# Secret from Muscle: Enabling Secure Paring with Electromyography


## Abstract

Forming secure pairing between wearable devices has become an important problem in many scenarios, such as mobile payment, private data transmission. This paper presents EMG-KEY, a system that can securely pair wearable devices by leveraging the electrical activity caused by human muscle contraction, that is, Electromyogram (EMG), to generate the secret key. Such a key can then be used by devices to authenticate each other's physical proximity and communicate confidentially. Extensive evaluation on 10 volunteers under different scenarios demonstrates that our system can achieve a competitive bit generation rate of 5.51 bit/s while maintaining a success matching rate of 88.84%. Also, the evaluation results with the presence of adversaries demonstrate our system is secure to strong attackers who can eavesdrop proximate wireless communication, capture and imitate the users' paring process with the help of camera.


## 1 Introduction

Nowadays we are witnessing the fast development of wearable devices. Such rapid growth leads to a prevalence of direct communications between devices in proximity and innovated many promising applications, such as: mobile payment, which enables users to make a purchase by interacting their mobile devices or smart watches with an electronic payment device [1]; Private data transfer implemented on many smart wristbands, *e.g.*, fitbit [5], can directly transmit user's biological data to authenticated mobile device or data collection hub in proximity. Along with the wide adoption of these applications are not only the convenience and fantastic use experience, but also an increasing concern about privacy and security, as the data transmitted is often highly sensitive and private. As a result, establishing a secure pairing becomes an important problem for wearable devices.

As wearable devices are often lack of convenient input method and have limited resources, researchers have proposed many novel systems to serve as alternatives of traditional PIN-code-based and cryptographic-based approaches. In these works, the vital part of creating a secure paring between devices is to ensure both devices obtain consistent and secret observations from an information source, which make them reach an agreement on same secret key. Such secret source can be the wireless channel measurement [14,26,31,35,42], human movements like gesture [11], or shaking trajectory [36], or ambient environment, *e.g.*, ratio [34], sound [45], or vibration [9]. However, since the characteristics and randomness of the secret source directly determine the robustness of secure pairing schemes, existing works still expose some disadvantages when facing strong attackers. Due the sharing nature of wireless medium, secure pairing schemes based on wireless channel measurement [14, 26, 31, 35, 42] are vulnerable to predictable channel attack, in which malicious adversary can use different methods, *e.g.*, block the Line-of-Sight (LOS) radio propagation between devices, to cause predictable variations in the wireless channel measurement. The secret key generated by movement-based approaches [11,36] can be inferred if the movement is captured by a camera and the ambient-environment-based works [9, 45] are threated by the eavesdropper and active attacker who can intentionally controls the ambient environment by making predefined noises or vibrations.

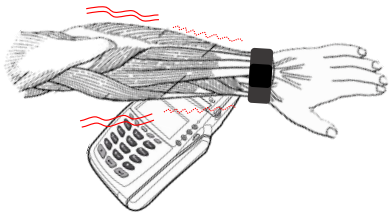


**Figure 1. Example application of EMG-KEY on Mobile Payment.**

The security limitations of the aforementioned techniques motivate us to design a more secure pairing system using the intrinsic signals residing inside human body, *i.e.*, the electric activity caused by human muscle contraction. The key insight is that, to perform human body movement, our central nerve system will send electrical signals to cause corre-

sponding muscle contraction. Such electrical signal propagates along with muscle fibers and can be captured by electrodes placed on the skin. The recorded signal is termed as *Electromyogram* (EMG), which has several promising characteristics. (i) Medical studies [22, 37] have proved that the EMG signal is a quasi-random process. This means the value of EMG will be statistically larger if we intent to generate stronger force, but the amplitude variation of EMG under a given force value is stochastic in nature. As a result, even if the gesture is imitated and the corresponding output force is estimated, the variation of EMG amplitude is still unable to be determined. (ii) The current volume and propagation area of EMG are quite subtle, only physical contact in proximity can sense the signal [22], which means the eavesdropping without contacting would be extremely hard, if not impossible. (iii) Fueled by the development of new human-machine interaction technologies, EMG sensor is increasingly adopted by many commercial wearable devices, *e.g.*, Myo armband [7], Athos gear [3], and Leo smart band [6]. These facts suggest that EMG signal can be leveraged as a secure source to generate secret key. Such key can be used by wearable devices to authenticate each other's physical proximity and then to communicate confidentially.

Inspired by this idea, we propose EMG-KEY, a system that securely pairs two wearable devices by using the EMG variation caused by human body movement, *e.g.*, hand gesture, as the secret source to generate cryptographic key. Our system consists of a smart wristband and a smart device equipped with EMG sensors. By physically contacting these devices to human body and perform an arbitrary gesture, EMG-KEY can generate secret keys from the captured EMG signals and use them to create a secure communication channel between devices. A typical application of EMG-KEY is the mobile payment, in which the transaction data is very sensitive and requires high security level. As shown in Figure 1, a user touches the payment device with his arm wearing the smart wristband, then he can make an arbitrary gesture, *e.g.*, clench the fist. The EMG signal caused by this gesture will be recorded by the EMG sensors embedded in the smart wristband and payment device. Then, both devices use the captured EMG signal to generate secret key. As both of their measurements are from the same source, they can reach consensus on the same secret key at high success rate while attackers have no clue about the secret key.

To realize such system, there are several challenges: First, it is not clear whether the randomness in EMG variation is sufficient to generate robust secret key. To answer this question, we formulate the generation of EMG as a random process model and gain several insights from theoretical study and empirical experiments on volunteers. Another challenge stems from the design of secret key extraction: although both devices involved in pairing are measuring EMG from the same source, there are still some inconsistency of the captured signals due to the different install locations, electrode attenuation, and hardware imperfection. To address this issue, we design a secret key generation algorithm based on the temporal variation shapes of EMG signal and leverage error correction coding [19] to alleviate the discrepancy. Extensive experimental results have confirmed the effectiveness and efficiency of our algorithm.

Our contributions in this work lay in the following aspects:

- As far as we know, we are the first to explore the possibility of using EMG to enable secure pairing for wearable devices. We have demonstrated that EMG is a good information source to build a secure pairing system due to its physical characteristics and stochastic nature.
- We propose EMG-KEY, a secure paring system for wearable devices, that can defend against many strong attackers and provides high security. In this system, we design and implement secret key generation algorithm based on the temporal shape variations of EMG signal and alleviate the inconsistency via error correcting coding.
- We comprehensively evaluate the performance of our system under different scenarios with 10 volunteers. The results indicate that our system can archive a high bit rate at 5.51 bit/s while maintaining a successful pairing rate of 88.84%. Also, the evaluation results with the presence of adversaries demonstrate our system is secure to strong attackers who can eavesdrop proximate wireless communication, capture and imitate the users' paring process with the help of camera.

The rest of paper is organized as follows. We first briefly introduce the preliminary of EMG and investigate its feasibility as a secret source, then define the threat model in Section 2. The system design and detailed implementation are discussed in Section 3. In Section 4, we describe our experimental methodology and evaluation metrics. Then, we present the performance of our secret key generation and resistance to attacks in Section 5 and Section 6. The discussion and related work are provided in Section 7 and Section 8, followed by a conclusion in Section 9.

## 2 Feasibility & Threat Model

In this section, we start with a brief introduction of EMG, and then formulate its generation as a random process model. From this model, we can theoretically verify that the randomness of EMG is sufficient for secure pairing. Apart from this, we also conduct empirical experiment on volunteers to demonstrate the feasibility of our system. After that, we discuss our target scenario and define the attack model.

### 2.1 Preliminary

The generation of physical movement in human body involves the activation of skeletal muscles [37]. As showed in Figure 2, skeletal muscle consists of dozens of elongated, cylindrical cells known as *muscle fibers*, which are attached to the bones of skeletons via tendons. Each muscle fiber is innervated by a moto-neurons and the contact region is termed as the *neuromuscular junction*, in which each axon lies in a groove on the surface of the muscle fiber called *motor endplate*. The moto-neuron and the set of muscle fibers it innervates compose the basic function unit of muscle, *i.e.*, *motor unit* (MU).

