Journal of Network Computing and Applications (2019) 4: 7-13
Clausius Scientific Press, Canada
DOI: 10.23977/jnca.2019.41002
EISSN 2371-9214

A Privacy Preserving Scheme for Incentive-Based Demand Response in Smart Grid

Shaomin Zhang[a,*], Kai Wang[b] , Baoyi Wang[c]

School of Control and Computer Engineering, North China Electric Power University, China
[a]zhangshaomin@126.com, [b]wangkaibule@sina.com, [c]wangbaoyiqj@126.com
**corresponding author*

Keywords: Data Privacy, Incentive-Based Demand Response, Smart Grid.

Abstract: The Incentive-Base Demand Response (IDR) programs in the smart grid provides the ability to shape the power demand on the demand side, which ensures better stablility than in the traditional power grid. However, the IDR programs require the customer's fine-grained power consumption data to be collected, which poses a serious threat to customer privacy. A IDR privacy preserving scheme is proposed in this paper which utilises a descent off-line electronic coin scheme for the extraction and redemption of rewards and has less computational costs than currently know IDR privacy preserving schemes.

1. Introduction

The research results from the smart grid have gradually been used in the practice of electricity production. One of them is the technique of smart meter, which has been adapted by many countries in replace with the traditional electromechanical meters. It is proven that smart meters have great advantages, such as the ability of remote meter reading collection and high metering precision with fine granularity. These advantages enable the instant communication between demand side and the power supplier and also the possibility for the electricity market to benefit from Demand Response (DR).

According to the U.S. Department of Energy, DR refers to "changes in electric use by demand-side resources from their normal consumption patterns in response to the varying electricity price, or to incentive payments designed to reduce electricity use when wholesale market prices are high or when system reliability is jeopardized" [1]. Unlike the other kinds of energy, the generation and consumption of the electricity power needs to be balanced instantaneously. In the traditional power grid, the common method to keep the grid stable during the peak hour is to increase the power supply from the power plant, which may involve a high cost. However, the smart grid has the ability to shape the power consumption of demand side by utilizing demand response, so the smart grid is more economic and even more reliable. There are two general types of DR programs. The first one is price-based demand response (PDR) which triggers demand side's response by adjusting the electricity price. Another is incentive-based demand response (IDR), which reward the customers who cut down their electricity consumption during an IDR program. Unlike the PDR, which has been used in the way such as "tier price" or "Time-of-Usage", the IDR currently has not been

widely applied. However, there's research shows it is the IDR that will contribute the major benefit that DR programs can provide{Goldman 2010 #3}. However, the IDR programs require for high resolution power consumption data, the granularity of which varies from one hour per measurement to several seconds. The collection of high resolution consumption data becomes a serious threat to customer privacy, due to the existence of Non-intrusive Appliance Load Monitoring (NALM) techniques[2,3]. Research in [4] shows a customer's daily pattern can be revealed by analyzing the consumption data with granularity of 15 min.

To address the privacy problem, Efthymiou et al. introduced the privacy preserving method in [5]. In this method, the fine-grained consumption data is stored in a pseudonym account and separated from customer's real identity. At the same time, the coarse data, like the monthly consumption, will still be sent to the power supplier with real identity for billing purpose. Gong et al. proposed a privacy preserving scheme for IDR programs in paper [6], their method is based on Efthymiou's idea which stores customer's fine-grained data in a pseudonym account.

In this paper, a new IDR privacy preserving scheme is proposed, which has a better computational performance than the one proposed in [6]. And also, the new scheme uses a decent off-line coin system for the implementation of reward extraction and redemption, so the new scheme will not suffer from the quasi-identifier attacks like [6] does.

The remaining of this paper is structured as follow: The basic cryptographic technologies used in this scheme are introduced in Section 2. The system model is illustrated in Section 3 and the detailed construction of the scheme is described in Section 4. Finally, conclusions are made in Section 5.

2. Related Techniques

2.1. Schnorr Signature

The Schnorr Signature [7][8] is designed to conduct digital signature task on devices with limited computation power. The algorithm can be represented as a tuple:$(\mathrm{Init}, \mathrm{KeyGen}, \mathrm{Sign}, \mathrm{Verify})$.

