Computing, Performance and Communication Systems (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/cpcs.2023.070102
ISSN 2371-8889 Vol. 7 Num. 1

A Certificateless Multi-Receiver Broadcast Signcryption Scheme for Demand Response

Shaomin Zhang[a,*], Jiajia Chang[b], Baoyi Wang[c]

School of Control and Computer Engineering, North China Electric Power University, Baoding, Hebei, 071003, China
[a]zhangshaomin@126.com, [b]changjiajia2022@163.com, [c]wangbaoyi@126.com
[*]Corresponding author

Keywords: Broadcast signcryption, privacy protection, demand response, smart home

Abstract: Under demand response, the power control centre needs to send some confidential information to smart home users in a timely manner. If the information is sent to each user individually, high communication costs will be incurred. Moreover, with the increasing number of users and services, frequent information interaction brings enormous pressure to the power communication system. To effectively solve this problem, a certificateless multi-receiver broadcast signcryption scheme for demand response is proposed. The Lagrange polynomial theorem is used to encrypt different messages, so that the control centre can send different demand response signals to different smart home users through a broadcast message, while ensuring the unforgeability of sending confidential messages. Experiments show that this scheme has lower computation cost.

1. Introduction

With the decline of distributed renewable energy system technology costs and the promotion of national energy policies, microgrids are considered to be an effective solution to reduce environmental impact and investment costs [1]. However, because of the instability of renewable energy and the sharp increase in household electricity consumption, there is a huge difference in peak and valley electricity consumption [2]. To effectively solve this problem, integrated demand response in the smart home has been a hot topic. Through the flexible management of various smart electrical devices to achieve the goal of "peak and valley reduction" as well as shifting the load to lower-priced periods to save household electricity costs [3].

Smart homes change their electricity consumption patterns in the form of demand response, rationally arrange household electrical equipment, and effectively alleviating the power supply tension of the power system [4]. However, with the increasing number of users and services, frequent information interaction brings enormous pressure to the power communication system [5]. Especially under demand response, the power control centre (CC) needs to send specific confidential messages to each smart home user in a timely manner. Encrypting different data separately would be time consuming and computationally expensive if traditional methods are used [6,[7]. To transmit these messages efficiently and securely, multi-recipient encryption schemes for secure communication have been proposed by researchers [8]. However, there are still some problems in some published articles that have not been resolved in microgrids.

Scheme [9] proposes a certificateless multi-receiver data transfer protocol, it can effectively reduce communication cost. And when the same secret message is sent to a group of recipients, only the authorized group of recipients can obtain confidential information from broadcast messages, and other users cannot obtain any useful information. The multi-receiver signcryption scheme proposed by schemes [10[12] can prevent broadcast messages from being leaked and guarantee the anonymity of the recipient's identity, but these schemes cannot send multiple different confidential information to different users in one broadcast data report. To improve the flexibility of the scheme, the scheme designed in literature [13] allows the sender to encrypt different messages for different recipients.

In addition, due to limited resources and the increasing number of smart meters, broadcast encryption schemes must be more secure and efficient. To further improve the computational efficiency, the scheme proposed in [14] outsources part of the receiver's authentication overhead to the gateway without exposing the user's privacy, but in the scheme, there is still a key escrow problem. The scheme proposed in literature [15] based on anonymous authentication can solve the key escrow. The Lagrangian interpolation theorem is introduced in [16] to encrypt n different messages into one ciphertext with lower computational cost.

In summary, to address the security issue of sending demand response control commands by broadcast in microgrids, a broadcast signcryption scheme for demand response is proposed, which can send different demand response signals to different smart home users through one broadcast message and effectively improve the transmission efficiency. Finally, the efficacy of the proposed scheme are presented through performance analysis.

2. Scheme Design

2.1. Design Ideas

In order to ensure the confidentiality, integrity and unforgeability of the commands sent by the control centre, and to guarantee the anonymity of the smart meters receiving the commands, a broadcast signcryption scheme is proposed. In the scheme, the control centre (CC) encrypts the demand response signals sent to different SMs based on polynomial theorem, and when a broadcast message is received, it can be decrypted only by the meter private key, and other users cannot get any information.

2.2. Scheme Model

The main participants involved in the proposed multi-receiver broadcast signcryption scheme are as follows: smart home, home energy management system (HEMS), smart meters (SMs), gateway (GW), CC and key generation centre (KGC), as shown in Figure 1.

KGC: Responsible for system initialization and generating system public parameters. KGC generates part of the private key for the meters and the control centre when they register.

CC: Based on electricity demand and supply, the generated demand response signal is sent to each meter.

SMs: Verify and decrypt the obtained broadcast messages and send them to the HEMS of the smart home.

