Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 72 (2015) 469 – 476

Procedia Computer Science

The Third Information Systems International Conference

The Direction of Lightweight Ciphers in Mobile Big Data Computing

Alya Geogiana Buja[a,b,]a* and Shekh Faisal Abdul Latip[a,]b*

[a]*INSFORNET – Crypto Research Group (CRYPTREG)*
Centre of Advanced Computing Technology (C-ACT), Universiti Teknikal Malaysia Melaka
76100 Durian Tunggal, Melaka, Malaysia

[b]*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Melaka (Jasin)*
77300 Merlimau, Melaka, Malaysia

Abstract

It is too fast. The advances of the computing technology are moving very fast and far from the era of gigantic machine. This advanced technology offers easy, fast and wide range of computing activities particularly users who want to use the Internet, regardless of time and place. In addition, this advanced technology can also connect more communication tool. At the same time, greater storage platform is also available as mobile computing cloud computing architecture adopted to carry out computer activities. However, the larger the network which is connected to a computer, the more susceptible the computer to the outside threats. Indirectly, the communication system and the information stored in the computer are also exposed. Therefore, in this paper, we has discussed on the evolution of the computing which begin with the distributed system until recent computing technology which we called Mobile Big Data Computing. Besides, in this paper, we define the term Mobile Big Data Computing. Our discussion focuses on the information security aspects for the security of storage and transmitted data. Ultimately, this paper discusses the direction of the lightweight cipher design consideration towards Mobile Big Data Computing.

Peer-review under responsibility of organizing committee of Information Systems International Conference (ISICO2015)

Keywords: Big Data Computing;Cipher;Cloud Computing;Lightweight;Mobile Computing

1. The Evolution of Computing Technology

The advances of the computing technology are moving very fast every year. Begin with the emergence of Distributed System of the computing era with big machines in year 1970 [18] it then moves to the small machines computing platform like laptop and personal tab (mobile computing) in year 1984 [10].

* Corresponding author. Tel.: +6-014-885-2844. *E-mail address*: geogiana@melaka.uitm.edu.my.
* Corresponding author. Tel.: 6-06-331-6575; fax: +6-06-331-6500. *E-mail address*: shekhfaisal@utem.edu.my.

Peer-review under responsibility of organizing committee of Information Systems International Conference (ISICO2015)
doi:10.1016/j.procs.2015.12.128

The advances of the computing technology are moving very fast every year. Begin with the emergence of Distributed System of the computing era with big machines in year 1970 [18] it then moves to the small machines computing platform like laptop and personal tab (mobile computing) in year 1984 [10]. With the creation of a small portable computer and is equipped with advanced technology, the users will get the services always aware of his will. For example, a pervasive computing enables advanced mobile phone users received any recent information about the campaign as soon as the last in front of a shopping mall. Pervasive computing offers intelligence to computing environment of user's device. The computing era for pervasive computing is focusing on the context-aware perspective. The power of users has increased through mobile computing. Next is ubiquitous computing environment which offers the user to do their computing tasks everywhere, anywhere and at any time. The era of the ubiquitous computing has started in 1991 initiated by Mark Weiser [19]. Weiser mentioned that ubiquitous computing environment involves the uses of the computing devices everywhere. Ark and Selker (1999) in [2] claimed that ubiquitous computing is the enhancement of the pervasive computing for the uses of the embedded small machine instead of the used of the big machine.

