

# Anonymous Attribute-based Credentials in Collaborative Indoor Positioning Systems

## Citation

Casanova-Marqués, R., Pascacio, P., Hajny, J., Torres-Sospedra, J., 2021. Anonymous Attribute-based Credentials in Collaborative Indoor Positioning Systems, in: Proceedings of the 18th International Conference on Security and Cryptography, SCITEPRESS - Science and Technology Publications, pp. 791–797.

## Year

2021

## Version

Peer reviewed version (post-print)

## Link to publication

<https://www.scitepress.org/Link.aspx?doi=10.5220/0010582507910797>

## Published in

SCITEPRESS - Science and Technology Publications

## DOI

<https://doi.org/10.5220/0010582507910797>

## License

This publication is copyrighted. You may download, display and print it for Your own personal use. Commercial use is prohibited.

## Take down policy

If you believe that this document breaches copyright, please contact the authors, and we will investigate your claim.

## BibTex entry

```
@inproceedings{BUT171515,  
  author="Raúl {Casanova-Marqués} and Pavel {Pascacio} and Jan {Hajný}  
and Joaquín {Torres-Sospedra}",  
  title="Anonymous Attribute-Based Credentials in Collaborative  
Indoor Positioning Systems",  
  booktitle="Proceedings of The 18th International Conference on  
Security and Cryptography (SECRYPT 2021)",  
  doi="10.5220/0010582507910797",  
  year="2021",  
  month="july",  
  pages="1--7",  
}
```

# Anonymous Attribute-based Credentials in Collaborative Indoor Positioning Systems

Raúl Casanova-Marqués<sup>1,2</sup><sup>a</sup>, Pavel Pascacio<sup>2,3</sup><sup>b</sup>, Jan Hajny<sup>1</sup><sup>c</sup> and Joaquín Torres-Sospedra<sup>2,4</sup><sup>d</sup>

<sup>1</sup>*Department of Telecommunications, Brno University of Technology, Brno, Czech Republic*

<sup>2</sup>*Institute of New Imaging Technologies, Universitat Jaume I, Castellón, Spain*

<sup>3</sup>*Electrical Engineering Unit, Tampere University, Tampere, Finland*

<sup>4</sup>*UBIK Geospatial Solutions S.L., Castellón, Spain*

{casanova, hajny}@vutbr.cz, pascacio@uji.es, torres@ubikgs.com

**Keywords:** Attribute-based Credentials, Collaborative Indoor Positioning Systems, Privacy, Anonymity, Bluetooth Low Energy, Wearables.

**Abstract:** Collaborative Indoor Positioning Systems (CIPs) have recently received considerable attention, mainly because they address some existing limitations of traditional Indoor Positioning Systems (IPSs). In CIPs, Bluetooth Low Energy (BLE) can be used to exchange positioning data and provide information (the Received Signal Strength Indicator (RSSI)) to establish the relative distance between the actors. The collaborative models exploit the position of actors and the relative position among them to allow positioning to external actors or improve the accuracy of the existing actors. However, the traditional protocols (e.g., iBeacon) are not yet ready for providing sufficient privacy protection. This paper deals with privacy-enhancing technologies and their application in CIPs. In particular, we focus on cryptographic schemes which allow the verification of users without their identification, so-called Anonymous Attribute-based Credential (ABC) schemes. As the main contribution, we present a cryptographic scheme that allows security and privacy-friendly sharing of location information sent through BLE advertising packets. In order to demonstrate the practicality of our scheme, we also present the results from our implementation and benchmarks on different devices.


## 1 INTRODUCTION


Wi-Fi and BLE fingerprinting are popular techniques for providing indoor positioning. They rely on the signal strength from multiple emitters (either Wi-Fi Access Points (APs) or BLE beacons). However, the Received Signal Strength (RSS) data used to estimate the positions have a strong noise component, therefore having a general positioning accuracy at meter level (i.e., a few meters) (Mautz, 2012). In addition, the deployment complexity, as well as relying on an infrastructure of beacons and servers, have become a serious problem for large organizations all around the world. Wearable-based CIPs are increasingly becoming popular over the last few years as a solution to address those problems in indoor positioning (Pascacio et al., 2021). The CIPs use the location of a


set of actors and their relative distances to 1) provide localization to external users and/or 2) improve the positioning accuracy of the current users that are collaborating (Khandker et al., 2019).