HEMS: The power dispatching is done according to the demand response signal sent by the meter, which can reduce the cost of electricity for customers and achieve the purpose of "peak and valley reduction" at the same time.

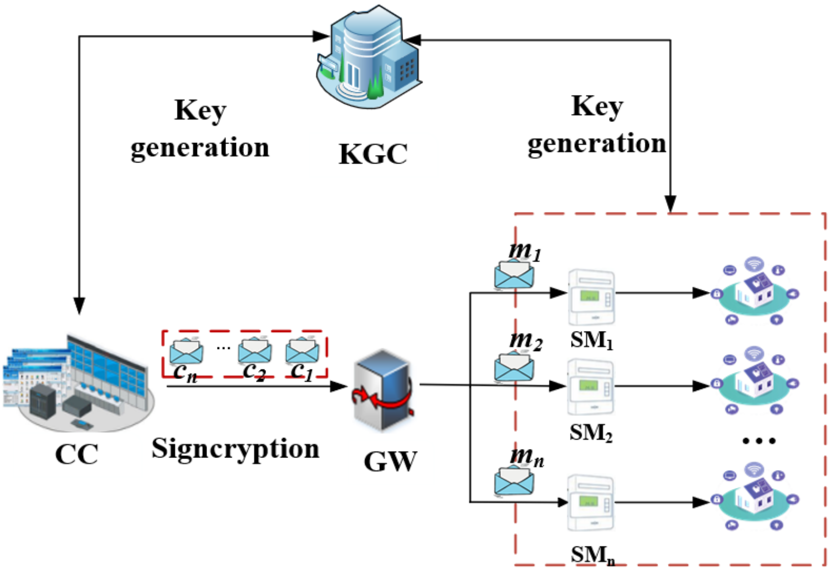

Figure 1: Data transmission architecture diagram.

2.3. Scheme implementation process

① KGC generates the system public parameters $Params$. SM$_i$ generate its own public and private keys based on the $Params$, and registers with KGC. KGC receives the registration request and uses the system master key $s \in \mathrm{Z}_\mathrm{q}^*$ to generate part of the public and private keys for it.

② The CC generates a specific demand response signal for each smart home user and sends it via a broadcast message to the GW, which is forwarded by the gateway to the SMs.

③ The SMs verify the legitimacy of the message from the CC broadcast $\sigma = \{U, L, V\}$, if it is trustworthy, receive it and forward it to the HEMS.

3. Scheme Implementation

3.1. System Initialization

KGC is responsible for the system initialization process and performs the following processes:

1) KGC selects a cyclic group G of order large prime number q, $P \in G$ is a generator of G, and selects hash function$H_1: \{0,1\}^* \times G^3 \to Z_q^*$, $H_2: \{0,1\}^* \times G^2 \to Z_q^*$, $\mathrm{H}_3: G \times \{0,1\}^* \times Z_q^* \times \{0,1\}^* \times \{0,1\}^{l2} \to \mathrm{Z}_\mathrm{q}^*$.

2) KGC selects a random number $s \in \mathrm{Z}_\mathrm{q}^*$ as the main private key, then computes the corresponding public key $P_{Pub} = sP \in G$.

3) Finally, KGC publishes the system security parameter $Params = \{q, G, P, P_{Pub}, H_1, H_2, H_3\}$.

3.2. Registration

SM$_i$ Registration:

1) SM$_i$ randomly selects $x_i \in Z_q^*$, and computes the partial public key $X_i = x_iP$. The report $\{id_i, X_i\}$ is sent to the KGC.

2) KGC selects a random number $r_i \in Z_q^*$ and computes:

$$R_i = r_iP\,,\, y_i = r_i + sH_1(id_i, X_i, R_i, P_{Pub}) \qquad (1)$$

Then the response report $\{R_i, y_i\}$ is sent to CC through the secure channel.

3) After SM$_i$ receives the report, it computes $h_i = H_1(id_i, X_i, R_i, P_{Pub})$ and verifies $y_i P = R_i + h_i P_{Pub}$, if the equation is true, SM$_i$ obtain private keys$s_i = x_i + y_i$ and public key $P_i = \{X_i, R_i\}$.

CC's registration process is similar, private key $s_{CC} = x_{CC} + y_{CC}$ (where $y_{CC} = r_{CC} + sH_1(id_{CC}, X_{CC}, R_{CC}, P_{Pub})$) and public key $P_{CC} = (X_{CC}, R_{CC})$ (where $X_{CC} = x_{CC}P$, $R_{CC} = r_{CC}P$ $(x_{CC}, r_{CC} \in Z_q^*)$) are stored.

