PRESERVING INTEGRITY AND PRIVACY OF DATA IN SMART GRID COMMUNICATIONS

Saeed Alishahi
Mashhad Electric Energy Distribution Company (MEEDC), Iran
s.alishahi@meedc.net

Seyede Masoome Seyyedi
Mashhad Electric Energy Distribution Company (MEEDC), Iran
M.seyedi2010@gmail.com

M.H.Yaghmaee
Mashhad Electric Energy Distribution Company (MEEDC), Iran
yaghmaee@ieee.org

Mohammad Alishahi
Mashhad Electric Energy Distribution Company (MEEDC), Iran
alishahi@mshdiau.ac.ir

ABSTRACT

Smart meter is an advanced energy meter that measures the amount of consumption of electrical energy and transmits data to a database at a utility server. Confidentiality and no modifying of smart meter readings are important because altered readings from the meter can lead to incorrect billing and false energy usage approximations.
In this paper we provide a pairing-free certificateless signcryption (CLSC) scheme based on elliptic curve for preserving privacy and integrity of data between the utility server and customer smart meters. CLSC at the same time achieves confidentiality and authentication by combining public-key encryption and digital signature. Our proposed scheme is capable of preventing different attacks such as Replay, Man-In-The-Middle and Spoofing attacks.

INTRODUCTION

Advanced Metering Infrastructure (AMI) is the major component in smart grid that consists of different devices, such as smart meters in the home or office, the data collector or concentrator node often located in the neighborhood, head end systems, hosts, routers, etc.
The smart metering infrastructures have a hierarchical structure as follow: electric appliances are connected to the smart meter by home network in order to report detailed energy consumption data. Smart meters measure the total energy consumption and data is sent to the next concentrator node by a neighborhood network. Concentrator nodes are monitor and collect data from several smart meters and data is sent to utility data centers.
The most important security objectives are availability, integrity and confidentiality. Availability is achieved by providing integrity and confidently of customer's information. Since smart meter is installed at customer's site, confidentiality and no modifying of smart meter readings are important. The main concern is about privacy because smart meter readings are private information such as number and kind of electrical devices, when the users are at home, when they use from devices, when they come back from work and etc.
Elliptic Curve Cryptography (ECC), a public key encryption method. For protocols based on elliptic curves, it is assumed that finding the discrete logarithm of a random point on an elliptic curve with respect to a common base point, is impractical. Size of elliptic curve determines difficulty problem [5].
Certificateless signcryption (CLSC) is one of the most significant security primitives in CL-PKC, and at the same time achieves confidentiality and authentication by combining public-key encryption and digital signatures, offering better overall performance and security.
In this paper we provide a pairing-free certificateless signcryption (CLSC) scheme based on elliptic curve for preserving privacy and integrity of data between the utility server and customer smart meters.
The rest of this paper is organized as follows: In section II the related work is described. The proposed CLSC scheme is given in section III. Section IV evaluates the proposed scheme and compared with previous designs. Finally the conclusion is given in section V.

RELATED WORK

In [1,2] a structured analysis on vulnerabilities and threats related to smart grids is proposed. The home area network (HAN) used for an AMI application should ensure adequate and secure communication between AMI and the terminal appliances. The proposed work given in [3] focuses on security aspects of communication between AMI and terminal residential appliances. This paper identifies wireless networking solutions such as ZigBee as the best mode for such communication.
The research on Elliptic Curve Cryptography system was started in 1985s. Elliptic curves which for the first time were introduced by Miller and Koblitz [4], play an important role in cryptography systems. In [5] Zheng proposes a new cryptography technique named "Signcryption" which combines the functions of digital signature and encryption algorithm for authentication and confidentiality. His scheme is based on discrete logarithm problem (DLP). In [6] Zheng proposes another signcryption scheme based on elliptic curve, which saves about 58% computational cost and saving about 40% communication cost than signature-then-encryption scheme based on elliptic curve. This plan provides the security requirements such as confidentiality, integrity and non-repudication. The scheme is based on discrete logarithm problem on elliptic curve (ECDLP).
The focus of [7] is on securing network

communications in AMIs. In particular, they propose the use of an identity based signcryption system to address the security issues of confidentiality and authenticity in an AMI communication network. The suitability of employing such identity-based cryptosystems in the context of smart grids is studied from the perspective of security requirements, implementation overhead and ease of management. Compared to other public-key systems, their proposed system provides scalable and secure communications among smart-meters, smart-appliances and monitoring sensors.

