Extended Diffie-Hellman Encryption for Secure and Efficient Real-Time Beacon Notifications

Liron David, Omer Berkman, Avinatan Hassidim, David Lazarov, Yossi Matias, and Moti Yung

Google Research

Abstract. Every computing paradigm involving communication requires new security protocols employing cryptography. For example, the Internet gave rise to TLS/SSL, and Mobile Computing gave rise to End-to-End Encryption protocols. In this paper, we address an emerging IoT paradigm involving beacons attached to things and security protocols associated with this new configuration.

Specifically, we address the "Beacon Notification Problem," a critical IoT paradigm aimed at providing secure and efficient real-time notifications from beacons to their owners. Since the beacon notification problem has not yet been formally defined, we begin by inspecting natural requirements based on the operational setting and establishing correctness, security, and privacy definitions through the use of cryptographic games.

To resolve the beacon notification problem, we propose a novel cryptographic tool we call XDHIES, which is a considerable extension of available Diffie-Hellman encryption schemes. We then show a new notification protocol built upon XDHIES and we prove that this cryptographic protocol is secure and private and successfully meets all the above problem's requirements.

1 Introduction

The IoT paradigm we address in this paper is the following emerging prototypical information-flow scenario: Assume Alice owns an item with no Internet connection and wishes to receive notifications about the item's status such as temperature, humidity, or battery level as well as notifications from nearby devices such as smartphones in the beacon's vicinity. To enable this, Alice attaches to her item a small broadcasting device, referred to as a beacon, which incorporates the required sensor. This beacon is paired with Alice's mobile phone, which enables the establishment of shared cryptographic keys for secure communication. During operation, the beacon broadcasts its ephemeral ID (EID) along with its status, which is encoded in a quantized format (e.g., low, med, high) using a small number of bits.

A device with IP connection in proximity to the beacon (typically a smartphone, referred to as an "observer") "hears" the beacon's broadcasts and forwards the received information (EID and status) to a cloud server (i.e., a typical app cloud server), along with its own message (e.g., its geo location), see Figure 1. The owner of this beacon should be promptly notified with both the beacon's status and the observer's message as soon as the data is received by the cloud server. In other words, the owner should receive its beacon's notifications in real-time.

We motivate the above scenario with the following two applications:

(1) Location-tracking A person traveling by plane wishes to track in real-time the location and temperature of its suitcase. The suitcase location may be important in case the suitcase gets lost and its temperature may be vital if the suitcase contains items sensitive to temperature extremes. To this end, the owner attaches a beacon with a temperature sensor to the suitcase and an observer adds its geo-location before forwarding the resulting notification to the owner (through the cloud server). The beacon's status (namely, its temperature) and the observer's location should remain private, allowing only the owner to track its suitcase and find out its status.

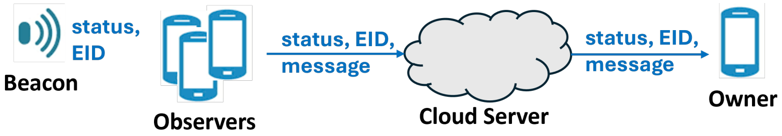

Fig. 1: The beacon notification configuration in IoT

(2) Proximity-based auction An anonymous donor has provided a valuable piece to a gallery for auction and desires (or is legally required) to limit real-time bids to individuals who can physically view and evaluate the piece. To facilitate this, the donor places a beacon next to the artwork, enabling observers in proximity to receive the beacon's broadcast, piggyback their bids and send the resulting notification to the owner (again, through the cloud server). It is imperative that bidders, submitted bids and the auction winner remain confidential. Here, the beacon's status may convey information about the temperature or humidity surrounding the piece to ensure that it is maintained within safe environmental conditions. This scenario may require a secure bi-directional connection to enable back-and-forth communication between bidders and the owner. While our beacon notification protocol can be easily extended to accommodate bi-directional communication, in this paper we focus on the uni-direction bidding case only.

1.1 Security, Privacy, and Integrity Requirements

To achieve secure and efficient notifications, we specifically require that a beacon notification protocol achieves the notions of security, privacy, and integrity described below.

- Security: (1) End-to-End security (beacon to owner) for the beacon's status; (2) End-to-End security (observer to owner) for any past and future messages from an observer near a beacon, even if this beacon's keys are compromised. This is referred to as "Perfect Backward and Forward Security."
- Privacy: Any beacon's broadcast must be pseudorandom and ephemeral to prevent tracking.
- Integrity: An observer should be able to verify that a received beacon's broadcast is valid before piggybacking its own secure message and forwarding both to the cloud server.

Beacons are the 'weak-link' in the system since they are

- More exposed to attacks: Beacons often operate far from their owners for extended periods, sometimes weeks or even months, making them vulnerable to physical attacks. In such attacks, adversaries could gain access to the beacon's secret keys, enabling them to decrypt any past and future messages from observers in the beacon's vicinity.
- Easier to compromise: Compromising the owner's system-side MANET (Mobile Ad-Hoc Network) component is a much more challenging task for attackers compared to breaching a user-controlled space.
- Undetectable when compromised: Unlike modern smartphones which can typically detect jailbreaking attempts, the owner cannot detect if its beacon has been compromised.

Therefore, it is important to ensure that even if the beacon is compromised, the security of any past and future messages from observers in its proximity remain protected. In other words, achieving perfect backward and forward security, as defined above, is crucial for maintaining the overall security of beacon-based applications.

Integrating the Protocol with Anti-Stalking Efforts Our protocol is designed to achieve end-to-end security while ensuring both privacy and integrity. An additional key concern with such beacon technology is the ability to abuse the system to track individuals without their consent (stalking). To address this, Apple and Google have implemented **anti-abuse measures** that strike a balance between privacy and protection against such threats [2].

Specifically, these measures involve incorporating a random identifying field in the beacon's broadcast: When the beacon is in proximity to its owner, the field remains randomized; however, if the beacon is separated from its owner for an extended period, the field becomes fixed. Fixing this field allows the (phone of a) subject who is under attack of stalking to detect the malicious beacon in its vicinity. These measures also include security mechanisms which are beyond the scope of this paper, to ensure that only certified beacons can onboard the service, with the ability to revoke them if they fail to adhere to the protocol.

These anti-abuse measures can be integrated into our beacon notification protocol as well. While these measures introduce a trade-off by reducing the beacon's privacy, they maintain all other security and integrity requirements. The goal of this paper is to present a protocol that satisfies all desired properties (while allowing privacy to be selectively relaxed as a countermeasure against abuse when necessary).

1.2 The State of the Art

Prior to the protocol introduced in this paper, the only protocol that achieved end-to-end secure beacon-location tracking, was the Apple's FindMy protocol [13]. However, the FindMy protocol does not adhere to our framework. Specifically, FindMy

1. does not support beacon status notifications (and clearly not their security);
2. does not provide perfect backward and forward security for messages from observers near a compromised beacon;
3. does not support efficient real-time communication. By 'real-time' communication, we mean that the owner should receive data as soon as it is available on the cloud server;
4. does not guarantee integrity;
5. and exposes the system to security attacks such as [7,5] (more details on these attacks in Section 10).

Apple's FindMy is built upon a pseudorandom version of DHIES [3] which we refer to as PR-DHIES. In this version, the PR-DHIES private key is an ephemeral pseudorandom value derived from a secret key shared between a beacon and its owner (and a nonce synchronized between the two). The beacon in FindMy broadcasts the (ephemeral and pseudorandom) public key corresponding to the PR-DHIES private key. Nearby observers encrypt their messages using this public key. The owner, using the secret key shared with its beacon, generates the corresponding PR-DHIES private key and decrypts the observers' messages.

1.3 Our New Cryptographic Scheme and Protocol

While PR-DHIES is sufficient for Apple's FindMy security requirements, it is insufficient for the stronger security and operational requirements of our beacon notification problem. In particular, to satisfy our security, privacy, and integrity requirements we develop a new cryptographic scheme and a new protocol. Our goal is to achieve the following objectives:

Adding Beacon's Status Input Simply appending a secure status to the beacon's broadcast (i.e., to the PR-DHIES public key) would increase the beacon's broadcast size. This is extremely undesirable as we explain below.

A beacon is power-consumption limited and operates on a coin-cell battery which should last a year or two. Since long messages deplete the beacon's battery, and in order to allow the system to rely on devices using BLE version 4 in which transmission length is extremely limited, the beacon's broadcast should be short.

Additionally, broadcasting a single long message by dividing it to multiple short frames is also undesired for two additional main reasons which deal with the system overall utility: First, due to the beacon's power limitations, it is designed to broadcast only once every 1-2 seconds, meaning that observers who are briefly in proximity to the beacon may miss some of the frames (and therefore the entire message). Second, to conserve observers' batteries when their screens are off, observers typically scan for beacon messages only periodically. As a result, fragmented messages greatly increase the chance that observers miss some of the frames.

