# IAA: Incentive-based Anonymous Authentication Scheme in Smart Grids

Zhiyuan Sui [*] Ammar Alyousef and Hermann de Meer

University of Passau, Innstr. 43, 94032 Passau, Germany
{suizhiyu, ammar.alyousef, demeer}@fim.uni-passau.de

**Abstract.** The traditional energy consumption calculation heavily relies on manual work, which is inefficient and error-prone. The Smart Grid, which integrates information and communication technologies into the electrical grid to gather information and manage energy production and consumption, may be a solution to this challenge. However, the resulting complex infrastructure and profusion of information may open up new attack vectors exploitable by malicious parties that could attack the grid itself or violate its consumers' privacy. In this paper, we indicate the increasing interests in providing conditionally anonymous authentication in the Smart Grid systems. While the consumption report stays anonymous, the consumers who voluntarily curtail their energy consumption, can confirm their curtailments in the scheme. Moreover, compared with the existing conditionally anonymous authentication schemes, our scheme is more efficient in computational and communication overhead for Smart Grid systems.

**Keywords:** Smart Grids, anonymous authentication, demand and response, privacy preservation, incentive.

## 1 Introduction

Smart Grid systems combine advanced communication and automated control technologies in order to increase flexibility and resilience of the infrastructure, save energy and reduce $CO_2$ emissions [1]. The integration of new technologies however leads to a completely new infrastructure, where the formerly isolated electrical grid, which is currently one of the most critical infrastructures, is blended with methods from Information and Communication Technologies (ICT). Households are equipped with intelligent smart meters and smart appliances and also the energy provider enhances its systems with new hardware and IP-based networking [2]. Smart meters measure energy consumption in a

[*] This work has received support by the EINS (FP7 NoE, grant no. 288021). The research leading to these results was supported by the "Bavarian State Ministry of Education, Science and the Arts" as part of the FORSEC research association. The first author is supported by the Chinese Scholarship Council.

much higher temporal resolution than conventional meters and send the gathered energy consumption data to the utility provider in order to achieve better monitoring, control and stability of the Smart Grid. At the power shortage time, the utility provider provides incentive payments to consumers for reducing their loads during reliability triggered events, but curtailment is voluntary. This new combination of energy network and ICT technology puts the security of the Smart Grid in question as it creates new ways to attack and tamper with the highly critical energy supply [3]. Two of the most challenging tasks are privacy and security. From an end user's point of view, the fine-granular energy consumption readings of a smart meter could be used to spy on and expose an user's activities at home. As shown in [4], the Smart Grids, which gather and analyze such information, lead to the large-scale creation of user profiles without a victim's consent or even his knowledge. This in turn could lead to personalized advertisements or discrimination against a user who is negatively classified according to his energy usage behavior. Therefore, the protection of a user's privacy is an essential necessity in the Smart Grid to achieve an adequate overall acceptance of this technology. On the other side, the security on the demand-response communication also needs to be ensured. As consumption data are transmitted through networks, the number of attack vectors vastly increased with the introduction of networked ICT in electrical meters. [5].

To find a technological approach that provides both privacy as well as security was a great research interest over the last couple of years. While there were many different approaches in this direction [6] [7], the reward distribution relies on the trusted third party so far. Once it is attacked, consumers' privacy will be leaked. In this paper, we design an anonymous authentication scheme for incentive-based demand response programs, named IAA. Specifically, the contributions of IAA are twofold.

1. Firstly, IAA can achieve strong anonymity and reward support. The electricity utility broadcasts the energy usage instruction to consumers and advises them to reduce their energy consumption by an acceptable percentage, when it finds an imbalance between the energy consumption and production. The willing consumers will revoke their anonymity and get their corresponding rewards, while no other party is able to identify the source of other consumers' usage data.
2. Secondly, compared with previous anonymous authentication schemes, which can provide similar security properties, for one thing, IAA is identity-based; for another, the computational and communication overhead is independent with the number of consumers in IAA. Therefore, it is more suitable for large group Smart Grid systems.