Wearable devices are equipped with built-in technologies such as Wi-Fi and Bluetooth, which are capable of estimating users' positions and ubiquity in indoor environments. In particular, CIPs approaches based on BLE are one of the most popular solutions. Smartphones can send BLE advertisement packets (e.g., iBeacon), which can be used later to compute the relative distances between them with the gathered RSS values. This alternative presents a straightforward deployment and a good trade-off between power consumption and performance (Yang et al., 2020). However, high inter-connectivity to unknown devices and the lack of strong communication protocols in terms of security and privacy represent a weakness. Malicious actors could perform attacks such as spoofing or eavesdropping in unsecured collaborative systems (Chebli et al., 2019). These issues encouraged the development of more privacy-friendly solutions.

<sup>a</sup> <https://orcid.org/0000-0001-6653-867X>

<sup>b</sup> <https://orcid.org/0000-0001-9206-7496>

<sup>c</sup> <https://orcid.org/0000-0003-2831-1073>

<sup>d</sup> <https://orcid.org/0000-0003-4338-4334>

Existing CIPS are based on centralized schemes. A server-based solution facilitates more complex attacks such as user traceability or linkability of communications. Thus, it is necessary to move to a decentralized approach. Building a decentralized CIPS using BLE technology represents a major challenge due to the reduced space available in BLE packets, which depends on the Bluetooth version (Bluetooth SIG, 2019). This hinders the use of standard algorithms such as RSA, DH or AES for information encryption and user authentication. Attribute-based authentication schemes allow users to anonymously and selectively prove possession of their personal attributes such as age, citizenship, negative SARS-CoV-2 test or location data. Elliptic curve cryptography and the reduced size of its keys can tackle the aforementioned problems and provide anonymity, unlinkability, untraceability and selective disclosure of attributes.

In light of the identified problems, in this work we pursue the decentralization of collaborative indoor positioning systems based on BLE beacons, while providing, through elliptic curve cryptography and anonymous attribute-based authentication schemes, a secure and privacy-friendly system for exchanging location data.

## 1.1 Related Work

In the literature there are several articles that address anonymity, security, and privacy issues of IPSs from different perspectives (e.g., Wireless Sensor Network (WSN) or Internet of Things (IoT)). However, only very few of them focus on collaborative positioning and/or BLE beacon approaches. One of the most interesting papers is proposed by (Kang et al., 2018), which is based on the open-source Eddystone BLE format proposed by (Hassidim et al., 2016). Eddystone BLE format introduces a scheme to mitigate tracking and security threats. The core of the scheme is cloud-based Ephemeral Identifiers (EID), which ensures only authorized members to properly identify the BLE standard beacons.

Up to now, far too little attention has been paid to CIPSS. (Zidek et al., 2018) developed a scheme named Bellrock which combines an ecosystem of standard beacons and user-based beacons. Bellrock provides access control to standard beacons and anonymity to user-based beacons by using three techniques to generate pseudo-anonymous identifiers (random, synchronized, and encrypted) that can be unmasked by a server.

(Destiarti et al., 2017) proposed the Data Transmission Scheme for Indoor Mobile Cooperative Localization System that works over Wi-Fi. The scheme

uses AES-128 to encrypt the message, MD5 to construct the HMAC and RSA-2048 to encrypt both the AES key and the HMAC. Their approach might not be well suited as the system remains vulnerable to man-in-the-middle attacks during the RSA key-pair exchange, leading to a total loss of confidentiality and message integrity.

A key problem with the aforementioned proposals lies in server-dependency, turning the system into a centralized environment. This method could suffer from a plethora of pitfalls such as denial of service (DoS), spoofing, etc.

Some preliminary work on ABCs was carried out several decades ago by (Chaum, 1985), (Brands, 2000), and (Camenisch and Lysyanskaya, 2001). In subsequent years, much more information on ABCs has become available about practical applications (Arfaoui et al., 2015), revocation protocols (Camenisch et al., 2010) and the use of more efficient algebraic structures (Chase et al., 2014), (Barki et al., 2016), and (Ringers et al., 2017). Due to the high computational complexity required by these schemes, practical implementation on constrained devices is still a challenge, researchers need to find a scheme that satisfies their specific needs. As far as we know, no studies have been published on ABC schemes applied to CIPSS.

## 1.2 Our Contribution

In order to fill the gap found in the literature, we propose a new decentralized privacy-preserving user authentication mechanism for CIPSS with ABC. Our solution combines zero-knowledge proofs with a revocation scheme based on lifetime and provides anonymity, unlinkability and untraceability.