Hence the beacon's broadcast should be a short non-fragmented message. To enable the beacon to securely broadcast its status without increasing its broadcast's length, we propose extending PR-DHIES to support a status input, so that the status encryption be integrated into the PR-DHIES broadcast public key without increasing the public-key's length.

Adding Perfect Backward and Forward Security PR-DHIES does not provide perfect backward and forward security: if the secret key shared between the beacon and its owner is exposed then so are the PR-DHIES private keys generated from this key, allowing the adversary to decrypt all the messages generated by observers in the beacon's vicinity.

To limit the time window in which the adversary can decrypt messages, periodic re-pairing to refresh the shared secret key between the owner and its beacon can be used. However, this approach does not guarantee perfect backward and forward security. An adversary who compromises the beacon's secret key can decrypt all messages from observers near the beacon during the period between the previous and the next re-pairing events. The time between re-pairing events in some applications may be long, as the owner and beacon could be separated for extended periods, leaving a long window of time during which an adversary could potentially decrypt past and future messages within the window.

The beacon and its owner may periodically apply a one-way function to update their shared secret key during the time window between two re-pairing events. However, this approach still does not guarantee perfect backward and forward security: An adversary who compromises the beacon's secret key can still decrypt all future messages during this time window (as the output of a one-way function applied to a known secret remains computable by the adversary). Additionally, the adversary can decrypt all past messages generated since the last key update.

Thus, to guarantee the security of **all** past and future messages encrypted with beacon PR-DHIES public keys, we further extend PR-DHIES. This allows us to achieve perfect backward and forward security without increasing the length of the PR-DHIES public key broadcast.

Adding Efficient Real-Time Operation and Integrity To enhance privacy with respect to the server, FindMy is designed so that the server cannot link beacon notifications to their respective owners. As a result, owners must actively query the server to retrieve notifications from their beacons. However, this polling-based approach is not conducive to efficient real-time communication.

Frequent queries intended to approximate real-time updates can generate substantial communication overhead as well as significantly increased power consumption on the owner's device, potentially discouraging continued use of the service. Moreover, this design choice introduces vulnerabilities to various security attacks, such as those demonstrated in [7,5].

This motivates the need for an alternative cloud server routing mechanism, where the server forwards messages from observers directly to the intended owners. While such an alternative approach may momentarily reveal the intended owner of each message, the server retains this information only briefly, hence the violation of privacy relative to the server is minimized. Such an approach must also ensure the integrity of the public keys used by observers.

1.4 Contributions

Our central technical contribution is XDHIES, a novel considerable extension of DHIES which integrates a status input and provides inherent perfect backward and forward security for any past and future message encrypted using the XDHIES broadcast public key. Building on XDHIES, we propose a beacon notification protocol with a new routing scheme inspired by Eddystone-EID [10]. Unlike FindMy, our routing ensures integrity, enables efficient real-time communication, and mitigates security attacks [7,5]. Finally (and, again, unlike FindMy), we prove that our new beacon notification protocol meets the security, privacy, and integrity requirements.

The beacon notification protocol was applied to real-world products. As this is a cryptographic design paper, our focus is on the theoretical analysis that led to the development of this product. Specifically, we concentrate on formally defining the problem and its security requirements based on engineering specifications, designing the cryptographic solution, proving its properties, and conducting a time-and-complexity analysis, as is standard in cryptographic research (the analysis was reflected in the experiments conducted by the engineering team, which is an issue out of the scope of this work).

2 Threat Model and Requirements

In this section, we formally define the beacon notification problem, along with its associated correctness, security, privacy, and integrity requirements. These requirements are carefully derived from the discussion above regarding the emerging new IoT setting.

2.1 Problem Definition

As described above, the beacon notification problem aims at forwarding both a status from a beacon and a message from an observer in this beacon's vicinity to the beacon's owner. The notification, therefore, includes both the beacon's status and the observer's message. Let t_b be the system's starting time and let t_e be the system ending time. We assume that the system's lifetime $t_e - t_b$ is polynomial in the security parameter n. In addition, let S be the set of all possible status messages.

Next we formally define the Beacon Notification Problem. Let

$$\mathsf{BcnNtf} = (\mathsf{Init}, \{\mathsf{Bcn_i}\}_{\mathsf{i}=1}^{\mathsf{w}}, \mathsf{Obs}, \mathsf{Svr}, \{\mathsf{Own_i}\}_{\mathsf{i}=1}^{\mathsf{w}})$$

be a set of probabilistic polynomial-time algorithms. Specifically,

- The `initialization algorithm` Init takes as input a security parameter 1^n and a parameter 1^w indicating the number of owners in the system (for simplicity of presentation we assume that this number is known a priory), and outputs cryptographic parameters: (1) $\mathcal{K}_i$ intended for beacon i for each $i \in [1, w]$; (2) $\mathcal{K}'_i$ intended for owner i for each $i \in [1, w]$; and (3) $\mathcal{M}$ intended to the cloud server ($\mathcal{M}$ stands for a mapping table as will be described later).
- The `operation algorithm` which is a collection of events, each being an instance of one of the following atomic algorithms:
  - The *i*`'th beacon's algorithm` Bcn_i takes as input a time $t \in [t_s, t_e]$ and a status $s \in S$, and outputs its broadcast
  $$\mathsf{Bcn}_i(t, s).$$
  - An `observer` Obs takes as input a beacon's output x (which is expected to be $\mathsf{Bcn}_i(t, s)$ for some i, t and s) and a message m, and outputs
  $$\mathsf{Obs}(x, m).$$
  - The `cloud server algorithm` Svr takes as input an observer's output y (which is expected to be $\mathsf{Obs}(\mathsf{Bcn}_i(t, s), m)$ for some i, t, s and m) and outputs the index of the beacon that initiated y
  $$\mathsf{Srv}(y) := i.$$
  The cloud server then delivers y to the i'th owner.
  - The *i*`'th owner's algorithm` Own_i takes as input the cloud server's output y (which is expected to be $\mathsf{Obs}(\mathsf{Bcn}_i(t, s), m)$ for some t, s and m) and outputs
  $$\mathsf{Own}_i(y) := s, m.$$

2.2 Security

Beacon's status CCA-security Informally, we require that an adversary who can observe both a beacon's outputs and observers' outputs, and who has read-access to the cloud server data, would be unable to expose the beacon's status messages. Formally,

Definition 1. *(Beacon's status CCA-security) Let $i \in [1, w]$ be a beacon, let $\mathsf{Bcn} := \mathsf{Bcn}_i$, let $\mathsf{Own} := \mathsf{Own}_i$, and let $\mathcal{A}$ be an adversary in the following game $Exp^{CCA}_{BcnStat,\mathcal{A}}(n)$:*

- *Adversary $\mathcal{A}$ receives access to: (1) $\mathcal{M}$ (the cloud server's security parameter), (2) the beacon oracle $\mathsf{Bcn}()$, and (3) the owner oracle $\mathsf{Own}()$.*
- *Adversary $\mathcal{A}$ chooses two status messages s_0, s_1 and time t_c such that t_c is distinct from all times t in the queries to $\mathsf{Bcn}()$ and $\mathsf{Own}()$ that adversary $\mathcal{A}$ has already made. It then sends t_c, s_0, s_1 to the challenger.*
- *The challenger chooses a random bit $b \in \{0, 1\}$ and returns $x = \mathsf{Bcn}(t_c, s_b)$ to adversary $\mathcal{A}$.*
- *Adversary $\mathcal{A}$ continues to have access to $\mathcal{M}$ and the oracles as before, where: (1) the parameter t for any call to $\mathsf{Bcn}()$ must be distinct from t_c; and (2) $\mathsf{Own}()$ cannot be queried with $y = \mathsf{Obs}(x, m)$ for any m (that is, we do not allow to decrypt the challenge x).*
- *Adversary $\mathcal{A}$ returns b' and wins if $b' = b$.*

We say that BcnNtf achieves beacon's status CCA-security if for any PPT adversary $\mathcal{A}$ there exists a negligible function negl such that

$$\Pr[Exp^{CCA}_{BcnStat,\mathcal{A}}(n) = 1] \leq \frac{1}{2} + negl(n).$$

Observer's message CCA-security with perfect backward and forward security Informally, we require that an adversary who can observe both a beacon's outputs and observers' outputs, has read-access to the cloud server data, and possesses knowledge of the beacon's secret keys, would be unable to expose any past/current/future messages from observers generated by this beacon's output. Note that providing an adversary with access to the beacon's secret keys is required to assure perfect backward and forward security. Formally,

Definition 2. *(Observer's message CCA-security with perfect backward and forward security) Let* $i \in [1, w]$ *be a beacon, let* $\mathsf{Bcn} := \mathsf{Bcn}_i$*, let* $\mathsf{Own} := \mathsf{Own}_i$*, and let* $\mathcal{A}$ *be an adversary in the following game* $Exp^{CCA}_{ObsMsg,\mathcal{A}}(n)$*:*