In 2003, Al-Riyami and Paterson [8] introduced the concept of certificateless public key cryptography (CL-PKC), which eliminates the use of certificates as in the traditional PKC and solves the key escrow problem that is inherent in identity based cryptography. CL-PKC scheme [8] is based on bilinear maps.

Since the notion of CLSC was introduced in 2008 [9], most concrete constructions of the existing schemes [9, 10] are built from bilinear maps. In [11,12], two pairing-free CLSC schemes based on DLP were proposed. Moreover, the times of the modular exponential operation of these CLSC schemes [11,12] are still high. [11] requires three modular exponential operations by sender and two modular exponential operations by receiver. [12] requires six modular exponential operations by sender and eight modular exponential operations by the receiver.

In elliptic curve cryptography, bilinear pairings are functions that map a pair of elliptic curve points to an element of the multiplicative group of a finite field [14]. In pairing-based cryptosystems, the computation cost of the pairing is high[12]. The relative computation cost of the pairing is approximately 20 times higher than that of the scalar multiplication over elliptic curve group [13].

CERTIFICATELESS SIGNCRYPTION WITHOUT PAIRING

In this paper, we propose a new efficient pairing free certificateless signcryption scheme based on elliptic curve. In our proposed scheme, public and private key of each entity is produced based on CL-PKC and transmission of data between entities is based on signcryption technique. Our CLSC scheme involves three parts: a key generation center (KGC), a sender with an identity ID_A and a receiver with an identity ID_B.

In order to prevent replay attack, we use timestamp concepts. Timestamps have a key role in freshness of messages. In our proposed scheme it is assumed that each device such as smart meter, data collector, concentrator node or utility server, has a unique identification number like a serial number. Initially, each device to be able to decrypt received messages and signs the messages, must get the partial private key from the KGC. KGC has a master key, which keeps it secret and using it to generate user's partial private key. Our CLSC scheme consists of the following eight phases:

Setup

In this phase, we should select and publish some parameters. KGC performs the following steps:

1) Selects a k-bit prime p and determines $\{F_q, E/F_q, G, P\}$.
   - A field size q, where either q=p in case that p is an odd prime (the common practice), or $q = 2^m$ in case that q is a prime power.
   - For $q = 2^m$: two parameters $a, b \in F_q$ are used to define the elliptic curve equation E over $y^2 = x^3 + ax + b (\mathrm{mod}\, q)$. In case that $q > 3$, where $4a^3 + 27b^2 \neq 0 (\mathrm{mod}\ q)$. E should be divisible by a large prime number with regard to the security issue raised by Pohlig and Hellman [4].
   - For $q = 2^m$: the elliptic curve equation E over $y^2 + xy = x^3 + ax^2 + b$ where $a, b \in F_q, b \neq 0$, together with the point at infinity ∞. In both cases, E is an (additively written) abelian group with the point ∞ serving as the identity.
   - P: a base point of elliptic curve F with order n.
   - n: the order of point P, where n is a prime, $n \times P = O$ and $n > 2^{160}$.
2) Randomly selects $s \in Z_n^*$ as the master private key and computes the master public key $Q_{KGC} = s.P$.
3) KGC chooses two cryptographic secure hash functions $H_1 : \{0,1\}^* \rightarrow Z_n^*$ and $H_2 : \{0,1\}^m \rightarrow Z_n^*$
4) KGC secretly keeps the master key s, publishes $Params = \{F_q, E/F_q, p, Q_{KGC}, H_1, H_2\}$ as system parameters.

Production of device-primary keys

During the manufacture of a device (e.g. smart meter, concentrator node, utility server …), a pair of device-primary keys, $ID - DR_A$ and $KGC - DR_A$ and Params are embedded into the device. $ID - DR_A$ Key is unique identification number of each device (e.g. serial number). KGC chooses a random number $s_1 \in Z_n^*$, computes $KGC - DR_A$ using the following equation:

$$KGC - DR_A = s + H_1(ID - DR_i).s_1 \qquad (1)$$

Before a device can communicate with other devices in the smart grid network it must get the partial private key from the KGC so it must make registration to KGC. The primary keys are used for initial communication.

Extract partial private key

For receiving partial private key, sender (A) itself should communicate with KGC. This algorithm takes master key, a user's identifier and system parameters as input, and returns the user's ID-based partial private key. KGC computes partial private key and issues it to the users through secret channel. With this algorithm, for user A with identity $ID-DR_A$, KGC works as follows.

