SolarKey

Battery-free Key Generation Using Solar Cells

Bo, W. E.I.; Weitao, X. U.; Mingcen, G. A.O.; Guohao, L. A.N.; Kai, L. I.; Chengwen, L. U.O.; Zhang, J. I.N.

DOI
10.1145/3605780

Publication date
2023

Document Version
Final published version

Published in
ACM Transactions on Sensor Networks

SolarKey: Battery-free Key Generation Using Solar Cells

BO WEI, Newcastle University, United Kingdom
WEITAO XU, City University of Hong Kong SAR, China
MINGCEN GAO,
GUOHAO LAN, Delft University of Technology, The Netherlands
KAI LI, CISTER Research Centre, Portugal
CHENGWEN LUO and JIN ZHANG, Shenzhen University, China

Solar cells have been widely used for offering energy for Internet of Things (IoT) devices. Recently, solar cells have also been used as sensors for context awareness sensing due to their sensitivity to varying lighting conditions. In this article, we are the first to use solar cells for symmetric key generation. To generate symmetric keys, we take advantage of photovoltage measurements generated from solar cells equipped with a pair of IoT devices. Symmetric keys are essential for pairing IoT devices and further securing wireless communication. Despite the sensitivity to varying lighting conditions, challenges still remain for the use of solar cells for key generation, such as time unsynchronisation and noisy measurements. To solve these challenges, we design a novel key generation framework, SolarKey, which includes the starting point detection and a compressed sensing-based two-tier key reconciliation method. Extensive experiments have been conducted to evaluate the performance of our proposed key generation method in various environments, which shows the proposed method can improve the key matching rate by up to 25%. We also conduct security analysis and the randomness test, which shows that SolarKey is resilient to common attacks such as the eavesdropping attack and the imitating attack and sufficiently random.

CCS Concepts: • **Security and privacy → Symmetric cryptography and hash functions**; • **Human-centered computing → Ubiquitous and mobile devices;**

Additional Key Words and Phrases: Key generation, battery free, solar cells, compressed sensing

ACM Reference format:
Bo Wei, Weitao Xu, Mingcen Gao, Guohao Lan, Kai Li, Chengwen Luo, and Jin Zhang. 2023. SolarKey: Battery-free Key Generation Using Solar Cells. *ACM Trans. Sensor Netw.* 20, 1, Article 7 (October 2023), 24 pages.
https://doi.org/10.1145/3605780

1 INTRODUCTION

Recently, **Internet of Things (IoT)** devices have been becoming ubiquitous in smart homes, smart factories, smart farms, and so on. Due to the large scale of deployment, IoT devices usually adopt

Authors' addresses: B. Wei (corresponding author), Newcastle University, Urban Sciences Building, 1 Science Square, Newcastle upon Tyne, NE4 5TG, United Kingdom; email: bo.wei@newcastle.ac.uk; W. Xu, City University of Hong Kong, Unit 20D, Man Lai Court Tower 1, No 49 Man Lai Road, Tai Wai, Hong Kong SAR China, 999077; email: weitaoxu@cityu.edu.hk; M. Gao, Working in Google, 1507 El Oso Dr, San Jose, California, United States, 95129; email: gaomingcen@gmail.com; G. Lan, Department of Software Technology, Delft University of Technology, Van Mourik Broekmanweg 6, 2628 XE Delft, The Netherlands; email: g.lan@tudelft.nl; K. Li, CISTER Research Centre, Rua Dr. António Bernardino de Almeida 431, 4249-015 Porto, Portugal; email: kai@isep.ipp.pt; C. Luo and J. Zhang, 3688 Nanhai Avenue, Shenzhen University, Shenzhen, China, 518060; email: {chengwen, jin.zhang}@szu.edu.cn.

1550-4859/2023/10-ART7 $15.00
https://doi.org/10.1145/3605780

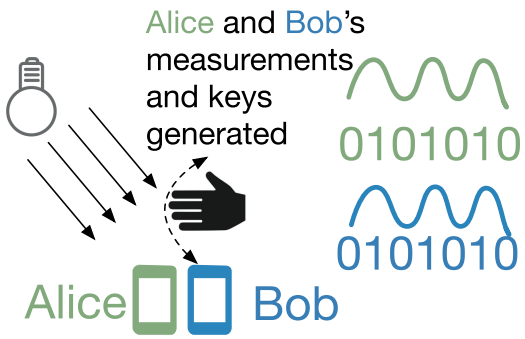


Fig. 1. Proposed system.

wireless communication to share data with the assistance of the integration of radio chips (such as WiFi, Bluetooth, LoRa, etc.). However, the broadcast nature of wireless communication offers weaker security than wired communication. The cryptographic key agreement is necessary to secure wireless **device-to-device (D2D)** communication. Public key cryptography is a popular solution for securing wireless communication, but the heavy computation of public key generation solution makes its large-scale application on resource-constrained IoT devices infeasible [13, 43, 46]. Therefore, IoT devices usually use symmetric key cryptography instead for the confidentiality and integrity of wireless communication.

Many secret key generation methods have been proposed in the literature based on wireless channel characteristics [43, 46, 49], ambient audio signal [12, 33], and motion sensors [11, 34, 48]. However, one key limitation of these systems is the huge energy consumption from sensor data collection, which generates a significant burden for resource-constrained IoT devices. This leads to the advantage of using solar panels, which, as energy harvesters, do not require any energy to power themselves. A vision for IoT devices in future is to be battery-free, i.e., IoT will be self-powered by energy harvesters. We can envision that IoT devices, such as smartwatches, mobile phones, and environment monitoring sensors, will no longer need batteries. As one of the promising energy harvesting techniques, solar cells have been widely used in IoT devices as a substitution for traditional batteries. Many context awareness applications have also been enabled by solar-powered devices, thanks to the sensitivity of solar cells to ambient illuminations [19, 38]. We can envision in the future that more IoT devices will be solar-powered to solve the constraints of batteries. As novel side-channel information, the energy harvesting patterns provide us with a unique chance for key generation. Unfortunately, how to achieve efficient and secure D2D communication for these solar-powered devices is a completely new research problem and has not been studied yet.

To bridge this gap, we conduct the first study to investigate the feasibility of using solar cells to generate symmetric keys for IoT devices. Our study is based on the fact that amplitudes of photovoltage measurements from solar cells are decided by the lighting conditions of the surrounding environment. Therefore, two neighbouring solar cells can be interfered with by similar active lighting condition variance (as shown in Figure 1). In Figure 1, Alice and Bob are two legal users who use IoT devices equipped with solar panels. The active lighting condition variance can be sensed by those solar cells integrated into IoT devices, which is then used to generate symmetric keys. Another advantage of this method is to eliminate the use of **certification authority (CA)**, as in the IoT context, CA is not always available. Another advantage of this application is that it does not need frequent wireless communication compared with the wireless channel-based key generation methods [21, 37, 43, 51], network-based time synchronisation methods.

One motivation application scenario of the proposed method is social interaction. Here, we show two application scenarios:

— Application Scenario 1: Two users could put solar cell–powered mobile devices (e.g., smart watches and mobile phones) in the vicinity and shake hands over those mobile devices. Using our proposed system, we aim to explore interference to solar cells integrated into mobile devices, which will trigger symmetric key generation. The generated keys will be used for paring and sharing information between two parties, such as exchanging e-business cards, friending each other on social networks, and so on.
— Application Scenario 2: Another application scenario is device paring for nearby devices, such as a user's wearable bands without touchscreens. The conducted gestures over devices can trigger the pairing devices instead of pairing with conventionally inputting secret code.

To achieve an efficient and robust key generation system for solar-powered IoT devices, we need to address the following non-trivial challenges:

— ***Challenge 1:*** The accurate time synchronisation between the pair of devices is critical to ensure a high key agreement rate. Several shifting bits between a pair of devices during key generation could result in a large number of mismatches from the subsequent measurements. To facilitate time synchronisation for IoT application scenarios, many proposed methods are based on the communication delay [20, 25, 41]. In contrast, we propose to apply photovoltage measurements directly for time synchronisation. Compared with timestamp-based time synchronisation methods, our proposed method can mitigate the synchronisation error caused by poor quality wireless communication as well as reduce frequent wireless transmission caused by network-based time synchronisation.
— ***Challenge 2:*** The second challenge is the decrements in the key matching rate due to the device noise and the sensitivity of solar cells. Measurements from solar panels are 1-dimensional photovoltage. Although the collection of measurements from solar panels does not require any energy, its low resolution signals cannot provide much information as other high dimensional measurements, such as cameras capturing QR codes. To address this challenge, we exploit a two-tier key reconciliation method to enhance the key matching rate. Specifically, the two tiers remove the ambiguous bits and conduct key corrections. To increase the confidentiality of our proposed key matching method, we leverage a *compressed sensing*-based key reconciliation method to increase key generation performance while defending against malicious attackers.

To summarise, the contributions of the article are shown as follows:

— To the best of our knowledge, the proposed work is the first to use solar cells to enable key generation.
— We propose a novel and effective time synchronisation method and key generation method with the use of compressed sensing theory. A novel two-tier reconciliation method is used to remove the ambiguous bits and correct the mismatched keys. The compressed sensing-based reconciliation method has been leveraged to improve the key matching rate.
— Extensive evaluations in the real environment have been conducted to show the performance and efficacy of our proposed method. We also conduct a security analysis to show the potential attacks and the secureness of the proposed method against these attacks.

In the rest of this article, Section 2 discusses the related works. Section 3 shows the feasibility study. Followed by that, Section 4 shows the details of our designed battery-free key generation method, SolarKey. In Section 5, we perform extensive evaluations in real environments and evaluate the proposed method to show its efficacy and robustness. Section 6 shows attack models and performs security analysis. Section 7 concludes the article.

2 RELATED WORKS

2.1 Key Generation Method

Many key generation methods have been proposed for IoT D2D communication. In this section, we show the details of the existing methods.

Two devices in the physical vicinity can have similar observations from collected signals of sensors, which have been leveraged for key generation. Many types of signals have been used, such as radio signal [21, 37, 43, 51], audio [32], and surrounding context [24]. Specifically, Diffie-Hellman protocol, the public cryptographic key exchanging mechanism, was used in Reference [37] on radio signal to verify the physical proximity of a pair of devices. References [21, 51] eliminated the use of the Diffie-Hellman protocol but suffered from the low key generation rate. The surrounding context was adopted for key generation in Reference [24], but a relatively long duration was needed for obtaining sufficient information and paring devices.

