COOB: Hybrid Secure Device Pairing Scheme in a Hostile Environment

Sameh Khalfaoui[1,2(✉)], Jean Leneutre[2], Arthur Villard[1], Jingxuan Ma[1], and Pascal Urien[2]

[1] EDF R&D, 7 Boulevard Gaspard Monge, 91120 Palaiseau, France
{sameh.khalfaoui,arthur.villard,jingxuan.ma}@edf.fr
[2] LTCI, Télécom Paris, Institut Polytechnique de Paris, Paris, France
{jean.leneutre,pascal.urien}@telecom-paris.fr

Abstract. Due to the scalability limitations, the secure device pairing of Internet of Things objects cannot be efficiently conducted based on traditional cryptographic techniques using a pre-shared security knowledge. The use of Out-of-Band (OoB) channels has been proposed as a way to authenticate the key establishment process but they require a relatively long time and an extensive user involvement to transfer the authentication bits. However, the context-based schemes exploit the randomness of the ambient environment to extract a common secret without an extensive user intervention under the requirement of having a secure perimeter during the extraction phase, which is considered as a strong security assumption.

In this paper, we introduce a novel hybrid scheme, called COOB, that efficiently combines a state-of-the-art fast context-based encoder with our Out-of-Band based scheme. This protocol exploits a nonce exponentiation to achieve the temporary secrecy goal needed for the authentication. Our method provides security against an attacker that can violate the secure perimeter requirement, which is not supported by the existing contextual schemes. This security improvement has been formally validated in the symbolic model using the TAMARIN prover. Based on our implementation of the Out-of-Band channel, COOB enhances the usability by reducing the pairing time up to 39% for an 80-bit OoB exchange while keeping an optimal protocol cost.

Keywords: Internet of Things · Security · Secure device pairing · Out-of-band channel · Context-based pairing · Formal methods

1 Introduction

With the growing demand for personal gadgets and sensors, the use of a decentralized device-to-device (D2D) communication system has become a necessity for numerous applications in the context of Internet of Things (IoT) like Smart-Homes, Intelligent Transportation Systems (ITS) and Smart Metering and Mon-

N. Park et al. (Eds.): SecureComm 2020, LNICST 336, pp. 419–438, 2020.
https://doi.org/10.1007/978-3-030-63095-9_27

itoring (SMM). This decision is based on the inefficiency of a centralized communication solution to meet the scalability and the interoperability goals. Therefore, the protection of this communication channel requires the use of a secure key establishment protocol between the devices, known as *Secure Device Pairing* (SDP). This process ensures that the communicating nodes agree on the same symmetric encryption key, which represents an initial trust establishment between devices that have no pre-shared knowledge (a certificate, a shared password or a symmetric key). The no prior secret condition is motivated by two reasons. The first one is the unfeasibility of exploiting a Public Key Infrastructure (PKI) due to the growing numbers of heterogeneous IoT devices. The second reason is the *Zero-Trust* policy that disapproves of trusting the manufacturer with delivering the initial pre-shared pairing keys to avoid any vulnerabilities or breaches related to a third party.

Two main techniques are used to achieve these goals. The first one uses a pre-authenticated auxiliary channel that is also known as a location limited or a human assisted channel [3]. However, in this work we will refer to it as an *Out-of-Band* (OoB) channel. These channels suffer from low data-rates, which results in a long pairing time. This drawback can severely affect the user-experience. Therefore, the optimization of this usability criteria is considered a necessity for such protocols. The second technique ensures authentication through a proof of co-presence based on the randomness of the ambient environment. This method is better known as *Context-based Pairing* or *Zero-Interaction Protocols* (ZIP) [11]. Even though this type of pairing schemes is optimal in terms of usability and user-friendliness, it demands a safe zone where no attacker is assumed present to avoid any risks related to facing a well-equipped adversary. This can be quite hard to guarantee by a regular user and quite easy to take advantage of by an adversary that can hide a sensor in that, allegedly, safe environment.

In this work, we propose a novel device pairing scheme that is able to efficiently combine an existing fast contextual key agreement protocol with an authenticated Out-of-Band channel. Our hybrid protocol, called COOB, has two distinct components. The first one is a contextual module where we take advantage of any fast and reliable contextual key agreement technique. The second component is a protected OoB channel that guarantees at least the authenticity and the integrity of the exchanged information. This design provides a security improvement in comparison with the existing context-based schemes since it is robust against a powerful contextual attacker. This adversary can sense and even control the ambient environment surrounding the two legitimate devices. Furthermore, it provides a usability improvement by reducing the protocol completion time in comparison with the existing pairing schemes that rely solely on a low data-rate OoB channel. In addition, COOB maintains a reduced cryptographic cost of only two hash computations for each device. In order to reach this level of optimality, a nonce exponentiation is exploited while constructing the Diffie-Hellman public keys to temporarily hide their real values, as described in Sect. 3.3.

The main contributions of this paper are summarized as follows:

(I) We design a novel hybrid pairing protocol that efficiently combines a contextual based and an Out-of-Band based pairing techniques to enhance the security and the usability aspects.
(II) We evaluate the security of our scheme by providing a proof estimating the attack success probabilities under two adversary models. Also, we formally validate the security of our design in the symbolic model using the TAMARIN prover.
(III) We implement the Out-of-Band protocol on two Raspberry Pi 4B. Then, we conduct a time efficiency analysis to estimate the usability improvement provided by the contextual module.

The rest of this paper is organized as follows. Section 2 discusses relevant work to OoB and context-based pairing schemes and highlights the limitations of each category. Section 3 describes our protocol along with the assumptions and the threat model taken into account. Section 4 evaluates the security of our scheme and formally validates its robustness in the symbolic model using the TAMARIN prover. Section 5 describes the protocol implementation on the Raspberry Pi 4B and outlines the results of the time efficiency estimation and, lastly, Sect. 6 concludes our work.

