Journal of Electrotechnology, Electrical Engineering and Management (2023) **DOI: 10.23977/jeeem.2023.060108**
Clausius Scientific Press, Canada **ISSN 2560-6697 Vol. 6 Num. 1**

An Efficient Certificateless Aggregate Signcryption Scheme in V2G

Baoyi Wang[a,*], Ronghua Yi[b], Shaomin Zhang[c]

School of Control and Computer Engineering, North China Electric Power University, Baoding, Hebei, 071003, China
[a]wangbaoyi@126.com, [b]aspiring_yironghua@163.com, [c]zhangshaomin@126.com
[*]Corresponding author

Keywords: V2G, Electric vehicle, Certificateless aggregate signcryption

Abstract: When EVs are charging and discharging or enjoying other services, it is crucial to protect the communication data between electric vehicles and charging service control centers. Guaranteed confidentiality and y-verification of information, and it takes a long time to verify when a large number of EV users are signing confidentiality at the same time. For those problems. We proposes a certificate-free aggregated signcryption scheme for V2G based on the assumption of Diffie-Hellman difficulty problem. A bilinear mapping operation is used to add the identity information of EV users and charging service companies into the signature and ciphertext respectively to hide the user identity information. In the aggregation verification phase, only two fixed bilinear mapping operations are used, which can effectively improve the computational efficiency.

1. Introduction

V2G (Vehicle-to-Grid) technology combines EV (Electric Vehicle) and smart grid, V2G has a great contribution in "peak and valley reduction" to relieve the load of the grid, but then there is a problem of privacy of the user or the vehicle information leakage [1]. Once the information is leaked, it will bring some trouble to the users, such as the attacker gets the information about the location, then it can easily get other sensitive information about the user by tracking and monitoring the EV user; it can also infer the EV user's electricity consumption habit based on the battery status; it can even determine the vehicle's activity range through the vehicle power information at different times, and advance to measure the EV The vehicle's power information at different times of the day can even be used to determine the vehicle's range of activity and advance to the EV user's daily life path. These security risks will cause EV users to be on the fence about V2G services [2]. As the number of EVs rises, their impact on the power system is increasing. In order to effectively mitigate the fluctuations caused by EVs entering the grid, charging service control centers need to adjust tariffs according to the real-time electricity consumption of EVs, and the energy interaction between various entities inevitably generates a huge amount of information data, which puts a huge pressure on the network. Therefore, a lightweight privacy protection scheme for V2G networks needs to be designed to improve the security of energy transactions in V2G networks and protect the private data of electric vehicle users [3].

Many researchers are working on convergent signing algorithms and information protection schemes for electric vehicle users in V2G networks. Saxena et al. designed a new network security and privacy protection architecture to support V2G networks based on a bilinear pairing technique to improve authentication efficiency through a bulk authentication protocol and to ensure forward privacy and identity anonymity of vehicles [4].Chen et al. proposed a blockchain-based ring-signature privacy protection method that uses ring-signature technology to guarantee the anonymity of vehicle users in the service process, as well as the authenticity and integrity of data transmission and the fairness of transactions, guaranteeing the anonymity, confidentiality, and integrity of user transaction data [5].LIU et al. propose a certificate-free aggregated signature scheme that uses only public parameters and Zhang et al. applied aggregated signatures and encryption to fully anonymous blockchain in the Bitcoin blockchain system [6-7].Wang et al. proposed a related scheme of aggregated signatures and encryption whose performance meets the requirements of in-vehicle systems, but there is a large room for improvement in computing efficiency [8]. He et al. used blockchain to implement the incentive for EVs in V2G, using anonymous addresses as the receiving address of the incentive, taking into account the privacy of EVs and aggregators[9] .Zhao et al. proposed a CLASC scheme, which uses a bilinear mapping operation with higher operational efficiency but lower security[10]. Niu et al. applied multi-recipient signatures to a heterogeneous cryptosystem to design an aggregated signatures algorithm in a heterogeneous environment, which allows secure communication between multiple senders and multiple receivers, effectively improving the efficiency of the communication system, and for receivers, preventing the disclosure of user information of legitimate receivers to unauthorized users by applying Lagrange interpolation formulas. Although satisfying the need for privacy protection, there are security issues [11].

