Recent Trends in Energy Efficient Security Implementation for Resource Constraint Devices

[1]C.G.Thorat, [2]V.S.Inamdar

[1]Department of Electronics and Telecommunication, College Of Engineering, Pune
[1]Department of Computer Engineering, RSCOE, Tathawade - 33
[2]Department of Computer Engineering and Information Technology, College Of Engineering, Pune

Abstract: Security is essential for any resource constrained devices. But along with security battery life is a critical performance and user experience metric for many resource constrained devices. While programming for resource constraint devices there is need to adapt various energy efficient computation trends. Many factors affect power consumption of a computing device like hardware, platform, implementation and etc. This paper will give insights for different energy efficient computation for resource constraint devices.

Index Terms **- Energy efficiency, Resource Constraint devices, Silicon Efficiency.**

I. INTRODUCTION

Networking technology has taken a lead in a common culture for interchanging of the data very rapidly. With this different security issues have been raised. Therefore the information which we transfer or receive over different networks has to be protected. Private information like passwords, credit cards, banking transactions and social security numbers need to be protected.

Cryptography is one of the oldest research area which aims to provide security at device level as well as network level. With the decreasing cost of silicon chips and an internet access this tremendous amount of data has started to go beyond our capability of storing and processing, leading to a vast inefficiency gap between silicon technology and the big data. Figure 1 show the data warehouse growth rate compared to the silicon growth rate guided by Moore's Law, estimated in 2003 and projected to today as well as future.

At international level we can see that there is continuous rise in world population. With this increased population and cutting cost in ICT devices there is a huge demand in ICT applications. This has been caused a fast increasing gap between the inefficiency and demand for energy. If, as the World Economic Forum proposes [1], by using this data it can be commented energy consumed by security with normal computation is the highest one due to economic growth in this century. But with this scenario we will face some critical technical challenges as we can see in Fig. 1. The energy wall however becomes even worse when security becomes another important design metric other than performance. Not only do we have all kinds of personal devices that all require various levels of security, but we also have huge amounts of confidential data in the devices, cloud or workstations which needs to be protected.

Therefore, it is necessary to well balance security level and the required energy consumption overhead, to mitigate the security risks. It has been observed that there is a large gap between Moore's Law and the reality, while the extremely applied security mechanisms further increase such gap. We shall pay more attention to energy-aware security mechanisms with more systematic lightweight cryptographic design methodologies

While designing this lightweight cryptography algorithms focus need to be apply for security analysis. Various algorithms such as PRESENT, PICOLO, CLEFIA, LED, LEA FANTOMAS and SPECK have been designed in this area. Among these PRESENT and CLEFIA are accepted as an ISO standard for lightweight encryption algorithms. CLEFIA is designed by Sony.

In an electronic circuit, the registers consume much more power than the combinatorial logic. The power consumption of these registers is directly proportional to the number of transitions being used or in other words, the number of bits modified. Typically, the multiplication operation will consume more power than squaring operation.

Along with the lightweight cryptography there are certain other approaches also present such as DNA cryptography, encoding techniques and homomorphic encryption. In the next section we will firstly brief DNA cryptography based encryption techniques. After that P-coding based encryption techniques are discussed which are mainly derived for MANET and VANET. In wireless sensor network (WSN) where energy efficiency is a key issue different encryption schemes which are lightweight are discussed. Homomorphic encryption is also a one new thrust area for the researcher which is discussed in last part of the paper. At the algorithmic level lightweight cryptography approaches are illustrated in the same section.