It is through the contraction of muscle fibers that we form the movement. It starts with an electrical excitation sent from our nerve system to the muscle fibers which activates the

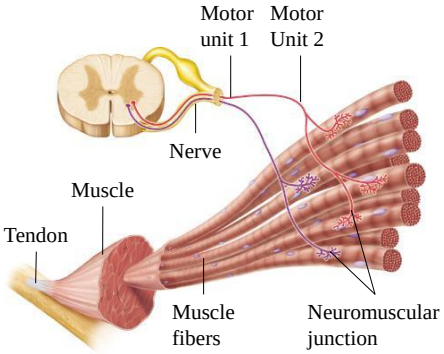



**Figure 2. Anatomy of Muscle [33].**

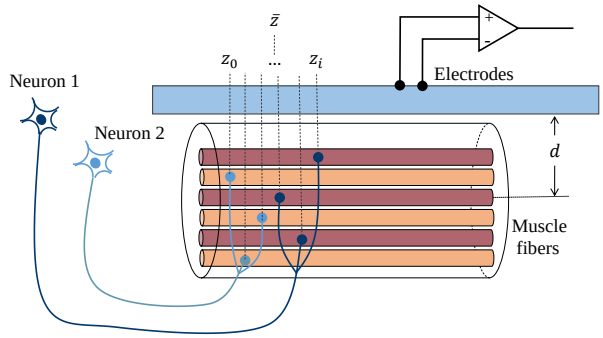



**Figure 3. EMG modeling.**

acetylcholine-gated channel in the end-plate and allows large amount of positive sodium to flow into the muscle fiber [15]. This positive influx causes the local depolarization of the fiber membrane and initiates the *muscle fiber action potential*. Such action potential spreads along the muscle fibers innervated by this moto-neuron and results in their contraction. The frequency at which the muscle fibers are stimulated by their innervating axon is called the *motor unit firing rate* and multiple motor units will be recruited during a movement to meet requirement of output force.

By placing electrodes on the skin around the contracting muscle, the electrical activity during muscle contraction can be captured and the recorded data is the surface EMG signal.

## 2.2 EMG Modeling

As a complicated biological process, EMG begins with the nerve impulse sent from moto-neuron, which spreads over end-plates and yields the muscle fiber action potential. The action potential propagates along fibers and tissues, and eventually captured by electrodes on the skin. To quantify this process, let us consider an example showed in Figure 3, in which a set of muscle fibers are innervated by two moto-neurons. The contact regions where the axons of neurons meet muscle fiber are labeled as $z_0, \ldots, z_i$, and the mean is $z_m$. Let $d$ be the average distance between the muscle and skin is defined a $d$, and $w$ is the spacing between electrodes.

When a motor unit is recruited, the moto-neuron sends excitation impulse to initiate the muscle fiber action potential. It is evidenced [37] that the firing pattern of moto-neuron is quasi-random, *i.e.*, the average firing rate grows with the increasing force requirement, but the occurrence of each impulse is stochastic in nature; Moreover, the firing patterns of different motor units are essentially independent [22]. Let random function $R_q(t)$ describe the firing pattern of the $q$-th motor unit. Then, the overall firing pattern of motor units recruited is:

$$R(t) = \sum_{q=1}^{Q} R_q(t) \tag{1}$$

When the nerve impulse arrives the muscle fiber, it causes the depolarization of the fiber membrane and generates the muscle fiber action potential. This action potential propagates from end-plates to electrodes at a conduction velocity $u$ and can be described as:

$$p(t) = Aut(2-ut)e^{-ut}, \tag{2}$$

where $A$ is a scale factor and $u$ is the conduction velocity, both of which are determined by fiber membrane properties.

However, one may notice that the geographic distribution of end-plates, *i.e.*, the starting point of the action potential propagation, are quite different. This can be viewed as time shift from $z_m$ and described by the convolution of delta shift function:

$$D(t) = \sum_{m=1}^{M} \delta(t-\tau_m), \tag{3}$$

where $\tau_m = \frac{z_m - \bar{z}}{u}$ is the time shift caused by the distance between $z_m$ and $\bar{z}$.

Combining these factors together, we can quantify the EMG generation using the following model:

$$\begin{aligned} EMG(t) &= \sum_{q=1}^{Q} \left\{ R_q(t) * D_q(t) * p(t) * e(t) \right\} \\ &= \sum_{q=1}^{Q} \left\{ R_q(t) * \left[ \sum_{m=1}^{M_q} \delta(t-\tau_m) * p(t) \right] * e(t) \right\}, \end{aligned} \tag{4}$$

where $Q$ is the number of motor units which are recruited in contraction, $M_q$ is the number of muscle fibers innervated by $q$-th motor unit. The $e(t)$ is the transfer function of electrodes, which is defined by the electronic properties of electrodes and its relative location with respect to muscle.

From this model, we can gain several useful insights:

- To generate a movement, it often requires multiple motor units to be involved. However, the number of recruited motor units $Q$ is determined by the force requirement. Thus, even under the same movement, the number of recruited motor units can be different.
- Even the gesture can be captured by camera and the output force might be inferred, the attacker still is agnostic about user's EMG signal due to the stochastic nature of firing patterns of motor units.
- The personal difference in the end-plate distribution, conduction velocity of muscle fiber membrane and even

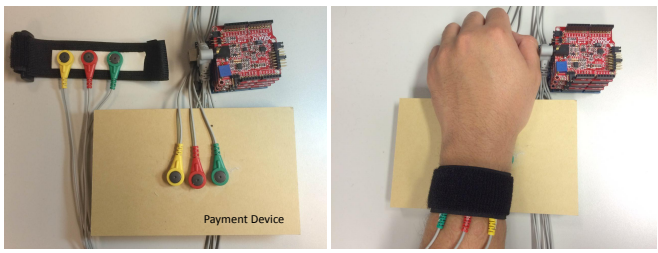



**Figure 4. Prototype of EMG-KEY, which consists of a wristband and payment device, both of which are equipped with Olimex EMG sensors and controlled by Arduino UNO board.**

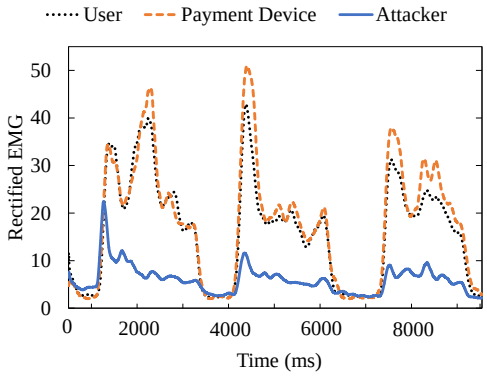



**Figure 5. Rectified EMG signals from user, payment device, and attacker.**

muscle fatigue level also introduce additional discrepancies between the EMG signal generated users and attackers.

Apart from these observations, we also find the current volume of EMG signal is quite small (around $\pm 1.5mv$), and propagation area is limited to the skin above contracting muscles, which implies eavesdropping without physically contacting in close proximity is extremely hard. All of these observations suggest that EMG could be a good randomness source to generate secret key.

## 2.3 EMG as Secret Source

To validate the feasibility of using EMG to generate secret key, we build a prototype based on Arduino UNO development board [2] and Olimex EMG shield [8]. As showed in Figure 4, the prototype consists of a wristband and a payment device, both of which are equipped with Olimex EMG sensors.

Similar to the mobile payment scenario, we ask a volunteer $A$ to wear our wristband, and put his hand on the payment machine. Meanwhile, there is another volunteer $E$ acting as the attacker, who is also wearing the same type of wristband and can observe every gesture made by user $A$. To simulate the worst case, both user and attacker are required to perform an easy-to-imitate gesture, *i.e.*, slowly clutch their fist and then release it, and repeat it for 3 times.

Figure 5 gives an example of the rectified EMG signal (for the details of rectification, see Section 3) obtained from wristbands of user $A$ and attacker $E$, and the payment device $B$. The pairwise Pearson correlation coefficients are also present in Table 1. We can notice some interesting observations: (i) For the same person, even he is making the same gesture, the EMG measurement can be different for each time; (ii) Although it does exists some slight differences, the EMG signals recorded from user $A$'s wristband and payment device are highly simimar in their variation shapes and strongly correlated, evidenced by a correlation coefficient of 0.98. (iii) The correlation between attacker and legitimate devices are not minor (around 0.69). Such correlation derives from the fact that the attack can clearly observe the gesture and easily imitate it. As the EMG amplitude is a quasi-random process with respect to output force, the general rise and drop trend at the begin and end of gesture can be easily imitated, but it fails on the matching of the small scale variation during the gesture.