Channel information in various wireless communication techniques has drawn much attention for key generation recently, such as ZigBee [9, 17], WiFi [16, 22, 42], and 5G [10]. Among these methods, the **Received Signal Strength Indicator (RSSI)** is a popular channel characteristic, but a consequential defeat for RSSI-based method is a low key generation rate. **Channel State Information (CSI)**-based method [43] is thus employed to increase the key generation rate, because CSI, obtained from the physical layer, has a higher resolution compared with RSSI. Furthermore, electromyogram sensors [49] and electrode sensors [28] can sense signal in body channel and thus are applied for key generation for body wearable devices.

Many other sensors available in mobile devices are also applied for key generation. Many research works studied the use of **Inertial Measurement Units (IMUs)** to detect the shared motions for key generation. References [8, 23] use the motions captured from IMUs to secure the authentication. References [31, 35, 48] use a similar philosophy and detected the activities for body wearable device pairing. Heartbeat, as a measurement without users' intervention, is applied for the key generation as well [15, 29, 45]. Additionally, acoustic signals have been used for key generation for mobile devices [2, 7, 12, 18, 32, 33, 44].

2.2 Solar Cell Sensor Application

Many context awareness applications have been proposed using solar cells as sensors, because the variance of the generated photocurrent can provide useful spatial and temporal information. Solar cells have been used for localisation and activity recognition by analysing the light emitter model [27] in mobile devices. The locations of the solar-powered home can also be estimated using solar energy information without breaking the anonymity [5], and the system can achieve 20 km accuracy. Machine learning technique was also used for place recognition with the assistance of solar cells [36]. Using battery-free solar cells, context awareness applications, such as gesture recognition systems and indoor localisation, have been developed [19, 40]. Varshney et al. [38] also enabled visible light sensing in their system.

3 FEASIBILITY STUDY

In this section, we study the feasibility of the use of solar cells for symmetric key generation.

3.1 Photovoltage Measurement Similarity

The most important characteristic for the feasibility of symmetric key generation is the similarity of the generated photovoltage measurements from a pair of IoT devices when they are placed in the vicinity. As sensors, solar cells are very sensitive to lighting conditions. When the neighbouring devices are interfered with actively and simultaneously (e.g., by hand gesture), the similar patterns of signal measurements can be obtained due to the same surrounding lighting conditions. We

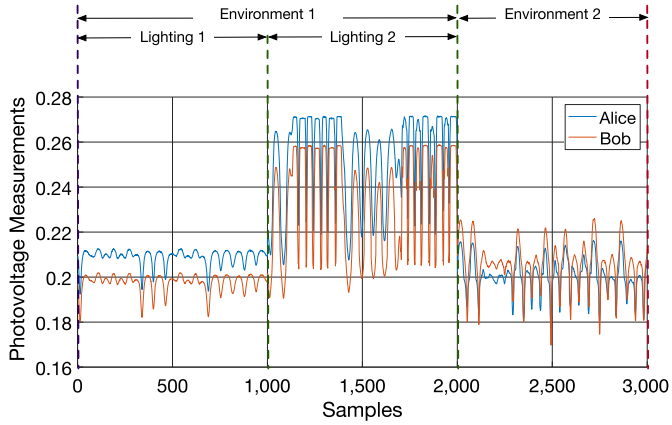


Fig. 2. Photovoltage measurement similarity.

conduct a preliminary experiment in an indoor environment to validate the similarity and consistency of the photovoltage measurements. Figure 2 shows similar patterns of photovoltage measurements from one pair of devices in the vicinity. This similarity and consistency of the photovoltage measurements pave the foundation for the use of solar cells for symmetric key generation. However, there still remain two challenges: measurements mismatching when generating keys due to time unsynchronisation[1] and measurement dissimilarity caused by device noise. In Section 4, we propose a novel time synchronisation method, multi-quantisation, and a two-tier key reconciliation method to address these challenges.

3.2 Temporal Irrelevance of Photovoltage Measurements for Key Generation

Since the surrounding lighting condition may change over time, we validate the efficacy of the use of solar cells with temporal change. In particular, we simulate different lighting conditions with an LED desk lamp. The user then conducts gestures between the LED desk lamp and solar cells. Due to the vicinity of the two legitimate devices, the interference caused by the user's gestures affects both of them simultaneously, which is used for key generation. Figure 2 confirms the obvious correlations between the measurements from the two devices under different lighting conditions.

3.3 Spatial Irrelevance of Photovoltage Measurements for Key Generation

In addition, we show the feasibility of the use of solar cells with respect to spatial irrelevance. We conduct gestures over two devices in two environments:

— *Environment 1:* the office with two lighting conditions.
— *Environment 2:* a bedroom during the day without lights on.

Figure 2 clearly shows the similarity of photovoltage measurements in two environments. This preliminary experiment shows the feasibility of the use of our proposed method in different environments.

4 METHOD

4.1 System Overview

Figure 3 shows the details of our proposed system. Alice and Bob are two legitimate devices that need a symmetric key to encrypt their messages and pair with each other. First, both devices

[1]The measurements in Figure 2 are synchronised using the method introduced in Section 4.3.

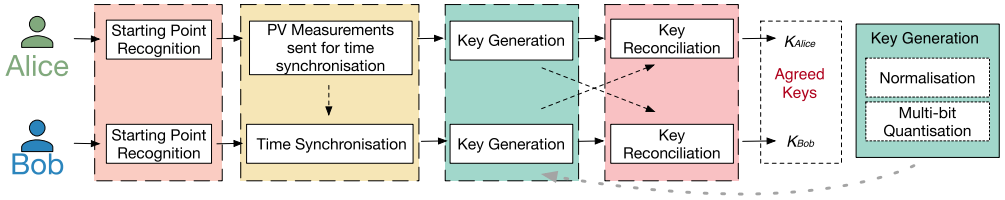


Fig. 3. System overview.

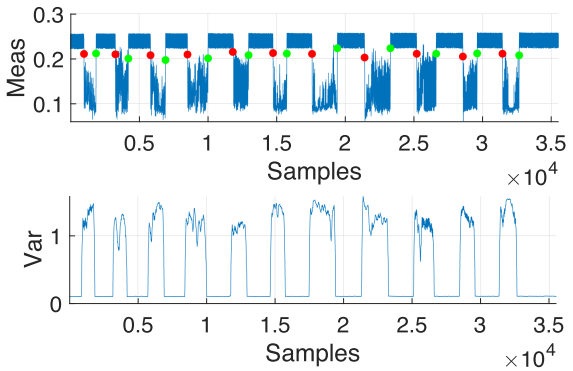


Fig. 4. Top: Photovoltage measurements with detected start points (red dots) and end points (green dots); Bottom: Variance values for moving windows.

start key generation by detecting a starting point. Then, one window of photovoltage measurements from Alice and Bob is exchanged for time synchronisation. Once two devices are time-synchronised, multi-bit quantisation is performed to derive the initial keys. Next, we exploit a novel two-tier reconciliation method to increase the key matching ratio. Finally, Alice and Bob agree on the same key to secure their communication.

4.2 Start and End Points Detection

The first step is to detect the start and end points to embrace measurements for the key generation. In particular, we use a simple variance-based mechanism to detect the start and end points, since gestures above solar cells can cause variance in photovoltage measurements. We first use the amplitudes in the beginning silent photovoltage measurements collected without any gesture interference and calculate the average silence level σ as the offset. Then, measurements remove the offset σ and are used to calculate the variance within each moving window. One threshold is used to detect measurements with gestures. The measurements within the moving window whose variances are above the threshold are selected for the key generation. Figure 4 shows an example of the start and end point detection method. The raw measurements are demonstrated in Figure 4 (above) with their variances shown in Figure 4 (bottom). The range of measurements with the start points (red dots) and end points (green dots) for key generation are detected using the corresponding variances above the threshold.

4.3 Automatic Time Synchronisation

Once the system detects one start and end points for the key generation, a window-based key generation method will be performed to generate keys (key generation method will be discussed

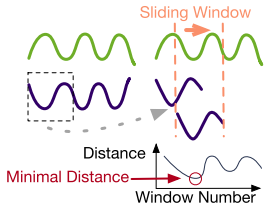


Fig. 5. Automatic time synchronisation.

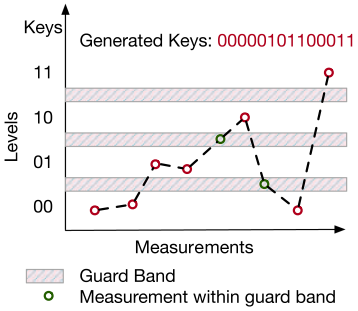
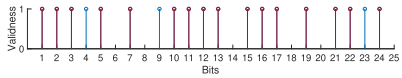


Fig. 6. Multi-bits quantisation.

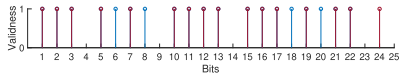
later in Section 4.4). The window-based key generation method is based on the similarity of each measurement within corresponding windows from two devices, so time synchronisation is very important. The measurement shift due to time unsynchronisation can cause severe key mismatching. Furthermore, similar measurements that fall in different windows could have different normalised values. To improve the key matching rate, we propose an accurate automatic time synchronisation scheme based on photovoltage measurements. In our proposed method, **Dynamic Time Warping (DTW)** is employed on photovoltage measurements to enable automatic time synchronisation. Figure 5 shows one example of the use of the automatic time synchronisation method. Specifically, one window of photovoltage measurements S_{w1} from the first legitimate device Alice is sent to the second legitimate device Bob. Then, Bob uses S_{w1} to compare the similarity of the collected photovoltage measurements S_{w2}. The length of S_{w2} is $n \times |S_{w1}|$ where n is 10 in our implementation. One sliding window S^i_{w2} with the window size $|S_{w1}|$ is applied on S_{w2} to calculate the DTW distance d_i between S_{w1} and S^i_{w2} and compare the similarity. The jth sample from Bob is picked to synchronise his time with Alice, where d_j is the global minimum and below a threshold d_{thr}.

