H2B: heartbeat-based secret key generation system using piezo vibration sensors

ABSTRACT
With growing popularity of wearable devices, security for body area network (BAN) becomes an important issue as wearables deal with private sensory information for a range of tasks. Previous studies have shown that the heartbeat signal, specifically interpulse interval (IPI) can be used to generate symmetric cryptographic keys. However, IPI readings are usually sampled by either Electrocardiogram (ECG) or Photoplethysmogram (PPG) which are inappropriate for wearable devices due to their cost and energy. In this paper, we demonstrate that the subtle motions caused by heartbeat can be sensed by wearable piezo vibration sensors on multiple body locations, and can be further explored to generate secret bits. Based on this finding, we design and implement the first heartbeat-based key generation system using piezo sensors, named Heartbeats-to-Bits (H2B). The main challenge with piezo-based IPI is high mismatch rate. We experimentally find out that piezo-based IPI can provide 2.9 bits entropy in each IPI. To this end, we apply an inverted cumulative distributed function (ICDF)-based quantization method to fully extract entropy and propose a novel Compressive Sensing (CS)-based reconciliation protocol to overcome high mismatch rate key. We implement H2B with off-the-shelf piezo sensors and evaluate the performance on the dataset from 23 participants. Our evaluation results show that CS-based reconciliation method can improve the success rate of H2B from 34.2% to 95.6% compared to the state-of-the-art reconciliation method. Moreover, we analyze three types of possible attacks and demonstrate that H2B is robust to these attacks. Finally, we confirm that piezo sensors-based H2B system is more energy-efficient compared to off-the-shelf wearable ECG system.

CCS CONCEPTS
• Computer systems organization → Embedded systems; Redundancy; Robotics; • Networks → Network reliability;

KEYWORDS
ACM proceedings, IJ backlogX, text tagging

ACM Reference Format:

1 INTRODUCTION
With recent advances in wireless sensor networks and embedded computing technologies, the popularity of wearable devices, such as FitBit and Apple Watch, is skyrocketing. A recent survey [36] shows that the wearable market is beaming with hundreds of different types of products including smart glasses, smart jewelry, electronic garments, smart shoes, skin patches, and even implanted medical devices (IMDs). We are heading to a future where users are expected to have more than one wearable device continuously monitoring their bodies and providing advanced health and other services [18].

In such multi-wearable scenario, wearable devices may deal with private sensory information for a range of tasks, such as data aggregation, sensing coordination, data relaying (from body to cloud). To protect private information, body area networks (BAN) usually rely on symmetric cryptographic keys for communication. Traditional approaches to distribute keys that require pre-deployment in the network initialization stage are not scalable with growing number of wearables. Exploiting biometrics as shared key sources has become an efficient cryptographic scheme, as this type of system can provide the advantages of plug-n-play and transparency.

Among all biometrics, the interpulse interval (IPI), which refers to the time interval of heartbeat, is a common choice of the key source for wearables, especially IMDs. IPI of heartbeat has been proved to have a high level of entropy [31], thus can ensure the security of cryptographic systems. Previous researches in this direction [19, 34, 48] are mainly based on Electrocardiogram (ECG) signals and a few of them [19, 41, 42] exploited Photoplethysmogram (PPG). Piezo vibration sensor, especially polyvinylidene fluoride (PVDF) piezopolymer, is proved to be an effective tool for wearable devices, which can harvest energy from ambient human motions, also draws research attention [24, 32]. We can expect more piezo sensor-installed wearables in the future market.

In this article, we explore the potential of IPI measured by piezo sensors as a secret source and design a symmetric key generation system, named Heartbeat2Bit (H2B), based on IPI from piezo sensors. The significance of this work are threefold: 1. Compared to ECG and PPG, piezo vibration sensors are usually lightweight, cost-efficient (the off-the-shelf piezo sensor used in H2B prices US$5.6), and energy-efficient (see Section 5.6) solution for wearable devices. 2. Piezo vibration sensor-based energy harvesting scheme for wearables, which can harvest energy from ambient human motions, also draws research attention [24, 32]. We can expect more piezo sensor-installed wearables in the future market. 3. IPI is a biometric can be measured using ECG, PPG, piezo sensors, etc. As such, it enables cross pairing among devices with different sensors. By studying piezo sensor-based system, we can extend the IPI-based cryptographic system to a wider range of wearable devices. To the best of our knowledge, there has been no attempt of exploiting IPI measured by piezo vibration sensor as a source for key generation.
We envision the usage of H2B primarily for wearable devices that has close contact with user’s body as these devices can detect and measure user’s heartbeat pulses and further use them to establish common cryptographic keys for secure communications. For example, one day morning, a user Jane gets up from bed and wears a smart wristband (Alice) on her wrist. She wants to read some information from her pacemaker (Bob) which is inside her chest. She starts H2B on the smart wristband, and after a short while, Alice and Bob automatically establish a secret key by measuring Jane’s IPI. Finally, Bob transfers privacy sensitive data to Alice via the proposed compressive sensing-based information reconciliation method to fully extract the entropy. The complete H2B system and the key potential of piezo-based IPI and implement a quantization is discussed in Section 2. In Section 3, we experimentally analyze Sensing (CS)-based reconciliation method to correct mismatch in function(ICDF)-based quantization method to fully extract entropy challenges, we firstly apply an inverted cumulative distribution based IPI is significantly larger than ECG-based IPI. Facing this sensor. In Section 3.2 later, we can see the mismatch rate of piezo-sensor. We experimentally show that CS-based reconciliation method to correct mismatch in piezo-based IPI. Then, we propose and apply a novel Compressive Sensing (CS)-based reconciliation method to correct mismatch in quantized bits.

