verify the public key. Thus, the issues associated with certificates needs to be considered, such as storage, revocation and distribution. Such issues are of particular importance when a PKI contains many different CAs. In other words, there are many different types of certificates [18,19]. If one type of certificate wants to be verified by a different CA, under this condition, the structure of PKI becomes complex. Besides establishing such a scheme, there are significant costs to build out a PKI. Due to the usefulness of PKI, many papers that have pointed out the importance of discussing issues emerged in the construction of PKI [20,21].

In order to avoid problems derived from the use of certificates, both Identity-Based Public Key Cryptography (ID-PKC) [22,23] and Certificateless Public Key Cryptography (CL-PKC) [24,25] do not use a certificate to prove the relationship between the users' identities and their public keys. In the schemes for ID-PKC and CL-PKC, users just use their public information as their public keys, such as phone numbers or e-mail addresses and thus the verification of a public key is intuitive. However, both ID-PKC and CL-PKC need to produce the key pair through a key generator center (KGC), which means that a third-party certifier needs to be involved in this scenario. Recently, smart phones, tablets and personal computers are widely and conveniently used by users to communicate with other users through real-time online communication. Most of these devices now have cameras that the users can use to see the partners. As such, it is not necessary to involve a third party to prove the relationship between a user's identity and his/her public key. The users can verify the communication partner's public key by themselves. It is extremely intuitive and reasonable to use the technique of biometric recognition [26,27] to deal with authentication problems in the field of information security, especially for real-time video communication where both the communication partners are online. This approach can reduce complexity, such as that associated with a key revocation mechanism and interoperability among different certification authorities in a PKI. This can be accomplished by embedding biometrics into the public key.

Therefore, our aim in this paper is to take advantage of real-time online communication to capture an image of the communication partner to authenticate the public key of the partner and then exchange a session key to protect the communication. Accordingly, the basic idea of this paper is to generate a cryptographic public key from a user's biometrics, especially for RSA—one of the most widely used cryptosystems in the world today. In this method, the key must be verified with the presence of the user's biometrics. The key is derived from the user's biometrics and is strongly user-dependent. It is very easy to convince others about the authenticity of the owner. Additionally, the derived biometrics key also significantly reduces the costs associated with certificates (i.e., reduction of cost of storage, delivery and revocation) because the key is self-certified with the user's biometrics. Once the public key is verified, digital envelope technology can be applied to secure the content of the communication without worrying about an impostor. Therefore, in this paper, without using PKI to provide the certificate to prove the correlation between a user's identity and his/her public key, schemes for the RSA cryptosystem and fuzzy extractors are used to authenticate and generate key agreement. Taking advantage of real-time communication, people can check on each other through the camera in real time and a third party is unnecessary.

The remainder of this paper is organized as follows. Section 2 presents related work for the proposed cryptosystem. The proposed scheme is described in Section 3. Section 4 presents our simulation of the proposed scheme. Section 5 discusses the security of the proposed scheme. Finally, Section 6 draws conclusions.

2. Related Works

The major analytical operations required within the proposed biometrics-based encryption system are a portion of the RSA, including unbalanced RSA and fuzzy extractors, which are illustrated in this section.

2.1. RSA

In 1978, Ron Rivest, Adi Shamir and Leonard Adleman proposed a public-key cryptography algorithm called RSA [10], which is based on the difficulty of factoring large integers. This algorithm with complex number generation, exponential manipulation and modular mathematics has become a mainstay of Internet security. In the RSA scheme, a user creates and publishes a public key that is the product of two large prime numbers and keeps the prime factors secret. With the user's public key, the other user can use the public key to encrypt a message. Only the owner of public key who has knowledge of the prime factors can decode the message. The RSA scheme involves three steps, including key generation, encryption and decryption, which are illustrated as follows: that is, d is the modular multiplicative inverse of e (modulo λ(n))

1. Key generation:

    a. Generate two large random primes p and q and the size of two prime numbers should be of similar length.
    b. Compute $N = pq$ and $\varphi(N) = (p-1)(q-1)$.
    c. Select a random integer e, where $1 < e < \varphi(N)$, such that $gcd(e,\varphi(N)) = 1$, where gcd is the greatest common divisor.
    d. Compute the unique integer d, $1 < d < \varphi$, such that $ed = 1$ $(mod\ \varphi(N))$, that is, d is the modular multiplicative inverse of e $(modulo\ \varphi(N))$.
    e. Public key is (N, e); private key is d.

2. Encryption: During encryption, suppose that user Alice wants to send a message M to user Bob and then she will use the authentic public key (N, e) of Bob which has been published to encrypt the message M into cipher text C, where

$$C = M^e (mod\ N)$$

3. Decryption: During decryption, as Bob receives the encrypted message C, he can decrypt the message because he owns the private key d and obtains the original message M, where

$$M = C^d (mod\ N)$$

2.2. Unbalanced RSA

Based on the difficulty of factoring integers or computing discrete logarithms in an infinite field, RSA is able to achieve a computationally secure method. However, advances in computational number theory and the availability of computing power have rapidly increased, which means that the sizes of moduli need to be increased to assure safety.

In 1995, Shamir proposed a variant RSA cryptosystem called unbalanced RSA [28]. The difference between unbalanced RSA and traditional RSA is the size of prime numbers p and q. In traditional RSA, the size of p and q are the same and are chosen by the user. However, in unbalanced RSA, the size of p and q are different.

Shamir observes that the RSA cryptosystem is usually used to exchange short messages, such as exchanging a session key for symmetric cryptosystems or authentication information, so limiting clear text m in the range of $[0, p - 1]$ is not a serious constraint. Since the legitimate recipient only needs to carry out operations for modulo p, the other prime q can be chosen to be large enough to prevent attacks by general integer factorization algorithms. For example, for extremely cautious users, Shamir suggests choosing a p of 500 bits and a q of 4500 bits.