- *Adversary* $\mathcal{A}$ *receives access to: (1)* $\mathcal{M}$ *(the cloud server's security parameter), (2) the beacon's keys* $\mathcal{K}$ *(the compromised beacon's secrets for perfect backward and forward security), and (3) the owner oracle* $\mathsf{Own}()$*.*
- *Adversary* $\mathcal{A}$ *chooses a desired time* t_c*, a status* s*, and two distinct messages* $m_0 \neq m_1$*. It then sends* t_c, s, m_0, m_1 *to the challenger.*
- *The challenger chooses a random bit* $b \in \{0, 1\}$ *and returns*

$$y = \mathsf{Obs}(\mathsf{Bcn}(t_c, s), m_b)$$

  to adversary $\mathcal{A}$*.*
- *Adversary* $\mathcal{A}$ *continues to have access to (1), (2) and (3) above, but cannot query* $\mathsf{Own}()$ *oracle with* y*.*
- *Adversary* $\mathcal{A}$ *returns* b' *and wins if* $b' = b$*.*

We say that BcnNtf *achieves observer's message CCA-security with perfect backward and forward security if for any PPT adversary* $\mathcal{A}$ *there exists a negligible function negl such that*

$$\Pr[Exp^{CCA}_{ObsMsg,\mathcal{A}}(n) = 1] \leq \frac{1}{2} + negl(n).$$

2.3 Privacy

Informally, we require that an adversary observing the outputs of a beacon, would be unable to distinguish these outputs from random values. Formally,

Definition 3. *(Beacon's Indistinguishability) Let* $i \in [1, w]$ *be a beacon, let* $\mathsf{Bcn} := \mathsf{Bcn}_i$*, and let* $\mathcal{A}$ *be an adversary in the following game* $Exp_{BcnInd,\mathcal{A}}(n)$*:*

- *The challenger chooses a random bit* b*.*
- *If* $b = 0$*, the beacon's oracle* $\mathsf{Bcn}()$ *remains unchanged; otherwise if* $b = 1$ *then* $\mathsf{Bcn}()$ *is replaced with a random function* Rand *which returns random values in the range of* $\mathsf{Bcn}()$*.*
- *Adversary* $\mathcal{A}$ *guesses* b' *and wins if* $b' = b$*.*

We say that BcnNtf *achieves beacon's indistinguishability if for any PPT adversary as above there exists a negligible function negl such that*

$$\Pr[Exp_{BcnInd,\mathcal{A}}(n) = 1] \leq \frac{1}{2} + negl(n).$$

2.4 Unforgeability

Informally, we require that the cloud server is unable to forge a valid beacon's broadcast despite the fact that it is equipped with the means of recognizing valid beacon broadcasts. Since beacon broadcasts are pseudorandom this, in turn, means that the cloud server cannot generate valid observer messages. Formally,

Definition 4. *(Beacon's Broadcast Unforgeability) Let $i \in [1, w]$ be a beacon, let $\mathsf{Bcn} := \mathsf{Bcn}_i$, and let $\mathcal{A}$ be an adversary in the following game $Exp_{BcnFrg,\mathcal{A}}(n)$:*

- *Adversary $\mathcal{A}$ receives read-access to $\mathcal{M}$.*
- *Adversary $\mathcal{A}$ wins if succeeds to generate $\mathsf{Bcn}(t, s)$ for some t and s.*

We say that BcnNtf *achieves beacon's broadcast unforgeability if for any PPT adversary $\mathcal{A}$ there exists a negligible function negl such that*

$$\Pr[Exp_{BcnFrg,\mathcal{A}}(n) = 1] \leq negl(n).$$

2.5 Integrity

Informally, we require that an observer is able to verify the reliability of a received beacon's broadcast before using it to encrypt its message. That is, we require that an adversary with access to beacons' outputs, observers' outputs, and read-access to the cloud server data, will be unable to generate a value which is not a valid output of any beacon, but yet the observer accepts it. Formally,

Definition 5. *(Beacon's Integrity) Let $\mathcal{A}$ be an adversary in the following game $Exp_{BcnInt,\mathcal{A}}(n)$:*

- *Adversary $\mathcal{A}$ receives access to: (1) $\mathcal{M}$, (2) beacon's oracle $\mathsf{Bcn}_i()$ for any $i \in [1, w]$, and (3) owner's oracle $\mathsf{Own}_i()$ for any $i \in [1, w]$.*
- *Adversary $\mathcal{A}$ generates v and wins if (1) there does not exist i, t, s such that $v = \mathsf{Bcn}_i(t, s)$; and (2) $\mathsf{Obs}(v, m) \neq \perp$ for any m.*

We say that BcnNtf *achieves beacon's integrity if for any PPT adversary $\mathcal{A}$ there exists a negligible function negl such that*

$$\Pr[Exp_{BcnInt,\mathcal{A}}(n) = 1] \leq negl(n).$$

2.6 Correctness

Definition 6. *(*BcnNtf *correctness) It is required that for every $i \in [1, w]$, time $t \in [t_s, t_e]$, status $s \in S$, and message m*

$$(s, m) = \mathsf{Own}_{\mathsf{Svr}(\mathsf{Obs}(\mathsf{Bcn}_i(t,s),m))}(\mathsf{Obs}(\mathsf{Bcn}_i(t, s), m)).$$

3 Background: DHIES and Preliminaries

Our protocol extends the Diffie-Hellman public encryption scheme DHIES [3]. In this section we describe DHIES and its security and then describe the pseudo-random version of DHIES, we call PR-DHIES.

Definition 7. *(Group Generator) Let* $\mathsf{GroupGen}$ *be a probabilistic polynomial-time (PPT) algorithm that, on a security parameter input* 1^n*, outputs a description of a cyclic group* $\mathbb{G}$*, its prime order* q*, and a generator* $g \in \mathbb{G}$*. Run* $\mathsf{GroupGen}(1^n)$ *to obtain the public parameters* $(\mathbb{G}, q, g)$*.*

Definition 8. *(DHIES [3]) Let* $\mathsf{SYM} = (\mathcal{E}, \mathcal{D})$ *be a private-key authenticated-encryption scheme. We run* $\mathsf{GroupGen}(1^n)$ *to obtain* $(\mathbb{G}, q, g)$*. Let* KDF *be a key derivation function* $\mathsf{KDF} : \mathbb{G} \to \{0,1\}^n$*.* $\mathsf{DHIES} = (\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ *is the following three-tuple of algorithms defining public-key encryption:*

- $\overline{\mathcal{K}}$*: Chooses a uniform* $x \in \mathbb{Z}_q$*, sets the private key* $sk = x$ *intended for the decryption function* $\overline{\mathcal{D}}_{sk}$*, and outputs the public key* $pk = g^{sk}$*.*
- $\overline{\mathcal{E}}_{pk}(m)$*: Chooses a uniform* $z \in \mathbb{Z}_q$*, computes* g^z *and sets* $k = \mathsf{KDF}((pk)^z)$*. Computes* $c = \mathcal{E}_k(m)$ *and outputs* (g^z, c)*.*
- $\overline{\mathcal{D}}_{sk}(\hat{c}, c)$*: Returns* $\perp$ *if* $\hat{c} \notin \mathbb{G}$*. Else sets* $k = \mathsf{KDF}((\hat{c})^{sk})$*. If authentication succeeds it returns* $m = \mathcal{D}_k(c)$*, else returns* $\perp$*.*

Definition 9. *(negligible) A function* f *from the natural numbers to the non-negative real numbers is negligible if for every positive polynomial* p *there exists an* N_0 *such that for all integers* $n > N_0$ *it holds that* $f(n) < 1/p(n)$*.*

Throughout the paper, we chose a security parameter n which will determine the suitable space of keys and will be suitable for the desired security definition of all cryptographic functions.