The contributions of this work can be summarized as follows:

- We conduct a world first study to experimentally analyze the key potential piezo-based IPI. Our result shows that there exists 2.9 bit entropy can be extracted from each IPI. To this end, we apply a ICDF-based quantization method to extract the entropy.
- We propose H2B, a novel symmetric key generation system exploiting IPIs captured using PVDF piezo sensor. In H2B, we propose and apply a novel CS-based reconciliation method to overcome the high level of measurement variation inherent in piezo sensors.
- We provide a proof of concept implementation of H2B using off-the-shelf piezo sensor and evaluate H2B with 23 participants. We experimentally show that CS-based reconciliation method improves the success rate to generate a 128-bit key from 34.2% to 95.6% compared to the state-of-the-art reconciliation method.
- We conduct comprehensive attack analysis shows that H2B is highly robust against typical attacks.
- Finally, we conduct a power consumption analysis. Our results show that H2B is a power-efficient system to sample IPI and generate symmetric key compared to off-the-shelf wearable ECG devices.

The rest of the paper is organized as following. Related work is discussed in Section 2. In Section 3, we experimentally analyze the key potential of piezo-based IPI and implement a quantization method to fully extract the entropy. The complete H2B system and the proposed compressive sensing-based information reconciliation protocol are presented in Section 4. Finally, we show the prototype devices and all evaluation results in Section 5, before concluding the paper in Section 6.

2 RELATED WORK

2.1 Biometrics-based Key Generation

Biometrics is the most popular trend in key generation for BAN [35]. Among all biometrics, electrocardiograms (ECGs) are most common choice of key material. Previous works in this direction either extracted frequency domain features or IPIs for the entropy source. Systems [11, 40–43] based on frequency domain features can always generate keys in faster rates with high matching rate between two parties. However, these works did not provide an information theoretical analysis on whether the randomness source contains sufficient entropy for key generation. In fact, Bagade et al. stated that the frequency domain features do not provide forward secrecy and the key secret can be revealed from historical heartbeat data [2].

To address above problem, Poon et. al developed a system that exploited IPIs as the entropy source instead of insecure frequency domain features in [31]. However, a cryptographic system can only extract average 4 bits from each IPI. Hence, it takes approximately 40 seconds to generate a 128-bit key, lacking usability compared to frequency domain-based method. Taking security as the primary requirement for a cryptographic system, B2B follows IPI-based key generation method direction.

As biometric measurements are inherent imperfect, extracted IPIs from two legitimate devices can have a certain amount of mismatch. The works in this direction employed various reconciliation approaches, such as fuzzy vault [19, 41, 42, 54], to overcome this challenge.

Xu et al. introduced an IMD security system named IMDGuard by using a ‘guardian’ device to control access and transmission of confidential data in IMDS [48]. This system requires IMD and the guardian agree on a symmetric key. The author thereby developed a key agreement mechanism based on IPIs in ECGs. The weakness of IMDGuard is that their study was mainly based on datasets and is lacked of system implementation and thus the performance of the system in realistic environment. Hu et. al developed a general system named Ordered-Physiological-Feature-based Key Agreement(OPFKA) protocol considering both frequency features and IPI features [19]. For reconciliation, they hid their secret by randomly permute IPI information, (similar with Cascade reconciliation [20]) and exchanged the information to generate the same symmetric key. Both IMDGuard and OPFKA require exchanging messages between two pairing parties via an unauthenticated channel for reconciliation. Due to the information leakage from message exchanges, Rostami et al. presented a man-in-the-middle (MITM) attack that are able to comprise IMDGuard and OPFKA [33]. Rostami et. al later developed an IMD authentication system named Heart2Heart (H2H) with a rigorous security analysis [34]. Instead of using a reconciliation approach, they accepted two keys within a certain hamming distance as an agreement to address the problem of measurement noise.

Besides ECGs, signals from another heartbeat measurement tools, Photoplethysmogram (PPG), were also investigated in several papers [19, 41, 42]. However, IPIs from blood pressure pulse, which
H2B: heartbeat-based secret key generation system using piezo vibration sensors

can be measured using piezo vibration sensors, were not exploited as a key material by previous works. It is because that the measurement noises in the piezo vibration sensors are significantly larger than those in ECG and PPG. To this end, B2B presents a humble first step to develop a cryptographic system based on IPIs extracted from noisy piezo signals by a suite of signal processing algorithms and a novel CS-based reconciliation method.

2.2 Reconciliation

Information reconciliation has been widely studied in wireless cryptographic system for BAN to correct measurement errors, non-symmetric noise and/or interference [37, 51]. To correct mismatch between two pairing parties, reconciliation protocol allows two parties exchange the information via an insecure channel. From information theoretical view, reconciliation protocol trades off security for error correction capacity. More information exchanged via the insecure channel usually results in wider error correction capacity, and more information leakage.

The popular information reconciliation protocols include Cascade [20, 46, 55], and error correcting code(ECC)-based method. Note that fuzzy vault [21] can be broadly considered as an extension of ECC-based method. In Cascade protocol, two parties segment and permute the bit streams randomly into small blocks. By exchanging the permutation and the parity of each block, two parties can correct the differences of the bit streams. In ECC-based method, two parties treat their bit streams as a distorted version of a secret key and derive the secret key using various ECC codes including low-density parity-check (LDPC) [27], BCH code [14], Reed-Solomon code (RS) [52], Golay code [25], Turbo code [1], etc. Mismatches are corrected by exchanging the difference between their own bit stream and the secret key. Overall, ECC-based method has a wider error correction capacity with more information leakage compared to Cascade.

In this work, we introduce a novel CS-based reconciliation method to overcome the measurement error issue. Although the security of CS as an encryption method has been already investigated [7, 8, 53], there is no CS-based information reconciliation protocol developed. The advantage of this method is that we can balance the trade-off between error correction capacity and information leakage by adjusting compression rate, which is a parameter in CS. The details of proposed method will be introduced in Section 4.2 later.

