Telling Secrets in the Light: An Efficient Key Extraction Mechanism via Ambient Light

Youjing Lu, *Graduate Student Member, IEEE*, Fan Wu, *Member, IEEE*, Qianyi Huang, Shaojie Tang, *Member, IEEE*, and Guihai Chen, *Senior Member, IEEE*

***Abstract*— Due to the benefits of small latency, low energy consumption and increased data rate, device-to-device (D2D) communication is recognized as one of the promising techniques in the 5G era. However, the distributed nature of D2D communication makes it non-trivial to generate symmetric keys for the involving parties. Many efforts have been devoted to dynamically generate cryptographic keys for D2D communication in mobile network. However, most of them have limited applicability to practical scenarios due to low key generation efficiency or limited compatibility with commercial mobile devices. In this paper, we design an ambient light based key generation approach, which works on commercial off-the-shelf mobile devices, and achieves high key generation efficiency. We observe that mobile devices (e.g., smartphones, tablets) are often equipped with ambient light sensors and devices sense different light intensities at different angles towards the light source. We conduct a set of measurement study, and the results show that the light sensor data have several nice properties, i.e., space-varying, sensitive to the angle of measuring device, and time varying. These properties demonstrate that the ambient light is a good medium for secret key generation. We implement a prototype on different mobile devices, and conduct extensive experiments to evaluate its performance. The experiment results show that compared with the state-of-the-art key generation methods, our approach has a superior performance in key generation efficiency and robustness.**

***Index Terms*— Key generation, ambient light sensing, device-to-device communication.**

I. Introduction

DEVICE-TO-DEVICE (D2D) communication reforms the traditional communication paradigm of cellular networks [1]–[3]. It enables two mobile users communicate directly without the assistance of Base Stations (BSs) or core network. Due to the close proximity and potentially favorable channel conditions, D2D communications outperform on throughput, delay, and energy efficiency, making the communication more effective. Thanks to its efficiency, D2D communication supports both high data rate services (e.g., image/file transfer) and latency sensitive services (e.g., video sharing, gaming) [1], [4]. But many mobile users are deeply concerned about the privacy leakage of their information during the transmission [5]–[7]. In D2D applications, a significant amount of sensitive and private information, i.e., bank accounts, passwords, health conditions, etc., are transmitted through the untrusted public wireless channels, which can be eavesdropped by the attackers, who are interested in such sensitive information contents.

To secure the communication in mobile network, an intuitive solution is to encrypt the transmitted information. Encryption makes the transmitted information incomprehensible to attackers. D2D communication is usually ad-hoc, where is no preexisted and trusted management for secret key generation and distribution [8]–[10]. The traditional key exchange protocols, e.g., Diffie-Hellman (DH) protocol [11], rely upon the computational hardness of assumption, and its vulnerabilities have been identified in [12].

Considering the privacy and security of D2D communications, it is a necessity to generate secret keys for the parties involved in D2D communication. Most existing efforts exploit the inherent randomness shared by the mobile entities to extract the secret key. More specifically, they put mobile devices into physical proximity and use common environment characteristics as proof identities or common secrets for generating the secret key [9], [10], [13]–[17]. For example, Hershey *et al.* first proposed the method of bit generation for secret key sharing in [13]. Since then various channel measurements for key generation have emerged, including one-dimensional measurements, e.g., Angle of Arrival (AOA) [14] and Received Signal Strength (RSS) [10], [18], [19]; multi-dimensional measurements, e.g., Channel State Information (CSI) and Channel Impulse Response (CIR) [20]–[23].

However, previous efforts have limited applicability to practical scenarios due to low key generation rate, limited compatibility with commercial mobile devices, or the requirement of using the same type of mobile devices. For example, radio-telepathy generates secret key from the CIR of wireless channel, from which we can only get about one secret bit per second [9]. ProxiMate generates less than five bits

Manuscript received January 15, 2020; revised July 12, 2020; accepted September 9, 2020. Date of publication September 22, 2020; date of current version January 8, 2021. This work was supported in part by the National Key Research and Development Program of China under Grant 2019YFB2102200; in part by the China NSF under Grant 61972252, Grant 61972254, Grant 61672348, and Grant 61672353; in part by the Joint Scientific Research Foundation of the State Education Ministry under Grant 6141A02033702; and in part by the Alibaba Group through Alibaba Innovation Research Program. The associate editor coordinating the review of this article and approving it for publication was P. Li. *(Corresponding author: Fan Wu.)*

Youjing Lu, Fan Wu, and Guihai Chen are with the Shanghai Key Laboratory of Scalable Computing and Systems, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: luyoujing@sjtu.edu.cn; fwu@cs.sjtu.edu.cn; gchen@cs.sjtu.edu.cn).

Qianyi Huang is with the Institute of Future Networks, Southern University of Science and Technology, Shenzhen 518055, China, and also with the Peng Cheng Laboratory, Shenzhen 518066, China (e-mail: huangqy@sustech.edu.cn).

Shaojie Tang is with the Department of Information Systems, Naveen Jindal School of Management, The University of Texas at Dallas, Richardson, TX 75080 USA (e-mail: tangshaojie@gmail.com).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2020.3023930

per second in most scenarios [8]. Although some wireless channel measurement based key generation methods have high key generation efficiency [22], [23], they need the channel measurements provided by specialized hardware, e.g., they use CSI tool with the support of a special wireless interface card (i.e., Intel WiFi Link 5300, or Atheros AR 9380) [24]. However, in order to reduce the energy consumption, most of mobile devices do not provide the API for detailed channel measurement. FREE can achieve high key generation efficiency, but it requires the users to use the same type of mobile devices [25].

To address these deficiencies, we seek a key generation method that can achieve high key generation efficiency and is compatible with commercial off-the-shelf mobile devices. In this work, we propose to use ambient light, as our medium, to generate the secret key. Our study is motivated by two observations. First, the commodity mobile devices, e.g., smartphones, are often equipped with light sensors to sense the ambient light and adjust the brightness of the screen, saving the battery life. Second, measurement results show that light sensor data have several nice properties, i.e., space-varying, sensitive to the angle of measuring device (mobile devices sense different light intensities at different angles towards the light source), and time-varying. These properties demonstrate that ambient light is a good medium for secret key generation.

Although the idea sounds straight-forward, there are two challenges when generating secret keys from ambient light sensor data. The first is how to enable a group of mobile devices to sense as similar light intensity as possible, as light sensor data are the random sources for the key generation. The second is how to acquire an identical secret key from their similar light sensor data. For the first challenge, we move and rotate the group of mobile devices together along the same trajectory so that all of them have the same continuously changing angles to the light sources to ensure that their light sensor data have high similarity. For the second challenge, we propose a novel quantization method to quantize the light sensor data into bit streams and then reconciliate the mismatched bits in the bit streams to make them identical so that the group of mobile devices can finally generate the same secret key.

To achieve this idea, we design a key generation approach, named AKEM. AKEM contains two stages. In the first stage, we put different mobile devices in proximity and move them together along the same trajectory. In the second stage, their sensed light data are quantized into bit streams and reconciliated to solve their mismatched bits to generate identical bit sequences. To eliminate the possible privacy leakage caused by the reconciliation, we conduct privacy amplification on the bit sequence to acquire the final secret key.

To evaluate the performance of AKEM, we implement its prototype on different commodity mobile devices, and conduct extensive experiments in different scenarios. Experiment results demonstrate that AKEM improves the key generation rate greatly and achieves satisfactory robustness.

The main contributions of this work are summarized as follows.

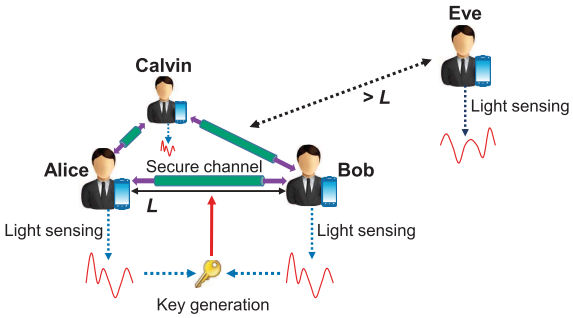


Fig. 1. System model. Alice, Bob, and Calvin are located together in physical proximity. All of them want to secure their exchanged information transmitted through public wireless channel. Then, their mobile devices are moved and rotated together along the same trajectory to sense the ambient light. The sensed light data provide them the randomness for generating the common cryptographic key, which constructs secure channels among them. A passive adversary Eve cannot sense the similar light data for generating the same key, due to out of the proximity of legitimate users and unreplicated light sensor data.