3.3. Signcryption

At this stage, the power control centre sends different confidential messages to multiple meters through broadcasting, and any meter that is not in the broadcast message list will not be able to obtain any information, and the meters that receive the message will not be able to obtain any information about other users, ensuring their confidentiality. Suppose the list of meters that need to receive messages is: $ID = \{id_1, id_2, \cdots, id_n\}$, and the message sent to each meter is set to $m_i = \{0,1\}^{l1}$.

1) CC selects $u \in Z_q^*$ and computes $U = uP$.

2) CC uses the public keys of all receiving meters to compute h_i and Q_i, as follows:

$$h_i = H_1(id_i, X_i, R_i, P_{Pub}), Q_i = u(X_i + R_i + h_i P_{Pub}), \text{ where } i = 1, 2, \cdots, n. \quad (2)$$

3) CC randomly selects $\omega = \{0,1\}^{l2}$ and computes $\alpha_i = H_2(id_i, U, Q_i)$, $c_i = m_i \| \omega$.

4) CC computes the polynomial function $f(x)$, and obtains a set of coefficients $L = \{g_0, g_1, \cdots, g_{n-1}\}$.

$$f(x) = \frac{(x-\alpha_2)\cdots(x-\alpha_n)}{(\alpha_1-\alpha_2)\cdots(\alpha_1-\alpha_n)} c_1 + \cdots + \frac{(x-\alpha_1)\cdots(x-\alpha_{n-1})}{(\alpha_n-\alpha_2)\cdots(\alpha_n-\alpha_{n-1})} c_n = g_{n-1}x^{n-1} + \cdots + g_1 x + g_0 (mod\ p) \quad (3)$$

5) CC computes $h = H_3(U, L, \omega)$, $V = s_{CC} + uh$ and sends the report $\sigma = \{U, L, V\}$ to SMs via GW.

3.4. Unsigncryption

After receiving the broadcast report $\sigma = \{U, L, V\}$, SM_i perform the following actions:

1) SM_i computes $Q_i' = s_i U$, $\alpha_i' = H_2(id_i, U, Q_i')$. Then calculate $c_i = f(\alpha_i')$ to obtain m_i and ω.

2) Compute $h = H_3(U, L, \omega)$ and $h_{CC} = H_1(id_{CC}, X_{CC}, R_{CC}, P_{Pub})$.

3) Verify whether the equation $V \cdot P = X_{CC} + R_{CC} + P_{Pub} \cdot h_{CC} + U \cdot h$ is valid, if it is, then receive m_i. Otherwise reject.

3.5. Power Dispatch

The SMs transmit the received demand response signals to the HEMS. HEMS is responsible for scheduling the entire household equipment, shifting the load within a selected time frame to level the load curve and achieve the goal of "peak and valley reduction". And the HEMS can shift the load to the low-cost hours to save the household electricity bill. Additionally, smart home users equipped with electric vehicles (EVs) can also reduce the charging cost by managing the charging and discharging time. The EVs can be charged in low-price hours; then, the surplus stored electricity can be released into the microgrid to obtain reasonable profits when the electricity prices seem high.

4. Scheme Analysis

This part will compare the computation costs of our scheme with four related schemes [10], [11], [12] and [15]. The well-known MIRACL library [17] is used to quantify the Time cost of referring cryptographic operations. The scheme based on bilinear pairing selects the A-type supersingular elliptic curve (SS512 curve) and Tate pairing, and uses the standard elliptic curve secp160r1 for ECC [18]. Table 1 shows the average elapsed time for 10000 executions corresponding to different cryptographic operations, the time overhead of other operations is small and can be ignored.

Table 1: Time cost of referring cryptographic operations.

Symbol	Description	Time (ms)
T_p	Time of bilinear paring	11.21
T_{map}	Time of map to point hash function	0.061
T_m	Time of multiplication in group	0.013
T_e	Time of exponentiation in group	1.153
$T_{m_{ecc}}$	Time of scale multiplication operation in ECC	1.702

According to the time cost in Table 1, the computation cost of signcryption and unsigncryption under different schemes is computed respectively. The Table 2 shows that the computation cost of the proposed scheme is smaller.

Table 2: Comparisons of the computation costs.