**Table 1. Pearson correlation coefficient among user $A$, payment device $B$ and attacker $E$**

| corr(A, B) | corr(A, E) | corr(B, E) |
|---|---|---|
| 0.98 | 0.69 | 0.66 |

These observation corresponds to our insights from EMG modeling in Section 2.2, which provides additional support for the feasibility of using EMG signal as secret source.

## 2.4 Threat Model

In our scenario, two legitimate devices, both of which does not have priori about each other, would like to communicate confidentially. We assume both devices are equipped with EMG sensors. To associate them successfully, the user need to put them close (around 4 cm) above the acting muscle and physically contact with the skin.

For the threat model, we assume there exists a powerful attacker, who know the exact details of our system and can observe all the gestures made by user, or even use camera to capture it for further analysis. Besides, he can imitate the same gesture as user's. Moreover, all the packets transmitted through the wireless channel can be eavesdropped by the attacker.

In such a threat model, the attacker can first record the user's gesture and wait until the successful association between legitimate devices, then starts to eavesdrop and save all the traffic transmitted through this communication link. After that, he can imitate user's gesture and use the same secret key generation algorithm to produce a secret key, and then try to use such key to decode the encrypted packets. We term such an attack as *copy attack*.

# 3 System Design

In this section, we present the design of EMG-KEY in detail. We start with the rectification process and noise removal of raw EMG signal, introduce the secret key generation, and then move to the discussion on how to alleviate the discrepancies caused by electrodes transfer function and hardware imperfection. The Figure 6 provides an overview of our system.

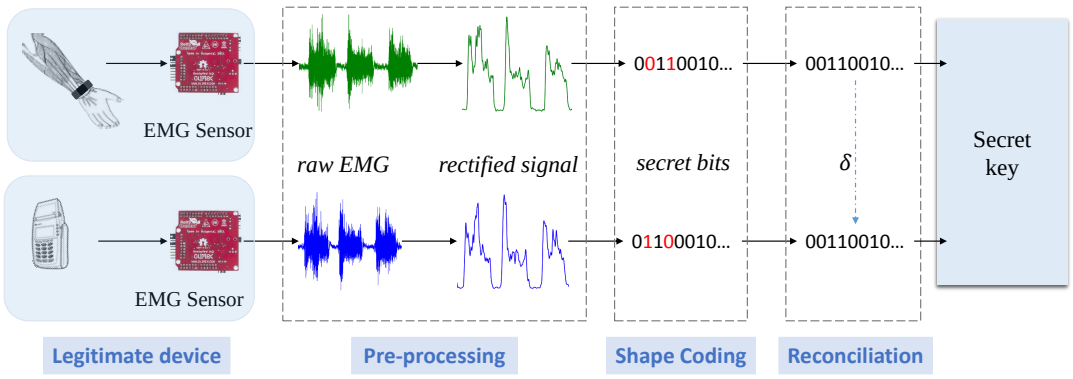



**Figure 6. Overview of EMG-KEY.**

## 3.1 Pre-processing

As discussed in Section 2.1, the EMG signal can be modeled as the convolution result of firing pattern of motor-neurons, distribution of end-plates, muscle fiber action potential and electrode transfer function. To magnify the effect of neuron firing pattern, rectification is a common applied approach [22]. The Root-Mean-Square-based rectification of EMG signal $x(t)$, is defined as:

$$EMG_{rect}(t) = \sqrt{\left[\frac{1}{T}\int_{t-T}^{T} x^2(\tau)d\tau\right]}, \quad (5)$$

where $T$ is the window size which controls the trade-off between smooth envelope against transient variations of EMG signal. In our system, we set this value to be 0.8 seconds.

Also, during the recording of EMG, there are many sources of noise and interference, such as the electrical noise caused by the friction between electrodes and skin, or the power line interference. We notice that the most energy of noise are either less that 10 Hz (friction noise) or concentrate around 50 Hz (power line interference, the frequency of which can be different among countries). Besides, the majority of arm EMG is above 20 Hz [15]. Thus, a high-pass filter with cut-off frequency of 15 Hz and a notch filter implemented based on Chebyshev IIR filter are adopted to alleviate the interference of these noises . Figure 7(a) and 7(b) show an example of raw EMG and corresponding rectified signal.

By applying the rectification and filtering on raw EMG measurement, we can obtain the rectified EMG. In what follows, we demonstrate how to generate secret key based on it.

## 3.2 Secret Key Generation

The goal of secret key generation scheme is to fully exploit the randomness of EMG signal and encode into secret bits as high rate as possible. To this end, a commonly-used approach is to divide the EMG signal into segments, and then encode the signal by quantizing the segment amplitude into several levels. Such a method can preserve most information of the signal, while it may also introduces many additional mismatched bits, as we can observe in Figure 5 that the signal amplitudes of legitimate devices are not exactly coincident.

Apart from the differences existed in EMG amplitude, we also notice that, compared with amplitude volume, the variation trends of legitimate devices are highly correlated. Moreover, the variation shapes of attacker's EMG are significantly different from the legitimate devices. Thus, we choose to encoding the EMG signal by using their variation shapes.

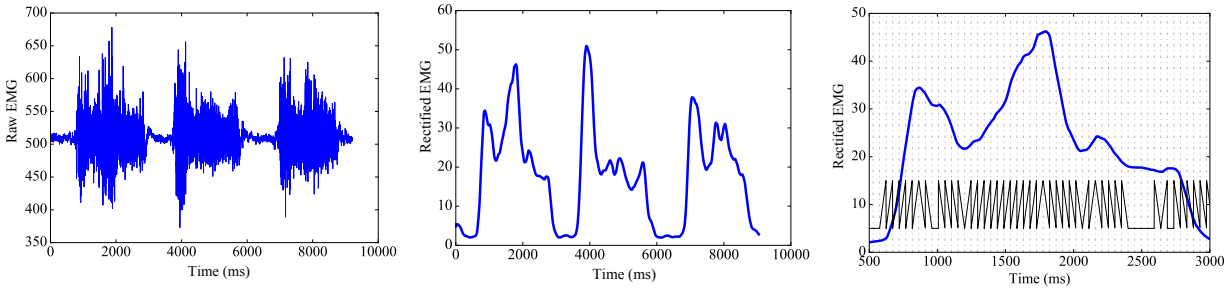
Our encoding algorithm is consists of three steps: First, divide the rectified EMG $S$ into small segments of size $w$. For each segment, we define three templates of variation shapes, *i.e.*, *rise*, *drop* and *stay* according to their amplitude variation. After that, we use Fast Dynamic Time Warping [28] to compute the distance between segment and shape templates and find out its most-matching shape. Then, we use the binary representation of corresponding shape ID as the *secret key*. Algorithm 1 elaborates this process.

**Algorithm 1** Shape-based Secret Key Generation.

**Input:**
Rectified EMG signal $S$, coding window $w$
**Output:**
Secret bit list $L = [c_0, c_1, ..., c_n]$

$ind \leftarrow 0$
**while** $ind + w < size(S)$ **do**
  $s = S[ind : ind + w]$
  $rise = [min(s) + i * d/w$ for $i$ in $0 : w]$
  $drop = [max(s) - i * d/w$ for $i$ in $0 : w]$
  $stay = [\frac{max(s)-min(s)}{2}$ for $i$ in $0 : w]$
  template list $T \leftarrow [rise, drop, stay]$
  $dis \leftarrow \infty, c \leftarrow NULL$
  **while** $tid < size(T)$ **do**
    $d = fastDTW(s, T[tid])$.
    **if** $d < dis$ **then**
      $c \leftarrow toBinary(tid)$
      $dis \leftarrow d$
    **end if**
  **end while**
  $L \leftarrow c$
**end while**
**return** $L$

Let $V$ be the number of possible variation shapes. Since we translate the shape code obtained from each segment into




(a) Raw EMG (b) Rectified EMG (c) Close-up of shape-based encoding

**Figure 7. Flow of EMG-KEY.**

two-bit binary code, the rate of secret bit generation can be computed as:

$$\text{bit rate} = \frac{1}{w}\log_2 V, \tag{6}$$

where $V = 3$ in our case, *i.e.*, $tid = \{0,1,2\}$.

An example result of the shape-based encoding algorithm is presented in Figure 7(c), in which the blue line is the rectified EMG signal and the black line within each coding window is the approximated shape of this segment.