- We propose to use ambient light sensor data to generate secret key. We conduct a variety of measurements and validate the properties of ambient light sensor data, i.e., space-varying, sensitive to the angle of measuring, and time-varying, which all demonstrate that ambient light is an appropriate medium for key generation.
- We propose AKEM, where users move and rotate the mobile devices together to get similar light measurements. In order to reduce the quantization error and improve key generation efficiency, we present a novel quantization method to adapt to the light sensor data which have great different ranges in indoor and outdoor environments.
- We implement our design on different mobile devices. Evaluation results show that AKEM can generate 260 secret bits in a second, which is higher than existing key generation methods.

The rest of the paper is organized as follow. Section II presents the system model and attack model. Section III introduces the background of ambient light and analyzes the feasibility of using sensed light data for key generation. Section IV gives the design details of AKEM. Section V analyzes the security of AKEM. Section VI evaluates the performance of AKEM. Section VII discusses the practical application of AKEM. Section VIII briefly reviews the related work. Section IX concludes this paper.

II. System and Attack Model

In this section, we present our system and attack model.

We first illustrate the system model, which is shown in Fig. 1. There are three legitimate users, named Alice, Bob, and Calvin, and a passive adversary, Eve. The legitimate users have no prior shared secret. To prevent Eve from eavesdropping their private communication, these legitimate users need to protect their transmissions by cryptographic keys. The legitimate users are equipped with off-the-shelf mobile devices, e.g., smartphones, tablets. The maximum distance between any two of legitimate users is within L, as shown

in Fig. 1. Eve is out of the proximity of legitimate users, and he is equipped with a mobile device, which also can sense the ambient light.

Our goal is to utilize the similar ambient light sensor data to generate secret key among legitimate users while achieving significantly higher key generation rate and lower bit mismatched ratio, resisting the passive attacks from the adversary Eve. We assume that the legitimate users are willing to make some efforts (e.g., rotating the mobile devices) to achieve this goal.

Next, we analyze several possible attacks from the adversary, Eve. Eve can eavesdrop all signals transmitted wirelessly by legitimate users. Eve is also able to sense the ambient light and has the same computational capability as the legitimate users. He tries his best to guess the key generated by legitimate users. We assume that Eve cares about the exchanged information and thus he is interested cracking the encryption among the legitimate users. Hence, he has no intention to jam the wireless channels or hinder the key generation process among legitimate users. Based on these assumptions, we mainly consider the following three possible passive attacks from Eve:

- Eavesdropping: Eve can overhear all messages transmitted through the public wireless channel among legitimate users. Then, Eve can analyze these eavesdropped messages and try to guess the generated cryptographic key.
- Detecting-simultaneously: We suppose that Eve knows the method of key generation and the settings of parameters. Then, he can generate secret key from ambient light measurements by performing the same operations as the legitimate users. The main limitation for Eve is that he cannot get too close to the legitimate users. His distance to any legitimate user is larger than L.
- Repeating-afterwards: When these legitimate users finish all key generation operations and leave the original location, Eve can come to this location and imitate their operations to sense the ambient light for generating the secret key.

III. Preliminaries

In this section, we introduce the background knowledge of ambient light, and study the feasibility of using light sensor data for key generation.

A. Ambient Light and Light Sensor

Light is everywhere. The importance of the light to human is just like the air to human. People live in the light, and use the light for illumination, energy resource, communication, etc. In our daily life, there are many light sources, including natural light sources and artificial light sources. The natural light sources include sun, moon, lightning, which are changing over time. Artificial light sources include various fluorescent lamps, LEDs, which are relatively stable.

Both ambient light indoor and outdoor can be affected by different light sources and changing shadowing. For indoor environment, such as laboratory, the ambient light intensity at a certain location is affected by many factors, i.e., the number of fluorescent lamps and LEDs, daylight, the distance to light sources, shadowing of different kinds of furniture, moving people, and other objects, etc. When the light sources change, the ambient light sensed at the same location changes subsequently. For more dynamic indoor environment, e.g., a busy shopping mall, where exist more artificial light sources and changing shadowing (i.e., moving people). The light intensity changes more rapidly. Ambient light in outdoor open space is mainly affected by natural light sources. However, in a crowded place, like a busy playground, where exists many infrastructures, fluorescent lamps, trees, and visitors, the ambient light intensity sensed at a certain location also changes rapidly due to the changing distribution of light sources and shadowing.

Mobile devices are always equipped with ambient light sensors, and use them to sense the ambient light intensity to adjust the brightness of the screen so as to save the battery life.

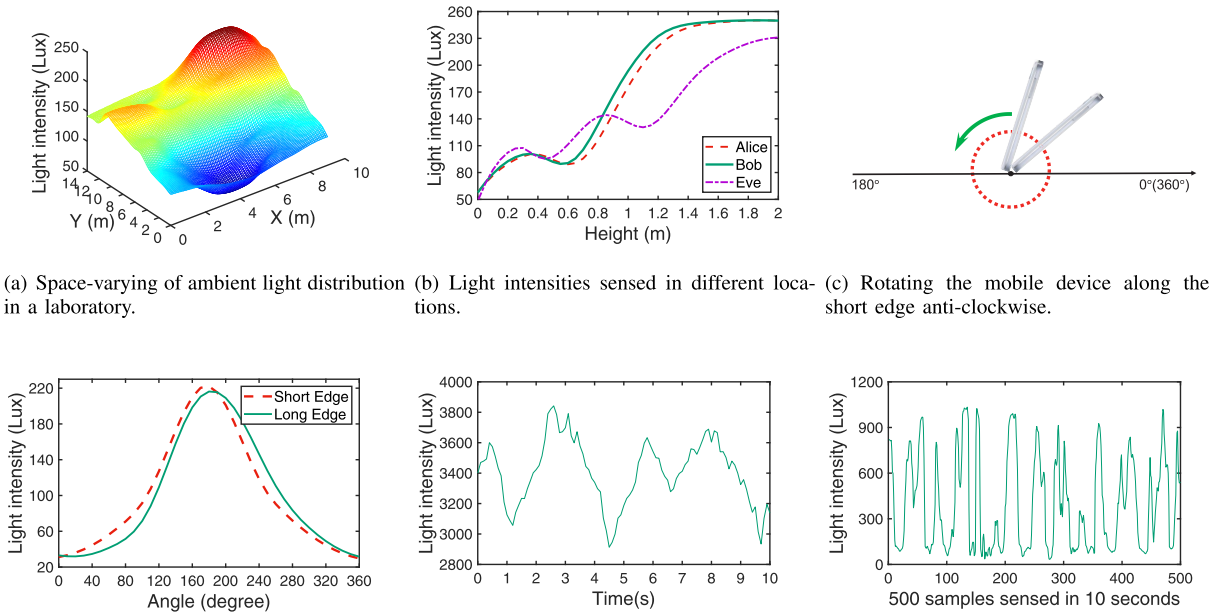
B. Feasibility Study

We study the feasibility of using ambient light sensor data for key generation through extensive measurements.

1) Space-Varying: As we mentioned above, changing light sources and shadowing can affect the light intensity, which brings the space-varying property of ambient light. We have conducted extensive measurements to study the light intensity distribution in both indoor and outdoor environments. For indoor environment, we measured the ambient light intensity distribution of a 10×14 m^2 laboratory area using 10 Nexus 7 tablets, which are equipped with ambient light sensors. We took one of the corners as the origin of the coordinates, and measured the light intensity every 10 cm along the horizontal and vertical coordinates. There are some shadowing sources such as furniture, appliances, moving staffs, etc., in this room. As shown in Fig. 2(a), the indoor light intensity distribution is non-uniform, which illustrates the property of space-varying.

