**TELKOMNIKA Telecommunication, Computing, Electronics and Control**
Vol. 18, No. 1, February 2020, pp. 228~233
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i1.14798 

# Salsa20 based lightweight security scheme for smart meter communication in smart grid

**S. M. Salim Reza[1], Md Murshedul Arifeen[2], Sieh Kiong Tiong[3], Md Akhteruzzaman[4], Nowshad Amin[5], Mohammad Shakeri[6], Afida Ayob[7], Aini Hussain[8]**
[1,4]Faculty of Engineering and Built Environment, The National University of Malaysia, Malaysia
[1,3,5,6]Institute of Sustainable Energy, Universiti Tenaga Nasional, Malaysia
[1,2]Department of Information and Communication Technology, Bangladesh University of Professionals, Bangladesh
[7,8]Department of Electrical, Electronic & Systems Engineering, The National University of Malaysia, Malaysia

**Article Info**

***Article history:***

Received Aug 30, 2019
Revised Nov 30, 2019
Accepted Dec 25, 2019

***Keywords:***

Elliptic curve cryptography
Salsa20
Security
Smart grid
Smart meter

**ABSTRACT**

The traditional power gird is altering dramatically to a smart power grid with the escalating development of information and communication technology (ICT). Among thousands of electronic devices connected to the grid through communication network, smart meter (SM) is the core networking device. The consolidation of ICT to the electronic devices centered on SM open loophole for the adversaries to launch cyber-attack. Therefore, for protecting the network from the adversaries it is required to design lightweight security mechanism for SM, as conventional cryptography schemes poses extensive computational cost, processing delay and overhead which is not suitable to be used in SM. In this paper, we have proposed a security mechanism consolidating elliptic curve cryptography (ECC) and Salsa20 stream cipher algorithm to ensure security of the network as well as addressing the problem of energy efficiency and lightweight security solution. We have numerically analyzed the performance of our proposed scheme in case of energy efficiency and processing time which reveals that the suggested mechanism is suitable to be used in SM as it consumes less power and requires less processing time to encrypt or decrypt.



***Corresponding Author:***

S. M. Salim Reza,
Faculty of Engineering and Built Environment,
The National University of Malaysia,
Selangor, Malaysia.
Email: salim4419@gmail.com

## 1. INTRODUCTION

Smart grid (SG) is revolutionizing the conventional power infrastructure by enhancing reliability, efficiency and sustainability as well as offers real time energy consumption, ensures power flow, reduces greenhouse gas emissions [1, 2]. It is envisioned as the next generation power system that integrates information and communication network with the traditional power infrastructure. This networking facility enables the utility providers to deliver and distribute the power to the consumers according to their requirements. They can monitor and control the power consumption, usage and electricity bill through advanced metering infrastructure (AMI) which is the central networking infrastructure of SG. Smart meter (SM) is the core networking device of AMI which establishes full duplex communication link among the consumers and the service providers. Through this duplex link the SM sends energy consumption report to the utility providers from the smart electrical appliances and retrieves electricity bill for the consumers.

This heavy dependability on communication network makes the power grid vulnerable to the adversaries. The adversary can intrude the network and launch various cyber attacks to disrupt the normal operation of the power grid through SM as SM is the central networking device between the home area network (HAN) and neighborhood area network (NAN).

Cyber attacks can be classified as insider attack and outsider attack [3]. In outsider attack, an adversary can attack the network without notifying the network administrator. The adversary can alter the data sent by the smart meter or manipulate the energy related data. Also, power outage can occur due to cyber attacks which can lead to hazardous situation in the network. Therefore, for protecting the network from attackers and ensuring privacy of the users, it is important to design security mechanisms that are compatible with the power infrastructure. The critical infrastructure of power grid imposes challenges to design and implement security mechanism to prevent any kind of cyber attacks and user privacy from the attackers. The SM is a resource constraint electronic device that requires light weight and resource efficient security mechanism to secure the communication among various devices. However, the conventional cryptography mechanisms are not resource efficient and suitable to use in SM security as these mechanism consumes extra power, requires high processing time and introduces overhead. Recently, various types of schemes have been proposed in the literature focusing resource efficiency of the SM.