The main contributions are the following:

- To the best of our knowledge, we present the first decentralized security scheme for CIPSS based on BLE advertising.
- We define a scheme that provide anonymous location data sharing, decentralized authentication and offline revocation.
- We provide a security analysis on the proposed solution.
- We describe the implementation results.

The rest of the paper is organized as follows. Section 2 gives a brief overview of the system model. Section 3 thoroughly details the cryptographic design of the scheme. Section 4 analyzes the security. Section 5 presents the implementation results. Finally, Section 6 reports some conclusions.

## 2 SYSTEM OVERVIEW

The system model is depicted in Figure 1 and consists of the following entities:

- **Issuer (I)**: is responsible for issuing the personal attribute  $m_{ID}$  to a user using the `Issue` algorithm. The  $m_{ID}$  attribute represents the user identifier obtained during registration in the system. The `Issue` algorithm provides the user with cryptographically signed credentials that are valid within the system. Access credentials consist of the values  $\sigma, \sigma_{x_0}, \sigma_{x_r}, \sigma_{x_{ID}}$ .
- **Revocation Authority (RA)**: removes invalid users. Access control is achieved through the revocation credential  $\sigma_{x_r}$ , issued from the revocation attribute  $m_r$ . Attempting to authenticate with the revoked credentials will result in failure. To reduce the complexity of the system, we will consider from now on the revocation authority and the issuer as the same entity (I).
- **User (U)**: enrolls in the system to use the collaborative indoor positioning system. Every user holds unique credentials generated by the issuer and the revocation entity  $(\sigma, \sigma_{x_0}, \sigma_{x_r}, \sigma_{x_{ID}})$ , then, the user can anonymously prove their possession to the verifier using the `Show` algorithm.
- **Verifier (V)**: verifies the possession of the user attribute using the `Verify` algorithm. If the attribute ownership is verified successfully, the verifier will be able to use the location information to position themselves. Otherwise, the information is rejected.

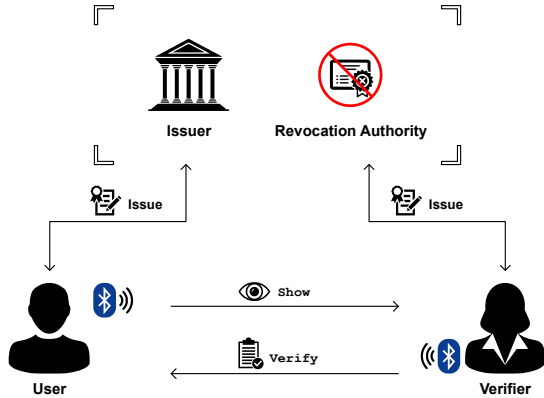


Figure 1: System structure.

Initially, all devices registered in the system behave as Users. When one of them needs to improve its position, it temporarily assumes the role of Verifier. This role can be used to ensure that the information is provided by a valid user.

There are two modes of operation for the User and Verifier roles: the active mode and the passive mode.

User operation modes: 1) *Active mode*: responds to verifier requests and assists them with positioning by actively participating in the system. 2) *Passive mode*: remains unnoticed in the system and does not respond to verifier requests. In this mode, the user does not interact with the system.

Verifier operation modes: 1) *Active mode*: actively requests location data from nearby users to improve its position. 2) *Passive mode*: remains hidden in the system and waits for other verifiers to request location data. In this mode, positioning is not possible if there are no active verifiers nearby.

Figure 2 depicts each of these four modes. User A acts in active mode, user B acts in passive mode, verifier C acts in active mode, and verifier D acts in passive mode.

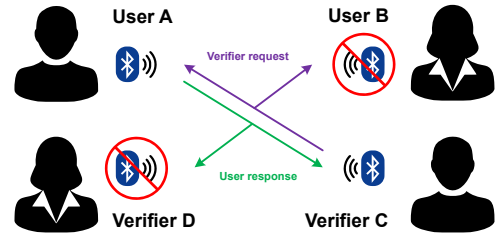


Figure 2: System roles and operation modes.

These modes of operation are useful for improving privacy in environments where there are few devices, and it may be easy to determine their identity. In this case, the user or verifier can go into passive mode and disappear from the system. We will not go into further details because it is beyond the scope of this paper.