For these problems, we proposes a certificateless aggregate signcryption scheme for V2G networks. In the certificateless cryptographic environment, the bilinear mapping operation is used to hide the real-time charging data of EV users in the signcryption, which ensures the security and efficiency of the signcryption.

2. Related technology

2.1. Difficult problems related to elliptic curves

(1) Elliptic curve discrete logarithm problem

For a given group G of order large prime q and a generating element of that group is P, Hard to answer for any element $a \in Z_q^*$ in a finite field with known $aP \in G$ and P.

(2) Computational Diffie-Hellman problem

For a given group G of order large prime q and a generating element of this group is P, Hard to answer $abP \in G$ for any element $a, b \in Z_q^*$ in a finite field with known $aP, bP \in G$ with P.

2.2. Bilinear mapping

The bilinear mapping addition and multiplication cycle groups are denoted as G_1 and G_2, respectively, and the orders are all prime q. P denotes the generating element of G_1.

1) Bilinearity: For any $Q \in \mathrm{G}_1$, there exist $a, b \in Z_q^*$ such that $e(aP, bQ) = e(P, Q)ab$.

2) $e(P, P) \neq 1$.

3) $e(Q, R)$ is computable for any $Q, R \in \mathrm{G}_1$.

3. Detailed construction and design of the Scheme

3.1. Scheme Introduction

There are five main phases including initialization, key generation, EV user signcryption, DA aggregated signcryption and CSCC decryption. KGC initializes the system and generates key pairs for each registered user. After the EV user establishes wireless communication with the charging pile device using the cell phone for authentication, the charging pile will provide charging/discharging service for the EV and monitor the real-time charging data of the EV (such as battery status, load data, motor parameters and metering and billing data, etc.). The EV user will sign the real-time charging data and send it to the Data Aggregator (DA) via the charging pile, which will aggregate the received signatures and send them to the CSCC for decryption.

3.2. Scheme model

According to the V2G architecture, an architecture diagram of real-time data aggregation and signing for EV charging consisting of EV, charging pile, data aggregator, key production center, and charging service control center is constructed. As shown in Figure 1.