Definition 10. *(Oracle Diffie-Hellman Assumption ODH [3]) Run* $\mathsf{GroupGen}(1^n)$ *to obtain* $(\mathbb{G}, q, g)$*, let* $\mathsf{KDF} : \mathbb{G} \to \{0,1\}^n$*, and for* $w \in \mathbb{Z}_q$ *let* $\mathsf{KDF}_w(X) := \mathsf{KDF}(X^w)$*. The ODH assumption is the following: For any PPT adversary* $\mathcal{A}$*, there exists a negligible function negl such that*

$$\begin{aligned}
&\Pr[u \xleftarrow{R} \mathbb{Z}_q; v \xleftarrow{R} \mathbb{Z}_q; \mathcal{A}^{\mathsf{KDF}_v(\cdot)}(g^u, g^v, \mathsf{KDF}(g^{uv})) = 1] \\
&- \Pr[u \xleftarrow{R} \mathbb{Z}_q; v \xleftarrow{R} \mathbb{Z}_q; \mathcal{A}^{\mathsf{KDF}_v(\cdot)}(g^u, g^v, \{0,1\}^n) = 1] \\
&\le negl(n).
\end{aligned}$$

Definition 11. *(*$Exp^{CCA}_{ASYM,\mathcal{A}}(n)$*) Let* $\mathcal{A}$ *be an adversary in the following game* $Exp^{CCA}_{ASYM,\mathcal{A}}(n)$*:*

- *The challenger randomly chooses a private key* $sk = r \in \mathbb{Z}_q$ *and sends the public key* $pk = g^r$ *to adversary* $\mathcal{A}$*.*
- *Adversary* $\mathcal{A}$ *has access to the decryption oracle* $\overline{\mathcal{D}}_{sk}(\cdot,\cdot)$*.*
- *Adversary* $\mathcal{A}$ *sends to the challenger two distinct messages* $m_0 \neq m_1$*.*
- *The challenger chooses a random bit* $b \in \{0,1\}$ *and sends* $y = \overline{\mathcal{E}}_{pk}(m_b)$ *to adversary* $\mathcal{A}$*.*
- *Adversary* $\mathcal{A}$ *continues to have access to the decryption oracle as before, but it cannot apply the decryption oracle on* y*.*
- *Adversary* $\mathcal{A}$ *returns* b' *and wins if* $b' = b$*.*

We say that ASYM achieves CCA-security if for any PPT adversary $\mathcal{A}$ *there exists a negligible function negl such that*

$$\Pr[Exp^{CCA}_{ASYM,\mathcal{A}}(n) = 1] \le \frac{1}{2} + negl(n).$$

Theorem 1. *[3] If the Oracle Diffie-Hellman (ODH) assumption holds and the private-key authenticated-encryption scheme* SYM *used in* DHIES *is CCA-secure, then* DHIES *is CCA-secure.*

Proof. In [3].

Definition 12. *(Pseudorandom Function (PRF)) Let* PRF *be a keyed function* $\mathsf{PRF} : \{0,1\}^n \times \{0,1\}^* \to \mathbb{Z}_q^*$ *where the first parameter is the key and* q *is a parameter. For a key* k*, we denote* $\mathsf{PRF}(k,t)$ *by* $\mathsf{PRF}_k(t)$*. We say that* PRF *is a pseudorandom function if for all polynomial time distinguishers* D *there exists a negligible function* $negl$ *such that*

$$\left|\Pr[D^{\mathsf{PRF}_k(\cdot)}(1^n) = 1] - \Pr[D^{\mathsf{Rand}(\cdot)}(1^n) = 1]\right| \leq negl(n),$$

where Rand *is a random function of the same domain and range as* PRF*.*

3.1 PR-DHIES: Pseudorandom DHIES

In the DHIES protocol a random private key sk is utilized. However, this approach is not sufficient in our context: In the beacon notification problem, privacy concerns dictate that a beacon's broadcasts look to an eavesdropper independent from one another. Since a beacon's public key pk is used to encrypt messages to the beacon's owner, the beacon cannot independently select a random sk and broadcasts the corresponding pk. Instead, as is the case in the FindMy protocol, a pseudo-random version of DHIES is utilized in the beacon scenario. In this version, the beacon and its owner share a (symmetric) secret key x, and sk is generated based on a pseudo-random function of a shared nonce (in our case the current time t) keyed with x. This ensures that a beacon and its owner can independently generate the same private key sk.

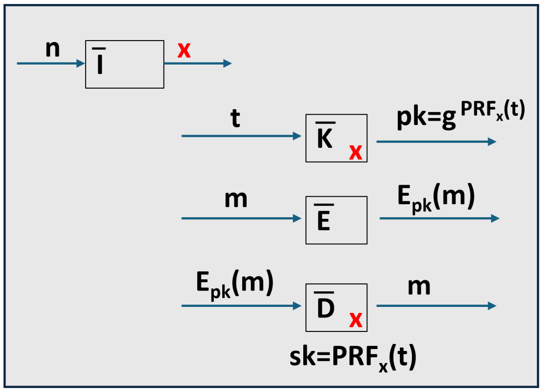

Fig. 2: PR-DHIES

This pseudo-random DHIES, which we denote "PR-DHIES", is defined as follows (see Figure 2):

Definition 13. *(PR-DHIES) Let* $\mathsf{SYM} = (\mathcal{E}, \mathcal{D})$ *be a private-key authenticated-encryption scheme. We run* $\mathsf{GroupGen}(1^n)$ *to obtain* $(\mathbb{G}, q, g)$*. Let* KDF *be a key derivation function* $\mathsf{KDF} : \mathbb{G} \to \{0,1\}^n$*.* $\mathsf{DHIES} = (\overline{\mathcal{I}}, \overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ *is the following four-tuple of algorithms defining public-key encryption:*

- $\overline{\mathcal{I}}(n)$*: Chooses a uniform* $x \in \{0,1\}^n$ *intended for both the key-generation function* $\overline{\mathcal{K}}_x$ *and the decryption function* $\overline{\mathcal{D}}_x$*.*
- $\overline{\mathcal{K}}_x(t)$*: Sets the private key* $sk_t = \mathsf{PRF}_x(t)$ *and outputs the corresponding public key* $pk_t = g^{sk_t}$*.*

- $\overline{\mathcal{E}}_{pk_t}(m)$: *Chooses a uniform* $z \in \mathbb{Z}_q$, *computes* g^z *and sets* $k = \mathsf{KDF}((pk_t)^z)$. *Computes* $c = \mathcal{E}_k(m)$ *and outputs* (g^z, c).
- $\overline{\mathcal{D}}_x(t, (\hat{c}, c))$: *Returns* $\perp$ *if* $\hat{c} \notin \mathbb{G}$. *Else sets* $sk_t = \mathsf{PRF}_x(t)$ *and* $k = \mathsf{KDF}((\hat{c})^{sk_t})$. *Returns* $m = \mathcal{D}_k(c)$ *if authentication succeeds, and* $\perp$ *otherwise.*

Notice that the framework of public key encryption implemented by PR-DHIES is of the form $(\overline{\mathcal{I}}, \overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ rather than the normal $(\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ framework. Specifically, this framework could be defined as follows:

Definition 14. *(Pseudorandom Public-Key Encryption) The framework consists of the following four probabilistic polynomial-time algorithms* $(\overline{\mathcal{I}}, \overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$:

- $\overline{\mathcal{I}}(n)$: *the initialization function* $\overline{\mathcal{I}}$ *takes a security parameter* n *and generates a secret key* $x \in \{0,1\}^n$.
- $\overline{\mathcal{K}}_x(t)$: *the key-generation function* $\overline{\mathcal{K}}_x$ *takes a time parameter* t *and returns a pseudorandom public key* pk_t.
- $\overline{\mathcal{E}}_{pk_t}(m)$: *the encryption function* $\overline{\mathcal{E}}_{pk_t}$ *takes a message* m *and returns its encryption.*
- $\overline{\mathcal{D}}_x(t, c)$: *the decryption function* $\overline{\mathcal{D}}_x$ *takes an encryption* c, *a time parameter* t, *and decrypts it to get the respective* m.

The pseudorandom public-key encryption framework fails to meet two crucial requirements for beacons:

1. While such a framework allows a beacon to generate and broadcast a pseudorandom public key, it does not support additional inputs. This would force the beacon to broadcast its beacon status (in encrypted form) alongside the public key thus increasing the broadcast length. However, as discussed in the introduction, this is highly undesirable, as the beacon's broadcast should be short and unfragmented.
2. The framework does not support perfect backward and forward security. That is, if an adversary reveals the beacon's secret x, it can calculate the corresponding PR-DHIES private keys sk_t for all past and future values of t and can therefore decrypt any past and future messages. However, as discussed in the Introduction, achieving perfect backward and forward security is crucial in our beacon scenario.

We next define a new pseudorandom public-key encryption framework which extends the above $(\overline{\mathcal{I}}, \overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ framework to address the missing requirements. We then establish the new framework's security criteria.

4 Extended Pseudorandom Public-Key Encryption Framework

We formally define the new framework and subsequently establish its security requirements.

