Practical Privacy-Preserving ECG-Based Authentication for IoT-Based Healthcare

Pei Huang, *Student Member, IEEE,* Linke Guo, *Member, IEEE,* Ming Li, *Member, IEEE,* and Yuguang Fang, *Fellow, IEEE*

***Abstract*—In current healthcare systems, patients use various types of medical Internet of Things devices for monitoring their health conditions. The collected information (personal health records) will be sent back to hospitals for diagnosis and quick responses. However, severe security and privacy leakages with regard to data privacy and identity authentication are incurred because the monitored health data contains sensitive information. Therefore, the data should be well protected from unauthorized entities. Unfortunately, traditional cryptographic approaches or password-based mechanisms cannot fulfill the privacy and security demands in health monitoring due to their low efficiency and knowledge-based property. Biometric authentication overcomes these deficiencies and successfully verifies the inherent characteristics of humans. Among all biometrics, the electrocardiogram (ECG) signal is the most suitable one due to its medical properties. However, the security and privacy objectives of ECG-based authentication usually fail in practice due to the noise interferences in the collected ECG data and the privacy breach of the ECG database. In this paper, we propose a practical scheme that can reliably authenticate patients with noisy ECG signals and provide differentially private protection simultaneously. The effectiveness and efficiency of our scheme are thoroughly analyzed and evaluated over online datasets. We also conduct a pilot study on human subjects experiencing different exercise levels to validate our scheme.**

***Index Terms*—Authentication, biometrics, eHealth.**

I. Introduction

THE AGING population and prevalence of chronic diseases have led to high demand for long-term in-home health monitoring. With the rapid development of sensing technology, intelligent health monitoring Internet of Things (IoT) devices, such as electrocardiogram (ECG) patch, blood pressure band, pulse oximeter, etc., can collect health data and provide real-time feedback to patients and hospitals, either as a warning of impending medical emergency or as a monitoring aid during exercises [1]. In particular to this IoT-based healthcare, health data is considerably sensitive because it reveals inherent characteristics of patients. According to the Health Insurance Portability and Accountability Act (HIPAA), patient health records (PHRs) should be encrypted before releasing [2]. Besides, the access to health data should also be restricted to unauthorized entities. However, traditional methods only verify "what you possess" (e.g., an ID card) or "what you remember" (e.g., a password) to authenticate individuals, and conventional cryptographic approaches on protecting data privacy are not efficient [3], especially for the case of emergency.

Biometric authentication, which overcomes the above drawbacks and verifies "who you are" [4], has been extensively studied and enabled current state-of-the-art biometric systems to accurately recognize individuals based on biometric trait, such as face, iris, fingerprint, voice, and gait, acquired under controlled environmental conditions from patients [5]. Biometrics are inherent to humans and unique among individuals, so they can be used to authenticate patients with small probability of forging identities. However, most biometrics, such as fingerprint, face, or iris, have the following drawbacks: 1) extra sensors other than sensors for medical monitoring purpose are acquired; 2) less help on medical diagnosis; and 3) easily get lost or stolen, all of which prevent them from being deployed in medical environments. Therefore, the ECG signal is a more suitable choice in practical applications. Suppose that a patient Alice has chronic diseases requiring long-term monitoring. A medical IoT for ECG monitoring is equipped to collect her ECG signal daily, especially during exercise, for timely emergency detection. Since her ECG signal is already acquired during the monitoring, it is convenient for her to authenticate herself with her ECG signal. Therefore, the security improvement and medical data diagnosing can be fulfilled simultaneously.

Nevertheless, the requirement for controlled environmental conditions in biometric authentication is contradictory to the properties of the IoT-based health monitoring. During the long-term monitoring, which should work all the time to detect any health emergency timely, the environmental condition is changing due to patients' mobility. The ECG signal monitoring during exercises, when most chronic heart diseases take place, is especially important. However, existing schemes [6]–[8] only deal with online datasets or resting ECG signals, while the ECG signals in real situations are usually contaminated by

Manuscript received March 25, 2019; revised May 28, 2019; accepted June 30, 2019. Date of publication July 16, 2019; date of current version October 8, 2019. The work of L. Guo was supported in part by the National Science Foundation under Grant IIS-1722731 and Grant ECCS-1710996. The work of M. Li was supported in part by the National Science Foundation under Grant ECCS-1849860 and Grant CNS-1924463. The work of Y. Fang was supported in part by the National Science Foundation under Grant IIS-1722791. *(Corresponding author: Linke Guo.)*

P. Huang and L. Guo are with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634 USA (e-mail: peih@clemson.edu; linkeg@clemson.edu).

M. Li is with the Department of Computer Science Engineering, University of Texas Arlington, Arlington, TX 76010 USA (e-mail: ming.li@uta.edu).

Y. Fang is with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: fang@ece.ufl.edu).

Digital Object Identifier 10.1109/JIOT.2019.2929087

noise and artifacts, such as muscle movement and patch displacement when the patient is moving. The authentication and diagnosis cannot be successfully performed with noisy ECG signals. On the other hand, the secrecy protection of ECG signals is also problematic while it is pivotal in preventing adversaries from stealing or forging a legitimate patient's ECG signal and breaking into her medical records [9]. The highly sensitive property of ECG signals (e.g., revealing illness) further magnifies the significance of privacy preservation.

Contributions: To overcome the above limitations, we propose a scheme, that is able to authenticate patients with noisy ECG signals while ensuring the privacy of stored templates. Our contributions are summarized as follows.

1) The proposed ECG-based authentication is reliable even with noisy inputs. The noise detection and elimination are real time. Thus, the application of ECG-based authentication becomes more practical than ordinary ones for daily use, especially for long-term health monitoring.
2) The most common daily exercises, i.e., walking, running, and jumping, are included. Our scheme can detect the motions and adapt the algorithm according to current moving status.
3) The privacy of ECG templates is protected by providing indistinguishability. The sensitivity of ECG signals is considered while the authentication accuracy is preserved after optimized privacy enhancement.
4) Our scheme is tested on signals with real world noises instead of artificially added noises.

II. Preliminaries

A. Basic Features, Noise, and Artifacts in the ECG Signal

The ECG signal is an electrical signal reflecting the electrophysiologic patterns of the human heart muscles when the heart is depolarizing and repolarizing. Different ECG signals conform to a similar fundamental morphology, while exhibiting personalized traits, such as relative timing of the various peaks, beat geometry, and responses to stress and activity [10]. The personalized traits are distinctive among human subjects and can be quantified in time domain and frequency domain. Thus, the human identity authentication is enabled via ECG signals. As illustrated in Fig. 1(a) and (b), a typical ECG complex consists of various fiducial components, such as P wave, PR interval, QRS complex, J point, ST segment, and T wave. The QRS complex is the most recognizable and unique part of a ECG signal, which is frequently utilized for feature extraction in human authentication [11].

In practice, ECG-based authentication may far from being accurate because ECG recording is always contaminated by noise and artifacts. The actual personal traits are hard to be directly detected in noisy ECG signals, so the authentication process fails if using the inaccurate features. The most common high-amplitude ECG noises [12] that cannot be removed by simple in-band filtering are electromyogram (EMG) signal interference, baseline wander (BW), muscle artifact, and electrode movement. The ECG signals recorded during exercises

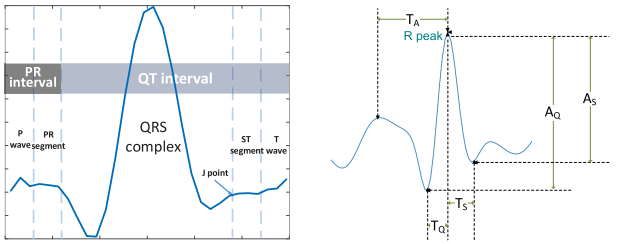


Fig. 1. ECG waveforms. (a) Typical ECG complex. (b) Features.

are contaminated by unwanted signal components with greater energy.

