Article

Secure Visible Light Communication Technique Based on Asymmetric Data Encryption for 6G Communication Service

Yong Up Lee

College of Software, Hallym University, 1 Hallymdaehak-gil, Chuncheon, Gangwon-do 24252, Korea; yulee@hallym.ac.kr; Tel.: +82-033-248-2344

Received: 6 October 2020; Accepted: 30 October 2020; Published: 4 November 2020

Abstract: Security in residential and business establishments has become an area of considerable importance. To provide enhanced security using conventional visible light (VL) communication, the characteristics of which allow for easy access by nearby intruders, a new VL communication technique is proposed in this paper. The novel VL communication system is based on a data encryption method using asymmetric encryption, and it is proposed for use in smart indoor services in the 6th generation communication environment. The asymmetric encryption capability is studied by comparison with the conventional technique, the optimum key length for the public or private encryption codes is determined under the criterion of the minimum estimation error. Moreover, the error performance is analyzed with various RSA encryption keys and data lengths to verify the performance of the proposed technique. A real experiment is performed to evaluate the proposed technique using an implemented test bed, and the success rates of the VL communication technique with and without RSA coding are evaluated by a real experiment with a test bed under an indoor laboratory VL channel. We believe it is evident that the VL communication technique based on asymmetric encryption yields superior error performance compared to that without encryption for optimal lengths of the encryption key and data bits.

Keywords: visible light communication; 6G communication; asymmetric encryption scheme; optimal key length; real experiment; performance enhancement

1. Introduction

Smart indoor services, such as those in homes, factories, buildings, shopping malls or hospitals, have conventionally been applied using data control schemes with low rates and small datasets, and control processes employing wireless or visible light techniques are frequently required for such services. In these cases, the visible light (VL) communication method [1,2], which is regarded as a key technique in 6th generation (6G) communication [3–5], is naturally preferable to other wireless communication methods owing to its excellent security, high accuracy, safety (because of the use of a VL signal), and low installation costs.

Numerous studies [6–13] and standardization work [14] have been carried out on VL communication services. In particular, secure VL communication services based on encryption algorithms to enhance security performance have been studied, some examples of which are summarized here. A study on the VL communication technique based on asymmetric encryption was undertaken in a broadcasting system with a high transmission rate and large data [15], and a general encryption key distribution system using VL was investigated in a wireless LAN system [16]. Moreover, the performance analysis of a transceiver using the direct sequence spread spectrum method for communication between vehicles and LED-based traffic lights was reported [17], and the

optimum spread code was investigated in an indoor VL communication system [18]. A stream encryption key utilizing a binary sequence is used instead of a block key for data encryption in wireless communication. It has been established that the stream encryption key exhibits the properties of public and symmetric keys. Furthermore, the VL positioning technique based on pseudo-noise (PN) code has been demonstrated to provide the best encryption capability among the known stream encryption keys (such as PN, Gold or Kasami keys) under normal of the signal-to-noise ratio (SNR) conditions [19]. The asymmetric Rivest–Shamir–Adleman (RSA) encryption technique with public and private keys exhibits superior security performance over the symmetric encryption scheme based solely on a public key [20].

In this study, a VL communication technique using asymmetric data encryption is investigated as a real implementation and an extension of our earlier research [21]. The purpose of this approach is to provide security enhancements to conventional VL communication techniques for smart indoor services under the 6G communication environment, which normally allows easy access to nearby intruders owing to the characteristics of visible signals.

We contend that the asymmetric encryption scheme is preferable for the security enhancement of smart indoor services based on VL communication in the 6G communication environment and proceed accordingly. Asymmetric encryption scenarios for the VL communication system are investigated. Furthermore, the statistical properties of the RSA encryption key (i.e., public key and private key set) are compared under various prime number conditions, the asymmetric encryption capability is studied by comparison with the conventional technique, the optimum key length for the public or private encryption codes is determined under the criterion of the minimum estimation error, the dependence of the security performance on the key and data lengths is analyzed by means of a simulation study, and the success rates of the VL communication technique with and without RSA coding are evaluated by a real experiment with a test bed under an indoor laboratory VL channel.

The remainder of this paper is organized as follows: In Section 2, we discuss the VL communication methodology, a signal model for secure VL communication with data encryption, and the characteristics of the encryption key. In Section 3, we present a real experiment using a specific test bed and performance tests of the proposed technique via computer simulations. Finally, the conclusions of this study are provided in Section 4.

2. VL Communication Technique Based on Data Encryption

2.1. Methodology

In the 6G communication environment illustrated in Figure 1, high-frequency bands are used for ultrafast-speed transmissions, and different frequencies are dynamically used, especially unlicensed bands, to enjoy the benefits of the sharing architecture. For example, VL communication is a promising high-rate technique to replace conventional WLAN, as people spend most of their time (more than 80%) indoors.