A lightweight authentication mechanism has been proposed in [4] named LiSA which incorporates elliptic curve cryptography (ECC) and ensures mutual authentication, anonymity, reply attack prevention and it takes less execution time. In [5] the authors have mentioned that as a resource constrained device the smart meter needs lightweight cryptography mechanism for securing the network. The authors have proposed physically unclonable function (PUF) based lightweight security solution. In [6] an authentication scheme has been proposed based on one-time password scheme to ensure mutual authentication between SM and the servers of the SG. The authors in [7] have proposed a sign-cryption mechanism for the security of SM which reduces maintenance cost of traditional key management infrastructure. PKI based physical layer assist mutual authentication (PLAMA) mechanism has been proposed in [8] for two-way communication in smart meter which is lightweight and provides faster authentication process. The authors in [9] have proposed an efficient message authentication scheme with non-repudiation service which also ensures low power consumption, but they did not prove power consumption issue clearly. In [10] the authors have proposed a novel authentication scheme based on ring oscillator physically unclonable functions for AMI network. The authentication mechanism ensures security for the communication between SM and utility company. It is secured, storage efficient and low latency. PUF and CSI based encryption mechanism has been proposed in [11] to ensure authentication and integrity of the network. Electricity forecasting based security and privacy scheme has been proposed in [12] which declines the overhead introduced by communication and computation. The authors in [13] has proposed a low overhead authentication mechanism to ensure security between SM and utility company. A framework based on anonymization has been proposed in [14] to enhance the security of the SG. Public key-based approach has been demonstrated in [15] which ensures authentication, integrity, confidentiality and non-repudiation but public key based schemes are not energy efficient. To establish secure communication between consumers and substations, the authors in [16] proposed an ECC based authentication scheme but it is unable to ensure forward secrecy [17]. Shared secret key and random number based lightweight cryptography mechanism has been proposed in [18] for communication between supervisory node and control node. PUF and one way hash function based cryptography has been introduced to establish security among SM and service provider [19].

In this paper, we propose to use a lightweight energy efficient cryptography scheme named Salsa20 [20] for securing the SM network. Salsa20 is based on ARX (addition, rotation and XOR). In conjunction with Salsa20, we suggest to use elliptic curve based authentication scheme before any data exchange takes place using Salsa20. Section 2 discusses the SM network. In section 2 we discuss our proposed solution. In section 4 we analyze the proposed scheme numerically and section 5 concludes the paper.

## 2. SMART METER NETWORK

Smart meter network covers HAN, building area network (BAN) and NAN, transmission, distribution, service provider, market and operation management according to the NIST [21-23]. Figure 1 demonstrates the HAN network. HAN is a network inside the home utilized to monitor, record and collect energy usage data from the electrical appliances connected to the network. The smart energy devices connected wirelessly with the SM sends energy consumption data of the electrical appliances. The utility company can collect the energy consumption data through the SM using these energy devices as well as the home owners can also monitor their energy consumption data at the SM. However, the wireless connectivity is vulnerable to cyber attacks that can cause major damage to the network. Therefore, it is a vital requirement to secure this network to protect the power grid form the adversaries.

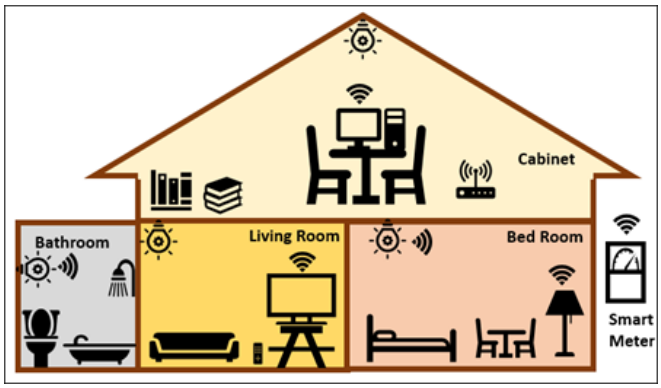


Figure 1. Architecture of smart meter network

## 3. PROPOSED METHOD

### 3.1. Initialization phase

SM and another connected device with SM will perform initial authentication using elliptic curve cryptography [24]. For encryption and decryption based on elliptic curve, each electrical device say $i$, chooses a generator point $g$ in $E_p(a, b)$, a private key $n_i$ such that $n_i < n$ where $n$ is the smallest positive integer number for which $n \times g = \otimes$. Then the chosen generator point with the elliptic curve $E_p(a, b)$ are made publicly available by the electrical node. After that the electrical device $i$ computes its public key as $P_i = n_i \times g$ and then shares with the SM. To encrypt a message for SM say $j$, device $i$ computes cipher text pair by choosing a random number lets say $k$ as,

