Anonymous Data Collection Scheme from Short Group Signatures

Jan Hajny¹, Petr Dzurenda¹, Lukas Malina¹ and Sara Ricci²

¹Department of Telecommunications, Brno University of Technology, Technicka 12, Brno, Czech Republic
²Department of Mathematics and Computer Science, Universitat Rovira i Virgili, Avda. Paisos Catalans 26, Tarragona, Spain

Keywords: Group Signatures, Anonymity, Privacy, Revocation, Identification, Efficiency.

Abstract: Data collection schemes are used for secure and reliable data transfer from multiple remote nodes to a central unit. With the increasing importance of smart meters in energy distribution, smart house installations and various sensor networks, the need for secure data collection schemes becomes very urgent. Such schemes must provide standard security features, such as confidentiality and authenticity of transferred data, as well as novel features, such as the strong protection of user’s privacy and identification of malicious users. In this paper, we provide the full cryptographic specification of a novel scheme for secure privacy-friendly data collection that is designed for computationally restricted user devices and supports all the security, privacy-protection and inspection features. Using the scheme, data can be anonymously collected from almost all types of devices, including simple sensors and smart meters. On the other side, malicious users can be efficiently identified and revoked. Furthermore, we provide the practical results of our implementation of the scheme on embedded devices, smart phones, smart cards, smart watches, computers and servers so that the efficiency can be thoroughly evaluated on various platforms.

1 INTRODUCTION

Currently, there are proven cryptographic mechanisms that are able to guarantee the basic security properties in classical computer networks containing mostly PCs and servers. However, the structure of communication networks is changing in recent years and the infrastructures are becoming more and more heterogeneous, comprising industrial devices, small personal wearable devices, sensors, microcontrollers, etc. These devices are often very computationally constrained, which prevents the usage of standard cryptographic techniques for securing the communication. Lightweight cryptography mechanisms are being sought for the deployment on such devices. On the other side, the number of such personal devices is huge and quickly rising with the expansion of IoT networks, smart grids, cyber physical systems, etc. In some scenarios, millions of constrained devices communicate with one another and with central nodes. That is the case of sensor networks, in particular smart metering systems. In such applications, millions of relatively simple devices produce data that are collected by central nodes. Providing security in such environment is difficult, as the constrained devices are very limited in computational power and memory on one side and the central nodes must securely collect a very high number of messages from various sources on the other side.

In addition to the traditional requirements on confidentiality and authenticity, new demands on privacy protection are being imposed, mostly by EU regulations, but also by some U.S. strategic plans (NST, 2011). That leads to the design of technologies that limit any disclosure of private information that is not necessary for the system functionality. However, such privacy-enhancing features are often extremely costly regarding computational resources.

In this paper, we propose a cryptographic scheme based on group signatures that is designed to address the challenges identified above. Our anonymous data collection scheme allows constrained devices to efficiently generate group signatures on their data. Therefore, the collectors can be assured that data are collected from trusted sources and were not modified during a transfer. The signatures are fully anonymous, untraceable and unlinkable, thus supporting the full set of privacy-enhancing features. The collector learns that the signature was created by a trusted group member, but the concrete identity stays undisclosed. As an additional key feature, our scheme also provides efficient revocation, i.e., a practical mecha-
We present the full cryptographic description of all protocols of the scheme, show the efficiency analysis and the results of our implementation on devices with diverse computational power, from smart cards, microcontrollers to standard PCs. By showing also practical results, we prove the readiness of the scheme for a real-world use. Besides the straightforward use in data collection systems, we also note other applications, such as e-ticketing, transportation and e-IDs.