4.4 Key Generation

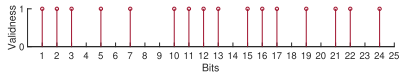
Multiple Bit Quantisation: Once the automatic time synchronisation process finishes, unity-based normalisation is applied on windows of measurements, which makes them have a range between the minimum value 0 and the maximum 1 for key generation. When generating keys using photovoltage measurements, we leverage the multiple bit quantisation method [9]. Figure 6 shows one example of the key generation method. Specifically, the amplitudes of normalised photovoltage measurements in non-overlapping windows are used. When using the multi-bit quantisation, guard bands are designed for each consecutive level. The use of guard bands can significantly increase the bit agreement rate and eliminate the effect of noise. When using multiple bits quantisation with m-ary, $m-1$ guard bands are inserted into each pair of neighbouring levels. Measurements that fall into the scope of guard bands will be removed. The remaining measurements



(a) Valid Bits from Alice



(b) Valid Bits from Bob



(c) Shared Valid Bits

Fig. 7. Example of ambiguous bit removal method. Red spots in (a) and (b) show the shared valid bits.

are coded based on their corresponding levels, i.e., $L_i = (v_{is}, v_{ie} - g]$, where v_{is} and v_{ie} are the boundary of the ith level, $i \in [1, m-1]$. g is the size of the guard band. $g = \frac{\alpha \times (L_{max} - L_{min})}{m}$, where α is the ratio of the band, L_{max} and L_{min} are the maximum and minimal measurements within that window. The $n = log_2 m$ bits will be given to each level. According to the levels of photovoltage measurements, a sequence of secret keys is extracted for each window. Now, Alice and Bob have generated the initial raw symmetric keys independently.

4.5 Two-tier Key Reconciliation Method

The initial raw symmetric keys generated by Alice and Bob are usually not identical, so the reconciliation method is used to correct mismatched keys. We use a two-tier key reconciliation method, which includes the ambiguous bit removal tier and the key correction tier. While a similar strategy has been used in Reference [39], this article focuses on the use of solar cells for symmetric key generation, solving corresponding challenges (such as time synchronisation and noisy measurements due to low-resolution signals) and providing the evidence of its feasibility using extensive evaluations. Here, we show the details of these two tiers.

4.5.1 Ambiguous Bit Removal Tier. The use of guard bands leads to the issue that the removal of measurements within the guard levels may result in accumulating mismatches for the following keys generated by measurements. Due to initial mismatched keys caused by the noise or deployment displacement, it is inevitable that measurements from one device fall in guard levels while the corresponding measurements from the other one do not. This results in the shift and mismatching of its following generated keys. Therefore, we adopt ambiguous bit removal as the first tier for the proposed key reconciliation method.

The ambiguous bit removal tier aims to locate the valid keys that exist in both devices. Due to open-air wireless communication, only sharing the locations of valid keys can preserve the sensitive information of generated keys. Once Alice and Bob exchange the location information of valid keys, they select the shared locations of valid keys and only use these valid keys for further key correction. Figure 7 shows an example of the ambiguous bit removal method. For simplicity, we assume we generate 1 bit for each sample, i.e., 0 or 1. We use the first 10 samples to explain. Alice generates keys at positions {1,2,3,4,5,7,9,10} while Bob generates keys at positions {1,2,3,5,6,7,8,10}. The valid keys mean the bits generated at common locations of Alice's key and Bob's key. In this example, the common locations are {1,2,3,5,7,10}. So, they exchange these locations and only keep the bits generated at their common locations. Suppose Alice's initial key is "10010101" and

Bob's initial key is "10001011." The bits with underlines mean invalid keys whose corresponding measurements fall in the guard level. If Alice and Bob only keep valid bits, then Alice will generate "100011," and Bob will obtain "100001." Please note, there is still one mismatched bit (the second last bit whose original location is 7), because the ambiguous bit removal tier only considers the validness of generated keys. Ambiguous bit removal solves the accumulating errors caused by invalid key mismatching and significantly increases the key matching rate.

4.5.2 Key Correction Tier. Even with the use of the guard band and ambiguous bit removal tier, the noise from the hardware may still result in the mismatching of generated keys. Therefore, an additional key correction tier is introduced to correct the mismatching key for Alice and Bob. In this article, we use compressed sensing-based key correction method [15]. The reason for the use of compressed sensing is two-fold. First, the compressed sensing-based key correction method can improve security over wireless communication between a pair of legitimate IoT devices. To secure the generated keys, the compressed sensing-based key reconciliation method employs one random matrix to compress and encrypt sent keys. The random matrix is mutually agreed upon by those legitimate IoT devices, which is also common knowledge to the attacker Eve. The sent keys can only be recovered when conditions are met with the assistance of ℓ_1 minimisation, the key component of compressed sensing. Second, the use of compressed sensing can significantly reduce the size of the sent keys and thus minimise the use of the communication band. Therefore, in our proposed method, we use the compressed sensing-based key correction method. In the following of this section, we first introduce the background of compressed sensing and then show the details of the compressed sensing key correction method.

4.5.3 Background of Compressed Sensing. Compressed sensing is widely used to compress sparse signals from high dimension to low dimension [3, 6]. Suppose x is a sparse vector with the dimension N and we use S to denote the number of non-zero elements in x. Then the x is sparse when $S << |x|$. We use a project matrix P with the dimension $M \times N$ to compress the vector x, where $M < N$, and obtain compressed vector y, i.e., $y = Px$. However, this equation is under-determined and cannot be solved using a standard method. The compressed sensing theory has been proposed to solve this under-determined problem when x is sparse. Vector x can be recovered using the following equation:

$$\arg\min_{x} \|x\|_1 \quad \text{subject to } \|y - Px\|_2 < \epsilon. \tag{1}$$

Equation (1) is solvable if the following two conditions can be met: **Condition (1):** The project matrix P needs to follow the **Restricted Isometry Property (RIP)** [6]. For IoT devices, a random Bernoulli matrix with equal possibilities of $\pm 1s$ is often used due to its efficiency of computation [41]; **Condition (2):** $M > Slog(N/S)$ should be met, which is a sufficient condition, and $M > S$ is a necessary condition.

4.5.4 Compressed Sensing-based Key Reconciliation Method. The use of the compressed sensing method is based on the sparsity of mismatching bits between the initial valid keys from Alice k'_{Alice} and Bob k'_{Bob}. In other words, $\Delta k = k'_{Alice} - k'_{Bob}$ is sparse with few non-zeros elements. Once those non-zeros elements are recovered, the keys from Alice and Bob can be matched. Now, one random project matrix P whose elements follow symmetric Bernoulli distribution is stored in both Alice and Bob. Alice uses the project matrix P to encrypt her initial key K'_{Alice}, i.e., $y'_{Alice} = PK'_{Alice}$, and sends y'_{Alice} to Bob using the wireless communication. Bob also uses the project matrix to obtain $y'_{Bob} = PK'_{Bob}$. Once Bob receives y'_{Alice}, Bob calculates $\Delta y = y'_{Alice} - y'_{Bob} = PK'_{Alice} - PK'_{Bob} = P(K'_{Alice} - K'_{Bob}) = P\Delta k$. As discussed above, the percentage of the mismatching bits between the legitimate devices Alice and Bob's initial keys is usually low, so Δk is sparse and solvable according

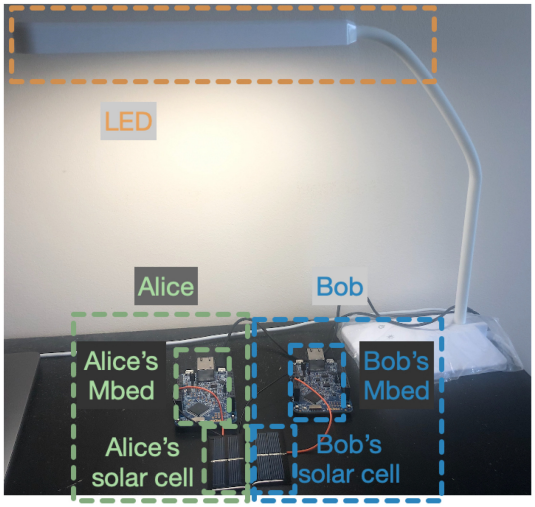


Fig. 8. Hardware in the experiments.

to compressed sensing theory [3, 6], i.e.,

$$\arg\min_{\Delta k} \|\Delta k\|_1 \quad \text{subject to } \|\Delta y - P\Delta k\|_2 < \epsilon. \tag{2}$$

Bob then uses Δk to derive his agreed key $k_{Bob} = k'_{Bob} \oplus \Delta k$, which is supposed to be the same as the k'_{Alice}.

Because Alice and Bob exchange messages in the public channel, the attacker Eve can spoof one of the legitimate devices and modify these messages. To ensure integrity, we use the **message authentication code (MAC)**, which is also called **message integrity code (MIC)** as previous key generation systems [48, 50]. Additionally, the exchanged messages will leak some side information to Eve, and this problem can be solved by privacy amplification [4]. Specifically, we apply the universal hash function on the generated keys to improve privacy.

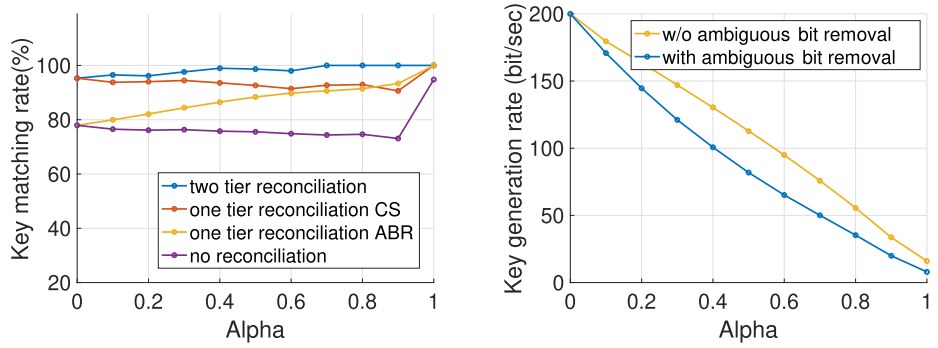
5 PERFORMANCE EVALUATION

5.1 Experiment Setup

Figure 8 shows the experiment setup. We implement the prototype with solar cells acting as sensors as a part of a photovoltage measurement reader, which is attached to **analog-to-digital converter (ADC)** on the IoT devices Mbed FRDMs [1]. The lighting conditions are continuously sensed by solar cells and sent to the IoT device for key generation. The default experiment environment is the office with lights on, and one light is approximately 2 meters above the solar cells. The user of legitimate devices conducts gestures between the light above and the solar cells. We also test our testbed using an LED as shown in Figure 8 and evaluate the performances under various lighting conditions.