2 Related Work

Numerous secure device pairing solutions rely on an Out-of-Band channel with specific security properties to send information that validates what has been exchanged on the In-Band channel, referred to as the In-Band channel. This is due to the unfeasibility of performing the authentication based on a single channel that is controlled by a Dolev-Yao intruder [9], as demonstrated in [7] using BAN Logic analysis [6]. This powerful adversary is assumed to have a perfect knowledge of the protocol and he is able to overhear, block, delay, replay and forge any transmission over that channel. However, he is not able to perform any computational attacks against the cryptographic functions. As a consequence of adopting this intruder model, the usage of the In-Band channel without having pre-shared secrets is not sufficient to provide the desired security guarantees for the key exchange process. Therefore, there is a need for an auxiliary communication link on which the authentication of the exchanged keys can happen. These channels can be constructed based on audio, visual or haptic transmissions. Due to their special nature and their communication properties, they provide an initial level of security that is sufficient to primarily guarantee the integrity of the data and the demonstrative identification [3], which is ensuring that the communicating devices on these channels are the intended ones for pairing. Other security objectives might be provided in some cases such as the confidentiality and the data origin authenticity. These assumptions on the OoB channel reduce the attacker capabilities in comparison with his abilities on the In-Band channel. In this context, we adopt the Out-of-Band security classification in the work of

Mirzadeh et al. [25] that defines the three following categories: the *confidential* channel which eliminates all attacker capabilities, the *protected* channel that limits the adversary powers to intercepting, blocking and delaying the messages which breaks the confidentiality assumption and affects the guarantee of the message reception. Finally, the *authentic* channel grants the attacker the additional capabilities to replay messages that were exchanged in previous sessions which violates the data freshness guarantee [30].

Some proposals such as Secure Simple Pairing (SSP) [4] and Push Button Configuration (PBC) [2] exploit the short-range radio communications, such as the Near Field Communication (NFC), as an Out-of-Band channel. Unfortunately, this technology is not secured against an attacker that is sufficiently close to the pairing objects as demonstrated in the work of Akter et al. [1]. Thus, we will not consider it as a secure option of an OoB channel. In the work of Fomichev et al. [10], a selection of pairing proposals that rely on Out-of-band channels have been thoroughly described based on their nature (radio [2,4], visual [26,36], acoustic [13,32] or haptic [21,27]), the degree of the user involvement and the application context of the pairing. The latter criteria classes the pairing use-cases into categories that have related security threats and objectives. The significant limitations of these channels are their low data-rates and their need for a extensive user intervention. The former drawback is due to the quality of the interfaces on the commercial IoT products, which makes the transfer of long hashes or keys not possible. Some of the proposed schemes rely on the human user to *setup* the devices for the exchange, to *relay* an information from one device to another, to *compare* a short authentication string on both objects or to simply *generate* a secret PIN and to enter it in both devices [10]. As an example, the security of the pairing scheme MANA III [12] is based on the confidentiality of the PIN entered by the user. Even though the confidential OoB channels are not considered as a reliable option due to the feasibility of eavesdropping attacks on the acoustic, the visual and the haptic transmissions using side-channel analysis techniques [14]. Another prominent threat in the protocol design is the predictable human input. This vulnerability is considered as a *Human-factor error* that, if not well designed, might compromise the effective security of the protocol [17].

Due to the usability challenges related to the use of Out-of-Band channels such as the long pairing completion time and the extensive human involvement as shown in [17,20], the research focus has shifted toward a more autonomous authentication technique based on a proof of co-presence. These protocols use the randomness of the ambient environment to extract a contextual information on both devices within a specific area called the *authentication zone*. This parameter represents the area where the legitimate devices are required to be placed in order to enhance the usability of the protocol by minimizing the errors when sensing the environment. The contextual information can be either used to extract a key for encryption later on [23], a fingerprint of the device location [15] or as a way to encode a secret between the pairing parties [34]. Based on the close proximity assumption, the two objects are expected to have similar

measurements of the chosen environmental metrics, which will result in a similar contextual security parameters. The choice of the metrics should be based on aspects such as: the **location dependency** that explains the changes in the contextual measurements when we change the position of the sensor, the **static randomness** that guarantees the extraction of contextual information with a sufficient entropy when the devices are static and finally, the **unpredictability** aspect that guarantees the unfeasibility of a prediction attack on the contextual measurements. There are multiple context-based schemes that use the audio as a source of randomness such as [18,29]. In the work of Schürmann et al. [29], the authors used an audio fingerprint of the energy fluctuation between the frequency bands coupled with a fuzzy commitment [16] in order to exchange a key between two co-located devices. Also, the work of Karapanos et al. [18] exploits the acoustic environment by computing a similarity score using the average of the maximum cross-correlation of audio samples applied on a set of one-third octave bands. This result is then compared to a fixed threshold to decide the co-presence of the devices. This metric is based on the unpredictability of the acoustic signals received in the dynamic scenarios where these schemes were tested. Unfortunately, this choice does not satisfy most of the previously mentioned criteria such as the location dependency and the static randomness in quite environments. In the work of Fomichev et al. [11], it has been proven that the microphones heterogeneity increases drastically the error rates of the contextual pairing, which makes the scheme less robust against contextual attacks. Also, we can never discard the risk of *audio amplification*, as discussed in [29], where the adversary uses a directional microphone to amplify the audio signals, which makes him able to reconstruct the fingerprint and get hold of the shared secret.

Another variant of contextual protocols relies on a number of metrics from the ambient radio environment as a proof of physical proximity such as the *Receiver Signal Strength Indicator* (RSSI) [23,28] and the *Channel State Information* (CSI) [33,34]. These protocols are based on the assumption that devices within a close range and using a high frequency radio technology perceive the same unpredictable changes in the signal strength in short periods of time. Therefore, they are able to extract high entropy contextual information that can be ultimately used in exchanging a secret or deriving an encryption key. This hypothesis satisfies our three main criteria mentioned above but it has been recently proven in [31] that the RSSI can be manipulated by the adversary. This attack has been demonstrated using a fake Wi-Fi access point on which the transmission power is adapted to the location of the target device so that it computes the wanted signal strength indicator. On the other hand, the CSI measurements represent the propagation of the signal in terms of scattering, fading and power decay with respect to their physical location. This metric becomes rapidly de-correlated between two devices as the distance between them increases. It is also highly unpredictable due to its dependency on the ambient environment as shown in [34]. Such properties of the CSI are used to provide a high random bit generation rate that can reach hundreds of bits per second. The authenticity and the

confidentiality of the secret are guaranteed against a passive attacker outside the *safe zone* but its resilience in the face of an active adversary is still considered under investigation since it has been theoretically proven feasible by the work of Zafer et al. [35]. In this paper, we combine the two types of secure device pairing protocols in order to benefit from the fast contextual secret agreement in the context-based schemes to reduce the pairing completion time in comparison with the protocols relying solely on the low data-rate Out-of-Band channels. Also, we exploit the advantages of the Out-of-Band channels in terms of security under a threat model which deals with an ambient environment controlled by the attacker. Such strong intruder represents the Achilles' heel of any existing contextual scheme, especially without the requirement of human interactions such as performing some pattern of movement or taping, as suggested in [15].