The remainder of this paper is structured as follows: Section 2 describes the works that employ crytosystems to achieve the security in Smart Grids up till now. In Section 3, the preliminaries, which are later on required in this paper, are explained in detail, while Section 4 explains our proposed scheme that features both anonymity and security. The security requirements are proved in Section

5. Section 6 compares the computational and communicational performance of our scheme with previous works. Section 7 concludes this paper.

## 2 Related Work

In order to achieve security in the Smart Grid systems, identity based signature schemes and anonymous authentication schemes are widely utilized.

Identity based signature (IBS) was introduced by Shamir [8]. The public key is generated from the user's identity in an IBS. IBS eliminates the overhead for checking the validity of the certificates. In reference [9], So et al. propose an IBS for Smart Grids, which does not require pre-device software setup from the users, and simplifies the key management mechanism. Nicanfar et al. [10] propose an efficient authentication and key management mechanism for Smart Grid communication. It prevents from various attacks while reducing the management overhead. Li et al. [11] integrate a homomorphic encryption algorithm and IBS to ensure the privacy and trustworthiness in Smart Grids. However, the key pairs are generated from a key generation server (KGS) in IBS. It assumes that the KGS is completely trustworthy.

Anonymous authentication schemes, e.g. group signatures and ring signatures, are also widely used in Smart Grids for privacy and security. In [12], He et al. employ the group signature to distribute the trustworthiness for the Smart Grid. Only the law authority can ask the information from electricity utility and group manager to revoke the anonymity of the target users. However, it assumes that the law authority is fully trustworthy. Chu et al. [13] construct an anonymous authentication to inquire the usage history records. This scheme cannot ensure the voluntary consumers, who curtail their consumption, can get their rewards. More than that, the computational cost and communication overhead are increasing with the number of the members in the ring signature. There are usually hundreds of smart meters in the Smart Grid system, while the computational resources of smart meter are limited.

In this paper, in conjunction with IBS, we construct an incentive-based anonymous authentication scheme to ensure the demand-response communication between the electricity utility and smart meters. Consumers are categorized according to their behavior. The consumers, who follow the electricity utility's instructions, can get their rewards, while others still stay anonymous. Compared with the previous schemes, on the one hand, IAA is third party free; on the other hand, it is more efficient in terms of the communicational and computational cost.

## 3 Preliminaries

We list several necessary notations and definitions for our work in this section.

### 3.1 Bilinear Map

In IAA, we employ the bilinear map to construct an anonymous authentication scheme. The bilinear map operation is based on elliptic curves. $\kappa$ is a random integer. Input $\kappa$, a prime number $p$ of size $\kappa$, is selected. $\mathbb{G}$ is a cyclic additive groups of order $p$. $\mathbb{G}_T$ is a multiplicative group of order $p$. $P$ is a generator of $\mathbb{G}$. A function $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is said to be a bilinear map if it satisfies the following properties:

1. **Bilinearity:** $e(aP, bP) = e(P, P)^{ab}$ for all $P \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p^*$.
2. **Non-degeneracy:** $e(P, P) \neq 1$.
3. **Computability:** $e(P, P)$ is efficiently computable, for all $P \in \mathbb{G}$.

### 3.2 Computational Assumptions

IAA is based on three computational assumptions

1. **Gap-Discrete Logarithm (Gap-DL) assumption** There is no probabilistic polynomial time (PPT) algorithm that can compute a number $x \in \mathbb{Z}_p^*$ from a tuple $(T, \mu)$, where, $\mu \leftarrow \mathbb{G}$ and $T = x\mu$.
2. **Decisional Diffie-Hellman (DDH) assumption** There is no PPT algorithm that can distinguish between a tuple $(\mu, x\mu, \mu', T)$ and a tuple $(\mu, x\mu, \mu', x\mu')$, where $\mu, \mu', T \leftarrow \mathbb{G}$ and $x \leftarrow \mathbb{Z}_p^*$.
3. $q-$**Strong Diffie-Hellman (**$q-$**SDH) assumption** There is no PPT algorithm that can compute a pair $(c, (1/(x + c))P)$, where $c \in \mathbb{Z}_p^*$, from a tuple $(P, xP, ..., x^qP)$, where $P \leftarrow \mathbb{G}$ and $x \leftarrow \mathbb{Z}_p^*$.