4.1 Defining the Extended Framework

Definition 15. *(Extended Pseudorandom Public-Key Encryption) The new framework consists of the four probabilistic polynomial-time algorithms* $(\overline{\mathcal{I}}, \overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$:

- $\overline{\mathcal{I}}(n)$: *the initialization function* $\overline{\mathcal{I}}$ *takes a security parameter* n *and generates two sets of random keys* $\mathcal{K}$ *and* $\mathcal{K}'$, *where* $\mathcal{K}$ *is intended to the key-generation function and* $\mathcal{K}'$ *is intended to the decryption function.*

- $\overline{\mathcal{K}}_{\mathcal{K}}(t,s)$*: the key-generation function* $\overline{\mathcal{K}}_{\mathcal{K}}$ *takes a time parameter* t *and a small domain parameter* s*, and returns a pseudorandom public key* $pk_{t,s}$ *which incorporates the encryption of* s*.*
- $\overline{\mathcal{E}}_{pk_{t,s}}(m)$*: the encryption function* $\overline{\mathcal{E}}_{pk_{t,s}}$ *takes a message* m *and returns its encryption.*
- $\overline{\mathcal{D}}_{\mathcal{K}'}(c)$*: the decryption function* $\overline{\mathcal{D}}_{\mathcal{K}'}$ *takes an encryption* c*, and decrypts it to get the respective* s *and* m*.*

4.2 Defining the Framework's Security

Definition 16. *(*$Exp^{s\text{-}CCA}_{ASYM,\mathcal{A}}(n)$*) Let* $\mathsf{ASYM} = (\overline{\mathcal{I}}, \overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ *be an extended pseudorandom public-key encryption scheme and let* $\mathcal{A}$ *be an adversary in the following game* $Exp^{s\text{-}CCA}_{ASYM,\mathcal{A}}(n)$*:*

- *The challenger randomly chooses* $\mathcal{K}, \mathcal{K}'$*.*
- *Adversary* $\mathcal{A}$ *has access to both the key-generation oracle* $\overline{\mathcal{K}}_{\mathcal{K}}(\cdot,\cdot)$ *and the decryption oracle* $\overline{\mathcal{D}}_{\mathcal{K}'}(\cdot)$*.*
- *Adversary* $\mathcal{A}$ *chooses two distinct messages* $s_0 \neq s_1$ *and* $t_c \in [t_s, t_e]$ *such that* t_c *is distinct from all values of* t *used in the queries above. It then sends* t_c, s_0, s_1 *to the challenger.*
- *The challenger chooses a random bit* $b \in \{0,1\}$ *and sends* $pk_{t_c,s_b} = \overline{\mathcal{K}}_{\mathcal{K}}(t_c, s_b)$ *to adversary* $\mathcal{A}$*.*
- *Adversary* $\mathcal{A}$ *continues to have access to both* $\overline{\mathcal{K}}_{\mathcal{K}}(\cdot,\cdot)$ *and* $\overline{\mathcal{D}}_{\mathcal{K}'}(\cdot)$ *as before, where: (1) the parameter* t *for any call must be distinct from* t_c*; and (2) the decryption oracle cannot be queried with* $y = \overline{\mathcal{E}}_{pk_{t_c,s_b}}(m)$ *for any* m *(that is, we do not allow to decrypt the challenge* pk_{t_c,s_b}*).*
- *Adversary* $\mathcal{A}$ *returns* b' *and wins if* $b' = b$*.*

We say that ASYM achieves s-CCA security if for any PPT adversary $\mathcal{A}$ *there exists a negligible function negl such that*

$$\Pr[Exp^{s\text{-}CCA}_{ASYM,\mathcal{A}}(n) = 1] \leq \frac{1}{2} + negl(n).$$

Definition 17. *(*$Exp^{m\text{-}CCA}_{ASYM,\mathcal{A}}(n)$*) Let* $\mathsf{ASYM} = (\overline{\mathcal{I}}, \overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ *be an extended pseudorandom public-key encryption scheme and let* $\mathcal{A}$ *be an adversary in the following game* $Exp^{m\text{-}CCA}_{ASYM,\mathcal{A}}(n)$*:*

- *The challenger randomly chooses* $\mathcal{K}$ *and* $\mathcal{K}'$*.*
- *Adversary* $\mathcal{A}$ *has access to* $\mathcal{K}$ *(the compromised secret keys for perfect backward and forward security). It also has access to the decryption oracle* $\overline{\mathcal{D}}_{\mathcal{K}'}(\cdot)$*.*
- *Adversary* $\mathcal{A}$ *chooses* t_c*, a short domain message* s_c*, and two distinct messages* $m_0 \neq m_1$ *and sends* t_c, s_c, m_0, m_1 *to the challenger.*
- *The challenger calculates* $pk_{t_c,s_c} = \overline{\mathcal{K}}_{\mathcal{K}}(t_c, s_c)$*, chooses a random bit* $b \in \{0,1\}$*, and returns*

$$y = \overline{\mathcal{E}}_{pk_{t_c,s_c}}(m_b)$$

  to adversary $\mathcal{A}$*.*
- *Adversary* $\mathcal{A}$ *continues to have access to all oracles and keys as above, but cannot query the decryption oracle with* y*.*
- *Adversary* $\mathcal{A}$ *returns* b' *and wins if* $b' = b$*.*

We say that ASYM achieves m-CCA security with perfect backward and forward security if for any PPT adversary $\mathcal{A}$ *there exists a negligible function negl such that*

$$\Pr[Exp^{m\text{-}CCA}_{ASYM,\mathcal{A}}(n) = 1] \leq \frac{1}{2} + negl(n).$$

Definition 18. *($Exp^{Ind}_{ASYM,\mathcal{A}}(n)$) Let* $\mathsf{ASYM} = (\overline{\mathcal{I}}, \overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ *be an extended pseudorandom public-key encryption scheme and let $\mathcal{A}$ be an adversary in the following game $Exp^{Ind}_{ASYM,\mathcal{A}}(n)$:*

- *The challenger chooses a random bit b and $\mathcal{K}$.*
- *If $b = 0$, the key-generation function $\overline{\mathcal{K}}_{\mathcal{K}}$ remains unchanged; otherwise if $b = 1$ then $\overline{\mathcal{K}}_{\mathcal{K}}$ is replaced with a random function* Rand *which returns random values in the range of $\overline{\mathcal{K}}_{\mathcal{K}}$.*
- *Adversary $\mathcal{A}$ guesses b' and wins if $b' = b$.*

We say that ASYM achieves indistinguishability if for any PPT adversary as above there exists a negligible function negl such that

$$\Pr[Exp^{Ind}_{ASYM,\mathcal{A}}(n) = 1] = \frac{1}{2} + negl(n).$$

5 The XDHIES Scheme

We present XDHIES, an extended pseudorandom public key scheme. We explain below how XDHIES extends PR-DHIES to achieve the two crucial requirements discussed above.

5.1 Embedding Beacon's Status

To enable secure status transmission in the beacon's broadcast while preserving the length of a single PR-DHIES public key, we incorporate the status as an additional input to the pseudorandom function thus embedding (or "folding") the status within the public key. This approach allows the beacon to broadcast only the public key, which now includes the embedded status. Hence, the public key at time t becomes

$$pk = g^{\mathsf{PRF}_x(t,s)}$$

where x is the symmetric key shared between the beacon and its owner.

Obviously, decryption of the value pk to get status s cannot be achieved by applying an inverse function, since this would require solving a discrete log problem and inverting the PRF. Instead, since the number of different status messages s is relatively small (recall that the status s is composed of only a few bits), decryption of a beacon's status can be easily done in a brute-force manner or by maintaining a small table.

5.2 Providing Perfect Backward and Forward Security

The key idea enabling the beacon notification protocol to achieve perfect backward and forward security is to prevent the beacon from holding critical secrets. In this way, even if an adversary compromises the beacon and reveals its secret key, it cannot decrypt any messages. Our solution is inspired by the security principle of "separation of duties," specifically as applied in key-insulated cryptography [12,11], where a server "helps" an entity susceptible to key extraction by periodically refreshing its secret key. In our case, the owner plays the role of the "helping" entity.

We designed XDHIES to incorporate such a secret separation. Specifically, XDHIES separates the secrets required for key-generation from those needed for decryption. We provide the beacon with only the information necessary for generating public keys and give the owner, who is the trusted entity, the information required for decryption, that is, the information necessary for generating the secret keys.

In particular, we provide the decryption function with a random value $r \in \mathbb{Z}_q$ and provide the key-generation function with g^r. The key-generation function uses g^r as its base-point generator instead of g and applies the exact same operations as before (i.e., this modification is transparent to the function). Consequently, r is known only to the owner who does not share it with the beacon. The beacon's public key at time t with status s is then:

$$pk = (g^r)^{\mathsf{PRF}_x(t,s)}.$$

This separation of responsibilities between the key-generation function (representing the beacon) and the decryption function (representing the owner) neutralizes the risk of compromising the beacon's secret keys since the beacon is no longer the "holder of all secrets." The XDHIES private key for decryption is then

$$sk = r \cdot \mathsf{PRF}_x(t,s).$$

As can be seen, even if an adversary reveals the beacon's secrets (x, g^r), it cannot reveal r, and is therefore unable to compute the XDHIES private key and decrypt past or future messages based on this XDHIES private key.

