UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

An Improved Blockchain Technique for Secure Land Registration Data Records

Salman Humdullah, Siti Hajar Othman, Muhammad Najib Razali, Hazinah Kutty Mammi, Rabia Javed
Faculty of Business and Management
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia
Email: salman.humdullah@gmail.com, {hajar, mnajibmr, hazinah }@utm.my, javed.rabia@graduate.utm.my

Submitted: 28/2/2021. Revised edition: 8/7/2021. Accepted: 11/7/2021. Published online: 15/11/2021
DOI: https://doi.org/10.11113/ijic.v11n2.291

***Abstract*—The land is a very valuable asset for any government. It's government job to ensure that the land registration and transfer are done without any fraud, good speed and transparency. The current land registration method employed by the governments are not open to frauds, hacks, and corruption of land records. Fraud is one of the major problems in land registration methods. In this study, the goal is to develop the framework by incorporating the blockchain technique that secures the land data during the land registration and transfer phases by preventing the fraud. The use of blockchain gives us the transparent, decentralized and robust infrastructure to build our framework upon. The blockchain technology is implemented with the asymmetric keys encryption/decryption that securely stores the land registration/transfer data. The data is held using encrypting with the public key of the landowner and storing a hash of the data. The use of the cryptographic function of hashing using SHA. The comparison of using SHA 256 and SHA 512 is given and discussed. The dataset used to compare results is created using 200 records of JSON objects with each object being identical for both SHA256 and SHA512 to remove data bias. The proposed framework with the SHA 512 performed 29% faster than the SHA 256. The results indicate our proposed framework performing better than the works proposed in current research land registration techniques.**

***Keywords*—Land Registration, Blockchain, Hashing, SHA 256, SHA 512, Optimization, Fraud, Secure Data**

I. INTRODUCTION

Land registration process is a series of complex operations of sharing and processing sensitive data that requires a decentralized environment. Current technology only concentrates on the less secure database storage and expose to any misconduct. As the land registration methods require complexities and challenges in terms of land tenure security at a high-risk scale, the land registration system's security level needs to be put at the highest level. Fraud is one of the major problems which is currently a severe problem of land registration methods. Also, the land registration process facing a long process problem. The land title is the confirmation that this land is already registered and has the owner of this land. The reason for ownership is to perceive property rights, which incorporates data relating to land region, area, limits, just as a proprietorship, and title of the ardent property. However, the land is registered, but there are many causes of fraud in which land registration data can be quickly deleted and or edited. Since land is an asset, and any fraud can cause a loss in a lot of money, it becomes very crucial that the registration of land becomes speedy, transparent, and with less fraud. In this research, a framework for secure data storage of land registration using blockchain is proposed. Blockchain offers the solution with its underlying technology. Blockchain is decentralized, transparent, and fast compared to the traditional centralized software approach. For the validation of the proposed framework, a comparison is performed between proposed and existing methods.

Currently developed or proposed land registration systems vary from one country to another, and thus the majority of the descriptive literature directs the attention at the domestic reader. Most literature is on the techniques developed locally or nationally, and the literature is produced in their local language. Some focus is usually given to some general ideas on land registration, including short descriptions of some main classifications. In several countries, the laws made in the 19th century under the geographic-political (colonial rule) still provide the basis of the system of land registration, even though the conditions of the past have changed quite radically since that time. The methods developed in these countries share the basis, but these countries also have common official languages. Important groups can be divided into the Spanish (and Portuguese) speaking countries, the French-speaking countries, and the British Commonwealth. There is an exception, more recently the countries with territories that belonged to Habsburg's Austro-Hungarian Empire have common laws or the same regulation regarding land registration (even though they do not have a common language). Since most of the countries of the world have been under British rule at some point in history, this is the reason the majority of the nations will find their essential land registration being the same. Native English-speaking experts have the upper hand in the field. There are relatively more and studying a lot of countries' systems becomes quite easy. Also, English is the most used academic language in the world, as well. Unfortunately, some of these British authors or their opinions seem not to ignore other systems and the practices outside of their system. However, the situation has improved in the 1990s. Even if they become informed about different types of plans, they often map the terms to the English common law terminology. Even within the Anglo-Saxon world, there is an incredible diversity in legal traditions and terminologies, especially between Great Britain and the United States.