### 3.3 Zero Knowledge Proof

IAA extensively employs non-interactive zero knowledge proof (ZKP) protocol. ZKP is first proposed by Goldwasser et al. [14]. The purpose of ZKP, denoted as $\mathrm{PK}\{(x) : C = xP\}$, is to help a prover convince a verifier that he holds the knowledge $x$, without leaking any information about $x$ during the verification process. ZKP are widely utilized in digital authentication schemes, e. g. Schnorr Signature [15].

### 3.4 BBS+ Signature

BBS+ signature is initiated by Au et al. [16]. BBS+ signature is proved unforgeable without random oracles under $q-$ SDH assumption. It allows generation of a single signature for a message. Nguyen constructs an efficient knowledge proof of the signature and message without revealing any useful information about either [17].

### 3.5 Network Model

In our network model, we assume that the usage data is transmitted by the wide area network (WAN). The network model mainly consists of two entities: the electricity utility (EU) and the smart meter (SM). The communication between SMs and the EU is through wireless network technology. We assume that each EU communicates with multiple SMs in a concrete area, and the number of SMs is large enough for each SM to cloak its real identity.

The SM is the energy consumption reporting device present at each consumer's site. The SM reports consumers' energy usage report with the transformed credentials to the EU regularly. Therefore, no one can link the usage report to its source. In IAA, the cooperative consumer would like to curtail his consumption and prove his cooperation. Because each SM corresponds to a concrete consumer, we assume that the cooperative consumer can be confirmed via the real identity of the SM.

The EU is an infrastructure that is controlled by the electricity company and is in charge of the SMs in a concrete area. It collects and analyzes the usage data from SMs periodically, and broadcasts consumption related instructions to customers, according to the usage data. It is unnecessary for the EU to cloak its real identity. In our scheme, the EU's real identity is always considered public.

### 3.6 Security Requirements

In our anonymous authentication scheme, the main aim is to ensure trustworthiness of the data from both EU and SMs while ensuring the privacy of legitimate users habits. IAA can satisfy the following security requirements simultaneously:

1. The adversary is able to modify neither the consumption reports from SMs, nor the instruction from the EU (data integrity).
2. The EU can determine whether the signature derives from a legitimate source (identity authentication).
3. The consumer, who does not follow the instructions, cannot produce a valid signature to cheat out of rewards (reward-support).
4. The adversary cannot trace an uncooperative consumer's identity using the usage report (strong anonymity).

## 4 Proposed Scheme

IAA consists of the following procedures: setup algorithm, joining, anonymous report, demand generation and voluntary response protocols. In the setup algorithm, the EU generates its key pair and publishes its public key. During the joining procedure, each SM cloaks its secret key in the credential with Gap-DL assumption. And then, the EU authorizes the credential with BBS+ signature. Finally, the SM obtains a key pair authorized by the EU. After joining into the Smart Grid system, the SM reports its energy consumption data regularly (normally every 15 minutes). The SM transforms all its credentials, and proves its secret information to the EU by zero knowledge proof. Therefore, the EU can confirm whether the signature is from a legitimate SM without the SM's identity. The EU broadcasts the instructions with the signature to the SMs, once it finds that the energy consumption is too large to produce in the demand generation protocol. The consumer checks the timestamp and confirms that the signature is valid. During the voluntary response protocol, if the consumer would not like to cooperate, he just ignores the instruction, and his usage profile is still under anonymity; otherwise, he curtails the energy consumption and proves his curtailment with IBS during voluntary response.

### 4.1 Setup

The EU executes the setup algorithm to generate its long term key pair:

1. On input $\kappa$, the bilinear pairing instance generator returns a tuple $(p, \mathbb{G}, \mathbb{G}_T, e, P)$ as defined in Subsection 3.1.
2. Randomly choose three elements $Q, H, G \leftarrow \mathbb{G}$ and an integer $\gamma \leftarrow \mathbb{Z}_p^*$, hide its secret key in $P_{pub}$: $P_{pub} = \gamma P$.
3. Choose collision resistant hash functions $\mathcal{H}_1$: $\{0,1\}^* \rightarrow \mathbb{G}$; $\mathcal{H}_2 : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$.
4. Keep its secret key $\gamma$ and publish its public key $(P, Q, H, G, P_{pub})$ and hash functions ($\mathcal{H}_1$, $\mathcal{H}_2$).