In unbalanced RSA, let G be a publicly known random bit generator that can convert the users' identity u into a unique 5000 bit value t, as $t = G(u)$. Once the users produce their unique value t, they choose a random prime number p with 500 bits. The users restrict the other prime number q in the range $[a, a + 250]$ where a is bigger than or equal to t/p, so that $N = pq$ is very close to the target value t. It is clear that the difference between N and t, that is, $s = N - t$, is about 550 bits. Then the users can publish s as their own public key and the other users can recover modulus N of the user by having the user's identity u and public key s, as $N = G(u) + s$.

Later, Gilbert et al. [29] pointed out that a malicious attacker could recover the user's secret keys from simple implementations of Shamir's algorithm. Shamir observed that a redundancy in the message could avoid having the attacker forge a message that is bigger than a prime number p to get the user's private keys. However, Gilbert et al. pointed out that it does not suffice to add just any redundancy to the message. The malicious attacker can betray the secret keys of the users through their action. Above all, it is necessary to use the redundancy in plaintexts carefully, so that the recipients cannot reveal any decrypted message.

2.3. Fuzzy Extractors

The secret component of cryptography traditionally relies on uniformly distributed and precisely reproducible random strings. Since biometric data is not a fixed value each time it is measured, it is not suitable to directly generate the key from biometric data. In 2008, Dodis et al. presented a scheme to demonstrate how to transform biometric data into a cryptographic key that was primitively called a fuzzy extractor [30]. In the scheme, the biometric data is extracted to a random string R in a noise tolerant way. Suppose the biometric data is inputted again as b', if the difference between b and b' is under the threshold, the extracted string R can be recovered. To reproduce the extracted string R, the aid of a helper string P is provided. Three metrics are used to construct fuzzy extractor scheme:

(1) Hamming metric, which is the number of symbol positions that differ between b and b': (2) Set difference metric, which is the size of the symmetric difference of two input sets between b and b'; and (3) Edit metric, which is the number of insertions and deletions needed to convert b' into b.

Fuzzy extractor generator *Gen.* is shown in Figure 1, which can transform the inputted biometric data into a helper string P for a fixed length and an extracted string R. The owner of biometric data can reproduce the extracted string R by inputting his/her biometric b' which is limited within a range with a threshold and a published helper string P to create a representation of fuzzy extractors *Rep.*, as shown in Figure 2.

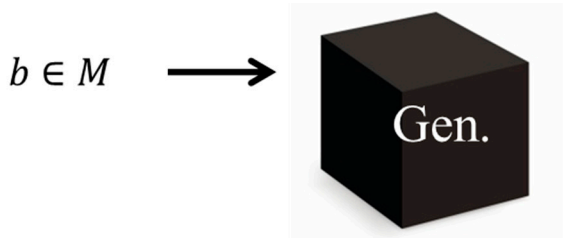

Figure 1. The generator of fuzzy extractors.

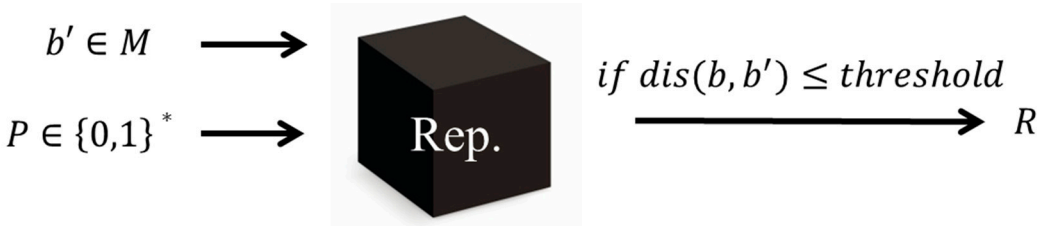

Figure 2. The representation of fuzzy extractors.

3. Proposed Scheme

In the proposed scheme, the users' public keys are produced from their biometric values and session key is exchanged. Figure 3 shows a communication scenario for the proposed scheme. In this scenario, user Alice wants to talk to Bob through real-time communication software. Before they start to chat formally, they can see each other clearly through the video. As they say hello and confirm that the other side is their communication partner, they can begin to execute the key agreement protocol.

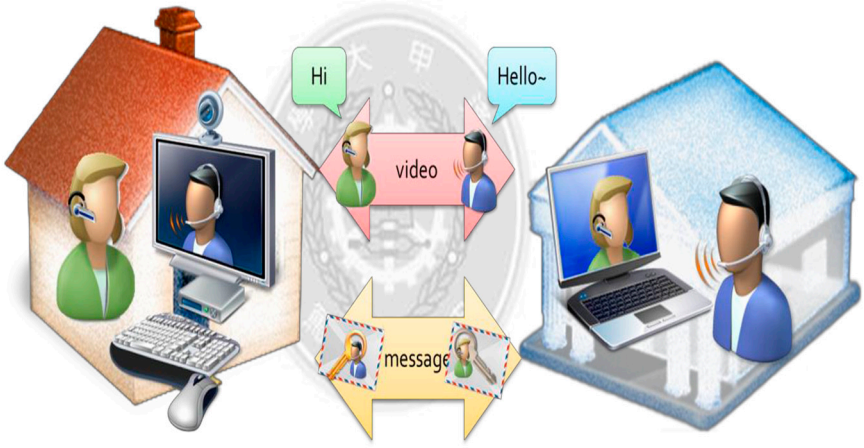

Figure 3. The communication scenario of proposed scheme.

The proposed scheme is divided into two phases: the initialization phase and the authentication and key agreement phase. In initialization phase, the communication partners produce their public keys from the biometric information obtained from each user's face. In the authentication and key

agreement phase, the user authenticates the identity of their communication partner. Furthermore, they can recover and verify the communication partner's public key and then exchange the session key with them. Before introducing the proposed scheme, the notions used in our scheme are described in Table 1.

Table 1. Notions of the Proposed Scheme.