### 3.3 Reconciliation

After the secret key generation, each device ends up with an $n$-bit secret key independently. However, due to the space between the devices and imperfection in electrodes' properties, *e.g.*, signal amplification gain and resistance to noise, the transfer function $p(t)$ of each EMG sensor can be different. As a result, there are still some discrepancies in the EMG variation shapes which inevitably leads to mismatching bits among the secret keys.

The purpose of reconciliation is to alleviate the mismatching of the secret keys between legitimate devices. The rationale is that, the secret keys of legitimate devices can be viewed as two different distorted versions of the same signal as both of them are derived from the same EMG source. By employing the error correction coding [19], the number of the mismatching bits can be reduced.

Specifically, given two legitimate devices $A$ and $B$, the secret keys they obtained from secret key generation are $k_a$ and $k_b$, the mismatching bits between which are defined as $\varepsilon$. Let $C(n,k)$ be an Error Correction code (ECC) that encodes $k$-bit message into $n$-bit code to resist $r$-bit random error. Function $f(\cdot)$ and $g(\cdot)$ are the corresponding encoding function and decoding function. To perform the reconciliation, device $A$ first computes the offset $\delta$ between $k_a$ and its corresponding codeword:

$$\delta = k_a \oplus f\big(g(k_a)\big), \tag{7}$$

Then, device $A$ transmits this offset data to device $B$ via a public communication link, *e.g.*, WiFi or bluetooth. Once device B receives the $delta$, it can deduce $k_a$ as follows:

$$k_a\prime = \delta \oplus f\big(g(k_b \oplus \delta)\big), \tag{8}$$

If the mismatching rate $\varepsilon$ can be roughly estimated, an appropriate error correction code $C$ can be leveraged to ensure $k_a\prime$ equals to $k_a$ with a high probability.

We understand this process not only reduces the mismatching bits between the secret keys of legitimate devices, but also leaks a partial information about the secret key, as the $\delta$ is transmitted over a public communication link and may be eavesdropped by attacker. However, it can be theoretical proved that there are only $(n-k)$ bits of information leakage [34]. Moreover, since the secret key during is derived from the random variation of EMG signal, the offset information $\delta$ in each pairing procedure varies independently. Therefore, the attacker still cannot infer $k_a$ by observing $\delta$. To ensure that no partial information leakage, we can further reduce every $n$-bit secret sequence to $k$-bit sequence, *e.g.*, use $g(k_a)$ as the secret key instead of $k_a$. As a result, after the reconciliation, the valid bit generation rate will be reduced by a factor of $\frac{n-k}{n}$.

In our implementation of EMG-KEY, we employ the binary Golay Code $G(23,12)$ [19] in the reconciliation stage. It is a perfect linear error-correction code, which encodes 12-bit of data into a 23-bit word and can detect any 7-bit errors or correct any 3-bit errors in each 23-bit block.

## 4 Experimental Methodology

**Experiment Setup:** In our experiment, we build up a prototype of EMG-KEY as shown in Figure 4. It includes a wristband and a device that acts as the payment device, both of which are embedded with Olimex EMG/EKG sensor [8] with a sampling frequency at 250 Hz controlled by Arduino UNO develop board [2]. Based on this prototype, we have implemented the shape-based secret key generation scheme in Python 2.7 and performed the reconciliation via Golay Code $G_{23}(23,12)$.

**Testing Scenario:** To conduct comprehensive evaluation, we have recruited 10 volunteers (7 males and 3 females) to conduct extensive experiments: Nine of them act as normal users while one simulates the attacker. In each experiment, the user is required to wear the wristband on his/her arm, physically contact with the electrodes on the payment device in proximity (around 4 cm) as showed in Figure 4, and then perform a gesture to initiate a secure pairing. During this process, an attacker who wears the same type of wristband is standing nearby in such way that he can clearly observe the gestures, and exactly imitate them. To simulate the worst case in real application, we intentionally ask users to perform simple gestures which are easy to be imitated, *e.g.*, slowly clutch then release fist. We evaluate the information leakage

during the reconciliation process by letting the attacker know the exact offset data between legitimate devices during each pairing process. All the the EMG signals measured from devices, and corresponding secret keys generated during these experiments are recorded for further analysis. Since we perform 10 experiments on each user, there are $30 \times 10 = 300$ data in total.

**Performance Metrics:** Throughout the evaluation, four metrics are employed to measure the performance of our system.

- *Bit generation rate* is the number of valid secret bits we can generate per second. A higher bit generation rate implies a shorter pairing procedure and thus provides a better user experience. In our system, the bit generation rate is directly determined by the lenthg of EMG segment $w$, the number of predefined variation shapes $V$ and the choice of error correction code $n,k$:

$$BGR = \frac{k}{wn}\log_2 V, \tag{9}$$

  where $V = 3$ in our case.

- *Bit Mismatching rate* reflects the level of inconsistency between secret keys. It is defined as the number of mismatched bits divided by the length of secret key:

$$BMR = \frac{bitcount(k_a \neq k_b)}{min(|k_a|,|k_b|)}. \tag{10}$$

  A low bit mismatching rate ensures the legitimate devices to agree on the same secret key and pair successfully at high possibility. In our system, some factors can obviously affect the bit mismatching rate, *e.g.*, the distance between devices, the choice of error correction code, and even the complexity of gesture.

- *Entropy* is a measurement of information contained in a data [20]. Given a random variable $X = [x_0, x_1, ..., x_i]$, its entropy can be computed as:

$$H(X) = -\sum_i Pr[x_i]\log_2 Pr[x_i], \tag{11}$$

  where $Pr[x_i]$ is the probability of $i$-th value of $X$. In our case, we use the segment-wise entropy to measure the randomness information contained in secret key by counting the frequencies of different variation shapes.

- *Mutual information* measures the mutual dependence between two variables [20], which quantifies the amount of information obtained about one random variable $X$ through the another variable $Y$ as:

$$I(X;Y) = \sum_{y\in Y}\sum_{x\in X} p(x,y)\log\frac{p(x,y)}{p(x)p(y)}. \tag{12}$$

  In our evaluation, we use this metric to measure the information leakage between user and attacker. If the mutual information between $X$ and $Y$ is zero, then it means we can not gain any information about $Y$ by only observing $X$, or *vice versa*.

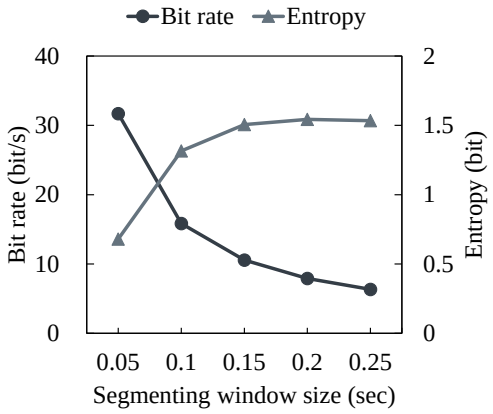



**Figure 8. The bit rate before reconciliation. A small coding windows size results in high bit rate, but reduces the information contained in the generated key.**

# 5 Performance of Secret Key Generation

This section evaluates the performance of our secret key generation scheme.

We begin with the examination on the choice of coding windows size and error correction code, which directly determine the bit generation rate and bit mismatching rate of our system. According to the result, our system can generate secret bits at a rate of 5.51 bit/s, while retains a low bit mismatching rate by employing Golay Code in the reconciliation stage.

After that, we move to the investigation on the impact of confounding factors, namely, the distance between devices, the placement of electrodes and the gesture complexity. The evaluation results demonstrate that, by placing the devices within 4 centimeters, our system can provide a good performance with a simple gesture and is robust to the electrode placement.

## 5.1 Effect of Parameters

### *5.1.1 Bit Generation Rate*

An important performance indicator for a secret key generation scheme is *how fast it generates secret bits*. For our system, the bit generation rate before reconciliation directly depends on the coding window size $w$ used to segment EMG signals in the shape-based secret key generation. Although a small coding window gives us a high bit generation rate, it also reduces the information contained in the generation secret key as the uncertainty of possible variation shapes within each window becomes smaller. As we can image, if we set the coding window size to an extreme small value, then all the variations in each coding window will be very minor and can be approximated by a horizontal-line, *i.e.*, the "stay" shape.