In the smart indoor service based on VL communication on the left of Figure 1, the signals generated by two VL transmitters are simultaneously radiated into a VL channel. Several two-dimensional cells are constructed in the VL channel and a VL receiver executes the signal reception on a single predetermined cell. One VL signal is captured by the VL receiver; however, this VL signal can be intercepted by intruders. Therefore, we consider converting the conventional technique into an advanced VL communication technique based on data encryption.

An advanced VL communication system with data encryption can be incorporated to overcome the security weaknesses inherent in the 6G communication smart indoor service. In this work, we focus on asymmetric RSA encryption owing to its superior encryption capabilities over other methods, and the methodology thereof is proposed as follows.

The VL channel depicted in Figure 1 is time invariant and it is based on short-range communication (that is, several meters) via the dominant line-of-sight path and multiple weak reflected paths. The path

loss typically has an inverse sixth or higher power attenuation dependence on the communication distance and the fading effect is compensated for by the photodiode diversity effect [22]. In this work, it is assumed that the VL channel contributed by weak reflected paths is negligible in the indoor environment of Figure 1. Thus, the channel impulse response $h_{vlc}(t)$ is approximated as per Equation (1) [23]:

$$h_{vlc}(t) \approx h_{LOS}\delta(t), \quad (1)$$

where h_{LOS} is the channel gain of the dominant direct path and $\delta(\cdot)$ is an impulse response function.

The VL transmitters depicted in the top left of Figure 1 generate the sensing control information, encode it with an asymmetric RSA encryption scheme (public key), and radiate it to the VL channel with a low rate and small communication data format for the smart indoor service in the 6G communication environment. The VL receiver subsequently captures the transferred sensing data in the VL channel (that is, receiving cell C_i in the center left of Figure 1), decodes the encrypted sensing data with a private RSA key, and recovers the sensing signal.

Even if the sensing data are simultaneously captured by an uninvited intruder within the VL channel, it is difficult to decode the intercepted sensing data without the private RSA key. To overcome these challenges resulting from the security weakness, co-channel interference, and overlapping of reception domains, *secure* VL communication with an asymmetric RSA encryption scheme is considered herein.

Figure 1. Example of signal interception owing to security weakness, reception error by co-channel interference, or overlapping of reception domain in environment of smart indoor service based on VL communication for 6G communication.

2.2. Signal Model

To realize VL communication and asymmetric RSA encryption, we consider the VL communication process illustrated in Figure 2 for the smart indoor service. The signal model suitable for this scheme is described below.

The plain text x_s (or control command) in the function diagram of Figure 2 is represented with the binary digital data of L bit frames:

$$x_s \equiv x_s(t) = \sum_{k=0}^{L-1} b_k p(t - kT), \quad (2)$$

where b_k is the signal intensity with a value of 1 or 0, $p(\cdot)$ is the binary digital pulse shape, and T is the time of one bit. The plain text x_s (binary digital data) is transformed into different plain text x_{s10} in decimal form, and a public key set (n_{10}, e_{10}) and private key set (n_{10}, d_{10}) are assigned by the generation algorithm [24] of the RSA encryption key. This process is completed by considering the

random prime numbers p , q and setting $n_{10} = pq$; thereafter, $\phi(n) = (p-1) \times (q-1)$ and a public key e_{10} , which is a co-prime for $\phi(n)$, are selected such that $1 < e_{10} < \phi(n)$, and a private key d_{10} is obtained from the equation $e_{10}d_{10} = 1 \pmod{\phi(n)}$ with the modulo operation in Figure 2.

Figure 2. Function diagram for secure VL communication system based on asymmetric encryption scheme, with VL transmitter and receiver illustrated in (a) and (b), respectively.

Furthermore, the M -bit public key e_{10} is described as

$$e_{10} \equiv e_{10}(t) = \sum_{i=0}^{M-1} k_{ie} p(t - iT_e), \quad (3)$$

and the N -bit private key d_{10} is described as

$$d_{10} \equiv d_{10}(t) = \sum_{j=0}^{N-1} k_{jd} p(t - jT_d), \quad (4)$$

where $k_{ie}, k_{jd} \in \{0, 1, \dots, 9\}$ are the amplitudes of the public and private keys, and T_e, T_d are the bit durations of the public and private RSA keys, respectively.

Subsequently, the plain text x_{s10} is encrypted with the public key e_{10} in the VL transmitter of Figure 2. The RSA encrypted text y_{t10} is determined as follows:

$$y_{t10} = \text{enc}(x_{s10}, e_{10}) = [x_{s10}]^{e_{10}} \pmod{n_{10}}, \quad (5)$$

where $\text{enc}(\cdot)$ represents an encryption operation. The RSA encrypted text in decimal form is converted into the binary encrypted text y_{t2} again and modulated with the carrier signal; that is, it is modulated by an on/off keying–non-return zero (OOK–NRZ) scheme, as in the conventional VL communication technique. The encrypted and OOK–NRZ-modulated asymmetric RSA signals are radiated into the VL channel in Figure 2.

Subsequently, the VL communication signal y_t is described as

$$y_t(t) = Ay_{t2}(t) \times \sin(2\pi f_0 t + \theta), \quad (6)$$

where A , f_0 , and θ are the signal amplitude, frequency, and carrier signal phase, respectively.