2.2. Identity-based Signature

In an identity-based signature[9], the signer's public key is the signer's public identity, so no extra cost for generating the public key for the signer. The identity-base signature can be represented by a tuple $(\mathrm{Init}, \mathrm{IBSKeyGen}, \mathrm{IBSSign}, \mathrm{IBSVerify})$

2.3. Off-line Electronic Coin

In paper [11], Brands proposed an off-line coin scheme. In this scheme, Brands describes a electronic coin which allows to be used as electronic money to conduct a trade. However, the most important feature of this scheme is the buyer's real identity cannot be deduced from the coin. In this paper, the off-line coin scheme is used as rewards from the electricity market given to the customer whoever responses during an IDR program.

3. System Model

The system model is illustrated in Figure 1. When an IDR program is necessary, the electricity market will send a signal to the demand response provider (DRP). A DRP is the communication bridge between the electricity market and customers. During an IDR program, the DRP will monitor the fine-grained data from customers' pseudonym accounts and compare real consumption to the

customer's consumption pattern. If the customer indeed has reduced his power consumption during an IDR program comparing with his consumption pattern, then the DRP will give the customer some rewards according to the contribution the customer has made. The rewards will be stored in the pseudonym accounts as the fine-grained consumption data.

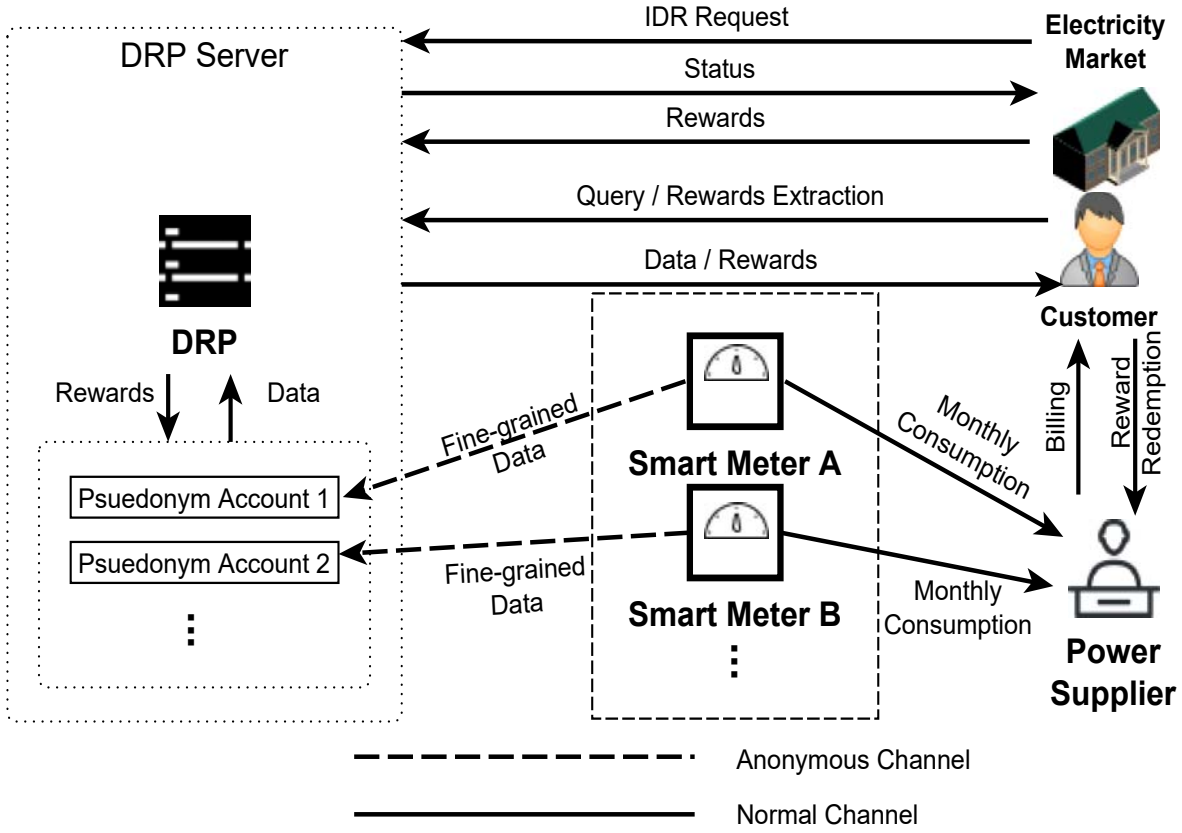

Figure 1: The System Model.