### 4.2 Joining

The joining protocol is carried out between the EU and each SM. Each SM is equipped with a tamper-resistant black box [18]. Each black box has its key pair **(SK, PK)**. The EU has access to the public key **PK**. In additional, each black box would generate an internal private seed specific to itself. The seed is stored securely within the black box and is never disclosed or changed, as the black box is assumed to be tamper-resistant. Additionally, a secure public key signature scheme, including a signing algorithm **sig** and a verification algorithm **ver**, has been selected for a SM with key pair **(SK, PK)**. Each SM shows its real identity and produces its key pair during the following protocol: At first, the SM randomly generates an integer $x \leftarrow \mathbb{Z}_p^*$ as its secret key using its internal seed. Then, the SM computes a commitment $C$ on the value $x$: $C = xP$ and generates a signature $\sigma =$**sig**$(C \| \mathrm{ID})$. The SM sends $C \| \mathrm{ID}$ as well as its signature $\sigma$ to the EU. The commitment $C$ essentially binds the SM's secret key $x$. Upon receiving $C$, the EU executes the verification algorithm to check the validity of the signature using **PK**. If **ver**$(C \| \mathrm{ID}$, $\sigma$, **PK**$)$=valid, the EU computes the credential $\alpha = \mathcal{H}_2(ID)$, $S = \frac{1}{\gamma+\alpha}(C + Q)$ and sends $S$ to the SM. The SM confirms the correctness of the credential by checking equation $e(S, \alpha P + P_{pub}) = e(C + Q, P)$ holds. The SM's secret key is $x$, and its public key is $(C, S)$.

### 4.3 Anonymous Report

In order to achieve the almost real-time usage report, a SM and the EU can run the anonymous report protocol to produce a legitimate signature as following: Firstly, by using the knowledge of $x$, the SM binds the usage data $m$ and the timestamp $t$ with the element $T$. The SM computes $\mu = \mathcal{H}_1(m\|P\|P_{pub}\|G\|H\|Q\|t)$ and $T = x\mu$. The SM then proves $e(S, \alpha P + P_{pub}) = e(xP + Q, P)$ and $T = x\mu$ with the following non-interactive zero knowledge proof Equation 1:

$$\mathrm{PK}\left\{ \begin{pmatrix} S \\ x \\ \alpha \end{pmatrix} : \begin{array}{l} e(S, \alpha P + P_{pub}) = e(xP + Q, P) \\ T = x\mu \end{array} \right\} \tag{1}$$

The procedure of the proof is formally described below:

1. The SM randomly picks integers $r, k_0, k_1, k_2, k_3 \leftarrow \mathbb{Z}_p^*$.
2. In order to cloak its identity information, the SM transforms its original credential $S$ into a temporary one $U = S + rH$, where $r \in \mathbb{Z}_p^*$, and calculates $R = rG$, $M_1 = k_1 G$, $M_2 = k_2 G - k_3 R$, $N = k_0 \mu$, $V = e(P, P)^{k_0} e(H, P_{pub})^{k_1} e(H, P)^{k_2}$ $e(U, P)^{-k_3}$.
3. The SM calculates $g = \mathcal{H}_2(T\|R\|U\|M_1\|M_2\|N\|V\| \; m\|t)$, $s_0 = k_0 + gx$, $s_1 = k_1 + gr$, $s_2 = k_2 + gr\alpha$, $s_3 = k_3 + g\alpha$.

The SM can show that both the temporary credential and the element $T$ correspond to the same key pair $x$, $\alpha$ and $S$ without leaking any information of them. Given two signatures, it is impossible to determine whether they are produced by the same SM, or to identify the SM. Consequently, anonymity is achieved. In the end, the SM outputs $(T, R, U, g, s_0, s_1, s_2, s_3)$ as the signature.

After the receipt of the usage report, the EU checks the validity of the timestamp. Then, the EU executes the report reading algorithm to check whether the signature does prove the knowledge of a discrete logarithm $x$ as well as the knowledge of the valid credential $S$.