To measure the effect of space-varying, we compared the light intensities sensed in different locations. We put two legitimate smartphones (Alice and Bob) in adjacent positions, and the distance between them was 10 cm. We recorded their sensed light data by holding them together at different heights simultaneously, ranging from $0\sim2$ m. We also recorded the sensed light data from Eve, who was located 20 cm away from Alice and Bob. As shown in Fig. 2(b), we can see that Alice and Bob have sensed similar ambient light data, which verify that strong correlation exists in adjacent positions. Eve's sensed light data are obviously different from Alice or Bob. This is due to the space-varying property of ambient light distribution. It means that when the distance between two mobile devices is greater than a certain distance, the ambient light sensed by the two mobile devices have little correlation due to non-uniform light distribution.

2) Sensitive to the Angle of Measuring Mobile Device: To validate this property, we have measured light intensity at different angles in indoor and outdoor environments. In this set of experiments, we rotated a smartphone from 0° to 360° along the short edge of itself, as shown in Fig. 2(c). We recorded the light intensities at different angles, as shown in Fig. 2(d).



(a) Space-varying of ambient light distribution in a laboratory.

(b) Light intensities sensed in different locations.

(c) Rotating the mobile device along the short edge anti-clockwise.

(d) Light intensities sensed by the mobile device rotated along the short edge and long edge, respectively.

(e) Time-varying light intensity in outdoor environment.

(f) Rotating and moving the smartphone randomly in indoor scenario.

Fig. 2. The properties of ambient light: space-varying, sensitive to the angle of measuring mobile device, and time-varying.

We can see that the light intensity is very low when the rotation angle is $0°$. This is because the smartphone is back facing the light sources and only picks up a little light. The light intensity gradually increases when we increased the rotation angle. The light intensity is maximal when the rotation angle is around $180°$. This is because that the light sensor is facing the light source and picks up more direct light from light sources. However, the light intensity gradually decreases with larger rotation angle, due to less light received. We also rotated the smartphone from $0°$ to $360°$ along the long edge of itself, the measurements show similar results as the case of short edge, as shown in Fig. 2(d). So the sensed light intensity is verified to be sensitive to the different rotation angles of the mobile device. Thus, the mobile device senses different light intensity at different angles.

3) Time-Varying: Based on our measurements and observations, we find the distribution of light intensity is also time-varying, with the participation of natural light source and movement. For example, Fig. 2(e) shows the measurement results for a fixed point outdoor during 10 seconds. We can see the light intensity changes as time goes. We need to point out that the light intensity on a spot in indoor scenario is relatively stable when the light sources and surrounding shadowing are not changing. But the motion of devices still can offer enough varying light data. Fig. 2(f) shows the 500 samples sensed in 10 seconds by rotating and moving the smartphone randomly in indoor scenario. We can see the light intensity changes obviously when we rotate and move the smartphone randomly. When the light is relatively stable, the randomness of measurements is mainly provided by the rotation and moving of the mobile devices.

In summary, the results show the three significant properties of ambient light sensor data, i.e., space-varying, sensitive to the angle of measuring mobile device, and time-varying.

IV. Design

In this section, we present the challenges, ideas, and design details of AKEM.

A. Design Rationale

The above three properties validate the feasibility of using sensed light data for key generation. Space-varying, sensitive to the angle of measuring mobile device, and time-varying can offer users enough randomness for generating the secret key. Space-varying and time-varying can help users resist the above mentioned attacks.

We next try to exploit the ambient light sensor data as the inherent randomness to generate the common secret key, constructing a secure channel for the legitimate users. The main challenges are how to generate similar random patterns from the ambient light and how to extract a common secret key from the similar patterns.

For the first challenge, our idea is to move and rotate the mobile devices along a common trajectory to sense the ambient light with a same frequency f_s, acquiring similar light intensity data (In our experiments, we fix these devices on a bracket to guarantee that they are moved and rotated along the same trajectory. In practice, one legitimate user can stack the devices up in the same direction and expose their light sensors, which are on top of screens, and then move them together). We next consider normalizing these sensor data, and

then exploiting the largest relative change pairs in their sensor data to be the source of randomness to reduce the influence of the senor data difference caused by different sensitivity of light sensors from different manufacturers.

For the second challenge, we quantize the above mentioned largest relative change pairs into binary bit streams, separately. To make the bit streams of legitimate devices identical, the legitimate users exchange some information for reconciliating the mismatched bits. To eliminate the risk of secret key leakage caused by the exchanged information, the devices conduct privacy amplification operations on their reconciliated bit sequence to acquire the final secret key.

B. Design Details

In the light of our basic idea, the design of AKEM consists of the following stages, initialization, sensing, quantization, reconciliation, and privacy amplification. For ease of presentation, we take an example of key generation among three legitimate users, Alice, Bob, and Calvin.

1) Initialization and Sensing: In the initial stage, the legitimate users need to synchronize the start time for sensing the ambient light. Alice, as an initiator, broadcasts a synchronization signal to other legitimate users. After time t_Δ, all the legitimate users start sensing. Here we do not require very precise synchronization, because AKEM does not simply quantize the light intensity of start point and is able to tolerate some minor errors. In our approach, the biggest sampling rate is 50Hz, and thus it costs 20ms to get a light intensity sample. The time difference of Alice and Bob start sensing is t_Δ, which is theoretically no more than 6.7×10^{-7}ms when the distance between Alice and Bob is 20cm (Radio propagation speed $c \approx 3.0 \times 10^{-7}$m/s, and $t_\Delta = \frac{d}{c}$). 6.7×10^{-7}ms is not enough to get a light intensity sample. The two devices can leverage the Wi-Fi/Bluetooth module for synchronization. According to [26], the synchronization error is less than 1ms. Therefore, our approach can tolerate this minor synchronization error.

The legitimate users start sensing the ambient light with frequency f_s, and store the sensor data locally. To illustrate it formally, the sensor data are denoted as below:

$$M_u = \left\{ {m_u}^1, {m_u}^2, \cdots, {m_u}^i, \cdots, {m_u}^p \right\}^T, \tag{1}$$

where u = Alice/Bob/Calvin, denotes different users, ${m_u}^i$ represents the light intensity recorded by the user.

2) Quantization: Users need to quantize the light sensor data into secret bit streams. Here we design a method for them to find the exact source of randomness.

Seeking Largest Pairs: In this quantization method, we use the largest relative intensity change in certain intervals to be the exact source of randomness. As we mentioned above, legitimate users' light sensors have different sensitivities as they are made by different manufactures. So it is hard to acquire a secret key directly from their light sensing. To eliminate the difference, legitimate users first normalize their sensed light data, respectively. Since the mobile devices are moved and rotated together along the same trajectory when sensing the ambient light, their sensed light data have many identical relative changes. Then, we exploit the relative changes on light intensity to design an appropriate randomness seeking method.

Algorithm 1 Seeking Largest Changing Pairs

Input: Light sensor measurement array $M = \left\{ m^1, m^2, \cdots, m^i, \cdots, m^n \right\}$, total length n.
Output: Sensing sequence Q.

```
S_x = max(m^1, m^2, ..., m^i, ..., m^n);
foreach i=1 to n do
    s^i = m^i / S_x;
for k = 8: 2 : n do
    Γ = ∅;
    foreach j=1 to n-k do
        Γ = Γ ∪ ⟨s^j, s^{j+k}⟩;
    Find the largest ⟨s^p, s^q⟩ in Γ;
    Take s^p, s^q as a tuple (s^p, s^q) and add them into Q;
return Q;
```

As shown in Algorithm 1, the main idea is seeking the largest relative change pairs in the same intervals of users' measurements to find the exact source of randomness. The algorithm takes an array of ambient light sensor readings as input and returns a sensing sequence Q. We first normalize the input and set the first interval length as 8 to make the intervals long enough. Every iteration is to find the largest relative intensity change pair in a certain interval. For example, in an iteration when the interval is τ, we find the largest relative change pair in

$$\left\{ \left\langle s_u^1, s_u^{1+\tau} \right\rangle, \left\langle s_u^2, s_u^{2+\tau} \right\rangle, \cdots, \left\langle s_u^{n-\tau}, s_u^n \right\rangle \right\}, \tag{2}$$

where $\langle x, y \rangle$ denotes the relative change between x and y. In each iteration, we will find the largest intensity change pair $\langle s_u^p, s_u^q \rangle$, then we add them into the sensing sequence Q. To improve the efficiency, we can acquire enough pairs by altering the time interval every iteration.

After running the above algorithm, Alice, Bob, and Calvin acquire the sensing sequence Q_A, Q_B, and Q_C locally, respectively.

