Certificateless Secure Anonymous Key Distribution Scheme for Smart Grid

Jennifer Batamuliza
University of Rwanda (UR)
African Center of Excellence in Data Science (ACE-DS)
PhD Candidate in Data Mining
University of Kigali (UoK)

ABSTRACT
Smart Grid is a modern digital metering system that has been introduced to replace the traditional electricity infrastructure by collecting and utilizing information generated from different consumers automatically. Many researches have been conducted on the secure communication sessions to address the key issue of security in smart grid communication. Existing secure anonymous key distribution scheme for smart grid brings challenge such as key escrow problem in identity based encryption and identity based signature. In this paper we incorporate the first concept of certificateless in order to solve the key escrow problem that is found in identity based signature scheme and an identity based encryption scheme. Our proposed scheme achieves key escrow resilience which has not been achieved by previous work in this field.

Keywords
Certificateless, anonymity, Smart Grid, Smart Meters.

1. INTRODUCTION
Smart Grid is a modernized electricity management and distribution system, it is a bidirectional digital technology whereby electric power and data information flow. The proposed smart grid applications use devices known as smart meters which are electronic and installed at the household or industry from where they record electricity that is used and sends the information at a certain interval to the service provider to enable billing. Smart meters have two way communications with the service provider. The smart meters communicate to the service provider about how electricity is being used at the customers' side and smart meters can receive messages in return from the service provider. Smart meter collects information of how power is consumed in a building in a real time manner and the smart meter sends information to the service provider who is in charge of distributing electricity.
Smart grid is reliable, efficient and transparent. This replaces the traditional way which is a one way analog technology that has many users with few generators. The modern technology can serve a large number of users' efficiently [1], [2]. Smart grid has positive impact to consumers as well as providers.

The bidirectional communication between the user and the service provider will help the user cut-off his cost on electricity depending on his need and how much he planned to spend on electricity. Smart grid provides high quality robust service hence the electricity disruption such as blackouts which causes inconvenience to consumers are avoided [3].

However, smart grid has brought some privacy and security issues besides its benefits. This happens because the consumer has to give more information such as its identity, email, location and more to the provider in an insecure channel while communicating and thus hackers can easily hack the consumer data which will help them invade his household or fabricate readings. Smart meters are devices which have sensors and communicators and can monitor electricity usage in a household and after it does some cryptographic computing in its small processing unit that is volatile too and send information to the service provider. The smart meter facilitates the two way communication, smart meters are installed outside the household and it is physically exposed to everyone hence giving space to whoever wants to perform bad act[4][11].

To solve that problem of owners information being exposed to the outsiders or being compromised by hackers, User anonymity is needed to hide personal information, unfortunately the smart meter cannot handle large computations because of the limited capacity to handle cryptographic computations [12] and [13] thus the use of authenticated key management scheme. Mutual authentication is achieved in a way that not only the user can authenticate the provider but also provider can authenticate the user. This is possible with the computation of session key to be used by both parties while exchanging information. Symmetric key cryptography means that there has to be only one key that is shared by both parties which is used for communication between parties. When the key is compromised it means that all communications that where made before will be revealed hence creating insecurity on both sides. A Public Key Infrastructure (PKI) is any system supporting [14] the deployment of Public Key Cryptography which is a combination of hardware, software and policies needed to deploy and manage certificates to produce trust in public keys. Registration Authority (RA) authenticates individuals/entities, optionally checking for the possession of private key matching public key. Later it passes off result to Certification Authority. Certification Authority (CA) Issues certificates by issuing signatures binding public keys and identities. Both parties need authentic copy of CAs public key. Directory of public keys/certificates may involve in the distribution of Certificate Revocation List (CRL) or online certificate status checking (OCSP).The PKI is not convenient to use because it has to manage many certificates hence it requires a lot of space, it also has revocation issues. Apparently, elimination of certificates produces a far simpler infrastructure. Shamir in (1984) proposed an identity based public key cryptosystem

[15] whereby Public keys are derived directly from system identities (e.g. an e-mail address or IP address). Private keys are generated and distributed to users by a trusted authority

(TA) who has a master key then user can safely encrypt to provider without consulting a directory and without checking a certificate. ECC is a public key cryptosystem [16], [17] that has been adopted of recent due to its advantages over RSA and discrete logarithm problem (DLP). ECC security relies on

elliptic curve logarithm problem. ECC can use much smaller key sizes and small computation cost to achieve same security as RSA and Discrete Logarithm problem [18]. This use of much shorter key favors smart grid because of the limited processing chip found in smart meter. Boneh and Franklin [19] in Crypto. 2001 proposed Identity based encryption scheme which uses bilinear maps over super singular elliptic curves.