5.3 XDHIES Definition

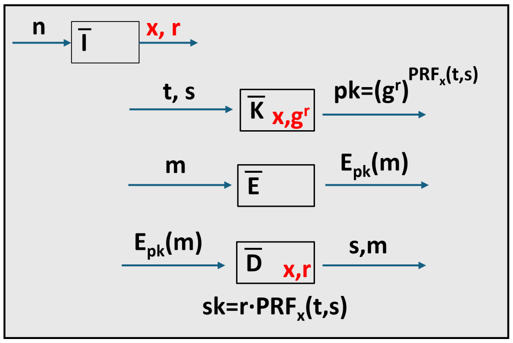

Fig. 3: XDHIES

Definition 19. *(XDHIES) Let* $\mathsf{SYM} = (\mathcal{E}, \mathcal{D})$ *be a private-key authenticated-encryption scheme. We run* $\mathsf{GroupGen}(1^n)$ *to obtain* $(\mathbb{G}, q, g)$*. Let* KDF *be a key derivation function* $\mathsf{KDF} : \mathbb{G} \to \{0,1\}^n$*.* $\mathsf{XDHIES} = (\overline{\mathcal{I}}, \overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ *is the following four-tuple of algorithms defining extended pseudorandom public-key encryption:*

- $\overline{\mathcal{I}}(n)$*: Chooses a uniform* $x \in \{0,1\}^n$ *and a random* $r \in \mathbb{Z}_q$*. Additionally generates table* Tbl *for the decryption function as follows: for any* $s \in S$ *and* $t \in [t_s, t_e]$ *sets* $pk_{t,s} = g^{r \cdot \mathsf{PRF}_x(t,s)}$ *and stores the entry* $(t,s) = \mathsf{Tbl}[pk_{t,s}]$*. Sets* $\mathcal{K} = (x, g^r)$ *which is intended for the key-generation function and sets* $\mathcal{K}' = (x, r, \mathsf{Tbl})$ *which is intended for the decryption function.*
- $\overline{\mathcal{K}}_{x,g^r}(t,s)$*: For a given pair of* (t,s) *sets the corresponding private key* $sk_{t,s} = \mathsf{PRF}_x(t,s)$ *and returns the corresponding public key* $pk_{t,s} = (g^r)^{sk_{t,s}}$*.*
- $\overline{\mathcal{E}}_{pk_{t,s}}(m)$*: Chooses a uniform* $z \in \mathbb{Z}_q$*, computes* g^z *and sets* $k = \mathsf{KDF}((pk_{t,s})^z)$*. Computes* $c = \mathcal{E}_k(m)$ *and outputs* (g^z, c)*.*
- $\overline{\mathcal{D}}_{x,r,\mathsf{Tbl}}(h, \hat{c}, c)$*: Returns* $\perp$ *if* $h \notin \mathsf{Tbl}$ *or if* $\hat{c} \notin \mathbb{G}$*. Otherwise, applies* $(t,s) = \mathsf{Tbl}[h]$*, sets* $sk_{t,s} = r \cdot \mathsf{PRF}_x(t,s)$ *and calculates* $k = \mathsf{KDF}((\hat{c})^{sk_{t,s}})$*. Returns* s *and* $m = \mathcal{D}_k(c)$ *if authentication succeeds.*

6 Security Proofs for XDHIES

Theorem 2. *XDHIES is s-CCA secure.*

Proof. To prove this, we define XDHIES-R, a variant of XDHIES where we replace every appearance of the pseudorandom function $\mathsf{PRF}_x(\cdot,\cdot)$ with $\mathsf{Rand}(\cdot,\cdot)$, where $\mathsf{Rand}(\cdot,\cdot)$ is a random function returning a random value in $\mathbb{Z}_q^*$.

Clearly, for any PPT adversary $\mathcal{A}$, there exists a negligible function *negl* such that

$$\Pr[\mathrm{Exp}^{\text{s-CCA}}_{\text{XDHIES},\mathcal{A}}(n) = 1] - \Pr[\mathrm{Exp}^{\text{s-CCA}}_{\text{XDHIES-R},\mathcal{A}}(n) = 1] \leq \mathit{negl}(n).$$

The challenge in the s-CCA game of XDHIES-R is $pk_{t_c,s_b} = g^{r\cdot\mathsf{Rand}(t_c,s_b)}$. Since the value t_c is only used to generate the challenge (and is not used in any of the oracle calls) and since the encryption is a random group element, it follows that

$$\Pr[\mathrm{Exp}^{\text{s-CCA}}_{\text{XDHIES-R},\mathcal{A}}(n) = 1] = \frac{1}{2}.$$

Therefore Theorem 7 follows.

Theorem 3. *XDHIES is m-CCA secure with perfect backward and forward security.*

Proof. To prove the above, let $\mathcal{A}$ be an adversary against the m-CCA security of $\mathsf{XDHIES} = (\overline{\mathcal{I}}, \overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$. We build an adversary $\mathcal{A}'$ against the CCA-security of $\mathsf{DHIES} = (\overline{\mathcal{K}'}, \overline{\mathcal{E}'}, \overline{\mathcal{D}'})$:

- The DHIES challenger randomly chooses a private key $r \in \mathbb{Z}_q$ and sends the public key $pk = g^r$ to adversary $\mathcal{A}'$.
- Adversary $\mathcal{A}'$ generates $x \in \{0,1\}^n$ and sends x, pk to adversary $\mathcal{A}$. Additionally, adversary $\mathcal{A}'$ generates Tbl with entries $(t,s) = \mathsf{Tbl}[pk^{\mathsf{PRF}_x(t,s)}]$ for any $s \in S$ and $t \in [t_s, t_e]$.
- Adversary $\mathcal{A}'$ runs adversary $\mathcal{A}$ and simulates an XDHIES decryption oracle call $\overline{\mathcal{D}}_{x,r,\mathsf{Tbl}}(h, \hat{c}, c)$ as follows: adversary $\mathcal{A}'$ returns $\perp$ if $h \notin \mathsf{Tbl}$ or $\hat{c} \notin \mathbb{G}$, and otherwise applies $(t,s) = \mathsf{Tbl}[h]$ and returns the pair $(s, \overline{\mathcal{D}'}_r(\hat{c}^{\mathsf{PRF}_x(t,s)}, c))$.
  Indeed, the shared symmetric decryption key in $\overline{\mathcal{D}'}_r(\hat{c}^{\mathsf{PRF}_x(t,s)}, c)$ is $(\hat{c}^{\mathsf{PRF}_x(t,s)})^r$ which is equal to $\hat{c}^{r\cdot\mathsf{PRF}_x(t,s)}$, the shared symmetric decryption key in $\overline{\mathcal{D}}_{x,r,\mathsf{Tbl}}(h, \hat{c}, c)$.
- Adversary $\mathcal{A}$ chooses t_c, a short domain message s_c, and two distinct messages $m_0 \neq m_1$ and sends t_c, s_c, m_0, m_1 to adversary $\mathcal{A}'$. Adversary $\mathcal{A}'$ sends m_0, m_1 to its DHIES challenger.
- The DHIES challenger chooses a random bit $b \in \{0,1\}$ and sends to adversary $\mathcal{A}'$

$$(y_1, y_2) = \overline{\mathcal{E}'}_{g^r}(m_b).$$

- Adversary $\mathcal{A}'$ sends to adversary $\mathcal{A}$ the challenge

$$y = (pk^{\mathsf{PRF}_x(t_c,s_c)}, y_1^{1/\mathsf{PRF}_x(t_c,s_c)}, y_2).$$

  The pair $(y_1^{1/\mathsf{PRF}_x(t_c,s_c)}, y_2)$ is indeed a correct challenge for adversary $\mathcal{A}$ since $y_1^{1/\mathsf{PRF}_x(t_c,s_c)}$ is a random group element (because y_1 is), and since

$$(y_1)^r = (y_1^{1/\mathsf{PRF}_x(t_c,s_c)})^{r\cdot\mathsf{PRF}_x(t_c,s_c)}.$$

- Denote $(\overline{y_0}, \overline{y_1}, y_2) := y$. Adversary $\mathcal{A}$ continues to have access to the decryption oracle as above, but we forbid the adversary from querying the decryption oracle with $y_v = (\overline{y_0}^v, \overline{y_1}^{(1/v)}, y_2)$ for any v. While this requirement is stronger than not querying with y as required in the m-CCA definition (Definition 17), this requirement is reasonable since $\overline{y_1}$ is an ephemeral public key which is random and is thus independent of $\overline{y_0}$.
- Eventually, adversary $\mathcal{A}$ returns its guess b', and adversary $\mathcal{A}'$ returns this guess b' to its challenger.

Since the view of adversary $\mathcal{A}$ in $\mathrm{Exp}^{\text{m-CCA}}_{\text{XDHIES},\mathcal{A}}$ is identical to the view of adversary $\mathcal{A}$ when its experiment is simulated by adversary $\mathcal{A}'$, it holds that:

$$\Pr[\mathrm{Exp}^{\text{CCA}}_{\text{DHIES},\mathcal{A}'}(n) = 1] = \Pr[\mathrm{Exp}^{\text{m-CCA}}_{\text{XDHIES},\mathcal{A}}(n) = 1].$$

The assumed CCA-security of DHIES, thus implies Theorem 3.

Theorem 4. *XDHIES achieves indistinguishability.*

Proof. Since $\overline{\mathcal{K}}_{x,g^r}(t,s) = g^{r \cdot \mathsf{PRF}_x(t,s)}$, and the adversary has access only to $\overline{\mathcal{K}}_{x,g^r}(\cdot,\cdot)$, the theorem is implied from the pseudorandomness of PRF_x.