To find out the optimal coding window size, we compute the bit generation rate and segment-wise entropy of generated secret keys with respect to different values of $w$. As shown in Figure 8, we observe that, with the growth of coding window size, the bit generation rate drops quickly, but the entropy contained in each segment increases and then converges to 1.54 bits per segment (Theoretically, maxi-

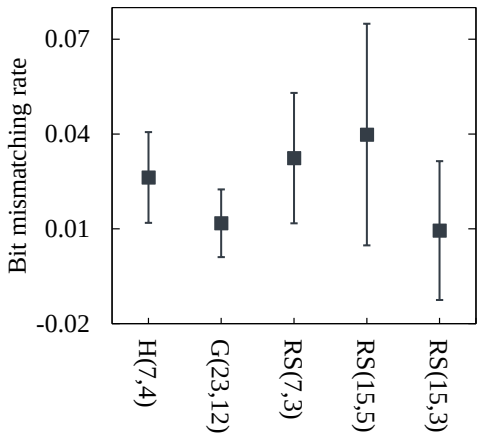



**Figure 9. Performance of different error correction coding scheme. Golay Code outperforms the other ECC codes.**

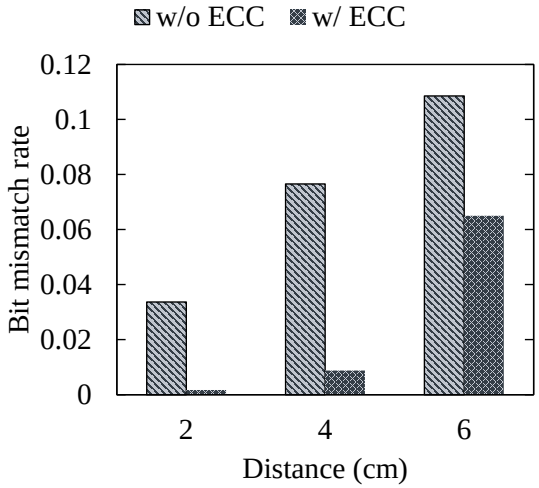



**Figure 10. The bit mismatching rate under different distances between legitimate devices. A larger distance boosts the inconsistency in devices' EMG measurements and thus results in more mismatching bits in generated secure key.**

mum entropy$= -\sum_1^3 \frac{1}{3}\log_2\frac{1}{3} \approx 1.58 bit/segment$). To preserve sufficient randomness, we set the coding windows size to 0.15 seconds in our system, which leads to a bit generation rate of 10.57 bit/s and 1.51 bits information per segment.

Note that this is not the final bit rate of EMG-KEY, because the reconciliation process will sacrifice a part of bit rate for the alleviation of mismatching bits due to the adoption of error correction coding. In the next section, we will analyze its impact on system performance.

### *5.1.2 Choice of Error Correction Code*

Due to the spacing between devices, differences in electrodes' properties and hardware imperfection, there are some discrepancies in the EMG measurements of the legitimate devices, which inevitably leads to mismatching bits among the generated secret keys. To alleviate such inconsistency, error correction code is adopted in the reconciliation stage. As a result, the choice of error correction coding algorithm, as well as its setting, *i.e.*, $n$ and $k$, do not only define the bit mismatching rate of our system, but also causes a loss of valid bit rate.

To examine the effectiveness of different ECC codes, three candidate codes are employed: (i) *Hamming Code*, which is a linear perfect error correction code that encodes 4-bit data into 7-bit code by adding 3 parity bits. (ii) *Golay code*, a well-known linear code which translates 12-bit message into 23 bits in such a way that any 3-bit error can be corrected. (iii) *Reed-Solomon code (RS)* is a cyclic code designed to detect and correct multiple errors. By adding check symbols to the raw data, a RS code, *RS(n, k)*, can correct up to $\lfloor\frac{n-k}{2}\rfloor$ bits of error. Such property make it suitable for burst errors and thus is widely adopted in many data storage applications [19]. Table 2 lists the ECC codes used in our evaluation, plus their parameters and properties, *i.e.*, code word length $n$, code length $k$, error-correcting ability $r$, information leakage and bit loss ratio.

**Table 2. Candidates of error correction codes**

| Code | n | k | r | Leakage | Bit loss |
|---|---|---|---|---|---|
| Hamming Code | 7 | 4 | 1 | 0.43 | 0.57 |
| Golay Code | 23 | 12 | 3 | 0.48 | 0.52 |
| RS(7, 3) | 7 | 3 | 2 | 0.57 | 0.43 |
| RS(15, 5) | 15 | 5 | 5 | 0.67 | 0.33 |
| RS(15, 3) | 15 | 3 | 6 | 0.8 | 0.2 |

Additionally, we collect a data set of raw EMG signals and corresponding secret keys from 10 users as described in Section 4. The average bit mismatching rate before reconciliation of this data set is 0.065 and the standard deviation is 0.029. We feed these data into the reconciliation process with different ECC codes and compare their performances in Figure 9.

From this figure, we find that, although Reed-Solomon Code with $n = 15, k = 3$ has the lowest average bit mismatching rate, Golay code $G(23,12)$ is a better choice as it performs more stably among different data records. Besides, we notice the standard deviation of linear ECC codes, *e.g.*, Hamming Code and Golay Code, are generally smaller than the Reed-Solomon code. This can be explained by the fact that Reed-Solomon code may introduce more mismatching bits if the number of mismatching bits exceeds its correction ability due to its nonlinear nature.

According to this result, we adopt the Golay Code, $G(23,12)$, in our system and use it in the rest of evaluations. According to Equation 9, the final bit generation rate of EMG-KEY is $\frac{12}{0.15\times 23}\times\log_2 3 \approx 5.51$ bit/s. Such bit rate outperforms the conventional PIN-code-based secure pairing, in which the average bit rate is 4.96 bit/s [11].

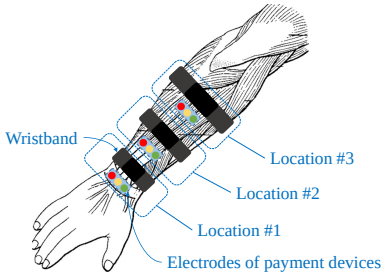



**Figure 11. Illustration of electrodes placements. The distances among different placements are 4 centimeters while the spacing between wristband and payment device in each experiment is fixed to 2 centimeters.**

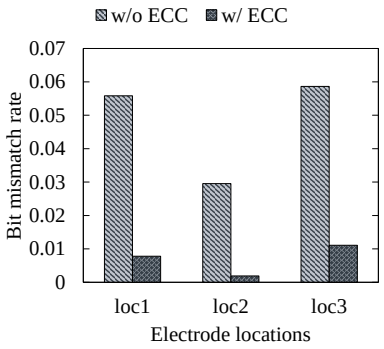



**Figure 12. Bit mismatching rate of different electrode placements. Location 2 outperforms the other locations as the EMG signal is much stronger and less interfered in this region.**

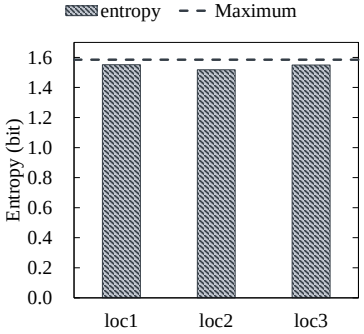



**Figure 13. Entropy of secret key generated at different electrode placements. They are relatively stable, which suggests different placements of electrodes are acceptable.**

## 5.2 Impact of Confounding Factors

### *5.2.1 Secure Distance between Devices*

In our application scenario, both legitimate devices need to be placed on the skin closely to ensure a secure pairing. Since EMG signal is a subtle electrical activity, it can only be precisely sensed near the contracting muscles. In addition, the EMG signals measured by devices are actually a composition of several individual EMG signals from different muscles. Moreover, as a complex organ, a human arm consists of 23 muscles, each of which has different functions [33]. Due to these facts, we can image large distance between the legitimate devices can increase their inconsistency in the EMG measurements, which eventually introduces additional mismatching bits.

To evaluate *how close the devices need to be placed to ensure a successful pairing*, we conduct extensive experiments on the volunteers by placing the wristband and payment device in different distances. Figure 10 shows the corresponding bit mismatching rate between legitimate devices.