1.1 Related Work

Wu and Zhou [20] proposed a key management scheme for smart grid. Their scheme is a combination of symmetric key and elliptic curve asymmetric. The former uses Needham Schroeder authentication and the latter uses ECC. The objectives of their schemes were strong service, scalability, fault tolerance, accessibility and efficiency. Unfortunately Xia and Wang [21] found that the scheme proposed by [20] was vulnerable against man-in-the-middle attacks. Hence they proposed a key distribution protocol that resists man-in-the-middle attacks. They solve higher costs incurred in performing certificate verification from PKI and also computations that cannot be handled by smart meter. Later Park et al. [22] showed that the scheme that was proposed by Xia and Wang [21] was not resistant to impersonation attack and unknown key share (UKS) attack was not true. Their scheme does not support smart meter anonymity that is needed by smart meters and service servers to achieve security. Wang proposed [23] [24], and identity- based and authenticated key agreement protocols following many identity- based key agreement protocols that have been proposed and none seem to be secure. Wang used Weil/Tate pairing whose security is proved with random oracle. However his schemes do not have anonymity which is a way of securing smart meter by hiding his identity while authenticating itself to the service provider thus allowing hacker to get access to smart meter hence security issues arises to the household owner. Wang [25] proposed a password protected smart card scheme which is a remote authentication between client and remote server that is used for protection against card reader impersonation without the smart card later. Also the HMQV protocol [26] authenticated Diffie-Hellman protocol, all these proposed schemes have no anonymity hence considered insecure. However, all of them do not support user (smart meter) anonymity. Tsai and Lo [27] proposed a scheme for secure communication to be achieved between smart meter and service provider. Tsai and Lo came up with this idea after surveying a number of proposed schemes and finding that all these schemes do not achieve security because of lack of anonymity. Therefore Tsai and Lo proposed a scheme that has anonymity. They used identity- based signature scheme and identity based encryption scheme for the key distribution scheme. Using one private key, a smart meter can anonymously access service provided by the service provider without the help of a trusted anchor in the authentication session. This makes their scheme different from other previously proposed authenticated schemes in this field.

1.2 Motivation

Existing secure anonymous key distribution scheme for smart grid suffers from key escrow problem because of the use of identity based encryption and identity based signature.

Using one private key, a smart meter can anonymously access service provided by the service provider without the help of a trusted anchor in the authentication session. This makes their scheme different from other previously proposed authenticated schemes in this field. Unfortunately it brings key escrow problem. In this paper we present the concept of certificateless in Certificateless Secure Anonymous Key Distribution Scheme in order to solve the key escrow problem that is found in identity based signature scheme and an identity based encryption scheme. Our proposed scheme achieves key escrow resilience which has not been achieved by any previous work in this field.

1.3 Our Contribution

We proposed a Certificateless Secure Anonymous Key Dis-tribution Scheme for Smart Grid in order to solve the key escrow problem that is found in identity based signature scheme and an identity based encryption scheme that was proposed by Tsai and Lo [27]. Key Generation Center acts as a third party in between the smart meter and service provider but it is not fully trusted by the two parties because it can also be malicious thus attacking the system because it knows the full private keys for smart meter and service provider. Thus a certificateless scheme is used to get rid of key escrow problem by allowing Key Generation Center to only provide partial key. Our scheme not only outperforms the previous schemes but also achieves key escrow resilience which has not been achieved by previous work in this field. Also our scheme will still make sure that anonymity of the smart meter goes in hand with certificateless scheme to resist attacks while sending data.

Our scheme is secure, efficient and also has forward security.

2. PRELIMINARIES

This important part will give a summarized introduction on basic mathematical background, the elliptic curve group, system model as well as the objectives for the proposed scheme.

2.1 Notations

We have listed some notations used in the whole paper in Table 1 to simplify with reading throughout this paper.