3 COOB

3.1 System Model

Our protocol is based on two main building blocks: a *contextual module* and an *Out-of-Band module*. These two components are used in an optimal manner to benefit from the advantages of both types of pairing. Our scheme does not rely on a specific sensing technology or a precise choice of an Out-of-Band channel. It takes as an input a *reliable* and *fast* contextual key agreement protocol and a *protected* OoB channel that guarantees the integrity and the authenticity of the information transmitted. The human interaction needed is only limited to placing the devices in close proximity and pushing a button, which is used as a way to provide user feedback about the correctness of the pairing process. This modular design gives the protocol two main advantages: an *adaptive nature* to the recent enhancements in both research directions and a *flexibility* toward the existing interfaces on the constrained objects. In the upcoming protocol description, we will apply a contextual extractor proposed in [34] due to its fast generation rate and a visual communication channel for the Out-of-Band module.

3.2 Assumptions and Threat Models

We take into account the scenario where two devices, Alice and Bob, try to pair by authenticating their public Diffie-Hellman keys exchanged over the In-Band channel. We assume that the *discovery* phase, where the two devices gain knowledge of each other, has been correctly established by the user. The details of this phase are considered out of the scope of this work. The target devices of our protocol need, based on the choice of the contextual part, a Bluetooth module to communicate on the In-Band channel and a Wi-Fi chipset able to extract the CSI measurements. Also, we need, based on the choice of the Out-of-Band channel, a LED and a button as interfaces on the initiator device, named Alice, a LED and a light-sensor as interfaces on the enrollee, named Bob. Additionally, we need enough computational power to handle the Diffie-Hellman key computations [8].

We take into account the existence of a powerful Dolev-Yao [9] adversary that is able to control both the In-Band channel and the ambient environment surrounding the pairing participants such as the audio, the radio (Wi-Fi, Bluetooth and GPS) and even the physical environment (temperature, humidity, altitude and their combinations). This capability is not limited to a single target device since we assume that the attacker can be in the same context as all of the legitimate objects for an unlimited period of time. Furthermore, in our analysis we consider the feasibility of computational attacks that are targeting the cryptographic functions that rely solely on a short secret as the source of randomness. This assumption makes the security evaluation of our scheme more realistic with respect to the use of short secrets to perform the ad-hoc pairing. Therefore, we assume the existence of two kind of attackers in our evaluation: the first one is an **ordinary contextual intruder** that is not able to suppress any existing contextual information and is not allowed inside a pre-defined *safe zone* fixed by the pairing scheme assumptions. The second one is a **sophisticated contextual intruder** that is able to sense and ultimately control the ambient environment, which makes him aware of the secret extraction outcome in both devices. The latter threat model might seem unrealistic but it has been proven in [31] that such attacks, against co-presence authentication systems, are possible using a form of a "ghost-and-leech" technique [19]. Due to the close proximity of the pairing parties, the adversary might use a leech and a ghost at the same place. The leech plays the role of an eavesdropping device that senses the environment and send it back to the attacker using a fast digital communication, i.e a microphone or a photo-sensor. On the other hand, the ghost plays the role of a device that controls the environment, i.e a speaker or a laser.

3.3 Our Proposal

In this section, we present a novel approach that combines an Out-of-Band based scheme with a context-based protocol to provide a usability improvement in term of reducing the pairing time in comparison with the previously proposed OoB-based protocols relying on a low-bandwidth Out-of-Band channel. Furthermore, our approach presents a security enhancement against a sophisticated contextual attacker without an extensive user involvement, which is not supported by the previously proposed contextual schemes. Our protocol takes advantage of a DH exponentiation that temporarily hides the real values of the public keys in order to reach the optimal security provided by our two hash verifications. Furthermore, this technique avoids the additional use of cryptographic commitment schemes to minimize the communication and computation costs required, as detailed in Sect. 3.3.

Our proposal is split into two main steps. First, we will briefly introduce, in the background Sect. 3.3, the contextual module where we will highlight the key aspects of the TDS protocol [34] used in our scheme. Then, we will explain our choice of the Visible Light Communication (VLC) as our Out-of-Band channel. Secondly, we will present the exchanges of our protocol, COOB, that combines the two previously mentioned blocks in an optimal manner in terms of time,

communication and computational efficiency by exploiting the advantages of a nonce exponentiation technique.

Background

Contextual Module

As mentioned above in Sect. 3.1, we will apply the fuzzy extractor used in the work of Xi et al. [34] that exploits the channel state readings from a Wi-Fi access point that is publicly agreed upon. Due to the close proximity of the two legitimate devices (within an authentication zone $0.4\lambda \approx 5$ cm), they receive highly correlated CSI amplitude measurements as highlighted in Fig. 1. The sensing of the ambient environment will be initiated by each device respectively at the beginning of the discovery phase.

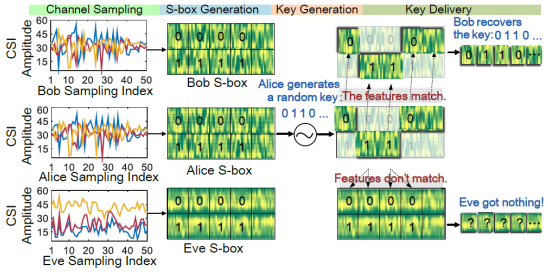

Fig. 1. The main steps of TDS [34]

After gathering a sufficient number of samples, Alice will try to synchronize the sampled data with the other device by sending a sequence of values to Bob marking the beginning of the valid samples that will be used in the encoding process. The S-box in our case will represent a $(2 \times l)$-matrix where l is the bit-length of the secret. Each element of the matrix will include a number $m \times n$ of CSI samples that uniquely represent a bit value 0 or 1, where m is the number of sub-carriers used and n is the number of measurements per sub-carrier. Thus, two consecutive $m \times n$ samples need to be distinct in order to reflect a 0 or a 1 bit. After uniquely identifying each block of the matrix, an l-bit secret is independently generated by Bob and then, for each bit, he sends its corresponding block in the S-box. As an example, if the secret starts with the sequence 0110 then Bob will send the first 0-block, the second 1-block, the third 1-block and the fourth 0-block as illustrated in Fig. 1. Since Alice has computed a similar S-box due to the reception of similar CSI samples, she will decide whether the received i^{th} block represents a 0 or a 1 bit value based on a comparison with her i^{th} column in her matrix. However, the adversary will not be able to reconstruct the original message due to his different measurements, which result in a different matching box. In this design, we will use Reed-Solomon (RS) codes to ensure that Alice can correct a number of bits fewer than a fixed limit. This will guarantee the reconstruction of the secret by only a legitimate

device inside the *authentication zone*. Readers willing to learn more about the TDS scheme can consult the original paper [34].