Step 1: A constructs a packet containing $ID-DR_A$, system parameters, signs the whole packet by $KGC-DR_A$ to form a digital signature, SIG. A works as follow:

1) Randomly select $r \in Z_n^*$.
2) Computes $R = r \times P = (x_1, y_1)$ and $v = x_1 \bmod n$ (if v=0 then go back to step 1).
3) Message $m = (params \| ID-DR_A)$, computes $e = H_2(m)$ and $SIG = (eKGC-DR_A + r) \bmod n$.
4) Sends (m, R, SIG) packet with SIG to KGC.

Step 2: KGC receives the packet with SIG, verifies SIG using $KGC-DR_A$ as follow:

1) Computes $v = x_1 \bmod n$.
2) $e = H_2(m)$.
3) KGC can validate SIG by checking whether the equation $Sig \times P - R = eKGC-DR_A \times P$ holds.

Step 3: KGC calculates the partial private key of A if the equation holds. Using the following steps:

1) KGC computes $Z_A = H_1(ID-DR_A)$.
2) Randomly selects $y \in Z_n^*$, computes $Y = y \times P$ and partial private key for A: $d_A = s.Z_A + y$

KGC works as follows to send d_A to A through secret channel in step 4.

Step 4: KGC encrypts d_A by $ID-DR_A$ to form $d_A^{'}$ and then signs $d_A^{'}$ by its private key to form SIG_1. KGC sends $d_A^{'}$ and SIG_1 to A (signature like step1).
Computes $d_i^{'} = E_{ID-DR_i}(d_A)$ and $SIG_1 = Sign(d_A^{'})$.

Step 5: A receives $d_A^{'}$, verifies SIG_1 by KGC's public key and then decrypts $d_A^{'}$ by $KGC-DR_A$ to obtains d_A.
A can validate its partial private key by checking whether the equation $d_A \times P = Q_{KGC}.H_1(ID-DR_A) + Y$ holds. The partial private key is valid if the equation holds and vice versa. A device primary key pair is only used for device registration for a single device. KGC will ignore duplicated use of any key pair. Phases1-3 are performed by KGC, while phases 4-8 are performed by user.

Set-Secret-Value

Select a random number $x_A \in Z_n^*$ as secret value.

Set-Public-Key

Taking Params, an A's partial public key d_A and its secret value x_A as input, this algorithm generates Q_A for the user with identity id_A as follows: $Q_A = (x_A + d_A) \times p$.

Set private key

It takes Params, A's partial private key d_A and the secret value x_A as input, and returns the A's full private key SK_A.
$sk_i = x_i + d_i$
A can use SK_A, for next communication with other devices in the smart grid network.

Signcrypt

In this phase for transmitting message from smart meter to the utility server or vice versa, these operations are done. We assume that sender is A and receiver is B. To send a message $M \in \{0,1\}^m$ to B, A works as follow:

1) Randomly select $r \in Z_n^*$.
2) Computes $R = r \times P = (x_1, y_1)$ and $v = x_1 \bmod n$ (if v=0 then go back to step 1).
3) A produces its timestamp t_1 with its local time or trust time server. Computes $T_A = H_1(t_1) \bmod n$, $K = T_A.r \times Q_B = (x_k, y_k)$.
4) Computes $k = H_1(v \| x_k \| y_k)$ as session key.
5) Generates cipher text $C = M \oplus k$.
6) Computes $e = H_2(M \| T_A \| ID_A \| ID_B)$
7) Computes $S = (esk_A + r) \bmod n$.
8) A sends the signcrypted text $\sigma = (C, R, S, T_A, ID_A)$ p to B.

Unsigncrypt

Upon receiving a new message for unsigncrypt a cipher text $\sigma = (C, R, S, T_A, ID_A)$, the receiver B acts as follows:

1) By using R, computes $v = x_1 \bmod n$.
2) Produces its timestamp and computes $T_B = H_2(t_2) \bmod n$.
   B checks whether $0 < T_B - T_A < \alpha$ for receiving message. B accepts the message if the above equation is true otherwise neglects the old message. α is delay time between sending and receiving of a message in the communication link.
3) Computes $K = R \times sk_B.T_A = (k_1, k_2)$.
4) Computes $k = H_1(v \| x_k \| y_k)$.

5) Decrypts cipher text $M = C \oplus k$.
6) Computes $e = H_2(M \| T_A \| ID_A \| ID_B)$.
7) B accept M if $SP - R = eQ_A$, otherwise A does not send this message to B.

In figure1 the details of proposed CLSC scheme is shown.