Reference	Signcryption	Unsigncryption
[10]	$T_p + (n+1)T_{m_{ecc}} + T_e + 2T_{map}$ $= 1.702n + 12.187ms$	$T_p + T_{map} = 11.271ms$
[11]	$(2n+1)T_{m_{ecc}} = 3.404n + 1.702ms$	$4T_{m_{ecc}} = 6.808ms$
[12]	$(n+1)T_p + (n+2)T_{m_{ecc}} + 2T_e + nT_{map}$ $= 12.973n + 16.92ms$	$3T_p + (n+3)T_{m_{ecc}} + T_e$ $= 1.702n + 38.889ms$
[15]	$(2n+1)T_{m_{ecc}} = 3.404n + 1.702ms$	$5T_{m_{ecc}} = 8.51ms$
Our scheme	$(2n+1)T_{m_{ecc}} = 3.404n + 1.702ms$	$4T_{m_{ecc}} = 6.808ms$

5. Conclusions

To transmit confidential demand response signals efficiently, a multi-receiver broadcast signcryption scheme for demand response is proposed. The process of sending different messages to multiple SMs in a broadcast report by the control centre based on Lagrange polynomial theorem is described in detail. And the anonymity of the identity of the smart meter receiving the command can be guaranteed. Moreover, the computational overheads of the signcryption and unsigncryption processes of this scheme and several other schemes are compared respectively.

References

[1] Z. Wang, M. Sun, C. Gao, X. Wang, and B. C. Ampimah, "A new interactive real-time pricing mechanism of demand response based on an evaluation model," Applied Energy, vol. 295, p. 117052, 2021.

[2] Y. Ma, X. Chen, L. Wang, and J. Yang, "Investigation of Smart Home Energy Management System for Demand Response Application," Frontiers in Energy Research, vol. 9, p. 772027, 2021.

[3] B. Yu, F. Sun, C. Chen, G. Fu, and L. Hu, "Power demand response in the context of smart home application," Energy, vol. 240, p. 122774, 2022.

[4] G. Hafeez et al., "Efficient energy management of IoT-enabled smart homes under price-based demand response program in smart grid," Sensors, vol. 20, no. 11, p. 3155, 2020.

[5] J. Yao, Z. Li, Y. Li, J. Bai, and P. Lin, "Transmission Strategy of GOOSE Service based on Cellular Multimedia Broadcasting in Smart Grid," in 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC), 2019.

[6] Q. Li and G. Cao, "Multicast authentication in the smart grid with one-time signature," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 686-696, 2011.

[7] Z. M. Fadlullah, N. Kato, R. Lu, X. Shen, and Y. Nozaki, "Toward secure targeted broadcast in smart grid," IEEE Communications Magazine, vol. 50, no. 5, pp. 150-156, 2012.

[8] S. Maiti and S. Misra, "P2B: Privacy preserving identity-based broadcast proxy re-encryption," IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 5610-5617, 2020.

[9] J. Shen, Z. Gui, X. Chen, J. Zhang, and Y. Xiang, "Lightweight and certificateless multi-receiver secure data transmission protocol for wireless body area networks," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1464-1475, 2020.

[10] S. Niu, L. Fang, M. Song, F. Yu, and S. Han, "An ID-based Broadcast Encryption Scheme for Cloud-network Integration in Smart Grid," KSII Transactions on Internet and Information Systems (TIIS), vol. 15, no. 9, pp. 3365-3383, 2021.

[11] X. Yu, W. Zhao, and D. Tang, "Efficient and provably secure multi-receiver signcryption scheme using implicit certificate in edge computing," Journal of Systems Architecture, vol. 126, p. 102457, 2022.

[12] J. Zhang and P. Ou, "Privacy-preserving multi-receiver certificateless broadcast encryption scheme with de-duplication," Sensors, vol. 19, no. 15, p. 3370, 2019.

[13] C. Peng, J. Chen, M. S. Obaidat, P. Vijayakumar, and D. He, "Efficient and provably secure multireceiver signcryption scheme for multicast communication in edge computing," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6056-6068, 2019.

[14] J. Qiu, K. Fan, K. Zhang, Q. Pan, H. Li, and Y. Yang, "An efficient multi-message and multi-receiver signcryption scheme for heterogeneous smart mobile IoT," IEEE Access, vol. 7, pp. 180205-180217, 2019.

[15] Y. Ming, X. Yu, and X. Shen, "Efficient anonymous certificate-based multi-message and multi-receiver signcryption scheme for healthcare internet of things," IEEE Access, vol. 8, pp. 153561-153576, 2020.

[16] L. Deng, "Anonymous aggregate encryption scheme for industrial Internet of Things," IEEE Systems Journal, vol. 14, no. 3, pp. 3999-4006, 2019.

[17] Shamus Software, "Multiprecision integer and rationalarithmetic cryptographic library (MIRACL), " 2021, http://www.certivox.com/miracl/.

[18] M. Qu, "Sec 2: Recommended elliptic curve domain parameters,"Certicom Res., Mississauga, ON, Canada, Tech. Rep. SEC2-V er-0.6, 1999.