1.1 State of the Art

The work on anonymous data collection schemes became intensive only very recently, with the deployment of smart metering technologies into practical installations. However, the cryptographic primitives, that are the main building blocks of these schemes, are known for more than a decade. The core building blocks are the group signatures, allowing users to create signatures using their private keys and verifiers to verify the signatures using a common public key. The research into group signatures was started by the seminal work of Chaum and van Heyst in (Chaum and Van Heyst, 1991). A large number of group signatures has been proposed, e.g., in (Camenisch and Lysyanskaya, 2003; Boneh et al., 2004; Delerablée and Pointcheval, 2006; Hwang et al., 2011; Boneh and Shacham, 2004; Ferrara et al., 2009; Kim et al., 2011). In particular, the scheme called BBS (Boneh et al., 2004) serves as a fundamental building block for many security solutions (e.g., (Lin et al., 2007) and (Zhang et al., 2008)). Recently, short randomizable signatures were proposed (Pointcheval and Sanders, 2016) that allow efficient proofs of signature knowledge and creating group signatures by signing the individual users’ private keys by the manager’s private key. For the verification, only the manager’s public key is necessary. We take the same approach in our scheme.

Furthermore, some privacy preserving solutions based on pseudonyms have been proposed, e.g., in (Finster and Baumgart, 2013; Rottondi et al., 2015; Raya and Hubaux, 2007; Rottondi et al., 2015; Raya and Hubaux, 2007). However, the solutions based on pseudonyms are usually inefficient as they require users to switch between many (pseudo)identities, thus need expensive cryptographic material and multiple keys.

Both the group signature schemes and the pseudonymous schemes mostly lack efficient revocation mechanisms that are scalable enough for large applications with millions of constrained user devices. Either the revocation function needs very expensive computations (such as bilinear pairings) or is rather tailored for authentication and access control schemes (such as (Camenisch et al., 2016; Hajny and Malina, 2013)).

As a result, we lack a practical data collection scheme that is provably secure, with short and fast signatures, with efficient revocation mechanisms and providing all privacy-enhancing features.

1.2 Our Contribution

We propose a novel cryptographic scheme that we call an anonymous data collection scheme that is instantiated using the wBB signature (Boneh and Boyen, 2008) and the efficient proofs of their knowledge (Camenisch et al., 2016). On a general level, we take the approach of (Pointcheval and Sanders, 2016), i.e., we let the manager sign all users’ private keys. The users then prove the knowledge of such a signature and the verifier checks the proof using the manager’s public key. Our scheme is unique in the following properties:

- provides all privacy-enhancing features: anonymity, unlinkability, untraceability,
- the signatures are small and constant: the size is below 169 B using a strong 224 b curve,
- the signature generation is fast: requires no bilinear pairing and only 5 exponentiations,
- the signature verification including revocation check is efficient: requires only 2 pairings and \(O(|\RL|)\) exponentiations,
- the scheme is built using primitives with formal security proofs.

Besides the cryptographic design, we also provide the complete implementation results and benchmarks on a wide spectrum of devices, i.e. smart cards, micro-controllers and PCs. The practical results certify the usability in practice using contemporary cryptographic parameters recommended by NIST (Barker, 2016).

2 PRELIMINARIES

2.1 Notation

We describe the proof of knowledge protocols (PK) using the efficient notation introduced by Camenisch and Stadler (Camenisch and Stadler, 1997). The protocol for proving the knowledge of discrete logarithm

\(1\text{Revocation List}\)
2.4 Weak Boneh-Boyen Signature

The weak Boneh-Boyen (wBB) signature scheme (Boneh and Boyen, 2008) can be used to efficiently sign (blocks of) messages. Furthermore, the signature scheme can be easily integrated with the zero-knowledge proofs so that the knowledge of signed messages (and signatures themselves) can be proven anonymously, unlinkably and untraceably. We recall the signing and verification algorithms below, the efficient proofs of knowledge are described, e.g., in (Camenisch et al., 2016).