If a communication signal arrives at the VL receiver through the VL channel, the VL communication signal y_r acquired at the VL cell C_i in the constructed VL channel is considered to be protected from interception:

$$y_r(t) = h_{vlc}(t) \times y_t(t) = Ah_{LOS}y_{t2}(t)\sin(2\pi f_0t + \theta') + \eta(t), \quad (7)$$

where θ' is the phase component, $\times$ is a convolution operator, and $\eta(t)$ is additive white Gaussian noise. The received signal (or control command) proceeds through a band-pass filter, is OOK demodulated by a non-coherent detection scheme, is received as the demodulated binary digital signal y_{r2} , and is reconverted into the decimal form during the VL reception process indicated in Figure 2. The encrypted text y_{r10} is then decrypted with the private key d_{10} for the asymmetric RSA decryption process in the VL receiver depicted in Figure 2, and the RSA decrypted text or recovered plain text $\hat{x}_{r10}$ is estimated as

$$\hat{x}_{r10} = dec(y_{r10}, d_{10}) = [y_{r10}]^{d_{10}} \{mod n_{10}\}, \quad (8)$$

where $dec(\cdot)$ represents the decryption operation. The text is reconverted into a binary digital signal $\hat{x}_{r2}$, the VL communication process is completed, and the recovered plain text $\hat{x}_r$ is nearly identical to the original plain text x_s .

Following the RSA encryption process in the VL transmitter illustrated in Figure 2, the power P_{enc} generated from the LED array is usually as follows: $P_{enc} = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-T/2}^{T/2} |y_t(t)|^2 dt$.

The total power P_T transferred into the VL channel is expressed by Equation (9):

$$P_T = I(\phi) \times P_{enc}, \quad (9)$$

where the light intensity $I(\phi)$ is represented by $I(\phi) = [(1 + m) / 2\pi] \cos^m \phi$ with the angle of irradiance ϕ , assuming that the LED array is diffuse with a Lambertian emission pattern and the emission order is m .

Once the signal received at the photodiode in the VL receiver has been decoded, the recovered power is determined as follows:

$$P_{dec} = P_L(\phi, \psi, D) \times P_{enc}, \quad (10)$$

where $P_L(\phi, \psi, D) = \cos \phi \cos \psi T(\psi)g(\psi) S / \pi$ yields the path loss through the VL channel, $T(\psi)$, $g(\psi)$ are the characteristic functions of the optical filter and concentrator, respectively, S is the receiving area of the photodiode, D is the distance between the LED array and photodiode, and ψ is the angle of incidence. Then, the reconstructed signal power can be obtained as

$$P_{dec} = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-T/2}^{T/2} |\hat{x}_r(t)|^2 dt. \quad (11)$$

2.3. RSA Encryption Key

As the security performance of the proposed VL communication system is mainly dependent on the data encryption and decryption processes, we explore the statistical properties of the RSA encryption key in this section. The statistical properties of the public and private keys are directly related to the capabilities of the asymmetric RSA encryption and decryption processes.

Figure 3 provides a summary of the key functions for the asymmetric RSA encryption and decryption processes in the proposed technique, which are described in detail in the following. Plain text is used (for example, the text of five characters “VLC” is selected) for VL communication, and according to the ASCII table, these can be expressed as the decimal numbers 34, 118, 108, 99, and 34.

Figure 3. Key function diagram for asymmetric Rivest–Shamir–Adleman (RSA) encryption and decryption processes in proposed VL communication technique for smart indoor service of Figure 1.

If the public key set (that is, $(n_{10}, e_{10}) = (77, 17)$) is given by the key generation function of the VL transmitter and the plain text is encoded by the public key (that is, $e_{10} = 17$) through an asymmetric encryption process in Figure 3, the plain text is converted into encrypted text (that is, the numbers 34, 76, 76, 76, and 34) for secure VL communication.

The asymmetric decryption process in Figure 3 can also be described as follows: the encrypted text (that is, numbers 34, 76, 76, 76, and 34) is transferred to the VL receiver through the VL channel. The private key set, namely $(n_{10}, d_{10}) = (77, 53)$, is provided by the generating function of the RSA decryption key in the VL receiver and the encrypted text is decoded by the RSA private key (that is, $d_{10} = 53$) through the asymmetric decryption process.

Thereafter, the encrypted text is reconverted into plain text (the decimal numbers 34, 118, 108, 99, and 34), which is the same as the original plain text (“VLC”). The objective of the asymmetric encryption process is to *protect* the plain text; that is, to restrict access from adjacent interference or intruders.

It is expected that the statistical performance of the asymmetric encryption process is *dependent* on the bit number; that is, the length of the encryption key. Table 1 displays various public and private key sets obtained from the RSA key generation process.

Table 1. Example of various asymmetric RSA encryption keys.