Then, these bit sequences need to be transformed into bit streams. In our experiments, the light data sensed indoor range from a few tens of Lux to a few hundreds of Lux; the light data sensed outdoor range from a few tens of Lux to tens of thousands of Lux, where Lux is the unit of light intensity. The range of light intensity changes are pretty large and non-uniform. To reduce the quantization error, an adaptive quantization method is required.

Inspired by the non-uniform quantization of Pulse Code Modulation (PCM), we present a new quantization method. Given that both Android and iOS API use 32 bit to record the value of light intensity, and the maximum light intensity in our experiment is lower than 2^{19} Lux, so we quantize the maximum light intensity into 2^{19} intervals, as listed in Table I. To trade off between key generation efficiency and quantization error, we use 8 bits to encode a sensed light sample. The first 4 bits are segmental code, and the last 4 bits are internal code. We divide the 2^{19} intervals into 16 segments.

TABLE I
SEGMENTAL CODE (c_1 c_2 c_3 c_4)

Segment NO.	Segment bits	Dynamic range	Segment NO.	Segment bits	Dynamic range
1	0000	$0 \sim 2^4$	9	1000	$2^{11} \sim 2^{12}$
2	0001	$2^4 \sim 2^5$	10	1001	$2^{12} \sim 2^{13}$
3	0010	$2^5 \sim 2^6$	11	1010	$2^{13} \sim 2^{14}$
4	0011	$2^6 \sim 2^7$	12	1011	$2^{14} \sim 2^{15}$
5	0100	$2^7 \sim 2^8$	13	1100	$2^{15} \sim 2^{16}$
6	0101	$2^8 \sim 2^9$	14	1101	$2^{16} \sim 2^{17}$
7	0110	$2^9 \sim 2^{10}$	15	1110	$2^{17} \sim 2^{18}$
8	0111	$2^{10} \sim 2^{11}$	16	1111	$2^{18} \sim 2^{19}$

TABLE II
INTERNAL CODE (c_5 c_6 c_7 c_8)

Interval	Internal bits	Interval	Internal bits
0	0000	8	1000
1	0001	9	1001
2	0010	10	1010
3	0011	11	1011
4	0100	12	1100
5	0101	13	1101
6	0110	14	1110
7	0111	15	1111

Each segment has a 4-bit segmental code (c_1 c_2 c_3 c_4). For each segment, we divide it into 16 intervals uniformly, and assign them with a 4-bit code (c_5 c_6 c_7 c_8), as listed in Table II.

We have an example for this quantization method. Suppose the largest light intensity pair in Q is $(1.2\times10^{-4}, 4.9\times10^{-2})$, then the code calculated for 1.2×10^{-4} is as follow, $1.2 \times 10^{-4} \times 2^{19} = 62.9$, which is in the third segment, so the c_1 c_2 c_3 c_4 is 0010. The interval for third segment is $\frac{2^6-2^5}{16} = 2$, and $62.9 = 32+2\times15+0.9$, which is in the 16^{th} interval, so the internal bits (c_5 c_6 c_7 c_8) is 1111. Finally, the code calculated for 1.2×10^{-4} is 00101111.

According to this non-uniform quantization method, Alice, Bob, and Calvin quantize their sensing sequences and then get the bit stream D_A, D_B, and D_C respectively.

3) Information Reconciliation: Once Alice, Bob, and Calvin get the quantized bit stream D_A, D_B, and D_C, they need to reconciliate their mismatched bits. To avoid exposing the bit stream, they cannot compare them directly. Then, we apply a cryptographic method to address this problem. In the communication field, error correcting code techniques are extensively used to reconcile approximate information. So we are inspired to improve an secure sketch method [27] to reconcile the mismatched bits.

Improved secure sketch generates a shared information s about the input X, and s does not expose X, then s and $\hat{X}$, which is close to X on hamming distance, can be used to recover X. We assume Alice, Bob, and Calvin hold bit stream D_A, D_B, and D_C (dis(D_A, D_B)<t, dis(D_A, D_C)<t, and dis(D_B, D_C)<t). Here dis(x, y) is the hamming distance between x and y. We use a $[n, k, 2t+1]_2$ error code (where n is codeword length, k is message length, and t is error-correction capability) to correct errors in D_B and D_C even though D_B and D_C may not be in codeword set C [28]. In information reconciliation, Alice randomly selects a random codeword c from C and computes $s = D_A \bigoplus c$. Then Alice sends s to Bob and Calvin. After receiving s, Bob and Calvin compute the shift s from D_B and D_C, to get $\hat{c_1} = D_B \bigoplus s$ and $\hat{c_2} = D_C \bigoplus s$, respectively. As an example, suppose $|D_A| = |D_B| = |D_C| = 64$ bit, dis(D_A, D_B) = dis(D_A, D_C) = 11. In our case, Alice, Bob, and Calvin can employ a $[63, 16, 2\times11+1]_2$-BCH codes to correct error bits. Alice uses the first 63 bit of D_A to compute s and sends it with the hash value $h(D_A)$ to Bob and Calvin. Bob and Calvin correct error bits in the first 63 bit of sequence D_B and D_C, then they use $h(D_A)$ as a reference to determine the sequence D_A, respectively.

4) Privacy Amplification: Next, we need to eliminate the risk of secret key leakage due to exchanging information in the reconciliation phase. We notice that the error correcting information is public to all of legitimate users and adversaries, it can be used by adversaries to guess part of the secret key. Therefore, we need to remove the possible leaked portions of secret key. To address this problem, privacy amplification is an effective technique.

Privacy amplification reduces the length of the final secret sequence to ensure the confidentiality of the secret key. Let Alice, Bob, and Calvin use universal hash functions, randomly chosen from well-known hash function families, to get fixed short length sequence from the original long sequence. Generally, privacy amplification generates a short sequence with high entropy rate from a long sequence with low entropy. *Leftover hash lemma* [10], [29] is the most popular technique used for privacy amplification to extract randomness from imperfect random sources. We implement this method in this paper.

In the dark environment, there is no light sources offering the light for ambient light sensing, and it limits the applicability of AKEM. To address this problem, we consider using the flashlights of the mobile devices to provide lights for AKEM. In our experiments, we can turn on one device's flashlight to increase the intensity of ambient light. We can easily know the produced light distribution also have the properties of space-varying, sensitive to the angle of measuring mobile device. These properties are also validated by the extensive measurements.

V. SECURITY ANALYSIS

In this section, we analyze the security performance of AKEM under the above mentioned attacks.

A. Against Eavesdropping Attack

Under the eavesdropping attack, the information exchanged by legitimate users is transmitted through the public wireless channel, which can be eavesdropped by the adversary Eve. We analyse what information can be obtained by Eve. The first interaction among legitimate users is in the initial stage, when the initiator Alice sends a notification signal to other legitimate users for synchronization and then receives feedback signals from other legitimate users. The second interaction is in the information reconciliation stage, when Alice sends s to

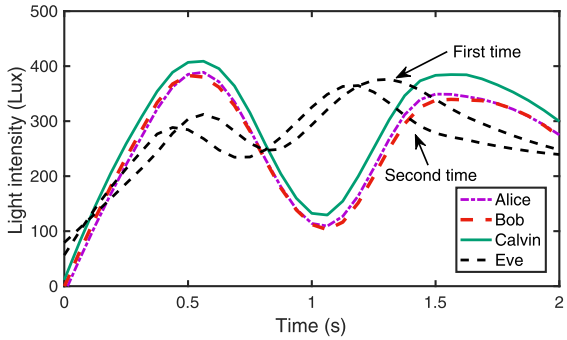


Fig. 3. Sensed light data are irreproducible. The first three volunteers as legitimate users, Alice, Bob, and Calvin, sense the ambient light along the same trajectory. After they finished the key generation steps, the last volunteer, as adversary Eve, moves to the same position and performs the same operations to sense the ambient light twice. But he cannot get the similar light data of legitimate users.

other legitimate users. The transmitted information s includes the XOR result of D_A and a codeword c. The number of codewords in C is 2^{63} in our case. It is very hard for Eve to guess the secret key from s if the length of D_A is long since the computation overhead grows exponentially. In addition, privacy amplification technique prevents information leakage from s. Therefore, Eve cannot guess any information about the secret key by eavesdropping the interactions among legitimate users.