To simplify the protocol description in the upcoming sections, we will model this technique as a fuzzy-commitment scheme [16] that uses two similar contextual bit-values r_{c_a} and r_{c_b} generated respectively by Alice and Bob. These two variables will represent the S-box process of encoding and decoding based on the CSI features. The transfer of the blocks V_b by Bob will be modeled as $V_b = r_{c_b} \oplus Encode(r_b)$ where $Encode(.)$ is the Reed-Solomon encoding function. This message will be decoded on the other side using r_{c_a} as follows: $r_b = Decode(r_{c_a} \oplus V_b)$ where $Decode(.)$ is the Reed-Solomon decoding function. The feasibility of this modeling is due to the similarity between the concept of representing a bit by multiple random information and the idea of hiding its value using a random contextual bit and an XOR operation.

Out-of-Band Module

In our proposal, we need two Out-of-Band channels that limit the attacker capabilities to blocking, delaying and eavesdropping on the transmissions. These channels will be differentiated based on their nature and their degree of human interaction as described in Sect. 2. The first Out-of-Band channel will have the purpose of exchanging an authentication parameter and the second one will serve as a final validation step of the pairing. Due to the constrained nature of our target devices, we decided to choose a simple unidirectional visible light OoB channel based on a LED on the initiator (Alice) and a light sensor on the enrollee (Bob). This choice is based on the nature of the channel since it is hard for an attacker to replay or forge a message without being detected by the user. Also, it is less susceptible to the ambient noise than the acoustic or the haptic channels and easier to setup due to the close proximity assumption. For the second one, we decide to include a very limited user action represented by pushing a button on Alice after receiving a signal from Bob. This signal can vary between a vibration, a sound or a simple LED blink. This choice of human-aided channel will provide the user with an explicit feedback about the state of the pairing process.

Protocol Description

After the discovery phase, the devices become aware of each other and agree on the Diffie-Hellman public parameters (the cyclic group $\mathbb{G}$, the generator g and a big prime p). At the same time, they start sensing the environment in order to collect a sufficient number of samples to perform the contextual encoding and decoding operations. They generate their ephemeral DH private keys (a and b), two secret l-bit nonces (r_a and r_b) and they dpublic keys ($g^{a-r_a}\ mod\ p$ and $g^{b-r_b}\ mod\ p$). In addition, Alice generates a hashing key K_h to avoid any exhaustive search attempts on the nonce r_a using a simple hash output $h(ID_A, ID_B, g^a, r_a)$. To simplify the expressions, we will refer to the DH keys as g^{a-r_a} and g^{b-r_b}, without the modulus operation. In Fig. 2, we represent the In-Band exchanges by the black circles ●, while the blue ● and the red circles ● refer, respectively, to the Out-of-Band exchanges that are intended to perform the verification and the validation of the pairing.

Alice initiates the pairing process, as depicted in Fig. 2, by sending g^{a-r_a} to Bob along with its identifier ID_A and the keyed hash $h_{K_h}(ID_A, ID_B, g^a, r_a)$ in the message ❶ on the In-Band channel. Afterwards, she begins the construction of her S-box using the CSI values that come after the sequence S_A, which has been shared with Bob for synchronization purposes. At this point, the enrollee starts constructing his S-box using the CSI values that come after S_A. This operation is modeled by the construction of a contextual nonce r_{c_b}. Then, he transmits the parameters ID_B, g^{b-r_b} along with the fuzzy commitment scheme $V_b = r_{c_b} \oplus Encode(r_b || [g^{a-r_a}]_i^{i+l-1})$ to Alice in the message ❷ on the In-Band channel. The parameter i is computed as follows $i = r_b \ modulus \ (|g^{a-r_a}| - l)$ where the values $|g^{a-r_a}|$ and $[g^{a-r_a}]_i^{i+l-1}$ represent, respectively, the number of bits and an l-bit truncation of the modified public key g^{a-r_a} starting at the bit number i. At the reception of the previous message, Alice extracts the secret parameter $\hat{r_b}$ using her contextual parameter r_{c_a} as follows $\hat{r_b} || \widehat{[g^{a-r_a}]}_{\hat{i}}^{\hat{i}+l-1} = Decode(r_{c_a} \oplus \widehat{V_b})$. Then, she verifies the correctness of the reconciliation of $\hat{r_b}$ based on the verification of $\widehat{[g^{a-r_a}]}_{\hat{i}}^{\hat{i}+l-1}$. The l-bit verification of g^{a-r_a} is used to improve the contextual mismatch detection time, which provides a way to enhance the usability in the case of an inattentive user placing the devices far apart. At this point, Alice sends the XOR of the three values $\hat{r_b}$, r_a and $\widehat{[g^b]}_{\hat{j}}^{\hat{j}+l-1}$ in the message ❸ over the protected OoB channel. The parameter $\hat{j}$ is computed as follows $\hat{j} = \hat{r_b} \ modulus \ (|g^b| - l)$ and the symbol $\hat{x}$, in our description, represents an expected value x that is suspected to be modified by the adversary. Subsequently, Bob recomputes $\hat{r_a} = r_a \oplus \hat{r_b} \oplus \widehat{[g^b]}_{\hat{j}}^{\hat{j}+l-1} \oplus r_b \oplus [g^b]_j^{j+l-1}$ and sends to Alice a keyed hash $h_K(ID_A, ID_B, \widehat{g^a}, g^b)$, using the shared key $K = (g^{a-r_a}.g^{\hat{r_a}})^b$, in the message ❹ on the In-Band channel. Then, Alice verifies the keyed hash received in the previous message and she confirms the verification by sending the hashing key K_h to Bob in the message ❺ on the In-Band channel. Finally, Bob verifies the keyed hash received in message ❶. Then, he provides a signal to the user, in the message ❻, to notify Alice of his validation by asking him to push a button on the other device.

The reason behind the use of the nonce exponentiation is to temporarily hide the real values of the legitimate devices DH public keys from the attacker. This secrecy is needed to guarantee the correctness of the hash verification of Alice. To better explain this requirement, we will describe an attack scenario. First, we start by assuming that we use the real DH keys instead of the hidden ones. The adversary injects his own DH public key g^x in the message ❷. At this point, the adversary has a perfect knowledge of the secret DH key computed by Alice, $K_A = g^{xa}$. Therefore, he has all the parameters needed to recompute the keyed hash sent in message ❹ which will lead to bypassing the verification on Alice's side even when the value of Bob's nonce in the contextual commitment, sent in message ❷, has not been revealed by the attacker. As a consequence, the use of the real values of the DH public keys bounds the protocol security to a single hash verification instead of two. Thus, we will have only l bits of