Notion	Description
Gen.	Generator of Fuzzy Extractors
Rep.	Reputation of Fuzzy Extractors
b	Biometric information
P	A helper string for Fuzzy Extractors
R	An extracted string for Fuzzy Extractors
p, q	The prime numbers for RSA
N	A modus for RSA
α	A security parameter

3.1. Initialization Phase

In the initialization phase, both Alice and Bob need to use their own webcam to capture their face information in order to produce their public key. Afterwards, by using a scheme for fuzzy extractors, they can produce their own extracted string R. Utilizing the concept of unbalanced RSA, they can produce their private RSA keys. Finally, the communication partners broadcast some information in a public network to help the other party recover and verify the public key.

In the initialization phase for the users, Alice and Bob, prepare their public keys and produce their RSA private keys as shown in Figure 4, which is detailed in the following steps:

Step 1. Users Alice and Bob capture their respective faces using their own camera to produce biometric information b_A and b_B.
Step 2. Helper string P and extracted string R are produced by using fuzzy extractors.
Step 3. Generator G transforms the extracted string into value t_A with a fixed length. The size of t_A is close to N of RSA.
Step 4. Alice and Bob randomly choose a large prime number p.
Step 5. Using prime number p and value t, Alice and Bob produce public value a.
Step 6. Randomly choose a prime number q. To let q multiplied by p be closed to value t, the size of q is restricted in a fixed range $[a, a + 2^a]$, where a is a security attribute.
Step 7. According to Steps 4 and 6, we can get the prime numbers, p and q, of the RSA and calculate $N = p \times q$.
Step 8. The difference between N and t is s, that is, $s = N - t$. And both of the users will publish s and P to provide the other with the ability to recover their information.

It is special in the scheme that extracted string R can be converted into the public key N of RSA. An unbalanced RSA scheme is typically applied to a smart card and the size of prime numbers p and q are different. However, this feature of unbalanced prime numbers is not suitable in the proposed scheme. In other words, there are no smart cards used in our scheme. Moreover, it is unnecessary to store any information. The problem of storage can be ignored. Hence, the size of the prime numbers is similar.

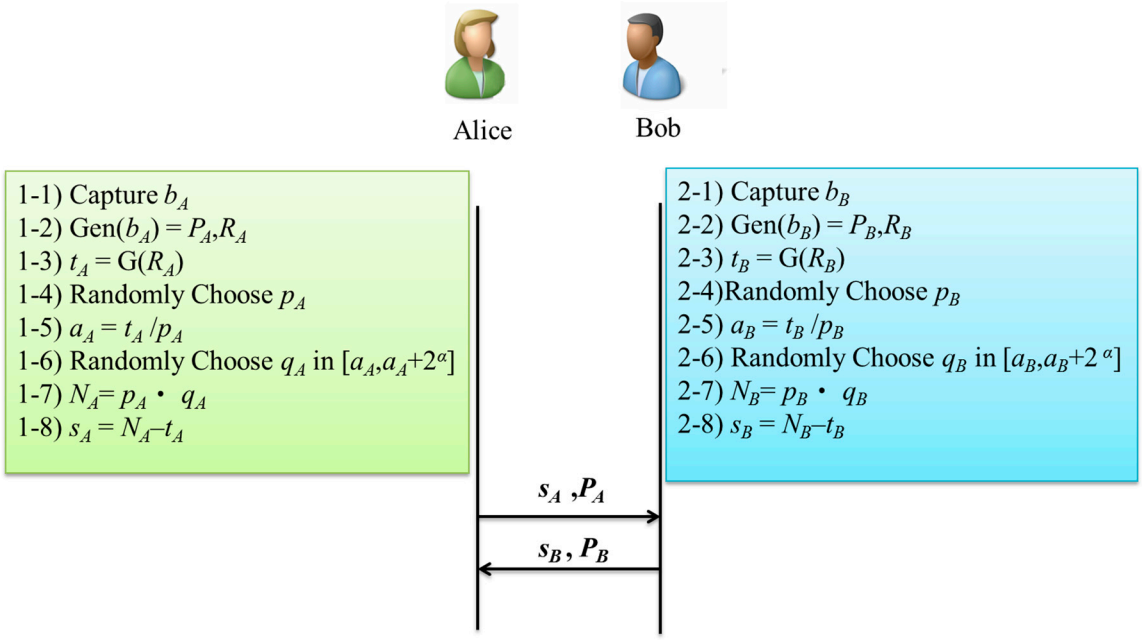

Figure 4. The initialization phase.

3.2. Authentication and Key Agreement Phase

After beginning contact with the other party, Bob can check if the other side is the real person whom he wants to talk with by using his camera. Because he is familiar with Alice, he makes a determination of whether she is the real person, or someone pretending to be her. As he confirms that Alice is the person he wants to talk with, he presses the camera to obtain Alice's biometric template which is then used to check Alice's public key.

Concurrently, Alice makes a determination through the video that Bob is her expected communication partner and she presses a button to capture Bob's biometric template. In other words, Alice can verify the public key of Bob by herself from the video. As soon as she confirms that the communication partner is correct, she will start to verify the correctness of Bob's public key. Bob does the same. Subsequently, both of them are in mutual authentication. The authentication and key agreement phase are shown in Figure 5, which is described in detail as follows:

Step 3.1 Using *Gen.* of the fuzzy extractor, Alice can recover Bob's extracted string R_B.

Step 3.2 In order to get Bob's modus N_B, Alice inputs Bob's extracted string R_B, to obtain the value t_B.

Step 3.3 Following the previous step, Alice uses the value t_B and the public information s_B, which she obtained in the initialization phase to compute Bob's modus N_B.

Step 3.4 In this step, Alice can use Bob's N_B and Bob's public key e_B to encrypt the random number K_A and send the encrypted message C_A to Bob.

Step 4.1 Using *Gen.* of the fuzzy extractor, Bob can recover Alice's extracted string R_A.