## 3 CRYPTOGRAPHIC DESIGN

This section describes the protocol for user authentication in a collaborative indoor positioning system.

### 3.1 Preliminaries

The symbol  $\mathcal{H}$  denotes a secure hash function. We write  $a \xleftarrow{\$} A$  when  $a$  is sampled uniformly at random from  $A$ . Let  $e$  denote a bilinear map  $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ .

### 3.2 Protocol Specification

First, the user must be registered in the system by sending their personal information to the issuer. The issuer generates the credentials and sends them to the user. The user can now legitimately participate in the system. This algorithm will be denoted as `Issue`.

When the verifier wants to improve their position, a BLE advertisement packet with a timestamp will be broadcast. The nearby users will compute the proof of knowledge and transmit it via another BLE packet. This algorithm will be denoted as Show.

Finally, the verifier will ensure through the proof of knowledge that the user has valid credentials and will use the location information to position themself. This algorithm will be denoted as Verify.

### 3.2.1 Issue

To register the user in the system and generate the valid credentials, the user and the issuer perform the algorithm shown in Figure 3.

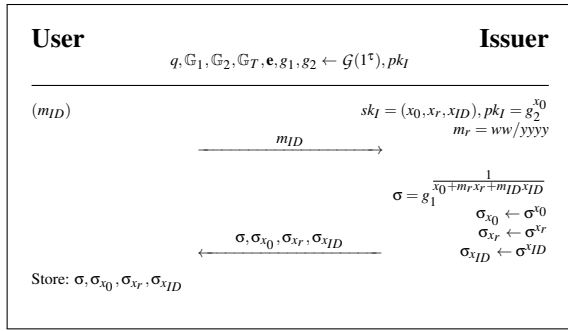


Figure 3: Definition of the Issue algorithm.

- The user U performs the following steps:
  - 1) Introduces personal information in the app.
  - 2) Establishes a secure communication channel with I and sends  $m_{ID}$ .
- The issuer I performs the following steps:
  - 1) Generates the user's private keys  $x_r$  and  $x_{ID}$ .
  - 2) Signs the attributes  $m_r$  and  $m_{ID}$  with the issuer's secret key as  $\sigma = g_1^{\frac{1}{x_0 + m_r x_r + m_{ID} x_{ID}}}$ ; and computes auxiliary values  $\sigma_{x_0}, \sigma_{x_r}, \sigma_{x_{ID}}$ , where  $\sigma_{x_0} \leftarrow \sigma^{x_0}$ ,  $\sigma_{x_r} \leftarrow \sigma^{x_r}$ , and  $\sigma_{x_{ID}} \leftarrow \sigma^{x_{ID}}$ .
  - 3) Sends  $\sigma$  and auxiliary values  $\sigma_{x_0}, \sigma_{x_r}, \sigma_{x_{ID}}$  to the user U.

### 3.2.2 Show and Verify

To broadcast the location information and the proof of knowledge, and subsequently verify that it comes from a legitimate user, the user and the verifier will run the algorithms shown in Figure 4.

- The verifier V performs the following steps:
  - 1) Generates a nonce based on the current time.
  - 2) Creates a BLE advertising packet with the nonce and broadcasts it.

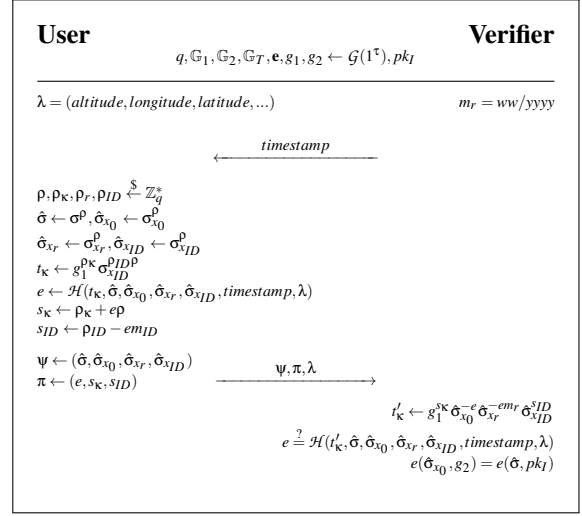


Figure 4: Definition of the Show and Verify algorithms.