$$C_M = (kg, P_M + kP_j)$$

where, $P_M$ is the point in which the message $M$ has been encoded following a suitable encoding process. To decrypt the message sensor node $j$ performs following operation:

$$P_M + kP_j - n_j(kg)$$

$$= P_M + k(n_j g) - n_j(kg)$$

$$= P_M$$

That is node $j$ first multiplies the first point of the cipher text with its private key and subtracts from the second point. A malicious node needs to know the random number $k$ for decrypting the message and it is difficult to compute $kg$ given $g$. Utilizing elliptic curve cryptography, the SM and the other smart devices will share their identity for authentication purpose. After completing authentication, the SM will exchange data with other devices using low powered cryptography called Salsa20.

### 3.2. Data exchange phase

In this section we discuss the data exchange between SM and the connected appliances. We have suggested to use Salsa20 [20] stream cipher as the encryption mechanism as it is a lightweight security mechanism for exchanging meter read in and other information. Another version of Salsa20 is ChaCha20. In another work we have proposed ChaCha20 as the encryption and decryption mechanism. Here, we have compared ChaCha20 and Salsa20 in the performance evaluation section. Salsa20 takes input of 16 words and outputs 16 words. Like other cryptography algorithms Salsa20 also has a round function which operated repeatedly on some data to get the result. Salsa20's round function itself consists of 4 quarter round function. The quarter round functions can be stated as,

$$b^{\wedge} = (a + d) <<< 7$$

$$c^{\wedge} = (b + a) <<< 9$$

$$d^{\wedge} = (c + b) <<< 13$$

$$a^{\wedge} = (d + c) <<< 18$$

where, a, b, c, d are initial state words of 32 bits in length. Initial state matrix is 16 words, but the quarter round function operates on 4 32-bit words at a time. The initial state matrix can be defined as shown in Figure 2.

| | | | |
|---|---|---|---|
| Constant | Key | Key | Key |
| Key | Constant | Input | Input |
| Input | Input | Constant | Key |
| Key | Key | Key | Constant |

Figure 2. Initial matrix of Salsa20

## 4. PERFORMANCE EVALUATION

This section discusses the performance of the suggested method for SM. The performance evaluation through numerical analysis done here are expected to apply to SM and electrical appliances as well. We have numerically analyzed the performance of the suggested method in terms of energy consumption and processing time. As these two parameters can be used to analyze whether a scheme is lightweight or not, therefore we have examined to analyze in case of energy utilization and processing time. In the Table 1 demonstrates the parameters considered for numerical analysis.

Table 1. Numerial Parameters

| Procssor | Intel Core 2 Duo |
|---|---|
| Processors operating voltage | 0.8500V to 1.5V |
| Processors operating frequency | 2.13 GHz(Cycles/Second) |
| Current | 20.67 Amp |
| Current/Cycle | 9.70 Amp |
| Salsa20 Speed | 3.90 Cycles/Byte |
| ChaCha20 speed | 3.95 Cycles/Byte |

Energy consumption: this evaluation parameter denotes computational energy meaning the amount of energy consumed by a cryptography scheme when it operates encryption or decryption operation, transmission energy meaning the energy required to transmit packets to a receiving node, reception energy meaning the amount of energy needed to receive a packet. it is important to analyze energy efficiency as most of the wireless devices (specially SM) are battery powered and suffers from battery power limitation. Thus, designing energy efficient security scheme will enhance the lifetime of the devices. To evaluate energy consumption of our proposed scheme and ChaCha20, we have utilized the following equation [25]:

$$E = \frac{CC/B}{CC/S}\ I\ V$$

where, CC/ B denotes clock cycles required per byte for encryption and decryption. CC/S denotes clock cycle requires per second by the processor. I is the current and V is the operating voltage. Figure 3 demonstrates the comparison of energy consumption of Salsa20 and ChaCha20 which reveals that Salsa20 takes less power than ChaCha20 and makes the proposed scheme lightweight to be used in SM, whereas the other cryptography schemes like AES, DES requires lots of computational power which is not suitable for lightweight electronic device. Table 2 shows the energy consumption values for two schemes named Salsa20 and ChaCha20.