1) Elliptic Curve Group: The elliptic curve E over a prime finite field F_p represents the set of points (x, y) defined by the equation $y^2 = x^3+ax+b \bmod p$ with a, b $\in F_P$, and with the discriminant $4a^3 + 27b^2 \neq 0 \bmod p$. The above pair of points on F_P also has the intercepting point is at infinity; a point O as the point found at infinity or zero point, which is the additive identity of the group. The left-hand side has a degree of 2 while the right-hand side has a degree of 3. This means that a horizontal line can intersect the curve in three points if all roots are real. However, a vertical line can intersect the curve at most in two points over real numbers using a special class of elliptic curves of the form. Elliptic Curve Cryptography uses addition as an analog of modulo multiply, and repeated addition as an analog of modulo exponentiation. The hard problem is the elliptic curve logarithm problem. Definition 1 (Computational Deffie-Hellman: Given a tuple {P, aP, bP} $\in$ G for some a, b $\in_R Z^*_p$, the CDH problem in G is to compute the element abP.

Table 1. Notations and Descriptions

Notations	Descriptions
SM	Smart Meter
SP	Service Provider
PKG	Public Key Generator
ECC	Elliptic Curve Cryptography
DHP	Diffie-Hellman Problem
PKI	Public Key Infrastructure
CA	Certificate Authority
CDH	Computational Diffie-Hellman Assumption
F_p	A prime Finite Field
E/F_p	The elliptic Curve Over F_p

2.2 System Model

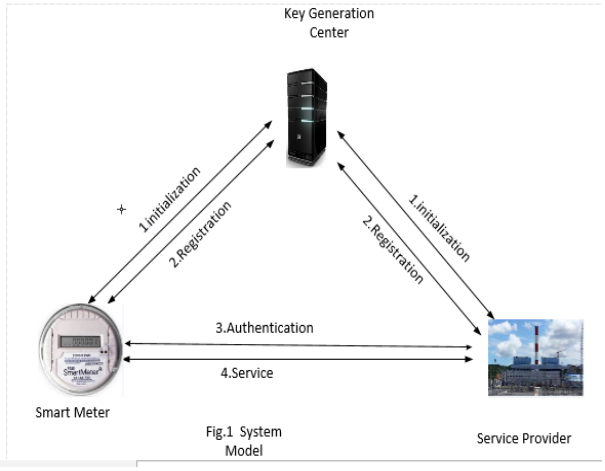

Fig 1: System model

Three types of entities are used in the system model above: Smart Meter(SM), Service Provider (SP), lastly the Key Generation Center (KGC). Smart Meter: SM is a device that is electronic and it is installed at the household or industry from where it records electricity that is used and sends the information at a certain interval to the SP to enable billing, SM needs to be preloaded with public parameters and registered with the KGC first before asking for any service from SP.

Service provider: SP is the electricity plant that provides electricity to households and industries at large. With the help of SM the electricity plant will distribute electricity as well as receiving information from smart meter in certain interval about the consumption and thus it is easy for the plant to perform billing as well as monitor and distribute its services. It also needs to be preloaded with public parameters and also registered with KGC before it can give service to the clients.

Key Generation Center (KGC): KGC is the registration center for SMs and SPs. KGC acts as a third party in between them but it is not fully trusted by the two parties because it can also be malicious thus attacking the system because it knows the full private keys for SMs and SPs. Thus a certificateless scheme is used to get rid of key escrow problem by allowing KGC to only provide partial key.

2.3 Objectives

(1)Anonymity: The Smart Meter authenticates itself anonymously to the service provider to prevent hackers from capturing its identity and later use it to get certain information such as knowing when the house owner is in or out and plan theft act. (2) Mutual Authentication: Both can authenticate each other by performing some algorithm. Hence prevention of Man-in-the-middle. (3) Session Key Establishment: A session key is established to enable communication between both parties in a simpler and safer way. (4) Key Escrow resilience: The KGC only knows the partial key and cannot derive full private key thus it is not able to impersonate neither the SM nor the SP. (5) Non-Repudiation: SM cannot deny performing certain unwanted behavior.

3. OUR PROPOSED PROTOCOL

This protocol consists of three phases, including Initialization, Registration and Authentication phases.

1. System Initialization

To initialize the system, KGC performs the following steps:

KGC first chooses master key $x \in_R Z^*_p$ and computes master public key $P_{Pub} = x \cdot P$. After that, KGC chooses five secure hash functions as follows: $H_1 : \{0, 1\}^* \times G \rightarrow Z^*_p$, $H_2 : \{0, 1\}^* \times G \times \{0, 1\}^* \rightarrow Z^*_p$, $H_3 : \{0, 1\}^* \times G^5 \rightarrow Z^*_p$, H_4: $\{0, 1\}^* \times G^5 \rightarrow \{0, 1\}^*$,

H_5: $\{0, 1\}^* \times G^4 \times \{0, 1\}^* \rightarrow Z^*_p$.