- Nearby users  $u_i$  perform the following steps after they have received the timestamp:
  - 1) Checks that the timestamp generated as a nonce by the verifier is less than 2 seconds from the current time to avoid replay attacks.
  - 2) Generates the randomizers  $\rho, \rho_K, \rho_r, \rho_{ID}$ .
  - 3) Computes  $\hat{\sigma}, \hat{\sigma}_{x_0}, \hat{\sigma}_{x_r}, \hat{\sigma}_{x_{ID}}$ , where  $\hat{\sigma} \leftarrow \sigma^\rho$ ,  $\hat{\sigma}_{x_0} \leftarrow \sigma_{x_0}^\rho$ ,  $\hat{\sigma}_{x_r} \leftarrow \sigma_{x_r}^\rho$ , and  $\hat{\sigma}_{x_{ID}} \leftarrow \sigma_{x_{ID}}^\rho$ .
  - 4) Computes the attribute proof of knowledge  $t_K$  as  $t_K \leftarrow g_1^{\rho_K} \sigma_{x_{ID}}^{\rho_{ID}}$ .
  - 5) Calculates the cryptographic hash  $e$  as  $\mathcal{H}(t_K, \hat{\sigma}, \hat{\sigma}_{x_0}, \hat{\sigma}_{x_r}, \hat{\sigma}_{x_{ID}}, timestamp, \lambda)$  and the auxiliary proof of knowledge values  $s_K, s_{ID}$ , where  $s_K \leftarrow \rho_K + e\rho$  and  $s_{ID} \leftarrow \rho_{ID} - em_{ID}$ .
  - 6) Creates a BLE advertising packet with the location information  $\lambda$  and the proof of knowledge  $\Psi \leftarrow (\hat{\sigma}, \hat{\sigma}_{x_0}, \hat{\sigma}_{x_r}, \hat{\sigma}_{x_{ID}}), \pi \leftarrow (e, s_K, s_{ID})$ , and transmits it by broadcast.
- Nearby verifiers  $v_i$  execute the following steps after receiving  $\Psi, \pi$ , and  $\lambda$ .
  - 1) Recomputes the attribute proof of knowledge  $t'_K$  as  $t'_K \leftarrow g_1^{s_K} \hat{\sigma}_{x_0}^{-e} \hat{\sigma}_{x_r}^{-em_r} \hat{\sigma}_{x_{ID}}^{s_{ID}}$ .
  - 2) Calculates the cryptographic hash using  $t'_K$  as  $\mathcal{H}(t'_K, \hat{\sigma}, \hat{\sigma}_{x_0}, \hat{\sigma}_{x_r}, \hat{\sigma}_{x_{ID}}, timestamp, \lambda)$  and checks if it matches the value of  $e$ .
  - 3) Computes the bilinear pairing  $e(\hat{\sigma}_{x_0}, g_2) = e(\hat{\sigma}, pk_I)$  to verify the credentials were emitted by the issuer.

## 3.3 Bluetooth Integration

The proposed scheme transmits information using BLE advertising packets. Bluetooth 4.2 and earlier

defined a payload size of 31 bytes for a single BLE advertisement packet. However, since it is impractical to pack both the positioning data and the proof of knowledge into 31 bytes, we have considered version 5.0 of the BLE protocol. Bluetooth 5.0 introduced a significant improvement by increasing the capacity of advertising packets. With Low-Energy Advertising Extensions, the advertisement payload can hold up to 254 bytes (Bluetooth SIG, 2019).

To build the structure of the BLE advertising packet, we have assumed the structure depicted in Figure 5.

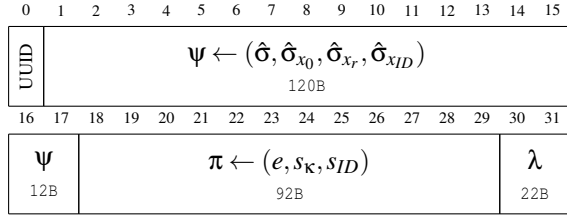


Figure 5: Definition of the BLE advertising payload.

The UUID field occupies 8 bytes, the proof of knowledge  $(\psi, \pi)$  consists of 224 bytes, and there is a free space of 22 bytes for the positioning data  $(\lambda)$ . This part is explained in detail in Section 5.

## 4 SECURITY ANALYSIS

The protocol is composed of the following parts: the anonymous credentials scheme, the revocation scheme and the positioning information. In this section we provide a brief informal security analysis of each of them.