Processing time: It defines the time required for the processor to perform encryption or decryption of a size of data. The cryptography scheme which takes less processing time will perform fast than the cryptography scheme which requires large processing time. Also, fast processing time will reduce end to end delay. The required time can be calculated as,

$$time = \frac{Data\ Size}{Speed}$$
$$speed = \frac{CC/S}{CC/B}$$

where, speed denotes bytes per second or throughput. Figure 4 demonstrates the processing time required by ChaCha20 and Salsa20 which clearly reveals that Salsa20 takes less processing time which makes the processing of data faster. Table 3 shows the processing time comparison of Salsa20 and ChaCha20.

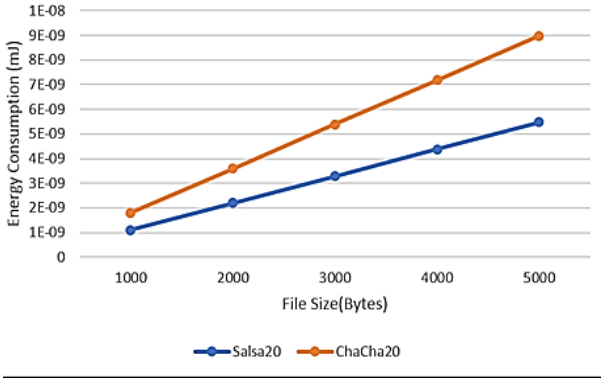


Figure 3. Comparison of computational energy consumption of Salsa20 and ChaCha20

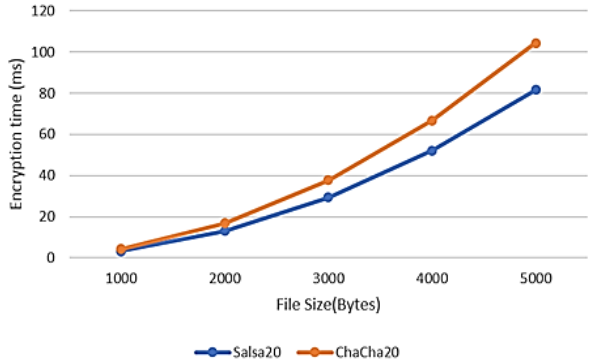


Figure 4. Comparison of processing time of Salsa20 and ChaCha20

Table 2. Computational energy consumption of two schemes

| File Size | Salsa20 enrgy consumption(mJ) | ChaCha20 energy consumption(mJ) |
|---|---|---|
| 1000 | $1.06 \times 10^{-9}$ | $1.91 \times 10^{-9}$ |
| 2000 | $2.13 \times 10^{-9}$ | $3.83 \times 10^{-9}$ |
| 3000 | $3.21 \times 10^{-9}$ | $5.39 \times 10^{-9}$ |
| 4000 | $4.37 \times 10^{-9}$ | $7.05 \times 10^{-9}$ |
| 5000 | $5.41 \times 10^{-9}$ | $9.00 \times 10^{-9}$ |

Table 3. Processing time comparison of two schemes

| File Size | Salsa20 Processing time (ms) | ChaCha20 Processing time (ms) |
|---|---|---|
| 1000 | 0.91 | 0.93 |
| 2000 | 17.98 | 18.67 |
| 3000 | 29.87 | 39.02 |
| 4000 | 51.01 | 68.37 |
| 5000 | 80.48 | 101.98 |

In this section we have analyzed the proposed scheme in case of energy utilization and processing time. Our purpose was to ensure a lightweight security scheme for a low powered electronic device SM. The numerical analysis of energy consumption and processing time clearly shows that the suggested scheme Salsa20 performs better and Salsa20 requires less processing time and computational energy which makes it lightweight.

## 5. CONCLUSION

In this paper, we have addressed the problem that the SM is a resource constrained electronic device which requires lightweight security mechanism for securing the network but most of the proposed protocols or methods can not satisfy the requirements needed to be lightweight as they consume huge processing power and takes huge processing time to complete its operation. Therefore, we have suggested to use ARX based simple lightweight stream cipher algorithm named Salsa20 to be used in SM for securing the power grid. Along with Salsa20, we have also proposed ECC based authentication before exchanging any data. ECC is

also energy efficient and it is a public key-based approach. Thus, before exchanging information using Salsa20, the SM authenticates with the legitimate device. We have numerically analyzed the performance in case of energy utilization and processing time. Figures 3 and 4 reveals that our suggested mechanism consumes very less energy and takes very less processing time which makes it suitable to be used in SM. In future, we will analyze the suggested security scheme in terms of its security performance.