\[
\begin{align*}
\text{Setup:} & \quad \text{On input security parameter } k, \text{ generate a bilinear group } (q, G_1, G_2, G_T, e, g_1, g_2) \leftarrow G(1^k). \text{ Take } s \leftarrow \mathbb{Z}_q, \text{ compute } pk = g_2^s, \text{ and output } sk \text{ as private key and } pk = (q, G_1, G_2, G_T, g_1, g_2, e, pk) \text{ as public key. } \\
\text{Sign:} & \quad \text{On input message } m \in \mathbb{Z}_q \text{ and secret key } sk, \text{ output } \sigma = g_1^{rs}. \\
\text{Verify:} & \quad \text{On input the signature } \sigma, \text{ message } m, \text{ and public key } pk, \text{ output } 1 \text{ iff } e(\sigma, pk) \cdot e(\sigma^m, g_2) = e(g_1, g_2) \text{ holds. }
\end{align*}
\]

Showing the constant signature \( \sigma \) multiple times would make the protocol linkable. All user sessions would be linkable to a single profile, which would make the resulting scheme very privacy unfriendly. To avoid linkability of signatures, users can only prove the knowledge of a valid signature by using the proof defined in (Camenisch et al., 2016). In this proof, the user chooses a random value \( r \leftarrow \mathbb{Z}_q \) and computes randomized auxiliary values \( \sigma' = \sigma^r \) and \( \sigma = \sigma^{-m} g_1^r \). Then, the knowledge of a signature is proven by constructing the zero-knowledge proof \( \pi = PK(\{m, r \mid \sigma = \sigma'^{-m} g_1^r \}) \) and verifying \( e(\sigma, g_2) = e(\sigma', pk) \). The verifier is convinced, that the user indeed knows a valid signature on a known message, although the proof does not release any of these values.

The wBB signatures were proven existentially unforgeable against a weak (non-adaptive) chosen message attack under the \( q \)-SDH assumption (Boneh and Boyen, 2008).

2.5 Group Signatures from Randomizable Proofs of Signatures

Group signatures (Chaum and Van Heyst, 1991) allow users to sign messages using their private keys without being identifiable or traceable, as the signatures are verified by a single, general public key.
There are many proposals for group signatures, focusing on size, speed of construction, security or advanced features. For our data collection scheme, we adopt the approach used in (Pointcheval and Sanders, 2016), i.e., we let the manager to sign the private keys of users (sk) using a signature scheme σ (wBB in our case) that allows efficient randomizable proofs of the signature knowledge, resulting in signature σ(sk). Proving the manager’s signature knowledge using SPK (Signature Proof of Knowledge) then allows the construction of user’s group signatures on messages (SPK{sk : σ(sk)}(m)). Using such a construction, each user has his own private key but the signatures are verified using a common manager’s key. Furthermore, all signatures are anonymous, untraceable and unlinkable.

3 CRYPTOGRAPHIC DESIGN

3.1 General Architecture

Three types of entities interact in our data collection scheme: a manager, a user and a collector.

- **Manager**: the manager generates cryptographic parameters and keys. It also enrolls new users (devices) and revokes invalid ones.
- **User**: the user is represented by its device, such as a smart meter, sensor or some wearable device. It is the source of data that are signed and transferred to the central device (collector).
- **Collector**: the collector represents the central node that collects all data from users and verifies the group signatures.

The entities interact in the following cryptographic algorithms and protocols.

- \((pk, sk_m, par) \leftarrow \text{Setup} \leftarrow 1^X\): on the input of security parameter \(X\), the algorithm generates the public systems parameters \(par\) (implicit input of all other algorithms), the public key shared by all users \(pk\) and the private key of the manager \(sk_m\). The \text{Setup} algorithm is run by the manager.
- \((sk_i, rd) \leftarrow \text{Register} \leftarrow (id_i, sk_m):\) on the input of the manager’s private key \(sk_m\) and the user identifier \(id_i\), the register protocol outputs the user’s private key \(sk_i\) and updates the manager’s revocation database \(rd\). The \text{Register} algorithm is run as an interactive protocol between the manager and the user.
- \(\text{sign}(sk_i, m) \leftarrow \text{Sign} \leftarrow (m, id_i, sk_i):\) on the input of the message \(m\), user’s identifier \(id_i\) and its private key \(sk_i\), the algorithm outputs the signature on the message \(\text{sign}(sk_i, m)\). The algorithm is run by the user.