7 The Beacon Notification Protocol

Let $\mathsf{XDHIES} = (\overline{\mathcal{I}}, \overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ be the XDHIES encryption scheme described above with group parameters $(\mathbb{G}, q, g)$. Let H be a cryptographic hash function $H : \mathbb{G} \to \{0,1\}^n$, and let PRF be a pseudorandom function $\mathsf{PRF} : \{0,1\}^n \times \{0,1\}^* \to \mathbb{Z}_q^*$.

Our beacon notification protocol is built upon the XDHIES scheme. In Section 2.1 we define five-tuple of algorithms

$$\mathsf{BcnNtf} = (\mathsf{Init}, \{\mathsf{Bcn_i}\}_{\mathsf{i=1}}^{\mathsf{w}}, \mathsf{Obs}, \mathsf{Svr}, \{\mathsf{Own_i}\}_{\mathsf{i=1}}^{\mathsf{w}})$$

which constitute the interface of the beacon notification protocol. Below we complete the definition of these five algorithms by providing the algorithmic details. We start with some general details and then delve into each algorithm.

First, a beacon broadcasts every second or two, but in practice it only changes its broadcast every fixed time period T (e.g., 15 minutes) in order to save battery.

Second, to achieve efficient real-time communication, enable integrity and mitigate security attacks such as [7,5], the design of the cloud server in our beacon notification protocol is inspired by Eddystone-EID [10]. In particular, the cloud server is provided with a mapping table $\mathcal{M}$ associating the beacons' broadcasts with the beacons' respective owners. That is, for each beacon i the mapping table $\mathcal{M}$ has an entry for every possible beacon's broadcast in $[t_s, t_e]$. We refer to the table $\mathcal{M}$ as the "beacon-to-owner mapping table." We note that in practice $\mathcal{M}$ is generated piecewise on the fly: the time axis is divided into consecutive non-overlapping time periods of, say, 24 hours, and at the start of each time period the cloud server is provided only with the part of the mapping table corresponding to the that time period.

Third, generating the beacons' broadcasts requires knowledge of the respective beacon's secret key, so that the cloud server cannot generate the mapping table $\mathcal{M}$ by itself. Instead, each owner generates the possible broadcast values of its beacon and sends them to the server. The server then unifies the received values from all owners into the complete mapping table $\mathcal{M}$.

Fourth, recall that a beacon's broadcast is its public key (within which the beacon's status is embedded). To prevent the cloud server from using these public keys to forge observers' messages, the cloud server's mapping table $\mathcal{M}$ is keyed by a cryptographic hash of the beacons' public keys instead of the public keys themselves. We assume that the observer does not collude with the server to send the actual public key instead of the hash to the cloud server, for the following reasons: (a) The observer's protocol is implemented within the MANET component of the device (typically a smartphone), which cannot be easily modified by the user without being detected by the remote operational integrity service; and (b) The server is economically incentivized to adhere to the protocol specifications to avoid potential business, reputation, or revenue losses, and will thus not cooperate with any unauthorized entities outside the defined protocol (and in the future, the server may be deployed within a Trusted Execution Environment (TEE) for enhanced assurance).

- $\mathsf{Init}(1^n, 1^w)$:
  1. Beacon and Owner keys initialization: For each $i \in [1, w]$: apply $\overline{\mathcal{I}}(n)$ to get random $r_i \in \mathbb{Z}_q$ and $x_i \in \{0,1\}^n$.
  2. Owner tables initialization: For any $i \in [1, w]$, generates Tbl_i as follows: For any $s \in s$ and $t \in [t_s, t_e]$
  $$\mathsf{Tbl}_i[H(g^{r_i \cdot \mathsf{PRF}_{x_i}(\lfloor t/T \rfloor, s)})] := (\lfloor t/T \rfloor, s).$$
  3. Cloud server keys initialization: Generating $\mathcal{M}$ as follows: for all $i \in [1, w]$, $t \in [t_b, t_e]$, and $s \in S$:
  $$\mathcal{M}[H(g^{r_i \cdot \mathsf{PRF}_{x_i}(\lfloor t/T \rfloor, s)})] := i.$$
  4. Key distribution: Let
  $$\mathcal{K}_i = (x_i, g^{r_i}), \mathcal{K}'_i = (x_i, r_i, \mathsf{Tbl}_i).$$
  $\mathcal{K}_i$ is given to the i'th beacon, $\mathcal{K}'_i$ is given to the i'th owner and $\mathcal{M}$ is given to the cloud server. We note that each pair of $\mathcal{K}_i$ and $\mathcal{K}'_i$ is generated locally in private by the respective owner and $\mathcal{M}$ is combined by the cloud server from the pieces sent by all owners as described above.
- $\mathsf{Bcn}_i(t, s)$: On input time t and status s, applies $\overline{\mathcal{K}}_{x_i, g^{r_i}}$ to get $pk_{i,t,s}$, and returns
  $$\mathsf{Bcn}_i(t, s) = pk_{i,t,s} = g^{r_i \cdot \mathsf{PRF}_{x_i}(\lfloor t/T \rfloor, s)}.$$
- $\mathsf{Obs}(pk, m)$: On input pk and a message m, if $H(pk) \notin \mathcal{M}$ returns $\perp$; otherwise returns:
  $$\mathsf{Obs}(pk, m) = (H(pk), \overline{\mathcal{E}}_{pk}(m)).$$
- $\mathsf{Svr}(h, (\hat{c}, c))$: On input $(h, (\hat{c}, c))$ where h is expected to be the hash value of the i'th beacon's public key $pk_{i,t,s}$ for some i, t and s and $(\hat{c}, c)$ is expected to be $\overline{\mathcal{E}}_{pk_{i,t,s}}(m)$ for some message m, if $h \notin \mathcal{M}$ it returns $\perp$; otherwise forwards $(h, (\hat{c}, c))$ to the corresponding owner which is
  $$\mathsf{Svr}(h, (\hat{c}, c)) = \mathcal{M}[h] = i.$$
- $\mathsf{Own}_i(h, (\hat{c}, c))$: If $h \notin \mathsf{Tbl}_i$ returns $\perp$; otherwise, returns
  $$\mathsf{Own}_i(h, (\hat{c}, c)) = \overline{\mathcal{D}}_{x_i, r_i, Tbl_i}(h, \hat{c}, c)$$
  which is s, m if authentication succeeds, and $\perp$ otherwise.

8 Protocol Security and Privacy Proofs

In this section we prove that our beacon notification protocol achieves the security, privacy, unforgeability, integrity, and correctness requirements.

Theorem 5. *(Beacon's status CCA-security) The beacon notification protocol achieves beacon's status CCA-security according to Definition 1.*

Proof. Implied from the s-CCA security of XDHIES (Theorem 2).

Theorem 6. *(Observer's message CCA-security) The beacon notification protocol achieves observer's message CCA-security with perfect backward and forward security according to Definition 2.*

Proof. Implied from the m-CCA security of XDHIES (Theorem 3).

Theorem 7. *(Beacon indistinguishability) The beacon notification protocol achieves indistinguishability according to Definition 3.*

Proof. Implied from the indistinguishability of XDHIES (Theorem 4).

Theorem 8. *(Unforgeability) The beacon notification protocol achieves unforgeability according to Definition 4, where H is modeled as a random oracle.*

Proof. Implied directly from the pseudorandomness of $\mathsf{Bcn}()$ and the randomness of H in the mapping table $\mathcal{M}$.

Theorem 9. *(Integrity) The beacon notification protocol achieves integrity according to Definition 5.*

Proof. Implied from the fact that the observer verifies with the cloud server that a received beacon's output is valid before using it.

Theorem 10. *(Correctness) The beacon notification protocol is correct according to Definition 6.*

Proof. We need to show that

$$(s, m) = \mathsf{Own}_{\mathsf{Svr}(\mathsf{Obs}(\mathsf{Bcn}_i(t,s),m)}(\mathsf{Obs}(\mathsf{Bcn}_i(t, s), m)).$$

Recall that $\mathsf{Bcn}_i(t, s) = pk$ where $pk = g^{r_i \cdot \mathsf{PRF}_{x_i}(t,s)}$. Thus

$$\mathsf{Obs}(\mathsf{Bcn}_i(t, s), m) = (H(pk), \overline{\mathcal{E}}_{pk}(m)),$$

and

$$\mathsf{Svr}(H(pk), \overline{\mathcal{E}}_{pk}(m)) = \mathcal{M}[H(pk)] = i.$$

Therefore, the i'th owner finds (t, s) from $\mathsf{Tbl}_i[H(pk)]$, computes $sk = r_i \cdot \mathsf{PRF}_{x_i}(t, s)$, uses it to decrypt $m = \overline{\mathcal{D}}_{sk}(\overline{\mathcal{E}}_{pk}(m))$, and output s, m.