Prime Numbers (p, q)	Public Key Set (n_{10}, e_{10})	Private Key Set (n_{10}, d_{10})
(11, 7)	(77, 17)	(77, 53)
(11, 127)	(1397, 223)	(1397, 1147)
(11, 1231)	(13,541, 5303)	(13,541, 167)
(11, 12,343)	(135,773, 40,231)	(135,773, 15,931)

As an example, using the prime numbers $p = 11$, $q = 7$ in Table 1, and given that $n_{10} = pq = 77$; set $\phi(n) = (p - 1)(q - 1) = 60$, then take a public key $e_{10} = 17$, which is a co-prime for $\phi(n)$, where $1 < e_{10} < 60$, and we obtain a private key $d_{10} = 53$ from the relation $17d_{10} = 1 \{mod(60)\}$ with the modulo operation. The remaining public and private key sets of Table 1 are obtained via a similar process with various combinations of the prime numbers $p = 11$, $q = 127$, 1231, and 12,343.

We can observe from Table 1 that the bit number (length) of the public key or private key increases as the value of the prime number increases, and the bit number of the public key is always *not equal* to that of the private key. This difference in the bit number of the public or private key between the transmitter and receiver provides a security advantage.

Figure 4 presents the autocorrelation function characteristics of the 16-bit public key for the various combinations of the prime numbers (p, q) in Table 1.

Figure 4. Autocorrelation function characteristics of 16-bit public key set in relation to prime numbers $(p, q) = (11, 7)$, $(11, 127)$, $(11, 1231)$, and $(11, 12,343)$.

It can be observed from Figure 4 that the autocorrelation function (black solid dotted line) for the public key set $(n_{10}, e_{10}) = (13,541, 5304)$ generated by the prime numbers $(p, q) = (11, 1231)$ exhibited the smallest fluctuations among the various combinations of the prime numbers (p, q) of Table 1 under SNR = 20 dB. The interval between the main lobe and side lobe also had the smallest value, indicating the best security performance owing to the orthogonality of the encryption key. Therefore, the small-value public key set $(n_{10}, e_{10}) = (13,541, 5304)$ generated by the prime numbers $(p, q) = (11, 1231)$ provided the best security performance for the RSA encryption process under good SNR conditions (i.e., SNR = 20 dB).

Figure 5 presents the autocorrelation function characteristics of the private key with respect to the key length for the various combinations of the prime numbers (p, q) in Table 1 and SNR = 20 dB. It can be observed that the autocorrelation of the 16-bits private key exhibited similar fluctuations for the various combinations of the prime numbers $(p, q) = (11, 7)$, $(11, 127)$, $(11, 1231)$, and $(11, 12,343)$ under normal SNR conditions.

Figure 5. Autocorrelation function characteristics of 16-bit private key set with prime numbers $(p, q) = (11, 7)$, $(11, 127)$, $(11, 1231)$, and $(11, 12,343)$.

This confirms that the 16-bit private key set provided similar security performance for various prime number combinations similar to the characteristic of the 8-bit private key set, compared with a previous research [21].

3. Experiments and Performance Analysis

3.1. Numerical Study of Asymmetric Encryption Process

A numerical study was designed to investigate the signal flow of the asymmetric encryption and decryption function diagram depicted in Figure 2 by computer simulation. The SNR was 0.27 or -5.68 dB. The normal conditions of the LED transmitted power, the irradiance angle of the LED array, the photodiode incident angle, the photodiode field of view, and the photodiode receiving area were given for numerical simulation study of LED and photodiode characteristic: the LED transmitted power was $P_{enc} = 20$ mW, the irradiance angle of the LED array was $\phi = 3^\circ$, the photodiode incident angle was $\psi = 10^\circ$, the photodiode field of view was $\psi_c = 20^\circ$, and the photodiode receiving area was $A = 0.78$ cm².

In the simulation study, we set the plain text x_s to the ASCII character “U”, which is equal to the decimal number “85” or the 16-bit binary number 0000000001010101. The signal output for the generation of plain text in the VL transmitter-based asymmetric encryption scheme in Figure 2a is represented as the binary digital waveform in Figure 6a.

The key generation for the asymmetric RSA encryption process is described as follows: The prime numbers $p = 11$, $q = 7$ were selected and generated $n_{10} = 77$, the function $\phi(n) = 60$, and a public key $e_{10} = 13$ that was a co-prime for $\phi(n)$, where $1 < e_{10} < 60$; this resulted in a private key $d_{10} = 37$ from the relation $7d_{10} = 1 \{mod(60)\}$.

The waveform of the public key is illustrated in Figure 6b, where the public key was the 16-bit binary number 0000000000001101. The waveform output of the private key in Figure 2b was equal to that of Figure 7c where the private key was the 16-bit binary number 000000000100101.

The plain text of the binary number representation 0000000001010101 (the character “U”) was encoded into the encrypted signal of the binary number 0000000001001100 (the decimal number “76”) by the public key with the binary number 0000000000001101 (the decimal number “13”). The encrypted signal is represented by the waveform in Figure 6c. The encrypted signal was again modulated by the OOK–NRZ scheme following the asymmetric RSA encryption process.

The encrypted and modulated signal was then radiated into the VL channel, and the radiated signal for the VL channel is illustrated in Figure 6d.