5.2 Goals, Metrics, and Methodology

The goal of our evaluation is to show the performance and robustness of our proposed methods. First, we discuss the effect of the designed two-tier reconciliation method. Next, we study the impact of the parameter selection in the proposed method. Third, we conduct the experiments in various environments, lighting conditions, interference, and mobility to investigate the feasibility



(a) Key Matching Rate (b) Key Generation Rate

Fig. 9. The effect of key reconciliation method.

of the use of solar cells for key generation. Fourth, we also discuss the effect of the proposed time synchronisation method. Finally, we demonstrate the randomness of the generated keys.

In this section, we will use the following metrics to evaluate our proposed method:

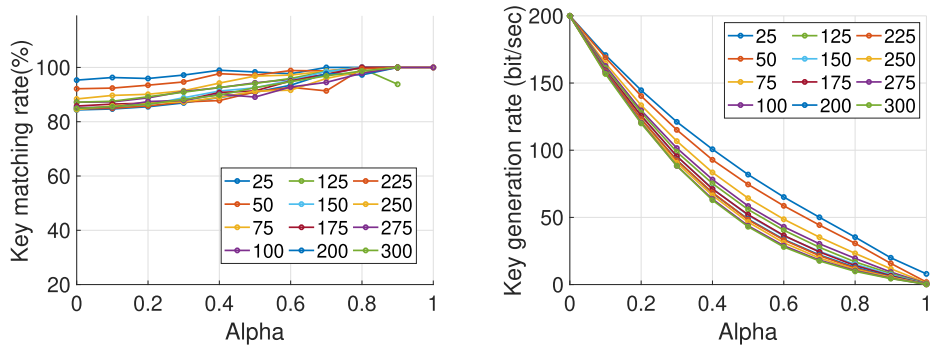
— Key agreement rate: the percentage of matching keys generated by Alice and Bob.
— Key generation rate: the key generation speed in the number of generated bits per second (bit/sec).
— Entropy: Entropy demonstrates the randomness of the generated keys. With its range $[0, 1]$, a larger entropy value indicates the generated keys have more randomness.

In the following part, we will show the performances of the proposed methods compared with the state-of-the-arts, using various parameters and in different lighting conditions.

5.3 The Effect of Reconciliation Method

In this section, we show the effect of the proposed two-tier reconciliation method. As discussed, due to the noise and the use of the guard levels for multi-bit quantisation, the sequential photo-voltage measurements from Alice and Bob cannot be exactly matched. Therefore, we proposed a two-tier reconciliation method, including an ambiguous bit removal tier and a key correction tier. Comparing with state-of-the-arts, we show the key matching rate and key generation rate of key generation methods without reconciliation (*no reconciliation*), with only ambiguous bit removal (*one-tier reconciliation ABR*, used in Reference [34]), with only compressed sensing reconciliation (*one-tier reconciliation CS*, used in Reference [47]), and with both the ambiguous removal and CS reconciliation (*two-tier reconciliation*). In this experiment, the window size is set as 25, and the bit per sample in the multi-bit quantisation method is 2.

Figure 9 shows the key matching rates and key generation rates using different reconciliation methods. From Figure 9(a), we can see that without the use of any reconciliation method, the key matching rate is 77.93% when α is 0, and the key matching rate gradually decreases to 73.08% with α 0.9. As discussed in Section 4.5, discarded bits whose measurements fall into the guard level may only exist in one device, which results in the shifting error for its following bits when calculating the key matching rate. When α is 1, only the measurements whose values are exactly the same as that of boundary levels of multi-bit quantisation are assigned bits. Therefore, its matching rate is usually high, while its key generation rate is very low. When the ambiguous bit removal method is applied, the key matching rate increases from 77.93% to 95.29% with α 0.1 and from 74.36% to 100% with α 0.7. It can be seen that the removal of ambiguous bits can significantly improve the



(a) Key Matching Rate (b) Key Generation Rate

Fig. 10. The effect of window size.

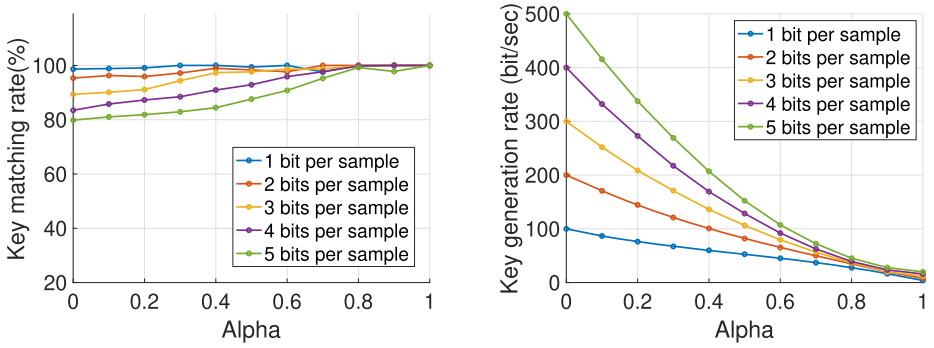
key matching rate. When we only use the compressed sensing-based key correction method, the key matching rates increase up to approximately 20% from that without reconciliation. When the other tier with compressed sensing-based key correction method is used, the key matching rate is further improved from 95.29% to approximately 100%, regardless of the value of α. In terms of key generation rates, it is expected that key generation rates decrease with an increase of α. The ambiguous bit removal can further affect the key generation rate. As shown in Figure 9(b), there is a gap between with ambiguous bit removal and without that, because of the use of the ambiguous bit removal method, will remove the disagreed keys and thus decrease the key generation rate. When α is 0.4, the key generation rates are 100 bits/sec and 130 bits/sec, respectively. This also shows the key marching rate and key generation rate is a tradeoff. Our proposed architecture can significantly enhance the key matching rate and slightly decrease key generation speed by trimming the ambiguous bits.

5.4 Impact of Window Size

In this section, we discuss the effect of the window size used for the window-based normalisation in the key generation. The used bit per sample in this experiment is 2. Figure 10 shows key matching rates and key generation rates using different window sizes from 25 to 300 photovoltage measurements with an interval of 25. It clearly shows that the use of the smaller window increases key matching rates and key generation rates. This is because increasing window size will more likely have noise. The noise, especially the peak noise from one legitimate device, can result in the reduction of the performance of the key matching rate and key generation rate, because the window-based normalisation relies on the value range of measurements within that window. Please note, when α is higher (e.g., 0.9 or 1), there may be no remaining bits with wide guard bands after applying ambiguous bit removal, so the key generation rates are then 0. Therefore, in the following experiments, we set the default window size as 25.

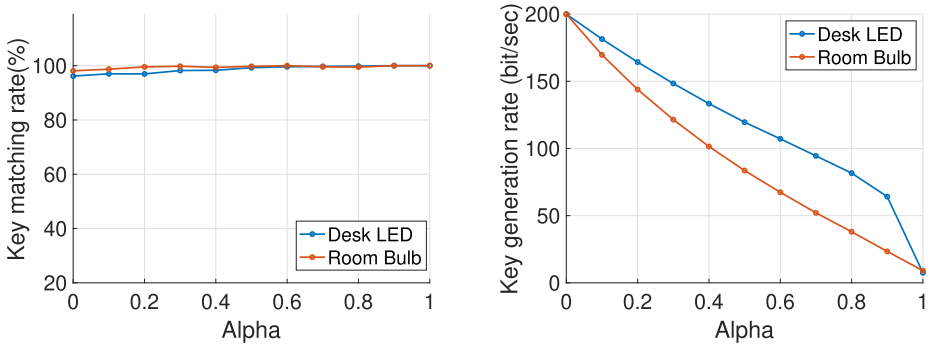
5.5 Impact of Bit per Sample

In this experiment, we show the effect of bit per sample for multi-bit quantisation. The window size is 25, as explained in the previous subsection. Figure 11 shows the key matching rate and key generation rate using different bits per sample, i.e., 1, 2, 3, 4, and 5 bits per sample. When using 1 bit per sample for key generation, the key matching rates stay stable at nearly 100%, but the key generation rates are very low compared with that using other bits per sample. It is expected that with the use of larger bits per sample, the key generation rates increase, while the key matching rate



(a) Key Matching Rate (b) Key Generation Rate

Fig. 11. The effect of bit per sample.



(a) Key Matching Rate (b) Key Generation Rate

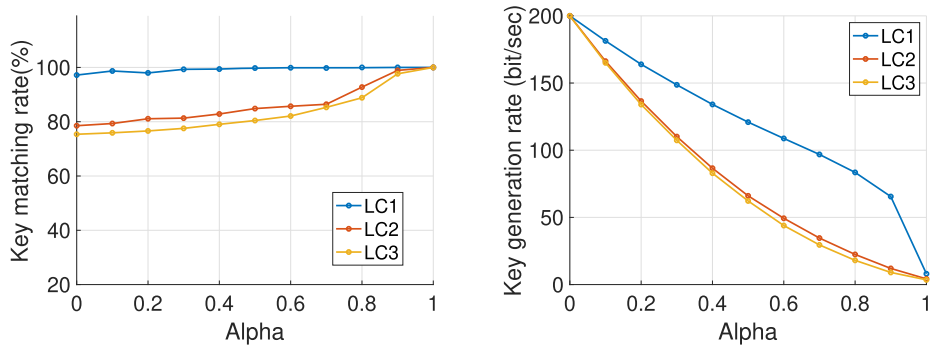
Fig. 12. The effect of lighting distance.

decreases. When using 2 bits per sample, the key matching rate is 95.33% with α 0, and it increases to a comparable level as that of the use of 1 bit sample with *alpha* 0.4. In future experiments, we will use 2 bits per sample as the default value, because it has a competitive key matching rate and relatively high key generation rate.