- \(0/1 \leftarrow \text{Verify} \leftarrow (\text{sig}(sk_i, data), m, pk):\) on the input of the message \(m\), signature \(\text{sig}(sk_i, m)\) and the public key \(pk\), the algorithm returns 1 iff the signature is valid and 0 otherwise. The algorithm is run by the collector.
- \(id_i \leftarrow \text{Revoke} \leftarrow (rd, \text{sig}(sk_i, data)):\) on the input of the manager’s revocation database \(rd\) and a signature \(\text{sig}(sk_i, m)\), the algorithm outputs the identifier \(id_i\) of the signer.

The algorithms and protocols must fulfill the following security properties of group signatures defined by Bellare et al. (Bellare et al., 2005). The manager is trusted not to impersonate signers.

- **Correctness**: signatures are verified correctly iff generated by valid and honest users.
- **Anonymity**: all signatures are anonymous, untraceable and unlinkable to all entities except the manager.
- **Traceability**: the manager can de-anonymize, link and trace signatures.

The privacy-enhanced data collection scheme is presented in Fig. 2.

3.2 Instantiation using wBB Signatures

We instantiate the algorithms and protocols of the data collection scheme presented in the previous section using the wBB signature (Boneh and Boyen, 2008) and its efficient proof of knowledge (Camenisch et al., 2008).
2016). On a high level, we let the user to obtain a wBB signature on his private identifier from the manager. Then, the user proves the knowledge of such a signature anonymously and efficiently using the Schnorr-like zero-knowledge protocol for proving the knowledge of a discrete logarithm (Camenisch and Stadler, 1997). For the conversion from the proof of knowledge to the signature, we use the Fiat-Shamir heuristics (Fiat and Shamir, 1987).

We present the concrete algorithm and protocol instantiations below.

3.2.1 Setup

\((pk, sk_m, par) \leftarrow \text{Setup} \leftarrow 1^\mathcal{K}\): the algorithm inputs the security parameter \(\mathcal{K}\) and generates the bilinear group with parameters \(par = (\varphi, G_1, G_2, G_T, e, g) \in G_1, g_2 \in G_2\) satisfying \(|\varphi| = \mathcal{K}\). It also generates the manager’s private key \(sk_m \leftarrow \mathcal{Z}_q\) and computes the public key \(pk = g^{sk_m}\). It outputs the \((pk, par)\) as a public output and the \(sk_m\) as the manager’s private output.

3.2.2 Register

\((sk_i, rd) \leftarrow \text{Register} \leftarrow (id_i, sk_m):\) the protocol is distributed between the user and the manager. The manager inputs his private key \(sk_m\) and the user inputs his private identifier \(id_i\). The protocol outputs the wBB signature \(sk_i = g^{sk_m + id_i}\) to the user over a secure channel and updates the manager’s revocation database \(rd\) by storing \(id_i\).

3.2.3 Sign

\(\text{sig}(sk_i, m) \leftarrow \text{Sign} \leftarrow (m, id_i, sk_i):\) the algorithm inputs the user’s private identifier \(id_i\), his private key \(sk_i\) and the message to be signed. It outputs the signature \(\text{sig}(sk_i, m)\) that consists of the following elements \((g', sk'_m, sk_i, \pi)\):

- \(g' = g\): the generator raised to a randomly chosen randomizer \(r \leftarrow \mathcal{Z}_q\).
- \(sk'_m = sk'_m\): the user’s private key raised to the randomizer.
- \(sk_i = sk_i^{−id_i}\): the randomized private key raised to the user identifier.
- \(\pi = \text{SPK}\{(id_i, r) : sk_i = sk_i^{−id_i} \land g' = g'(m)\}\): proof of knowledge of \(r\) and \(id_i\) signing the message \(m\).