From this figure, we observe a growing trend of bit mismatching rate with the increase of distance between devices, which corresponds to our previous analysis. Also, a distance within 4 centimeters can still maintain a good performance with the help of reconciliation, but larger distance than this will exceeds the correcting ability of the ECC code and ends up with a high mismatching rate.

### *5.2.2 Placement of Electrodes*

Apart from the distance between devices, another factor deriving from the subtle propagation nature of EMG and complex composition of human arm muscle is the placement of electrodes. Although the muscles of forearm are elongated and often distributed over the whole forearm, one may concern whether there is difference if we place the electrodes at different locations.

To evaluate the impact of electrode placement, we design three groups of experiments, in each of which the electrodes of the wristband and payment device are placed at different locations as shown in Figure 11. The distances among different placements are 4 centimeters while the spacing between wristband and payment device in each experiment is fixed to 2 centimeters.

We first evaluate the bit mismatching rate under each placement and the result is presented in Figure 12. An immediate observation from this figure is that the mismatching rate at location 2 is lower than location 1 and 3. This is because that, the location 1 is relatively far away from the contracting muscles, while the location 3 is often covered with more fat and tissues, which is evidenced to be able to hinder the propagation of EMG [37]. Compared with these two locations, the EMG measured at location 2 is much stronger and less interfered, which leads to a better performance. However, we also find that, with the help of reconciliation process, the performance at location 1 and 3 are still acceptable as most mismatching bits in secret keys can be significantly reduced by error correction code.

Also, to quantify the randomness level of secret keys generated under different electrode placements, the segment-wise entropy is computed and reported in Figure 13. A higher segment-wise entropy indicates more randomness will be included in each segment and thus the secret key is harder to be attacked. Note that, since we use three predefined shapes to approximate the EMG variation in the shape-based secret key generation, the theoretical upper-bound of the segment-wise entropy is achieved if all these shapes occur in the secret key randomly and uniformly. Thus, the maximum can is computed as: $max(H) = -\sum_1^3 \frac{1}{3}\log_2\frac{1}{3} \approx 1.58 bit/segment$, which is represented by the dashed line above the bars. According to this figure, the entropies of secret keys generated under different electrode placement are relative identical and all of them are approaching the theoretical maximum. This indicates most of the information of EMG randomness is preserved no matter where the electrodes are placed.

### *5.2.3 Gesture Complexity*

As our system requires users to perform a gesture to initiate the pairing process, one natural question is *whether the complexity of gestures can affect the system's performance and security level*. This question comes along with an in-

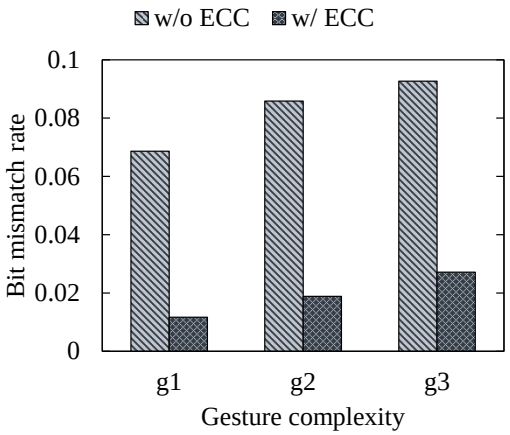



**Figure 14. Effect of gestures with different complexity.**

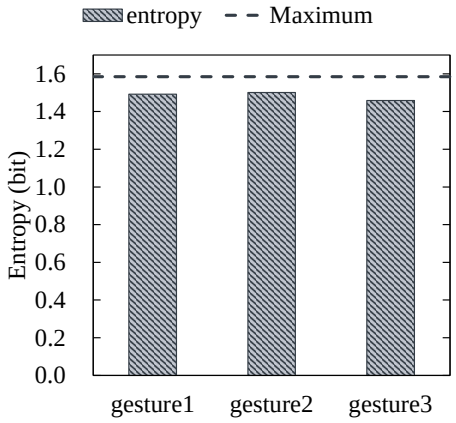



**Figure 15. Effect of gestures with different complexity.**

tuitive idea that the high-complexity gestures are hard to be imitated, which thus may introduce more robustness to attacks.

To explore the answer, we design three gestures with increasing complexity, namely, $g1$, $g2$ and $g3$. In $g1$, the user slowly clutches the fist, then release it gently. The second gesture, $g2$, requires users to clutch and release the fist quickly and repetitively. In the last gesture with highest complexity, the users are asked to randomly moves their fingers quickly as they wants.

Figure 15 shows the performance of secret key generation under gestures of different complexity. We surprisingly find that the bit mismatching rate is getting higher with the growth of gesture complexity. Upon further analysis, this turns out to be rooted in the fact that the complex gesture, such as moving fingers randomly, is often accomplished by the collaboration of several muscles, so there are multiple individual EMG signals interfered with each other during the complex gesture. Moreover, some of individual EMG signals are quite minor and can be easily overwhelmed by the others. As a result, the interference between individual EMG signals leads to an obvious inconsistency in the EMG measurements between legitimate devices, and eventually results in the degradation of performance.

Given such frustrating result, a major concern is whether the simple gesture can provide enough randomness for secure pairing. To this end, we again employ the segment-wise entropy to evaluate the randomness level provide by gestures with different complexity and present the result in Figure 15. We notice the complex gestures actually does not provide information gain. Also, the entropy of simplest gesture, *i.e.*, slowly clutch and then release the fist, is about 1.51 bit/segment, which almost approaches the theoretical upper bound of 1.58 bit/segment.

These two results implies that, although the high-complexity gesture does not provide any additional enhancement to our system, the simple gesture will suffice as it can preserve enough randomness and provide a good bit mismatching rate.

# 6 Resistance to Attacks

In this section, we evaluate the security performance of our system. Throughout the experiments, we assume there exists a strong attacker who is able to:

- know every details of our pairing algorithm;
- stand in close proximity, precisely observe and capture all the gestures made by users during pairing process;
- exactly imitate these gestures;
- eavesdrop and decode all the packets sent via a public communication link, *e.g.*, WiFi, Bluetooth or NFC;

In order to examine the our system's robustness to such strong attacker, we conduct extensive experiments on 10 volunteers, in which nine of them act as normal users while one simulates the attacker to imitate their gestures. Each user is asked to perform the pairing process 30 times with presence of attacker and there are $10 \times 30 = 300$ pairing records in total.

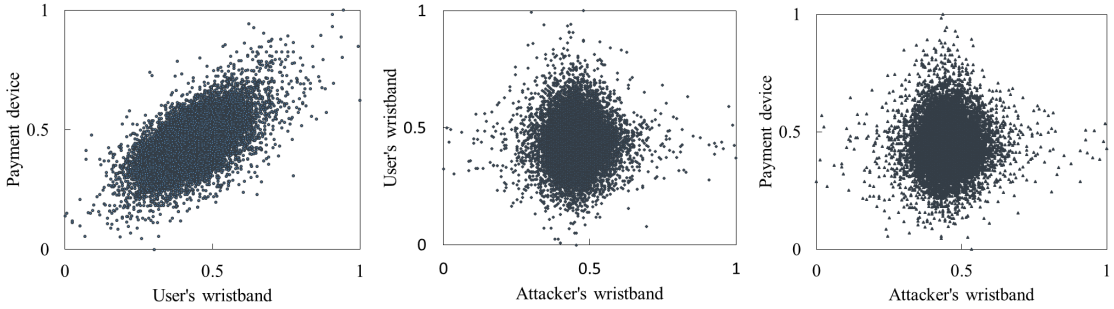
We start the evaluation with the analysis on the information leakage to the attacker. The experiments demonstrate the attacker can only obtain a negligible amount of information about the legitimate device even he can exactly imitate user's gesture.

After that, we take a close look at the bit matching rate of secret keys generated by different users and attackers, from which we can find the bit mismatching rate of attacker is significantly high even with the adoption of ECC code.

## 6.1 Information Leakage

To visualize the correlation between the EMG measurements of devices, we present the pairwise scatter-plots of the normalized EMG measurement of each pair of devices when both user and attacker are performing the same gesture synchronously in Figure 16.