B. Singular Value Decomposition

How to recover and conduct feature extraction from a noisy ECG record is quite challenging. Singular value decomposition (SVD) [13] is a method to decompose orthonormalized eigenvectors from the input matrix, which holds the fundamental features of the input and separate orthogonal components in the input.

Definition 1: Let $\boldsymbol{A}$ be a real $m \times n$ matrix with $m \geq n$, then $\boldsymbol{A} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^T$, where $\boldsymbol{U}^T\boldsymbol{U} = \boldsymbol{V}^T\boldsymbol{V} = \boldsymbol{V}\boldsymbol{V}^T = \boldsymbol{I}_n$, $\boldsymbol{\Sigma} = \text{diag}(\sigma_1, \ldots, \sigma_n)$. The matrix $\boldsymbol{U}$ consists of n orthonormalized eigenvectors associated with the n largest eigenvalues of $\boldsymbol{A}\boldsymbol{A}^T$, and the matrix $\boldsymbol{V}$ consists of the orthonormalized eigenvectors of $\boldsymbol{A}^T\boldsymbol{A}$. The diagonal elements of $\boldsymbol{\Sigma}$ are the non-negative square roots of the eigenvalues of $\boldsymbol{A}^T\boldsymbol{A}$; they are called singular values, which are assumed to be: $\sigma_l \geq \sigma_2 \geq \cdots \geq \sigma_n \geq 0$. Thus, if $\text{rank}(\boldsymbol{A}) = r$, $\sigma_{r+1} = \sigma_{r+2} = \cdots = \sigma_n = 0$.

C. Differential Privacy

Traditional cryptographic methods are burdensome to protect ECG signals and the encrypted ECG signals can hardly be used for diagnosis. Hence, we introduce differential privacy as defined in [14], which is first defined on databases. Databases D_1 and D_2 differ in at most one element if one dataset is a proper subset of the other and the larger database contains just one additional row.

Definition 2 (Differential Privacy): A randomized function $\mathcal{K}$ gives ϵ-differential privacy if for all data sets D_1 and D_2 differing on at most one element, and all $S \subseteq \text{Range}(\mathcal{K})$

$$\Pr[\mathcal{K}(D_1) \in S] \leq \exp(\epsilon) \times Pr[\mathcal{K}(D_2) \in S]. \quad (1)$$

The probability is taken is over the coin tosses of $\mathcal{K}$.
Thus, the risk of privacy leakage increased after this element participating in a database is bounded by $\exp(\epsilon)$. The differential privacy with privacy budget ϵ is named as $(\epsilon, 0)$-differential privacy.

The Laplace mechanism is a basic differential privacy mechanism, which adds Laplace-distributed noise variables to the query result.

Definition 3 (The Laplace Mechanism): Given any function $f : \mathbb{N}^{|\mathcal{X}|} \rightarrow \mathbb{R}^k$, the Laplace mechanism is defined as

$$M_L(x, f(), \epsilon) = f(x) + (Y_1, \ldots, Y_k) \quad (2)$$

TABLE I
NOTATIONS AND DEFINITIONS

Notation	Definition
$\boldsymbol{M}$	a 2-D matrix containing inputs from ECG channels
$\mathcal{M}_h$	the h-th row/channel in $\boldsymbol{M}$
$\mathcal{M}_v^T$	the v-th column/sample input in $\boldsymbol{M}$
$m_{i,j,h}$	the i-th element in the j-th segment of $\mathcal{M}_h$
$\widehat{\boldsymbol{M}}, \widetilde{\boldsymbol{M}}$	the denoised and perturbed version of $\boldsymbol{M}$
H, N	the channel number, sampling time duration for $\boldsymbol{M}$
T_S, T_Q, T_A	fiducial features regarding time durations
A_S, A_Q	fiducial features regarding amplitudes
$\boldsymbol{U}, \boldsymbol{V}, \boldsymbol{\Sigma}$	singular vector decomposition representation
A, ν	acceleration and speed for motion detection
$\mathbb{K}_h$	the divergence between two ECG signals on channel h
$\mathbb{K}$	the overall divergence between ECG inputs and ECG template
$\mathcal{C}, \widetilde{\mathcal{C}}$	the Legendre polynomial fitting coefficients of $\mathcal{M}_{j,h}$, $\widetilde{\mathcal{M}}_{j,h}$
$\mathring{\mathcal{C}}$	the fitting coefficients after soft thresholding

where Y_i are independent identically distributed random variables drawn from $\text{Lap}(\Delta f/\epsilon)$.

The query result returned to the requester is a perturbed one based on the ground truth $f(x)$. This mechanism preserves $(\epsilon, 0)$-differential privacy.

D. Notations

For clarity, we use different font styles to describe matrices, vectors, and elements, which are the bold type, the calligraphic type, and the normal one, respectively. An example is listed in Table I, together with some other notations appear in this paper and their corresponding definitions.

III. ECG-Based Authentication in Noisy Environments

A. Overview

Fig. 2 demonstrates how our authentication system captures features, generates templates, and successfully authenticates patients even when the input signals are contaminated by noises. A patient's ECG signals are first obtained using a wearable ECG acquisition module and then transmitted to a processing device via wireless communication channel (e.g., Bluetooth). After receiving the signals, the device applies SVD to de-noise the signal. The features are then extracted and stored as templates in the device as well as in the hospital's database. Later, when the patient requests for her health data, an authentication request is issued to the device and the hospital. Her ECG signals and other data from motion sensors are recorded. Her motion will be inferred from sensors and her ECG signals are de-noised according to the detected motion status. Features are then extracted from the de-noised signals concurrently and transmitted securely to the device and hospital. They will be compared with templates to verify the patient's identity.

B. Attack Model and Challenge

ECG signals and their features can be captured and stored for indefinite amount of time. Given enough accurate features, it is possible to reconstruct the desired ECG signal at a later time. Eberz *et al.* [15] generated synthetic ECG signals from feature distributions to launch attacks against ECG biometrics.

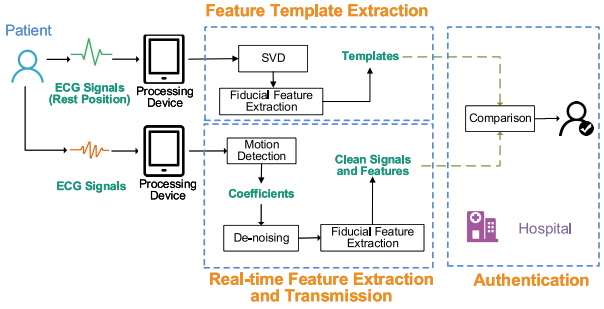


Fig. 2. System architecture.

In our model, the attacker intends to access the patient's data without stealing the patient's ECG template directly. Therefore, the adversary tries to infer a patient's ECG feature statistics from the template database. This attacker is physically outside the hospital, but he can query the ECG template database stored at the hospital and get the distribution of ECG statistics. A simple example is that he gets the distribution for all patients' templates for the first query, and he retrieves the distribution after making a query to the dataset without patient Alice at the next time. By subtraction, the attacker knows Alice's features. Hence, based on a number of intermediate querying results, the attack can aggregate results and successfully infer Alice's ECG information. This kind of inference attack on databases is extremely common. Finally, the attacker reproduces Alice's ECG signal and pretends to be Alice by authenticating himself with the acquired ECG information.