In actual VL communication for smart indoor services in the 6G communication environment, the radiated signal may be severely distorted by noise effects or co-channel interference as well as severe path loss. We considered only the channel effect of additive white Gaussian noise in this simulation. The signal received at the photodiode is represented in Figure 7a for the condition of SNR = -5.68 dB.

The received signal was demodulated by the band-pass filter of the non-coherent detector scheme depicted in Figure 2b and decrypted by the private RSA key with the binary number 000000000100101 (the decimal number “37”), resulting in the waveforms illustrated in Figure 7b,c, respectively. The recovered signal is represented in Figure 7d, which was the binary number 0000000001010101 (the decimal number “85” or the ASCII character “U”).

It can be concluded from this simulation study that the proposed VL communication technique and asymmetric RSA encryption process were effectively implemented with the public and private RSA encryption key lengths and 16-bit data length under SNR conditions above -5.68 dB.

Figure 6. Signal waveforms of major functions in proposed VL transmitter of Figure 2a.

Figure 7. Signal waveforms of major function outputs in proposed VL receiver of Figure 2b.

3.2. Estimation Error Depending on RSA Encryption Key

The performance analysis of the estimation error of the VL communication system with various RSA encryption keys is described in this section. The estimation error calculated for the proposed VL receiver in Figure 2b is described as $\epsilon = |\hat{x}_{r2} - x_s|$, where $\hat{x}_{r2}$ is the waveform of Figure 7d and x_s is the waveform of Figure 6a. Subsequently, the root mean square error (RMSE) of the signal estimation can be written as

$$\text{RMSE} \equiv \sqrt{\sum_{l=1}^n \frac{\epsilon_l^2}{n}}, \quad (12)$$

where n is the number of samples.

The simulation studies were performed with the MATLAB software tool to evaluate the performance of the proposed technique. The VL communication simulator was constructed with the same architecture as that in Figure 2, where 8-bit data of plain text or the VL control command x_s were generated, encrypted by an 8-bit public encryption key (n_{10}, e_{10}) generated under various

combinations with four q prime numbers ($q = 7, 127, 1231$, and $12,343$) and $p = 7$, or with four p prime numbers ($p = 7, 127, 1231$, and $12,343$) and $q = 7$, and modulated with the OOK–NRZ scheme. Moreover, the modulated and encrypted signals were emitted into the VL channel of the additive white Gaussian noise effect.

The transferred signal was captured by the photodiode of the VL receiver, demodulated by the band-pass filter, decoded with the 8-bit private RSA key (n_{10}, d_{10}), and reconverted into 8-bit original plain text. To investigate the dependence of the estimation error on the RSA encryption method, the RMSE of Equation (12) was calculated using the constructed simulator, the results of which are represented in Figures 8 and 9.

Figure 8. Root mean square error (RMSE) performance depending on various q prime numbers in proposed VL communication technique based on asymmetric encryption scheme.

Figure 9. RMSE performance depending on various p prime numbers in proposed VL communication technique based on asymmetric data encryption scheme.

Figure 8 demonstrates three important points: First, the proposed VL communication technique provided better RMSE performance as the q prime number *increased*; for example, the performance curve for the RSA key set with prime numbers $p = 7$ and $q = 1231$ (black diamond dotted line in

Figure 8) was the *best* among the RSA keys with $p = 7$ and $q = 7, 11, 127$, and 1231. Its result matches with the previous research [21].

Second, the proposed method yielded effective RMSE performance under public and private RSA keys with high values (the 3- and 4-bit decimal numbers in Table 2), as indicated by the black diamond dotted line in Figure 8. Finally, the VL communication technique with or without RSA encoding exhibited similar RMSE performance in the case of RSA keys with two-bit decimal numbers in Table 2 (public and private RSA keys with low values).

Table 2. Public and private RSA key sets generated by various q prime numbers.

Prime Numbers (p, q)	Example of Public Key Set		Example of Private Key Set	
	(n_{10}, e_{10})	Public Key Length	(n_{10}, d_{10})	Private Key Length
(7, 7)	(49, 29)	2-bit decimal number	(49, 5)	1-bit decimal number
(7, 11)	(77, 53)	2-bit decimal number	(77, 17)	2-bit decimal number
(7, 127)	(889, 223)	3-bit decimal number	(889, 139)	3-bit decimal number
(7, 1231)	(8716, 457)	3-bit decimal number	(8716, 2713)	4-bit decimal number

Similarly, Figure 9 demonstrates three interesting facts. First, the proposed VL communication technique provided better RMSE performance as the p prime number increased. It matches with the previous research result [21]. For example, the RMSE performance for the RSA key set with the prime numbers $q = 7$ and $p = 1231$ (black diamond dotted line in Figure 9) was the best among the RSA key sets of Table 3. Second, the proposed method achieved effective RMSE performance under public and private RSA keys of high values (the keys with 4-bit decimal numbers in Table 3). Finally, the proposed technique with and without RSA encoding exhibited similar RMSE performance with RSA keys of 2-bit decimal numbers in Table 3 (public and private RSA keys with low values).