From Figure 16(a), we can clearly observe that the EMG signal from payment device increase linearly with respect to the measurement from user's wristband, which implies there exists a strong correlation between them. On the other hand, even through the attacker is imitating the user's gesture synchronously, his/her EMG measurement does not appear




(a) User vs. payment device (b) Attacker vs. user (c) Close-up of shape-based encoding

**Figure 16. Flow of EMG-KEY.**

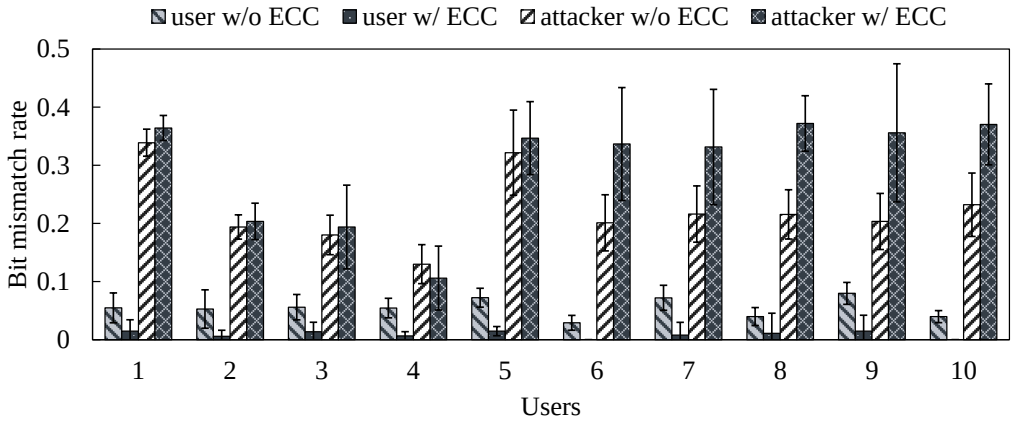



**Figure 17. Bit mismatching rate of users and copy attackers.**

much connection with user or payment device according to Figure 16(b) and 16(c).

To further quantify the amount of information can be learned by imitating the gesture, we compute pairwise mutual information between devices in Table 3. We note that, by measuring the EMG variation in close proximity, the wristband can obtain 1.158 bits of information about the payment device's corresponding secret key. On the contrary, the attacker, albeit imitating the gesture synchronously, can only have 0.29 bits of information about it. This indicates, the legitimate devices have 4 times more information about each other than the attacker can have.

**Table 3. Mutual information among user's wristband $A$, payment device $B$, and attacker's devices $E$**

| | **A vs. B** | **A vs. E** | **E vs. B** |
|---|---|---|---|
| **Mutual info.** | 1.158 | 0.290 | 0.274 |

## 6.2 The Performance of Copy Attacker

In this section, we further assume that the attacker can get the offset information $\delta$ transmitted in the reconciliation stage between legitimate devices via eavesdropping, and try to deduce their secret key during the pairing process.

In oder to simulate such attack, we design an experiment in which the offset information $\delta$ between legitimate devices is explicitly shared with the attacker via public communication and the same reconciliation is perform by attacker to help the estimation of secret key used by legitimate devices. The bit mismatching rate is used to quantify the possibility that attacker can have the same secret key as legitimate devices.

The evaluation result on 10 volunteers (30 pairing experiments for each volunteer) is reported in Figure 17. We can find that the bit mismatching rate between user's wristband and payment device can be efficiently reduced by the reconciliation process (the final average bit mismatching rate is $8.924 \times 10^{-3}$). However, the attacker can not benefit from such process: the bit mismatching rate between the key deduced by attacker and the real secret key used even increase after the adoption of the error correction code, which ends up with an average bit mismatching rate of 0.298. This is because that, if the number of mismatched bits exceeds the error correcting ability of ECC code, some matched bits might be erroneously flipped and thus more mismatching bits are introduced.

As a result, it is impossible for attacker to hack the pairing process even he can eavesdrop the offset information. Consider using a 4-bit PIN code as traditional Bluetooth pairing, which has a equivalent 13.2 secret bits [34], the successful pairing rate between legitimate devices is $(1-0.008924)^{13.2} \approx 88.84\%$, while the attacker can only have $(1-0.298)^{13.2} \approx 0.94\%$ chance to deduce the same secret key.

# 7 Discussion

In this section, we discuss the practical issus of our system, and possible directions of future exploration.

**EMG Wearables.** As the major security of our system relies on the employment of EMG signal, one may question *whether the EMG sensor is available for wearable devices*. According to our study, there are already several wearable products are embedded with EMG sensors, *e.g.*, Myo armband [7], Athos gear [3], and Leo smart band [6], which enable many promising applications. For instance, the Myo armband can recognize the user's gesture and provides a new way for human-computer interaction, while the Athos gear can monitor the contraction state of muscle and be used to help physical training. We envision that, in the near future, there will be more wearable devices equipped with EMG sensors due to the fast development of Augmented Reality (AR) and healthcare market [4, 41].

**Threat of electromagnetic emanation.** Recent studies have exposed a new threat derived from electromagnetic emanation (EM). By using the electromagnetic nature of devices, it is possible for adversaries to eavesdrop the information [25] or even perform the EM signal injection attack, in which the attacker manipulates the input to the device by emitting chosen electromagnetic waveforms [47]. However, such attacking techniques can not defeat our system. First, due to the fact that the EMG voltage is unobtrusive (often withing $\pm 10$ mv), it is extremely hard to eavesdrop its EM radiation in practical. Also, the EM signal injection attacks can be prevented in the design of hardware.

**Multi-Channel EMG.** To make our system more reliable and practical, there are some possible directions worth to explore in the future. The first one is *the adoption of multi-channel EMG*. To measure the muscle activity accurately, many existing wearable devices are equipped with more than one EMG sensor. We believe that the performance of our system can be further enhanced if the EMG signals from different channel can provide more information and randomness. Also, our current system only employ three basic shapes to quantify the EMG variation, more fine-grained quantization level can be adopted to improve the system's performance.

# 8 Related Work

## 8.1 Secure Pairing

Many techniques have been proposed to enable secure pairing between mobile devices based on pre-shared secrets. A variety of information sources have been exploited to generate shared secret keys without prior information exchange. Such sources can be wireless channel measurements [14, 26, 31, 35, 42], human motion [11, 36], vibration [9], or ambient environments [34, 45]. Azimi et al. [14] are among the first to leverage the channel reciprocity to generate secret keys from wireless signal strength. Jana et al. [26] propose an environmental-adaptive key generation scheme to boost the bit generation rate. Liu et al. [31] take one step further by using the fine-grained channel state information (CSI) as the reciprocal information to extract more information for key generation in OFDM systems. Similarly, Puzzle [42] leverages the frequency shapes of channel measurements to obtain more robust secret bits. Checksum Gestures [11] uses a single-continuous gesture to generate an authentication code to replace the traditional PIN input for wearables. Mayrhofer [36] establishes a secure link between two devices by shaking them together, and leverages their trajectories as the shared information. instead of using hand-incurred motion, Ving [9] leverages the vibration of a desk as the shared secret for all devices on the desk. Ambient environment based approaches authenticate the proximity of two devices based on ambient wireless signals [34] or ambient audios [45]. Different from these approaches, EMG-KEY leverages muscle contraction inside human body as the source, which is secure to proximate eavesdroppers and even camera-based shoulder-surfers.

## 8.2 EMG Analysis

Traditionally, EMG is used by clinic doctors and biomedical scientist to study the muscle fatigue [17, 24, 30], neuromuscular diseases [16, 23, 46] and human kinesiology [10, 39]. In recent years, the EMG is also widely adopted to enable different promising applications, e.g., controlling prosthetic [13, 40], emotion recognition [18, 21], and speech recognition [27, 32]. Apart from this, extensive effort has been devoted to the exploration of using EMG as an interface of Human-machine interaction [12, 29, 38, 43, 44]. As a complementation, our work propose a method to leverage EMG signal to pairing wearable devices.

# 9 Conclusion

In this work, we propose a secure pairing system for wearable devices by exploring the randomness embedded in the EMG signal. We design a shape-based secret key generation scheme and leverage error correction code to alleviate the inconsistency between devices. Extensive experiments on ten volunteers indicates our system is robust to many confounding factors and can achieve a competitive bit generation rate of 5.51 bit/s while maintaining a high successful pairing rate around 88.84%. Also, evaluation result with the presence of copy attackers demonstrate our system can defend against strong attacks.

# 10 References


[1] Apple pay. http://www.apple.com/apple-pay.

[2] Arduino uno. https://www.arduino.cc/en/Main/ArduinoBoardUno.