The rest of the paper is organized as follows: Section 2 defines land registration and blockchain related works. In Sections 3, defines the Asymmetric Encryption Algorithm. In Section 4, the proposed framework of secure land registration and transfer using improved blockchain technique is explained. Section 5 presents the results obtained and discusses the results in quantitative and qualitative aspects. Section 6 concludes the work. Section 7, suggests further work that can be done to further enhance the work

II. Related Work

Many attempts for the digitization of land registration methods have been mostly unsuccessful because they have been built on client-server architecture, lack of government interest. Toaha and S. Khan (2008, pp. 46–51) proposed a system that intends to digitize all the steps, from cadastral surveying to creating new database records [1]. The satellite images of Google Earth software which are available for the public would greatly assist cadastral surveys. Diverse issues ranging from security of data to access and data entry. The proposed system should minimize hassle, expenditure, delays, and staff dishonesty. Tembo, Nkwae, and Kampamba (2014 pp. 1–13) addressed the possible hurdles of electronic registration of Land records and proposed a model for re-engineering the Land registration system [2]. The proposed system will necessitate changes in the Law about what and how land records must be submitted for registration and what is admissible as evidence of submission. Publicly online(web) systems also play an essential role in the land registration process. Different authors have addressed the various challenges regarding online land registration application. Oyetayo, Alias, Tan, Iyanu, and A. Olatunbosun (2017, pp. 1–12) investigated using an online network of the land registration the quickest way to solve the problem. An online web-based solution was designed to check the status of their application through the web [3].

Yapa, Heanthenna, Bandara, Prasad, and Y. Mallawarachchi (2018, pp. 75–80) proposed a blockchain method of land registration [4]. This system uses machine learning for land value prediction. Krishnapriya and Sarath (2019, pp. 1708–1715) proposed Blockchain-based land registry system [5]. This method's problem is that they are using SHA 256 that is suited for backward legacy systems, whereas SHA 512 is a much better option. The second point is using the third-party server to store user data that should be made to keep in the blockchain itself. Their research's objective was on the manual effort reduction rather than making secure data storage on the blockchain.

Different blockchain solutions are used to solve the central architecture problems; Turkanović, Hölbl, Košič, Heričko, and Kamišalić (2018, pp. 5112–5127) used the SHA 256 hashing in one of the blockchain implementations [6]. The secure land registration using blockchain proposed by Krishnapriya and Sarath (2019, pp. 1708–1715) [5] in their work they used SHA 256 hashing technique. The SHA 256 hashing technique works for older generations of 32-bit computing devices, but the more recent 64-bit computing devices do not perform better. Hence, land registration still needs to improve on securing land record data and the transfer of land with high efficiency. Therefore, the need to identify the framework of blockchain technology for land registration is essential.

III. Asymmetric Encryption Algorithm

The core of our research is to make land data secure and for that RSA public/private keys are used. The 2048 bits' length of keys is used for security. The mode for encryption used is EAX mode (encrypt-then-authenticate-then-translate). It is an Authenticated Encryption with Associated Data (AEAD) algorithm designed to simultaneously provide authentication and privacy of the message (authenticated encryption) with a two-pass scheme, one pass for achieving privacy, and one for authenticity for each block as in Fig. 1.

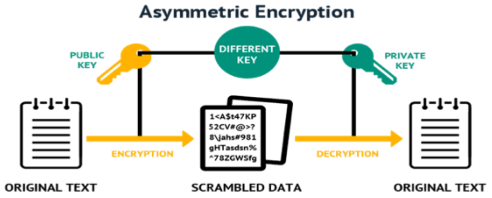

Fig. 1. Asymmetric Encryption

The proposed framework secures using the following equations 1 to 4: Let assume K_{PR}, K_{PB} be the private key and public key respectively. The encryption and decryption process are:

$$Encrypted\ data = encrypt(K_{PB},\ Data) \quad (1)$$

$$Encrypted = EncodeBase64(Encrypted\ Data) \quad (2)$$

To reverse we have to decode and then decrypt to get our original data back.

$$Encrypted\ Data = DecodeBase\ 64(\ Encrypted\ ) \quad (3)$$

$$Plain\ Data = decrypt(K_{PR}, Encrypted\ Data) \quad (4)$$

Since K_{PR} is only available with the owner and is offline is more secure. The data attribute which we encrypt is based on the JSON data structure. JSON is a short form of JavaScript Object Notation. The JSON data is very flexible, and more attributes can be added as per the needs.