KGC publishes the system parameters $\{F_p, E/F_p, P, G, P_{Pub}, H_1, H_2, H_3, H_4, H_5\}$ and keeps the master key x secretly.

2. Registration

A. Service Provider

The service provider (SP) registers with the KGC before it provides any service to SM by performing the following: SP with identity ID_{sp} chooses $a_{IDsp} \in \{0, 1\}^*$ as its user secret key and computes the corresponding public key $PK_{sp} = a_{IDsp} \cdot P$. SP will send its own identity ID_{sp} to the KGC. After receiving ID_{sp} from SP, KGC will perform the following:

(a) KGC will randomly choose $y_{sp} \in_R Z^*_p$

(b) Compute $Y_{sp} = y_{sp} \cdot P$.

(c) Compute $h_{sp} = H_1(ID_{sp} \| Y_{sp})$.

(d) Compute $z_{sp} = y_{sp} + h_{sp} \cdot x$ as partial private key.

KGC sends (z_{sp}, Y_{sp}) to SP, SP will compute its full private key and also KGC will send the SM the tuple (ID_{sp}, Y_{sp}).

B. Smart Meter

The SM registers with the KGC before it requests for any service from SP by performing the following: SM with identity $ID_{sm} \in \{0, 1\}^*$ will choose $s_{IDsm} \in \{0, 1\}^*$ SM will compute its public key $PK_{sm} = s_{IDsm} \cdot P$. SM will then send the identity ID_{sm} to the KGC. Upon receiving ID_{sm} from SM, KGC will perform the following:

KGC will randomly choose $y_{sm} \in_R Z^*_p$

Compute $Y_{sm} = y_{sm} \cdot P$.

Compute $h_{sm} = H_1(ID_{sm} \| Y_{sm})$.

Compute $z_{sm} = y_{sm} + h_{sm} \cdot x$ as partial private key.

KGC will send (z_{sm}, Y_{sm}) to SM, SM will then compute its full private key.

3. Authentication

SM performs the following:

(a) Chooses $a \in_R Z^*_p$.

(b) Computes $T_A = aP$.

(c) Chooses $t_c \in (0, 1)^*$ as the time stamp.

(d) Compute $r = H_2(ID_{sp}, PK_{sm}, Y_{sm}, T_A, t_c)$.

SM computes $C_1 = rP$.

$C_2 = H_3(r(PK_{sp} + Y_{sp} + H_1(ID_{sp}, Y_{sp})P_{pub})) \oplus (ID_{sm} \| PK_{sm} \| Y_{sm} \| t_c \| T_A)$.

SM Sends a service request message Req = $[C_1, C_2]$ to the service provider. SP upon receiving Req = $[C_1, C_2]$ from SM, SP will perform the following:

(a) $(ID_{sm} \| PK_{sm} \| Y_{sm} \| t_c \| T_A) = H_3((a_{IDsp} + z_{sp})C_1) \oplus C_2$.

(b) Check the freshness of t_c.

(c) Computes r '= H_2 (ID_{sm}, PK_{sm}, Y_{sm}, T_A, t_c).
(d) Computes (H_2 (ID_{sm}, PK_{sm}, Y_{sm}, T_A, t_c)) P = C_1, if it holds then SP proceeds to the next step.
(e) SP chooses b $\in_R$ Z^*_p.
(f) Computes T_B = bP.
(g) Chooses t_c ∈ (0, 1)* as the time stamp.
(h) Computes k = H_4 (T_A, T_B, t_c, H_1 (ID_{sm})).
(i) Computes R = (k + T_B) P. SP will then send (R, t_c) to SM.
SM upon receiving (R, t_c) it will perform the following steps:
(a) Check the freshness of t_c.
(b) Compute k ' = H_4 (T_A, T '$_B$, t_c, H_1 (ID_{sm})).
(c) R ' = (k '+ T '$_B$) P.
(d) Check if R = R ', if this holds then T_B = T '$_B$. Thus the shared key is k = H_4 (T_A, T_B, t_c, H_1 (ID_{sm})). Smart meter authenticates the service provider of his choice and they can start communicating independently without involving KGC and without KGC knowing their shared key. SM will then send the Service Provider a signed message for verification, If verification is passed successfully, then SP authenticates the SM.
SM will perform the following:
(a) α = H_5(M, T_A, ID_{sp}, ID_{sm}, Y_{sm}, P_{Pub}).
(b) β = a + α(r s_{IDsm} + z_{sm}).
SM will then send the σ = (Y_{sm}, T_B, β) to SP.
Given: ID_{sp}, PK_{sm}, T_A, σ = (Y_{sm}, T_B, β). SP will compute α.
α = H_5(M, T_A, ID_{sp}, ID_{sm}, Y_{sm}, P_{Pub}).
Verify whether the equation βP = T_A + α(r · PK_{sm} +Y_{sm} + $h_{sm}P_{Pub}$) holds. If this holds then verification was successful.