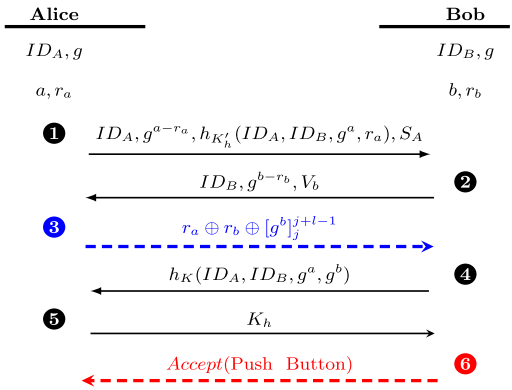

Fig. 2. COOB: Hybrid key agreement scheme (Color figure online)

security when we used $2l$ bits of authenticated exchanges against an ordinary contextual intruder which is not optimal. One possible solution to this issue is to use a commitment scheme, which needs two separate messages to provide the temporary secrecy property for a single public key. This requirement adds in a computation and communication cost of 4 exchanges for the two keys. This complexity can be easily avoided using the DH exponentiation to hide the public values while relying on a fuzzy commitment scheme that is based on a random ambient information source. Also, this contextual technique makes the ordinary contextual attacker unable to reveal the values of the nonces for the entire protocol run with the exception of a successful random guess. Accordingly, this provides a permanent confidentiality of these security parameters instead of a temporary property. This approach makes the protocol optimal in term of security with less computational cost than the first proposal and, most of all, without adding a communication cost.

This novel approach combines two pairing techniques using two short nonces as a way of hiding the legitimate DH public keys from the attacker in order to prove their authenticity later on based on two hash verifications. The values r_a and r_b are protected by the discrete logarithm problem, which makes it hard for an adversary to retrieve them from the keys g^{a-r_a} and g^{b-r_b}, especially without the knowledge of the private keys a and b. To the best of the authors' knowledge, COOB is the first scheme that combines the contextual and the OoB based pairing. This has been made possible using the exponential challenge-response technique that hides Alice's DH public key g^a. This security measure makes the adversary unable to recompute the keyed hash and fail to bypass the verification. Our hybrid protocol relies on a very constrained set of human interactions that consists of placing the devices in close proximity and pushing a button on the initiator (Alice) to confirm the pairing.

There are two main advantages with respect to each category of pairing mechanisms. **In comparison with the previously proposed context-based schemes**, we provide an attack success probability of 2^{-l} against a sophisticated

contextual attacker that is able to violate the safe zone without detection and to completely control the environment. **In comparison with the same OoB-based protocol structure that only uses the Out-of-Band channel to transfer** $2 \times l$**bits**, we provide less pairing completion time due to the fast generation of the contextual information relying on TDS [34], which takes at maximum 2 s to agree on a 256-bit key. However, an average time of 8.6 s is required for a 6-digit numerical comparison, performed by the user, with a 10% mismatch rate related to human factor errors, as stated in the work of Kumar et al. [20]. The usage of automated pairing schemes that are highly preferred by the study participants, such as HAPADEP [32] and Blinking Lights [26], scores between 10.6 and 28.8 s only for exchanging a 15-bit authentication string. Therefore, for sending $2l$ bits on the out-of-Band channel, we would need twice the time, which is not convenient for the user.

4 Security Analysis

4.1 Security Evaluation

We begin our analysis by assuming, at this moment, that the attacker is **outside the safe zone**, which makes him unable to predict or to collect the same contextual information measured by the two legitimate devices. Therefore, he is unable to send his own contextual commitment.

A MitM attack scenario starts by blocking the message of Alice ❶ and by replacing it with the following construction: $ID_A, g^{a'-r'_a}, h_{K'_h}(ID_A, ID_B, g^{a'}, r'_a)$, where x' represents an attacker induced value. Then, the adversary blocks the message ❷ and sends to Alice his own version: $ID_B, g^{b'-r'_b}, V_e$. The parameter V_e can be a legitimate contextual commitment computed by Bob or an old one replayed by the attacker. Afterwards, Alice retrieves the nonce $\hat{r_b} = Decode(r_{c_a} \oplus V_e)$ and sends the message ❸, that contains the value $r_a \oplus \hat{r_b} \oplus \widehat{[g^{b'-r'_b+\hat{r_b}}]}_{\hat{j}}^{\hat{j}+l-1}$, over the protected Out-of-Band channel which guarantees the integrity and the authenticity. Subsequently, Bob retrieves $\hat{r_a}$ using the following equation:

$$\hat{r_a} = r_a \oplus \hat{r_b} \oplus \widehat{[g^{b'-r'_b+\hat{r_b}}]}_{\hat{j}}^{\hat{j}+l-1} \oplus r_b \oplus [g^b]_j^{j+l-1} \tag{1}$$

Using $\hat{r_a}$, Bob recomputes the public key of Alice $\widehat{g^a} = g^{a'-r'_a+\hat{r_a}}$ and the DH secret key $\widehat{K_B} = g^{ba'}$. Then, he uses it to compute the second verification hash $h_{\widehat{K_B}}(ID_A, ID_B, g^{a'-r'_a+\hat{r_a}}, g^b)$ and sends it to Alice in the message ❹. The initiator verifies the hash using her key $K_A = g^{a(b'-r'_b+\hat{r_b})}$ and sends the hashing key K_h to Bob in the message ❺, which will be blocked and replaced by K'_h. At this moment, Bob is able to verify the keyed hash received in the message ❶ using the parameter K'_h induced by the adversary, the nonce $\hat{r_a}$ and the public key $\widehat{g^a} = g^{a'-r'_a+\hat{r_a}}$.

The easiest way for the attacker to bypass the hash verification of Alice, **hash verification I**, is to block the message ❹ and recompute the initiator

key $K_A = g^{a(b'-r'_b+\hat{r_b})}$ but he can only compute $K_E = g^{b'(a-r_a+r'_a)}$. This means that the optimal solution for the attacker is to use the legitimate contextual information $V_e = V_b$ in order to have the equality $\hat{r_b} = r_b$ and to satisfy the equation

$$r'_b = r_b \tag{2}$$

As for the hash verification of Bob, **hash verification II**, the attacker needs to satisfy the following equation when constructing the message ❶:

$$r'_a = \hat{r_a} \tag{3}$$

To summarize the results of the previous security analysis, the attacker needs to satisfy two main conditions

$$\begin{cases} r'_a = \hat{r_a} \\ r'_b = r_b \end{cases}$$

The parameters r'_a and $\hat{r_a}$ are completely independent as shown in Eq. 1, which means that we have an attack success probability $P_{s_B} = 2^{-l}$. The same property applies on the values r'_b and r_b, which provides an attack success probability of $P_{s_A} = 2^{-l}$.