The challenge in blocking this kind of attackers is how to carefully protect the privacy of templates as well as their statistics, so that the inferred ECG signal will not be validated while the template still provides enough information for Alice to authenticate herself.

C. Template Acquisition and Training

Assume that the ECG acquisition module allows H independent signal channels for inputs. For clarity, we use different font styles to describe matrices, vectors, and elements, which are the bold type, the calligraphic type, and the normal one, respectively (e.g., $\boldsymbol{M}$, $\mathcal{M}_h$, and $m_{i,j,h}$).

1) Data Recording and Training: The patient stays in a rest position while recording her ECG signal and the entire data is recorded as a $H \times N$ matrix $\boldsymbol{\Omega}$, which has H ECG channels and the signal in each channel is sampled for N times. Since the data is recorded during rest position with negligible noise interference, the signal can be directly decomposed with SVD to train singular vectors for signal and noise separation: $\boldsymbol{\Omega} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^T$, where $\boldsymbol{\Sigma}$ is a diagonal matrix whose diagonal entries are the singular values of $\boldsymbol{\Omega}$. Both $\boldsymbol{U}$ and $\boldsymbol{\Sigma}$ are saved for further noise elimination.

2) Fiducial Feature Extraction: After obtaining the eigenvalues, R peak locations are first detected and the signals are segmented with a window with size W centering at R peaks. After truncation, the remaining signals are denoted as $\boldsymbol{M}$. $\mathcal{M}_{j,h}$ is the jth segment on the hth channel in $\boldsymbol{M}$. The locations of R peaks $\text{loc}(R)_{j,h}$ in each $\mathcal{M}_{j,h}$ are marked to synchronize signals for authentication. The fiducial features that we plan

to select from one segment are described in Fig. 1(b). When processing $\mathcal{M}_{j,h}$, all features from the last segment $\mathcal{M}_{j-1,h}$ are updated as following.

1) *Average Activation Time $T_A^{j,h}$:* The average time length from the peak of P waves, which are the local maximum before a R peak, to R peaks

$$T_A^{\text{new}} = \text{loc}(R)_{j,h} - \text{loc}\big(\max V\big[0 : \text{loc}(R)_{j,h}\big)\big)$$
$$T_A^{j,h} = \Big[(j-1)T_A^{j-1,h} + T_A^{\text{new}}\Big]\Big/ j.$$

2) *Average QR Duration $T_Q^{j,h}$ and Amplitude $A_Q^{j,h}$:* $T_Q^{j,h}$ is the average time length from the first minimum points before R peaks (locate in Q waves) to R peaks, and $A_Q^{j,h}$ is the average difference between their amplitudes

$$T_Q^{\text{new}} = \text{loc}(R)_{j,h} - \text{loc}(\min V\big[0 : \text{loc}(R)_{j,h}\big)$$
$$T_Q^{j,h} = \Big[(j-1)T_Q^{j-1,h} + T_Q^{\text{new}}\Big]\Big/ j$$
$$j \times A_Q^{j,h} = (j-1)A_Q^{j-1,h} + V(R)_{j,h} - V(Q)_{j,h}.$$

3) *Average RS Duration $T_S^{j,h}$ and Amplitude $A_S^{j,h}$:* $T_S^{j,h}$ is the average time duration from R peaks to the first minimum points after R peaks (locate in S waves), and A_S^t is the average difference between their amplitudes

$$T_S^{\text{new}} = \text{loc}(\min V[\text{loc}(R)_{j,h} : W]) - \text{loc}(R)_{j,h}$$
$$T_S^{j,h} = \Big[(j-1)T_S^{j-1,h} + T_S^{\text{new}}\Big]\Big/ j$$
$$j \times A_S^{j,h} = (j-1)A_S^{j-1,h} + V(R)_{j,h} - V(S)_{j,h}.$$

D. Authentication in Noisy Environments

In practice, the patient is usually moving while authenticating with backend servers. Therefore, we propose a solution for patients under light exercise level to accomplish successful authentication. The "light exercise level" here is defined as: ECG signals are contaminated by noises so that the morphology of the ECG signals is distorted in time domain and fiducial features are hard to be directly extracted from signals. The muscle movement, patch displacement, and heart rate changes are the main contributions. However, the exercise level is not too high to produce destructive changes (e.g., lost of R peaks) to ECG signals. A typical example of light exercise level is walking, where the user's heart rate is slightly boosted and the chest is experiencing moving so the patch may be distached from the chest bursty.

1) Motion Detection: Our ECG monitor is a portable one worn on waists or arms with embedded accelerometer and gyroscope. Accelerometer (e.g., on x-axis) measures the sum of acceleration and gravity component, $D_{\text{acl}}(x) = A(x) + \text{grav}(x)$, and angle rotation data from gyroscope (e.g., on x-axis) is denoted as $D_{\text{gyr}}(x)$. The linear acceleration and velocity are easy to get by subtracting the gravity component, but angular velocity needs a complementary filter [16] to take the advantage of both sensors' properties. The linear accelerations, linear velocity, and the angle velocity on x-axis at time t are calculated as

$$A_{\text{lin}}^t = \sqrt{A^2(x) + A^2(y) + A^2(z)}$$
$$v_{\text{lin}}^t = A_{\text{lin}}^t \Delta t + v^{t-1}$$
$$v_{\text{ang}}^t(x) = \frac{d\Big[\alpha' \arctan\Big(\frac{A(x)}{\sqrt{A(y)^2 + A(z)^2}}\Big)\Big]}{dt} + (1-\alpha')D_{\text{gyr}}(x)$$

where α' is a parameter that balance the data from accelerometer and gyroscope to produce accurate angle velocity.

The angle velocities on y and z axes, $v_{\text{ang}}^t(y)$ and $v_{\text{ang}}^t(z)$, are calculated in the similar way as $v_{\text{ang}}^t(x)$. The angle degrees at time t are also known given velocities. According to acceleration, velocities, and angle degrees, the motions are categorized into walking, running, and jumping, which are the most common exercises in daily life. In general, running has higher speed on XY plane than walking and jumping. Using angular information alone is hard to distinguish between walking and running, but it can help us tell them from rest positions, such as sitting and lying, because walking and running involve more vigorous muscle activities [17]. Then, we take advantage of the gravity component $\text{grav}(z)$ to separate running from jumping, since the locations of people's arms/waists when jumping are higher than when running. Finally, we calculate the angle degrees in case that it is misclassified as other exercises when the patient is moving her arm during rest positions.

2) Motion-Aware Noise Elimination: If the patient's motion is detected and classified, the input ECG signal $\boldsymbol{M}'$ is supposed to be contaminated with unwanted signal components. As the noise space is time-orthogonal to ECG signal space, the singular values of signal space is stable, so the noises in the input can be easily discarded by reconstructing ECG signal from the stored $\boldsymbol{U}$ and $\boldsymbol{\Sigma}^2$ for $\boldsymbol{M}'$

$$\mathcal{S}' = \boldsymbol{U}^T\boldsymbol{M}', \quad \widehat{\mathcal{S}'} = [s_1' \cdots s_r' 0 \cdots 0], \quad \widehat{\boldsymbol{M}'} = \boldsymbol{U}\widehat{\mathcal{S}'}$$

where $\mathcal{S}'$ is divided into $\widehat{\mathcal{S}}$ and $\bar{\mathcal{S}}$ corresponding to the signal and the noise subspaces. The ECG signal is recovered from signal subspace as $\widehat{\boldsymbol{M}'}$.