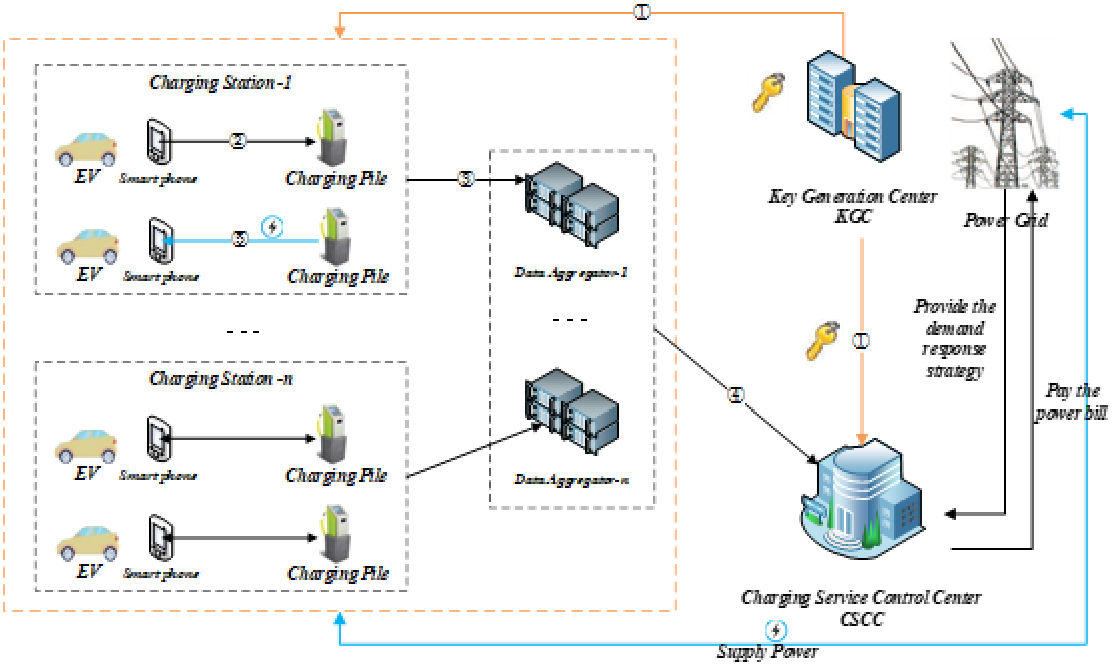

Figure 1: Scheme structure of this paper

CP: Charging pile not only provides charging services, but also communicates wirelessly with the cell phones of electric vehicle users. It monitors the data of the service process and sends the real-time charging data of EVs to the data aggregator while the EVs are charging/discharging.

EV: When EV is connected to CP, EV user can sign and encrypt its charging real-time data and public key and send it to CP.

DA: Data Aggregator aggregates the signcryption data generated during EV power transactions within a charging station and sends that aggregated sign-off to CSCC.

KGC: The Key Generation Center, as a secure trusted third party, can initialize the system parameters and generate keys for the parties in the system.

CSCC: The charging service control center decrypts and verifies the aggregated signcryption data from the data aggregator, adjusts the tariff in real time according to the users' electricity consumption, and plays a macro-regulatory role in the stability of the grid. It also regulates the charging piles in the market.

3.3. Scheme implementation process

The program implementation process is shown below.

① KGC performs system initialization and calculates partial keys for EV users and charging service control center.

② The EV user signs the real-time charging data and the public key, and sends the signatures to the data aggregator via the charging pile in the charging station.

③ The data aggregator aggregates the signatures within a station and sends them to the charging service control center.

④ The charging service control center verifies the aggregated signature data and decrypts it to obtain real-time EV charging data.

⑤ The charging post continues to provide charging service for electric vehicles.

4. Scheme implementation

4.1. Key generation phase

In this paper, we set the security parameter as k and generate large prime numbers $p, q(q|p-1)$. The $(G_1,+)$ and $(G_2,\cdot)$ cyclic groups, both of order q, and P is a generating element of G_1. The bilinear mapping $e:(G_1 \cdot G_2) \to G_2$ and the three secure hash functions are $H_1:\{0,1\}^* \to G_1, H_2:\{0,1\}^* \times \{0,1\}^* \times G_1 \to G_2, H_3:\{0,1\}^* \to \{0,1\}^{lm}$ (lm denotes the message bit length).

1) System initialization. The system is initialized by KGC, $\theta \in Z_q^*$ is randomly selected as the system master key and kept secret, $P_{pub} = \theta P$ is computed, and the public system parameters $par = \{G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3\}$.

2) Generate partial private key. KGC calculates $Q_i = H_1(u_i)$, $D_i = \theta Q_i$, and transmit D_i and D_c to EV user u_i and charging service controller u_c respectively through secure channel.

3) Generate user private key. EV user private key is generated by EV user participation and verify the equation $e\left(Q_i, P_{pub}\right) = e(D_i, P)$, if the equation holds, it means that part of the private key is legitimate. EV user u_i randomly selects the secret value $x_i \in Z_q^*$ and generates user private key pair $sk_i = (x_i, D_i)$. Where the private key of CSCC $sk_c = (x_c, D_c)$ is generated in the same way.

4) Generate user public key. EV user calculate public key $pk_i = x_i P$. Where the CSCC public key $pk_c = x_c P$ is generated in the same way.

4.2. Electric vehicle users to Signcryption

EV user u_i signcryption its charging real-time data m_i and sends it to the CP. the signcryption process is as follows.

1) EV user u_i randomly selects $r_i \in Z_q^*, R_i = r_i P, U_i = r_i Q_i$.