The two verifications are sequential, which means that the execution of the second phase depends on the success of the first one. Therefore, the total success probability of the whole MitM attack is $P_s = P_{s_A} \times P_{s_B} = 2^{-2l}$. This analysis is better highlighted in Table 1 where the assumptions on Eq. 3 and Eq. 2 are made and the corresponding success probabilities are computed. In this context, $m_A = |h_K(ID_A, ID_B, \widehat{g^a}, g^b)|$ and $m_B = |h_{K_h}(ID_A, ID_B, g^a, r_a)|$ were used to express the probability of a collision on the hash functions. Based on this analysis, the MitM attack success probability is bounded by 2^{-2l}.

In the case of an **ordinary contextual attacker**, we will have the same results as the ones indicated in Table 1. This fact is explained by the confidentiality assumption on the contextual information, which protects the parameters r_a and r_b from being revealed by the adversary.

In the case of a **sophisticated contextual attacker**, he has the capacity to gain knowledge of Bob's secret r_b based on computing an S-box similar to the

Table 1. MitM attack success probability

Verification phases	$r'_a = \hat{r_a}$ & $r'_b \neq r_b$	$r'_a \neq \hat{r_a}$ & $r'_b \neq r_b$	$r'_a \neq \hat{r_a}$ & $r'_b = r_b$	$r'_a = \hat{r_a}$ & $r'_b = r_b$
Hash verification I	✗	✗	✓	✓
Hash verification II	✗	✗	✗	✓
Upper bound of the successful attack probability	2^{-m_A}	$2^{-(m_A+m_B)}$	2^{-m_B}	2^{-2l}

ones constructed by the legitimate devices. Even though he knows Bob's true DH public key g^b and Alice's secret based on the message ❸, he still has to satisfy Eq. 3, which still guarantees the mutual authentication with an attack success probability $P_s = 2^{-l}$. To the best of the authors' knowledge, this property is not maintained by any context-based protocol relying on the unpredictability aspect of the ambient environment.

4.2 Formal Validation

To validate the correctness of the protocol in the symbolic model, we perform a formal verification using the TAMARIN prover [24], a powerful validation tool for security protocols. In our analysis, we begin with the evaluation of the confidentiality of the secret keys and nonces of Alice and Bob. Then, we evaluate an authentication property referred to as *injective agreement* [22]. This lemma verifies that the protocol guarantees to Alice that if she completes a protocol run with Bob to agree on a key K, then Bob has been apparently running the protocol with Alice and the two devices agreed on the same value. This property will be tested in both ways to guarantee a mutual authentication as mentioned in our code[1]. The multiple-session attack was not considered in our evaluation since we have no persistent secret during multiple protocol executions. These assumptions reflect the consequences of a Man-in-the-Middle attack where the adversary performs the actions described in Sect. 4.1.

This tool adopts the Dolev-Yao intruder model on its public channel, which grants the attacker with a complete control over it. Thus, it satisfies our attacker model requirements on the In-Band channel. However, the protected Out-of-Band channel is modeled in the tool such that it prevents the attacker from forging or replaying any messages. As for the *blocking* and the *delaying* actions, the adversary is already able to temporarily or permanently stop the process of sending an information, even on the protected channel. Our sophisticated contextual attacker is represented as a Dolev-Yao intruder that has perfect knowledge of contextual information of the two devices, r_{c_a} and r_{c_b}, which grants him a perfect reconstruction of the nonce r_b. Even though there is a lack of a modular exponentiation in the tool, we can model, to a certain degree, these operations to reach the full capabilities of the intruder. Nonetheless, the XOR properties were recently modeled in TAMARIN v1.4.1 but the tool does not support multiple executions of this operation, as required in message ❸ on the Out-of-Band channel. This computational burden is caused by the multiple algebraic properties of the XOR. To ease the computation, we modeled our own approximation of the XOR operation using a simpler constructor functions $xorc(.,.)$ to apply the operation on two variable inputs.

To guarantee the correctness of the protocol execution, a set of restrictions must be indicated in the TAMARIN model. We enforced the use of an initialization rule that provides all the devices with the same contextual information. We

[1] The TAMARIN model of COOB can be found in https://github.com/samehkhalfaoui/COOB-TAMARIN-model/blob/master/COOB_model.spthy.

imposed also the uniqueness of the private DH keys and of the authentication nonces to avoid any multi-session attack. Finally, we apply the hash equality restriction that stops the protocol run when the hash verification does not hold, which represents the case of an attack detection.

Table 2. COOB evaluated properties in the symbolic model

Property	Result	
	Ordinary contextual attacker	Sophisticated contextual attacker
Secrecy of r_c	✓	✗
Secrecy of r_a	✓	✗
Secrecy of r_b	✓	✗
Secrecy of Alice's key	✓	✓
Secrecy of Bob's key	✓	✓
Alice-to-Bob injective agreement	✓	✓
Bob-to-Alice injective agreement	✓	✓

The results of the lemmas highlighted in Table 2 validate the robustness of our protocol in the symbolic model even in the presence of a sophisticated contextual attacker that can break the secrecy of the authentication nonces during the protocol run. The outcomes are either ✓ when the property is validated or ✗ when the property does not hold and an attack trace is provided by the tool. We use the automated proofs with the default heuristic and the default proof tree exploration. The validation lasts 84 mins and is conducted on a computer with an Intel(R) Core^{TM} i5 − 9400H CPU @ 2.5 GHz × 8 processor, 32 GB of RAM, running Ubuntu 18.04.4 LTS.

Moreover, this analysis shows that an attacker will not be able to mount an MitM attack resulting in the agreement on different keys on each device and guarantees the secrecy of the computed key has been validated for both Alice and Bob. Therefore, this analysis validates the mutual authentication property between the legitimate pairing parties chosen by the user and the secrecy of the communication link established for the post pairing phase. The case of multi-session attacks has not been addressed in this validation for two reasons. First of all, it adds significant computation cost due to the unbounded number of sessions that needs to be considered. Secondly, our scheme regenerates fresh parameters at the beginning of each session, which makes the assumption of having persistent security knowledge between two distinct protocol runs invalid. Therefore, relying on the security parameters from an earlier execution of the scheme is considered as a MitM attack where the adversary is trying to guess the appropriate nonce values, as explained in Sect. 4.1.

5 Implementation

5.1 Experimental Setting

We implement COOB using Python 2 on two Raspberry Pi 4B. This choice of cards is mainly motivated by the simplicity of the extraction and the manipulation of the CSI measurements for a future implementation of the contextual module. The first Raspberry Pi is connected to a source of light, for example an LED, and the second one is connected to a photo-resistor in order to construct a protected visual OoB channel. We use the Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol based on a Koblitz curve secp256k1, SHA-256 for hashing and Bluetooth as our In-Band channel. As for the choice of the elliptic curve domain parameters, we use by default in our implementation the recommended specifications provided in [5].