B. Against Detecting-Simultaneously Attack

Under the detecting-simultaneously attack, the legitimate users are located in proximity, and the adversary Eve is located out of the proximity of legitimate users, as shown in Fig. 1. Here the adversary Eve cannot get close to these legitimate users, who are sensing the ambient light intensity. But Eve can use the synchronization signal as an indicator to start sensing ambient light. However, he still cannot sense similar light data as the legitimate users due to the properties of space-varying. In addition, Eve cannot rotate or move his mobile device along exactly the same trajectory as the legitimate users. Thus, Eve cannot generate the same secret key as legitimate users from his ambient light sensor data. Thus, AKEM can resist the detecting-simultaneously attack.

C. Against Repeating-Afterwards Attack

Under the repeating-afterwards attack, after the legitimate users finish key generation procedure, Eve can move to the same location to repeat the same operations as legitimate users performed, trying to generate the same secret key. We conduct experiments to test if Eve can generate the same secret key. We invite four volunteers to play as Alice, Bob, Calvin, and Eve. Everyone holds a mobile device, equipped with an ambient light sensor. The mobile devices of Alice, Bob, and Calvin are moved and rotated together to sense the ambient light, and the sensed light data are shown in Fig. 3. When these legitimate users finished the key generation, Eve move to the same position to sense the ambient light twice by imitating the movements of legitimate users, and the sensed light data are also shown in Fig. 3. We can see the obvious difference between the light data of Eve and the legitimate users. That is mainly because the distribution of light intensity is time-varying, Eve cannot acquire similar light sensor data to reproduce the same secret key. In addition, Eve cannot move or rotate the mobile device along exactly the same trajectory or at exactly the same speed as the legitimate users. In fact, the legitimate users can use more complex rotating and moving trajectory on purpose to better resist the possible attacks.

VI. Evaluation

In this section, we present the prototype implementation, experiment setup, and the performance results of AKEM.

A. Implementation

We conduct extensive experiments in different scenarios with four volunteers, named as Alice, Bob, Calvin, and Eve. The first three of them are the legitimate users, and the last one is the adversary. We implement AKEM prototype on several kinds of mobile devices, i.e., Nexus 7, MEIZU MX 6, Xiaomi 3, and all of them are equipped with an ambient light sensor. The type of the ambient light sensor on Google Nexus 7 is AL3006, and its resolution is 1.0 Lux [30]. The type of the light sensor on Xiaomi 3 is ISL29009IROZ-T7A, and its resolution is 0.3 Lux [31]. The type of the light sensor on MEIZU MX 6 is APDS-9922, and its resolution is 1.0 Lux [32]. The three legitimate mobile devices are fixed on a bracket, and the default distance between any two of them is 5 cm. They are rotated and moved along the same trajectory, and the default trajectory is "8". We conduct our experiments in both indoor and outdoor environments.

We call the Android API for sensing the ambient light. The parameters of light sensor are configured by setting the Sensor. TYPE_LIGHT_FIELD. In general commercial Android devices, the sensing frequency f_s can be set as one of the following values, i.e., 50 Hz, 16.7 Hz, and 5 Hz. When the sensing frequency is set, the sensor manager will receive periodic SensorEvent from the light sensor, and the SensorEvent includes the light sensing measurement. Alice uses Bluetooth to broadcast a synchronization signal to other legitimate users to start sensing the ambient light. Once the ambient light sensing is finished, the system will call the function seeking_largest_changepair( ) automatically to find the exact source of randomness and return a sensing sequence. Then the sensing sequence is encoded into a bit stream by our non-uniform quantization method. Next, the legitimate users start to use the improved secure sketch method to reconciliate their mismatched bits. Then, they perform the privacy amplification operations to acquire the final secret key.

B. Setup and Metrics

We conduct a variety of experiments indoor and outdoor. Our indoor experiment environment is a 10×14 m^2 lab; the outdoor experiment environment is a big lawn in front of our office building. Additionally, the mobile devices are fixed on a bracket, and the distance between them is adjustable. Then,

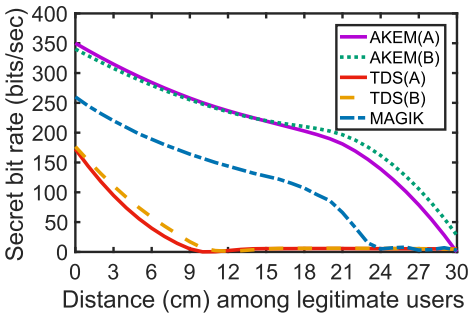


Fig. 4. Secret bit rate with different distances.

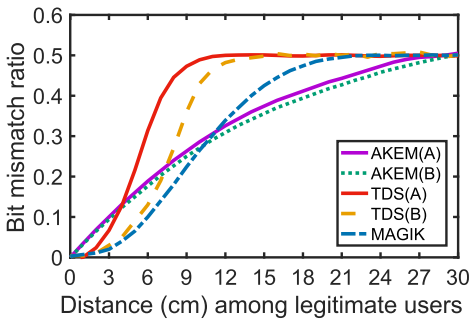


Fig. 5. Bit mismatch ratio with different distances.

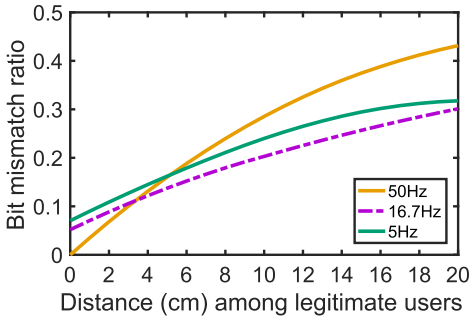


Fig. 6. Bit mismatch ratio with different sensing frequencies.

the mobile devices can be moved and rotated in the same trajectory to collect the ambient light sensing measurements.

To measure the system performance, we have the following metrics:

- Secret Bit Rate (SBR): SBR is the number of generated secret bits in a second. SBR can indicate the time needed for key generation and system efficiency.
- Bit Mismatch Ratio (BMR): BMR is the ratio of mismatched bits between all quantized bits of two mobile devices. BMR can indicate the system robustness. The smaller BMR, the higher robustness of key generation.
- Randomness and Entropy (RE): RE can evaluate the quality of the generated key. We use a widely used randomness measurement, NIST test, to measure the randomness of the generated key. We also compute the entropy of the generated secret key. The entropy can measure the uncertainty of the generated keys. The higher the entropy, the better the quality of the generated secret key.

C. The Influence of Distance

We change the distance among legitimate users to study how the distance influences the performance of AKEM. We set the sensing frequency as 50 Hz and the trajectory as "3".

Fig. 4 shows the secret bit generation rate in different distances, and the indoor and outdoor environment are labeled as "A" and "B", respectively. We find that the secret bit generation rate is greater than 200 bits/sec when the distance ranges from 0 to 20 cm. For comparison, we present the secret bit generation rate of the state-of-the-art key generation methods, i.e., TDS [23] and MAGIK [33]. We can see the secret generation rate of AKEM is obviously greater than that of TDS and MAGIK. The secret bit generation rate of AKEM decreases dramatically when the distance is greater than 20 cm. The main reason is that the ambient light distribution is space-varying. We also find the secret bit generation rate in indoor environment is higher than that in outdoor environment. The reason is that the ambient light intensity indoor changes more frequently and provides more randomness due to more factors, such as the shadowing of furniture, appliance, moving staffs, etc., affecting the ambient light.

Fig. 5 shows the bit mismatch ratio versus different distances in both indoor and outdoor environments. We find that the bit mismatch ratio increases as distance grows. The bit mismatched ratio of AKEM is higher than that of MAGIK, but lower than that of TDS when the distance ranges from 7 cm to 12 cm. But when the distance increases, the bit mismatched ratio of both TDS and MAGIK are greater than that of AKEM. We can see the mismatch ratio of AKEM is around 0.5 when the distance is around 27 cm. Therefore, AKEM outperforms TDS and AKEM on the bit mismatch ratio when the distance ranges from 12 cm to 27 cm.