However, directly applying SVD for reconstruction cannot eliminate noises efficiently due to the variability of ECG signals and motions. We also have to wait for the entire input matrix before denoising while motions may only happens in a short period during input. Therefore, we propose a weighted online SVD to let the algorithm automatically adapt to the variations.

According to the definition of SVD, $\boldsymbol{\Sigma}^2$ can be reformulated as $\boldsymbol{U}^T\boldsymbol{M}'\boldsymbol{M}'^T\boldsymbol{U}$. In our scheme, this eigenvalue-related matrix will be updated along with $\boldsymbol{U}$ when more authentication data moves in. During the authentication, we deploy Jacobian transformation to eliminate off-diagonal elements in $\boldsymbol{\Sigma}^2$ after receiving every signal sample to catch its precise features and adapt itself to new incoming ECG signals. To balance the template and incoming data, different weights are assigned with respect to motion status. The effect of newly sampled signals is relatively less important for more violent activities with smaller weight β given the fact that they are more heavily contaminated. The procedure is summarized in Algorithm 1, where $\boldsymbol{U}_v$, $\mathcal{S}_v'$, and $\boldsymbol{Q}_v$ are the eigenvectors, subspace matrix, and the Jacobian rotation matrix, [18] updated after receiving the vth input vector $\mathcal{M}_v'^T$ and $\alpha + \beta = 1$. After the training process, the close approximation of $\boldsymbol{\Sigma}^2$ is $\boldsymbol{Q}_N^T(\alpha\boldsymbol{\Sigma}_{N-1}^2 + \beta\mathcal{S}_N\mathcal{S}_N^T)\boldsymbol{Q}_N$, which will stored with other training results, including $\boldsymbol{U}_N$.

Algorithm 1 Motion-Aware De-Noising of ECG Signals

Initialization: $\boldsymbol{U}_0 = \boldsymbol{U}$, $\boldsymbol{\Sigma}_0^2 = \boldsymbol{\Sigma}^2$,$i = 0$
while $v \leq N$ **do**
  $v = v + 1$
  $\mathcal{S}_v = \boldsymbol{U}_{v-1}^{\mathrm{T}} \mathcal{M}_v'^{\mathrm{T}}$
  Update motion status. Assign α and β according to current motion status.
  $\boldsymbol{\Sigma}_v^{2\prime} = \alpha \boldsymbol{\Sigma}_{v-1}^2 + \beta \mathcal{S}_v \mathcal{S}_v^{\mathrm{T}}$
  $\boldsymbol{\Sigma}_v^2 = \boldsymbol{Q}_v^{\mathrm{T}} \boldsymbol{\Sigma}_v^{2\prime} \boldsymbol{Q}_v$
  $\boldsymbol{U}_v = \boldsymbol{U}_{v-1} \boldsymbol{Q}_v$
  $\widehat{\mathcal{S}}_v$=$[s_{v,1} \cdots s_{v,r} 0 \cdots 0]$, $\bar{\mathcal{S}}_v$=$[0 \cdots 0 s_{v,r+1} \cdots s_{v,r+n}]$
  Recover ECG signals as $\widehat{\mathcal{M}}_v' = \boldsymbol{U}_v \widehat{\mathcal{S}}_v$
end while
return $\widehat{\boldsymbol{M}}'$

3) Feature Extraction and Authentication: At each sampling time t, the system de-noises the ECG samples and finds out the needed fiducial features T_A, T_S, T_Q, A_S, and A_Q by detecting the maximum point (R peak) and nearby local maximum/minimum points. These fiducial features are computed and the signal is truncated in the same way as when training template. Meanwhile, each sample in the latest segments is compared with the template $\boldsymbol{M}$ without delay. The features are updated after each segment.

To quantify the segment comparison results for authentication, we leverage the concept of Kullback–Leibler divergence [19], which measures the similarity between two ECG signal segments. To avoid the drift between the template and inputs, the divergence computation starts after the detected R peaks in segments are synchronized with those in the template. At each sample time in the jth segment of the hth channel, $t \in [\mathrm{loc}_{R_j} - W/2, \mathrm{loc}_{R_j} + W/2]$, the divergence $\mathbb{K}_h$ is updated

$$t\mathbb{K}_h^t = (t-1)\mathbb{K}_h^{t-1} + \sum_i \left| m_{i,j,h} \log \frac{m'_{i,j,h}}{m_{i,j,h}} \right|. \tag{3}$$

The overall divergence is computed as the average over all channels

$$\mathbb{K}^t = \frac{\sum_{h=1}^{H} \mathbb{K}_h^t}{H}.$$

The authentication request is successful if $\mathbb{K}$ is below a threshold. Otherwise, the fiducial features will be compared with the template features. This patient is rejected if the distances between each pair of features exceeds a bound, but will be accepted as the features are close to the template.

IV. Privacy Enhancement

Now the patient is able to authenticate herself with her ECG signals, but the template signal and features are exposed to inference and reproduction attacks. In this section, we show how to statically protect the privacy of templates in the database via differential privacy without intolerably distorting authentication accuracy.

Before the privacy enhancement scheme, we use Legendre polynomials fitting [20] to preprocess ECG signals so that ECG signals are efficiently represented and compressed. Each channel in the template is matched with high order Legendre polynomials [21]. For the ease of description, our scheme is illustrated on a single channel. The Legendre differential equation [22] can be expressed as

$$\frac{d}{dx}[(1-x^2)\frac{d}{dx}p_n(x)] + n(n+1)p_n(x) = 0.$$

Solutions for Legendre differential equations when $n = \{0, 1, 2, \ldots, \kappa\}$ form a polynomial sequence called Legendre polynomials, which are denoted by $p_n(x)$. Suppose that the location of the first R peak in the template is in line with $x = 0$, then the κ-degree equation used for fitting data is given as

$$y(x) = \sum_{r=1}^{k'} \left[c_{0,r} + \sum_{1}^{\kappa} c_{i,r} p_i(x - \mathrm{loc}(R)_r) \right]. \tag{4}$$

A. Basic Design

Given a template matrix $\boldsymbol{M}$, the algorithm first uses $k'(\kappa+1)$ polynomial coefficients to fit a single channel with k' segments in the template. Since each segment is compared independently, we denote the coefficients for one segment as $\mathcal{C}_{j,h} = \{c_{0,j,h}, c_{1,j,h}, \ldots, c_{\kappa,j,h}\}$. Then, the Laplace noise $\mathrm{Lap}(\lambda)$ is applied to $\mathcal{C}_{j,h}$

$$\Pr(\mathrm{Lap}(\lambda) = x) = \frac{1}{2\lambda} e^{-\epsilon|x|/\lambda} \tag{5}$$

whose mean is 0 and variance is $2\lambda^2$. The noises added to $\mathcal{C}_{j,h}$ is denoted as $\mathrm{Lap}^{\kappa}(\lambda)$ and the perturbed outputs are $\widetilde{\mathcal{C}}_{j,h} = \mathrm{Lap}^{\kappa}(\lambda) + \mathcal{C} + j, h$. Finally, the algorithm computes the noisy signal segments $\widetilde{\mathcal{M}}_{j,h}$ from the fitting equation $\tilde{m}_{i,j,h} = \tilde{c}_{0,j,h} + \sum_{k=1}^{\kappa} \tilde{c}_{k,j,h} p_{k,j,h}(x - \mathrm{loc}(R)_{j,h})$.