The Out-of-Band module apply an On-Off Keying (OOK) modulation and it takes 0.2 s to send one bit value. This transmission rate is explained by the choice of the photo-resistor and the capacitor at the receiving side as shown in Fig. 3. This RC light detection circuit is used because of the digital nature of the Raspberry Pi pins and their inability to read analogue inputs. Therefore, the charging time of the RC circuit is used as a reference when applying an internal counter to detect the existence of a light pulse when compared with a threshold computed with regard to the ambient luminosity level at the time of pairing.

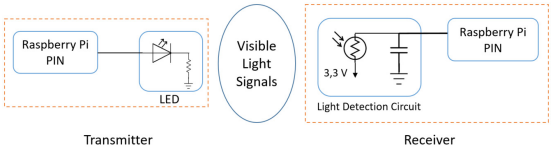

Fig. 3. Visual Out-of-Band channel design

The contextual module is assumed to apply a reconstruction threshold that represents the maximum number of bits that can be corrected by the Reed-Solomon codes during the secret reconciliation phase. We fixed the value of the threshold to 20% of the total hidden value bit-length $|r_b| + |[g^{b-r_b}]_j^{j+l-1}| = 2 \times l$ to tolerate any encoding errors by the legitimate devices. This fault tolerance is expected to increase the contextual secret message bit-length $|V_b| = \lceil 2.4 \times l \rceil$ while providing a more reliable encoding scheme.

5.2 Preliminary Performance Evaluation

For the moment, we compute an estimation of the time needed by the chosen contextual module, based on the published results of the TDS protocol performance in the work of Xi et al. [34], in order to approximate the pairing time required by our hybrid protocol COOB. First, we refer to a metric denoted *bit*

generation rate that represents the number of secret bits that are agreed upon by both devices over the whole protocol execution time. This measure includes the time required for the CSI information extraction, the S-Box computation and the transfer of the encoded bits. For a distance separating the two devices ranging between 3 and 4 cm, the TDS secret bit generation rate ranges between 100 to 180 bits per second for multiple scenarios, both static and mobile. In our analysis, we take the average value of 140 bits per second to approximate the required time for pairing to estimate the performance COOB in comparison with an OoB-based pairing protocol that transfers $2l$ bits. These two scheme provide the same level of security. In order to clearly evaluate the performance of our scheme, we compare it to the same protocol design in terms of exchanges, key manipulation and cryptographic primitives but without the contextual module. The pairing time of the $2l$-bit Out-of-Band scheme was averaged over 10 protocol runs that were conducted for a number of bits l varying between 16 and 80 bits. The results were analyzed to provide a time percentage gain that reflects the added value of our modular hybrid design.

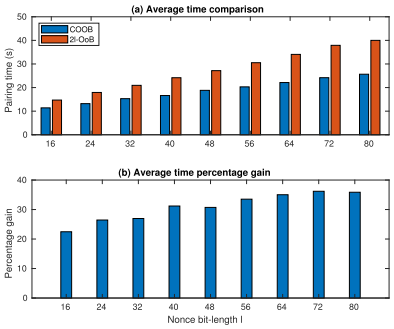

Fig. 4. Pairing time performance comparison: COOB vs 2l-OoB scheme

As highlighted in Fig. 4-(a), the pairing time imposed by a solely OoB-based scheme that sends $2l$ bits on the Out-of-Band channel grows rapidly to reach 40 s for a bit-length $l = 80$ bits. Our implemented OoB-based protocol achieves a better performance compared to the published usability results in the work of Kumar et al. [20] that take on average 28.8 s for $l = 15$ bits on a visual channel. Therefore, we will be using our OoB pairing protocol performance results to conduct a more realistic comparative study. Our hybrid scheme takes advantage of the fast contextual agreement module to keep the required association time within a reasonable limit equal to 25 s. This comparison is better described using a time percentage gain that reflects COOB pairing time reduction while maintaining the same level of security. This time optimization ranges between 22 and 39%, as shown in Fig. 4-(b), for a nonce bit-length l between 16 and 80. In a high security level scenario, a higher secret bit-length is required for both the DH keys and the nonces, which makes the use of a typical OoB-based

scheme extremely unsuitable. Furthermore, the risk of dealing with a sophisticated contextual attacker prevents the use of a context-based pairing scheme. These inconveniences can be mitigated using COOB since the time gain can exceed 50% of the whole pairing time required by the other OoB-based schemes and a level of security can be assured by the use of an Out-of-Band channel that only transfers half of the authentication bits.

Our hybrid design guarantees a optimal pairing time in comparison with the other schemes that rely on low-bandwidth Out-of-Band channels. This time reduction enhances the usability aspect of the device pairing process without demanding an extensive user involvement. Also, this can also be handy in the case of a group device pairing where the time of use of an Out-of-Band channel grows linearly with the number of paired devices. Thus, applying our pairwise pairing scheme to this scenario will provide a further time optimization in comparison with the use of multiple OoB communications.

6 Conclusion

In this paper, we designed a hybrid secure device pairing protocol that efficiently combines the use of an Out-of-Band channel with an existing fast contextual encoding scheme. Our protocol exploits a Diffie-Hellman nonce exponentiation approach, applied in the context of device pairing, that achieves the temporary secrecy goal desired in the key authentication process. The use of this technique results in an optimal computation and communication cost in comparison with the traditional cryptographic commitment schemes. This technique imposes an optimal computation and communication cost in comparison with the traditional cryptographic commitment schemes.

COOB provides security against a sophisticated contextual attacker that completely controls the ambient environment. This adversary model is not supported by the existing context-based device pairing protocols. In addition, we formally validated our design in the symbolic model using the TAMARIN prover. Furthermore, our scheme reduces the pairing time up to 39% compared to the OoB-based schemes by relying on a state-of-the-art fast contextual pairing protocol. This optimization enhances the usability and the reliability aspects in comparison with the existing OoB-based schemes.

Acknowledgement. This work was supported by the SEIDO lab (The joint research laboratory for Security and Internet of Things between EDF R&D and Télécom Paris.). The authors would like to thank Dr. Ivan GAZEAU for his support in the formal verification of the protocol.