D. The Influence of Sensing Frequency

We change the sensing frequency to study how it influences the system performance. The results are shown in Fig. 6. We can see that the mismatched bit ratio with high sensing frequency, i.e., 50 Hz, is lower than that with low sensing frequencies, i.e., 5 Hz and 16.7 Hz. The reason is that the collected light data under higher frequency is more sensitive to subtle difference, and can capture more peaks, while the collected light data under lower frequency miss many important peaks, which cause a higher mismatch ratio. However, this situation changes as distance grows. The reason is that the difference of light data sensed by different users increases as distance grows, and the collected light data with high frequency can record more misleading peaks, which cause a higher mismatch ratio.

E. The Influence of Moving Trajectory

To study how moving trajectory influences the performance of AKEM, we collect light sensor data indoor and outdoor under different trajectories, i.e., "0", "1", "3", and "8". As shown in Fig. 7, we can see that the complexity of moving trajectory influences the mismatch ratio obviously.

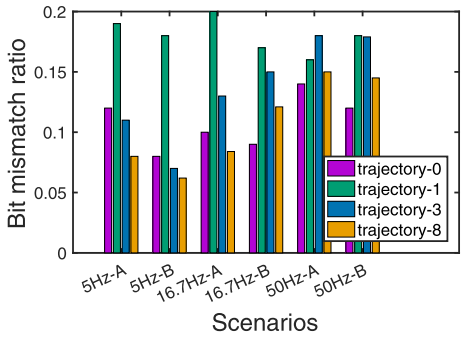


Fig. 7. Bit mismatch ratio with different trajectories.

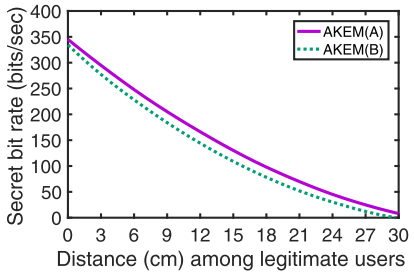


Fig. 8. Secret bit rate with different distances in the dark environment.

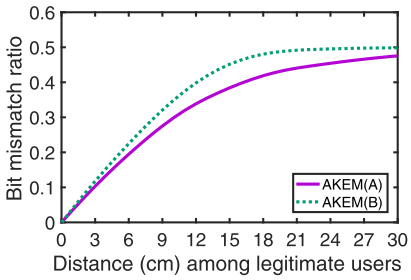


Fig. 9. Bit mismatch ratio with different distances in the dark environment.

TABLE III
NIST STATISTICAL TEST RESULTS

Test	Indoor	Outdoor
Monobit Frequency	0.659	0.743
Longest Run of 1s	0.640	0.644
FFT	0.507	0.818
Approximate Entropy	0.834	0.757
Cumulative Sums (Fwd)	0.532	0.623
Cumulative Sums (Rev)	0.818	0.824
Block Frequency	0.681	0.760
Runs	0.768	0.842
Serial	0.520	0.681
	0.644	0.727

The more complicated the moving trajectory, the lower the bit mismatch ratio. The reason is that we can collect more diverse light sensor data patterns when moving and rotating along more complicated trajectories, and we can capture more different peaks to reduce the bit mismatch ratio. Besides, the bit mismatch ratio indoor is lower than that outdoor with the same sensing frequency. The reason is also that the ambient light data vary more rapidly indoor, and we can collect more different peaks to reduce the mismatched bit ratio.

F. Performance of AKEM in the Dark Environment

As mentioned above, we use the flashlights of mobile devices to be the light sources in the dark environment. Then, we also evaluate the performance of AKEM in the dark environment. Fig. 8 shows the secret bit rate of AKEM with different distances in the dark environment. We can find that the secret bit rate is more than 200 bit/s when the distance is shorter than 10 cm, and the secret bit rate also decreases with growing distance. Fig. 9 shows the bit mismatch ratio with different distances in the dark environment. We can find that the bit mismatch ratio of both indoor and outdoor approach 0.5 when the distance is larger than 18 cm. The results show that AKEM also can achieve a high bit rate in the dark environment.

G. Randomness of Generated Keys

We test the randomness of the secret key generated by AKEM. For experiment setting, the distance among legitimate users ranges from $0 \sim 20$ cm and the sensing frequency is 50 Hz. Previous efforts used NIST test to measure the randomness of generated bits [23], [34]–[37]. Here we also utilize NIST test to measure the generated 300 secret sequences under different distances in both indoor and outdoor environments, and compute their average p-values for 8 types of tests, listed in Table III. The sequence is marked as random if all p-values are greater than 0.05. We can see the keys generated by AKEM pass all types of tests. Thus, the generated keys have good randomness.

H. Conditional Min-Entropy of Generated Keys

To evaluate the security of generated secret keys under the eavesdropping of Eve, we compute their conditional min-entropy $\widetilde{H}_{\infty}(X/Y)$, which is defined as

$$\widetilde{H}_{\infty}(X/Y) \stackrel{def}{=} -\log(E_{y \leftarrow Y}[\max_x Pr[X = x|Y = y]]) \quad (3)$$

in [38], [39]. Eve is located 20cm away from legitimate users in indoor and outdoor environments. Conditional min-entropy is used by many previous efforts to measure the knowledge of the adversary to the secret key [34], [35], [40], [41]. For simplifying the computation of conditional min-entropy, we set the lengths of variable X and variable Y as 1. We analyze the bits at the corresponding position of these two bit strings, and conduct the analysis on all pairs of bit strings generated by Alice and Eve to get the average conditional probability $Pr[X = x|Y = y]$ and the expectation $E_{y \leftarrow Y}[\max_x Pr[X = x|Y = y]]$ to compute the average min-entropy. Fig. 10 shows the (average-case) conditional min-entropy of generated keys indoor and outdoor. We can see the conditional min-entropy indoor and outdoor are at least greater than 0.83, and some of them approximate 0.95. Thus, the generated keys show satisfactory security against the eavesdropping of adversary Eve.

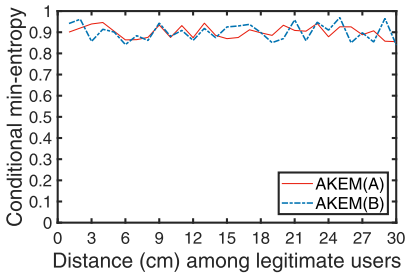


Fig. 10. Conditional min-entropy of generated keys.

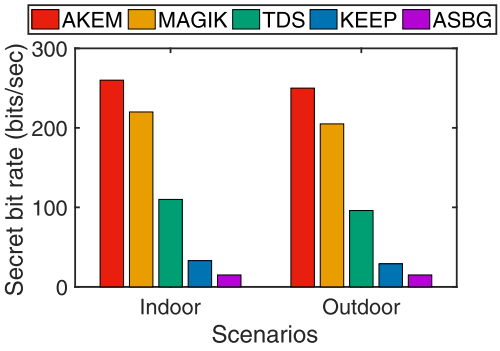


Fig. 11. Comparison with different approaches on secret bit rate.

I. Comparisons With Existing Key Generation Approaches

We compare AKEM with the state-of-the-art key generation approaches, i.e., MAGIK [33], TDS [23], KEEP [22], and ASBG [10]. MAGIK extracts secret key from dynamic geomagnetic field. TDS and KEEP use the fine-grained Channel State Information (CSI) recorded by CSI tool to extract secret key. ASBG extracts secret key from wireless signal strength in real environments. To align the baseline of comparison, we set appropriate parameters for these approaches. For MAGIK, we set the distance between legitimate users as 10 cm, and the sampling frequency as 50 Hz. For TDS, we set the block size β as 6, and the distance as 4 cm. For KEEP and ASBG, we set α and the fragment size as 0.35 and 50, respectively, to ensure a low bit mismatched ratio. For AKEM, we also set the distance as 10 cm, and the sensing frequency as 50 Hz. We compare them indoor and outdoor.

We compare the secret bit generation rate of different approaches in Fig. 11. It shows that AKEM has an obvious higher key generation rate than other approaches.

We also compare the entropy of different approaches in Fig. 12. The entropy can represent the randomness of the generated keys from the perspective of uncertainty. We can see that AKEM has pretty high entropy.

In summary, AKEM has a high key generation rate and great performance on the entropy.