3 KEY GENERATION POTENTIAL OF PIEZO-BASED IPI

3.1 IPI Preliminary

Interpulse interval (IPI) generally refers the time interval between two consecutive heartbeats. A heartbeat cycle in ECG is characterized by the combination of three of the graphical deflections (Q, R and S waves), which is also known as QRS complex. IPI in ECG is defined as the time interval between two consecutive R-peaks, which are the local maximum points of QRS complex. The mechanism for measuring heartbeat using vibration or motion sensors is different from ECG. After each heartbeat, the blood is ejected from the heart into arteries. The arteries expand to accommodate the blood, then recoil [13]. The expansion and recoiling effect, known as the blood pressure pulse, can be measured on skin near arteries (e.g. radial artery in the wrist) using motion or vibration sensors. Specifically, we found out that the pulse signals can be measured on 5 different body locations (chest, wrist, neck and ankle) as shown in Figure 1 and 2. Moreover, piezo sensors on the chest does not require skin contact to derive the heartbeat signal. This makes H2B feasible with wearable devices that can be placed in the chest pocket, such as smartphone.

The curves of heartbeat cycle on different body locations do not follow a same pattern like QRS complex. However, it is still possible to use a local peak point (either maximum or minimum) to represent each heartbeat and further extract IPI. To this end, we define IPI measured by pressure sensors as the time interval from two consecutive peaks.

3.2 Piezo-based IPI as Secret Source

The secret source for symmetric cryptographic protocols must satisfy two conditions [11]. Firstly, randomness condition: for security purpose, the generated key must be cryptographically random, or independently and identically distributed (i.i.d.). Secondly, proximity condition: for usability purpose, the final keys generated from

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>the signal length of bit vector</td>
</tr>
<tr>
<td>M</td>
<td>the length of compressed key</td>
</tr>
<tr>
<td>s</td>
<td>bit vector (or raw key) after quantization</td>
</tr>
<tr>
<td>y</td>
<td>compressed key</td>
</tr>
<tr>
<td>Φ</td>
<td>compressing matrix</td>
</tr>
<tr>
<td>κ</td>
<td>sparsity, the number of non-zero elements in a vector</td>
</tr>
<tr>
<td>κA,B,A</td>
<td>sparsity of key Alice (x_{A,B,A})</td>
</tr>
<tr>
<td>κA,B,A,E</td>
<td>sparsity of mismatch vector between Alice and Bob, and between Alice and Eve</td>
</tr>
<tr>
<td>i</td>
<td>order for the SG filter</td>
</tr>
<tr>
<td>k</td>
<td>number of frames for the SG filter</td>
</tr>
<tr>
<td>a</td>
<td>compression rate</td>
</tr>
</tbody>
</table>
The following text describes the potential of piezo-based IPI as a secret source. To examine the potential of piezo-based IPI as a secret source, we built several prototype wearable devices (see Section 5.1) and collected a preliminary dataset from 8 volunteers. We also followed the IPI extraction and quantization process of a well-cited ECG-based system, Heart2Heart (H2H) [34] to benchmark piezo-based IPI against ECG-based IPI. An important parameter that can influence the result is sampling rate. In this experiment, we selected 360Hz in accordance with H2H. The dataset of piezo-based IPI to find out how much entropy can be extracted from each IPI and introduce a quantization approach to extract the entropy.

Table 2: Comparison of entropy and mismatch rate

<table>
<thead>
<tr>
<th>Bit</th>
<th>piezo-based IPI</th>
<th>ECG-based IPI (H2H Results)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Entropy</td>
<td>Mismatch Rate</td>
</tr>
<tr>
<td>8 (MSB)</td>
<td>0.05</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0.44</td>
<td>0.010</td>
</tr>
<tr>
<td>6</td>
<td>0.64</td>
<td>0.069</td>
</tr>
<tr>
<td>5</td>
<td>0.98</td>
<td>0.174</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0.328</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0.428</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0.452</td>
</tr>
<tr>
<td>1 (LSB)</td>
<td>1</td>
<td>0.498</td>
</tr>
</tbody>
</table>

3.3 Entropy from Each IPI

Entropy denotes how much information contained in a source. In the symmetric key generation, entropy of common secret in a source quantitatively illustrates the key potential of this source. It is a physical feature of the source and not affected by applications. Ideally, a 100%-efficient symmetric key generation system can extract all entropy in a source to generate a symmetric key. It will require zero-noise sensor and full knowledge of the source. In practical, the amount of entropy can be extracted for key generation depends on sampling, extraction, and quantization procedures, and it is always smaller than the entropy in the source. In this section, we analyze the dataset of piezo-based IPI to find out how much entropy can be extracted from each IPI and introduce a quantization approach to extract the entropy.

Recommended by NIST [5], a symmetric key must have at least 128-bit entropy, i.e. a 128-bit key comprised of all 1-bit entropy bits, to prevent the brute-force attack. According to the result in Table 2, we can only extract 0.98-bit entropy (Bit 5) from each IPI. To generate a 128-bit, we need to sample 131 IPI values, requiring a long key generation time. However, the previous quantization approach does not exploit all key potential of piezo-based IPI. In H2H, IPI readings were converted directly to a Gray-code representation in the quantization procedure. This approach wastes key potential of IPI as because the quantization results have three low entropy bits (Bit 6-8). Attackers can find out rules to guess the key if these bits are adopted in the secret key. Therefore, we have to discard these bits and along with the entropy contained in these bits. In this sense, we can extract more entropy from each IPI if we quantize original IPI values to a bit sequence that has only high-entropy bits. The root cause of the entropy waste is that IPI readings are not i.i.d., though the last four or five gray-coded bits are i.i.d. Figure 3(a) shows that IPI roughly follows a random normal distribution. To fully exploit the key potential, we need to quantize the original IPI values to a new value set in a uniform distribution.