3.2.4 Verify

\(0/1 \leftarrow \text{Verify} \leftarrow (\text{sig}(sk_i, m), m, pk, bl):\) the algorithm inputs the message \(m\), its signature \(\text{sig}(sk_i, m)\), a blacklist \(bl\) and the public key \(pk\). It checks the proof of knowledge signature \(\pi\) and checks that the signature is valid with respect to the manager’s public key using the equation \(e(\bar{sk}_i g', g_2) = e(sk'_m, pk)\). The collector also performs the revocation check \(\bar{sk}_i = sk_i^{−id_i}\) for all \(id_i\) values stored on the blacklist \(bl\). If the revocation check equation holds for any value on the blacklist, the signature is rejected. Otherwise, the signature is accepted if all other checks pass.
3.2.5 Revoke

\[ bl \leftarrow \text{Revoke} \leftarrow (rd, \text{sig}(sk_i, m)) : \text{the algorithm inputs a signature } \text{sig}(sk_i, m) \text{ and a revocation database } rd. \text{ It checks } \hat{sk}_i = sk_i^{id_i} \text{ for all } id_i \text{s in } rd. \text{ The id}_i \text{ that holds in the equation is put on a public blacklist } bl. \]

The Register, Sign and Verify algorithms are presented in CS notation in Fig 3.

4 SECURITY ANALYSIS

We imply the security of our scheme from the security of the building blocks. The wBB signature scheme used for signing the private keys is unforgeable against a non-adaptive chosen message attack under the \( q \)-SDH assumption (Boneh and Boyen, 2008). The group signature is an efficient proof of knowledge based on the standard zero-knowledge proofs (Camenisch and Stadler, 1997) that are complete, sound and zero-knowledge in the random oracle model.

4.1 Correctness

The proof \( \pi \) is always accepted for valid signatures, due to the completeness of the proof of knowledge protocol. The proof \( \pi \) is always reject for the invalid signatures, due to the soundness property of the proof of knowledge protocol.

The pairings are always accepted if a valid manager’s key is used in the signature:

\[ e(\hat{sk}_i g', g_2) = e(sk'_i, pk) \]  
\[ e(sk_i^{id_i} g', g_2) = e(sk'_i, g_2^{\text{sk}_n}) \]  
\[ e(g^{\text{sk}_n + id_i^{id_i}} g', g_2) = e(sk'_i, g_2^{\text{sk}_n}) \]  
\[ e(g^{\text{sk}_n + id_i^{id_i}} g, g_2) = e(sk'_i, g_2^{\text{sk}_n}) \]  
\[ e(s_{\text{sk}_n} g, g_2) = e(sk'_i, g_2^{\text{sk}_n}) \]  
\[ e(s_{\text{sk}_n} g, g_2) = e(sk'_i, g_2^{\text{sk}_n}) \]

4.2 Anonymity

The proof \( \pi \) is always anonymous, untraceable and unlinkable due to the zero-knowledge property of the proof of knowledge protocol.

Distribution of \( g', sk'_i, \hat{sk}_i \) is random and uniform in \( \mathbb{Z}_q \) as \( r \) is selected randomly and uniformly from \( \mathbb{Z}_q \). Thus, the values disclosed are indistinguishable from random elements.

4.3 Traceability

Provided the user’s private identifier \( id_i \), the signatures are linkable by \( \hat{sk}_i = sk_i^{-id_i} \).

5 IMPLEMENTATION RESULTS

We present the computational and communication complexity analysis in this section. Furthermore, we present the results of our practical implementation on several types of devices, including constrained devices and wearables here.