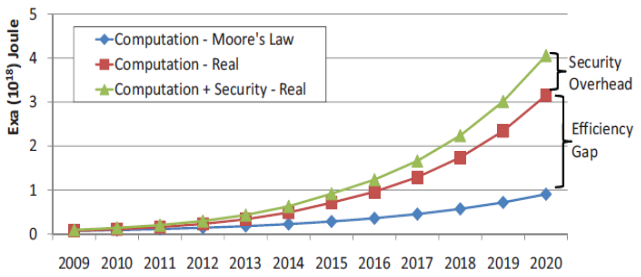

Figure 1: Energy consumed by computation only compared with energy consumed by adding security overhead. The trend is predicted up to 2020 based on data growth rate. [1]

II. SECURITY REQUIREMENTS

Similar to traditional networks, the goals of securing mobile computing can be defined by the following attributes: availability, confidentiality, integrity, authenticity and non-repudiation

a) Availability – Targeted for intended network services are available to the intended users.
b) Confidentiality – ensures that the transmitted information can only be accessed by the intended receivers and is never disclosed to unauthorized entities.
c) Authenticity - allows a user to ensure the identity of the entity it is communicating with. Without authentication, an adversary can masquerade a legitimate user, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of users.
d) Integrity - Information is never modified during transmission.
e) Non-repudiation – This ensures that a sender or receiver can prove the transmission or reception of i.e., a sender/receiver cannot falsely deny having received or sent certain data.

III. RELATED WORKS

3.1 DNA Cryptography

DNA cryptography can be defined as a hiding data in terms of DNA Sequence. It was invented by Leonard Max Adleman in the year 1999. Benefits of DNA computing are high storage capacity, vast parallelism and exceptional energy efficiency of biological DNA. There is no power required for DNA computing while the computation is taking place. The chemical bonds that are the building blocks of DNA happen without any outside power source.Multiple DNA crypto algorithms has been researched and published [2..8] like the Symmetric and Asymmetric Key crypto System using DNA, DNA Steganography Systems, Triple stage DNA Cryptography, Encryption algorithm inspired by DNA and Chaotic computing. In this paper we are presenting a DNA encryption technique based on matrix manipulation and secure key generation scheme. Review of various DNA crypto algorithms has done by Tausif Anwar (2014) in his paper. Author has mentioned the feature scope for reviewed techniques and from that it is underlined more work is need to be done to improve space and computational complexity.

3.2 P-Coding

The P-Coding technique is based on permutation encryption of the coded messages. In this scheme each node prefixes the Global Encoding Vector (GEV) to the packet. Permutation encryption operation randomly mixes the symbols of the messages and corresponding GEVs. Generally P-Coding scheme consists of three stages: source encoding, intermediate recoding, and sink decoding.

I) Source Encoding - Source Encoding considers in general that a source s wants to transmit h messages. Each message is prefixed with the GEV and permutation encryption operation is performed. Finally the encrypted message is generated.

II) Intermediate Recoding - As the symbols of messages and corresponding GEVs are rearranged by permutation encryption operation it is difficult to construct the source messages. The intermediate nodes have no idea of the key being used and hence it is difficult to decrypt the message.

III) Sink Decoding - At the sink node the cipher text is received and decrypted using the permutation decryption operation. Finally the original message is obtained by applying Gaussian elimination.

P-Coding is popular for scalability, robustness and less energy consumption. It is mainly used up till now in mobile adhoc network (MANET) [10] and vehicle adhoc network (VANET). P. Zhang propose P-Coding in his paper to where he perform lightweight permutation encryption on each message and its coding vector, P-Coding can efficiently thwart global eavesdroppers in a transparent way[11]. Another author has extended P-Coding scheme to improve security by key perturbation method [13]. Here key used is changed in each generation and only shared by source and sink in MANET.P-Coding is used with network coding to improve the efficiency in VANET [12]. Another method is proposed in which P-Coding is used with ELZW compression technique to have better performance than LZW compression technique. By eliminating spaces from the data file high compression is achieved [14].

3.3 Encryption in WSN

WSN is categorized in two ways first battery-powered and second solar-powered wireless sensor networks. In both the cases power is limited thus energy efficiency is needed here also. LEACH and Sec-LEACH achieves improvements in terms of network lifetime and security of the information [15]. The SET-IBS and SET-IBOOS protocols in [16] are implemented by using ID based digital signature and ID based online/offline digital signature. The SET-IBS protocol uses the ID based digital signature to solve orphan node problem. To improve the performance of the system energy aware Rule based scheme is proposed by author in [17]. Rule-based learning automata increase the network life time. Author has achieved better security by applying hashing technique and digital signature algorithm based on RSA. The learning automata are applied to select the best optional path for routing for data packets in a network. It improves the life time of network by saving the power of nodes. In WSN few researchers uses cellular automata to implement different security techniques.