1) Privacy Level: The privacy level achieved by the technique of differential privacy depends on the sensitivity of the data query. In our scenario, the query result for data is the set of Legendre polynomial coefficients. Therefore, the sensitivity of the Legendre polynomial fitting is defined as the maximum amount, the fitting coefficients can change when the ECG signal in that channel changes, which is much smaller than simply applying differential privacy to each signal sample. According to the definition of differential privacy, we use the Manhattan distance, $|\mathcal{C} - \mathcal{C}'|$, to measures the distances between two fitting coefficient vectors $\mathcal{C}$ and $\mathcal{C}'$.

Definition 4 (Legendre Polynomial Fitting Query Sensitivity): Denote the fitting query to one ECG segment in channel $\mathcal{M}_h$ is $\mathrm{LPoly}(\mathcal{M}_{j,h})$ and its result is $\mathcal{C}_{j,h}$. The Manhattan sensitivity of any query LPoly to one segment is the maximum distance of changing $\mathcal{M}_{j,h}$ to $\widetilde{\mathcal{M}}_{j,h}$

$$\begin{aligned} \Delta(L) &= \max \left| \mathrm{LPoly}(\mathcal{M}_{j,h}) - \mathrm{LPoly}_i(\widetilde{\mathcal{M}}_{j,h}) \right| \\ &= \max \left| \mathcal{C}_{j,h} - \widetilde{\mathcal{C}}_{j,h} \right|. \end{aligned}$$

The sensitivity bounds the drift in results of each query. For a query LPoly, the achieved privacy level is $\epsilon = \Delta(L)/\lambda$. Then, the problem of guaranteeing privacy while protecting accuracy turns into restricting the changes in fitting results and deciding a proper parameter λ. According to the query sensitivity, we define the privacy level of our algorithm as

Theorem 1: The results $\widetilde{\mathcal{M}}_{j,h}$ of our perturbation algorithm is ϵ-differentially private, where $\epsilon = [\Delta(L)/\lambda]$.

Proof: The coefficients obtained by adding Laplace noises $\mathrm{Lap}(\lambda)$ is ϵ-differentially private, and $\widetilde{\mathcal{M}}_{j,h}$ is reconstructed from coefficients, so it also follows ϵ-differentially privacy. ■

2) Accuracy Analysis: The accuracy of our perturbation algorithm is inversely represented by the faulty noisy query results. The results could be inaccurate due to the loss due to the approximate fitting and negative effects of the added noise. We define several metrics to quantify the accuracy as follows.

Definition 5 (Approximation Loss): The approximation loss is the loss of Legendre fitting with order $\kappa+1$ and more. The loss is the sum of amplitude differences between original ECG samples in segment $\mathcal{M}_{j,h}$ and the samples from signals reconstructed from Legendre polynomial coefficients

$$\mathrm{Loss}_{j,h} = \left| \mathcal{M}_{j,h} - \left[c_{0,j,h} + \sum_{k=1}^{\kappa} c_{k,j,h} p_{k,j,h}(x - \mathrm{loc}(R)_{j,h}) \right] \right|. \tag{6}$$

Definition 6 (Expected Negative Effect on Accuracy): Suppose that the distribution of noise follows $\mathbb{F}$, we formulate the expected deviation and the error probability of coefficients as the expected negative effects. The expected deviation neg_1 is the expected standard deviation between perturbed coefficients and original ones. The error probability neg_2 is the count of perturbed coefficients that exceed a threshold averaging over the polynomial degree

$$\begin{aligned}
\mathrm{neg}_1(\mathbb{P}(\mathcal{C}_{j,h})) &= \sqrt{\sum_{k=0}^{\kappa} \mathbb{E}_{\mathbb{F}} \left| c_{k,j,h} - \tilde{c}_{k,j,h} \right|^2} \\
\mathrm{neg}_2(\mathbb{P}(\mathcal{C}_{j,h})) &= \frac{\mathbb{E}_{\mathbb{F}} \mathrm{count}\left[\left| c_{k,j,h} - \tilde{c}_{k,j,h} \right| \geq \gamma \right]}{\kappa+1} \\
&= \Pr\left[\left| c_{k,j,h} - \tilde{c}_{k,j,h} \right| \geq \gamma \right].
\end{aligned}$$

Theorem 2: As $\lambda = [\Delta(L)/\epsilon]$, the expected negative effect of our algorithm is

$$\begin{aligned}
\mathrm{neg}_1(\mathbb{P}(\mathcal{C}_{j,h})) &= \sqrt{\kappa+1}\lambda \\
\mathrm{neg}_2(\mathbb{P}(\mathcal{C}_{j,h})) &= 1 - \frac{1}{2}\left[\exp\left(\frac{\gamma}{\lambda}\right) - \exp\left(\frac{-\gamma}{\lambda}\right) \right].
\end{aligned}$$

Proof: According to differential privacy's properties

$$\begin{aligned}
\mathrm{neg}_1(\mathbb{P}(\mathcal{C}_{j,h})) &= \sqrt{\sum_{k=0}^{\kappa} \mathbb{E}_{\mathbb{F}} \left| c_{k,j,h} - \tilde{c}_{k,j,h} \right|^2} \\
&= \sqrt{\sum_{k=0}^{\kappa+1} \mathbb{E}|\mathrm{Lap}(\lambda)|^2} = \sqrt{\sum_{k=0}^{\kappa+1} \lambda^2} = \sqrt{\kappa+1}\lambda. \\
\mathrm{neg}_2(\mathbb{P}(\mathcal{C}_{j,h})) &= \Pr\left[\left| c_{k,j,h} - \tilde{c}_{k,j,h} \right| \geq \gamma \right] \\
&= 1 - \left[\int_{-\infty}^{\gamma} \mathrm{Lap}(\lambda)(x)dx - \int_{-\infty}^{-\gamma} \mathrm{Lap}(\lambda)(x)dx \right] \\
&= 1 - \frac{1}{2}\left[\exp\left(\frac{\gamma}{\lambda}\right) - \exp\left(\frac{-\gamma}{\lambda}\right) \right].
\end{aligned}$$

■

Obviously, the choice of Legendre polynomial order attributes to the approximate loss, and the negative metrics are related to the choice of λ and the degree of polynomial fitting, where λ involves the query sensitivity $\Delta(L)$. To formally analyze the deviations, we assume all constituent sensitivity to be 1 as in [23], so $\Delta(L) = \kappa + 1$.

B. Extended Design

1) Observation: From the analysis above, we can show that the usefulness of the template is violated because the deviations are supremely large with a big κ. To reduce noises, we import an existing noise reduction approach, soft thresholding [24] with a threshold τ_θ, to constrain a coefficient $\tilde{c}_i$ in $\widetilde{\mathcal{C}}$ as c_i

$$c_i = \begin{cases} \tilde{c}_i - \tau_\theta, & \tilde{c}_i > \tau_\theta \\ \tilde{c}_i, & -\tau_\theta \leq \tilde{c}_i \leq \tau_\theta \\ \tilde{c}_i + \tau_\theta, & \tilde{c}_i < -\tau_\theta. \end{cases} \tag{7}$$

The principle behind is that the noises added to small coefficients are usually much larger than the coefficients of themselves, but the perturbed coefficients are still comparably small, so regulating them to zeros will make perturbed coefficients less noisy [25]. As for those important large coefficients, it cuts down the values of added noises to confine the drifts. The threshold τ_θ should be related to privacy budget and do not compromise the achieved differential privacy.