[3] Athos gear. https://www.liveathos.com.

[4] Devices with emg sensor. http://vandrico.com/wearables/device-categories/components/emg-sensor.

[5] Fitbit. https://www.fitbit.com.

[6] Leo smartband. http://leohelps.com.

[7] Myo armband. https://www.myo.com.

[8] Olimex emg shield. https://www.arduino.cc/en/Main/ArduinoBoardUno.

[9] J. Adkins, G. Flaspohler, and P. Dutta. Ving: Bootstrapping the desktop area network with a vibratory ping. In *Proceedings of the 2nd International Workshop on Hot Topics in Wireless*, pages 21–25. ACM, 2015.

[10] J. Ahlgren. Kinesiology of the mandible an emg study. *Acta odontologica scandinavica*, 25(6):593–612, 1967.

[11] I. Ahmed, Y. Ye, S. Bhattacharya, N. Asokan, G. Jacucci, P. Nurmi, and S. Tarkoma. Checksum gestures: continuous gestures as an out-of-band channel for secure pairing. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 391–401. ACM, 2015.

[12] C. Amma, T. Krings, J. Böer, and T. Schultz. Advancing muscle-computer interfaces with high-density electromyography. In *Proceed-*

*ings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 929–938, New York, NY, USA, 2015. ACM.

[13] A. H. Arieta, H. Yokoi, T. Arai, and W. Yu. Study on the effects of electrical stimulation on the pattern recognition for an emg prosthetic application. In *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, pages 6919–6922. IEEE, 2006.

[14] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust key generation from signal envelopes in wireless networks. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 401–410. ACM, 2007.

[15] R. Beck. Muscle fiber conduction velocity. *Wiley Encyclopedia of Biomedical Engineering*, 2006.

[16] A. Berardelli, J. Dick, J. Rothwell, B. Day, and C. Marsden. Scaling of the size of the first agonist emg burst during rapid wrist movements in patients with parkinson's disease. *Journal of Neurology, Neurosurgery & Psychiatry*, 49(11):1273–1279, 1986.

[17] B. Bigland-Ritchie, E. Donovan, and C. Roussos. Conduction velocity and emg power spectrum changes in fatigue of sustained maximal efforts. *Journal of applied physiology*, 51(5):1300–1305, 1981.

[18] B. Cheng and G.-Y. Liu. Emotion recognition from surface emg signal using wavelet transform and neural network. In *Proceedings of the 2nd international conference on bioinformatics and biomedical engineering (ICBBE)*, pages 1363–1366, 2008.

[19] G. C. Clark Jr and J. B. Cain. *Error-correction coding for digital communications*. Springer Science & Business Media, 2013.

[20] T. M. Cover and J. A. Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[21] M. De Wied, A. V. Boxtel, J. A. Posthumus, P. P. Goudena, and W. Matthys. Facial emg and heart rate responses to emotion-inducing film clips in boys with disruptive behavior disorders. *Psychophysiology*, 46(5):996–1004, 2009.

[22] S. R. Devasahayam. *Signals and systems in biomedical engineering: signal processing and physiological systems modeling*. Springer Science & Business Media, 2012.

[23] R. Ferri, M. Manconi, G. Plazzi, O. Bruni, S. Vandi, P. Montagna, L. FERINI-STRAMBI, and M. Zucconi. A quantitative statistical analysis of the submentalis muscle emg amplitude during sleep in normal controls and patients with rem sleep behavior disorder. *Journal of sleep research*, 17(1):89–100, 2008.

[24] P. A. Gribble and J. Hertel. Effect of lower-extremity muscle fatigue on postural control. *Archives of physical medicine and rehabilitation*, 85(4):589–592, 2004.

[25] Y. Hayashi, N. Homma, M. Miura, T. Aoki, and H. Sone. A threat for tablet pcs in public space: Remote visualization of screen images using em emanation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 954–965, New York, NY, USA, 2014. ACM.

[26] 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 *Proceedings of the 15th annual international conference on Mobile computing and networking*, pages 321–332. ACM, 2009.

[27] S.-C. S. Jou, T. Schultz, M. Walliczek, F. Kraft, and A. Waibel. Towards continuous speech recognition using surface electromyography. In *INTERSPEECH*, 2006.

[28] E. J. Keogh and M. J. Pazzani. Scaling up dynamic time warping for datamining applications. In *Proceedings of the sixth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 285–289. ACM, 2000.

[29] D. Kim, O. Hilliges, S. Izadi, A. D. Butler, J. Chen, I. Oikonomidis, and P. Olivier. Digits: freehand 3d interactions anywhere using a wrist-worn gloveless sensor. In *Proceedings of the 25th annual ACM symposium on User interface software and technology*, pages 167–176. ACM, 2012.

[30] L. Lindstrom, R. Magnusson, and I. Petersen. Muscular fatigue and action potential conduction velocity changes studied with frequency analysis of emg signals. *Electromyography*, 10(4):341, 1970.

[31] H. Liu, Y. Wang, J. Yang, and Y. Chen. Fast and practical secret key extraction by exploiting channel response. In *INFOCOM, 2013 Proceedings IEEE*, pages 3048–3056. IEEE, 2013.

[32] L. Maier-Hein, F. Metze, T. Schultz, and A. Waibel. Session independent non-audible speech recognition using surface electromyography. In *Automatic Speech Recognition and Understanding, 2005 IEEE Workshop on*, pages 331–336. IEEE, 2005.

[33] E. N. Marieb and K. Hoehn. *Human anatomy & physiology*. Pearson Education, 2007.

[34] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam. Proximate: proximity-based secure pairing using ambient wireless signals. In *Proceedings of the 9th international conference on Mobile systems, applications, and services*, pages 211–224. ACM, 2011.

[35] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radiotelepathy: extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 128–139. ACM, 2008.

[36] R. Mayrhofer and H. Gellersen. Shake well before use: Intuitive and secure pairing of mobile devices. *Mobile Computing, IEEE Transactions on*, 8(6):792–806, 2009.

[37] R. Merletti and P. A. Parker. *Electromyography: physiology, engineering, and non-invasive applications*, volume 11. John Wiley & Sons, 2004.

[38] P. Mistry, P. Maes, and L. Chang. Wuw-wear ur world: a wearable gestural interface. In *CHI'09 extended abstracts on Human factors in computing systems*, pages 4111–4116. ACM, 2009.

[39] F. Mokaya, R. Lucas, H. Y. Noh, and P. Zhang. Myovibe: Vibration based wearable muscle activation detection in high mobility exercises. UbiComp '15, pages 27–38, New York, NY, USA, 2015. ACM.

[40] D. Nishikawa, W. Yu, H. Yokoi, and Y. Kakazu. Emg prosthetic hand controller using real-time learning method. In *Systems, Man, and Cybernetics, 1999. IEEE SMC'99 Conference Proceedings. 1999 IEEE International Conference on*, volume 1, pages 153–158. IEEE, 1999.

[41] R. D. Peter Harrop, James Hayward and G. Holland. Wearable technology 2015-2025: Technologies, markets, forecasts. pages 285–289. IDTechEx, 2015 Feb.

[42] Y. Qiao, K. Srinivasan, and A. Arora. Shape matters, not the size: A new approach to extract secrets from channel. In *Proceedings of the 1st ACM workshop on Hot topics in wireless*, pages 37–42. ACM, 2014.

[43] T. S. Saponas, D. S. Tan, D. Morris, and R. Balakrishnan. Demonstrating the feasibility of using forearm electromyography for muscle-computer interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 515–524. ACM, 2008.

[44] T. S. Saponas, D. S. Tan, D. Morris, J. Turner, and J. A. Landay. Making muscle-computer interfaces more practical. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 851–854. ACM, 2010.

[45] D. Schurmann and S. Sigg. Secure communication based on ambient audio. *Mobile Computing, IEEE Transactions on*, 12(2):358–370, 2013.

[46] A. Subasi. Classification of emg signals using pso optimized svm for diagnosis of neuromuscular disorders. *Computers in biology and medicine*, 43(5):576–586, 2013.

[47] M. Vuagnoux and S. Pasini. Compromising electromagnetic emanations of wired and wireless keyboards. In *Proceedings of the 18th Conference on USENIX Security Symposium*, SSYM'09, pages 1–16, Berkeley, CA, USA, 2009. USENIX Association.