Other methods such as motion-based [34, 48] have a range of 50–200 Hz sampling rate and use 1 bit per sample. Reference [15] also has a limitation of low key generation rates. In this aspect, the proposed method (with 2 bit/sample and 100 Hz sampling rate) performs better and equivalently well as these existing methods. The use of acoustics-based [47] and wireless channel-based [43] methods can have better key generation rates, but they need a large amount of energy to power wireless transmission and acoustic devices (i.e., a microphone and a speaker).

5.6 Impact of Lighting Distance

In this section, we study the impact of the distance of lighting. We use two normal settings in this section. The first setting is the use of LED on the desk, and the second setting is the use of a bulb in a room. In both settings, there is only one lighting source. The solar panels are put under the light source and face it. The user interferes with the lighting between the lighting source and solar panels. Figure 12 shows the performance under these two distances. It is shown in Figure 12(a) that, in both lighting distances, the key matching rates can achieve equally good performances, which



(a) Key Matching Rate (b) Key Generation Rate

Fig. 13. The effect of lighting conditions.

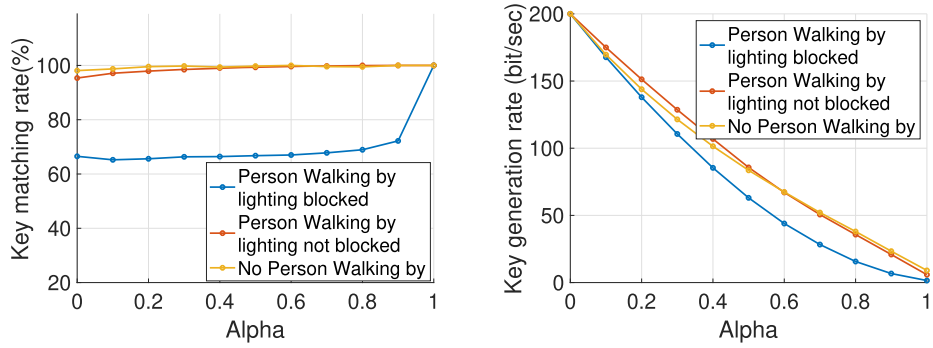
are all very close to 100%. When looking at key generation rates in Figure 12(b), using the desk LED can perform better than that using a room bulb. This is because other things in a room, such as furniture, PC monitors, and so on, reflect lights slightly. Although the reflected light is not as significant as the main lighting source, it affects measurements and key generation performance before key reconciliation. It is, however, clearly demonstrated in Figure 12(a) that our reconciliation method removes mismatched bits and helps achieve good key matching performance.

5.7 Impact of Lighting Conditions

The variance of the photovoltage measurements in the proposed method is from the interference of the lighting source using gestures. In reality, when there is more than one lighting source in the surrounding environment, the user's gestures are usually able to block one lighting source and thus the solar cells can still sense the stable lighting from the other lighting sources. If the other lighting sources are bright enough, then the conducted gestures cannot generate sufficient interference of photovoltage intake. In this experiment, we evaluate SolarKey in the following three lighting conditions to show the effect of the surrounding environment:

- **Lighting Condition 1 (LC1):** There is one bright main lighting source, and the user conducts gestures between the lighting source and solar cells to generate inference.
- **Lighting Condition 2 (LC2):** There are two main lighting sources with similar brightness. The user is only able to block one lighting source.
- **Lighting Condition 3 (LC3):** There is a bright main lighting source, but gestures conducted by the user are not between the light source and solar cells.

In this experiment, we will discuss the performance of key generation in these three different lighting conditions. Figure 13 shows the key matching rates and key generation rates in LC1, LC2, and LC3, respectively. It is shown that SolarKey performs the best in LC1, where it can achieve nearly 100% key matching rates with the value of α from 0 to 1. The key generation rate in LC1 significantly outperforms, which is up to 60 bit/sec more than that in LC2 and LC3. The direct interference between the primary lighting source and solar cells can improve the key generation performance, because it can generate significant interference to solar cells. This experiment also shows the lighting condition above the legitimate devices and gestures are important. The user needs to ensure to conduct gestures to interfere with the lighting. Additionally, this experiment illustrates the importance of places and the brightness of the main lighting sources to ensure the photovoltage measurements from solar cells can appropriately generate random keys.



(a) Key Matching Rate (b) Key Generation Rate

Fig. 14. The effect of people walking by.

5.8 Impact of Interference in Dynamic Environment

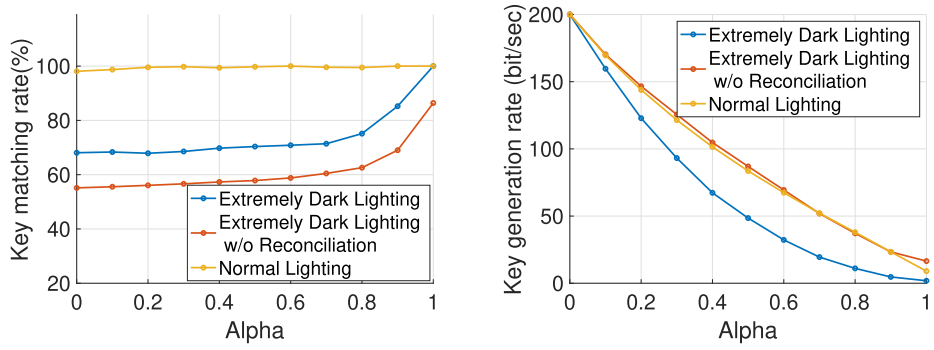
When using solar cells to generate keys, there may be people walking in the surrounding environment, which creates dynamic environments. In terms of the interference of the proposed key generation method in dynamic environments, there are two scenarios. First, one person walks around, but he does not block the lighting source. Second, the walking person blocks the lighting source occasionally. Experiments are conducted to show the performance in each dynamic environment. Figure 14 shows the key matching rates and key generation rates of those scenarios. The performance without any person walking by is also shown as the baseline. It can be found that the performance is not affected when the person does not block the lighting source, but the key matching rates and key generation rates drop significantly when the walking person blocks the lighting source occasionally. When the lighting is blocked and thus not sufficiently bright, the fluctuation caused by the gesture is not as noticeable as that in the bright lighting and hugely affected by the noise.

5.9 Effect in Extremely Dark Lighting

In this experiment, we evaluate the performance of our proposed method in an extremely dark environment. The experiment is conducted in the evening in an indoor environment, without any light on. The only lighting source is the screen of a 13-inch laptop display that is about 30 cm away from Alice and Bob. The user conducts gestures between the display and solar cells. Figure 15 shows the performance in the extremely dark lighting environment. It also shows the performance in normal lighting and extremely dark without any reconciliation method. In the extremely dark environment, the key matching rate is 68.09% with α 0 and gradually increases to 71.04% with α 0.7. With α being in [0.8, 1], the key matching rate increases, but the key generation rates are very low then. When comparing with the performance in normal lighting, the key matching rate decreases by 25% and the key generation rate also drops due to the low signal-to-noise level. The noise is consistent, while the signal level, the measurement fluctuation caused by gesture interference, is not able to result in a high level of impact. However, it is still obvious that the use of our proposed reconciliation method can increase up to approximately 15% of the key matching rate compared with the method without the use of reconciliation method and achieve 75.13% key matching rate with α 0.8 in such bad lighting condition.

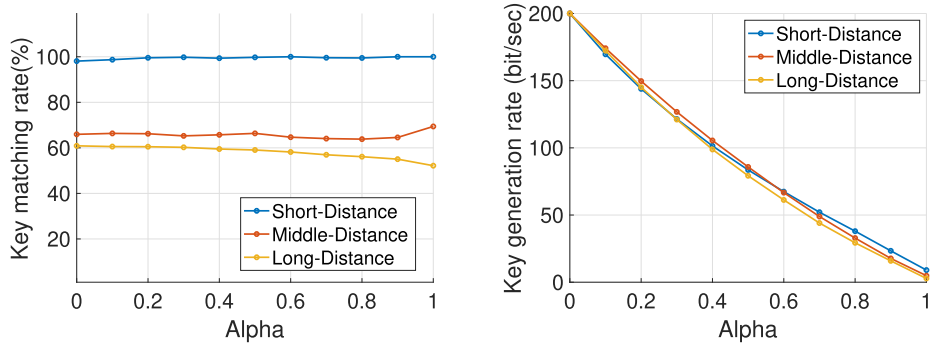
5.10 Effect in Distance between the Deployed Solar Cells

In this section, we discuss the effect of the distance of the deployed solar cells from a pair of IoT devices. Since solar cells are very sensitive to lighting conditions, the distance between solar cells



(a) Key Matching Rate (b) Key Generation Rate

Fig. 15. The effect of extremely dark environment.



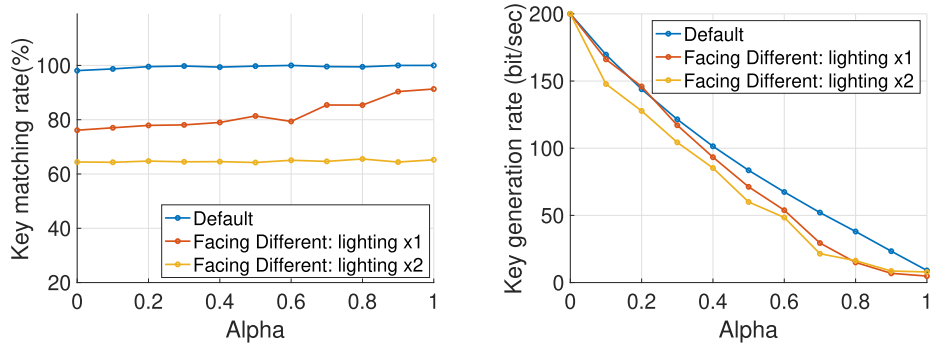
(a) Key Matching Rate (b) Key Generation Rate

Fig. 16. The effect of distance.

from a pair of IoT devices can affect the key generation performance significantly. To show the effect of the distance between a pair of IoT devices, we put solar cells from a pair of IoT devices at short-distance (neighbouring to each other), middle-distance (10 cm away from each other), and long-distance (20 cm away from each other), respectively. Having an LED over a pair of solar cells, the user's hand waves over the pair of solar cells to generate keys. The hand waving length is approximately 10 cm, which means the waving hands can affect the lighting data collection for both solar cells at short-distance simultaneously and can only affect one solar cell in long-distance once. When the user's hand waves over solar cells at middle-distance, it can completely affect one solar cell and partially affect the other one. Figure 16 shows the key matching rate and key generation rate for solar cells at different distances. Although the key generation rate is not influenced, the extent of the distance decreases the key matching rate significantly compared with nearly 100% key matching rate at short-distance (data are from the default setting). This confirms the requirement for the deployment of solar cells in the vicinity due to their sensitivity to lighting conditions. Based on the performance of the key matching rates of different distances, it is advised that the users put two devices sufficiently close. This is similar to many applications in real life as well, such as contactless payment.