Algorithm 1: Asymmetric Encryption Algorithm

```
1.  Parameter Initialization: The parameters needed are initialized
2.  Input: public key, land registration data
3.  Encryption: takes public key and data as input
4.  Encode: the data with “utf-8”
5.  Session Key: get random 16 bytes
6.  Cipher RSA: get PKCS1_OAEP from public key
7.  Encrypt Session Key: get encode by Cipher RSA encrypt method using Session Key with ‘base64’
8.  Cipher AES: get encode using AES session key and AES MODE_EAX with base64
9.  Ciphertext and tag: get encode cipher AES encrypt and digest data using base64
10. Encrypted: get Encrypt session key, nonce, tag, ciphertext
11. Return the Encrypted text from step 10
```

Algorithm 1, we are using the asymmetric encryption to encrypt the land data. The registration data includes owner id, owner name, land address, land title and the public key

Algorithm 2: Asymmetric Decryption Algorithm

```
1. Parameter Initialization: The parameters needed are initialized
2. Input: private key, land registration encrypted data
3. Extract: encrypted session key, nonce, tag, ciphertext from encrypted data using base 64
4. Cipher RSA: get PKCS1 OAEP using private key
5. Session key: get cipher RSA decrypt using enc session key
6. Cipher AES: get AES using session key and AES MODE_EAX with nonce
7. plain text: get cipher aes decrypt and verify using ciphertext and tag
8. Return the plan text from step 7
```

Algorithm 2, we are using the asymmetric decryption to decrypt the land data. The private key is needed to decrypt the data. Without which the land data is forever locked.

Algorithm 3: Land registration

```
1.  Parameter Initialization: The parameters needed are initialized
2.  Input: id, name, address, title and public key
3.  Land registration: fetch the blockchain
4.  Prepare data: The data that needs to be added is combined into JSON
5.  Unique land record: Check if all the land record is unique against the land address
6.  Encryption: encrypt the data using the public key
7.  Singed data: encrypted data is joined with the raw data
8.  Block creation: the data is added into the block
9.  Add to block: the created block is then pooled for the nodes to prepare it for insertion
10. The block data is sent to be added to the blockchain
```

The algorithm 3 uses the land record data and encrypt it and then signs it and then stores in a new block in the blockchain. The condition is that the address must be unique.

Algorithm 4: Land transfer

```
1. Parameter Initialization: The parameters needed are initialized
2. Input: block id is the id of the block
   name is the name of the owner
   old private key is the private key of the old owner for decryption
   new public key is the public key of the new owner for encryption
   id is the identification number (can be passport as well) of the new owner
3. Land transfer: fetch the block form blockchain against id
4. Decrypt data: using the old private key of the owner we will decrypt the data
5. Success metrics: check the step 12 produced a successful decryption. Only a successful decryption will enable the unlocking of the block
6. Prepare data for transfer: in case of successful decryption the extracted data will used to gain address and title of the land.
7. Singed data: prepared data in step 14 will be used to encrypt the new block with new public key of the new owner and the prepared data
8. The signed data will be added in a new block in the blockchain
```

Algorithm 4 takes the old private key and new public key of the owners to transfer the land block to the new owner in the blockchain. The security check is that the old land block data must be able to decrypt using the old private key of the owner to verify a true owner. After a successful decryption the new owner id and name are created in a new block and is added in blockchain.

IV. Proposed Framework

The research framework shows the outlines of the research. Each phase matches each objective. Since there are three objectives, three phases were identified in the research framework. The phases are labeled as Phase 1, Phase 2, and Phase 3. Each phase generates input for the following phase. The first step is the initial step which initiates the process of this research. Phase 1 is the land registration in which on client request the land is registered. In Phase 2, the land transfer process explains how the land is securely transferred from one owner to another. In Phase 3, the proposed framework's performance is evaluated by comparing it with the existing methods. The research framework for land registration and land transfer process through blockchain is explained in Fig. 2.