### 4.1 Anonymous Credentials

Following the security model defined by (Chase et al., 2014) for anonymous credential schemes, it is required to meet the following properties:

- *Correctness*: honest users can produce an accepting proof.
- *Unforgeability*: dishonest users cannot produce an accepting proof.
- *Anonymity*: users cannot be identified based on the values of attributes.
- *Key-Parameter Consistency*: every public key has a distinct private key.

Based on the random Oracle model in (Camenisch et al., 2019), the credential scheme used in our system has proven to be secure under the n-SCDHI assumption (defined below).

**Definition 1** (*n*-Strong Computational Diffie-Hellman Inversion Problem (SCDHI)). Let  $O^{\text{bb}}(\cdot)$  on input  $(m_1, \dots, m_n) \in \mathbb{Z}_q^{*n}$  add  $(m_1, \dots, m_n)$  to  $Q$  and output  $g^{1/(x_0 + \sum_{i=1}^n x_i m_i)}$ . Let  $O^{\text{dh}_i}(\cdot)$  on input  $h$  output  $h^{x_i}$ . Define the advantage of  $\mathcal{A}$  as follows.

$$\text{Adv}_{n\text{-SCDHI}}(\mathcal{A}) = \Pr \left[ (\mathbb{G}, g, q) \leftarrow \text{GroupSetup}(1^\kappa), \right. \\ (x_0, \dots, x_n) \xleftarrow{\$} \mathbb{Z}_q^{*n+1}, (y, m_1^*, \dots, m_n^*) \leftarrow \\ \left. \mathcal{A}^{O^{\text{bb}}(\cdot), O^{\text{dh}_0}(\cdot), \dots, O^{\text{dh}_n}(\cdot)}(g) : y = g^{\frac{1}{x_0 + \sum_{i=1}^n x_i m_i^*}} \wedge \right. \\ \left. (m_1^*, \dots, m_n^* \notin Q) \right]. \quad (1)$$

SCDHI is  $(t, \epsilon)$ -hard if no  $t$ -time adversary has advantage at least  $\epsilon$ .

### 4.2 Revocation Scheme

Following the security model defined by (Camenisch et al., 2016), it is required to meet the following properties:

- *Revocation Completeness*: unrevoked users will pass the revocation check.
- *Revocation Soundness*: revoked users will not pass the revocation check.
- *Revocation Privacy*: users will not lose privacy by proving an unrevoked revocation handle.

The revocation scheme is based on the epoch's expiration. In our solution, we set the epoch to one week and define the revocation attribute as follows:  $m_r \leftarrow ww/yyyy$ . When the credentials expire, the user must renew them, allowing weekly access control.

We assume that all users in the system have the date correctly set on their devices. When a user temporarily switches to the verifier role, they can produce the revocation attribute without requiring the user to disclose it.

### 4.3 Location Information

The positioning information is the critical component of the system. We outline the resistance of the protocol against some of the most common attacks that affect the integrity and confidentiality.

*Eavesdropping Attack*: A fraudulent user could monitor the communications and attempt to de-anonymize a legitimate user because the information is sent in plain text. Capturing communications is possible since the information is freely transmitted. However, removing anonymity and attempting to link a specific user to positioning data is extremely difficult. Each time a user transmits the position, the credentials are randomized.

*Replay Attack:* A malicious user could carry out this attack because the information is not altered. But after two seconds, the verifier transmits a new timestamp, invalidating the packet’s authentication. During verification with the new timestamp,  $e \stackrel{?}{=} \mathcal{H}(\dots, timestamp, \dots)$  will produce a different value and the verification will fail.

*Spoofing Attack:* A dishonest user could attempt to impersonate a legitimate user and try to provide fake information to the system. This attack is impractical because a user without valid credentials will be unable to authenticate the data.

*Tampering Attack:* A malicious user could attempt to modify an authenticated packet to alter the positioning of users. This attack is unfeasible because in case  $\lambda$  is modified,  $e \stackrel{?}{=} \mathcal{H}(\dots, \lambda)$  will produce a different value and the verification will fail.

## 5 IMPLEMENTATION RESULTS

In this section, we present the results of the implementation of our protocol on different smartphones. Table 1 shows the hardware and software specifications of the devices used.

