VNIVERSITAT DE VALÈNCIA

Citation for the original published paper:

F. Mousa et al., "Investigation of data encryption impact on broadcasting visible light communications," 2014 9th International Symposium on Communication Systems, Networks & Digital Sign (CSNDSP), 2014, pp. 390-394, doi: 10.1109/CSNDSP.2014.6923860

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Investigation of Data Encryption Impact on Broadcasting Visible Light Communications

Farag Mousa[1], Tran The Son [1], Andrew Burton[1], Hoa Le Minh[1], Zabih Ghassemlooy[1], Trung Q. Duong[2], Anthony C. Boucouvalas[3], Joaquin Perez[4], and Xuewu Dai[1]

[1] *Optical Communications Research Group, NCRLab, Faculty of Engineering and Environment, Northumbria University, Newcastle upon Tyne, NE1 8ST, UK*

{farag.mousa, tran.t.son, andrew.burton, hoa.le-minh, z.ghassemlooy, xuewu.dai}@northumbria.ac.uk

[2] *Queen's University Belfast, Belfast, BT7 1NN, UK,* trung.q.duong@qub.ac.uk

[3] *University of Peloponnese, Dept. of Telecoms Science and Tech., Tripoli, Greece,* acb@uop.gr

[4]*Optical Quantum and Communications Group, Institute of Telecommunications and Multimedia Applications (iTEAM), Universitat Politècnica de València, 46022, Spain*, joapeso@upv.es

***Abstract*—This paper investigates the impact of data encryption and decryption in indoor broadcasting visible light communications (VLC) system embedded in the physical layer. The RSA encryption has been implemented to provide a secure data transmission in the physical layer. The paper shows that the bit error rate (BER) performance for the un-secured and secured VLC systems (8 and 12-bit) for data rates of 2 and 12 Mbps. For a BER of 10^{-4} we show that there is 2-4 dB power penalties with the secured VLCs. Investigation of key length impact on the error propagation as well as power penalty is also carried out.**

Keywords— VLC; RSA; encryption; decryption; BER; power penalty.

I. INTRODUCTION

A visible light communications (VLC) system employing white light emitting diodes (LED) and an optical receiver can provide data communications within rooms, offices, trains, etc. A basic indoor broadcasting VLC system is shown in Fig. 1, capable of offering both illumination as well as data communications by using a number of LED arrays mounted on the ceiling of the room. An optical receiver located on a receiving plane, such as a desk, can capture the data from transmitted optical beams. Advantages of VLC compared to standard RF communications on indoor environments are highly secured data transmission (beam is confined within a well-defined area, therefore difficult to tap without the user not noticing it), free from electromagnetic interference, high power efficiency and it meets the human eye-safety standard [1].

Most existing research works on VLC systems are focused on improving the data rate over the limited bandwidth offered by LEDs, which is mainly due to the device structure [2], [3]. Gbit/s data rate communications has been achieved using complex modulation scheme and parallel transmission (multiple-input-multiple-output - MIMO) systems [4], [5]. There have been attempts to implement security with chaotic encryption methods in VLC [6]. Nevertheless the security issues in VLC application has not yet been considered thoroughly as in the RF counterpart. Further, the chaotic system will take remarkable time to compute outcome if the initial condition, which usually occurs in real systems, is missing.

The light beam is mainly confined and can be shaped in specific patterns using optics to provide the security feature for wireless communications in the physical layer, i.e. no light signal leakage outside the designated illumination area. However, any unauthorized user with optical receiver located inside this illumination area will be able to receive the signal but unable to decode it. Note that VLCs offer both illumination and data communications, therefore by nature the light foot print needs to be wide and potentially be observed by unauthorized users.

Data cryptography will add further security strength to the transmitted signal in VLCs by providing the intended users with a unique code (key). The encrypted light beam will provide a good protective measure against the unauthorized users who are within the illumination area. In [7] the initial work has investigated a security concept for the hybrid RF and VLC network; however it is mainly for supporting the key management in RF links. In this paper we propose an implementation of the encryption/decryption for VLCs by using the public key cryptography (RSA algorithm) in the physical layer and investigate the impacts of data encryption on VLC broadcasting, i.e., signal-to-noise ratio (SNR), penalty, and the time delay for decryption.