4. SECURITY ANALYSIS

In this section we analyze the security of our proposed protocol.

4.1 Correctness Analysis

In this part we will analyze encryption that is done by smart meter, decryption done by the Service provider. We then analyze the signing by the smart meter and verification performed by the service provider.
Once the SP receives *Req* = [C_1, C_2] from SM it will perform the following: H_3 ((a_{IDsp} + z_{sp})C_1) $\oplus$ C_2 = H_3(a_{IDsp}+ z_{sp})rp $\oplus$ H_3(r(PK_{sp} + Y_{sp} + H_1(ID_{sp}, Y_{sp})P_{pub})) $\oplus$ (ID_{sm}‖PK_{sm}‖Y_{sm}‖t_c‖T_A) = H_3(r(a_{IDsp} +(y_{sp} +h_{sp}x)p)) $\oplus$ H_3(a_{IDsp} + Y_{sp} + H_1(ID_{sp}, Y_{sp})P_{pub}) $\oplus$ (ID_{sm}‖PK_{sm}‖Y_{sm}‖t_c‖T_A) = (ID_{sm}‖PK_{sm}‖Y_{sm}‖t_c‖T_A).

Verification is performed by the Service provider as follows: $\beta P = T_A + \alpha(r \cdot PK_{sm} + Y_{sm} + h_{sm}P_{Pub})$. With the help of $T_A = aP$, $Z_{sm} = y_{sm} + h_{sm} \cdot x$,
$\beta = a + \alpha(r \cdot s_{IDsm} + z_{sm})$.
$\beta P = P(a + \alpha(r_{sIDsm} + Z_{sm}))$.
$= P(a + \alpha[(r \cdot s_{IDsm} + (y_{sm} + h_{sm} \cdot x))])$.
$= aP + \alpha(r \cdot s_{IDsm}P + P(y_{sm} + h_{sm} \cdot x))$.
$= T_A + \alpha(r \cdot PK_{sm} + Y_{sm} + h_{sm}P_{Pub})$.

5. COMPARISON WITH PREVIOUS PROTOCOLS

Table 2. Comparison on Security

Properties	**Xia and Wang[**27]	**J.L.Tsai and N.W.Lo[29]**	**Ours certificateless**
Low computing cost at SM	No	Yes	Yes
Mutual Authenticatio n	No	Yes	Yes
Anonymity	No	Yes	Yes
Perfect Forward Secrecy	No	Yes	Yes
Key Escrow Resilience	No	No	Yes
Pairing Costs	No	Yes	No
Man-In The Middle-Attack	No	No	No

Our proposed paper has key escrow resilience due to the certificateless whereby the KGC only has to give a partial private key to the user, not a full private key that permits him to have access to private information between the SM and SP. Scheme [27] does not have key escrow resilience because it is an identity- based encryption and identity based signature. Our proposed scheme use ECC which has no pairing costs. Unlike [27] Scheme which has pairing thus high computation cost.
Xia and Wang scheme has no pairings. Anonymity is found in both [27] and our scheme. Thus smart meter can anonymously authenticate itself to the service provider hence smart meter information is kept as a secret. Unlike Xia and Wang scheme which has no anonymity. Our scheme and scheme [27] both have mutual authentication thus they can authenticate each other. All the above schemes do not suffer from Man In
The middle - Attack. Xia and Wang scheme has a trusted anchor involved in their authentication session thus making it insecure. Unlike our own scheme and [27] which do not involve a third party while authenticating one another. We assume T_{mp} is the time to perform one multiplication point operation, T_m is the time to perform one multiplication operation, T_p is the time to perform one bilinear pairing operation, T_e is the time to perform one modular exponentiation operation, T_s is the time to perform one symmetric encryption/decryption operation, T_{cert} is the time to perform a certificate generation operation, $T_{cert-ver}$ is the time to perform a certificate verification operation and T_H is the time to perform a Map-To-Point operation.