9 Complexity of Time and Space

We next consider the complexity of each component in the beacon notification protocol:

Beacon: Beacon i computes the public key values, where a public key value is computed by a single group exponentiation (or more precisely a single elliptic curve multiplication) using the base g^{r_i}. This exponentiation can be performed very efficiently (following pre-computation) since the base is fixed (see [6]). The beacon broadcasts (the x-coordinate of) a single curve point. NIST recommends using 224-bit elliptic curves through year 2030 and 256-bit elliptic curves through and beyond year 2030.[1] Using these recommendations implies that the curve point broadcast by the beacon is of length 224 bit or 256 bit, respectively which is extremely small. The public key value computation time is in milliseconds and its power consumption is negligible relative to the power consumption of the beacon's communication. In fact, the beacon can operate on a small battery for at least a full year. The choice of a pseudo-random r_i is done via an extraction from a (possibly forward secure) pseudorandom generator (based on symmetric key operation) and a modular reduction in the field to get proper value from the drawn random long enough string.

Observer: The observer (which is a smartphone with much larger computation and power resources than those of the beacon) applies two group exponentiations per beacon in its vicinity: One exponentiation uses a fixed base (g) and the other uses a random base ($g^{r \cdot \mathsf{PRF}_x(t,s)}$) which the observer gets from a near by beacon. Again, the fixed-base exponentiation can benefit significantly from [6], but in any case computing two group exponentiations is reasonable and has negligible affect on the observer's battery (which is the primary concern with respect to observers).

Cloud server: The main complexity measure for the cloud server is the size of the mapping table. With 256-bit hash function and three different signal values, each entry in the table is composed of 128-bit for the hash of the public key value (by using, e.g., only 128 out of 256 bits of the hash value) and a 64-bit owner ID. Therefore, the size of each table entry is 192 bits. Consider for example a period of 24 hours and a new beacon broadcast every 20 minutes, namely 72 daily public key values. Then, the number of entries per beacon per 24 hours is $72 \times 3 = 216$ (the '3' represents the three possible battery values). Therefore required size per beacon is 216×192 bits $= 41.5$ KB. We consider two (very) different application scenarios below. The first application is a small city's sensory data collection with 1000 beacons. The size of the mapping table in this case is 41.5 MB - very small indeed. The second application is asset tracking. Here we assume 10^8 beacons. The size of the mapping table in this case is therefore 4.15 TB. This is certainly reasonable for a company with 10^8 users (or to its cloud provider).

The mapping table is implemented as a hash table, and therefore the lookup operation is very fast, taking a few milliseconds. For efficiency and privacy the table values are not retained beyond the day.

Owner: For each beacon, the owner needs to generate its Tbl table entries periodically. The owner then keeps the table to enable decryption and sends only the table's public key values to the server. Using the above parameters, each entry of Tbl requires 128 bits, 32 bits and 2 bits for the public key value, time and signal, respectively. For 24 hours and public key value change every 20 minutes, the table is of size 72×162 bits $= 12$ KB. Computing Tbl entails $72 \times 3 = 216$ exponentiations for computing the required public key values. Each group exponentiation is with a fixed base and can therefore be computed using the efficient algorithm of [6]. Due to the multiple exponentiations, the process of generating the Tbl table takes a few seconds but can nevertheless

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

be done without affecting user experience by either (1) pre-computing the exponentiations during the phone's idle times; or (2) computing the entries in small batches during the day instead of all at once (and similarly sending the table's computed public key values to the cloud server in batches during the day).

To summarize, the beacon notification protocol is efficient in all the relevant parameters and can be easily integrated in real-world applications (in fact, parts of it have already been adopted to and implemented within a concrete setting).

10 Related Work

Beacons and BLE broadcasting in particular are widely useful in real-life proximity applications: contact tracing systems like Google-Apple Exposure Notification (GAEN) [4,9] has been such an example for a mobile-to-mobile signaling. We also note that there are works that study the beacons privacy such as [8].

However, we are not aware of any work with respect to the beacon notification problem as derived from the IoT setting and defined in this paper (essentially a beacon to owner real-time signaling via an observer), hence we consider below the closest protocols for different and weaker versions of this problem as is reflected by industrial deployments.

Specifically, in Samsung's SmartTag [14] and Tile [1] the beacon does not send a status so obviously no beacon's status security is provided. In addition, SmartTag and Tile do not provide end-to-end security with respect to the observer's message.

Apple's FindMy [13], on the other hand, provides end-to-end security with respect to the observer's message but

- without forward and backward security for all future/past messages,
- without beacon's status support,
- without efficient real-time communication,
- without observer's message integrity,
- and without formal cryptographic definitions, threat model, and security proofs.

It is worth noting that FindMy aims at neither an efficient real-time communication nor observer's message integrity, due to not supporting beacon-to-owner mapping table. This lack of the beacon-to-owner association at the cloud server in FindMy provides strong anonymity to the owner with respect to the cloud server, but opens the door to two types of attacks: (i) Attacks [7,5] which use the FindMy network as a public database; and (ii) attacks where a beacon sends a weak key to an observer with the intention to reveal the observer's message (which is the location in the case of Apple's FindMy). Such attacks would succeed since the observer lacks the ability to validate the received public key. In contrast, achieving anonymity in our server model relies on the server honestly erasing its data after using it in real time for association. Finally, we note that Apple has published neither a detailed description of the FindMy protocol nor cryptographic proofs of its security.

We note that our embedding of the beacon's status within the beacon's broadcast (that is, within the public key), is completely different from the attack [7] on the FindMy system which embeds a bit-message in the transmitted public key. While in the attack [7] the bit-message is exposed, and worse, the observer's message is not secured since the attacker controls the respective private key, our protocol ensures secure-end-to-end property for the status and the observers' messages by using a randomized and authenticated public key incorporating an encrypted status.

11 Conclusions

We presented the general problem for the IoT involving broadcasting beacons and motivated their operational and security constraints. In particular, we derived and presented novel cryptographic definitions for the beacon notification problem including its security, privacy, and integrity requirements. To solve the problem we presented an extension for DHIES, which we called XDHIES, and built upon it our beacon notification protocol. We then proved that our resulting protocol achieves all the formalized requirements.

Furthermore, and looking forward, we believe that our new protocol, given its unique and comprehensive security features, its versatility, and its suitability for real-world IoT applications and their operational constraints, may be considered (entirely or partially) for standardization for global use in the IoT area.

References

1. Tile. `https://www.tile.com/`.
2. Apple and Google lead initiative for an industry specification to address unwanted tracking. `https://www.apple.com/newsroom/2023/05/apple-google-partner-on-an-industry-specification-to-address-unwanted-tracking`.
3. Abdalla, M., Bellare, M., and Rogaway, P. Dhaes: An encryption scheme based on the diffie-hellman problem. *IACR Cryptol. ePrint Arch. 1999* (1999), 7.
4. Apple, G. Privacy-preserving contact tracing. `https://covid19.apple.com/contacttracing`.
5. Bellon, A., Yen, A., and Pannuto, P. Demo abstract: Tagalong: A free, wide-area data-muling service built on the airtag protocol. In *20th ACM Conference on Embedded Networked Sensor Systems* (2022).
6. Brickell, E. F., Gordon, D. M., McCurley, K. S., and Wilson, D. B. Fast exponentiation with precomputation. In *Workshop on the Theory and Application of of Cryptographic Techniques* (1992), Springer, pp. 200–207.
7. BRÄUNLEIN, F. Send my: Arbitrary data transmission via apple's find my network, 2021. `https://positive.security/blog/send-my` (last visited 2022-12-13).
8. David, L., Hassidim, A., David, Y., and Yung, M. The battery insertion attack: Is periodic pseudo-randomization sufficient for beacon privacy? *Proceedings on Privacy Enhancing Technologies* (2025).
9. David, L., Hassidim, A., Matias, Y., and Yung, M. Scaling up gaen pseudorandom processes: Preparing for a more extensive pandemic. In *European Symposium on Research in Computer Security* (2022), Springer, pp. 237–255.
10. David, L., Hassidim, A., Matias, Y., Yung, M., and Ziv, A. Eddystone-eid: Secure and private infrastructural protocol for ble beacons. *IEEE Transactions on Information Forensics and Security* (2022).
11. Dodis, Y., Katz, J., Xu, S., and Yung, M. Strong key-insulated signature schemes. In *International Workshop on Public Key Cryptography* (2003), Springer, pp. 130–144.
12. Dodis, Y., Luo, W., Xu, S., and Yung, M. Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security* (2012), pp. 57–58.
13. Heinrich, A., Stute, M., Kornhuber, T., and Hollick, M. Who can find my devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System. In *Proceedings on Privacy Enhancing Technologies PETS* (2021), vol. 3, pp. 227–245.
14. Yu, T., Henderson, J., Tiu, A., and Haines, T. Privacy analysis of samsung's crowd-sourced bluetooth location tracking system. *USENIX Security Symposium* (2024).