We calculate that IPI readings from piezo sensors at 360Hz contains 6.2392 bit entropy. Note that this number is not how much entropy can be extracted from each IPI. The 6.2392-bit information contains both common secrets and random noise. This entropy is high-entropy bits have small mismatch rates and can be used as a common secret. The result shows that piezo-based IPI as a secret source faces a significantly higher bit mismatch rates compared to ECG-based IPI.
implies that IPI readings can be represented by a 6-bit random uniform distribution. We thereby quantize original IPI readings in a normal distribution into a set of \(2^6\) new values. The thresholds are calculated using inverted cumulative distributed function (ICDF) so that the new set will have equal counts in each value, and follow a uniform distribution. Figure 3(b) shows the distribution of quantized IPI values. After quantization, it roughly follows the uniform distribution and has 6 high-entropy bits as shown in Table 3. We then need to extracts bits for common secret and discards bits for random noises. According to Table 3, though mismatch rate is still high in three least significant bits, 3 most significant bits have a low mismatch rate and can be considered as common secrets. The total entropy contained in these 3 bits is 2.92 bits. It means adopting this quantization approach improves the entropy by a factor of 3.

The sampling rate is another parameter that can affects how much entropy can be extracted from Each IPI. As IPI denotes the time interval, the sampling rate will determine the resolution of IPI. Higher resolution captures more information and introduces more noises. Entropy in a source is a physical feature, so there exists a low bound for sampling rate, at which all entropy of common secret can be captured. At the low bound, we can reveal the entropy can be extracted from each IPI. It is also important to find the lowest possible sampling rate for resource-constraint wearable applications. Considering the mismatch correction capability of information reconciliation step introduced in Section 4.2 later, we use the average 15% mismatch rate as the threshold to decide whether a bit can be considered as a common secret.

Table 3: Comparison of entropy and mismatch rate

<table>
<thead>
<tr>
<th>Bit</th>
<th>Entropy</th>
<th>Mismatch Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 (MSB)</td>
<td>0.96</td>
<td>0.129</td>
</tr>
<tr>
<td>5</td>
<td>0.96</td>
<td>0.124</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0.194</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0.358</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0.348</td>
</tr>
<tr>
<td>1 (LSB)</td>
<td>1</td>
<td>0.432</td>
</tr>
</tbody>
</table>

To validate the randomness of bits extracted using the ICDF-based quantization approach, we apply the NIST suite of statistical tests by concatenating all bits in the extracted from the dataset. All NIST tests have p-values larger than 1% in Table 4. It implies the bit vector derived via the ICDF-based quantization approach satisfies the randomness condition.

### 3.4 Impact of Sampling Rate on Entropy

The sampling rate is another parameter that can affects how much entropy can be extracted from Each IPI. As IPI denotes the time interval, the sampling rate will determine the resolution of IPI. Higher resolution captures more information and introduces more noises. Entropy in a source is a physical feature, so there exists a low bound for sampling rate, at which all entropy of common secret can be captured. At the low bound, we can reveal the entropy can be extracted from each IPI. It is also important to find the lowest possible sampling rate for resource-constraint wearable applications. Considering the mismatch correction capability of information reconciliation step introduced in Section 4.2 later, we use the average 15% mismatch rate as the threshold to decide whether a bit can be considered as a common secret.

Figure 4 illustrates the impact of sampling rate on entropy. The total entropy of IPI readings is positively related to the sampling rate as expected. After we separate the entropy of common secret and that of random noise using ICDF-based quantization approach and 15% mismatch rate as the threshold, entropy of common secret is revealed to be a constant value, i.e. 2.9 bits. The low bound of sampling rate to capture all the entropy of common secret is 120 Hz. If we sample the piezo sensor below the low bound, information of common secret will be missing. Figure 4 also shows that there are at least 2 bits random noises, resulted from the measurement noises from piezo sensors.

Sampling at low bound 120 Hz, results shows that bits for common secret has a mismatch rate of 14.4%. This highlights the need for an efficient information reconciliation protocol that can correct the high bit mismatch rates in H2B, we propose a novel approach by formulating the information reconciliation problem as a compressive sensing (CS) problem (in Section 4). The evaluation (in Section 5.3) shows that it can improve IPI-based key generation performance compared to the state-of-the-art approach.
With key generation potential of IPI revealed in Section 3, we model WOODSTOCK’97, July 1997, El Paso, Texas USA

we implement a low pass filter and an Savitzky-Golay (SG) filter. To generate a

The mismatch rate of quantized IPI is approximately 15%.

4 H2B PROTOCOL DESIGN

Before we introduce the CS-based reconciliation method to correct mismatch after quantization, we review the principles of compressive sensing in this section to show the potential of implementing compressive sensing in information reconciliation protocol.

4.1 Principles of Compressive Sensing

Before we introduce the CS-based reconciliation method to correct mismatch, we review the principles of compressive sensing in this section to show the potential of implementing compressive sensing in information reconciliation protocol.

CS is an information theory [4, 29, 44] that proposes a method to recover a high dimension sparse signal from a number of measurements. Let $x \in \mathbb{R}^N$ be an unknown data vector, $y \in \mathbb{R}^M$ be a measurement vector, and $\Phi \in \mathbb{R}^{M \times N}$ be a projection matrix from a higher dimension ($N$) to a lower dimension ($M$). Here, both vector $y$ and matrix $\Phi$ are given, and the unknown vector $x$ needs to be determined. We can then write the problem in a linear form as:

$$y = \Phi x.$$  

(1)

If $M < N$, then Eq. (1) is under determined, and is impossible to be solved in a general form.