In Figure 1, we have reviewed the evolution of computing by introducing the Mobile Computing Big Data which is the advances of computing technology which facilitated by the advantages offered by computing technologies in mobile computing, cloud computing and big data computing [1]. Cloud Computing is a model of organizing computers for enabling convenient, ubiquitous, on demand network access to a shared pool of configurable IT resources. The rise of Cloud Computing and cloud data storage has been a precursor and facilitator to the emergence of Big Data Computing in 2001 [4]. Big data and its analysis are at the centre of modern science and business. These data are generated from online transactions, emails, videos, audios, images, click streams, logs, posts, search queries, health records, social networking interactions, science data, sensors and mobile phones and their applications. They are stored in databases and grow massively, and become difficult to capture, form, store, manage, share, analyse and visualize via typical database software tools. The term Mobile Cloud Computing was introduced not long after the concept of Cloud Computing in mid of 2007. Mobile Cloud Computing at its simplest refers to an infrastructure where both the data storage and data processing occur outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones into the cloud, bringing applications to not just smartphone users but a much broader range of mobile subscribers [7]. Mobile Big Data Computing can be defined as the advanced computing technology that utilizes the power and advantages of the existing computing technologies that now merged into one computing environment. This is where the users are becoming more powerful when they use these computing facilities. The user can optimized the advantages of mobile computing, big data computing and cloud computing infrastructure together to perform their tasks (refer Figure 1). The Mobile Big Data Computing can offer larger memory, larger storage capacity, and higher processing power (when everything is processed outside the mobile device, particularly in cloud computing environment).

However, with the creation of sophisticated and advanced technology, information security is increasingly threatened for both data in the network and storage. Therefore, this paper aims to review the existing lightweight ciphers and highlights some potential future works. Section 2 gives a brief description on information security while Section 3 presents some lightweight ciphers. Several open issues that can lead to the future works on lightweight ciphers are suggested in Section 4 and Section 5 concludes the paper.

2. The Information Security

The computing era is moving too fast. Starting with the distributed system, next it moved to mobile computing, pervasive computing, and ubiquitous computing and now is the big data computing. Yes, the computing advances offer the users with more powerful computing machines. The users can easily doing their tasks, store their information and communicated with others around the world. However, with these advances, the security level is decreasing when, the invented machines are getting smaller with limited

environment and power consumption, thus the implementation of the security is bounded to the resources available. The small devices cannot afford to implement the powerful and robust security measurement compared to the big devices with large capacity and high processing power. Therefore, if the security implementation is getting limited, the security level is getting easily to be compromised.

Our personal information is very confidential and must be protected. Information is a processed data which is meaningful for the user. Usually, the information then stored or transferred to other users. Cryptography is a field of study that securing information from both inside and outside attacker. To secure an information, it has to be encrypted before being transmitted and, once arrived at the other side, the information has to be decrypted.

The design of lightweight symmetric key ciphers has to be compatible and suitable with the resource limitation. Nowadays, with the rapid development and changing in ubiquitous computing, pervasive computing and mobile computing, symmetric key ciphers are now designed in a small scale and very light. These features enable the cipher to be implemented in small devices. In the current advances computing and communication, all personal and confidential information are now stored in individual personal mobile device, rather than on desktop. Mini devices have limitation in processing power and memory which are useful for a cryptographic algorithm to work.

In previous works, there were many lightweight cipher have been proposed. There are four categories of lightweight symmetric-key cryptographic algorithms:

- **Block Cipher**: The *plaintext* will be divided into blocks of predetermined size. These blocks of the *plaintext* will be passed to the function together with a *secret key* to produce the *ciphertext*.
- **Stream Cipher**: The bit string of *plaintext* or input will be *XORed* with the bit generated by the function to give a bit string of *ciphertext*.
- **Message Authentication Codes**: A key together with a message of arbitrary length will be the input to a function to produce a shorter fixed length bit string.
- **Hash Functions**: Arbitrary length of *plaintext* will be the input to a function to shorter fixed length bit string.

3. The Lightweight Ciphers Evolution

The evolution of the creation of lightweight cipher began with the invention of a primitive cipher that uses only primitive substitution and transposition techniques, and then the DES is created which in turn led to the creation of AES which is still used to this day to protect data in storage and in the network transmission (refer Figure 2).