The EU computes the hash values $\mu = \mathcal{H}_1(m\|P\|P_{pub}\|G\|H\|Q\|t)$ and $M_1' = s_1 G - gR$, $M_2' = s_2 G - s_3 R$, $N' = s_0 \mu - gT$, $V' = e(P, P)^{s_0} e(H, P_{pub})^{s_1} e(U, P_{pub})^{-g}$ $e(Q, P)^{g} e(H, P)^{s_2} e(U, P)^{-s_3}$ , then confirms that equation $g = \mathcal{H}_2(T\|R\|U\|M_1'\|$ $M_2'\|N'\|V'\|m\|t)$ holds. If it holds, the EU accepts the usage report; otherwise, the EU rejects the usage report.

### 4.4 Demand Generation

Once the EU finds that the energy consumption is larger than production, it executes the instruction generation protocol to advise some consumers to shut down their appliances:

The EU first defines the instruction $(\lambda, t_n)$. The EU then employ Schnorr Signature to generate a valid signature to prove its identity: It randomly picks $k_4 \leftarrow \mathbb{Z}_p^*$, computes $W = k_4 P$, $f = \mathcal{H}_2(\lambda\|t_n\|W\|P\|P_{pub}\|t)$ and $s_4 = k_4 - f\gamma$. At last, the EU broadcasts the instructions and the signature $(\lambda, t_n, s_4, f, t)$ to all SMs.

Upon receiving the usage instructions, the SM checks whether the timestamp and the instruction are valid. It computes $W' = fP_{pub} + s_4P$ , checks whether $f = \mathcal{H}_2(\lambda\|t_n\|W'\|P\|P_{pub}\|t)$. If they hold, the SM informs the consumer to shut down his appliances; otherwise, it just rejects the instruction and signature.

### 4.5 Voluntary Response

After receiving the instruction, if the consumers would like to curtail their consumption by $\lambda$, they will execute the voluntary response protocol with the EU.

The SM should confirm that its current usage data $m$ and the usage data $m^*$ at the timestamp $t^*$ satisfy the demand. The SM transforms his usage data $m^*$ timestamp $t^*$ into a hash value $\mu$: $\mu = \mathcal{H}_1(m^*\|P\|P_{pub}\|G\|H\|Q\|\ t^*)$, and hides its secret information $x$ into element $T'$: $T' = x\mu$. The SM proves that it has the knowledge of $x$. The SM randomly picks $k_5 \leftarrow \mathbb{Z}_p^*$, and computes $A = (k_5P + Q, P)$, $B = k_5\mu$, $h = \mathcal{H}_2(m^*\|T'\|A\|B\|C\|P\|P_{pub}\|G\|H\|Q\|t^*)$, $s_5 = k_5 - hx$. The SM sends the proof $(m, h, s_5,$ ID) to the EU.

Upon receiving the proof, the EU confirms that the signature $\sigma^*$ and the curtailment proof $(m, T', h, s_5,$ ID) have the same secret information $x$. The EU computes $A' = e(S, \alpha P + P_{pub})e(s_5P + (h' - 1)C, P)$, $B' = s_5\mu + h'T'$ and $\alpha = \mathcal{H}_2(\text{ID})$. The EU checks whether $h' = \mathcal{H}_2(m^*\|T'\|A'\|B'\|C\|P\|P_{pub}\|G\|H\|Q\|t^*)$ and $T = T'$ hold. If they hold and $(m - m^*)/m > \lambda$, the EU determines that the consumer curtailed his energy consumption, then sends incentive payments to the consumer for his cooperation.

## 5 Security Analysis

In this section, we state the security analysis. The analysis is divided into four classes: data integrity, authentication, reward support and strong anonymity.

### 5.1 Data Integrity

The integrity includes the integrity of anonymous reports and integrity of instructions in our IAA scheme. When the SM sends the energy consumption data to the EU, it cloaks its credential $(x, \alpha, S)$, and proves the credential with zero knowledge proof. During the demand response part, the EU's consumption instruction is signed by a Schnorr short signature [15]. Since the Schnorr short signature is provably secure under the Gap-DL problem in the random oracle model, the integrity can be ensured. As the result, IAA can make sure the integrity of the anonymous report and the instruction.