Table 3. Comparison on Computation Cost in Authentication Phase

Protocol	Smart Meter	Service Provider	KGC
Xia and Wang[27]	T_s	0	T_s
J. L. Tsai and N. W. Lo[29]	$4T_{mp}+T_e$	$2T_p + 3T_{mp} + T_e$	0
Ours	$5T_{mp} + 2T_m$	$8T_{mp}$	0

In these schemes, running time of the operations is got from the use of MIRACL. Windows xp operating system equipped with PIV3-GHz processor and 512 M bytes memory. Our ECC-

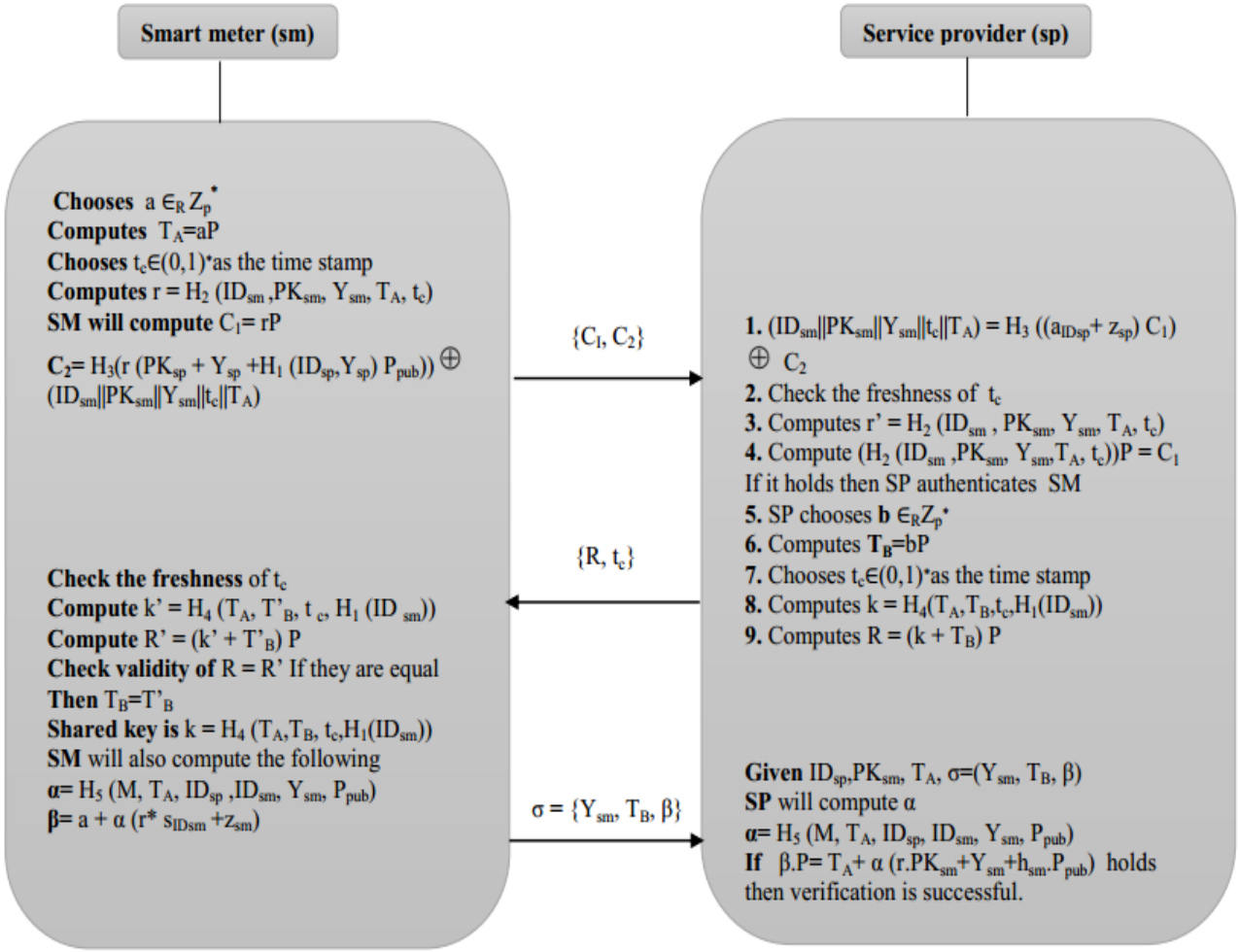

Fig 2: Proposed protocol.