4. The Design of the Privacy Preserving Scheme

4.1. Initialization of System Parameters

The DRP and power supplier will initialize the system parameter together. They first choose 5 prime numbers $(p, q_1, q_2, q_3, q_4, q_5)$ which satisfy $p = 1 + 2\prod_{i=1}^{5} q_i$ and create a multiplicative group $\mathbb{Z}_p^*$ and 5 subgroups of this group: $\mathbb{G}_{q_i} \leq \mathbb{Z}_p^*, i \in [0,5]$. The group generator $(g_1, g_2, g_3, g_4, g_5, g_6, g_7)$ satisfies $g_1 \in \mathbb{G}_{q_1}; g_2 \in \mathbb{G}_{q_2}; g_3 \in \mathbb{G}_{q_3}; g_4, g_5, g_6 \in \mathbb{G}_{q_4}; g_7 \in \mathbb{G}_{q_5}$. These groups will be used in different procedure in the proposed scheme. Then then construct hash function: $\mathcal{H}_{\text{sign}}: \{0,1\}^* \times \mathbb{G}_q \to \mathbb{G}_q$ for Schnorr Signature and $\mathcal{H}_{\text{ibs}}: \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_q \to \mathbb{G}_q$ for identity-based signature. Hash functions $\mathcal{H}_{\text{coin1}}: \mathbb{G}_{q_4} \times \mathbb{G}_{q_4} \times \mathbb{G}_{q_4} \times \mathbb{G}_{q_4} \times \mathbb{G}_{q_4} \to \mathbb{G}_{q_4}$ and $\mathcal{H}_{\text{coin2}}: \mathbb{G}_{q_4} \times \{0,1\}^* \times \{0,1\}^*$ will be used in the extraction and redemption of rewards. These hash functions are assumed to be collision resistent, which means it is hard to find two different inputs which result in the same output. Also the output of these hash functions looks to be random in the view of adversaries who don't know the secret key of these hash functions. Finally, the DRP and power supplier also generates secret keys for different operations: ibs_msk $\in \mathbb{G}_{q_1}$ is used to generate the identity-based signature key for customer's real identity, sm_ibs_msk $\in \mathbb{G}_{q_5}$, sm_ibs_msk $\in \mathbb{G}_{q_5}$, sm_sk $\in \mathbb{G}_{q_2}$, ibs_pmsk $\in \mathbb{G}_{q_3}$, coin_sk $\in \mathbb{G}_{q_4}$.

4.2. Customer Registration

A customer send his real identity REAL_ID and the unique identitification code from his smart meter SM_ID to the power suplier. The power supplier computes and send back to the customer his identity-based signature key pair: $(\text{PK\_IBS}, \text{SK\_IBS}) = \text{IBSKeyGen}(\mathbb{G}_{q_1}, \text{ibs\_msk}, ID)$ as well as the signature key pair for his smart meter:$(\text{PK\_SM\_IBS}, \text{SK\_SM\_IBS}) = \text{IBSKeyGen}(\mathbb{G}_{q_5}, \text{sm\_ibs\_msk}, \text{SM\_ID})$. Also the power supplier will sign on the SM_ID : $\text{SM\_SIGN} = (\text{SM\_Sig}, \text{SM\_SID}, \text{SM\_Nonce}) = (s, e, g_2^r) = \text{Sign}(\text{sm\_sk}, \text{SM\_ID})$, in which $\text{SM\_Sig} = r - ex$, $r \in_R \mathbb{Z}_{q_2}$, $x = \text{sm\_sk}$, $e = \mathcal{H}_{\text{sign}}(\text{SM\_ID}, g_2^r)$. The customer send SM_SIGN and the signature key pair $(\text{PK\_SM\_IBS}, \text{SK\_SM\_IBS})$ into his smart meter. The process is illustrated by Figure 2.