### 5.2 Authentication

The authentication of the IAA scheme is based on the $q-$SDH assumption. During the joining protocol, each SM's credential $C$ is signed by the EU with the BBS+ signature. BBS+ signature has been proved against chosen plaintext attack under the $q-$SDH assumption in the standard model. According to the analysis of the integrity, the anonymous report protocol is secure. Therefore, the third party cannot produce a valid signature without the help of the EU.

### 5.3 Reward-support

The voluntary response protocol is a identity-based signature scheme that derives from zero knowledge proof. It implies that the adversary cannot tamper the public key $\alpha$, which is from the collusion resistant function $\mathcal{H}_{\mathrm{ID}}$. According to the analysis of integrity, the adversary cannot produce a valid but illegitimate usage report to frame a legitimate consumer under the security of the zero knowledge proof. Therefore, from above aspects, IAA can make sure that the voluntary consumer can get corresponding rewards.

### 5.4 Strong Anonymity

The consumer's anonymity is based on the DDH assumption in our IAA scheme. A SM generates its energy usage data using its secure key $x$. The essence of the anonymous report protocol is to shuffle the credential $(x, \alpha, S)$ to a temporary one $(T, R, U, g, s_0, s_1, s_2, s_3)$. After that, the SMs send their messages and signatures through an anonymous network. Because $\mathcal{H}_1$ is a collision resistant function, under the DDH assumption, it is infeasible to decide whether two elements $T$ and $T_0$ are generated using the same secret information $x$. As such, no one can trace the legitimate signature from an honest SM unless he knows the secret key. Hence, our IAA scheme satisfies the anonymity requirement.

## 6 Performance Analysis

In this section, we evaluate the computational cost and the communication overhead required by our IAA scheme, and compare it with some previous works.

**Table 1.** Computational performance

| | Party | Computational cost | Mean | Deviation | 95% confidential interval |
|---|---|---|---|---|---|
| Set up | EU | $4G_p + G_m$ | 37.48ms | 0.69ms | [37.15ms, 37.81ms] |
| Joining | EU | $G_m$ | 3.76ms | 0.32ms | [3.60ms, 3.91ms] |
| | SM | $2G_p + 2G_m$ | 18.74ms | 0.35ms | [18.57ms, 18.90ms] |
| Report | SM | $G_p + 3G_e + 8G_m$ | 31,00ms | 0.68ms | [30.68ms, 31.32ms] |
| | EU | $2G_p + 4G_e + 8G_m$ | 48.62ms | 0.74ms | [48.27ms, 48.98ms] |
| Demand | EU | $G_m$ | 3.35ms | 0.13ms | [3.29ms, 3.41ms] |
| | SM | $2G_m$ | 4.57ms | 0.10ms | [4.52ms, 4.62ms] |
| Response | SM | $G_p$+$2G_m$ | 12.58ms | 0.18ms | [12.50ms, 12.67ms] |
| | EU | $2G_p + 5G_m$ | 34.91ms | 0.75ms | [34.55ms, 35.26ms] |

### 6.1 Computational Cost

Firstly, we discuss the computational cost in our IAA scheme. Compared with exponentiation $G_e$, multiplication $G_m$ and pairing evaluations $G_p$, the overheads of hash evaluations and arithmetic operations are very small. We emulate the scheme IAA on a Ubuntu 12.04 virtual operation system with a Intel Core i5-4300 dual-core 2.60 GHz CPU. We only use one core and 1 GB of RAM. To achieve 80 bits security level, we set the length of $\mathbb{G}$ to 161 bits and $p$ to 160 bits. Some bilinear pairing operation can be calculated in advance. The computational costs and simulation results are presented in Table 1.

Secondly, we compare the Anonymous report's computational cost variation in terms of the number of SMs with conditionally anonymous ring signature (CRS) [19] and deniable ring signature (DRS) [20], which can also achieve similar security properties. The comparison is based on PBC cryptography libraries [21] and MIRACL libraries [22]. Fig. 1 shows the comparison result of compuational cost for an anonymous report between a SM and the EU. According to the figure, it can be seen that the computational cost is constant in IAA. Instead, the computational cost and the number of SMs are directly related in CRS and DRS.