Table 1: HW and SW specifications of the smartphones.

| Device                 | CPU                  | OS         | Bluetooth | RAM  |
|------------------------|----------------------|------------|-----------|------|
| Samsung Galaxy S21+ 5G | Exynos 2100          | Android 11 | 5.0 LE    | 8 GB |
| Samsung Galaxy S20 FE  | Exynos 990           | Android 10 | 5.0 LE    | 6 GB |
| Samsung Galaxy A52     | SDM720G              | Android 11 | 5.0 LE    | 6 GB |
| Samsung Galaxy A32     | MTK D720 Dual + Hexa | Android 11 | 5.0 LE    | 4 GB |
| Samsung Galaxy S8      | Exynos 8895          | Android 9  | 5.0 LE    | 4 GB |

We have used elliptic curve cryptography for the implementation and design of the protocol. The implementation is based on the `mcl` cryptographic library (Shigeo, 2018). It allows us to create portable applications between different devices and operating systems and supports the optimal Ate pairing over BN curves. We use the 256-bit Barreto-Naehrig curve (BN254) provided by the library and compiled it using OpenSSL (The OpenSSL Project, 2003) and GMP (Granlund, 2014) as dependencies. We observed in (Hajny et al., 2018) that the GMP library achieves the best performance results for bilinear pairing operations. With this curve size, an uncompressed point occupies 64 bytes and a compressed point 33 bytes. The size of a scalar integer is 32 bytes. To reduce the size of the information, we have considered transmitting the points in their compressed form. Furthermore, we used the OpenSSL library to com-

pute cryptographic hashes. In particular, the SHA-2 function with a digest size of 224 bits.

We have implemented the protocol in C to measure the performance on a RaspberryPi 4. The execution on this device is in the order of  $\mu s$ . The smartphone application has been developed in Java and Kotlin. The Android NDK (Native Development Kit) allows us to implement parts of our app in native code, using languages such as C and C++. This allows us to call the `mcl` library functions through the Java Native Interface (JNI).

Finally, we benchmark the entire protocol without including the communication overhead to evaluate the performance and speed of the algorithms. The results of the execution are shown in Figure 6. We can see the execution of both protocols takes slightly more than 10 ms on the slowest device. During the development we used the Energy Profiler of Android Studio and did not detect an energy consumption impact.

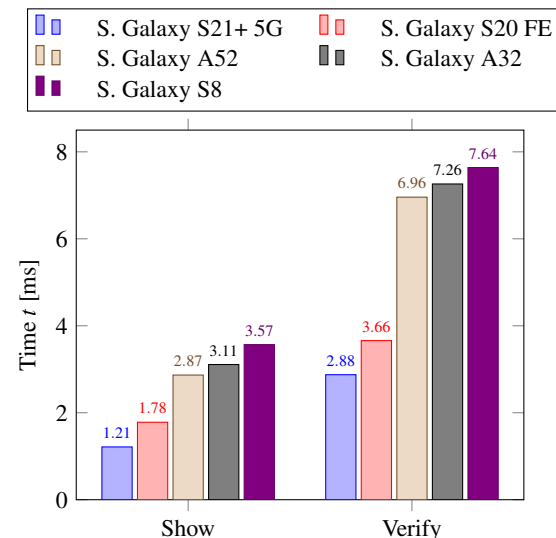


Figure 6: Speed comparison of the Show and Verify algorithms.

## 6 CONCLUSION

Our solution allows sharing anonymous location information in CIPs using BLE advertisement, providing real privacy in a fully decentralized system where sources of data can be trusted. Notwithstanding the relatively limited implementation on constrained devices, this work offers valuable insights into the security and performance of implementing anonymous ABC schemes on CIPs. As far as we know, we present the first fully decentralized scheme running over BLE. Our approach has proven to be efficient on

mobile devices and completely feasible for real-time environments. Next, we plan to improve the protocol to reduce the size of the cryptographic part, improve the revocation scheme, provide information encryption, and start deployment in real environments.

## ACKNOWLEDGMENT

The authors gratefully acknowledge funding from European Union's Horizon 2020 Research and Innovation programme under the Marie Skłodowska Curie grant agreement No. 813278 (A-WEAR, <http://www.a-wear.eu/>) and from Ministry of the Interior of the Czech Republic under grant VJ01030002. J. Torres-Sospedra acknowledges funding from INSIGNIA project (ref. PTQ2018-009981, MICINN).