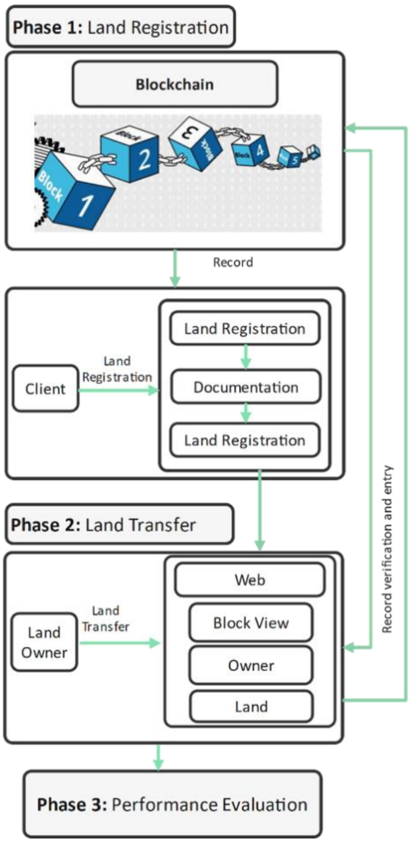

Fig. 2. Proposed Framework

The detail of Phase 1 is explained in Subsection A, while Subsection B Phase 2 is described, and lastly, Section V explains the performance evaluation phase of this research work.

A. Land Registration

Phase 1 of this research framework is land registration using blockchain. The primary blockchain is built. Basically, when a client wants to register a land, he/she has to visit the land registration office. In the land registration office, the administrator checks all the required documents of the client. After verifying these documents, the administrator enters the record in the blockchain. Given that the land must not be already registered. If the land is not already in blockchain, it implies that this land is new. The administrator enters the client's public key, client id/passport, land title, and land address. If the client has no public/private keys, these keys will be generated and handed over to the client. The system will check for any previous registration with the same land title, and if none is found, then the registration is recorded in the transaction. The data is stored in two ways. First raw data as key-value pair and second as encrypted with the client's public key is also a signed copy of the record stored in the block. After the land registration, the block mining process is carried out. In which record is recorded in the blockchain.

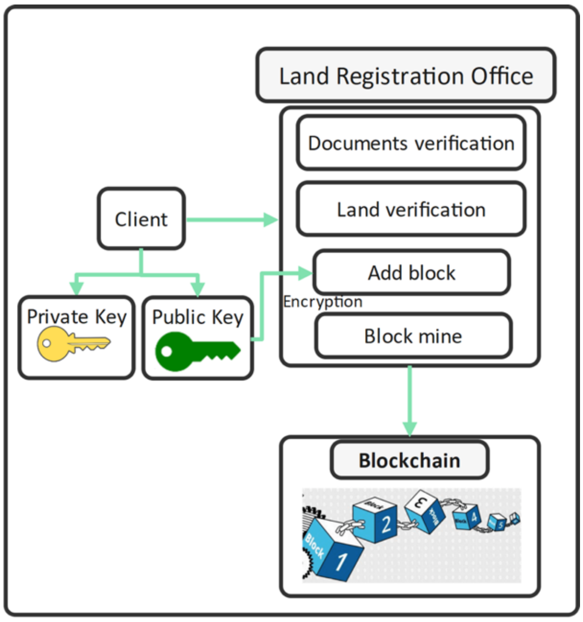

Fig. 3. Secure land registration using blockchain

B. Land Transfer

The research framework phase is land transfer in which the land transfer process is explained in detail. The proposed framework for land transfer is secured from the fraud of ownership because only the landowner has the right to transfer the property. The detail of each step involved in the land transfer process is explained in Fig. 4.

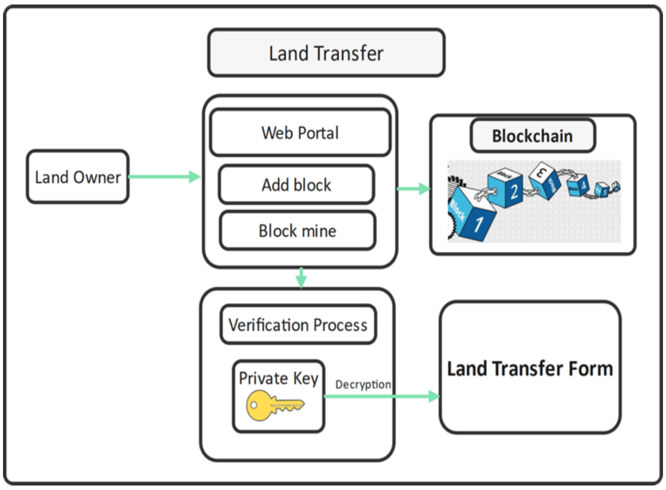

Fig. 4. Secure land transfer using blockchain

V. Experimental Results and Discussions

This section explains the results and discussion of the project. The results of this proposed research framework, the land registration and land transfer process, are efficient compared to the methods used in the current researched methods.