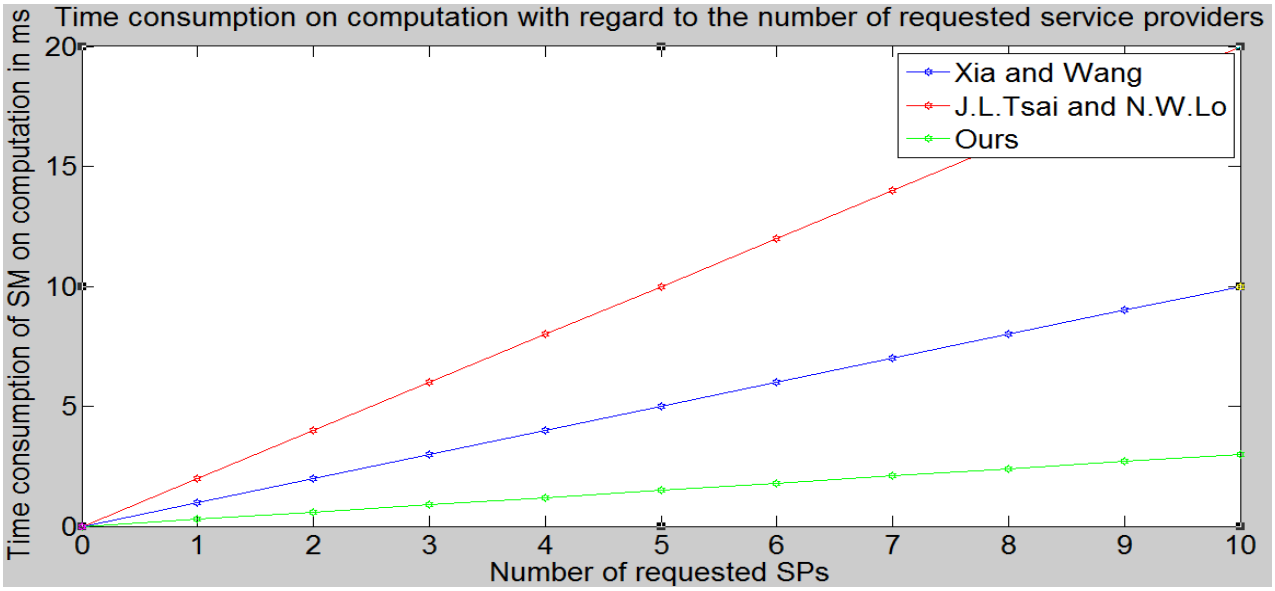

Fig 3: Time Consumption on Computation of Smart Meter with regard to the Number of Requested Service Provider

based protocol use Koblitz elliptic curve $y^2 = x^3+ax+b \ mod \ p$ with $a, b \in F_P$. Running time of the involved cryptographic operations on AP and client are listed in Table 4 below.

We have computations for the three protocols including our own protocol. Our proposed scheme consumes less time compared to other 2 as Such as in [27] at service provider 2 pairings are needed therefore (2 × 20.01) = 40.02ms is needed which is big. Additionally, in smart meter side exponential in Fp2 l. Therefore our scheme is better because of less computation time at smart meter side and less computation cost. We conclude that our scheme is better than the two schemes hence suitable is needed whose time is 11.20 whereas in our scheme at smart meter side we have no exponential for the smart meter which We have computations for the three protocols including our own protocol. Our proposed scheme consumes less time compared to other 2 as we can see. Such as in [27] at service provider 2 pairings are needed therefore (2 × 20.01) = 40.02ms is needed which is big. Additionally, in smart meter side exponential in Fp2 l. Therefore our scheme is better because of less computation time at smart meter side and less computation cost. We conclude that our scheme is better than the two schemes hence suitable is needed whose time is 11.20 whereas in our scheme at smart meter side we have no exponential for the smart meter which is a low power device.

Table 4. Cryptographic Operation Time in Milliseconds

Operations	Time
ECC-based scalar multiplication	0.83
Exponential in F_p^2	11.20
Pairing - based scalar multiplication	6.38
Pairing	20.01

6. CONCLUSION

A number of papers have been published in this field, none has been able to address the key escrow problem that arises as a result of Identity based encryption and identity based signature. Our paper focuses on solving key escrow problem by introducing certificateless. Apart from that, our paper also gets rid of pairing that was used in the previous scheme [27] by using ECC so as to reduce higher costs that comes with pairing. Security has been proved by random oracle model.