The rest of this paper is organized as follows. Section II discusses the data encryption/decryption principle and the algorithm used for VLC based broadcasting. The proposed model is described in Section III and then evaluated in Section IV including bit error rate (BER) and the power penalty for the encrypted VLC system. Section V concludes the paper and discusses some future works.

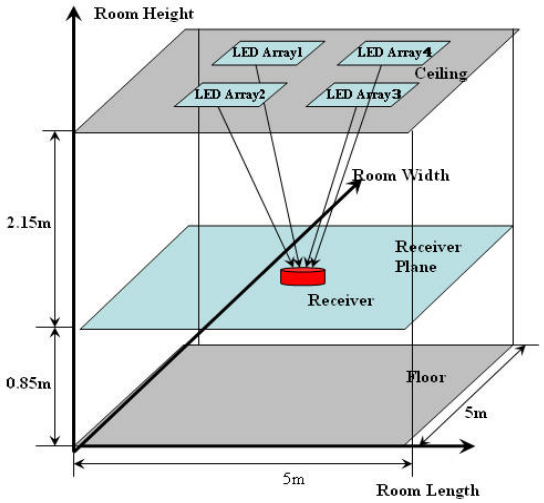


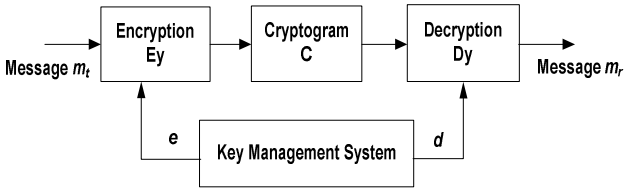
Fig. 1. A typical indoor VLC system

II. CRYPTOGRAPHY

A. Principle

The cryptography technique provides the capability in which information can be hidden in ciphers and then only detected by the authorized users who have the valid secret key, thus making it very difficult for the message to be cracked by un-authorized recipients. In this scheme the original message is enciphered (or in travesty from) so that only the authorized receiver can read the message (decipher it). Cryptography covers all the efforts to produce a secure transmission of information including different aspects, for example confidentiality, data integrity, authentication and non-repudiation. The mechanisms used to achieved these requirements are quite complex as outlined in [8].

In cryptography, there are three main elements including data encryption, data decryption, and key management unit. As shown in Fig. 2, encryption module (enciphering) includes the operations of converting the data stream into an unreadable form to all, i.e., cryptogram, except the intended recipient. At the receiver, the decryption module will decipher the encrypted message by the given key. The key management system manages generation, distribution, recognition, and reception of the cryptographic keys, which is the most crucial element in any cryptographic systems [9].



m_t Transmitted data
E_Y Encryption algorithm
e Encryption key
C_Y Cryptogram
m_r Received data
D_Y Decryption algorithm
d Decryption Key

Fig. 2. General cryptographic functions

There are two types of ciphers, symmetric and asymmetric. The former is known as the conventional encryption, which uses the same key for encryption and decryption of the data such as DES, AES and OTK [10]. The latter which is referred to as the public key cryptography encrypts and decrypts data by two different keys (public and private) [11]. The public key is used to encrypt the message whilst the private key is employed for decrypting the message.

In practice, there are two well-known public key algorithms: Rivest-Shamir-Adleman (RSA) and Elliptic curve cryptography (ECC). Though ECC is an emerging encryption algorithm, RSA is widely used in many security systems and still guarantees the security if the key length is long enough. Therefore, we have adopted it in this work [12].

B. RSA Algorithm

Key generation

In RSA, public and private keys are generated by a series of mathematical steps as follows:

1. Generate two large different prime numbers p and q
2. Compute $n = p \times q$
3. Compute the Euler Totient Function $\Phi(n) = (p-1) \times (q-1)$
4. Select a random the encryption key e, where $1 < e < \Phi(n)$, $\gcd(e, \Phi(n)) = 1$
5. Calculate the private exponent value for the decryption key d such that $d = e^{-1} \bmod \Phi(n)$
6. Public key = $[e, n]$ and private key = $[d, n]$ [13].