CS imposes the requirement that data vector $x$ is sparse; namely, most of the elements in $x$ are zeros. Let $\delta$ denote the number of non-zeros in $x$, then $x$ is sparse if $\delta \ll N$. $S$ in CS is termed as sparsity. CS theory states that we can recover data vector $x$ with an overwhelming probability by solving the following $\ell_1$ minimization problem:

$$\hat{x} = \arg\min_x \|x\|_1 \text{ subject to } \|y - \Phi x\|_2 < \epsilon,$$  

(2)

where $\epsilon$ is noise and provided Conditions C1 and C2 as follows.

- C1. $\Phi$ must obey the restricted isometry property (RIP). For example, $\Phi$ satisfies RIP if each element in $\Phi$ is $\pm 1$ with equal probability, i.e., symmetric Bernoulli distribution.
- C2. $M > S \times \log(N/S)$.

Note that C2 is a sufficient condition, and Wang et al. show that the necessary condition is [44]:


A symmetric cryptographic protocol requires a bit-for-bit equal key for Alice and Bob. After quantization, Alice and Bob generate the bit vectors $(x_{Alice}, x_{Bob}) \in \{0, 1\}$ respectively. However, we usually have $x_{Alice} \approx x_{Bob}$ in practice. In the context of information reconciliation, our intuition is that the mismatch between two keys $x_{Alice}$ and $x_{Bob}$ is sparse, therefore can be recovered from Eq. (2) efficiently.

4.2 Information Reconciliation Protocol with Compressive Sensing

In this section, we introduce the design and implementation of the CS-based reconciliation method to correct the mismatches between raw key generated by Alice and Bob. Figure 6 illustrates the flow-chart of information reconciliation protocol. The roles of Alice and Bob are interchangeable.

Firstly, Alice and Bob derive their own key candidate vectors $x_{Alice}$ and $x_{Bob}$ from local observation independently. Secondly, they project the vectors to lower dimension spaces (i.e., from $N$ to $M$, where $N \gg M$), with Eq. (1) respectively, namely $y_{Alice} = \Phi x_{Alice}$ and $y_{Bob} = \Phi x_{Bob}$, where $\Phi$ is a known key generation protocol parameter (i.e., a known symmetric Bernoulli matrix consisting of $\pm 1$ with equal probability). Thirdly, Alice transmits $y_{Alice}$ to Bob via an unauthenticated channel. On receiving $y_{Alice}$, Bob calculates mismatch vector $\Delta y_{A,B} = y_{Alice} \oplus y_{Bob}$ in a lower dimension space. The mismatch vector in a higher dimension space $\Delta x_{A,B} = x_{Alice} \oplus x_{Bob}$ will have approximately 15% non-zero elements only (sparse!), i.e., a small $S_{A,B}$. Furthermore, if project matrix $\Phi$ satisfies Conditions C1 and C2 in Section 4.1, $\Delta x_{A,B}$ can be
H2B: heartbeat-based secret key generation system using piezo vibration sensors

WOODSTOCK’97, July 1997, El Paso, Texas USA

Figure 6: Reconciliation protocol.

 recovered using Eq. (2) as:

\[ \Delta x_{A,B} = \underset{\Delta x_{A,B}}{\arg \min} \| \Delta x_{A,B} \|_1 \text{ subject to } \| \Delta y_{A,B} + \Phi \Delta x_{A,B} \|_2 < \epsilon. \] (3)

Finally, with \( \Delta x_{A,B} \), Bob can correct mismatches by deriving a new key \( x'_{Bob} = x_{Bob} \oplus \Delta x_{A,B} \), and \( x'_{Bob} = x_{Alice} \).

In this reconciliation protocol, the compressed key \( y_{Alice} \) is transmitted via a public channel. Assume that an attacker Eve has the full control of the public channel. She may eavesdrop and modify \( y_{Alice} \). We also assume she has the full knowledge of H2B and is able to reproduce the processing of H2B parallel with legitimate devices. Aiming at derive secret key \( x_{Alice} \), she may launch two types of attacks as follows.

**Attack 1**: Eve attempts to reconstruct \( x_{Alice} \) from \( y_{Alice} \) directly using Eq.(2).

**Attack 2**: Eve derives her own key with various attack attempts.

In Section 5.5 later, we discuss three different attack attempts in details, by which Eve derives her own key, i.e., \( y_{Eve} \). To calculate

\[ \Delta y_{A,E} = y_{Alice} \oplus y_{Eve}, \] where \( y_{Eve} = \Phi x_{Eve} \), followed by attempting to recover \( \Delta x_{A,E} \) with Eq. (3) by replacing \( \Delta x_{A,B} \) and \( y_{A,B} \) with \( \Delta x_{A,E} \) and \( y_{A,E} \), respectively, and obtain \( x_{Alice} \).

Let \( P = S_{\Delta A,B} \ast \log(N/S_{\Delta A,B}) \) and \( Q = \min(S_{Alice}, S_{AA,E}) \). We have:

**Corollary 1.** The CS-based reconciliation method is perfectly effective (i.e., Bob can recover \( \Delta x_{A,B} \) and \( x_{Alice} \) successfully) and secure (i.e., Eve is unable to recover \( \Delta x_{A,E} \) and \( x_{Alice} \) successfully) if

\[ P < M < Q \] (4)

**Proof:** If Bob cannot recover \( \Delta x_{A,B} \) and \( x_{Alice} \) with a \( \Phi \) that satisfies Condition C1 and \( M > P \), it is contradictory to Condition C2, which defines the sufficient condition for successful CS decoding with \( \ell_1 \) minimization. If Eve can recover \( \Delta x_{A,E} \) and \( x_{Alice} \) with \( M < Q \), it is contradictory to Condition C3, which defines the necessary condition for successful CS decoding with \( \ell_1 \) minimization for both Attacks 1 and 2 because \( Q \) is the minimum of \( S_{Alice}, S_{AA,E} \), which are the necessary conditions for successful \( x_{Alice} \) recoveries in Attacks 1 and 2 respectively.