In line with the current rapid development of computer technology as discussed in Section1, the design evolution in a cipher is became light for ensuring that a cipher is meet the needs of increasingly sophisticated computer technology such as wireless technology, sensors, RFID and others. The creation of modern and advanced technology of a computer causes the design of a cipher is good and robust enough to operate properly for protecting the user's data if it is implemented into any computer technology. As we all know, the creation of computer technology today is in the form of small size and have a limited memory space and small storage capacity. In addition, the operating power is low.

For example, AES has 128, 192 and 256 bits key and block size of 128 bits. Number of rounds is 10, 12 and 14, which is depending on the key size. However, for the lightweight cipher, as for example, KATAN and KTANTAN which have key size of 80 bits which is less than AES. Besides, the block size is also less than AES which is only 32, 48 and 64 bit. While for SERPENT cipher for example which has 128, 192 and 256 bits key, which is equal to AES but, it has only 11 rounds for the SERPENT - 192 while AES - 192 has 12 rounds.

Therefore, the lightweight cipher must be robust and secure like AES. Most lightweight cipher was designed based on AES and inherits some of the strong component in AES like S-box to prevent data intrusion by hackers easy. For example, ITUbee Cipher was designed using AES S - Box to maintain the robustness of the cipher. No of round of the cipher is 20 and it was designed based on the Fiestel Network. Section 3.1 discusses some lightweight block cipher. Most of the cryptosystem uses block cipher.

3.1. The Lightweight Block Cipher

Appendix A shows the design of several lightweight ciphers in terms of the key size, block size, round number, structure and gate count. KLEIN is a family of block ciphers, with a fixed 64-bit block size and a variable key length - 64, 80 or 96-bits. According to the different key length, this cipher is denoted by KLEIN-64/80/96, respectively. It is well-known that the key length and the block size are two important factors for a block cipher in the trade-offs between security and performance. Considering the performances in low-resource implementations, key registers and intermediate results have a significant effect on its footprint. Moreover, in ubiquitous computing, data flows are unlikely to be a high-speed throughput, which means a large block size or key length might be unnecessarily for data encryption and authentication. For security concerns, 64-bit key length might be vulnerable if one considers attack models based on pre-computation and large amounts of available storage.