VII. Discussion

To facilitate the comparison of AKEM under different conditions, we fix the mobile devices on a bracket in the experiments to conveniently adjust the distance among the

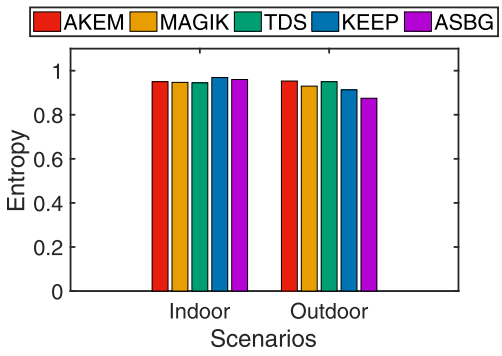


Fig. 12. Comparison with different approaches on entropy.

mobile devices and move them along the same trajectory. In practice, to generate the secret key, the users hold their own devices and move them together to sense the ambient light. Due to the differences in users' heights and moving pattern, their bit mismatch ratio may be higher than the case when the devices are fixed on the bracket. Thus, they may have a lower key generation efficiency in practice. To address this problem, we assume that one of the legitimate users holds all the mobile devices and moves the mobile devices together to sense the ambient light. Hence, all mobile devices are moved along the same trajectory, and the distances among them are almost 0 cm. In this scenario, AKEM can perform best. However, the prerequisite is that the users must trust each other and be willing to give their devices to another user. In the future work, we will study how to reduce the bit mismatch ratio without this prerequisite.

In our method, the participation of natural light sources or movement is necessary to resist against powerful attacks. Here we mainly consider a scenario, the attacker can be the maintenance or security personnel, who can control the lights and then tries to predict the secret key generated by legitimate users. It is obvious that the key generation is easily attacked when the distribution of light intensity is controlled. The participation of natural light source or movement makes the distribution of light intensity time-varying. Therefore, the attacker cannot control the light intensity sensed by users with the participation of natural light source or movement.

VIII. Related Work

We briefly review related works in this section.

There are many works for secret key generation. Hershey *et al.* first proposed to utilize the communication channel information to generate secret keys [13]. Subsequently, channel measurement based works have emerged in large numbers [9], [10], [14], [19], [42]–[54], including Arrive of Angle (AoA) [14], phase [42], [43], Received Signal Strength (RSS), etc [9], [10], [19], [44]. Channel State Information (CSI) and Channel Impulse Response (CIR) are also exploited as quantization signal sources [20]–[23], [55]–[58]. Xi *et al.* used the CSI to achieve key agreement among mobile devices [23]. However, they require the mobile devices provide the API for detailed channel measurement. Some researchers used acceleration and geomagnetic data of shaking process

to generate secret keys [33], [59], [60]. More specifically, Mayrhofer *et al.* used acceleration data of shaking process for secure device pairing and key generation [59], but they have limited applicability to practical scenarios due to low key generation rate.

There are some works using ambient light to authenticate legitimate users. Liu *et al.* used ambient light and sound for secure pairing [61]. LightTouch exploits visible light communication to secure RF channels [62]. But they still rely on Diffie-Hellman protocol, not the randomness from physical layer, to generate the secret key.

IX. Conclusion

In this paper, we have studied the problem of efficient secret key generation on commercial off-the-shelf mobile device. We have proposed a fast and robust key generation approach AKEM, which uses ambient light sensor data to generate secret key, securing wireless communication among legitimate users. We have carefully studied and validated the feasibility of using ambient light sensor data for key generation through extensive experiments. Compared with existing solutions for key establishment, AKEM mainly has two advantages: First, AKEM has a faster key generation rate. To generate a 256-bit cryptographic key, AKEM only needs one second; Second, AKEM can be implemented on commodity mobile devices without extra hardware. We also have implemented AKEM on smartphones and tablets. The results of experiments show the high efficiency and good robustness of AKEM.

Acknowledgment

The opinions, findings, conclusion, and recommendations expressed in this article are those of the authors and do not necessarily reflect the views of the funding agencies or the government.

References

[1] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1801–1819, 4th Quart., 2014.

[2] L. Militano, G. Araniti, M. Condoluci, I. Farris, and A. Iera, "Device-to-device communications for 5G Internet of Things," *EAI Endorsed Trans. Internet Things*, vol. 1, no. 1, pp. 1–15, Oct. 2015.

[3] P. Gandotra and R. K. Jha, "Device-to-Device communication in cellular networks: A survey," *J. Netw. Comput. Appl.*, vol. 71, pp. 99–117, Aug. 2016.

[4] Y. Zhang, E. Pan, L. Song, W. Saad, Z. Dawy, and Z. Han, "Social network aware Device-to-Device communication in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 177–190, Jan. 2015.

[5] M. Haris, H. Haddadi, and P. Hui, "Privacy leakage in mobile computing: Tools, methods, and characteristics," 2014, *arXiv:1410.4978*. [Online]. Available: http://arxiv.org/abs/1410.4978

[6] B. Krishnamurthy and C. E. Wills, "Privacy leakage in mobile online social networks," in *Proc. Wonference Online Social Netw.*, 2010, p. 4.

[7] P. Gandotra, R. K. Jha, and S. Jain, "A survey on device-to-device (D2D) communication: Architecture and security issues," *J. Netw. Comput. Appl.*, vol. 78, pp. 9–29, Jan. 2017.

[8] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "ProxiMate: Proximity-based secure pairing using ambient wireless signals," in *Proc. 9th Int. Conf. Mobile Syst., Appl., Services (MobiSys)*, 2011, pp. 211–224.

[9] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom)*, 2008, pp. 128–139.

[10] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, 2009, pp. 321–332.

[11] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[12] J.-F. Raymond and A. Stiglic. (Dec. 2000). *Security Issues in the Diffie–Hellman Key Agreement Protocol*. Accessed: Jun. 15, 2020. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.21.1971&rep=rep1&type=pdf

[13] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.

[14] T. Aono, K. Higuchi, M. Taromaru, T. Ohira, and H. Sasaoka, "Wireless secret key generation exploiting the reactance-domain scalar response of multipath fading channels: RSSI interleaving scheme," in *Proc. Eur. Conf. Wireless Technol.*, Oct. 2005, pp. 173–176.

[15] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 401–410.

[16] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1125–1133.

[17] M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani, "Context-based zero-interaction pairing and key evolution for advanced personal devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2014, pp. 880–891.

[18] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. Int. Conf. Comput. Commun. (INFOCOM)*, Mar. 2012, pp. 927–935.

[19] Z. Li, Q. Pei, I. Markwood, Y. Liu, and H. Zhu, "Secret key establishment via RSS trajectory matching between wearable devices," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 802–817, Mar. 2018.

[20] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.

[21] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. Int. Conf. Comput. Commun.*, Apr. 2013, pp. 3048–3056.

[22] W. Xi *et al.*, "KEEP: Fast secret key extraction protocol for D2D communication," in *Proc. IEEE 22nd Int. Symp. Qual. Service (IWQoS)*, May 2014, pp. 350–359.

[23] W. Xi *et al.*, "Instant and robust authentication and key agreement among mobile devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 616–627.

[24] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11 n traces with channel state information," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 1, p. 53, Jan. 2011.

[25] Y. Lu, F. Wu, S. Tang, L. Kong, and G. Chen, "FREE: A fast and robust key extraction mechanism via inaudible acoustic signal," in *Proc. 20th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Jul. 2019, pp. 311–320.

[26] M. Ibrahim *et al.*, "Verification: Accuracy evaluation of WiFi fine time measurements on an open platform," in *Proc. 24th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, 2018, pp. 417–427.

[27] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. Int. Conf. Comput. Commun.*, Apr. 2011, pp. 1422–1430.

[28] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Jan. 2008.

[29] S. N. Premnath *et al.*, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[30] D. I. Corporation. (Feb. 2012). *Al3006 Datasheet*. [Online]. Available: https://wenku.baidu.com/view/53adfe12866fb84ae45c8dd8.html

[31] Intersil. (2008). *Isl29009 Datasheet*. [Online]. Available: http://static6.arrow.com/aropdfconversion/23d75596f5467832449ac17191fde3544662abb/isl29009.pdf

[32] Broadcom. (Aug. 2016). *Apds-9922-001 Datasheet*. [Online]. Available: https://www.mouser.com/datasheet/2/678/APDS-9922-001-DS102-1501431.pdf

[33] F. Qiu, Z. He, L. Kong, and F. Wu, "MAGIK: An efficient key extraction mechanism based on dynamic geomagnetic field," in *Proc. INFOCOM-IEEE Conf. Comput. Commun.*, May 2017, pp. 1–9.