The design for a CS-based reconciliation becomes a problem to find a suitable \( M \). The upper bound \( Q \) is the secure threshold and the lower bound \( P \) is the effective threshold. Assume that H2B aims to generate a 128-bit key, so \( N = 128 \) and the attack schemes includes passive and presentation attacks (see Section 5.5). Figure 7 shows the distribution of \( P \) and \( Q \). We cannot find \( M \) satisfies Corollary 4.2 perfectly. To ensure the security of the system, \( M \) is selected to be 50 so that \( M < Q \) for all possible attacks. When \( M = 50 \), there exists 4.8% cases that \( M \leq P \), implying that there is 4.8% possibility that CS-based reconciliation fails to correct all mismatch.
Among known piezoelectric sensors, PVDF piezopolymer is usually used in low-frequency applications [12, 45]. Therefore, we built data samplers using off-the-shelf PVDF piezopolymer sensors (25 × 13 × 1 mm³, US$5.6), produced by TE Connectivity². The sensor features 180 Hz resonant frequency and 50 mV/g baseline sensitivity. The frequency of heartbeat is between 0.8 and 2 Hz [35] so the heartbeat pulse can be very weak. We thereby design an amplifying circuit for the PVDF piezopolymer sensor. The data logger used is the SensorTag produced by Texas Instruments³, which features a Cortex-M4 microcontroller, and a 2.4 GHz low power radio transceiver (for both Bluetooth Low Energy and IEEE 802.15.4) on board. Piezo sensors are sampled by 12-bit Analog-to-Digital (ADC) inside Cortex-M4 so the microcontroller can access them directly. All sampling data is saved on a onboard flash memory. The prototype device is shown in Figure 8.

A coarse synchronization is needed to ensure all legitimate devices capture IPI at the same time. Synchronization of Alice and Bob is achieved using a time-slotted channel hopping-based (TSCH) [15] time synchronization mechanism⁴. With TSCH, the timers in the devices are synchronized when they join the same network.

Figure 7: Sparsity when N = 128.

We assume that an attacker Eve has the full control of the public channel, so she may modify \( y_{Alice} \) in reconciliation step. A message authentication code (MAC) method is thereby implemented to verify the message [6]. We can simply code \( y_{Alice} \) to \( L_{Alice} = \{ y_{Alice}, MAC(y_{Alice}, y_{Alice}) \} \), by treating \( x_{Alice} \) as the shared secret. On receiving \( L_{Alice} \), Bob can obtain \( x_{Alice} \) as mentioned above and also protect the integrity and the authenticity of the message via the MAC method. If the message is modified, the derived \( x_{Bob}' \) will be different from \( x_{Alice} \) so that Bob cannot produce a correct \( L_{Alice} \) value. The message is thereby discarded. The MAC method also allows Bob to examine the reconciliation results. As shown in Figure 6, Bob will notify Alice for the final result to determine whether the key generation is successful. Finally, we apply SHA2-256 hashing algorithm on the successfully generated key to further amplify privacy.

5 EVALUATION

To evaluate the performance of H2B, we built prototype wearable devices containing PVDF piezopolymer sensors. We also collected another dataset that is different from the dataset used in system design. In this section, we provide the details of prototype devices, experiments and various evaluation results.

5.1 Prototype Device

Among known piezoelectric sensors, PVDF piezopolymer is usually used in low-frequency applications [12, 45]. Therefore, we built data samplers using off-the-shelf PVDF piezopolymer sensors (25 × 13 × 1 mm³, US$5.6), produced by TE Connectivity². The sensor features 180 Hz resonant frequency and 50 mV/g baseline sensitivity. The frequency of heartbeat is between 0.8 and 2 Hz [35] so the heartbeat pulse can be very weak. We thereby design an amplifying circuit for the PVDF piezopolymer sensor. The data logger used is the SensorTag produced by Texas Instruments³, which features a Cortex-M4 microcontroller, and a 2.4 GHz low power radio transceiver (for both Bluetooth Low Energy and IEEE 802.15.4) on board. Piezo sensors are sampled by 12-bit Analog-to-Digital (ADC) inside Cortex-M4 so the microcontroller can access them directly. All sampling data is saved on a onboard flash memory. The prototype device is shown in Figure 8.

A coarse synchronization is needed to ensure all legitimate devices capture IPI at the same time. Synchronization of Alice and Bob is achieved using a time-slotted channel hopping-based (TSCH) [15] time synchronization mechanism⁴. With TSCH, the timers in the devices are synchronized when they join the same network.

Figure 7: Sparsity when N = 128.

We assume that an attacker Eve has the full control of the public channel, so she may modify \( y_{Alice} \) in reconciliation step. A message authentication code (MAC) method is thereby implemented to verify the message [6]. We can simply code \( y_{Alice} \) to \( L_{Alice} = \{ y_{Alice}, MAC(y_{Alice}, y_{Alice}) \} \), by treating \( x_{Alice} \) as the shared secret. On receiving \( L_{Alice} \), Bob can obtain \( x_{Alice} \) as mentioned above and also protect the integrity and the authenticity of the message via the MAC method. If the message is modified, the derived \( x_{Bob}' \) will be different from \( x_{Alice} \) so that Bob cannot produce a correct \( L_{Alice} \) value. The message is thereby discarded. The MAC method also allows Bob to examine the reconciliation results. As shown in Figure 6, Bob will notify Alice for the final result to determine whether the key generation is successful. Finally, we apply SHA2-256 hashing algorithm on the successfully generated key to further amplify privacy.