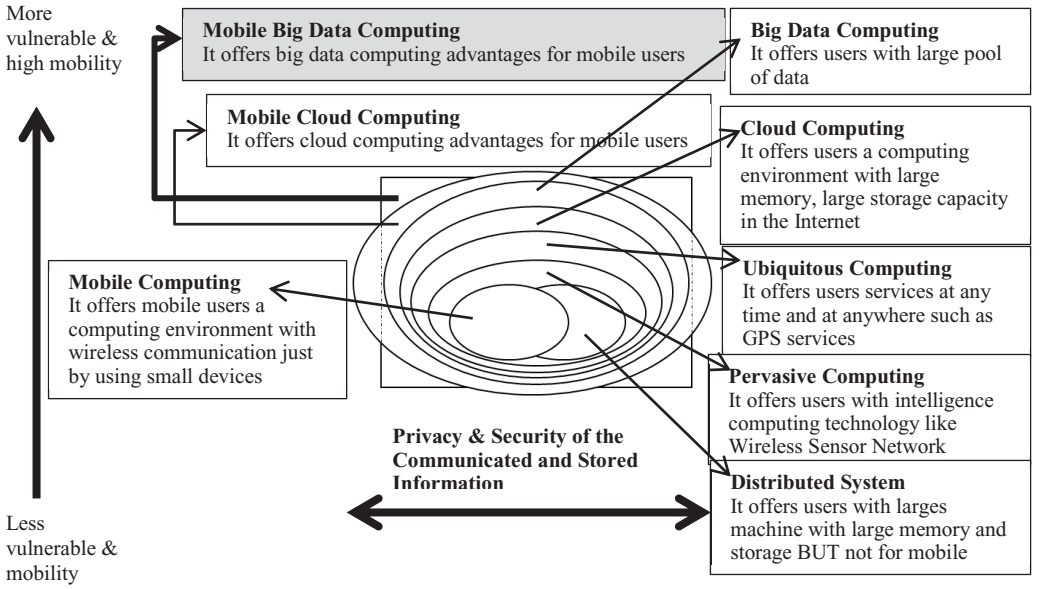

Figure 1: The Computing Evolution

KLEIN-64 have been recommended to be used for constructing single (double) block length hash functions or message authentication codes and KLEIN-80 and KLEIN-96 to be used for data encryption in any of the operation modes [9].

KATAN is a family of lightweight and feedback shift register-based block cipher. The design basically inspired by Trivium. There are three types of KATAN Cipher which are KATAN-32, KATAN-48 and KATAN-64. The differences between the various KATAN Ciphers are: The number of times the nonlinear functions are used in each round. All the ciphers in the KATAN family share the key schedule which accepts an 80-bit key and 254 rounds as well as the use of the same nonlinear functions. The KTANTAN family is very similar to the KATAN family up to the key schedule. The only difference between KATAN and KTANTAN is the key schedule part. While in the KATAN family, the 80-bit key is loaded into a register which is then repeatedly clocked, in the KTANTAN family of ciphers, the key is burnt and the only possible flexibility is the choice of sub key bits. Thus, the design problem in the KTANTAN ciphers is choosing a sequence of sub keys in a secure, yet an efficient manner [6].

The SIMON block cipher with an n-bit word (and hence a 2n-bit block) is denoted SIMON2n, where n is required to be 16, 24, 32, 48, or 64. SIMON2n with anm-word (mn-bit) key will be referred to as