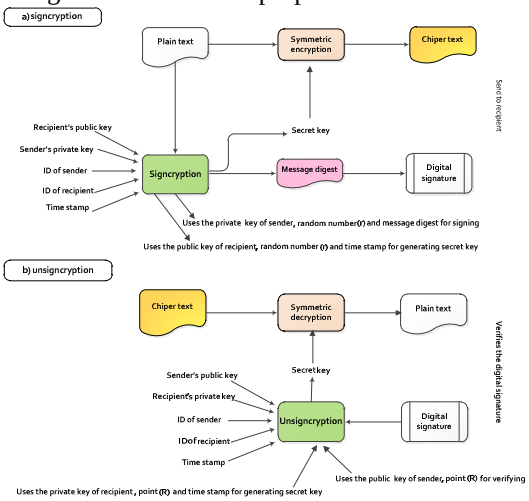

Figure 1: The proposed CLSC scheme

EVALUATION THE PROPOSED SCHEME

In this section, we evaluate the security performance of the proposed scheme. Most of these results are based on the elliptic curve discrete logarithm problem (ECDLP). ECDLP is a computational infeasible problem [4].

Confidently

The attacker to decrypt the cipher text C requires the secret key (k). As regards, the attacker just knows the point Q_B and P, if attacker tries to derive the secret key, it must solve the ECDLP. On the other hand the attacker does not have knowledge of secret parameter r or designated recipient's private key. As previously mentioned, this problem is computational infeasible.

Authentication

The recipient decrypts the cipher text C and gets the plain text M. It can use Eq. (2) to authenticate correctness of received message and sure no change message in the transmission process. The proposed scheme resistant to the man in the middle (MITM) attacks.

$$SP - R = eQ_A \quad (2)$$

Integrity

Integrity of the proposed scheme is proven using following equation:

$$K_A = T_A.r \times Q_B = T_A.r \times (x_B + d_B) \times P = T_A.r(x_B + sZ_B + y) \times P$$
$$K_B = R \times sk_B.T_A = r \times P \times (x_B + d_B) \times T_A = T_A.r(x_B + sZ_B + y) \times P \quad (3)$$

Both of participants calculate the same session key.

Unforgeability

The attacker to forge valid (M, R, S, T_A, ID_A) should have the private key of sender and the secret parameter r. Assume that the attacker with eavesdropped link channel, generates forge (M', R', S', T_A, ID_A), it must generate e' and S' using Eqs. (4), (5). The attacker to get the secret parameter r from $R = r \times G$, should solve the ECDLP firstly which is computationally infeasible. The attacker does not have private key of sender so it cannot forge (M', R', S', T_A, ID_A). Therefore, our proposed scheme satisfies unforgeability.

$$e = H_2(M' \| T_A \| ID_A \| ID_B) \quad (4)$$
$$S' = (e' sk_A + r) \bmod n \quad (5)$$

Non-repudiation

This feature is proven like unforgeability.

Forward secrecy

The forward secrecy of message means that if compromising the long term private key of sender x, the attacker is not capable of decrypting the previously signcrypted messages. The sender (A) uses the session key k for encrypting a message (M) and the session key has resilience to disclosure of secret parameter r. The attacker even got private key of sender sk_B and signcrypted text (C,R,S), who still cannot compute session key in Eq. (6). If it wants to get r from R, it should solve the computational infeasible problem ECDLP.

$$K = T_A.r \times Q_B = (x_k, y_k) \quad (6)$$

Public verification

Given (M, R, S, T_A, ID_A) anybody can verify the signature by checking the $SP - R = eQ_A$ condition, without any need for the private key of *A* or *B*. Therefore, our proposed scheme provides the public verification properties.

In table I, time complexity of various operation units to the time complexity of executing the modular multiplication is given[4]. In table II, time complexity of proposed scheme is compared with previous schemes. First of all, by considering execution time of each operator, total needed time cost for different schemes are identified. Then, with reference to table I, total times regarding needed time for modular multiplication operation is expressed. Considering table II, our proposed model has less time complexity and calculation cost than schemes [7,10,11,12] in signcryption and unsigncryption. Moreover, our proposed model doesn't need pairing compute. However, schemes

[8, 12] which are pairing based, bring about too much calculation cost in transmitter and receiver sides.