2) Noise Smoothing for Privacy Enhancement: The goal of soft thresholding is to minimize the variances of $\mathcal{C}-\mathcal{C}$ in order to alleviate the shifting of coefficients originating from noises. Given $\widetilde{\mathcal{C}}$ and (7), minimizing the variance error $\mathrm{Var}(\mathcal{C})-\mathrm{Var}(\mathcal{C})$ after soft thresholding can be formulated as

$$\begin{aligned}
\underset{\tau_\theta}{\text{minimize}} \quad & G = \sum_{i:\tilde{c}_i \notin [-\tau_\theta, \tau_\theta]} \left(\tilde{c}_i^2 + \tau_\theta^2 - 2|\tilde{c}_i|\tau_\theta \right) \\
\text{subject to} \quad & \tau_\theta \geq 0 \\
& G \geq \sum_i \tilde{c}_i^2 + 2(\kappa+1)\lambda^2.
\end{aligned} \tag{8}$$

Proof: Since $c_i = \tilde{c}_i - n_i$, the formulation of variance error can be simplified as following:

$$\begin{aligned}
&\mathrm{Var}(\mathcal{C}) - \mathrm{Var}(\mathcal{C}) = \frac{1}{\kappa+1} \sum_i \left({c_i}^2 - c_i^2 \right) \\
&= \frac{1}{\kappa+1} \sum_i \left[(c_i)^2 - (\tilde{c}_i - n_i)^2 \right] = \frac{1}{\kappa+1} \sum_i \left(c_i^2 - \tilde{c}_i^2 \right) - 2\lambda^2 \\
&= \frac{1}{\kappa+1} \left[\sum_{i:\tilde{c}_i \notin [-\tau_\theta, \tau_\theta]} \left(\tilde{c}_i^2 + \tau_\theta^2 - 2|\tilde{c}_i|\tau_\theta \right) - \sum_i \tilde{c}_i^2 \right] - 2\lambda^2
\end{aligned}$$

where n_i is the noise sampled from $\mathrm{Lap}(\lambda)$.

As $\sum_i \tilde{c}_i^2$ and $2\lambda^2$ are known, the objective function can reduced to $\sum_{i:\tilde{c}_i \notin [-\tau_\theta, \tau_\theta]} (\tilde{c}_i^2 + \tau_\theta^2 - 2|\tilde{c}_i|\tau_\theta)$. ■

We propose a searching algorithm on $\widetilde{\mathcal{C}}$ to calculate a suitable τ_θ. As shown in Algorithm 2, it first excludes a certain number of large $\tilde{c}_j$ from the range $[-\tau_\theta, \tau_\theta]$ and solve the quadric equation to let the objective function reach its potential minimum $\sum_i \tilde{c}_i^2 + 2(\kappa+1)\lambda^2$. If the potential minimum is not achievable, it computes the minimum distance between the objective function and the potential minimum. Then, it kicks one more $\tilde{c}_j$ out of range and begins another round of searching. Finally, it chooses the $\tilde{c}_j$ that satisfies the constraints and minimizes the objective function.

Theorem 3: The privacy guarantee is not degraded after soft thresholding.

Algorithm 2 Searching for the Optimized τ_θ

Computes $2(\kappa+1)\lambda^2$. Sort $|\tilde{\mathcal{C}}|$ in descending order and assign new indexes.
for $j = 0 : \kappa$ **do**
  The first j elements in the newly-ordered $|\tilde{\mathcal{C}}|$ exceed the range $[-\tau_\theta, \tau_\theta]$
  Compute $\sum_{k=1}^{j} \tilde{c}_k^2 + 2(\kappa+1)\lambda^2$
  Solve $(\kappa-j)\tau_\theta^2 - \left(2\sum_{k=j+1}^{\kappa} |\tilde{c}_k|\right)\tau_\theta - \sum_{k=1}^{j} \tilde{c}_k^2 - 2(\kappa+1)\lambda^2 = 0$
  if there is a solution and $\tau_\theta \geq 0$ and $|\tilde{c}_j| > q\tau_\theta \geq |\tilde{c}_{j+1}|$ **then**
    Store τ_θ in the first candidate vector.
  else
    Find the minimum point τ_θ of the formulation in Step 5
    if $\tau_\theta \geq 0$ and $|\tilde{c}_j| > \tau_\theta \geq |\tilde{c}_{j+1}|$ **then**
      Store τ_θ and its corresponding minimum in the second candidate vector.
    end if
  end if
end for
return the first element in this vector, otherwise return the element in the second vector with the smallest minimum

Proof: An intuitive proof is that the threshold τ_θ is produced merely on $\mathcal{C}$, which is generated on Lap(λ) and the λ itself, so the privacy guarantee is the same.

This theorem can also be proved in another mathematical way from the aspect of probability density function (pdf). The pdf of $\mathring{\mathcal{C}} - \mathcal{C}$ is the convolution of the pdf of Laplace noise and soft-thresholding errors, where the pdf of soft thresholding is a set of Dirac Delta functions $\text{amp}_i\delta(x - \text{loc}_i)$, whose amplitudes and locations have following properties:

$$\sum_i \text{amp}_i = 1, \qquad \forall i, \text{loc}_i \in [-\tau_\theta, \tau_\theta].$$

Hence, the probability of distinguishing a polynomial fitting coefficient from another after perturbing with Laplace noise and soft thresholding is

$$\frac{pdf[c_1 = t]}{pdf[c_2 = t]} = \frac{\text{Lap}(t - c_1) * \sum_i \text{amp}_i\delta(x - \text{loc}_i)}{\text{Lap}(t - c_2) * \sum_i \text{amp}_i\delta(x - \text{loc}_i)} = \sum_i \left[\text{amp}_i \exp\left(\frac{\Delta(L)}{\lambda}\right)\right] = \exp\left(\frac{\Delta(L)}{\epsilon}\right)$$

which achieves the same privacy budget ϵ as the basic perturbation scheme does. ■

V. Performance Evaluations

A. Data Collection

In our experiments, we use two online datasets in PhysioBank databases [26], which are MIT-BIH Arrhythmia (MA) database [27] and MIT-BIH Noise Stress Test (NST) database [28]. MA database contains two-channel ambulatory ECG recordings obtained from 47 subjects. The NST database adds artificial noises to the clean recordings No. 118 and No. 119 from the MA database, whose signal-to-noise ratios (SNRs) are 24, 18, 12, 6, 0, and −6 dB, respectively.

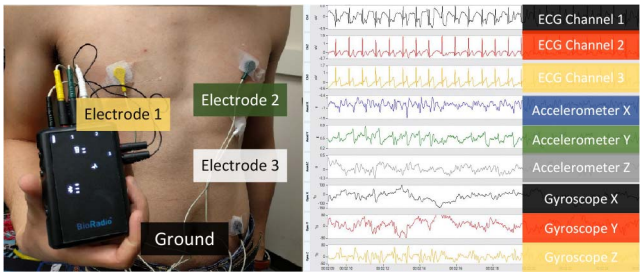


Fig. 3. Demonstration of recording and signals.

TABLE II
Datasets

Dataset	Gender	Age	Sampling	Duration
MA/NST	25(M) 22(F)	23-89	360 Hz	30 mins
Collected	20(M) 10(F)	21-40	250 Hz	20 mins

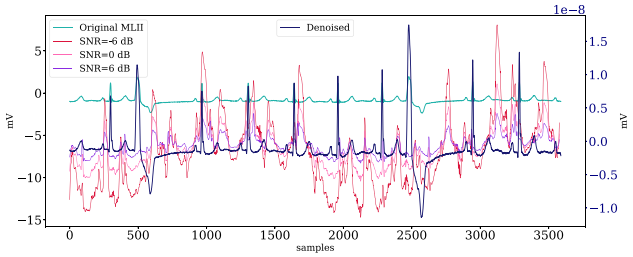


Fig. 4. De-noising result under different SNRs.