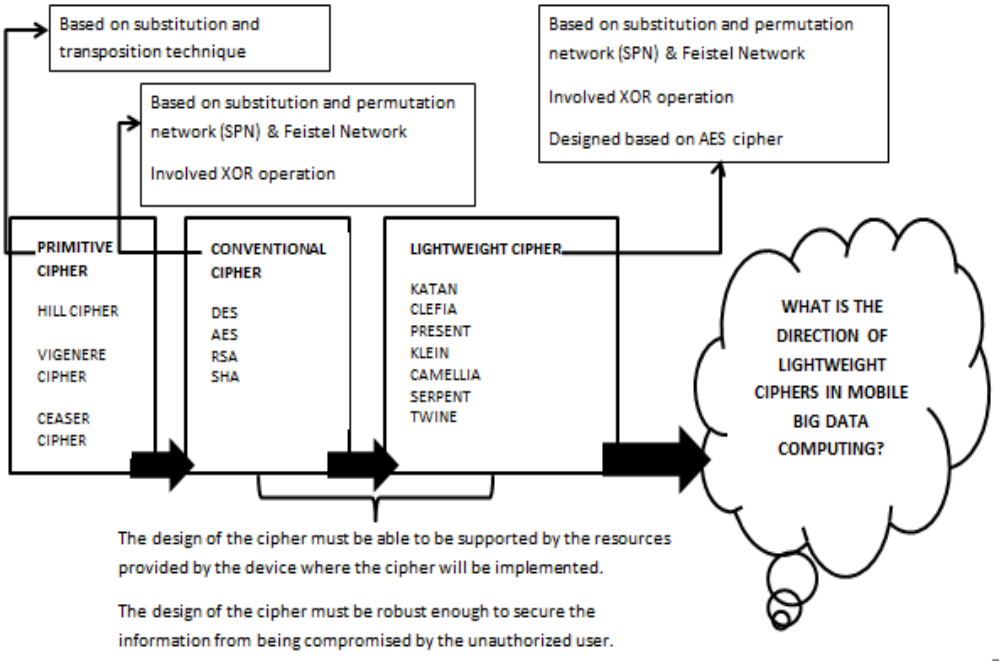

Figure 2: The Direction of Lightweight Ciphers in Mobile Big Data Computing

SIMON2n/mn. For example, SIMON64/128 refers to the version of SIMON acting on 64-bit plaintext blocks and using a 128-bit key. Each instance of SIMON uses the familiar Feistel rule of motion. The algorithm is engineered to be extremely small in hardware and easy to serialize at various levels, but care was taken so as not to sacrifice software performance [3]. While 128-bit blockcipher CLEFIA, supporting key lengths of 128, 192 and 256 bits, which is compatible with AES. CLEFIA achieves enough immunity against known cryptanalyses and flexibility for very efficient implementation in hardware and software. The fundamental structure of CLEFIA is a generalized Feistel structure consisting of 4 data lines, in which there are two 32-bit F-functions per one round [17].

4. Open Issues: The Direction of Lightweight Ciphers in the Mobile Big Data Computing

As discussed and reviewed in Section 1, the Mobile Big Data Computing was composed of Mobile computing, Cloud Computing, Big Data Computing and Mobile Cloud Computing. Therefore, the number of data and information stored in the Internet are getting increased. Besides, with those computing environment, the network is getting big and the security is getting low. The information is available and become vulnerable in the network. Therefore, in this paper we would like to come out with several research questions for the future works;

a. What is the possible design of a cipher to encrypt the structured and unstructured data in Mobile Big Data Computing?
b. What is the design of a cipher for a very small device which is smaller than a sensor node and RFID tag?
c. How is the hardware implementation specification of a cipher in Mobile Big Data Computing?
d. How is the software implementation specification for a cipher in Mobile Big Data Computing?
e. Will the new designed and developed cipher for Mobile Big Data Computing is secure and robust from the recent cryptanalysis techniques like side channel cube attack?
f. Does a cipher with only 1000 GE is secure enough in the Mobile Big Data Computing?

5. Conclusion

Information has to be protected either while in the storage or during the communication process regardless wired or wireless. In the era of mobile computing, the resource constraint was the main limitation for the cipher's design. The cipher should perform well in the limited resources in order to secure the information from attacks like modification of the information by the unauthorized user. With the advancement of the computer technology, the data in the Internet became too many and there is a need of an improved computing architecture which we called Mobile Big Data Computing. When there is too many data and too many devices connected, the more vulnerable the information. Therefore, the design of a cipher became important issues which have to be considered. Based on our survey, the advancement of the technology have changed the environment of computing whereby there are many data have to be processed and kept safe in a very big computing environment. The existing lightweight ciphers were created in the previous computing era and it might be obsolete in the mobile big data computing where we have to consider the software and hardware implementation carefully. Therefore, this paper concludes that a few issues in mobile big data computing have to be taken into consideration for improving the design of lightweight ciphers.

Acknowledgements

This work was supported by Ministry of Higher Education, Malaysia (SLAB Scholarship) and Universiti Teknologi MARA (UiTM) Malaysia.

Appendix A. The Lightweight Ciphers for Various Computing Environment

Cipher	Key Size	Block Size	Round Number	Code Size	Structure	Area of Gate Equivalent
CLEFIA [17]	128, 192, 256	128	18, 22, 26	4780,5010,4924	Unbalanced Feistal Network	4950
CAMELLIA	128, 192, 256	128	18, 24	9692	Balanced Feistal Network	14.12K
KLEIN [9]	64, 80, 96	64, 80, 96	12, 16, 20	1268	Substitution Permutation Network	1220
KATAN [6]	80	32, 48, 64	254	338	Key Schedule	1054
KTANTAN [6]	80	32, 48, 64	254	10516,11764,8348	Block cipher	688
LBlock	80	64	32	2024	Feistal Network	1320
LED	64, 128	64	32, 48	7004	Key Schedule	1872
mCrypton	64, 96, 128	64	12	1076	Substitution Permutation Network	2500
PICCOLO	80, 128	64	25, 31	1824	Combination Feistal Network and S-box	616
SEA	96	96	32	2132	Balanced Feistal Network	1333
SERPENT	128, 192, 256	128	10, 11, 32	19700	Substitution Permutation Network	18000
SIMON [3]	64, 72, 96, 128, 144, 192, 256	32, 48, 64, 96, 128	32, 36, 42, 44, 52, 54, 68, 69, 72	8185	Balanced Feistal Network	860
SPECK [3]	64, 72, 96, 128, 128, 192, 256	32, 48, 64, 96, 128	22, 23, 26, 27, 28, 29, 32, 33, 34	1342	ARX(add-rotate-xor)	2000
TWINE	80, 128	64	36	3796	General Feistal Network	1500