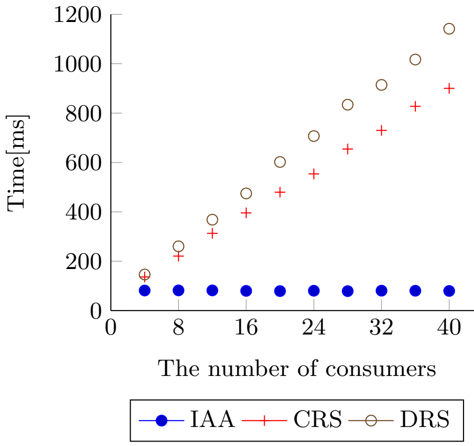

**Fig. 1.** Computational cost

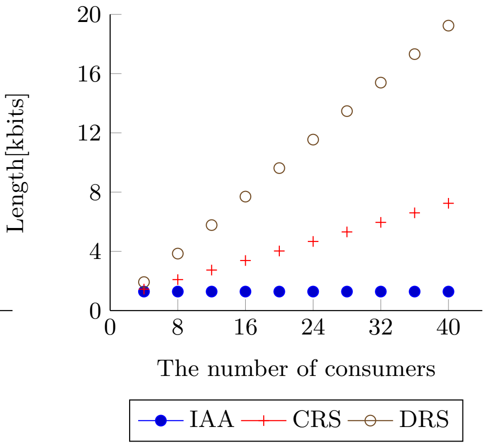

**Fig. 2.** Communication overhead

### 6.2 Communication overhead

In this subsection, we discuss the communication overhead between a SM and the EU. In the joining procedure, a SM sends a credential and its identity to the EU in form of $C\|\mathrm{ID}$, whose length is $\|\mathbb{G}\| + \|\mathrm{ID}\|$. During the anonymous report procedure, the EU reports the consumption data $m$ with the timestamp $t$ and signature $\sigma$, which is in form of $T\|R\|U\|g\|s_0\|s_1\|s_2\|s_3$. The size of $\sigma$ is $3\|\mathbb{G}\| + 5\|p\|$. In the Demand Generation protocol, the form of the signature is $f\|s_4$, whose size is $2\|p\|$. After the SM curtails the energy consumption, it sends the proof to the EU for asking the rewards. The form of the signature is $T'\|s_5\|h\|\mathrm{ID}$, whose size is $\|\mathbb{G}\| + 2p + \|\mathrm{ID}\|$. Here, we compare the signature size among IAA, CRS and DRS. The result is depicted in Fig. 2.

According to the Fig. 2, it can be seen that the communication complexity is $O(1)$ in our scheme. Compared with CRS and DRS, whose communication complexity is $O(q)$, where $q$ is the number of SMs in the system, the number of smart meters will not affect the communication cost in IAA.

According to our performance analysis, it can be seen that the communication and computational complexity is $O(1)$ in IAA, compared with the ring signatures [19] [20] that can also achieve our security requirements. In the both ring signature schemes, the authentication is based on the DL assumption. A SM must utilize other peer SM's public keys to cloak its identity. This requires that the SM calculates the signature for all SMs' public keys. The authentication of IAA is based on the $q-$SDH assumption. The SM produces its commitment. Then, the EU generates the credential to authorize the commitment. The anonymous report part employs the non-interactive zero knowledge proof to cloak the SM's credential. Therefore, the communication and computational cost is constant in IAA.

## 7 Conclusion

In this paper, we propose a novel incentive-based anonymous authentication scheme for demand-response management in Smart Grids. Our scheme guarantees the cooperative consumers can confirm their cooperation without harming the privacy of other consumers. The security analysis has demonstrated that our IAA scheme can achieve data integrity, identity authentication, reward support and anonymity simultaneously. According to the performance analysis, it can be seen our scheme has more advantage over the existing conditionally anonymous authentication schemes in terms of computation and communication overhead for Smart Grid systems. Therefore, we conclude our scheme solves the challenge of trading off between performance and security. However, the cooperative consumers have to revoke their anonymity to prove their curtailments. This leaks cooperative consumer's privacy at the power shortage time. For the future work, we will explore the new technologies to improve the IAA and provide the anonymous cooperation proof to the consumers.