Step 4.2 Bob inputs Alice's extracted string R_A, to obtain the value t_A.

Step 4.3 Bob will use the value t_A and the public information s_A, which he obtained in the initialization phase to compute Alice's modus N_A.

Step 4.4 Bob uses his private key d_B to decrypt the message C_A sent from Alice.

Step 4.5 Then Bob chooses the random number K_B. Bob can use Alice's N_A and Alice's public key e_A to encrypt the random number K_B and send this to Alice. The session key is $H(K_A || K_B)$.

Step 5.1 As Alice receives the message C_B, she decrypts the message and gets K_B. Alice can compute the session key as $H(K_A || K_B)$.

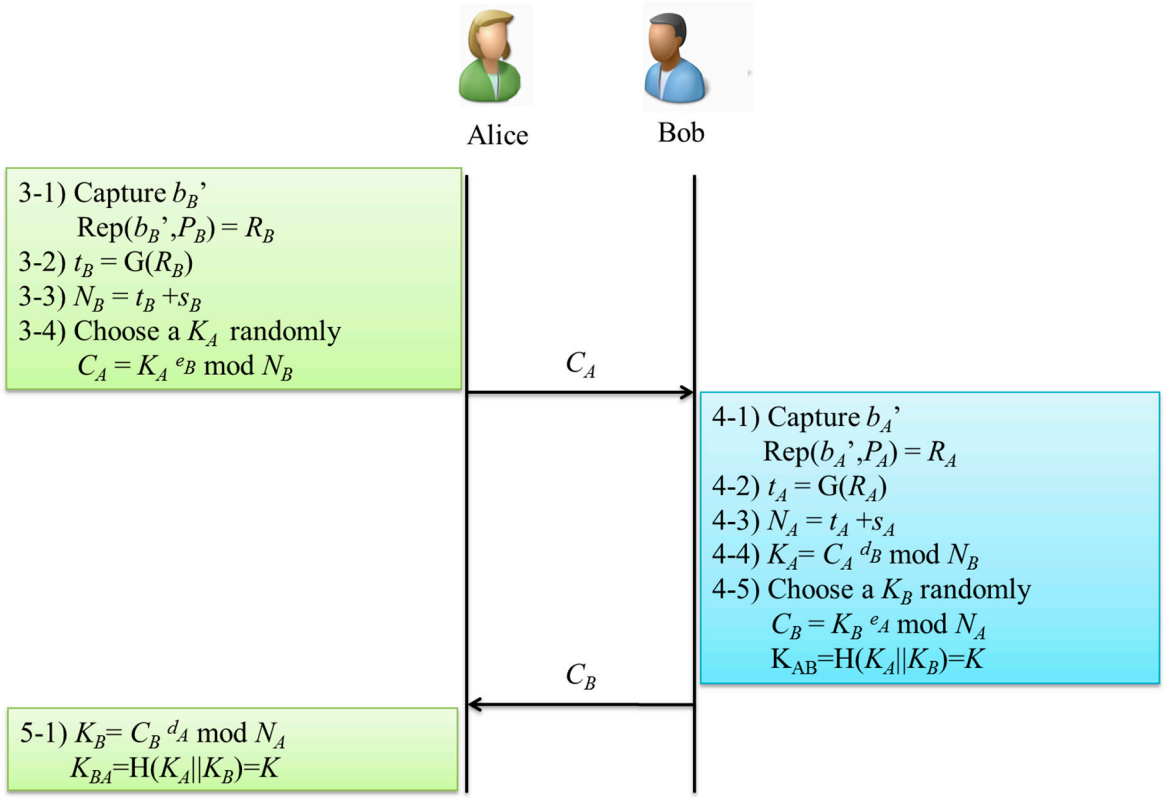

Figure 5. Authentication and key agreement phase.

By using the fuzzy extractor scheme, both Alice and Bob can produce the others' extracted string R. With the aid of the public value s, they can compute the other person's public key N, in order to exchange the value for the communication to compute the session key.

4. Simulations

The main objective of this paper is to provide the concept of taking advantage of biometric information for authenticating and generating key agreement without using PKI to protect real-time online communication. To further prove the applicability of this method, we developed a prototype system using our proposed biometrics based on RSA to secure real-time communication. Java was used as our major implementation tool and Javacv 1.4.1 was used to interact with the camera to capture the face from a user. Face++ was used to capture facial features. The experiment was conducted on an Asus PC running Windows 10 and an Intel i7-6700H1 CPU with 16 GB RAM in Taichung, Taiwan. Figure 6 shows the screen capture of the simulated prototype system of the proposed biometrics-based RSA cryptosystem. In this study, user Ally Chen wants to talk to Bob through the real-time communication system. Before they start to chat formally, they can see each other clearly through the video. As they say hello and confirm that the other side is their communication partner, they can begin to execute the key agreement protocol and convey message in secure tunnel. In the initialization phase, users need to capture their face biometrics by using their own cameras. By using Face++, the user received three feedback digits, including lift angle, horizontal rotation degree and plane rotation degree. With these feedback digits, a user adjusts their head to obtain consistent face features with minimal distortion. A face image with minimal distortion utilizing the combination of these three digits is then captured to derive a public key and an error-correcting code. Here, we used a (7, 4, 3) hamming code as our error-correcting code. A 3-bit error correcting code was generated for each feature value for a given face.