References

[1] A History of Cloud Computing. Retrieved Online: http://www.computerweekly.com/feature/A-history-of-cloud-computing.
[2] Ark, W.S., Selker, T., 'A look at human interaction with pervasive computers', IBM Systems Journal, 38: 4 (1999), pp. 504-07.
[3] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2013). The SIMON and SPECK Families of Lightweight Block Ciphers.*IACR Cryptology ePrint Archive*, *2013*, 404.
[4] Big Data. Retrieved Online: http://searchcloudcomputing.techtarget.com/definition/big-data-Big-Data.
[5] Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G., & Mickunas, M. D. (2003). Towards security and privacy for pervasive computing. In *Software Security—Theories and Systems* (pp. 1-15). Springer Berlin Heidelberg.
[6] De Canniere, C., Dunkelman, O., & Knežević, M. (2009). KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers. In*Cryptographic Hardware and Embedded Systems-CHES 2009* (pp. 272-288). Springer Berlin Heidelberg.
[7] Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless communications and mobile computing*, *13*(18), 1587-1611.
[8] Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. *Future Generation Computer Systems*, *29*(1), 84-106.
[9] Gong, Z., Nikova, S., & Law, Y. W. (2012). *KLEIN: a new family of lightweight block ciphers* (pp. 1-18). Springer Berlin Heidelberg.
[10] History of Mobile Computing. Retrieved Online: https://mobilecomputingproject.wordpress.com/2012/10/10/history-of-mobile-computing/
[11] Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on* (pp. 109-116). IEEE.
[12] Kagal, L., Finin, T., & Joshi, A. (2001). Trust-based security in pervasive computing environments. *Computer*, *34*(12), 154-157.
[13] Ladan, M. I. Mobile Computing: Security Issues.
[14] O'Connor, L., Gaskell, G., & Caelli, W. J. Security Issues in Distributed Computing. Retrived Online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.46.2449&rep=rep1&type=pdf
[15] OGIGĂU-NEAMȚIU, F. (2012). Cloud computing security issues. *Journal of Defense Resources Management (JoDRM)*, (02), 141-148.
[16] Sagiroglu, S., & Sinanc, D. (2013, May). Big data: A review. In *Collaboration Technologies and Systems (CTS), 2013 International Conference on* (pp. 42-47). IEEE.
[17] Shirai, T., Shibutani, K., Akishita, T., Moriai, S., & Iwata, T. (2007, January). The 128-bit blockcipher CLEFIA. In *Fast software encryption* (pp. 181-195). Springer Berlin Heidelberg.
[18] The History, Evolution & Trends in Distributed Computing. Retrieved Online: https://prezi.com/9gobleqbzgp-/the history-evolution-trends-in-distributed-computing/
[19]Ubiquitous Computing: Mark Weiser's Vision and Legacy. Retrieved Online: http://www.samkinsley.com/2010/03/12/ubiquitous-computing-mark-weisers-vision-and-legacy/
[20] Weiser, M. (1993). Some computer science issues in ubiquitous computing.*Communications of the ACM*, *36*(7), 75-84.
Cloud Computing.