The method to validate our proposed framework we used 200 blocks of data. Each data block consisted of 3008 bytes or 24,064 bits of data. The total size of blockchain becomes 200 x 3008 bytes is 587.5 Kilobytes of data. The data attribute we stored in the block is id, name, title, address, owner public key. We have used SHA 512 due to performance and security improvement compared to SHA 256, as explained in Fig. 4.

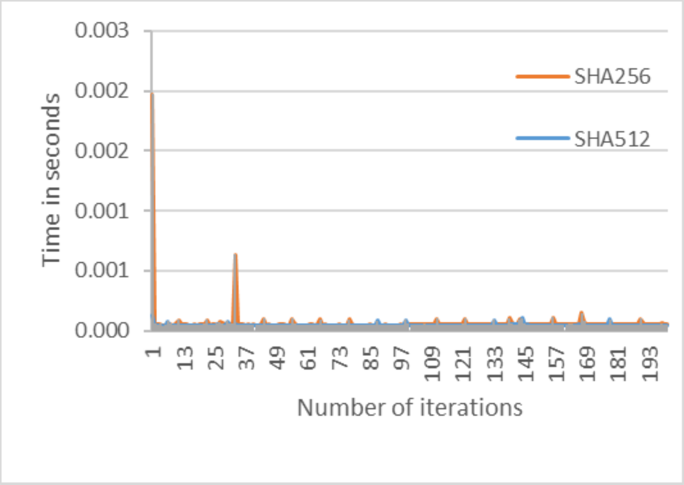

Fig. 5. Performance graph between SHA256 vs SHA512

The above graph contains 200 iterations of hashing of data; the orange line depicts SHA 256 processing time, and the blue line represents SHA 512. The high orange line shows more processing time while the subtle blue line represents quick hashing done by the SHA 512. The vertical axis represents the time in seconds it took to complete the hashing by both SHA functions on the blockchain's identical data blocks. The graph also shows that the SHA 512 is more efficient in hashing than the SHA 256.

The improvement achieved by using SHA512 is calculated by taking the average time of both hashing functions. The average time of SHA 256 is observed to be 68.90 microseconds, while the average time of SHA 512 is followed to 48.32 microseconds. The difference between the two is calculated by subtracting SHA256 – SHA 512. The percentage change was calculated using the equations from 5 to 7.

$$= 100 \times \frac{(Hash\ Time_{512} - Hash\ Time_{256})}{|Hash\ Time_{256}|} \tag{5}$$

$$= 100 \times \frac{(0.000048326253 - 0.000068923234\ )}{0.0000689232349395752} \tag{6}$$

$$\%\ Change = -29.8839\ \% \tag{7}$$

The calculated percentage of change is -29.8%. The negative sign indicates a decrease in time for SHA 512 when compared with SHA 256. This means that the SHA 512 is more efficient compared to SHA 256. The real improvement gained from using SHA 512 is 29.8%, which is better than SHA 256.

A. *Comparison with Existing Methods*

The proposed framework is also compared with state-of-the-art methods. Table 1 represents the difference between the enhancements suggested in this work with the previous ones. This proposed framework shows a better enhancement in performance and cryptographic security improvement compared to the previous work.