References

1. Akter, S., Chakraborty, T., Khan, T.A., Chellappan, S., Al Islam, A.A.: Can you get into the middle of near field communication? In: 2017 IEEE 42nd Conference on Local Computer Networks (LCN), pp. 365–373. IEEE (2017)

2. Alliance, W.F.: Wi-fi simple configuration technical specification, version 2.0. 5 (2014)
3. Balfanz, D., Smetters, D.K., Stewart, P., Wong, H.C.: Talking to strangers: Authentication in ad-hoc wireless networks. In: NDSS. Citeseer (2002)
4. Bluetooth, S.: Bluetooth core specification v5. 0. Bluetooth Special Interest Group: Kirkland, WA, USA (2016)
5. Brown, D.R.: Recommended elliptic curve domain parameters. Standards Efficient Cryptogr. Group Ver **1** (2010)
6. Burrows, M., Abadi, M., Needham, R.M.: A logic of authentication. Proc. Royal Soc. London. A. Math. Phys. Sci. **426**(1871), 233–271 (1989)
7. Claycomb, W.R., Shin, D.: Extending formal analysis of mobile device authentication. J. Internet Serv. Inf. Secur. **1**(1), 86–102 (2011)
8. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theor. **22**(6), 644–654 (2006). https://doi.org/10.1109/TIT.1976.1055638
9. Dolev, D., Yao, A.: On the security of public key protocols. IEEE Trans. Inf. Theory **29**(2), 198–208 (1983)
10. Fomichev, M., Álvarez, F., Steinmetzer, D., Gardner-Stephen, P., Hollick, M.: Survey and systematization of secure device pairing. IEEE Commun. Surv. Tutorials **20**(1), 517–550 (2017)
11. Fomichev, M., Maass, M., Almon, L., Molina, A., Hollick, M.: Perils of zero-interaction security in the internet of things. Proc. ACM Interactive, Mobile, Wearable and Ubiquitous Technol. **3**(1), 10 (2019)
12. Gehrmann, C., Mitchell, C.J., Nyberg, K.: Manual authentication for wireless devices. RSA Cryptobytes **7**(1), 29–37 (2004)
13. Goodrich, M.T., Sirivianos, M., Solis, J., Tsudik, G., Uzun, E.: Loud and clear: human-verifiable authentication based on audio. In: 26th IEEE International Conference on Distributed Computing Systems (ICDCS 2006), p. 10. IEEE (2006)
14. Halevi, T., Saxena, N.: Acoustic eavesdropping attacks on constrained wireless device pairing. IEEE Trans. Inf. Foren. Secur. **8**(3), 563–577 (2013)
15. Jin, R., Shi, L., Zeng, K., Pande, A., Mohapatra, P.: Magpairing: Pairing smartphones in close proximity using magnetometers. IEEE Trans. Inf. Foren. Security **11**(6), 1306–1320 (2015)
16. Juels, A., Sudan, M.: A fuzzy vault scheme. Designs, Codes and Cryptography **38**(2), 237–257 (2006)
17. Kainda, R., Flechais, I., Roscoe, A.: Usability and security of out-of-band channels in secure device pairing protocols. In: Proceedings of the 5th Symposium on Usable Privacy and Security, p. 11. ACM (2009)
18. Karapanos, N., Marforio, C., Soriente, C., Capkun, S.: Sound-proof: usable two-factor authentication based on ambient sound. In: 24th {USENIX} Security Symposium ({USENIX} Security 15), pp. 483–498 (2015)
19. Kfir, Z., Wool, A.: Picking virtual pockets using relay attacks on contactless smartcard. In: First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM 2005), pp. 47–58. IEEE (2005)
20. Kumar, A., Saxena, N., Tsudik, G., Uzun, E.: A comparative study of secure device pairing methods. Pervasive Mob. Comput. **5**(6), 734–749 (2009)
21. Lee, K., Raghunathan, V., Raghunathan, A., Kim, Y.: Syncvibe: fast and secure device pairing through physical vibration on commodity smartphones. In: 2018 IEEE 36th International Conference on Computer Design (ICCD), pp. 234–241. IEEE (2018)

22. Lowe, G.: A hierarchy of authentication specifications. In: Proceedings 10th Computer Security Foundations Workshop, pp. 31–43. IEEE (1997)
23. Mathur, S., Miller, R., Varshavsky, A., Trappe, W., Mandayam, N.: Proximate: proximity-based secure pairing using ambient wireless signals. In: Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services, pp. 211–224 (2011)
24. Meier, S., Schmidt, B., Cremers, C., Basin, D.: The TAMARIN prover for the symbolic analysis of security protocols. In: Sharygina, N., Veith, H. (eds.) CAV 2013. LNCS, vol. 8044, pp. 696–701. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39799-8_48
25. Mirzadeh, S., Cruickshank, H., Tafazolli, R.: Secure device pairing: a survey. IEEE Commun. Surv. Tutorials **16**(1), 17–40 (2013)
26. Saxena, N., Ekberg, J.E., Kostiainen, K., Asokan, N.: Secure device pairing based on a visual channel. In: 2006 IEEE Symposium on Security and Privacy (S&P'06), pp. 6-pp. IEEE (2006)
27. Saxena, N., Uddin, M.B., Voris, J., Asokan, N.: Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal RFID tags. In: 2011 IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 181–188. IEEE (2011)
28. Scannell, A., Varshavsky, A., LaMarca, A., De Lara, E.: Proximity-based authentication of mobile devices. Int. J. Secur. Networks **4**(1–2), 4–16 (2009)
29. Schürmann, D., Sigg, S.: Secure communication based on ambient audio. IEEE Trans. Mob. Comput. **12**(2), 358–370 (2011)
30. Sen, J.: Security in wireless sensor networks. Wireless Sensor Netw. Current Status and Future Trends **407**, 408 (2012)
31. Shrestha, B., Saxena, N., Truong, H.T.T., Asokan, N.: Sensor-based proximity detection in the face of active adversaries. IEEE Trans. Mob. Comput. **18**(2), 444–457 (2018)
32. Soriente, C., Tsudik, G., Uzun, E.: HAPADEP: human-assisted pure audio device pairing. In: Wu, T.-C., Lei, C.-L., Rijmen, V., Lee, D.-T. (eds.) ISC 2008. LNCS, vol. 5222, pp. 385–400. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85886-7_27
33. Xi, W., Li, X.Y., Qian, C., Han, J., Tang, S., Zhao, J., Zhao, K.: Keep: fast secret key extraction protocol for d2d communication. In: 2014 IEEE 22nd International Symposium of Quality of Service (IWQoS), pp. 350–359. IEEE (2014)
34. Xi, W., et al.: Instant and robust authentication and key agreement among mobile devices. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 616–627. ACM (2016)
35. Zafer, M., Agrawal, D., Srivatsa, M.: Limitations of generating a secret key using wireless fading under active adversary. IEEE/ACM Trans. Networking **20**(5), 1440–1451 (2012)
36. Zhang, B., Ren, K., Xing, G., Fu, X., Wang, C.: Sbvlc: Secure barcode-based visible light communication for smartphones. IEEE Trans. Mob. Comput. **15**(2), 432–446 (2015)