[34] C. Zenger, J. Zimmer, J.-F. Posielek, and C. Paar, "On-line entropy estimation for secure information reconciliation," in *Proc. 12th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services (MobiQuitous)*, 2015, pp. 254–259.

[35] C. Zenger, J. Zimmer, and C. Paar, "Security analysis of quantization schemes for channel-based key extraction," in *Proc. 12th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services (MobiQuitous)*, 2015, pp. 267–272.

[36] K. Moara-Nkwe, Q. Shi, G. M. Lee, and M. H. Eiza, "A novel physical layer secure key generation and refreshment scheme for wireless sensor networks," *IEEE Access*, vol. 6, pp. 11374–11387, 2018.

[37] A. Soni, R. Upadhyay, and A. Kumar, "Wireless physical layer key generation with improved bit disagreement for the Internet of Things using moving window averaging," *Phys. Commun.*, vol. 33, pp. 249–258, Apr. 2019.

[38] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Heidelberg, Germany: Springer, 2004, pp. 523–540.

[39] M. Edman, A. Kiayias, Q. Tang, and B. Yener, "On the security of key extraction from measuring physical quantities," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1796–1806, Aug. 2016.

[40] C. T. Zenger, M. Pietersz, J. Zimmer, J.-F. Posielek, T. Lenze, and C. Paar, "Authenticated key establishment for low-resource devices exploiting correlated random channels," *Comput. Netw.*, vol. 109, pp. 105–123, Nov. 2016.

[41] C. Chen and H. Yang, "Shared secret key generation from signal fading in a turbulent optical wireless channel using common-transverse-spatial-mode coupling," *Opt. Express*, vol. 26, no. 13, pp. 16422–16441, 2018.

[42] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2008, pp. 3013–3016.

[43] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.

[44] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2763–2776, Dec. 2014.

[45] J. Zhang, S. K. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–5.

[46] A. Ambekar, M. Hassan, and H. D. Schotten, "Improving channel reciprocity for effective key management systems," in *Proc. Int. Symp. Signals, Syst., Electron. (ISSSE)*, Oct. 2012, pp. 1–4.

[47] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "SmokeGrenade: An efficient key generation protocol with artificial interference," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1731–1745, Nov. 2013.

[48] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Extracting secret key from wireless link dynamics in vehicular environments," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2283–2291.

[49] X. He, H. Dai, Y. Huang, D. Wang, W. Shen, and P. Ning, "The security of link signature: A view from channel models," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2014, pp. 103–108.

[50] S. Sun, Y. Wu, B. S. Lim, and H. D. Nguyen, "A high bit-rate shared key generator with time-frequency features of wireless channels," in *Proc. GLOBECOM-IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–6.

[51] X. Wang, Y. Hou, X. Huang, D. Li, X. Tao, and J. Xu, "Security analysis of key extraction from physical measurements with multiple adversaries," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2018, pp. 1–6.

[52] X. Li, M. Wang, H. Wang, Y. Yu, and C. Qian, "Toward secure and efficient communication for the Internet of Things," *IEEE/ACM Trans. Netw.*, vol. 27, no. 2, pp. 621–634, Apr. 2019.

[53] W. Xu, S. Jha, and W. Hu, "Exploring the feasibility of physical layer key generation for LoRaWAN," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 231–236.

[54] M. Cao, D. Chen, Z. Yuan, Z. Qin, and C. Lou, "A lightweight key distribution scheme for secure D2D communication," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, Jun. 2018, pp. 1–8.

[55] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, no. 2, pp. 52–55, Feb. 2000.

[56] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Secure key generation from OFDM subcarriers' channel responses," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2014, pp. 1302–1307.

[57] F. Marino, E. Paolini, and M. Chiani, "Secret key extraction from a UWB channel: Analysis in a real environment," in *Proc. IEEE Int. Conf. Ultra-WideBand (ICUWB)*, Sep. 2014, pp. 80–85.

[58] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "Verification of key generation from individual OFDM subcarrier's channel response," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2015, pp. 1–6.

[59] D. Bichler, G. Stromberg, M. Huemer, and M. Löw, "Key generation based on acceleration data of shaking processes," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput. (UbiComp)*, 2007, pp. 304–317.

[60] R. Mayrhofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices," *IEEE Trans. Mobile Comput.*, vol. 8, no. 6, pp. 792–806, Jun. 2009.

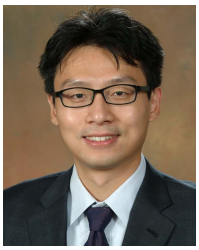
[61] D. Liu, J. Chen, Q. Deng, A. Konate, and Z. Tian, "Secure pairing with wearable devices by using ambient sound and light," *Wuhan Univ. J. Natural Sci.*, vol. 22, no. 4, pp. 329–336, Aug. 2017.

[62] X. Liang, T. Yun, R. Peterson, and D. Kotz, "LightTouch: Securely connecting wearables to ambient displays with user intent," in *Proc. IEEE INFOCOM-IEEE Conf. Comput. Commun.*, May 2017, pp. 1–9.

Youjing Lu (Graduate Student Member, IEEE) received the B.S. degree in information security from Anhui University in 2016. She is currently pursuing the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. Her research interests include key extraction, mobile sensing, and network traffic analysis.

Fan Wu (Member, IEEE) received the B.S. degree in computer science from Nanjing University in 2004 and the Ph.D. degree in computer science and engineering from the State University of New York at Buffalo in 2009. He has visited the University of Illinois at Urbana–Champaign (UIUC) as a Post-Doctoral Research Associate. He is currently a Professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University. His research interests include wireless networking and mobile computing, algorithmic game theory and its applications, and privacy preservation. He has published more than 150 peer-reviewed papers in technical journals and conference proceedings. He was a member of technical program committees of more than 90 academic conferences. He was a recipient of the first class prize for the Natural Science Award of China Ministry of Education, the NSFC Excellent Young Scholars Program, the ACM China Rising Star Award, the CCF-Tencent Rhinoceros bird Outstanding Award, and the CCF-Intel Young Faculty Researcher Program Award. He has served as an Associate Editor for the IEEE TRANSACTIONS ON MOBILE COMPUTING and an Area Editor for *Computer Networks*.

Qianyi Huang received the bachelor's degree from Shanghai Jiao Tong University and the Ph.D. degree from the Department of Computer Science and Engineering, Hong Kong University of Science and Technology. She is currently a Research Assistant Professor with Southern University of Science and Technology. Her research interests include ubiquitous communication and sensing in the Internet-of-Things and IoT security.



Shaojie Tang (Member, IEEE) received the Ph.D. degree in computer science from the Illinois Institute of Technology in 2012. He is currently an Assistant Professor with the Naveen Jindal School of Management, The University of Texas at Dallas. His research interests include social networks, mobile commerce, game theory, e-business, and optimization. He received the Best Paper awards in ACM MobiHoc 2014 and the IEEE MASS 2013. He also received the ACM SIGMobile Service Award in 2014. He served in various positions (as chairs and TPC members) at numerous conferences, including ACM MobiHoc and IEEE ICNP. He is an Editor of *Information Processing in the Agriculture* (Elsevier) and the *International Journal of Distributed Sensor Networks*.

Guihai Chen (Senior Member, IEEE) received the B.S. degree from Nanjing University in 1984, the M.E. degree from Southeast University in 1987, and the Ph.D. degree from the University of Hong Kong in 1997. He had been invited as a Visiting Professor by many universities, including the Kyushu Institute of Technology, Japan, in 1998, the University of Queensland, Australia, in 2000, and Wayne State University, USA, from September 2001 to August 2003. He is currently a Distinguished Professor with Shanghai Jiao Tong University, China. He has a wide range of research interests with focus on sensor network, peer-to-peer computing, high-performance computer architecture and combinatorics. He has published more than 200 peer-reviewed articles, and more than 120 of them are in well-archived international journals, such as the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, the *Journal of Parallel and Distributed Computing*, *Wireless Network*, *The Computer Journal*, the *International Journal of Foundations of Computer Science*, and *Performance Evaluation*, and also in well-known conference proceedings, such as HPCA, MOBIHOC, INFOCOM, ICNP, ICPP, IPDPS, and ICDCS.