Encryption/decryption

As shown in the transmit message m_t $(0 \le m_t < n)$ is encrypted by the public key at the sender by applying following expression [12]:

$$C = m_t^e \bmod n \quad (1)$$

At the receiver, the original message will be recovered by:

$$m_r = C^d \bmod n \quad (2)$$

III. SYSTEM DESCRIPTION AND SIMULATION SETUP

A. VLC Encryption and Decryption

Without loss of generality, it is assumed that the public and private keys are provided at the transmitter and receiver (i.e. during initialization session connections or presetting).

Fig. 3 illustrates the schematics system block diagram of RSA algorithm adopted in VLC systems shown in Fig. 1. The binary stream (data) is converted into k-bit parallel blocks (k = 8, 16, 32), where k is chosen as the same length as the key. These blocks are then converted into decimal values and encrypted by pre-defined public key as described in Eq. (1). The encrypted data is passed through a parallel-to-serial converter with an output in OOK-NRZ format which is used to intensity modulate the LED.

At the receiver end, following optical detection the reverse process of transmitter is implemented to recovery the original data signal. The private key is employed for decryption as described in the Eq. (2).

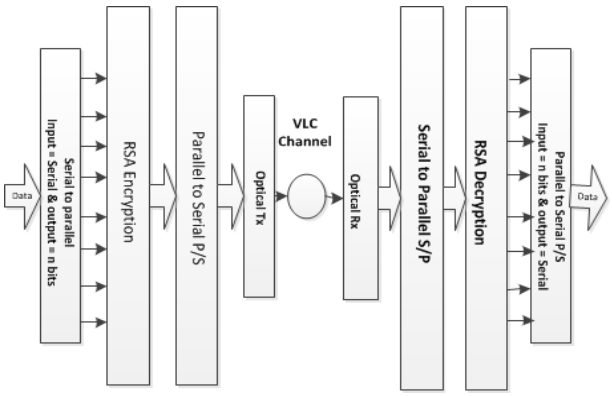


Fig. 3. Block diagram of RSA applied in VLC system

B. *Visible Light Communications Simulation Setup*

The VLC system shown in Fig. 1 is adopted for a standard room of size 5×5×2.5 m (width, length, and height) where the number of LED arrays used is 9 to provide good room illumination coverage. Here we consider both the line-of-sight (LOS) and diffused configurations. The system is numerically simulated in Matlab. The total received optical power P_{rx} by the user is given by:

$$P_{rx} = \sum_i \left(P_{tx} H_{LOSi}(0) + \int_{walls} P_{tx} dH_{refi}(0) \right), \quad (3)$$

where i is the index of the i^{th} LED transmitter. P_{tx} is the transmit power of LED. The LOS channel gain H_{LOSi} is computed as [1, 2] for $0 \le \psi \le \Psi_c$ where ψ is the light ray reception angle and Ψ_c is the maximum field of view (FOV) of the receiver.

$$H_{LOS}(0) = \frac{(m+1)A}{2\pi D_d^2} \cos^m(\phi)\, T_s(\psi) g(\psi) \cos(\psi) \quad (4)$$

where $T_s(\psi)$ and $g(\psi)$ are the gains of the optical filter and concentrator, respectively, m is the Lambertian order (m = -ln(2)/ln(cos($\phi_{1/2}$)), and $\phi_{1/2}$ is the semi angle of the LED. The optical concentrator gain is given by:

$$g(\psi) = \begin{cases} \frac{n^2}{\sin^2(\Psi_c)}, & 0 \le \psi \le \Psi_c \\ 0, & \psi > \Psi_c \end{cases} \quad (5)$$

where n is the refractive index of the concentrator. Hence the received optical power from the LOS path is given by:

$$P_{rx} = H_{LOS}(0) P_{tx} \quad (6)$$

The diffused signal is determined as the summation of all reflected beams to receiver. Each path gain is calculated as [9]:

$$dH_{ref}(0) = \frac{(m+1)A}{2\pi^2 D_1^2 D_2^2} \rho dA_{wall} \cos^m(\phi) \cos(\alpha) \cos(\beta)\, T_s(\psi) \times g(\psi) \cos(\psi), \quad (7)$$

The simulation model for the direct LOS and a single bounce simulation is shown in Fig. 4.