The user’s device has to compute only 5 exponentiations to construct the proof. On the other side, the verifier has to perform 2 bilinear pairings and 3 exponentiations to verify the proof. The revocation check time is linear to the number of revoked users and, therefore, requires \( O(|RL|) \) exponentiations, where \( |RL| \) is the number of revoked users. The computational and communication costs of our scheme is considerably reduced due to the use of EC cryptography which requires smaller keys compared to traditional protocols on a similar security level. Our signatures contain only 3 elements of \( \mathbb{G}_1 \) and 3 elements of \( \mathbb{Z}_p \). Therefore, using a strong 224 b elliptic curve, only 255 B need to be sent as a signature. In case that EC point compression is used, we can reduce the signature size to less than 169 B (1347 b). Hence, the size of \( \mathbb{Z}_p \) remains 224 b and the size of each element of \( \mathbb{G}_1 \) is 225 b rather than 448 b. This is especially significant in smart card communication scenarios, where the payload size of APDU message is restricted to 255 B if T=0 transmission protocol is used.

We implemented the Sign and Verify protocols, the full description of our algorithms is in Fig. 4.

5.1 Performance

Our proposal is particularly suitable for data collections systems, such as smart metering. In these systems, the data are anonymously collected by a central collector from the remote nodes. Furthermore, due to the fast signature generation speed and size efficiency, our scheme can by used in a wide range of other applications, such as e-ticketing and transportation e-IDs. For this reason, we performed the measurements on different kinds of devices, both constrained (wearables, embedded devices) and powerful (PC, server) ones. We considered the following test scenarios:

Smart Metering: smart houses are equipped with different types of sensors, e.g., for gas, water, or elec-
User i

Collector

\[ id_i, sk_i, m \]

\[ r, \rho r, \beta_{id_i}, \xi, Z \subset \mathbb{Z}_q \]

\[ g' = g^r \]

\[ sk' = sk^r \]

\[ t = sk'^{\beta_{id_i}} g^r \]

\[ e = H(g', sk_i', sk_i, t, m) \]

\[ s_r = \rho r - er \]

\[ s_{id_i} = \rho_{id_i} + e \rho \]

\[ g', s_{id_i}' = sk_i, e, s_r, s_{id_i} \rightarrow \]

\[ t = (sk_i g')^r s_{id_i}^{\beta_{id_i}} g^r \]

\[ e = H(g', sk_i', sk_i, t, m) \]

\[ e(s_{id_i} g', g_2) \]

Revocation Check:

\[ sk_i = sk_i^{\rho_{id_i}} \]
Table 3: Benchmarks of primitive operations.

<table>
<thead>
<tr>
<th>Curve</th>
<th>d159</th>
<th>d201</th>
<th>d224</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC op.</td>
<td>$E_{G_1}$ [ms]</td>
<td>$E_{G_1}$ [ms]</td>
<td>$E_{G_1}$ [ms]</td>
</tr>
<tr>
<td>SC</td>
<td>40</td>
<td>50</td>
<td>40</td>
</tr>
<tr>
<td>Phone 1</td>
<td>38</td>
<td>1.0</td>
<td>48</td>
</tr>
<tr>
<td>Phone 2</td>
<td>153</td>
<td>5.4</td>
<td>161</td>
</tr>
<tr>
<td>Watch 1</td>
<td>350</td>
<td>12.4</td>
<td>457</td>
</tr>
<tr>
<td>Watch 2</td>
<td>196</td>
<td>6.5</td>
<td>246</td>
</tr>
</tbody>
</table>