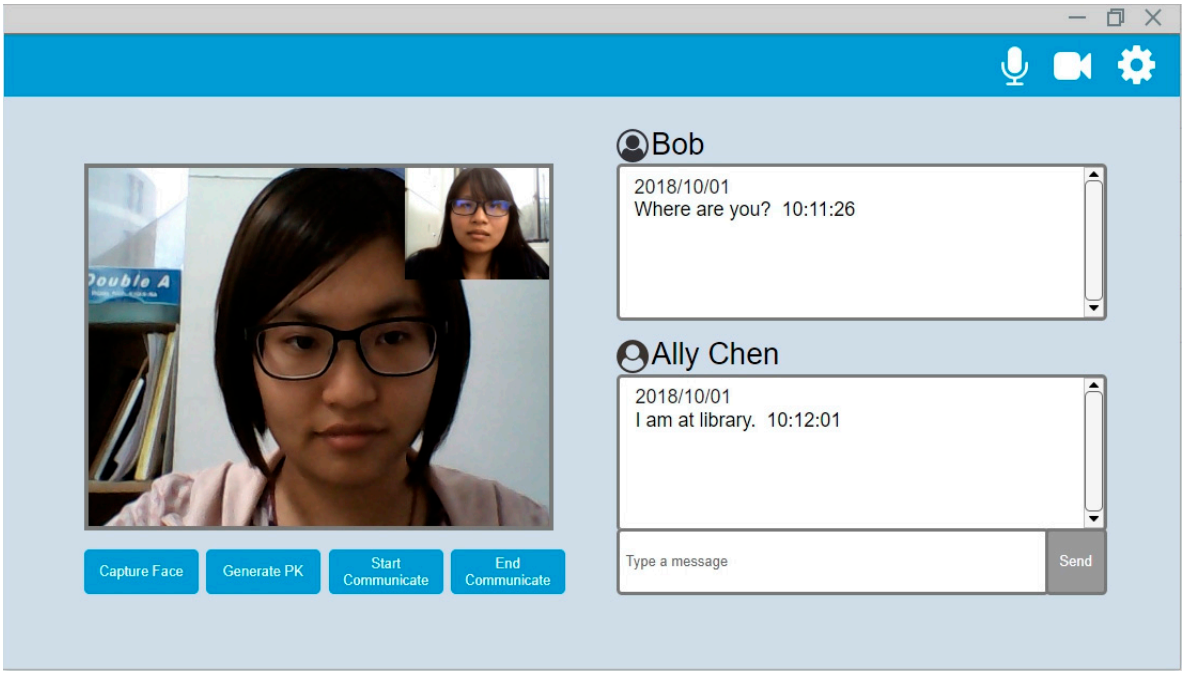

Figure 6. The prototype of the proposed biometrics-based RSA cryptosystem.

It is noted that the amount of feature nodes generated by Face++ is up to 108; however, only 10 were used as feature nodes in our prototype system. Forty-five distance values can be derived by linking two of ten feature nodes. With three feature nodes, we can derive the other 8 distance values. To sum up, there are 53 distance values that serve as the feature values to derive a public key for a user. Following the quantization concept described in Sutcu et al.'s method [31], the above 53 values can be mapped to 16 quantization levels and each level requires 4 digits to represent the level. To increase the precision of our prototype system, one digit representing gender was added to the public key for a user. Therefore, the total digit amount of a user public key is 53*4+1 = 213 bits. Once a user's public key is generated, his/her corresponding private key can be derived according to the generation rule given in RSA. As mentioned, each feature value has a 3-bit error-correcting code that needs to be generated. Therefore, the total error correcting code was 175 bits (53*3+2 scaling references). Here, scaling references are two reference values that serve as the scaling ratio and are used to make sure that a justified public key can be derived that is not affected by zoom in or zoom out.

User can decide to keep the generated private key and the error correcting code or not. It is worth to mention that the proposed biometrics-based scheme would not introduce any overhead in the normal communication. It is because that in our proposed scheme demonstrated in Section 3, both public-private key pair is generated real-time and only used once to exchange a random number and then create a secure communication channel for two users. Therefore, not only public key but also private key and error correcting code are not necessary to be stored. User always can use the camera to capture the face image of his/her communication partner to derive the corresponding public key. Next, the private key can be obtained based on the RSA algorithm. In our simulation environment, the public key and private key can be generated in one minute. In other words, the proposed cryptosystem is very suitable for real-time communication. Although the prototype system is simulated in PC environment, the proposed cryptosystem can also be implemented in smartphone or other mobile device with lower processing power. Although it takes a little longer for generating the public-private key pair, the key pair is only generated once during establishing secure communication channel for users. There is no extra cryptographic computing in the proposed cryptosystem once the secure channel is established. Therefore, the real-time communication would be guaranteed, even if the device is with lower processing power.

5. Security Analysis and Discussion

This section first discusses the security of the proposed biometrics-based RSA cryptosystem for use in real-time communication. Then the proof with Burrows–Abadi–Needham (BAN) logic [32] of the proposed scheme is demonstrated to prove that our scheme can achieve the session key agreement. Finally, the comparisons of security features with two existing schemes [26,27] are also listed to demonstrate the superiority of the proposed scheme.

5.1. Security Analysis

During the phases of authentication and key agreement, some information is transferred between two parties in a public network. The public information, s and P, are shared in the authentication phase. Suppose that the malicious adversary gets the information s and P, then the adversary can recover both Alice's and Bob's public key N. Based on RSA security, the public key N of RSA is primarily public, so the problem about leaked information is not concerned with the leak of a user's secret keys.

Considering another condition in the proposed scheme, if the adversary intercepts Alice's public information, s_A and P_A, the adversary can try choosing proper prime numbers p_{ma} and q_{ma}, such that $p_{ma} \cdot q_{ma} = N_{ma}$. Then the adversary may attempt to create forged public information s_{ma}, such that $N_{ma} = t_A + s_{ma}$ and publish the forged public information s_{ma} and Alice's helper string P_A to Bob. However, Alice's public information is published in the initialization phase and thus the adversary needs to know Alice's t_A in the beginning to produce a proper s_{ma} and N_{ma}. But the information for t_A is produced during the authentication and key agreement phase, thus it is initially unknown to the adversary. Moreover, each of the communications will be regenerated each time, thus the values known from this exchange cannot be used the next time.