Table 3. Public and private key sets depending on various p prime numbers.

Prime Numbers (p, q)	Example of Public Key Set		Example of Private Key Set	
	(n_{10}, e_{10})	Public Key Length	(n_{10}, d_{10})	Private Key Length
(7, 7)	(49, 29)	2-bit decimal number	(49, 5)	1-bit decimal number
(11, 7)	(77, 19)	2-bit decimal number	(77, 19)	2-bit decimal number
(127, 7)	(889, 23)	2-bit decimal number	(889, 263)	3-bit decimal number
(1231, 7)	(8716, 2833)	4-bit decimal number	(8716, 5197)	4-bit decimal number

It can be observed from the simulation results of Figures 8 and 9 that the proposed VL communication technique based on the asymmetric RSA encryption scheme yielded better RMSE performance with longer RSA key lengths under conditions with the same SNR value.

3.3. Estimation Error Depending on Data Bit Length

The estimation error of the proposed VL communication technique was studied for various data lengths (bit numbers). The VL communication simulator was constructed with the same architecture as that depicted in Figure 2, where the plain text x_s was generated, encrypted by a public RSA key (n_{10}, e_{10}) with q prime numbers ($q = 127$ and 1231), and modulated with the OOK–NRZ scheme. Furthermore, the modulated and encrypted signals were sequentially emitted into the additive white Gaussian noise VL channel.

Figure 10 indicates that the proposed VL communication technique generally exhibited *worse* RMSE performance as the data bits *increased*. For example, the performance curve for the 32-bit data VL communication (red cross dotted line of Figure 10) was the worst among the 8-, 16-, and 32-bit data VL communication under the RSA key set with $p = 7$ and $q = 127$.

Figure 10. RMSE performance comparison with 8-, 16-, and 32-bit data lengths under prime numbers $p = 7$ and $q = 127$ or 1231.

However, Figure 10 also demonstrates that the proposed technique provided better RMSE performance under the same data bit length conditions as the q prime number increased. For example, the RMSE performance for the RSA key set with the prime numbers $q = 1231$ and $p = 7$ (black solid dotted line of Figure 10) was better than that of the RSA key sets with the prime numbers $q = 127$ and $p = 7$ (magenta cross dotted line of Figure 10).

3.4. Real Experiment with Test Bed

The specific embedded test bed for implementing the VL communication methodology proposed in Section 2.1 was established using two general-purpose embedded boards, an LED array module, and photodiode modules, as illustrated in Figure 11. A real experiment was conducted with the test bed using the proposed technique, as indicated in Figure 11a,d.

Figure 11. Real VL communication experiment with proposed VL communication process and test bed.

The center of Figure 11a,c presents the specific embedded VL reception system with the photodiode module, where the asymmetric encrypted and OOK–NRZ-modulated signals captured at the VL

channel were demodulated and decoded using the private key. Similarly, the center top side of Figure 11a,b shows the prototype of the specific embedded VL transmission system with the LED array module, where the VL communication signal was encoded using the public key and processed by the OOK–NRZ scheme.

The real VL communication experiment based on the asymmetric encryption scheme was conducted under the condition of a distance of 55.2 cm between the two modules (the specific embedded VL reception and transmitter modules), as illustrated in Figure 11d. A laser distance meter and PC system controller (the secure VL transmitter and secure VL receiver in Figure 11a) were used for the distance measurement and 8- or 16-bit data generation. The luminance intensity was measured as 1862 lux at the receiving embedded module of the secure VL receiver using a lux meter.

The real experiment with the proposed VL communication process based on the asymmetric RSA encryption scheme shown in Figure 2 was executed as follows: The test bed illustrated in Figure 11a was operated, and the encrypted and modulated signals were generated by the secure VL transmitter and radiated into the VL channel. The data were provided as the binary number 01010101 (the decimal number “85”), the 8-bit public key in Table 4 used the binary number 00010001 (the decimal number “17”) for the RSA encoding with (11, 7) in Table 4, the encoded signal was provided as the binary value of 01001100 (the decimal number “76”), and the OOK–NRZ scheme was used for modulation in the transmitting embedded module of the secure VL transmitter.

Table 4. Results of real experiment with test bed.

Coding Method with Prime Numbers (p, q)	Example of Public/Private Key (e_{10}, d_{10})	Success Rate of VL Communication	Data Bit Length
Without coding	None	65%	8
RSA coding with (11, 7)	(17, 53)	80%	8
RSA coding with (11, 127)	(13, 97)	55%	16
RSA coding with (11, 1231)	(421, 1081)	55%	16

The secure VL receiver captured the encrypted and modulated signals in the VL channel by the photodiode module, decoded these by using the 8-bit private key with a binary value of 00110101 (the decimal number “53”) in Table 4 following the demodulation process, and recovered the signals into the data provided as the binary number 01010101 (the decimal number “85”). After 100 trial experiments, the success rate of the proposed VL communication exhibited a maximum value of 80% under an SNR above 5.58 (dB), as indicated in Table 4.