5.2 Experiment Design

The preliminary dataset used in system design was collected from 8 volunteers at various sampling rates (from 40 to 400Hz) for 1 minute. The test dataset for evaluation is collected from 23 volunteers at 120Hz for 5 minutes⁵. All participants wore five prototypes, as shown in Figure 1. During data collection, participants were asked to sit without any body movement.

Exploiting heartbeat data as the shared secret, performance of H2B may be sensitive to various activities. We collected data from 2 participants at 128 Hz for 10 minutes after exercises, and wakeup to evaluate the impact of different states.

5.3 Key Generation Success Rate

We benchmark the performance of the proposed CS-based reconciliation method against the state-of-the-art Error Correction Code (ECC)-based reconciliation [28, 49, 50]. The underlying ECC is selected to (15,3) Reed-Solomon (RS) code as described in [49], which is considered the best performing ECC for the information reconciliation.

The major performance metric for symmetric key generation is the probability for two independently generated keys to agree completely bit-by-bit after reconciliation, which is also referred to as key generation success rate. This is an important metric because if the keys do not match, the key generation process has to be restarted causing prolonged delays and user dissatisfaction.

<table>
<thead>
<tr>
<th>Reconciliation Method</th>
<th>Success Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS</td>
<td>0.956</td>
</tr>
<tr>
<td>RS(15, 3)</td>
<td>0.342</td>
</tr>
</tbody>
</table>

Other time synchronization methods such as Cheepsync [39] can also be used.

Ethical approval for carrying out this experiment has been granted by the corresponding organization (Approval Number HC17008).

Table 5: Success rate of H2B with different reconciliation method.

7Other time synchronization methods such as Cheepsync [39] can also be used.
8Ethical approval for carrying out this experiment has been granted by the corresponding organization (Approval Number HC17008).
Assume we want to generate a 128-bit key using H2B. 45 IPI values are required to generate a key. The success rate of CS-based reconciliation approach is 95.6% while conventional ECC-based reconciliation only has 34.2% success rate. The frequency of heartbeat is between 0.8 and 2 Hz [35] so it takes from 22.5 to 56.25 seconds to sample 45 IPI readings. A key generation attempt with 34.2% severely lacks practical usability. It is thereby necessary to implement CS-based reconciliation approach in H2B.

A key generation attempt that needs a time between 22.5 and 56.25 seconds still lacks usability, even if it has 95.6% success rate. In practice, we can schedule the sensor sampling periodically and store the latest 45 IPI readings in wearable devices. Each IPI reading contains only 3 bit information so the storage of IPI only takes 135 bit memory size. On request of key generation, H2B reads the 135-bit vector and processes the CS-based information reconciliation step to derive the final key. This can be completed in the order of milliseconds.

5.4 Impact of Different User’s States

Figures 9 and 10 show the histogram of raw IPIs within 15 minutes after user wake up and exercises respectively. Compared to the normal state in Figure 3, the mean value of raw IPIs does not change significantly after activities, but the randomness of IPI reduces. Within a short period of time after a user wakes up or finishes exercises, his heartbeat tends to be more stable than normal state and the level of heartbeat variability reduces. Quantitatively, the entropy can be extracted reduces to 2.29 bits after wakeup and 2.48 bits after exercises. By comparison, the entropy is above 2.9 bits at the normal state. To generate a 128-bit key, more IPI values are required, i.e. 56 after wakeup and 52 after exercise. On the other hand, devices still maintain proximity under different user’s states and the success rate of the final key is not influenced significantly.

5.5 Resiliency Against Attacks

H2B can be threatened from four main classes: violating confidentiality, compromising integrity or authenticity, or denying availability. Ensuring availability is out of the scope of this paper. Furthermore, wearables usually depend on short-range communication that makes availability attacks such as jamming difficult for an adversary. If short-range communication is jammed, the user can simply walk away from current location to overcome this type of attacks. We assume that attackers attempt to breach H2B by violating confidentiality and compromising integrity or authenticity.

Compromising integrity or authenticity can be prevented by implementing MAC in transmitted messages. As discussed in Section 4.2, Eve has full knowledge of the system and full control of the communication channel. She can launch an attack by submitting her own key during the information reconciliation stage. If her key has sufficient proximity with the secret key among legitimate devices, she can recover the secret key. In this section, we model three different attack schemes for Eve to derive a key: passive eavesdropping attack, active presentation attack and active video magnification attack.

We assume that all devices that can measure the heartbeat signals of a user are trustworthy. This means Eve cannot derive the real-time heartbeat signals, which directly represents the common secret. A user is assumed to be capable of detecting such attacks if an attacker tries to modify the on-body devices or place an adversary device on the user.

5.5.1 Passive Attacks. Eve attempts to pair her device with legitimate devices of a user by processing her own heartbeat data. We simulated passive attackers by mutual pairing of different participants. The evaluation on passive attackers also shows whether H2B produces distinctive keys for different users.

5.5.2 Presentation Attacks. We assume that Eve can access historical IPI data of a user. In presentation attacks, Eve attempts to pair with legitimate devices by submitting historical data. We simulated historical attacker by pairing keys generated by the same user during different times. This evaluation also shows whether the system provides forward secrecy.

Figure 11 shows the results of passive and historical attackers. The highest bit agreement rate is 70% for passive attacks and 74.17% for present attacks.

5.5.3 Video. Wu et. al. [47] developed a video magnification procedure that is capable of revealing bio-signals from a video footage of a person. The video is decomposed spatially and temporally to amplify variations occurring within a specified frequency (e.g., heart beating frequency range in our context). The technique has been employed in many applications including adult/infant heart beating tracking[17, 47]. We assume that an attacker Eve can film a video of user’s face and apply such technique to extract IPI data. She then uses the extracted IPI data to launch an active attack attempt. In our setup, a user (Alice) directly faces a video camera situated at a very close distance to produce the best IPI results, which is an unfair advantage given to Eva deliberately. A video of Alice’s face is analyzed using Eulerian Video Magnification [47] to extract...
the heart beating details as shown in Figure 12. The video frame rate is set to 30 and 120 frame per second (fps) respectively and the region of interest (ROI) is set to part of Alice’s forehead. Due to the presence of noise in the video, the amplification is applied using a narrow band filter 0.5 - 1.4 Hz as recommended in [47] for the best results, while the magnification factor was 60.