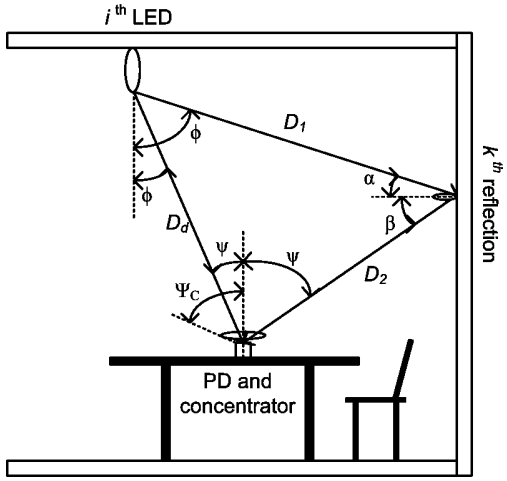


Fig. 4 Simulation model for the direct LOS and a single bounce.

The data signal $x(t)$ is generated using a pseudo random bit stream (PRBS) of length 2^{10}-1. The data is transmitted via the LED array and is given by:

$$x'(t) = x(t) \otimes h_{LED}(t) \quad (8)$$

where $h_{LED}(t)$ is the LED impulse response and $\otimes$ stands for convolution. Hence the received signal is given by:

$$y(t) = x'(t) \otimes h^0(t; S, D) + n(t) \quad (9)$$

where h^0(t) is the channel impulse response, and $n(t)$ is additive white Gaussian noise due to the ambient light sources. The channel impulse response $h^0(t; S, D)$ for a particular source $S(x,y,z)$ and detector $D(x,y,z)$ can be approximated by a scaled Dirac delta function. However, as the LED device is nonlinear, see the impulse response Fig. 5, and the channel is diffused, h_{chnl}(t) the light signal will undergo spreading due to multiple propagation as defined in Eq. (7).

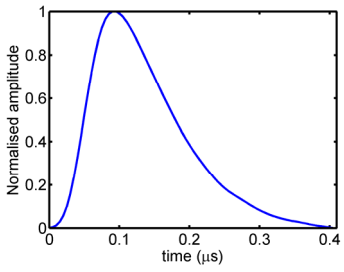


Fig. 5. OSRAM white LED impulse response

In the encrypted VLC system we have used the measured impulse response of OSRAM white LED, which has a raw bandwidth of 2.5 MHz, see Fig. 5 and the key simulation parameters presented in Table 1.

IV. Performance Evaluation

The secure VLC system is simulated using Matlab to determine the impact of security implementation on the LED-based VLC system. The key system performance indicators to investigate are the BER, and the power

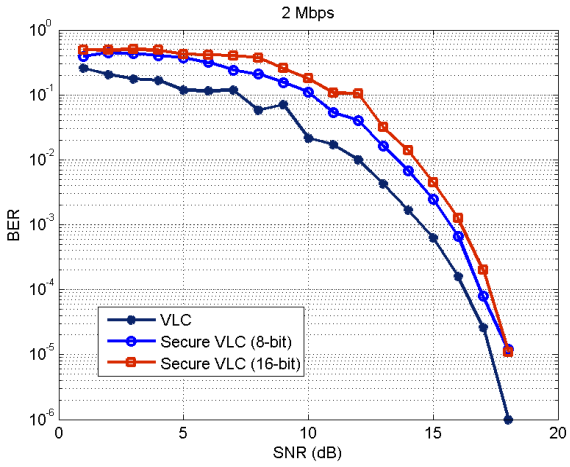
penalty. The VLC model was based on Eqs. (3) – (9) whereas the data encryption layer is followed by steps 1-6 and Eqs. (1) and (2). In this paper the maximum encryption key length used for simulation is limited to 16 bits. This is due to the constraints of computational power of PC and the simulator. However, we have kept the ratio between input and output data to and from the RSA Encryption block the same (see Fig. 3), i.e., $k/(k+1)$, which can be applied for longer key length as in practical applications. However, the simulation results obtained are still valid for predicting the impacts of encryption on VLC communications.