Similarly, the 16-bit public key used the binary number 0000000000001101 (the decimal number “13”) for the RSA encryption and the 16-bit private key used the binary number 0000000001100001 (the decimal number “97”) for the RSA decoding with the prime numbers (p, q) = (11, 127) in Table 4. After 100 trial experiments, the success rate of the proposed VL communication exhibited a maximum value of 60% under an SNR above 5.08 (dB).

Two interesting points can be observed from Table 4. First, the success rate of the VL communication based on the RSA encryption scheme was better than that of the VL communication without coding, as in the simulation results of Figure 8. Second, the success rate of the VL communication based on the RSA encoding scheme decreased as the data bit length increased, similar to the research results presented in Figure 10.

The results of the real experiment in Table 4 reveal that the success rate of the proposed VL communication technique based on the RSA encoding scheme was superior to that without coding, decreased as the data bit length increased, and exhibited better performance than that without RSA encryption under conditions of the same data length. Moreover, the additional channel coding scheme was naturally required as the data bits increased.

4. Conclusions

A notable feature of the asymmetric RSA encryption technique with public and private keys is that it provides better security performance; for example, the asymmetric encryption between the transmitter and receiver solves the problem inherent in distributing the secret key. Furthermore, we note that the asymmetric encryption scheme is preferred for security enhancement with smart indoor services using the VL communication technique, which is the key technique of 6G communication. The optimum key length for the public or private encryption code, the security performance of the VL communication as a function of the key and data lengths, and the asymmetric encryption scenario for a system with secure VL control have been studied in detail.

The security performance was found to be primarily dependent on the data encryption process, which was closely related to the statistical properties of the public and private keys in the asymmetric RSA encryption and decryption processes. As such, we could confirm that the public key set with $(n_{10}, e_{10}) = (13,541, 5304)$, generated by the prime numbers $(p, q) = (11, 1231)$, provided the *best* security performance for the RSA encryption process in the VL communication under normal SNR conditions, and the private key set provided similar security performance with various prime number combinations.

In the numerical study of the asymmetric data encryption algorithm, the proposed VL communication technique and asymmetric RSA encryption process were effectively implemented with various RSA key and data lengths under normal SNR conditions.

The RMSEs were calculated to investigate the estimation error of the VL communication as a function of the RSA encryption method and the simulation results were presented.

We observed from the simulation studies that the VL communication technique based on the asymmetric encryption usually provided better RMSE performance as the length of the p or q prime number increased, yielded effective RMSE performance under public and private encryption keys of high values, resulted in worse RMSE performance as the data bit increased, and yielded better RMSE performance under the condition of longer encryption keys under the same SNR values.

The real experiment demonstrated that the success rate of the VL communication technique based on RSA encoding was better than that without coding, decreased as the data bit length increased, and exhibited superior performance over that without RSA encryption for conditions of the same data length.

However, it must be acknowledged that, in its current form, the proposed VL communication technique requires higher computation time as well as more number of operations than the conventional technique. Hence, further research is required to optimize it and achieve secure multiband and ultrafast speed communication in the 6G communication environment.

Funding: This research was funded by [a National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT)] grant number [2020R1H1A200649].

Conflicts of Interest: The author declares no conflict of interest.

References

1. Rehman, S.U.; Ullah, S.; Chong, P.H.J.; Yongchareon, S.; Komosny, D. Visible Light Communication: A System Perspective—Overview and Challenges. *Sensors* **2019**, *19*, 1153. [\[CrossRef\]](#)
2. Pathak, P.H.; Feng, X.; Hu, P.; Mohapatra, P. Visible Light Communication, Networking, and Sensing: A Survey, Potential and Challenges. *IEEE Commun. Surv. Tutorials* **2015**, *17*, 2047–2077. [\[CrossRef\]](#)
3. Yang, P.; Xiao, Y.; Xiao, M.; Li, S. 6G Wireless Communications: Vision and Potential Techniques. *IEEE Netw.* **2019**, *33*, 70–75. [\[CrossRef\]](#)
4. Strinati, E.C.; Barbarossa, S.; Gonzalez-Jimenez, J.L.; Ktenas, D.; Cassiau, N.; Maret, L.; Dehos, C. 6G: The Next Frontier: From Holographic Messaging to Artificial Intelligence Using Subterahertz and Visible Light Communication. *IEEE Veh. Technol. Mag.* **2019**, *14*, 42–50. [\[CrossRef\]](#)