2) Electric vehicle user u_i is calculated to obtain:

$$Q_c = H_1(u_c)$$

$$a_i = e\left(Q_c, r_i P_{pub}\right),$$

$$T_i = H_3(u_c, a_i, R_i, pk_c, r_i pk_c);$$

$$c_i = (m_i||u_i) \oplus T_i;$$
$$h_i = H_2(c_i||U_i||u_c);$$
$$v_i = (r_i + h_i)(x_i Q_i + D_i);$$

3) EV user u_i computes the ciphertext σ_i and sends it to DA via CP.

$$\sigma_i = (R_i, U_i, c_i, v_i)$$

4.3. Data Aggregator to Aggregate signcryption

The data aggregator DA collects ciphertexts of EVs in a charging station at a fixed time t_j and aggregates them.

1) DA receives all the ciphertexts $\sigma_i\ (0 \leq i \leq n)$ in the charging station and calculates $V = \sum_{i=1}^{n} v_i$.

2) DA outputs the aggregated ciphertext σ and sends it to CSCC, where $time$ is the time stamp.

$$\sigma = \langle (R_i, U_i, c_i)_{i=1}^{n}, V, time \rangle$$

4.4. Charging service control center for decryption

There are 4 main steps as follows.

1) Charging service control center u_c calculation

$$a_i' = e(D_c, R_i);$$
$$T_i' = H_3(u_c, a_i', R_i, pk_c, x_c R_i);$$
$$m_i||u_i = c_i \oplus T_i';$$
$$Q_i = H_1(u_i);$$
$$h_i = H_2(c_i||U_i||u_c);$$

2) Verify whether the equation $e(V, P) = e\left(\sum_{i=1}^{n}(U_i + h_i Q_i), P_{pub} + \sum_{i=1}^{n} pk_i\right)$ holds, if it does, prove that σ is valid and output $m_i (0 \leq i \leq n)$, otherwise prove that the signature is invalid and output ⊥.

5. Security of the scheme

The security analysis of the scheme in this paper includes key correctness, ciphertext recoverability and legitimacy of the sending user.

5.1. Key Correctness Analysis

The EV user key consists of part of the private key of KGC and the secret value in the hands of the user. To ensure the reliability of the key passed from KGC, the correctness of the key passed from KGC is verified by the equation $e\left(Q_i, P_{pub}\right) = e(Q_i, \theta P) = e(\theta Q_i, P) = e(D_i, P)$.

5.2. Ciphertext recoverability and legitimacy of sending user

Since $m_i||u_i = c_i \oplus T_i' = c_i \oplus T_i$, $T_i' = H_3(u_c, a_i', R_i, pk_c, x_c pk_c)$, it is necessary to prove that $T_i' = T_i$ and $a_i' = a_i$ to prove the correctness of the plaintext message m_i as follows:

$$a_i' = e(D_c, R_i) = e(\theta Q_c, r_i P) = e(r_i P_{pub}, Q_c) = a_i$$

$$\begin{aligned} T_i' &= H_3(u_c, a_i', R_i, pk_c, x_c R_i) \\ &= H_3(u_c, a_i', R_i, pk_c, x_c r_i P) \\ &= H_3(u_c, a_i', R_i, pk_c, pk_c r_i) \\ &= T_i \end{aligned}$$

The plaintext message m_i is obtained by $m_i||u_i = c_i \oplus T_i' = c_i \oplus T_i$, verifying the recoverability of the ciphertext, and verifying the legitimacy of the sender's identity by verifying whether the equation $e(V,P) = e\left(\sum_{i=1}^{n}(U_i + h_i Q_i)\,, P_{pub} + \sum_{i=1}^{n} pk_i\right)$ holds. Ensure that the received plaintext is valid, and ensure the correctness of the whole signed secret.