Table 1. VLC system parameters

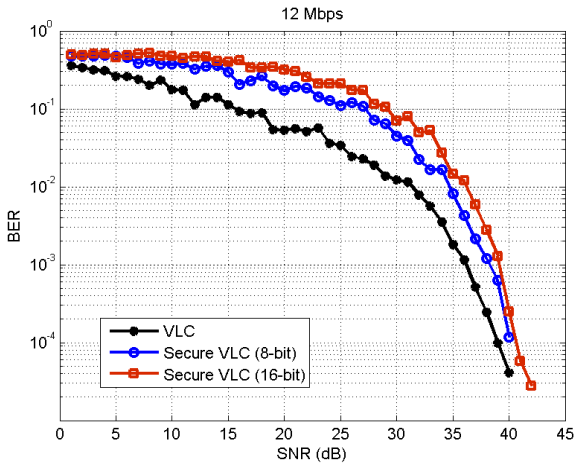
Parameters	**Values**
Room X	5 m
Room Y	5 m
RP to ceiling	2.5 m
LED half power angle $\phi_{1/2}$	70 deg
Wall reflection coefficient ρ	0.7
Number of reflections	1
Reflective area of wall dA_{wall}	0.02 m^2
Transmitter coordinates (9 arrays of LEDs)	(0.3,0.3) (2.5,0.3) (4.7,0.3) (0.3,2.5) (2.5,2.5) (4.7,2.5) (0.3,4.7) (2.5,4.7) (4.7,4.7)
LED raw modulation bandwidth	2.5 MHz
Concentration lens refractive index n	1.5
Optical filter gain $T_s(\psi)$	1
PIN detector FOV	60 deg
Detector area A	1 cm^2
Transmit optical power P_{tx}	1 W
Data format	NRZ-OOK
Key length	8 and 16 bits
Data block	8 and 16 bits

In this the simulation we transmit over 1×e6 bits over the channel. We assume perfect synchronization between the transmitter and receiver. At the receiver following capturing all 1×e6 bit we covert every 9-bit encrypted frame into an 8-bit data patter and compare them with the transmitted bits. For detection we sample every bit at its centre and compare the sampled value with a threshold level set to half the mean signal amplitude. As only 1×e6 bits are sent with every iteration of the simulation, we know exactly where the encrypted code begins and ends, hence there being no need for a preamble header and footer bits to be inserted into the code. However, in real practical applications both pre and post-ambles are required.

Figure 6 depicts the simulated BER performance against the received SNR for VLCs with and without the encryption. In Fig. 6(a) the data rate is 2 Mbit/s, which is well inside the 3-dB bandwidth of LED (approx. 3 MHz). At a BER of 10^{-3}, the power penalties ΔP of 1.2 dB and 1.8 dB compared to the back-to-back VLCs , for both encryption key lengths of 8 and 16, respectively. The power penalties are due to the block errors occurred in encrypted VLC rather than individual bit error in an unsecured VLC system. In secured VLCs when an error is occurred the receiver cannot decrypt the whole block thus resulting in a block error. However at lower BERs the power penalties induced are much smaller i.e. < 1 dB.



(a)



(b)

Fig. 6. BER vs. the received SNR of the received light beam at for the back-to-back VLC and encrypted links: (a) 2 Mbit/s. and (b) 12 Mbit/s

In Fig. 6(b) the data rate is at 12 Mbit/s, which is much higher than LED 3-dB modulation bandwidth. This test provides a good view of the excess power penalty due to "block error" when the system working at more at large erroneous regime. For the same BER performance the system requires much higher SNR, e.g. additional ~21 dB at a BER of 10^{-4}. Power penalties have also significantly increased to 2.2 dB and 3.25 dB for 8 and 16 bits, encryption key lengths, respectively.

Figure 7 depicts the power penalty against the data rate for 8 and 16 bits encryption key lengths at a BER of 10^{-3}. For the 8-bit case the power penalty is < 1.5 dB for the data rate up to 10 Mbit/s increasing to over 2 dB at the data rate of 12 Mbit/s. For the 16-bit case the power penalty profile is similar to the 8-bit but is on average higher by about 1-1.5 dB.

Though the performance of a secured VLC system is heavily dependent on the encryption key lengths, it is noted that the redundancy is relatively small. As the encryption key length increases the redundancy is further minimized.