5.11 Effect of Solar Panel Facing

In this section, we discuss the effect of the solar panel facing. The default experiment setting is two solar panels facing in the same direction as the only lighting in a room. The user infers the lighting



(a) Key Matching Rate (b) Key Generation Rate

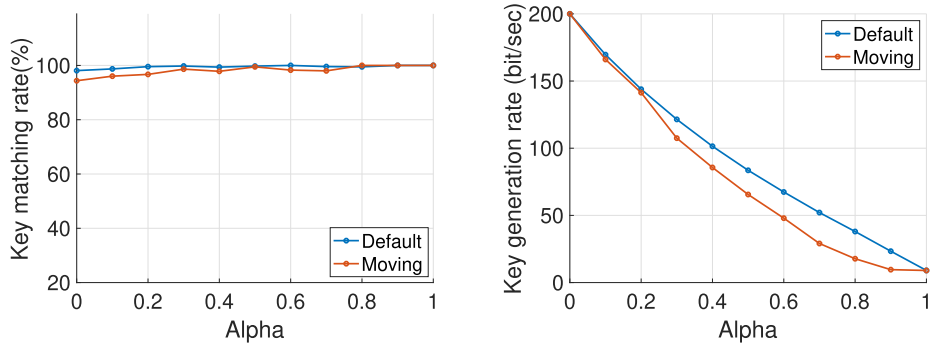
Fig. 17. The effect of facing.

to generate lighting variance to solar panels. To understand the effect of the solar panel facing, we make these two panels attach back-to-back. The user waves between one lighting source and these two panels. There are two situations here. First, there is only one lighting source. For example, in the evening, the only lighting source is one LED bulb. One solar panel faces the lighting source, while the other one faces the other side. The second situation is when multiple lighting sources exist, i.e., in addition to the LED bulb, the lighting is also from the window in the daytime. In this situation, each solar panel faces one lighting source. Figure 17 shows the key matching rates and key generation rates of different facings compared with the default setting. It is clearly shown that the key matching rates drop significantly when there are two lighting sources. This is because the user's waving can only influence one panel, while the lighting condition of the other panel does not change. When there is only one lighting source, the key matching rates are better, but they are still not as good as that in the default setting. This confirms that the indirect influence of lighting sources has a limited impact on photovoltage variance, which has the same finding as Section 5.7.

5.12 Effect of Mobility

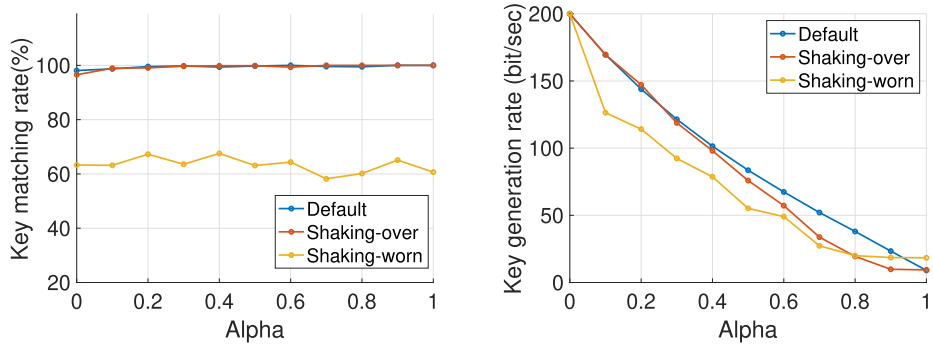
In this section, we will evaluate the performance of the designed system in the aspects of mobility, i.e., the key matching rates and generation rates when the solar panels are moving. As shown in Section 5.11, when solar panels face different directions, the key generation performances drop significantly. In this section, we let the solar panels face the lighting source, i.e., an LED bulb in a room, and carry the devices walking in this room. Since the designed key generation system is based on the lighting condition change, the movement of both neighbouring solar panels produces synchronous lighting changes. Figure 18 shows the key matching rates and key generation rates when two devices with solar panels are moving. For comparison, we also put the performance of a default experiment setting, i.e., in the room lighting condition, one hand actively interferes with the lighting. It clearly shows they can achieve equivalent good key matching rates. The key matching rates during moving are slightly lower. This is because the lighting variance caused by moving is not as obvious as that caused by a waving hand, which results in relatively more mismatched bits. However, the good performance of key matching rates shows the mismatched keys are removed by the designed two-layer key generation methods.

Another application case regarding mobility is the hand-shaking of users. There are two scenarios: Scenario 1: users shaking over IoT devices equipped with solar panels; Scenario 2: users shaking while wearing IoT devices equipped with solar panels. The main difference between these two scenarios is regarding the facing of solar cells as well. In Scenario 1, solar panels face the same



(a) Key Matching Rate (b) Key Generation Rate

Fig. 18. The effect of mobility.



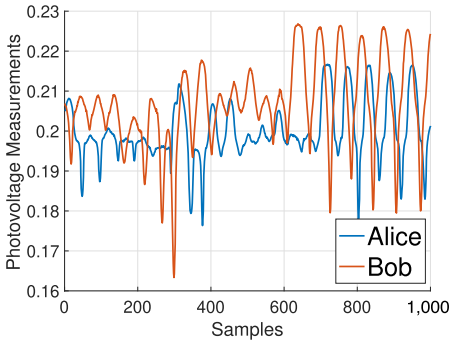
(a) Key Matching Rate (b) Key Generation Rate

Fig. 19. The performance during shaking.

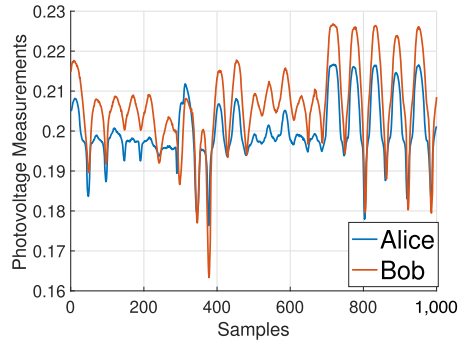
direction, while, in Scenario 2, solar panels face different directions. The lighting condition is normal, i.e., a room with an LED bulb as the only lighting source. Figure 19 shows the key matching rates and key generation rates in these two scenarios, as well as the performances in the default experiment setting. It is seen that, when users shake hands over two solar panels, the key matching rates stay as good as that in the default setting. This is because two users' shaking over panels is technically waving over two devices. When users wear devices and shake their hands, the key matching rates drop significantly, because panels face different directions. This confirms the same finding as shown in Section 5.11.

5.13 Effect of Time Synchronisation

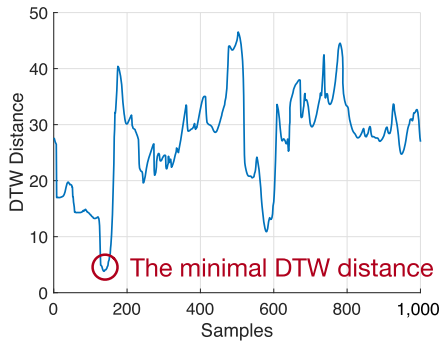
In this experiment, we show the performance of our proposed time synchronisation method. Figure 20(a) shows the first 1,000 starting samples without time synchronisation. There are two observations: (1) the shapes of two series of raw measurements are similar with different scales. The window-based normalisation will help make them consistent in the same scale to generate keys using its normalised measurements. (2) A consistent shifting clearly exists. This confirms the necessity of the use of time synchronisation to generate keys for different devices. We use the proposed time synchronisation method and calculate the DTW distance between the first window in Bob and the sliding windows in Alice. Figure 20(c) shows the corresponding DTW distances. In this experiment, the size of the starting window from Alice and the sliding window is 200. It can be



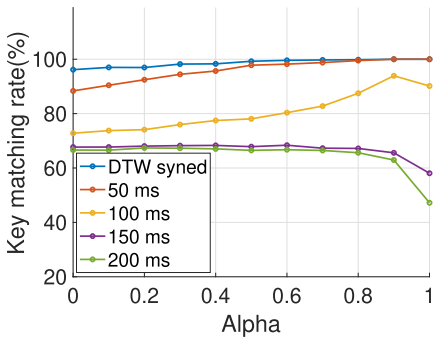
(a) Unsynchronised Measurements



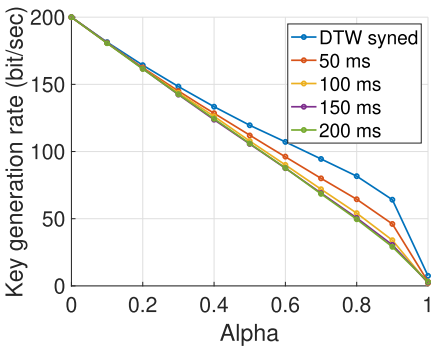
(b) Synchronised Measurements Using Proposed Time Synchronisation Method



(c) DTW Distance



(d) Key matching rates



(e) Key generation rates

Fig. 20. (a)–(c)The effect of the proposed time synchronisation method; (d) Key matching rates under different time shifts; (e) Key generation rates under different time shifts.

found that the 137th sliding window from Bob possesses minimal distance from the starting window from Alice, so the 137th measurement from Bob is synchronised with the 1st measurement from Alice. Figure 20(b) shows two series of measurements after applying the time synchronisation method. It can be seen that measurements from Alice and Bob are synchronised now.