If the adversary wants to use the principle of a replay attack to steal the message between Alice and Bob, the adversary will send the wrong message by utilizing the users' public key. However, the session key is determined by Alice and Bob, thus the forged message cannot let $H(K_A||K_B)$=$H(K_A||K'_B)$ or $H(K_A||K_B)$=$H(K'_A||K_B)$.

The attacks proposed by Gilbert et al. [20] also do not affect the security of our scheme. In the attacks, they assumed the sender is malicious and wants to betray the secret keys of the recipient. That means the recipient has not authenticated the identity of the sender. In the proposed scheme, however, mutual authentication occurs before exchanging messages. Aside from the next communication between the communication partners, all of the phases will be executed once again, so the secret keys of the RSA are not the same as in the previous exchange. Although a malicious actor may steal the secret keys of the recipient at this time, the secret keys are not suitable for use in a future exchange.

5.2. Proof with BAN Logic

In 1990, Burrows et al. design a formal logic analysis for authentication and key agreement schemes, it is called the BAN logic model [32]. Hence, we use BAN logic model to prove that our scheme can achieve the session key agreement. In order to describe formal semantics and analysis procedures, the notations and logical postulate rules used in BAN logic model are given as Table 2 [32,33].

Table 2. Notations and rules used in BAN logic model.

Notations	Description
P, Q	Two principals
X, Y	Two statements
$P\|\equiv X$	The principal P believes the statement X
$P\|\sim X$	The principal P once said the statement X
$P \lhd X$	The principal P see the statement X
$\| \xrightarrow{K} P$	The principal P has a public key K
$P \xleftrightarrow{K} Q$	The principals P and Q use the shared key to communicate
$\#(X)$	The statement X is fresh
$\{X\}_K$	The statement X encrypted under the public key K (Note that the matching private key is denoted $K-1$)

- The message-meaning rule

$$\frac{P| \equiv | \xrightarrow{\mathrm{K}} Q, P \lhd \{X\}_{K^{-1}}}{P|\equiv Q|\sim X}$$

- The nonce-verification rule

$$\frac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$$

- The freshness rules

$$\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)} \text{ and } \frac{P|\equiv \#(X,Y)}{P|\equiv \#(X)}$$

- The session-key rule

$$\frac{P|\equiv \#(K), P|\equiv Q|\equiv X}{P| \equiv P \xleftrightarrow{K} Q}$$

In the authentication and key agreement phase, the message exchange steps are written in M_1 and M_2.

$$M_1.\ \text{Alice} \longrightarrow \text{Bob} \ :\ C_A^1 = {K_A}^{e_B} \mathrm{mod} N_B,\ C_A^2 = \left(N_a || h(C_A^1)\right)^{d_A} \mathrm{mod} N_A$$
$$M_2.\ \text{Bob} \longrightarrow \text{Alice} \ :\ C_B^1 = {K_B}^{e_A} \mathrm{mod} N_A,\ C_B^2 = \left(N_b || h(C_B^1)\right)^{d_B} \mathrm{mod} N_B$$

We transform generic message exchange steps, M_1 and M_2, into the idealized form, I_1 and I_2.

$$I_1.\ \text{Alice} \longrightarrow \text{Bob} \ :\ \{K_A\}_{e_B},\ \{N_a, K_A\}_{d_A}$$
$$I_2.\ \text{Bob} \longrightarrow \text{Alice} \ :\ \{K_B\}_{e_A},\ \{N_b, K_B\}_{d_B}$$

We know that Alice uses her webcam to capture bob's face information for obtaining the public key of Bob. Alice also generates K_A and verifies N_b. Hence, we give the three assumptions apply to Alice:

$$A_1.\ \text{Alice}| \equiv | \xrightarrow{e_B} \text{Bob}$$
$$A_2.\ \text{Alice}|\equiv \#(K_A)$$
$$A_3.\ \text{Alice}|\equiv \#(N_b)$$

Three similar assumptions apply to Bob:

$$A_4.\ \text{Bob} \mid \equiv | \xrightarrow{e_A} \text{Alice}$$
$$A_5.\ \text{Bob} \mid\equiv \#(K_B)$$
$$A_6.\ \text{Bob} \mid\equiv \#(N_a)$$

Next, with I_1, I_2 and the assumptions we will prove that the proposed scheme can achieve the session key agreement under BAN logic model, as following:

Theorem: *Our scheme can achieve the session key agreement under BAN logic model.*

Proof:

In our scheme, Alice and Bob together coordinate the session key $K = H(K_A \| K_B)$. They must believe that this session key is shared between them. Hence, the goals are listed: G_1. Alice$| \equiv$ Alice $\overset{K}{\longleftrightarrow}$ Bob and G_2. Bob$| \equiv$ Alice $\overset{K}{\longleftrightarrow}$ Bob.

Applying the freshness rule to A_3, we could derive:

$$R_1. \text{ Alice } |\equiv \#(N_b, K_B)$$

Applying the freshness rule to R_1 and A_2, we could derive:

$$R_2. \text{ Alice } |\equiv \#(K)$$

Applying the message-meaning rule to A_1 and I_2, we could derive:

$$R_3. \text{ Alice } |\equiv \text{Bob}|\sim (N_b, K_B)$$

Applying the nonce-verification rule to R_1 and R_3, we could derive:

$$R_4. \text{ Alice } |\equiv \text{Bob}|\equiv (N_b, K_B)$$

From R_4, we could deduce that Alice believes in Bob believes in K_B, that is,

$$R_5. \text{ Alice } |\equiv \text{Bob}|\equiv K_B$$

Applying the session-key rule to R_2 and R_5, we could derive the goal G_1:

$$G_1. \text{ Alice}| \equiv \text{Alice } \overset{K}{\longleftrightarrow} \text{ Bob}$$