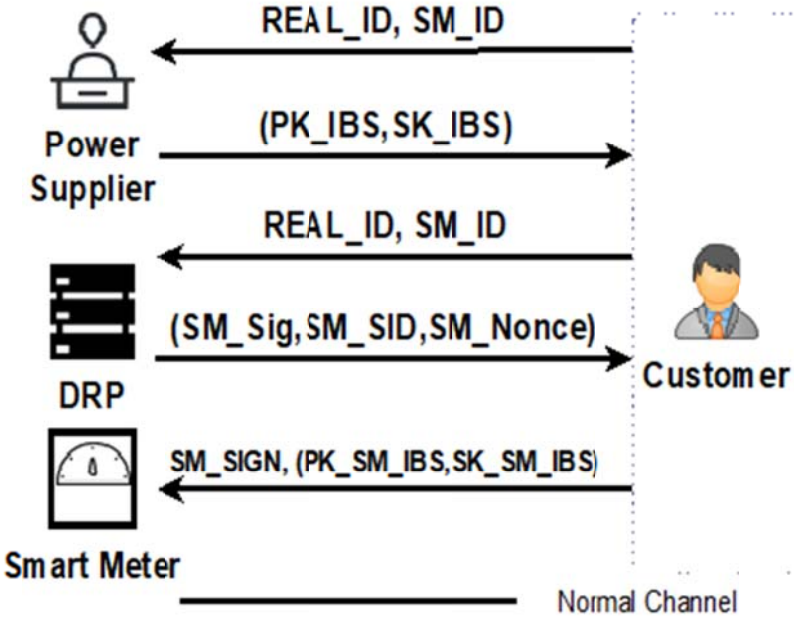

Figure 2: Customer Registration Process.

4.3. Pseudonym Account Registrartion (Through Anonymous Channel)

After a random delay after registering the real identity. The customer computes a Pedersen commitment $u = g_2^{e+k'}, e = \text{SM\_SID}, k' \in_R \mathbb{G}_{q_2}$ and $\gamma_1 = g_2^{r_1}, \gamma_2 = g_2^{r_2}, \gamma_3 = g_2^{r_3}$, in which $r_1, r_2, r_3 \in_R \mathbb{G}_{q_2}$ and anonymously request the DRP for a pseudonym account. The DRP verifies there's no previously existed record of u, then response to the customer with a random number $b \in_R \mathbb{Z}_{q_2}$. Customer then computes $s' = bs + r_3, y_1 = bk' + r_1, g^{y_2} = (g^k)^b g^{r_2}, s = \text{SM\_Sig}, g^k = \text{SM\_Nonce}$ and send (s', y_1, g^{y_2}) to the DRP. DRP continues to check $(\gamma_1)^x \gamma_2 g^{s'} u^{bx} \stackrel{?}{=} (g^{y_1})^x g^{y_2} \gamma_3, x = \text{sm\_sk}$. If the equation is satisfied, the DRP belives the validity of customer's identity, then stores u into database. The value of u can be used to refer to the registered pseudonym account in the further communication and is denoted as $\text{PSEUDO\_ID} = u$. Finally, the DRP provide a signature pair $(\text{PKP\_IBS}, \text{SKP\_IBS}) = \text{IBSKeyGen}(\mathbb{G}_{q_3}, \text{ibs\_pmsk}, \text{PSEUDO\_ID}||DT)$, in which PSEUDO_ID||DT denotes the text string of PSEUDO_ID concatenate with a public random string chosen by the DRP. The process is illustrated by Figure 3.