TABLE I. Difference between the proposed frameworks

Works Compared	**Proof of Work**	**SHA 256**	**SHA 512**
[7]	YES	YES	NO
[6]	YES	YES	NO
[8]	YES	NO	NO
[5]	YES	YES	NO
Our Proposed Framework	YES	YES	YES

The existing works in Table 1 are using the SHA 256. The reason for them using SHA 256 is due to the legacy system and hardware. The legacy systems are 32-bit architecture, and SHA 256 performs better over it. It is costly to upgrade all the legacy software and hardware to the relatively unknown 64-bit architecture. The SHA 512 is more cost effective than SHA

256 when used on the 64-bit computing devices [9]. The industry used SHA 256 due to its backward compatibility on the 32-bit computing devices. These 32-bit devices are used in servers and legacy systems due to which it will take some time to be replaced with new 64-bit computing devices. Our results in Fig. 5 also indicate that the SHA 512 over the 64-bit architecture performed far better than 32-bit architecture.

The hashing technique in the proposed framework gave better results. The SHA 512 internally uses 64 bits which for its initial hash values and round constants and the modern CPU architecture is 64 bits. The same bits give SHA 512 advantage when used over 64-bit architecture. That is one of the key reasons for the performance gain we were able to achieve. The industry standard for hashing used in state of the art is SHA 256 [6], [5]. Due to the performance gained from the SHA512 will be beneficial to the overall time saving of each transaction.

VI. Conclusion

The proposed framework secures the land registration data along with the land transfer data with the asymmetric keys using the blockchain. The fraud is prevented due to the hashing and encryption of the data and using of the peer-to-peer nodes of consensus mechanism. This, combined with the SHA 512, gives our proposed solution performance enhanced. This gives us ~30% more efficiency and improved performance.

VII. Future Work

The proposed framework can be improved by adding Merkel tree, which will benefit the integrity and validity of data, reduce the disk space, and information needed to be transmitted over the network. The other aspects of the project that can be improved are the reporting tools for all the land records which are being recorded. The secured data in our proposed blockchain can be further optimized using various compression techniques. This will allow the blockchain size to be reduced. This reduction in data will help reduce network traffic. Also, that will help the load on nodes. Furthermore, different encryption methods can be explored for asymmetric keys like elliptical curve cryptographic algorithm. There are areas in this study which can be extended to for further investigations.

References

[1] M. Toaha and S. Khan. (2008). Automated Digital Archive for Land Registration and Records. *Proc. 11th Int. Conf. Comput. Inf. Technol, ICCIT 2008*, 46-51. Doi: 10.1109/ICCITECHN.2008.4803029.

[2] E. Tembo, B. Nkwae, and J. Kampamba. (2014). Land Registration in a Digital Environment. *Engag. Challenges - Enhancing Relev.*, June, 1-13. [Online]. Available: http://www.fig.net/pub/fig2014/papers/ts02c/TS02C_tembo_kampamba_et_al_6786.pdf.

[3] B. S. Oyetayo, A. R. Alias, C. L. Tan, A. A. Iyanu, and A. Olatunbosun. (2017). Akademia Baru Internet Application for Online Cadastral Services : A Case Study in Nigeria Akademia Baru, 1(1), 1-12.

[4] I. Yapa, S. Heanthenna, N. Bandara, I. Prasad, and Y. Mallawarachchi. (2019). Decentralized ledger for land and Property Transactions in Sri Lanka Acresense. *IEEE Reg. 10 Humanit. Technol. Conf. R10-HTC*, 2018-Decem, 75-80. Doi: 10.1109/R10-HTC.2018.8629811.

[5] S. Krishnapriya and G. Sarath. (2019). Securing Land Registration using Blockchain. *Procedia Comput. Sci.* 171: 1708-1715. Doi: 10.1016/j.procs.2020.04.183.

[6] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić. (2018). "EduCTX: A Blockchain-based Higher Education Credit Platform, *IEEE Access*, 6, 5112-5127. Doi: 10.1109/ACCESS.2018.2789929.

[7] L. S. Sankar, M. Sindhu, and M. Sethumadhavan. (2017). Survey of Consensus Protocols on Blockchain Applications. *2017 4th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2017*. Doi: 10.1109/ICACCS.2017.8014672.

[8] P. S. Sajana M., Sethumadhavan, M. (2018). On Blockchain Applications: Hyperledger Fabric And Ethereum. *Int. J. Pure Appl. Math.* 118(18), 2965-2970. [Online]. Available: http://www.ijpam.eu.

[9] S. Gueron. (2012). Efficient Software Implementations of Modular Exponentiation. *J. Cryptogr. Eng.* 2(1), 31-43. Doi: 10.1007/s13389-012-0031-5.