Applying the freshness rule to A_6, we could derive:

$$R_6. \text{ Bob } |\equiv \#(N_a, K_A)$$

Applying the freshness rule to R_6 and A_5, we could derive:

$$R_7. \text{ Bob } |\equiv \#(K)$$

Applying the message-meaning rule to A_4 and I_1, we could derive:

$$R_8. \text{ Bob } |\equiv \text{Alice}|\sim (N_a, K_A)$$

Applying the nonce-verification rule to R_6 and R_8, we could derive:

$$R_9. \text{ Bob } |\equiv \text{Alice}|\equiv (N_a, K_A)$$

From R9, we could deduce that Bob believes in Alice believes in K_A, that is,

$$R_{10}. \text{ Bob } |\equiv \text{Alice}|\equiv K_A$$

Applying the session-key rule to R_7 and R_{10}, we could derive the goal G_2:

$$G_2.\ \text{Bob}| \equiv \text{Alice} \overset{K}{\longleftrightarrow} \text{Bob}$$

Therefore, according to the above inference processes, we have proven that the proposed scheme can achieve the session key agreement under BAN logic model. □

5.3. Comparisons

To demonstrate the advantage, the comparisons of security features with related schemes are listed in this section. Since the proposed scheme is the very first biometrics-based cryptosystem for securing real-time communication, we could only compare it with related schemes that also used biometric information for user authentication. Table 3 shows the security features provided by our scheme and other biometrics-based authentication schemes [26,27]. It is clear from comparison results listed in Table 3 that our scheme supports more security features which are crucial for real-time communication than other schemes.

Table 3. Comparisons of Attack resistance for various cryptosystem schemes.

Attack Resistance	Choi et al.'s Scheme [26]	Das' Scheme [27]	Proposed Scheme
Replay attack	Yes	Yes	Yes
Server masquerading attack	Yes	No	Yes
Mutual authentication	Yes	Yes	Yes
Biometric recognition error	Yes	No	Yes
User impersonation attack	Yes	Yes	Yes
Vulnerability to a DoS attack	Yes	Yes	Yes
Session key agreement	Yes	No	Yes
Database capture attack	No	No	Yes
Smart card attack	No	No	Yes
Man-in-the-middle attack	No	Yes	Yes

It is worth mentioning that, in our scheme, the key must be verified with the presence of the user's biometrics instead of using smart card in other schemes. Therefore, our proposed scheme can resist the smart card attack. The key in our scheme is derived from the user's biometrics and is strongly user-dependent, which is very easy to convince others about the authenticity of the owner. In addition, since the key is self-certified with the user's biometrics during real-time communication, no database is required to store biometrics information in the cryptosystem. Once the key is verified, digital envelope technology can be applied to secure the content of the communication without worrying about an impostor. Therefore, the derived biometrics key can not only significantly reduce the costs associated with storage, delivery and revocation but also resist database capture attack and man-in-the-middle attack.

6. Conclusions

This paper proposed a novel biometrics-based scheme for authenticated key agreement in real-time communication. With the universality of video cameras in communication devices, we assumed that communication partners can see each other through the Internet in real-time. The main objective of this paper is to provide the concept of taking advantage of biometric information for authenticating and generating key agreement without using PKI to protect real-time online communication. The proposed scheme makes use of a user's intuition to authenticate the other person who is known to her/him. Additionally, users' identities are confirmed with current encounters, rather than based on previous or future encounters. Even if the communication partners are not familiar with each other, it means the face-to-face mutual authentication function is not triggered under this situation, the proposed system still can derive users' public key based on users' biometrics and then

guarantees the security of the communication between two parties just likes the conventional public key cryptographic system. Since the PKI and third-party certifier is not involved in the proposed scheme, the proposed scheme is more practical compared with the conventional public key cryptographic system. Moreover, the public key with our scheme is produced from the user's biometric information and thus the relation between user identity and the public key is relative robust

To confirm the applicability of the proposed scheme, a prototype system is simulated. It is proved that a public/ private key pair can be generated in one minute. In other words, it confirms the proposed scheme is able to support real-time communication. The security analysis of the proposed scheme demonstrates that the proposed scheme is secure enough to resist malicious attacks. The proposed scheme is demonstrated to prove that our scheme can achieve the session key agreement with the proof with BAN logic. Moreover, the comparisons of security features with existing biometrics-based authentication schemes also demonstrate the superiority of the proposed scheme. Although the prototype system is demonstrated able to support real-time communication, the simulation is conducted in PC environment in this work. In the future, we will try to implement the proposed scheme in smartphone or other mobile device to show the performance in devices with lower processing power. In addition, different authentication strategy, such as hybrid authentication protocol, can be proposed to deal with the situation when communication partners are not familiar with each other.

Author Contributions: Conceptualization, X.L. and W.-B.L.; Formal analysis, X.L., C.-C.L. and H.-L.W.; Investigation, W.-B.L. and Q.-A.B.; Methodology, C.-C.L.; Resources, W.-B.L.; Software, Q.-A.B.; Supervision, W.-B.L. and C.-C.L.; Validation, X.L. and C.-C.L.; Writing—original draft, X.L. and W.-B.L.; Writing—review & editing, C.-C.L.

Funding: This research was funded by (MOE (Ministry of Education in China) Project of Humanities and Social Sciences) grant number (17YJC880076), (the National Natural Science Foundation of China) grant number (61702102), and (Natural Science Foundation of Fujian Province, China) grant number (2018J05100).