We have also evaluated the performance of the proposed time synchronisation method by showing the key matching rates of various time differences of samples. Samples are shifted manually to

Table 1. Results of NIST Test and Entropy

NIST TEST	p-value
Monobit test	0.244
Frequency within block test	0.142
Runs test	0.032
Longest run ones in a block test	0.902
Binary matrix rank test	0.648
DFT test	0.305
Non overlapping template matching test	1.000
Maurers universal test	0.591
Serial test	0.334
Approximate entropy test	0.334
Cumulative sums test	0.157
Random excursion test	0.193
Random excursion variant test	0.370
Entropy	0.714

have mismatched measurements with 50 ms, 100 ms, 150 ms, and 200 ms shifts. Although the common network-based time synchronisation method can usually achieve less than 20ms accuracy, it occurs on many occasions that the time synchronisation error could reach more than 100 ms [26]. Figure 20(d) shows the key matching rates using the proposed time synchronisation method and different time shifts. It is clearly shown the key matching rates are no more than 70% when more than a 150 ms time delay. Although the key matching rates can achieve approximately 90% with Alpha 0.9 when the synchronisation error is 100 ms, the key matching rates are much worse compared with that using the proposed DTW time synchronisation method. Furthermore, the other key generation rates are only 1/3 compared with that using Alpha 0.3 (see Figure 20(e)). When the time shift is 50 ms, the key matching rates are as good as that with DTW when Alpha is more than 0.6. We can still see up to 10% key matching rates performance reduction with a smaller Alpha.

5.14 Randomness of the Keys

In addition to the key matching rate and key generation rate, we further test the randomness of generated keys by using the popular NIST Statistical Test Suite [30]. The results in NIST tests are shown in p-values that indicate whether the generated key is random or not. Conventionally, if p-values are greater than 0.01, then the generated keys are sufficiently random. Table 1 shows a list of results in the NIST test, which confirms that the keys generated by the proposed method SolarKey have high randomness. We also calculate the entropy to confirm the randomness of the proposed methods.

6 SECURITY ANALYSIS

6.1 Attack Model

Figure 21 shows common attack models. Two legitimate devices, Alice and Bob, intend to initiate a secure communication link using the symmetric key encryption method. One solar cell is equipped into each IoT device, and the photovoltage measurements collected from solar cells are used for key generation in the proposed system. The user conducts random gestures to interfere with the lighting conditions above the two devices, and the photovoltage measurement similarity from legitimate devices is leveraged to generate symmetric keys.

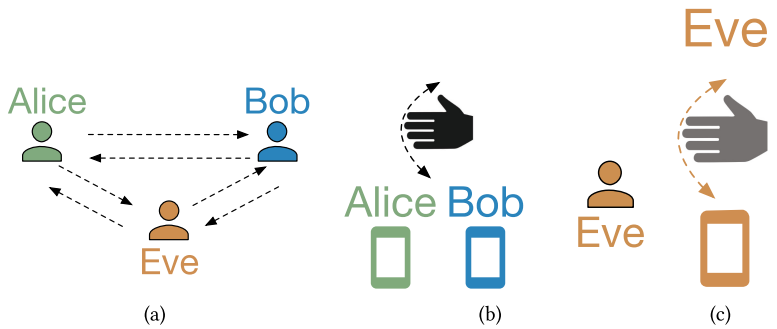


Fig. 21. Attack models: (a) Eavesdropping attack (b) Imitating attack step 1: Eve observes activities (c) Imitating attack step 2: Eve repeats gestures.

We assume that Eve, as an adversary IoT device, has the full knowledge of our key generation system. Eve can monitor the wireless communication and observe the gestures conducted by the user, as shown in Figure 21(b). The goal of Eve is to obtain the same key but not interrupt the key generation protocol to avoid Alice and Bob's awareness of the presence of Eve. Therefore, we do not consider **Denial-of-Service (DoS)** attack in this article. The above assumptions are also used in previous key generation systems [14, 43, 48]. Based on the analysis above, we consider the following attack models in the article: **Imitating attack:** When Alice and Bob generate keys (i.e., gestures conducted over Alice and Bob), Eve observes gestures. After Alice and Bob finish the key generation process and leave the location, the attacker can go to the same place with the same lighting condition and then try to repeat gestures to generate the same keys **(Attack 1)**. The attacker could stay at a different place to repeat gestures **(Attack 2)**, but it is not guaranteed that Eva can have the same lighting condition; **Eavesdropping attack:** Eve can eavesdrop all the messages transmitted in the wireless communication and intend to obtain the same encryption key with the eavesdropped messages **(Attack 3)**, but Eva does not repeat gestures in Attack 3. As a supplement, Eve could repeat the observed gestures from Alice and Bob to recover keys **(Attack 4)**.

In the article, we do not consider that Eve can both recover exact gestures and eavesdrop on all the messages transmitted in wireless communication. The same assumption is also used in Reference [39]. The exact gestures could be recovered by sophisticated computer vision methods with specific devices, such as depth cameras. However, the devices are usually noticeable to legitimate users where they are in the vicinity. Therefore, the attacker can only exactly recover legitimate users' gestures *at a distant location* using computer vision methods without being noticed by legitimate users. When Eve is at a distant location, it is beyond the communication range of Alice and Bob (Alice and Bob can limit the communication range by decreasing the wireless transmission power), so Eve cannot receive the exchanged messages in the "open-air" communication between Alice and Bob for key reconciliation. Eve's key generation performance will be exactly the same as the key generation using two measurements with no reconciliation in Figure 9, which shows that attacker Eve cannot achieve a satisfactory key matching rate without any conciliation methods. Please note, since gesture recovery using computer vision is out of the scope of this article, we assume that Eve can recover exact gestures in that situation.[2] Just like inputting passwords to an **automated teller machine (ATM)**, users are expected to cover the conducted gestures to avoid attackers finding keys.

[2]Due to noise, measurements generated from the same gestures cannot be exactly matched to the real measurements. Therefore, without reconciliation, the key matching rate will also be low.

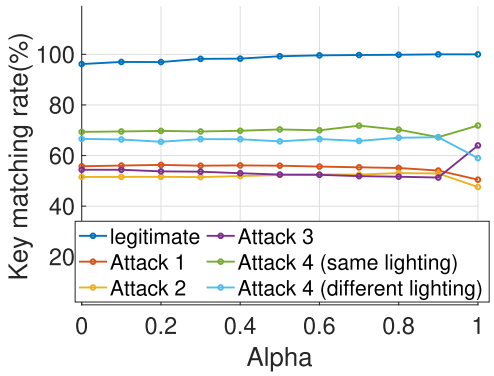


Fig. 22. Key matching rates under different attacks.

6.2 Performances

In this section, we perform the security analysis for our proposed method. As discussed in Section 6.1, Eve conducts imitating attack and eavesdropping attacks to discover the generated keys of legitimate devices. In the following part of this section, we will discuss how Eve conducts these attacks and their corresponding performances. The key generation rates under each attack are shown in Figure 22.

Against Imitating Attacks: When conducting Imitating Attacks (Attacks 1 and Attack 2), Eve uses the initial measurements to generate keys without any reconciliation. The key generation rates of Eve conducting Attack 1 and Attack 2 are shown in Figure 22. Compared with the nearly 100% key matching rates from legitimate devices, they can only achieve no more than 60% key matching rates. When Eve conducts the attack at the same place with the same lighting condition, its key matching rates are slightly better than those with different lighting conditions but significantly lower than that using legitimate devices. These results confirm the proposed method is secure against imitating attacks.

Against Eavesdropping Attack: When Eve performs Attack 3, she knows the projection matrix and captures the compressed generated keys. The size of the projection matrix is 80×128. As shown in Figure 22, after conducting ℓ_1 minimisation to recover keys, it can only achieve 50% key matching rates. The key generation rates of Eve conducting eavesdropping attack Attack 4 are also shown in Figure 22. They can only achieve no more than 70% key matching rates. Even though the key matching rates are better than that using Attack 1, Attack 2, and Attack 3, the performances are far below that of the legitimate devices. When conducting Attack 4 in the same lighting condition, the performance is slightly better than that in a different lighting condition. From the results in Figure 22, we can see that Eve can achieve at most approximately 75% key matching rate, while legitimate devices can obtain nearly 100% key matching rate. These results confirm the proposed method is secure against various attacks.

7 CONCLUSION

We conduct the first study to investigate the feasibility of using light to generate keys for solar-powered IoT devices. In this article, we propose a novel key generation method integrating compressed sensing techniques for a two-tier reconciliation method to increase the key matching rate up to 20% compared with no reconciliation method. We have conducted extensive evaluations to show the accuracy and efficacy of the proposed method and discuss the impact of many factors that affect the performance of the proposed method. We also confirm the randomness of the

generated keys by applying the NIST tests and calculating entropy. We further conduct the security analysis to confirm the security of the proposed method against various attacks. These attacks cannot achieve more than 80% key matching rates, while the proposed method can reach 100% key matching rates. Extensive evaluation results show that SolarKey is a secure and robust key generation scheme for future solar-powered IoT devices.

REFERENCES

[1] (n.d.). FRDM k64f, arm MBED. Retrieved from https://os.mbed.com/platforms/FRDM-K64F/

[2] Dania Qara Bala and Bhaskaran Raman. 2020. PHY-based key agreement scheme using audio networking. In *COMSNETS*. IEEE, 129–136.

[3] Richard G. Baraniuk. 2007. Compressive sensing [lecture notes]. *IEEE Signal Process. Mag.* 24, 4 (2007), 118–121.

[4] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. 1988. Privacy amplification by public discussion. *SIAM J. Comput.* 17, 2 (1988), 210–229.

[5] Dong Chen, Srinivasan Iyengar, David Irwin, and Prashant Shenoy. 2016. SunSpot: Exposing the location of anonymous solar-powered homes. In *BuildSys*. ACM, 85–94.

[6] D. L. Donoho. 2006. Compressed sensing. *IEEE Trans. Inf. Theor.* (2006), 1289–1306.