## REFERENCES


[1] N. Komninos, et al., "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933-1954, 2014.

[2] A. Siddiqua, et al., "A Review and Techniques in Smart Grid for Authentication of Messages," *International Journal of Latest Engineering and Management Research (IJLEMR)*, vol. 03, no. 03, pp. 91-96, Mar 2018.

[3] M. Jouini, et al., "Classification of security threats in information systems," *Procedia Computer Science*, vol. 32, pp. 489-496, 2014.

[4] S. Garg, et al., "LiSA: A Lightweight and Secure Authentication Mechanism for Smart Metering Infrastructure," *This paper has been accepted for publication in the IEEE Global Communications Conference (GLOBECOM'19)*, December 2019.

[5] S. Ryu, "PUF based Smart Meter Security with Sx Chain," *International Journal of Control and Automation*, vol. 9, no. 9, pp. 407-414, Sep 2016.

[6] Y. S. Lee, et al., "A Study on Secure Chip for Message Authentication between a Smart Meter and Home Appliances in Smart Grid," *2013 International Conference on IT Convergence and Security (ICITCS)*, pp. 1-3, 2013.

[7] E. U. Soykan, et al., "Identity based signcryption for advanced metering infrastructure," *2015 3rd International Istanbul Smart Grid Congress and Fair (ICSG)*, pp. 1-5, 2015.

[8] T. Ma, et al., "Physical Layer Assist Mutual Authentication scheme for smart meter system," *2014 IEEE Conference on Communications and Network Security*, pp. 494-495, 2014.

[9] J. Choi, et al., "An Efficient Message Authentication for Non-repudiation of the Smart Metering Service," *2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering*, pp. 331-333, 2011.

[10] M. Mustapa, et al., "Hardware-Oriented Authentication for Advanced Metering Infrastructure," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1261-1270, Mar 2018.

[11] A. M. Allam, "A Novel Non-cryptographic Security Services for Advanced Metering Infrastructure in Smart Grid," *Communications on Applied Electronics (CAE)*, vol. 3, no. 7, Nov 2015.

[12] A. Abdallah and X. Shen, "Lightweight Security and Privacy Preserving Scheme for Smart Grid Customer-Side Networks," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1064-1074, May 2017.

[13] I. Doh, et al., "Secure Authentication for Structured Smart Grid System," *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 200-204, 2015.

[14] S. Afrin and S. Mishra, "An anonymized authentication framework for smart metering data privacy," *2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1-5, 2016.

[15] D. Ghosh, et al., "A Lightweight Authentication Protocol in Smart Grid," *International Journal of Network Security*, vol. 20, no. 3, pp. 414-422, May 2018.

[16] K. Mahmood, et al., "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generation Computer Systems*, vol. 81, pp. 557-565, April 2018.

[17] Y. Chen, et al., "A Bilinear Map Pairing Based Authentication Scheme for Smart Grid Communications: PAuth," *IEEE Access*, vol. 7, pp. 22633-22643, 2019.

[18] Q. Wu and M. Li, "A Lightweight Authentication Protocol for Smart Grid," *IOP Conference Series: Earth and Environmental Science*, vol. 234, no. 1, pp. 1-6, 2019.

[19] P. Gope and B. Sikdar, "Privacy-Aware Authenticated Key Agreement Scheme for Secure Smart Grid Communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3953-3962, July 2019.

[20] D. J. Bernstein, "ChaCha, a variant of Salsa20," [Online], Available: https://cr.yp.to/chacha/chacha-20080120.pdf, 2008.

[21] N. Mengidis et al., "Blockchain and AI for the Next Generation Energy Grids: Cybersecurity Challenges and Opportunities," *Information & Security: An International Journal*, vol. 43, no.1, pp. 21-33, 2019.

[22] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344-1371, April 2013.

[23] Z. El Mrabet, et al., "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469-482, April 2018.

[24] W. Stallings, "Cryptography and Network Security," 4th Edition. Prentice Hall, pp. 310-312, 2005.

[25] A. Ahmad, et al., "Comparative Analysis of Different Encryption Techniques in Mobile Ad Hoc Networks (MANETS)," *International journal of Computer Networks & Communications (IJCNC)*, vol. 8, no. 2, pp. 89-101, March 2016.