By tracking the changes in mean intensity of pixels in ROI, Eva can obtain a heartbeat curve as shown in Figure 13. The raw IPIs are extracted using a peak detection algorithm. According to [3], the magnification method for detecting heart rates is not 100% accurate as measured by ECGs and the heartbeat measured by piezo sensors is not perfectly accurate either because of measurement noise. As a result, raw IPI values produced from the video differ significantly from those produced from the piezo sensors. Such differences of IPI value estimation from different methods can be up to 30% according to our data. Therefore, the bit agreement rate of the final keys generated by the two different methods for the same person (e.g., Alice) is expected to be low.

By using the IPI values produced from the video of the Alice to pair with those produced by the piezo sensor, the agreement rate is 64.53% for 30-fps video, and 66.67% for 120-fps video respectively. This result shows that the IPI values extracted from the video do not have good proximity with those from the piezo sensors. Moreover, to process a 90 second video, the processing time is 16 minutes for the 30-fps video, and 75 minutes for the 120-fps video respectively with a computer that has 8 GB RAM and an Intel i7 processor. Therefore, the valid period of the secret key may be set to a short duration (e.g., 5 minutes) to protect against this types of attacks. All three attack attempts have 0 success rate, indicating H2B is robust to these attacks.

5.6 Power Consumption

For practical use, we present a power consumption analysis of our prototype system of H2B in this section. The power consumption of H2B can result from three parts: data sampling, data processing, and data transmission. Due to recent development in ambient backscatter communication [22, 26], the energy consumption of wireless communication is negligible compared to data sampling and processing.

5.6.1 Power Consumption in Data Sampling. In our power measurement experiment, we connect the prototype device to a GDS-800 digital oscilloscope to measure the average power consumption for each sampling event. The measurement setup is shown in Figure 14. The SensorTag was running with the latest version of Contiki OS, in which the MCU was duty-cycled to save power. Moreover, all unnecessary components, including the ADC, SPI bus, and on-board sensors were powered-off when it was possible.

The low bound of sampling rate is 120 Hz. This results in 491.55\mu W power consumption in sampling the heartbeat signal with a single device. A typical battery for SensorTag, such as Panasonic CR2032, is of 3 V, 225 mAh, equivalent as 2.43 \times 10^6 mJ. Therefore, a typical

battery can support piezo data sampling at 120 Hz for $4.96 \times 10^6$ seconds.

To benchmark the power consumption of piezo sensor-based devices against wearable ECG devices, we choose an off-the-shelf wearable ECG sensor, CardioChipâ¬¢ ECG biosensor, as a baseline. This sensor features extremely low power consumption among all wearable ECG sensors on the market. It operates at 2.5mW and prices average US$55. Piezo sensors appears to be a cost and energy-efficient solution in this system compared to wearable ECG sensors.

5.6.2 Time and Energy Consumption in CS-based Reconciliation

The most computational-intensive processing in H2B is the mismatch vector recovery using Eq. (3) in the CS-based information reconciliation. Note that the recovery needs to be executed only in one of the two devices. It enables H2B to exploit the heterogeneity of wearable IoT architecture. We may implement CS-based reconciliation method in more powerful wearable devices, such as smartphone, or smartwatch, when they try to pair with more resource-constraint devices, such as smart wristbands, or implanted medical devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Time(ms)</th>
<th>Energy(mJ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung Smartwatch</td>
<td>135</td>
<td>83.8</td>
</tr>
<tr>
<td>Google Nexus 4</td>
<td>155</td>
<td>143.2</td>
</tr>
</tbody>
</table>

We implement this method on a smartwatch, i.e. Samsung Smartwatch and a smartphone, i.e. Google Nexus 4 for energy evaluation. The suggested compression rate $\alpha$ is 45% as discussed in Section 5.6.1. Assume that the length $N$ of raw key is 128 bit, the sensing matrix $\Phi$ has the size of $58 \times 128$.

Table 6 shows the mean result of the time and energy consumption in one time CS-based reconciliation. The time and energy consumption are using a widely used opensource tool called PowerTutor\(^6\). According to the results, CS-based reconciliation takes 155 ms and 143.2 mJ at the most. B2B generates key at approximately 3 bits per second. The processing time of 155 ms for CS-based reconciliation is only a small fraction of generating time for a 128-bit key. A typical battery for smartphone, such as Google Nexus 4, is of 3.8 V, 2100 mAh, equivalent as 2.9 $\times$ 10$^7$ mJ. Let us assume that a user make H2B run for 24 hours and generate key every 5 minutes. The energy consumed by CS-based reconciliation is 0.09% of the total energy in Google Nexus 4 only.

6 CONCLUSION

In this paper, we studied the key potential of piezo-based IPI and found out 2.9 bits entropy can be extracted from each IPI. The study also reveals that piezo-based IPI suffers from high mismatch rate, which reduces the success rate of key generation. To this end, we apply an inverted cumulative distributed function(ICDF)-based quantization method to fully extract entropy and propose a novel Compressive Sensing(CS)-based reconciliation protocol to overcome high mismatch rate key. Our evaluation results shows that CS-based reconciliation method can improve the success rate of the proposed system from 34.2% to 95.6% compared to the state-of-the-art reconciliation method. We further demonstrate that the system is robust against three types of attacks and is more energy-efficient compared to off-the-shelf wearable ECG system.

REFERENCES