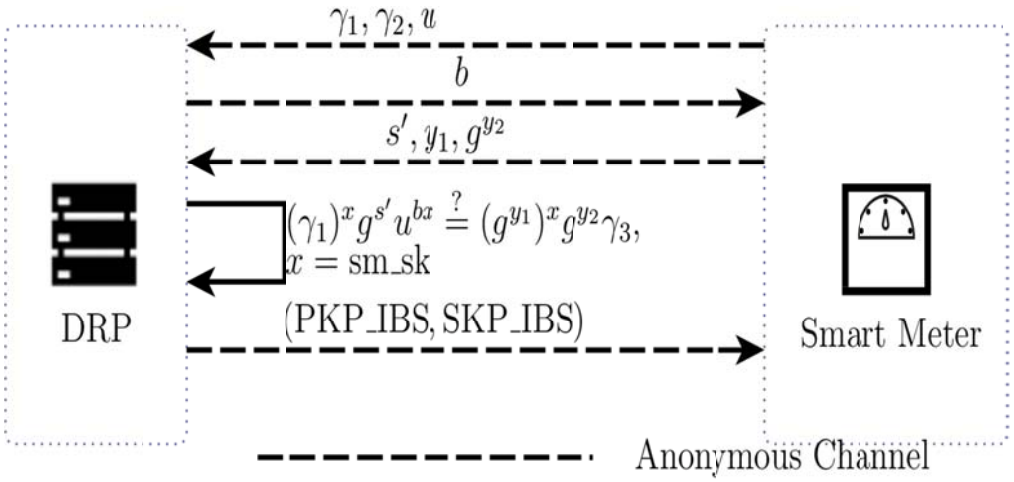

Figure 3: Pseudonym Registration Process.

The theorem below ensures the pseudonym account is unlinkable to the customer's real identity, and the possibility that a pseudonym has already been taken is negligible:

Theorem 1: The commitment $u = g_2^{e+k\prime}$ perfectly hides the value of e, and the possibility that there exists $(e', k''), e' \neq e$ is negligible.

And the Theorem 2 ensures an illegal customer cannot register a pseudonym account:

Theorem 2: If a customer does not posses a legal signature SM_SIGN, then the possibility for him to successfully register a pseudonym account is negligible.

4.4. Sending Metering Data

The smart meter will anonymously send to the DRP the high resolution consumption data m along with the signature generated by using the key SKP_IBS : $s = \text{IBSSign}(\text{PSEUDO\_ID}||\text{TD}, m, \mathbb{G}_{q_3})$. Also the smart meter will send the value of monthly consumption D to the power supplier, along with the signature generated by using the key SK_SM_IBS: $\delta = \text{IBSSign}(\text{SM\_SID}, D, \mathbb{G}_{q_1})$.

4.5. Query and Manage Pseudonym Account (Through Anonymous Channel)

By sign the query or management command with the key SKP_IBS, the customer can anonymously proof his ownership on his pseudonym account. In this way, the customer can query the consumption data stored in pseudonym account, extract the rewards or delete the pseudonym when the customer doesn't want to participate future IDR programs any more.

4.6. Extract Rewards from Pseudonym Accounts (Through Anonymous Channel)

To benefit from the rewards obtained by participating IDR programs, a customer needs to extract rewards from his pseudonym accounts first. The customer query his pseudonym account and send the reward extraction command. Then the following procedure is conducted to extract rewards:

1) Letting a random number $x = \text{coin\_sk}$ and $I = g_5^e$, $e = \text{SM\_SID}$. The customer uses the public key (g_4^x, g_5^x, g_6^x) announced by DRP to calculate $z = (Ig_6)^x = (g_5^x)^e g_6^x$. Then send I, z along with the request to extract rewards,

2) The DRP generate a tuple: $\{(a, b)|a = g_4^w, b = (Ig_6)^w, w \in_R \mathbb{Z}_{q_4}\}$ and send it to customer,

3) The customer calculates $\{(A, B, z')|A = (Ig_6)^s, B = g_5^{x_1} g_6^{x_2}, z' = z^s, s, x_1, x_2 \in_R \mathbb{Z}_{q_4}\}$ and s

should never be used and $A \neq 1$. Then the customer calculates $\{(a' = a^u g_4^v, b' = b^{su} A^v) | u, v \in_R \mathbb{Z}_{q_4}\}$ and $c' = \mathcal{H}_{\text{coin1}}(A, B, z', a', b')$, send $c = c'/u$ to the DRP,

4) DRP calculates $r = cx + w$ and remove a reward from the pseudonym account.

5) The customer verifies $g_4^r \stackrel{?}{=} (g_4^x)^c a, (Ig_6)^r \stackrel{?}{=} z^c b$, and calculate $r' = ru + v$. The reward now has been extracted from the account and has a signature $\delta = (z', a', b', r')$. The tuple (A, B, δ) is a reward that is available to be redeemed.