## References

1. Litos Strategic Communication, *The Smart Grid: An Introduction*, Tech. rep., U.S. Department of Energy, pp. 7, 1419, 22 (2008).
2. A. Yarali and S. Rahman, *Smart grid networks: Promises and challenges*, Journal of Communications 7 (2012) 409417.
3. C. Eckert, C. Krau and P. Schoo, *Sicherheit im Smart Grid - Eckpunkte fuer ein Energieinformationsnetz*. Stiftung-Verbundkolleg/Projekt Newise Nr. 90 (2011).

4. C. Efthymiou and G. Kalogridis, *Smart grid privacy via anonymization of smart metering data.* First IEEE International Conference on Smart Grid Communications (SmartGrid-Comm), IEEE, 2010, 238243.
5. Z. Fan, G. Kalogridis, C. Efthymiou, M. Sooriyabandara, M. Serizawa and J. McGeehan, *The new frontier of communications research: smart grid and smart metering.* Proceedings of the 1st International Conference on Energy-Efficient Computing and Networking, ACM, 2010, 115118.
6. P. McDaniel and S. McLaughlin, *Security and privacy challenges in the smart grid.* Security & Privacy, IEEE 7 (3) (2009) 7577.
7. Y.-L. Lo, S.-C. Huang and C.-N. Lu, *Non-technical loss detection using smart distribution network measurement data.* Innovative Smart Grid Technologies - Asia (ISGT Asia), IEEE, 2012, 15.
8. A. Shamir, *Identity-based cryptosystems and signature schemes.* In Advances in cryptology, pp. 47-53. Springer Berlin Heidelberg, 1985.
9. So, Hayden K-H., Sammy HM Kwok, Edmund Y. Lam, and King-Shan Lui. *Zero-configuration identity-based signcryption scheme for smart grid.* , 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2010, 321-326..
10. Nicanfar, Hasen, Paria Jokar, Konstantin Beznosov, and Victor CM Leung. ”” (2013): 1-12. *Efficient authentication and key management mechanisms for smart grid communications.* IEEE Systems Journal, (6)2013: 1-12.
11. Li, Hongwei, Xiaohui Liang, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. *EDR: An efficient demand response scheme for achieving forward secrecy in smart grid.* IEEE Global Communications Conference (GLOBECOM), 2012, 929-934.
12. He, D., Chen, C., Bu, J., Chan, S., Zhang, Y. and Guizani, M. *Secure service provision in smart grid communications.* Communications Magazine, IEEE, 50(8),2012, 53-61.
13. Chu, Cheng-Kang and Liu, Joseph K and Wong, Jun Wen and Zhao, Yunlei and Zhou, Jianying, *Privacy-preserving smart metering with regional statistics and personal enquiry services*, Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, 2013, 369-380.
14. Goldwasser, Shafi, Silvio Micali, and Charles Rackoff. ”The knowledge complexity of interactive proof systems.” SIAM Journal on computing 18.1 (1989): 186-208.
15. C. Schnorr and P. Claus *Efficient signature generation by smart cards.* Journal of cryptology 4.3 (1991): 161-174.
16. Au, Man Ho, Willy Susilo, and Yi Mu. *Constant-size dynamic k-TAA.* Security and Cryptography for Networks. Springer Berlin Heidelberg, 2006. 111-125.
17. L, Nguyen and R. Safavi-Naini *Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings.* Advances in Cryptology-ASIACRYPT 2004. Springer Berlin Heidelberg, 2004. 372-386.
18. Chen, L., Ng, S. L. and Wang, G. (2011). *Threshold anonymous announcement in VANETs.* Selected Areas in Communications, IEEE Journal on, 29(3), 605-615.
19. Zeng, S., Jiang, S. and Qin, Z., *An efficient conditionally anonymous ring signature in the random oracle model*, Theoretical Computer Science 461, 2012: 106-114.
20. Komano, Y., Ohta, K., Shimbo, A. and Kawamura, S., *Toward the fair anonymous signatures: Deniable ring signatures*, In Topics in CryptologyCT-RSA 2006: 174-191.
21. B. Lynn, *PBC library*, http://crypto.stanford.edu/pbc/.
22. *Multiprecision integer and rational arithmetic c/c++ library*, http://www.shamus.ie/