Vandana et. Al. have proposed a hybrid scheme comprising both type of encryption schemes i.e. Secrete key cryptography and public key cryptography both. In the proposed scheme the session key is distributed to various nodes using public key cryptography scheme which enhances security of network and also consumes less energy.

3.4 Silicon-efficiency

These are the practices rooted within the advancements in hardware design or hardware interaction comes under silicon-efficiency. Various CMOS-based hardware implementations for AES have been proposed. However, CMOS-based ASIC implementations tend to dissipate high static power in current deep sub-micron technology with their speed limited by low voltage operation [17]. In [19], a memristive CMOL implementation based on hybrid CMOS and ReRAM is introduced to improve the

performance of AES encryption. As the storage device is non-volatile, leakage current is cut-off completely when unused. However, the ReRAM serves primarily as reconfigurable interconnection. Although the distance between memory and logic circuits has been reduced in the hybrid design, the logic and memory are still separated.

In the abovementioned classical and hybrid memory-logic architectures, more power is expended on reading/writing the data than on performing the encryption operations [18]. Block-level in-memory architecture for Advanced Encryption Standard (AES) is proposed by Yuhao Wang in his paper [20]. The proposed technique, called DW (Domain wall)-AES, maps all AES operations directly to the domain wall nanowires. The entire encryption process can be completed within a homogeneous, high-density and standby-power-free non-volatile spintronic based memory array without exposing the intermediate results to external I/O interface. Domain-wall nano wires based pipelining and multi-issue pipelining methods are also proposed to increase the throughput.

3.5 Smart hardware management

Smart hardware management includes techniques ranging from smart sleeping, selective idle of unused components like storage units. By switching between symmetric-key and public-key encryption, based on an energy threshold, the level of security can be traded off against the urgency of energy-saving [21].

3.7 Homomorphic Encryption

Homomorphic encryption is an encryption technique in which computations are carried out directly on cipher text, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. There are two types of homomorphic schemes, one additive in which we use additive operators and other one is multiplicative in which we use multiplication operators. Scheme in which only additive operators are used is known as somewhat homomorphic encryption (SHE) [13]. But many applications required both the operations to be performed so another class of this scheme is known as fully homomorphic encryption (FHE) [14]. Different open research issues are discussed in paper [15].

IV. CONCLUSION

.For battery operated devices along with the security power consumption is also a one of performance metric. Power aware implementation of various security techniques is done at software level and hardware level. Combined study of all these approaches is presented in this paper.

V. ACKNOWLEDGEMENTS

This work is supported by university funding agency BCUD Maharashtra state. Special thanks to Computer engineering department, RSCOE for giving all kinds of support.

VI. REFERENCES

[1] Big data infographic. Technical report,Computer Science Corporation,2012. http://www.csc.com/insights/flxwd/78931- big data growth just beginning to explode.

[2] Weng –Long Chang, “Fast Parallel DNA-Based Algorithms for Molecular Computation: Quadratic Congruence and Factoring Integers,” IEEE Transaction Nano-Bioscience, vol. 11, no. 1, March 2012

[3] Gehani, T. LaBean, and J. Reif, “DNA-Based cryptography”, Lecture Notes in Computer Science, Springer, 2004.

[4] Yunpeng Zhang, Bochen Fu, and Xianwei Zhang, "DNA cryptography based on DNA Fragment assembly," In Information Science and Digital Content Technology (ICIDT), IEEE International Conference, vol. 1, pp. 179-182, 2012.

[5] Olga Tornea, and Monica E. Borda, "Security and complexity of a DNA-based cipher," IEEE Roedunet International Conference (RoEduNet), 11th, pp. 1-5, 2013.

[6] Borda, Monica, and Olga Tornea, "DNA secret writing Techniques," In Communications (COMM), 8th IEEE International Conference, pp. 451-456, 2010.

[7] Ashish kumar kaundal, “Feistel Inspired structure for DNA cryptography” in International Journal of Information Processing, 9(2), 57-75, Springer, June 2014.