Besides online datasets, we recruit 30 healthy subjects to record their ECG signals voluntarily. During recording, they perform different physical activities (resting, walking, running, and jumping). Data are collected with a lightweight wearable physiological monitor BioRadio 700-0016 and its software BioCapture, which is supported up to three leads. The electrode positions following Einthoven's system [29]. The recording situation and an example of recorded waveforms are illustrated in Fig. 3. The data descriptions are summarized as in Table II.

B. Effectiveness of De-Noising and Authentication

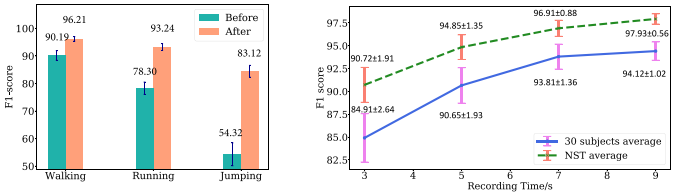
The de-noising and authentication process is performed on all dataset to test root mean square error (RMSE), divergence, and authentication accuracy. We import $F1$ score, which is defined below, to evaluate the accuracy of correctly verify whether a test instance is from the authorized user regardless of the physical movements

$$F1 = \frac{2 \times \text{TruePositive}}{2 \times \text{TruePositive} + \text{FalsePositive} + \text{FalseNegative}}.$$

We perform de-noising from "bad" signal entries in NST database and our collected data, then compare them with corresponding clean recordings. We chooses 100 segments with 10 s for each person, motion type, and SNR, and normalize all ECG recordings, then compute the average RMSE, divergence, and $F1$ score before and after de-noising.

TABLE III
AUTHENTICATION UNDER DIFFERENT TYPES OF MOVEMENT

Status	Walking	Running	Jumping
Divergence Mean	0.6116	1.8391	4.6458
Divergence STD	0.1634	0.3612	0.7483



(a) (b)

Fig. 5. $F1$ score performance. (a) Different motion types. (b) Different recording time.

1) De-Noising Stability Under Different SNRs: The de-noising reliability under different predetermined SNRs is evaluated using NST dataset, which can be observed in Fig. 4. Data collected from 30 subjects is not evaluated here because, it is hard to determine the SNR in a real ECG signal. The amplitudes of the original signal correspond to the left y-axis and those of the recovered signal correspond to the right y-axis. The differences between de-noised results are negligible so they are plotted as one line corresponding to the left y-axis. The outcomes for SNR ≥ 0 are clean ECG signals with identical QRS complexes and the RMSEs after normalizing are as small as 0.002. We can conclude than successful de-noising and authentication are guaranteed regardless of SNRs.

2) Motion Types: We extract 6600 segments lasting for 10 s from our collected data to compare the de-noising and authentication results for signals under different motion types, 3000 segments of which are collected during walking and the other 3000 and 600 segments come from running and jumping scenario, respectively. The numbers of segments are in correspondence to the recording time of each motion. The ECG signal undergoes small, continual noise interference when the objective is walking while experiencing large, continual/abrupt distortions with high energy when the subject is running/jumping. Table III and Fig. 5(a) use the divergences and $F1$ scores are to demonstrate the results. The unwanted signal component has relatively small energy when the patient is walking, so it is easy for the algorithm to recover the signal. However, the noise signal appearing when the patient keeps running or jumping is sometimes too sharp for the $\boldsymbol{U}$ to react and separate it from signals, which will jeopardize the stability of de-noising and authentication. Therefore, the authentication performance is the best when the subject is walking while being the worst for jumping, and the divergence [defined in (3)] and $F1$ score for jumping have the largest STDs.

Values in Fig. 5(a) also proves the effectiveness of de-noising. The $F1$ scores after de-noising all are increased compared to those before de-noising. The improvement for jumping is the most significant. It is almost meaningless to authenticate jumping subjects before de-noising, but the score is much more acceptable after de-noising.

3) Authentication Time: To evaluate the time efficiency, we calculate the average $F1$ scores when the authentication process ends after different lengths of recording time with all movement types. The means and STDs of authentication accuracy, are shown in Fig. 5(b). The scores indicate that the authentication performs better with longer recording time. It can be observed that the authentication becomes more accurate and stable with longer recording time, with smaller STDs and a $F1$ score over 94% for our collected data and 97% for NST dataset. A recording time of 3 s is not enough to reliably recognize the patient with a score around 85% for the real-life data and the improvement for time longer than 7 s is less significant. Therefore, we set the recording time for authentication as a constant, e.g., 7 s, in the following experiments from the aspects of accuracy and time efficiency.

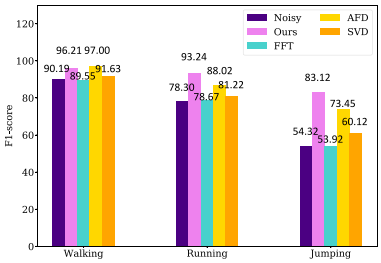


Fig. 6. $F1$ score comparison.

4) Experimental Results Comparison: To prove the superiority of our proposed ECG-based authentication scheme, we compare our scheme with other ECG-based mechanisms with noise cancellation. The comparison are done among the following schemes.

1) A basic nonlinear ECG features detection based on fast Fourier transform (FFT) [30].
2) A more advanced method based on adaptive Fourier decomposition (AFD) [31], which is implemented on the AFD toolbox developed by Wang *et al.* [32].
3) An SVD-based scheme in [33].

The aforementioned schemes are only tested on signals with artificially added noises, which are too simple compared to real scenarios. As shown in Fig. 6, the first simple method may work for artificially added noises, but it cannot distinguish real-world noises at all. Its authentication accuracy is very low because it cannot separate any noises from signals. The AFD-based one performs better than the previous straightforward one due to its adaptive feature, but it requires the estimated SNRs. We estimate some SNRs from the signal amplitudes and pass them to the algorithm, but the performance still falls behind our scheme when experiencing higher level of noises due to the inaccurate estimation on SNR of real-world signals. Moreover, the time consumption of AFD is high. Therefore, the AFD-based algorithm is not suitable for authentication purpose. The last SVD-based one cannot adapt itself to motion status as well as the variations in noises, so the reproduced ECG signal may be distorted and the authentication accuracy is not greatly boosted after de-noising.

C. Privacy Guarantee

1) ROC Curve: Receiver operating characteristic (ROC) curve is a graph to illustrate the classification performance under varied thresholds by plotting true positive rate against

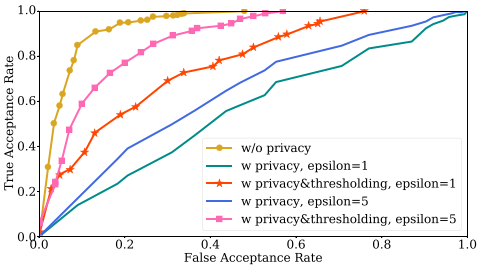
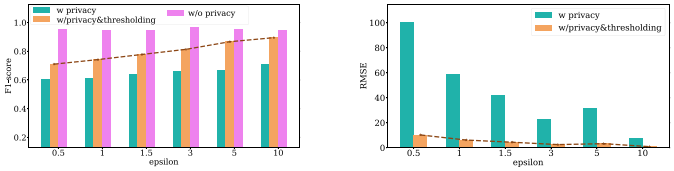


Fig. 7. ROC curve for different ϵ.