## REFERENCES

- Arfaoui, G., Lalande, J.-F., Traoré, J., Desmoulins, N., Berthomé, P., and Gharout, S. (2015). A practical set-membership proof for privacy-preserving NFC mobile ticketing. *Proceedings on Privacy Enhancing Technologies*, 2015(2):25–45.
- Barki, A., Brunet, S., Desmoulins, N., and Traoré, J. (2016). Improved algebraic MACs and practical keyed-verification anonymous credentials. In *Proceedings of the 2016 Selected Areas in Cryptography - SAC 2016*.
- Bluetooth SIG (2019). Core specification 5.2. Technical Report 5.2, Bluetooth Special Interest Group.
- Brands, S. A. (2000). *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press, Cambridge, MA, USA.
- Camenisch, J., Drijvers, M., Dzurenda, P., and Hajny, J. (2019). Fast keyed-verification anonymous credentials on standard smart cards. In *IFIP International Conference on ICT Systems Security and Privacy Protection*, pages 286–298. Springer.
- Camenisch, J., Drijvers, M., and Hajny, J. (2016). Scalable revocation scheme for anonymous credentials based on n-times unlinkable proofs. In *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, WPES '16, pages 123–133, New York, NY, USA. ACM.
- Camenisch, J., Kohlweiss, M., and Soriente, C. (2010). Solving revocation with efficient update of anonymous credentials. In Garay, J. A. and De Prisco, R., editors, *Security and Cryptography for Networks*, pages 454–471, Berlin, Heidelberg. Springer Berlin Heidelberg.
- Camenisch, J. and Lysyanskaya, A. (2001). *An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation*, pages 93–118. Springer Berlin Heidelberg, Berlin, Heidelberg.
- Chase, M., Meiklejohn, S., and Zaverucha, G. (2014). Algebraic MACs and keyed-verification anonymous credentials. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 1205–1216, New York, NY, USA. ACM.
- Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Commun. ACM*, 28(10):1030–1044.
- Chebli, M. S., Mohammad, H., and Al Amer, K. (2019). An overview of wireless indoor positioning systems: Techniques, security, and countermeasures. In *International Conference on Internet and Distributed Computing Systems*, pages 223–233. Springer.
- Destiarti, A. R., Kristalina, P., and Sudarsono, A. (2017). Secure data transmission scheme for indoor mobile cooperative localization system. In *2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA)*, pages 50–56. IEEE.
- Granlund, T. (2014). GNU MP: The GNU Multiple Precision Arithmetic Library. <https://gmplib.org>.
- Hajny, J., Dzurenda, P., Ricci, S., Malina, L., and Vrba, K. (2018). Performance analysis of pairing-based elliptic curve cryptography on constrained devices. In *2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 1–5. IEEE.
- Hassidim, A., Matias, Y., Yung, M., and Ziv, A. (2016). Ephemeral identifiers: Mitigating tracking & spoofing threats to ble beacons. [url: https://developers.google.com/beacons/eddystone-eidpreprint.pdf](https://developers.google.com/beacons/eddystone-eidpreprint.pdf) (visited on 06/15/2016).
- Kang, J., Seo, J., and Won, Y. (2018). Ephemeral id beacon-based improved indoor positioning system. *Symmetry*, 10(11):622.
- Khandker, S., Torres-Sospedra, J., and Ristaniemi, T. (2019). Improving rf fingerprinting methods by means of d2d communication protocol. *Electronics*, 8(1):97.
- Mautz, R. (2012). Indoor positioning technologies. *Geodätisch-geophysikalische Arbeiten in der Schweiz*.
- Pascacio, P., Casteleyn, S., Torres-Sospedra, J., Lohan, E. S., and Nurmi, J. (2021). Collaborative indoor positioning systems: A systematic review. *Sensors*, 21(3):1002.
- Ringers, S., Verheul, E. R., and Hoepman, J.-H. (2017). An efficient self-blindable attribute-based credential scheme. *IACR Cryptology ePrint Archive*, 2017:115.
- Shigeo, M. (2018). MCL library: A portable and fast pairing-based cryptography library. <https://github.com/herumi/mcl>.
- The OpenSSL Project (2003). OpenSSL: The Open Source toolkit for SSL/TLS. <https://www.openssl.org>.
- Yang, J., Poellabauer, C., Mitra, P., and Neubecker, C. (2020). Beyond beaconing: Emerging applications and challenges of ble. *Ad hoc networks*, 97:102015.
- Zidek, A., Tailor, S., and Harle, R. (2018). Bellrock: Anonymous proximity beacons from personal devices. In *2018 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 1–10. IEEE.