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

References

1. Panteli, N.; Dawson, P. Video conferencing meetings: Changing patterns of business communication. *New Technol. Work Employ.* **2010**, *16*, 88–99. [CrossRef]
2. Correa-Garcia, J.A.; Garcia-Benau, M.A.; Garcia-Meca, E. CSR communication strategies of colombian business groups: An analysis of corporate reports. *Sustainability* **2018**, *10*, 1602. [CrossRef]
3. Jeong, S.; Jeong, Y.; Lee, K.; Lee, S.; Yoon, B. Technology-based new service idea generation for smart spaces: Application of 5g mobile communication technology. *Sustainability* **2016**, *8*, 1211. [CrossRef]
4. Jarren, O. Mediatization in the age of online communication—Still a useful paradigm. *Oral Dis.* **2018**, *10*, 63–74.
5. Jebrane, A.; Meddah, N.; Toumanari, A.; Bousseta, M. New Real Time Cloud Telemedicine Using Digital Signature Algorithm on Elliptic Curves. *Lect. Notes Netw. Syst.* **2017**, *25*, 324–332.
6. Anton, D.; Gregorij, K.; Ruzena, B. User experience and interaction performance in 2D/3D telecollaboration. *Futur. Gener. Comput. Syst.* **2018**, *82*, 77–88. [CrossRef]
7. Farouk, A.; Tarawneh, O.; Elhoseny, M.; Batle, J.; Naseri, M.; Hassanien, A.E. Quantum key distribution over multi-point communication system: An overview. Quantum Computing: An Environment for Intelligent Large Scale Real Application. *Stud. Big Data* **2018**, *33*, 101–121.
8. Liu, Y.; Wang, Y.; Chang, G. Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2740–2749. [CrossRef]
9. Elhoseny, M.; Yuan, X.; El-Minir, H.K.; Riad, A.M. An energy efficient encryption method for secure dynamic WSN. *Secur. Commun. Netw.* **2016**, *9*, 2024–2031.
10. Rivest, R.L.; Shamir, A.; Adleman, L.M. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]

11. Zhang, C.; Luo, Y.; Xue, G. A new construction of threshold cryptosystems based on RSA. *Inf. Sci.* **2016**, *363*, 140–153. [CrossRef]
12. Lin, X.J.; Sun, L.; Qu, H. An efficient RSA-based certificateless public key encryption scheme. *Discret. Appl. Math.* **2018**, *241*, 39–47. [CrossRef]
13. Muhammad, K.; Hamza, R.; Ahmad, J.; Lloret, J.; Wang, H.; Baik, S.W. Secure Surveillance Framework for IoT systems using Probabilistic Image Encryption. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3679–3689. [CrossRef]
14. Yang, L.T.; Huang, G.; Feng, J. Parallel GNFS Algorithm Integrated with Parallel Block Wiedemann Algorithm for RSA Security in Cloud Computing. *Inf. Sci.* **2017**, *387*, 254–265. [CrossRef]
15. Tan, H.; Ma, M.; Labiod, H. A Secure and Authenticated Key Management Protocol (SA-KMP) for Vehicular Networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 9570–9584. [CrossRef]
16. Marchesini, J.; Smith, S. Modeling Public Key Infrastructures in the Real World. *Public Key Infrastruct. Lect. Notes Comput. Sci.* **2005**, *3545*, 118–134.
17. Al-Khouri, A.M. PKI in Government Digital Identity Management Systems. *Eur. J. ePractice* **2012**, *3*, 4–21.
18. Younglove, R.W. Public Key Infrastructure: How It Works. *Comput. Control Eng. J.* **2002**, *12*, 99–102. [CrossRef]
19. Muhammad, K.; Sajjad, M.; Baik, S.W. Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy. *J. Med. Syst.* **2016**, *40*, 1–16. [CrossRef] [PubMed]
20. Li, S.; Zhang, W.; Chen, W. The PKI Technology and Analysis of the Existing Problems. *Control Autom.* **2005**, *22*, 171–172. [CrossRef]
21. Szalachowski, P.; Chuat, L.; Perrig, A. PKI Safety Net (PKISN): Addressing the Too-Big-to-Be-Revoked Problem of the TLS Ecosystem. In Proceedings of the IEEE European Symposium on Security and Privacy, Saarbrücken, Germany, 21–24 March 2016; pp. 407–422.
22. Hölbl, M.; Welzer, T.; Brumen, B. An improved two-party identity-based authenticated key agreement protocol using pairings. *J. Comput. Syst. Sci.* **2012**, *78*, 142–150. [CrossRef]
23. Boneh, D.; Franklin, M. Identity-Based Encryption from the Weil Pairing. *Proc. Crypto* **2001**, *2139*, 213–229.
24. Teng, J.; Wu, C. A provable authenticated certificateless group key agreement with constant rounds. *J. Commun. Netw.* **2012**, *14*, 104–110. [CrossRef]
25. Mokhtarnameh, R.; Ho, S.B.; Muthuvelu, N. An Enhanced Certificateless Authenticated Key Agreement Protocol. In Proceedings of the 13th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea, 13–16 February 2011; pp. 802–806.
26. Choi, Y.; Lee, Y.; Moon, J.; Won, D. Security enhanced multi-factor biometric authentication scheme using bio-hash function. *PLoS ONE* **2017**, *12*, e0176250. [CrossRef] [PubMed]
27. Das, A.K. A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor. *Int. J. Commun. Syst.* **2017**, *30*, e2933. [CrossRef]
28. Shamir, A. RSA for paranoids. *CryptoBytes* **1995**, *1*, 1–4.
29. Gilbert, H.; Gupta, D.; Odlyzko, A. Attacks on Shamir's 'RSA for paranoids'. *Inf. Process. Lett.* **1998**, *68*, 197–199. [CrossRef]
30. Dodis, Y.; Ostrovsky, R.; Reyzin, L.; Smith, A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *J. SIAM J. Comput.* **2008**, *38*, 97–139. [CrossRef]
31. Sutcu, Y.; Li, Q.; Memon, N. Secure Biometric Templates from Fingerprint-Face Features. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR'07), Minneapolis, MN, USA, 17–22 June 2007. [CrossRef]
32. Burrows, M.; Abadi, M.; Needham, R. A Logic of Authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]
33. Yang, S.P.; Li, X. Defect in Protocol Analysis with BAN Logic on Man-in-the-Middle Attacks. *Appl. Res. Comput.* **2007**, *24*, 149–151.

© 2018 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 (http://creativecommons.org/licenses/by/4.0/).