[7] Jun Han, Albert Jin Chung, Manal Kumar Sinha, Madhumitha Harishankar, Shijia Pan, Hae Young Noh, Pei Zhang, and Patrick Tague. 2018. Do you feel what I hear? Enabling autonomous IoT device pairing using different sensor types. In *IEEE SP*. IEEE, 836–852.

[8] Lars Erik Holmquist, Friedemann Mattern, Bernt Schiele, Petteri Alahuhta, Michael Beigl, and Hans-W. Gellersen. 2001. Smart-its friends: A technique for users to easily establish connections between smart artefacts. In *Ubicomp*. Springer, 116–122.

[9] Suman Jana, Sriram Nandha Premnath, Mike Clark, Sneha K. Kasera, Neal Patwari, and Srikanth V. Krishnamurthy. 2009. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *MobiCom*. ACM, 321–332.

[10] Long Jiao, Ning Wang, and Kai Zeng. 2018. Secret beam: Robust secret key agreement for mmWave massive MIMO 5G communication. In *IEEE GLOBECOM*. IEEE, 1–6.

[11] Rong Jin, Liu Shi, Kai Zeng, Amit Pande, and Prasant Mohapatra. 2015. MagPairing: Pairing smartphones in close proximity using magnetometers. *IEEE Trans. Inf. Forens. Secur.* 11, 6 (2015), 1306–1320.

[12] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Capkun. 2015. Sound-proof: Usable two-factor authentication based on ambient sound. In *24th USENIX Security Symposium*. 483–498.

[13] Zi Li, Qingqi Pei, Ian Markwood, Yao Liu, and Haojin Zhu. 2017. Secret key establishment via RSS trajectory matching between wearable devices. *IEEE Trans. Inf. Forens. Secur.* 13, 3 (2017), 802–817.

[14] Qi Lin, Weitao Xu, Guohao Lan, Yesheng Cui, Hong Jia, Wen Hu, Mahbub Hassan, and Aruna Seneviratne. 2020. KEHKey: Kinetic energy harvester-based authentication and key generation for body area network. *Proc. ACM Interact., Mob., Wear. Ubiq. Technol.* 4, 1 (2020), 1–26.

[15] Qi Lin, Weitao Xu, Jun Liu, Abdelwahed Khamis, Wen Hu, Mahbub Hassan, and Aruna Seneviratne. 2019. H2B: Heartbeat-based secret key generation using piezo vibration sensors. In *IPSN*. ACM, 265–276.

[16] Hongbo Liu, Yang Wang, Jie Yang, and Yingying Chen. 2013. Fast and practical secret key extraction by exploiting channel response. In *INFOCOM*. IEEE, 3048–3056.

[17] Hongbo Liu, Jie Yang, Yan Wang, and Yingying Chen. 2012. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In *INFOCOM*. IEEE, 927–935.

[18] Youjing Lu, Fan Wu, Shaojie Tang, Linghe Kong, and Guihai Chen. 2019. FREE: A fast and robust key extraction mechanism via inaudible acoustic signal. In *MobiHoc*. ACM, 311–320.

[19] Dong Ma, Guohao Lan, Mahbub Hassan, Wen Hu, Mushfika B. Upama, Ashraf Uddin, and Moustafa Youssef. 2019. SolarGest: Ubiquitous and battery-free gesture recognition using solar cells. In *MobiCom*. ACM, New York, NY.

[20] Miklós Maróti, Branislav Kusy, Gyula Simon, and Ákos Lédeczi. 2004. The flooding time synchronization protocol. In *SenSys*. 39–49.

[21] Suhas Mathur, Robert Miller, Alexander Varshavsky, Wade Trappe, and Narayan Mandayam. 2011. ProxiMate: Proximity-based secure pairing using ambient wireless signals. In *MobiSys*. ACM, 211–224.

[22] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. 2008. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In *MobiCom*. ACM, 128–139.

[23] Rene Mayrhofer and Hans Gellersen. 2009. Shake well before use: Intuitive and secure pairing of mobile devices. *IEEE Trans. Mob. Comput.* 8, 6 (2009), 792–806.

[24] Markus Miettinen, N. Asokan, Thien Duc Nguyen, Ahmad-Reza Sadeghi, and Majid Sobhani. 2014. Context-based zero-interaction pairing and key evolution for advanced personal devices. In *CCS*. ACM, 880–891.

[25] David L. Mills. 1991. Internet time synchronization: The network time protocol. *IEEE Trans. Commun.* 39, 10 (1991), 1482–1493.
[26] David L. Mills. 2012. Executive Summary: Computer network time synchronization. Retrieved from https://www.eecis.udel.edu/~mills/exec.html
[27] Julian Randall, Oliver Amft, Jürgen Bohn, and Martin Burri. 2007. LuxTrace: Indoor positioning using building illumination. *Person. Ubiq. Comput.* 11, 6 (2007), 417–428.
[28] Marc Roeschlin, Ivan Martinovic, and Kasper Bonne Rasmussen. 2018. Device pairing at the touch of an electrode. In *NDSS*, Vol. 18. 18–21.
[29] Masoud Rostami, Ari Juels, and Farinaz Koushanfar. 2013. Heart-to-Heart (H2H): Authentication for implanted medical devices. In *CCS*. ACM, 1099–1112.
[30] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. 2001. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Technical Report. Booz-Allen and Hamilton Inc., McLean, VA.
[31] Dominik Schürmann, Arne Brüsch, Stephan Sigg, and Lars Wolf. 2017. BANDANA–Body area network device-to-device authentication using natural gAit. In *PerCom*. IEEE, 190–196.
[32] Dominik Schürmann and Stephan Sigg. 2011. Secure communication based on ambient audio. *IEEE Trans. Mob. Comput.* 12, 2 (2011), 358–370.
[33] Jiacheng Shang and Jie Wu. 2020. AudioKey: a usable device pairing system using audio signals on smartwatches. *International Journal of Security and Networks* 15, 1 (2020), 46–58.
[34] Yiran Shen, Bowen Du, Weitao Xu, Chengwen Luo, Bo Wei, Lizhen Cui, and Hongkai Wen. 2020. Securing cyber-physical social interactions on wrist-worn devices. *ACM Trans. Sensor Netw.* 16, 2 (2020), 1–22.
[35] Yingnan Sun, Charence Wong, Guang-Zhong Yang, and Benny Lo. 2017. Secure key generation using gait features for body sensor networks. In *BSN*. IEEE, 206–210.
[36] Yoshinori Umetsu, Yugo Nakamura, Yutaka Arakawa, Manato Fujimoto, and Hirohiko Suwa. 2019. EHAAS: Energy harvesters as a sensor for place recognition on wearables. In *PerCom*. 1–10.
[37] Alex Varshavsky, Adin Scannell, Anthony LaMarca, and Eyal De Lara. 2007. Amigo: Proximity-based authentication of mobile devices. In *Ubicomp*. Springer, 253–270.
[38] Ambuj Varshney, Andreas Soleiman, Luca Mottola, and Thiemo Voigt. 2017. Battery-free visible light sensing. In *VLCS*. ACM, 3–8.
[39] Bo Wei, Weitao Xu, Kai Li, Chengwen Luo, and Jin Zhang. 2022. i2Key: A cross-sensor symmetric key generation system using inertial measurements and inaudible sound. In *IPSN*.
[40] Bo Wei, Weitao Xu, Chengwen Luo, Guillaume Zoppi, Dong Ma, and Sen Wang. 2020. SolarSLAM: Battery-free loop closure for indoor localisation. In *IEEE/RSJ IROS*. IEEE.
[41] Bo Wei, Mingrui Yang, Yiran Shen, Rajib Rana, Chun Tung Chou, and Wen Hu. 2013. Real-time classification via sparse representation in acoustic sensor networks. In *SenSys*. 1–14.
[42] Wei Xi, Xiang-Yang Li, Chen Qian, Jinsong Han, Shaojie Tang, Jizhong Zhao, and Kun Zhao. 2014. KEEP: Fast secret key extraction protocol for D2D communication. In *IWQoS*. IEEE, 350–359.
[43] Wei Xi, Chen Qian, Jinsong Han, Kun Zhao, Sheng Zhong, Xiang-Yang Li, and Jizhong Zhao. 2016. Instant and robust authentication and key agreement among mobile devices. In *CCS*. ACM, 616–627.
[44] Pengjin Xie, Jingchao Feng, Zhichao Cao, and Jiliang Wang. 2018. GeneWave: Fast authentication and key agreement on commodity mobile devices. *IEEE/ACM Trans. Netw.* 26, 4 (2018), 1688–1700.
[45] Fengyuan Xu, Zhengrui Qin, Chiu C. Tan, Baosheng Wang, and Qun Li. 2011. IMDGuard: Securing implantable medical devices with the external wearable guardian. In *INFOCOM*. IEEE, 1862–1870.
[46] Weitao Xu, Sanjay Jha, and Wen Hu. 2018. LoRa-key: Secure key generation system for LoRa-based network. *IEEE Internet of Things Journal* 6, 4 (2018), 6404–6416.
[47] Weitao Xu, Zhenjiang Li, Wanli Xue, Xiaotong Yu, Bo Wei, Jia Wang, Chengwen Luo, Wei Li, and Albert Y. Zomaya. 2021. InaudibleKey: Generic inaudible acoustic signal based key agreement protocol for mobile devices. In *IPSN*. 106–118.
[48] Weitao Xu, Girish Revadigar, Chengwen Luo, Neil Bergmann, and Wen Hu. 2016. Walkie-Talkie: Motion-assisted automatic key generation for secure on-body device communication. In *IPSN*. IEEE, 1–12.
[49] Lin Yang, Wei Wang, and Qian Zhang. 2016. Secret from muscle: Enabling secure pairing with electromyography. In *SenSys*. ACM, 28–41.
[50] Kai Zeng, Daniel Wu, An Chan, and Prasant Mohapatra. 2010. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In *INFOCOM*. IEEE, 1–9.
[51] Jiansong Zhang, Zeyu Wang, Zhice Yang, and Qian Zhang. 2017. Proximity based IoT device authentication. In *INFOCOM*. IEEE, 1–9.

Received 11 April 2022; revised 6 March 2023; accepted 6 June 2023