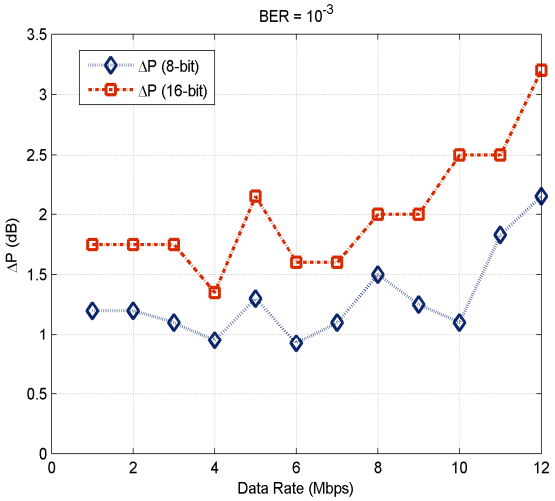


Fig. 7. Power penalty vs. the data rate for secured and unsecured VLC

V. CONCLUSION

The paper has investigated the VLC system performance with encryption in the physical layer. The results showed that the block error severely affected the system BER performance especially for the 16-bit encryption key length. The power penalties observed were ~1.2 dB and ~1.75 dB for the 8-bit and 16-bit encryption key lengths, respectively within the 3 dB LED bandwidth.

Though the selected key lengths in this paper were small mainly due to the limitation of computers and simulator, the results have generically indicated the trend of trading-off and error propagation as well as showing the minimum bandwidth loss of the secured VLC system.

In future longer key length will be implemented and the system performance will be evaluated to obtain the empirical relationship between the key and penalty.

ACKNOWLEDGMENT

Two of the authors, Mousa and Son have received PhD scholarships from Libyan and Vietnamese governments, respectively. The work is also supported by the EU Cost Action IC1101.

REFERENCES

[1] Z. Ghassemlooy, W. O. Popoola, and S. Rajbhandari, Optical Wireless Communications - System and Channel Modelling with Matlab, CRC publisher, ISBN: 978-4398-5188-3, August 2012.

[2] H. Le-Minh, D. C. O'Brien, G. Faulkner, L. Zeng, K. Lee, D. Jung and Y. Oh, "High-speed visible light communications using multiple-resonant equalization," *IEEE Photonics Technology Letters,* vol. 20, no. 15, pp. 1243 - 1245, 2008.

[3] J. Vucic, C. Kottke, S. Nerreter, K.-D. Langer, "513 Mbit/s visible light communications link based on DMT-modulation of a white LED," *IEEE Journal of lightwave technology,* vol. 28, no. 24, pp. 3512 - 3518, 2010.

[4] A. M. K. G. Cossu, P. Choudhury, R. Corsini, and E. Ciaramella, "3.4 Gbit/s visible optical wireless transmission based on RGB LED," in *the ECOC*, Amsterdam, Holland, 2012.

[5] A. Burton,H. Le-Minh, Z. Ghassemlooy, E. Bentley, and C. Botella, "Experimental demonstration of 50-Mb/s visible light communications using 4 x 4 MIMO," *IEEE Photonics Technology Letters,* vol. 26, no. 9, pp. 945 - 948, 2014.

[6] P. Canyelles-Pericas, A. Burton, L.-M. Hoa, Z. Ghassemlooy, and K. Busawon, "Chaos synchronization on Visible Light Communication with application for secure data communications," in *AFRICON 2013*, 2013, pp. 1 - 5.

[7] K. Okuda, M. Murata, T. Nakamura, W. Uemura, T. Yamamoto, "Proposal and development of encryption key distribution system using visible light communication," in *IEEE Consumer Electronics (ICCE 2011)*, Berlin, 2011, pp. 71-73.

[8] O. O. Khalifa, M. R. Islam, S. Khan, and M. S. Shebani, "Communications cryptography," in *Proceedings of RF and Microwave Conference (RFM 2004)*, 2004, pp. 220-223.

[9] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, Handbook of Applied Cryptography, CRC Press Inc., 1996.

[10] D. R. D. R. Stinson, Cryptography: theory and practice, London: Chapman Boca Raton, 2nd ed., 1995.

[11] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 5th ed., 2010 .

[12] N. Muhammad, J. M. Zain, and M. Y. Mohd Saman, "Loop-based RSA key generation algorithm using string identity," in *the 13th International Conference on Control, Automation and Systems (ICCAS)* , 2013, pp. 255-258.

[13] A. Al Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," in *the 3rd International Conference on Convergence and Hybrid Information Technology (ICCIT '08)*, 2008, pp. 505-510.