For future work, we are planning to further Secure Communication architectures. Different architecture designs have been used in Secure Communication for Smart Grid. Much work is required to customize these architectures in order to achieve efficiency, good performance and desired privacy under different scenarios. We propose to take a closer view of the above in our future work.

7. REFERENCES

[1] Yan, Y., Qian, Y., Sharif, H. and Tipper, D. 2013 A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges, IEEE Comm. Smart Grid

[2] Fang, X., Xue, G., Yang, D., and Misra, S. 2012"Smart Grid-The New and Improved Power Grid: A Survey," IEEE Comm. Power Grid.

[3] Moslehi, K. and Kumar, R. 2010. A Reliability Perspective of the Smart Grid, IEEE Trans. Smart Grid

[4] McDaniel P. and McLaughlin, S. 2009. Security and privacy challenges in the smart grid, IEEE Security Privacy

[5] X. Wang and P. Yi, 2011. Security framework for wireless

Communications in smart distribution grid, IEEE Trans. Smart Grid

[6] Flick, T., 2009. Hacking the smart grid, in Proc. Black Hat, Las Vegas, NV, USA

[7] Guidelines for Smart Grid Cyber Security, NIST Standard IR 7628, Aug. 2010

[8] Khurana, H. Hadley, M. Lu, N. and Frincke, D. A. 2010. Smart grid security issues, IEEE Security Privacy

[9] Nat. Inst. Stand. Technol. (Aug. 2010). Guidelines for Smart Grid Cyber Security: Vol. 3 Supportive Analyses and References. [Online]. Available: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628vol3.pdf

[10] Y. Strengers, 2010. Smart metering demand management programs: Challenging the comfort and cleanliness

habitus of households, in Proc. 20th Australasian Conf. Comput. -Human Interact. Design. Habitus Habitat.

[11] J. L. Tsai, N. W. Lo, 2015. Secure Anonymous Key Distribution Scheme for Smart Grid, IEEE Trans. Smart Grid

[12] H. Krawczyk, 2005. HMQV: A high-performance secure DiffieHellman pro- tocol, in Proc. CRYPTO, Santa Barbara, CA, USA

[13] Y. Wang, 2012. Password protected smart card and memory stick authentication against off-line dictionary attacks, in Information Security and Privacy Research. Berlin, Germany: Springer-Verlag

[14] Y. Wang, 2013. Efficient identity-based and authenticated key agreement protocol, in Transactions on Computational Science XVI. Berlin, Germany: Springer-Verlag

[15] Y. Wang, 2005. "Efficient Identity-Based and Authenticated Key Agreement Protocol". [Online]. Available: http://eprint.iacr.org

[16] J. H. Park, M. Kim, and D. Kwon, 2013. Security weakness in the smart grid key distribution proposed by Xia and Wang, IEEE Trans. Smart Grid

[17] S. Finster, 2013. Smart meter speed dating, short-term relationships for improved privacy in smart metering, in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Vancouver, BC, Canada, pp. 426431

[18] D. Wu and C. Zhou, 2011. Fault-tolerant and scalable key management for smart grid, IEEE Trans. Smart Grid

[19] Recommendation for Key Management, Part 1: General, NIST Standard SP 800-57, 2007

[20] J. L. Tsai, N. W. Lo, and T. C. Wu, Novel anonymous authentication scheme using smart cards, IEEE Trans. Ind. Informat., vol. 9, no. 4, pp. 20042013, Nov. 2013

[21] J. Xia and Y. Wang, 2012. Secure key distribution for the smart grid, IEEE Trans. Smart Grid

[22] D. Boneh and M. K. Franklin, 2001. Identity-based encryption from the Weil pairing, in Proc. CRYPTO, Santa Barbara, CA, USA

[23] A. Shamir, 1984. Identity-based cryptosystems and signature schemes, in Proc. Adv. Cryptol. (CRYPTO), Santa Barbara, CA, USA

[24] V. Miller, 1985. Use of elliptic curves in cryptography, in Proc. Adv. Cryptol. (CRYPTO), Santa Barbara, CA, USA

[25] N. Koblitz, 1987. Elliptic curve cryptosystems, Math. Comput.

[26] J. L. Tsai, 2014. An improved cross-layer privacy-preserving authentication in WAVE-enabled VANETs, IEEE Commun. Lett.

[27] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. (Jun. 1999). X.509 Internet Public Key Infrastructure Online Certificate Status ProtocolOCSP. [Online]. Available: http://www.ietf.org/rfc/rfc2560.txt