Because

$$\begin{aligned} e(v_i, P) &= e\big((r_i + h_i)(x_i Q_i + D_i), P\big) \\ &= e(r_i x_i Q_i + r_i D_i + h_i x_i Q_i + h_i D_i, P) \\ &= e(U_i + h_i Q_i, pk_i) e(r_i \theta Q_i + h_i \theta Q_i, P) \\ &= e(U_i + h_i Q_i, pk_i) e\big(U_i + h_i Q_i, P_{pub}\big) \\ &= e\big(U_i + h_i Q_i, P_{pub} + pk_i\big) \end{aligned}$$

So

$$\begin{aligned} e(V,P) &= e\left(\sum_{i=1}^{n} v_i\,, P\right) = e\left(\sum_{i=1}^{n}(r_i + h_i)(x_i Q_i + D_i)\,, P\right) \\ &= e\left(\sum_{i=1}^{n}(r_i + h_i) x_i Q_i\,, P\right) e\left(\sum_{i=1}^{n}(r_i + h_i)\theta Q_i\,, P\right) \\ &= e\left(\sum_{i=1}^{n}(U_i + h_i Q_i)\,, \sum_{i=1}^{n} pk_i\right) e\left(\sum_{i=1}^{n}(U_i + h_i Q_i)\,, P_{pub}\right) \\ &= e\left(\sum_{i=1}^{n}(U_i + h_i Q_i)\,, P_{pub} + \sum_{i=1}^{n} pk_i\right) \end{aligned}$$

5.3. Public verifiability of the scheme

Public verifiability means that the private information of the communicating parties is not involved in the process of computing the verification equation, and any third party can verify the validity of the signed secret by computing the verification equation. The verification equation of the scheme in this paper is $e(V,P) = e\left(\sum_{i=1}^{n}(U_i + h_i Q_i)\,, P_{pub} + \sum_{i=1}^{n} pk_i\right)$, which does not contain the secret information of EV users and charging service control center and satisfies the public verifiability.

6. Conclusion

In order to address the privacy security problem of electric vehicles when charging/discharging, this paper proposes a certificate free aggregated signature scheme based on bilinear mapping. The scheme protects the real-time charging data of electric vehicles while having less number of bilinear mapping operations, with higher operational efficiency and lower operational cost.

References

[1] Zhong W, Yu R, Xie S, Zhang Y, Yau DKY. On stability and robustness of demand response in V2G mobile energy networks. IEEE Trans Smart Grid 2018; 9(4): 3203–12.
[2] Li H, Han D, Tang M. A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing. IEEE Syst J 2021; 15(3):3189–200.
[3] Danish SM, Zhang K, Jacobsen H-A, Ashraf N, Qureshi HK. BlockEV: Efficient and secure charging station selection for electric vehicles. IEEE Trans Intell Transp Syst 2021; 22(7):4194–211.
[4] Saxena N, Choi B J. Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks[J].IEEE Transactions on information Forensics and Security, 2016, 11(7):1438-1452.
[5] Fuan Chen, Yi Liu. Blockchain-based V2G ring-signature privacy protection scheme without certificate [J]. Computer Engineering, Pages: 1-10, FEB 2023. https://doi.org/10.19678/j.issn.1000-3428.0065767.
[6] Liu C L, You L. A certificateless aggregate signature scheme [J]. Journal of Hangzhou Dianzi University (Natural Sciences), 2019, 39(6):12-17.
[7] Wang Z Y, Liu J W, Zhang Z Y, et al. Full anonymous blockchain based on aggregate signature and confidential transaction[J]. Journal of Computer Research and Development, 2018, 55(10):2185-2198.
[8] Wang Y J, Ding Y, Wu Q H, et al. Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(7):1779- 1790.
[9] Wang H, Wang Q, He D, et al. BBARS: Blockchain-based anonymous rewarding. Scheme for V2G networks [J].IEEE internet of Things Journal, 2019, 6(2):3676-3687.
[10] Liu J H, Zhao C X, Mao K F. Efficient certificateless aggregate signcryption scheme based on XOR [J]. Computer Engineering and Applications, 2016, 52(12): 131-135.
[11] Niu S F, Niu L, Wang C F, et al. Privacy-preserving multi-recipient aggregate signcryption for heterogeneous cryptography systems[J]. Computer Engineering & Science, 2018, 40(5):805-812.