Table I : Conversion of various operation units to TMUL

Definition	Conversion of various operation units to TMUL
Time complexity for executing the modular exponentiation	$T_{EXP} \cong 240T_{MUL}$
Time complexity for executing the modular addition	T_{ADD} is negligible
Time complexity for executing the modular multiplication	$T_{EC\_MUL} \cong 29T_{MUL}$
Time complexity for executing the multiplication of a number and an elliptic curve point	$T_{EC\_ADD} \cong 0.12T_{MUL}$
Time complexity for executing the addition of two points in an elliptic curve	$T_{INV} \cong 3T_{MUL}$

Table II. Comparison of proposed model's time complexity with previous models

Reference	Time complexity		Complexity in T_{MUL}	
	SC	USC	SC	USC
[7]	$3T_{EC-MUL} + T_{MUL} + T_{ADD} + 2pa$	$4T_{EC-MUL} + 3pa$	88 $T_{MUL} + 2pa$	116 $T_{MUL} + 3pa$
[10]	$3T_{EXP}$	$2T_{EXP}$	$720T_{MUL}$	$538T_{MUL}$
[11]	$6T_{EXP}$	$8T_{EXP}$	1440 T_{MUL}	1920 T_{MUL}
[12]	$T_{EC-MUL} + 2T_{MUL} + 3T_{ADD} + pa$	$4T_{EC-MUL} + pa$	31 T_{MUL} +pa	116 T_{MUL} +3pa
Ours	$2T_{EC-MUL} + 2T_{MUL} + T_{ADD}$	$3T_{EC-MUL} + T_{MUL}$	60 T_{MUL}	88 T_{MUL}

CONCLUSION

In this paper we proposed a new scheme of certificateless signcryption based on elliptic curve. It is suitable for creating safety in smart meter communications and data concentrator node at NAN network in smart grid. It doesn't need extra computation for certificate and has less bandwidth load compare with models [5,6] which are based on PKI. Additional, proposed CLSC is pairing free. Since paring is costly on elliptic curve, our proposed scheme has less calculation cost than models [7,12]. Our proposed model needs two point multiplication operations, two modular multiplication operations and one modular addition operation. It also needs three point multiplication operations and one modular multiplication operation for unsigncryption. Evaluation results confirm that our proposed scheme is more efficient than previous schemes.

REFERENCES

[1] Florian Skopik and Zhendong Ma, 2012, "Attack Vectors to Metering Data in Smart Grids under Security Constraints", in 36th International Conference on Computer Software and Applications Workshops, IEEE pp134-139.

[2] Florian Skopik, Zhendong Ma, Thomas Bleier and Helmut Gruneis, 2012, "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructure", in Science Direct, Elsevier, p.8.

[3] Araavinthan Visvakumar, Vinod. Namboodiri, Samshodh Sunku, Ward. Jewell and Fellow, 2011, "Wireless AMI application and security for controlled home area networks", in Power and Energy Society General Meeting, IEEE.

[4] Neal Koblitz, Alfred Menezes, Scott Vanstone, 2000, "The state of elliptic curve cryptography", Designs, Codes and Cryptography, p. 173-193.

[5] Yuliang Zheng, 1997," Digital signcryption or how to achieve Cost (Signature & Encryption) _ Cost(Signature)+ Cost(Encryption)", in: advances in Cryptology—Crypto_97LNCS 1294, Springer-Verlag, pp. 165–179.

[6] Yuliang Zheng and Hideki Imai, 1998, "How to construct efficient signcryption schemes on elliptic curves", in Elsevier Science B.C.

[7] Hayden K.-H. So, Sammy H.M. Kwok, Edmund Y.Lam and King-Shan Lui, 2010, "Zero-configuration Identity-based Signcryption Scheme for Smart grid", International Conference on Smart Grid Communications, IEEE,pp.321-326.

[8] Sattam Al-Riyami and Kenneth G. Paterson, 2003, "Certificateless public key cryptography". Advances in Cryptology (ASIACRYPT 2003), Springer-Verlag, LNCS, p. 452-473.

[9] M.Farshim and P.Barbosa, 2008, "Certificateless signcryption". ACM Symposium on Information, Computer and Communications Security (ASIACCS 2008), p. 369-372.

[10] J.Xiaofei, 2011, "Provably Secure Certificateless Signcryption Scheme without Pairing", in International Conference on Electronic & Mechanical Engineering and Information Technology, p. 4753-4756.

[11] Wenjian Xie and Zhang Zhang, "Certificateless Signcryption without Pairing", Cryptology ePrint Archive: Report 2010/187, Availablefrom: http://eprint.iacr.org/2010/187.pdf.

[12] Fagen Li, Masaaki shirase and Takagi Tsuyoshi, 2013, "Certificateless hybrid signcryption", Elsevier Science Direct, p: 324–343.

[13] Debiao H, Jianhua Chen and Rui Zhang, 2011, "An effient identity-base blind signature scheme without billinear pairings". Computer and Electical Engineering Elsevier, 444-450. doi: 10.1016.

[14] S.Caroline, 2010, "Privacy Enhanced Protocols using Pairing Based Cryptography".