4.7. Rewards Redemption

The customer communicate with the power supplier with his real identity, the power supplier now can charge the customer according to the monthly consumption sent by the smart meter. The customer can also present the extracted rewards to have them redeemed. To redeem a reward, the power supplier calculates $d = \mathcal{H}_{coin2}(r, \text{BD\_ID}, \text{DT}), r \in_R \mathbb{Z}_{q_4}$, in which BD_ID is the identification number of this power supplier and DT is a public random number chosen by the power supplier. Then the following procedure is conducted:

1) The customer present the reward to be redeemed: $(A, B, (z', a', b', r'))$,

2) The power supplier verifies $g_4^{r'} \stackrel{?}{=} (lg_4^x)^{\mathcal{H}_{\text{coin1}}(A,B,z',a',b')} a'$ and $A^{r'} \stackrel{?}{=} z^{\mathcal{H}_{\text{coin1}}(A,B,z',a',b')} b'$, then send d to the customer,

3) The customer calculates $(r_1, r_2) = (esd + x_1, sd + x_2), A = (Ig_6)^s, I = g_5^e, B = g_5^{x_1} g_5^{x_2} g_6^{x_3}$, in which $e = \text{SM\_SID}$

4) The power supplier verifies $A^d B \stackrel{?}{=} g_5^{r_1} g_6^{r_2}$, if the equation is satisfied, and there's no previous record of A in the database, the reward redemption is successful.

Theorem 4: There doesn't exist $A^d B \stackrel{?}{=} g_5^{r_1} g_6^{r_2}$, which satisfies $(g_5^{u_1} g_6)^s = (g_5^{u_2} g_6)^x, u_1 \neq u_2$.

If the power supplier has found a previous record of A, this means the customer is redeeming the same reward twice. To find out which customer has cheated, the power supplier use the information of (r_1, r_2) from previous redemption request, as well as the information (r_1', r_2') from this time, and calculate $(r_1 - r'_1)/(r_2 - r'_2)$, the value of which will be the value of SM_SID that belongs to the cheating customer.

5. Conclusion

A new privacy preserving scheme suitable for Incentive-Base Demand Response (IDR) is proposed in this paper. The new scheme preserves customer privacy by storing customer's fine-grained consumption data into a pseudonym account, so the Non-intrusive Appliance Load Monitoring technique cannot be used to violate customer's privacy. The new scheme also has considered all basic operations involved in an IDR program, including meter data transmitting, rewards extraction and redemption.

References

[1] Qdr, Q. (2006) Benefits of demand response in electricity markets and recommendations for achieving them. US Dept Energy, Washington, DC, USA, Tech Rep,

[2] Hart, G.W. (1992) Nonintrusive appliance load monitoring. Proceedings of the IEEE, 80, 1870–91.

[3] Huang, T.D., Wang, W.-S. and Lian, K.-L. (2015) A new power signature for nonintrusive appliance load monitoring. IEEE Transactions on Smart Grid, 6, 1994–5.

[4] Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E. and Irwin, D. (2010) Private memoirs of a smart meter. Proceedings of the 2Nd Acm Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, ACM, New York, NY, USA. pp. 61–6. https://doi.org/10.1145/1878431.1878446

[5] Efthymiou, C. and Kalogridis, G. (2010) Smart grid privacy via anonymization of smart metering data. First Ieee International Conference on Smart Grid Communications, pp. 238–43.
[6] Gong, Y., Cai, Y., Guo, Y. and Fang, Y. (2016) A privacy-preserving scheme for incentive-based demand response in the smart grid. IEEE Transactions on Smart Grid, 7, 1304–13.
[7] Koblitz, N. and Menezes, A.J. (2015) The random oracle model: A twenty-year retrospective. Designs, Codes and Cryptography, 77, 587–610.
[8] Schnorr, C.-P. (1991) Efficient signature generation by smart cards. Journal of Cryptology, 4, 161–74.
[9] Galindo, D. and Garcia, F.D. (2009) A schnorr-like lightweight identity-based signature scheme. International Conference on Cryptology in Africa, pp. 135–48.
[10] Pedersen, T.P. (1991) Non-interactive and information-theoretic secure verifiable secret sharing. Annual International Cryptology Conference, pp. 129–40.
[11] Brands, S. (1993) Untraceable off-line cash in wallet with observers. Annual International Cryptology Conference, pp. 302–18.