Table 4: Comparison with current short group signature schemes.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Sign Cost</th>
<th>Verify Cost</th>
<th>Sign Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>BBS (Boneh et al., 2004)</td>
<td>$9E_{G_1}+3E_{G_T}$</td>
<td>$1P+8E_{G_1}+2E_{G_T}+3E_{G_T}$</td>
<td>$(1545 \text{ b})$</td>
</tr>
<tr>
<td>DP (Delerablé and Pointcheval, 2006)</td>
<td>$8E_{G_1}+3E_{G_T}$</td>
<td>$1P+4E_{G_1}+3E_{G_T}$</td>
<td>$(1559 \text{ b})$</td>
</tr>
<tr>
<td>HLCCN (Hwang et al., 2011)</td>
<td>$7E_{G_1}+5E_{G_T}$</td>
<td>$1P+5E_{G_1}+2E_{G_T}+3E_{G_T}$</td>
<td>$(1375 \text{ b})$</td>
</tr>
<tr>
<td>ACJ (Achlioptas et al., 2000)</td>
<td>$12E_{G_1}$</td>
<td>$10E_{G_0}$</td>
<td>$(7328 \text{ b})$</td>
</tr>
<tr>
<td>CG (Camenisch and Groth, 2004)</td>
<td>$10E_{G_1}$</td>
<td>$10E_{G_0}$</td>
<td>$(8352 \text{ b})$</td>
</tr>
<tr>
<td>IMSTY (Hoshiki et al., 2006)</td>
<td>$7E_{G_1}$</td>
<td>$7E_{G_0}$</td>
<td>$(6155 \text{ b})$</td>
</tr>
<tr>
<td>HM G (Hajny et al., 2013)</td>
<td>$9E_{G_1}$</td>
<td>$10E_{G_0}$</td>
<td>$(7328 \text{ b})$</td>
</tr>
<tr>
<td>Our Scheme</td>
<td>$5E_{G_1}$</td>
<td>$2P+3E_{G_1}$</td>
<td>$(1035 \text{ b})$</td>
</tr>
</tbody>
</table>

The Fig. 5 and Fig. 6 show the time needed to identify a malicious user. The procedure requires to perform scalar multiplications on the considered device (the cost of this operation is depicted in Tab. 3). In case of the de-anonymisation procedure, the number of scalar multiplications is equal to the number of users. We stress, that the de-anonymisation procedure is expected to be performed on powerful devices and can be parallelized on their processors and cores (CPU/Cores). For instance, our PC (1/4), and server (2/8) are able go through the list of thousands of users and find the identity of a user in less than 4 min, see Fig. 5.

In the revocation check procedure, the PC (1/4) and server (2/8) are able to search the black list in less than 0.5 s, see Fig. 6.

5.2 Comparison

In this section, we provide the comparison of our scheme with the state-of-the-art group signature scheme with the state-of-the-art group signature.
schemes. We considered the efficient group signature schemes identified in (Malina et al., 2018). Tab. 3 shows the comparison of our scheme with these pairing and non-pairing based group signature schemes. Bilinear pairing and exponentiation operations are denoted as P and E, respectively. The execution time of each operation depends on the bitlength of the elements in respective groups and fields. In the pairing-based schemes, $G_1$, $G_2$, $G_T$, $Z_p$ denote different groups with the following bitlengths: $|G_1| = 175$ b, $|G_2| = 175$ b and $|G_T| = 1050$ b computed as $k \cdot |G_1|$, where $k$ is the embedding degree (e.g. $k = 6$). $|Z_p| = 170$ b denotes the field size of an elliptic curve. In the non-pairing schemes, $|G_n| = 1024$ b denotes the multiplicative RSA group with exponents from $|Z_q| = 160$ b. The total length of signatures depends on the security level chosen.

6 CONCLUSIONS

We presented a novel data collection scheme which is more efficient than comparable state-of-the-art schemes as shown in the comparative complexity analysis. The proposed scheme is built using primitives with formal security proofs and the security of the proposed scheme itself was proven.

Our proposal is particularly suitable for data collections systems, such as smart metering. However, our scheme can be also used in other areas of IoT, such as smart grids, Industry 4.0, e-ticketing, transportation e-IDs, due to the signature generation speed and short size.

Moreover, we provided the full implementation results from a wide range of devices, including IoT devices, to show the efficiency of our solution. A signature on the 112 b security level can be generated in 442 ms on a standard smart card, in 336 ms on a current smart phone and in 18 ms on the Raspberry Pi 3. Furthermore, our scheme provides fast revocation checks, the blacklisted user can be identified in less than 2 s.

ACKNOWLEDGEMENTS

Research described in this paper was financed by the Ministry of Industry and Trade grant # FV20354 and the National Sustainability Program under grant LO1401. For the research, infrastructure of the SIX Center was used.

REFERENCES


Anonymous Data Collection Scheme from Short Group Signatures