[8] Tushar Mandge ,Vijay Choudhary,” A DNA Encryption Technique Based on Matrix Manipulation and Secure key Generation Scheme,” Information Communication and Embedded Systems (ICICES), IEEE International Conference, pp.47-52, 2013.

[9] E Suresh Babua, C Nagarajub, MHM Krishna Prasad, “ Light-Weighted DNA based Hybrid Cryptographic Mechanism against Chosen Cipher Text Attacks,” International Journal of Information Processing, 9(2), 57-75, Springer,ISSN : 0973-8215,2015.

[10] N.R. Potlapally, S. Ravi, A.Raghunathan, and N.K. Jha, ‘‘A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols,’’ IEEE Transaction on Mobile Computing, vol. 5, no. 2, pp. 128-143, Feb.2006.

[11] Peng Zhang, Yixin Jiang, Chuang Lin and Yanfei Fan,”P-coding: secure network coding against eavesdropping attack” IEEE INFOCOM Proceedings, ISSN :0743-166X,Print ISBN: 978-1-4244-5836-3, pp. 1-9, March – 2010.

[12] Peng Zhang, Chuang Lin, Yixin Jiang, Yanfei Fan, and Xuemin (Sherman) Shen, “A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks,” IEEE Transanction on parallel and distributed system, vol. 25, no. 9, September 2014.

[13] Zekeriya Erkin, Thijs Veugen, Tomas Toft, and Reginald L. Lagendijk, “ Generating Private Recommendations Efficiently Using Homomorphic Encryption and Data Packing”, IEEE Transaction on Information forensics and security, vol. 7, no. 3, June 2012.

[14] K.Parmar, and D.C.Jinwala, "Symmetric-Key Based Homomorphic Primitives for End-to-End Secure Data Aggregation in Wireless Sensor Networks," Journal of Information Security, pp. 38-50, 2015.

[15] Haythem Hayouni, Mohamed Hamdi, "Secure Data Aggregation with Homomorphic Primitives in Wireless Sensor Networks: A Critical Survey and Open Research Issues" Proceedings of 2016 IEEE 13th International Conference on Networking, Sensing, and Control Mexico City, Mexico, April 28-30, 2016

[16] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Efficient and high performance parallel hardware architectures for the AES-GCM," IEEE Transaction. Comput., vol. 61, no. 8, pp. 1165–1178, Aug. 2012.

[17] S. Mathew, Farhana Sheikh , Michael Kounavis and Shay Gueron, "53 Gbps native GF(24)2 composite-field AES encrypt/decrypt accelerator for content-protection in 45 nm high performance microprocessors," IEEE J. Solid-State Circuits, vol. 46, no. 4, pp. 767–776, Apr. 2011.

[18] M. Alioto, "Ultra-low power VLSI circuit design demystified and explained: a tutorial," IEEE Transaction on Circuits and Systems vol. 59, no. 1, pp. 3-29, Jan. 2012.

[19] Z. Abid, A. Almaaitah, M. Barua and W. Wang, "Efficient CMOL gate designs for cryptography applications," IEEE Transaction Nanotechnol., vol. 8, no. 3, pp. 315–321, May 2009.

[20] Yuhao Wang, Leibin Ni, Chip-Hong Chang, "DW-AES: A Domain-wall Nanowire Based AES for High Throughput and Energy-efficient Data Encryption in Non-volatile Memory," DOI 10.1109/TIFS.2016.2576903, IEEE Transactions on Information Forensics and Security, 2016.

[21] Jong Min Kim, Hong Sub Lee, Junmin Yi, and Minho Park, "Power Adaptive Data Encryption for Energy-Efficient and Secure Communication in Solar-Powered Wireless Sensor Networks," Hindawi Publishing Corporation Journal of Sensors, Article ID 2678269, 2016.

[22] Niranjan Balasubramanian, Aruna Balasubramanian and Arun Venkataramani, "Energy consumption in mobile phones: a measurement study and implications for network applications," 9th ACM SIGCOMM conference on Internet measurement conference, Pages 280-293, Sept – 2013