5. Zhang, Z.; Xiao, Y.; Ma, Z.; Xiao, M.; Ding, Z.; Lei, X.; Karagiannidis, G.K.; Fan, P. 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. *IEEE Veh. Technol. Mag.* **2019**, *14*, 28–41. [\[CrossRef\]](#)
6. Haas, H.; Yin, L.; Chen, C.; Videv, S.; Parol, D.; Poves, E.; Alshaer, H.; Islim, M.S. Introduction to indoor networking concepts and challenges in LiFi. *J. Opt. Commun. Netw.* **2019**, *12*, A190–A203. [\[CrossRef\]](#)
7. Chow, C.-W.; Shiu, R.-J.; Liu, Y.-C.; Yeh, C.-H.; Liao, X.-L.; Lin, K.-H.; Wang, Y.-C.; Chen, Y.-Y. Secure Mobile-Phone Based Visible Light Communications with Different Noise-Ratio Light-Panel. *IEEE Photonics J.* **2018**, *10*, 1–6. [\[CrossRef\]](#)
8. Hussein, H.S.; Hagag, M.; Farrag, M.; Hussein, H.S. Extended Spatial-Index LED Modulation for Optical MIMO-OFDM Wireless Communication. *Electronics* **2020**, *9*, 168. [\[CrossRef\]](#)
9. Keskin, M.F.; Sezer, A.D.; Gezici, S. Localization via Visible Light Systems. *Proc. IEEE* **2018**, *106*, 1063–1088. [\[CrossRef\]](#)
10. Wang, H.; Kim, S. Decoding of Polar Codes for Intersymbol Interference in Visible-Light Communication. *IEEE Photonics Technol. Lett.* **2018**, *30*, 1111–1114. [\[CrossRef\]](#)
11. Fu, M.; Zhu, W.; Le, Z.; Manko, D. Improved visible light communication positioning algorithm based on image sensor tilting at room corners. *IET Commun.* **2018**, *12*, 1201–1206. [\[CrossRef\]](#)
12. Wu, F.; Chen, L.; Cai, S.; Wang, W. Experimental Study and Application of Response Mask Invariant Characteristic for Generalized Visible Light Communication Channel. *IEEE Photonics J.* **2018**, *10*, 1–12. [\[CrossRef\]](#)
13. Kumar, A.; Ghorai, S.K. High-gain and volume-efficient concave–convex lens for multiple-input multiple-output visible light communication system. *Opt. Eng.* **2020**, *59*, 035106. [\[CrossRef\]](#)
14. IEEE Standard for Local and Metropolitan Area Networks—Part 15.7: Short-Range Wireless Optical Communication Using Visible Light. In *IEEE Standard 802.15.7-2018 (Revision of 2011)*; IEEE: Piscataway, NJ, USA, 2011; pp. 1–309.
15. Mousa, F.; Son, T.T.; Burton, A.; Le Minh, H.; Ghassemlooy, Z.; Duong, T.Q.; Boucouvalas, A.C.; Perez, J.; Dai, X. Investigation of data encryption impact on broadcasting visible light communications. In Proceedings of the 2014 9th International Symposium on Communication Systems, Manchester, UK, 23–25 July 2014; pp. 390–394.
16. Okuda, K.; Murata, M.; Nakamura, T.; Uemura, W.; Yamamoto, T. Proposal and development of encryption key distribution system using visible light communication. In Proceedings of the 2011 IEEE International Conference on Consumer Electronics -Berlin (ICCE-Berlin), Berlin, Germany, 6–8 September 2011; pp. 71–73.
17. Terra, D.; Kumar, N.; Lourenço, N.; Alves, L.N.; Aguiar, R.L. Design, development and performance analysis of DSSS-based transceiver for VLC. In Proceedings of the 2011 IEEE EUROCON—International Conference on Computer as a Tool, Lisbon, Portugal, 27–29 April 2011; pp. 1–4.
18. Yi, Y.; Li, C.; Lee, K. Optimum Spread Code Applied in Indoor Visible Light Data Transmission for Optical Multipath Dispersion Reduction. *IETE Tech. Rev.* **2013**, *30*, 233. [\[CrossRef\]](#)
19. Lee, Y.U. Visible Light Localization Technique Based on the Stream Encryption Key. *IETE Tech. Rev.* **2015**, *32*, 454–461. [\[CrossRef\]](#)
20. Al Hasib, A.; Haque, A.A.M.M. A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography. In Proceedings of the 2008 Third International Conference on Convergence and Hybrid Information Technology, Busan, Korea, 11–13 November 2008; Volume 2, pp. 505–510.
21. Lee, Y.U.; Kang, K.-Y.; Choi, G. Secure Visible Light Encryption Communication Technique for Smart Home Service. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 0827–0831.
22. Al-Kinani, A.; Wang, C.-X.; Zhou, L.; Zhang, W. Optical Wireless Communication Channel Measurements and Models. *IEEE Commun. Surv. Tutorials* **2018**, *20*, 1939–1962. [\[CrossRef\]](#)
23. Jungnickel, V.; Pohl, V.; Nonnig, S.; Von Helmolt, C. A physical model of the wireless infrared communication channel. *IEEE J. Sel. Areas Commun.* **2002**, *20*, 631–640. [\[CrossRef\]](#)

24. Muhammad, N.; Zain, J.M.; Saman, Y.M. Loop-based RSA key generation algorithm using string identity. In Proceedings of the 2013 13th International Conference on Control, Automation and Systems (ICCAS 2013), Gwangju, Korea, 20–23 October 2013; pp. 255–258.

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

© 2020 by the author. 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/>).