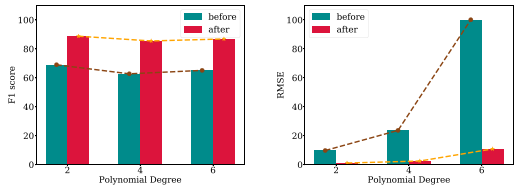
(a) (b)

Fig. 8. Effect of privacy bounds. (a) $F1$ score under different ϵ. (b) RMSE under different ϵ.

the false positive rate. Its area under curve (AUC) is an important metric to quantify the performance. In Fig. 7, AUCs for curves of $\epsilon = 5$ are larger than those for curves of $\epsilon = 1$, because higher ϵ indicates lower privacy bound, which brings worse privacy guarantee but better performance in terms of authentication accuracy. The classification ability after applying differential privacy is poor in the traditional academic point system, since the corresponding AUCs are merely between 0.6 and 0.7. However, after applying soft thresholding, the AUC of $\epsilon = 1$ becomes 0.766 and that of $\epsilon = 5$ is 0.861. Though it is still smaller than the AUC without privacy guarantee due to an inevitable tradeoff between privacy and utility, the performance is ranked as good, which means it is acceptable.

2) Different Privacy Bounds: Overall the performance is improved after soft thresholding as shown in Fig. 8(a) and (b). The trends in *F1 score* and RMSE show that the accuracy is lower with smaller privacy bound, which indicating stricter privacy demand. Although applying differential privacy with smaller privacy budgets ($\epsilon = 0.5$) will degrade the authentication service greatly with only around 70% accuracy even after soft thresholding, a patient can authenticate herself with her protected template with an accuracy rate about 90% when $\epsilon = 10$. This accuracy rate is close to the upper bound (the accuracy rate without applying differential privacy). It implies that the patient can enjoy the accurate authentication together with the protection of differential privacy if the budget is loosened. As shown in Fig. 8(b), the RMSE descends with the growing of ϵ due to the looser privacy requirement and the RMSE after soft thresholding can be reduced to the tenth of the one before thresholding. The deviation caused on ECG signals by differential privacy is reduced and the effectiveness of soft thresholding is verified.

3) Different Polynomial Degrees: Under choices of different Legendre polynomial order κ, we reconstruct signals $\widetilde{\mathcal{M}}$ from noisy coefficients and compute the summation of RMSE between $\widetilde{\mathcal{M}}$ and $\mathcal{M}$ and the $F1$ scores achieved. As shown in



(a) (b)

Fig. 9. Impact of different polynomial degrees. (a) $F1$ score. (b) RMSE.

TABLE IV
RUNNING TIME

	Training	Authentication	Privacy Enhancement
Mean/s	3.3591	0.7432	0.00071
STD/s	0.1071	0.0907	0.00046

Fig. 9(b), due to the enlarging sensitivity of $\widetilde{\mathcal{C}}$ when polynomial order κ is increasing, there is a slight drop in $F1$ score and dramatic rise in RMSE. The tremendous growth in RMSE does not substantially drop in $F1$ score because Legendre polynomials cover some uniqueness of ECG morphology and the uniqueness is retained even after applying differential privacy. Apparently, the performance is still enhanced by soft thresholding.

D. Efficiency Analysis

We implement our algorithms on Python 2.7 for over 10 000 iterations to estimate the running time. Evaluation results about running time are listed in Table IV. Training a template takes up about 3.359 s. Its swiftness enables timely online template training for patients. The average time for extracting fiducial features from a 10-s ECG signal and comparing it with the template is about 0.7432 s. The extended privacy enhancement scheme uses only 0.00071 s to fit the ECG template with polynomials, add noises to polynomial coefficients, smoothing noises, and reconstruct the signal from noisy coefficients. The running time of our scheme is small and stable, which indicates that the proposed scheme is efficient and causes negligible extra burden.

VI. Related Work

A. ECG-Based Authentication

Existing ECG-based authentication schemes rely on fiducial [34] or nonfiducial features (e.g., pulse active ratio [6], wavelet coefficients [7], [35], and Legendre coefficients [36]) to present ECG signal's characteristics. Due to the permanence of the ECG signal, the produced features are constant and sensitive, so privacy guarantee should be added. Chaotic functions [37] provide a solution for varying representation of features, but its stability is not yet validated. A scheme named fuzzy extractor is proposed in [38] for authentication and some works extend it to a reusable one [20], [39]. However, the authentication process in them is not efficient in that it is done as a step toward getting the key, and the clues needed for authentication may compromise the privacy of features. A more significant deficiency in works related to ECG-based authentication is that a majority of them do not consider the

active authentication. Sriram *et al.* [40] only estimated the BW under differential exercises when de-noising the signal and pay no attention to other noise contamination.

B. Noise Elimination in ECG signals

Either linear or nonlinear methods have been proposed [31] to eliminate noises in ECG signals. Linear methods do not consider the overlap between noise frequencies and signal frequencies. The wavelet-based methods [41] are the most widely used nonlinear approaches, but their accuracy is restricted by the choice of mother wavelet and they may lead to oscillations in the reconstructed ECG signals [42]. In order to solve these deficiencies, Wang *et al.* [31] proposed an adaptive wavelet decomposition. However, this scheme has a high demand on SNR when reconstructing signals. SVD [33] can effectively extract compressed features from the ECG signal and then recover a clean ECG signal from the noisy one. However, most traditional ECG signal decomposition with SVD has to be done after obtaining the entire ECG data matrix, which can bring down the efficiency of authentication. Moreover, almost all existing works are only tested on artificially added noises on real or simulated ECG signals, so there efficiency on real-world noisy ECG signals are doubtful. In this paper, we take the advantage of SVD and boost its efficiency when applying it to the authentication procedure.

VII. Conclusion

In this paper, we have presented an ECG-based authentication scheme for IoT-based healthcare that provides authentication ability when the ECG input is noisy and protects the privacy of stored ECG templates. Our scheme makes several novel contributions: preserve the timeliness of authentication by implementing light-weighted online algorithms; effectively disaggregate noises from ECG signals to ensure a reliable authentication; provide indistinguishability via differential privacy to prevent adversaries from inferring the patient's ECG information; improve the accuracy by applying soft thresholding while holding the claimed privacy guarantee. Our experimental evaluation on both online dataset and real-world experiments shows that the proposed approach can effectively and efficiently authenticate patients while ensuring the privacy of templates.

References

[1] J. Car, W. S. Tan, Z. Huang, P. Sloot, and B. D. Franklin, "eHealth in the future of medications management: Personalisation, monitoring and adherence," *BMC Med.*, vol. 15, no. 1, p. 73, 2017.

[2] S. P. Thacker, "HIPAA privacy rule and public health. Guidance from CDC and the U.S. Department of Health and Human Services," *Morbidity Mortality Weekly Rep.*, vol. 52, no. S1, pp. 1–17, 2003.

[3] K. Nguyen, C. Fookes, S. Sridharan, M. Tistarelli, and M. Nixon, "Super-resolution for biometrics: A comprehensive survey," *Pattern Recognit.*, vol. 78, pp. 23–42, Jun. 2018.

[4] A. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*, vol. 479. New York, NY, USA: Springer, 2006.

[5] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognit. Lett.*, vol. 79, pp. 80–105, Aug. 2016.

[6] S. Safie, N. Haris, A. Zainal, J. Soraghan, and L. Petropoulakis, "Comparison of pulse active (PA) modulation signal for electrocardiogram (ECG) authentication," in *Proc. IEEE Int. Conf. Signal Image Process. Appl. (ICSIPA)*, 2015, pp. 165–168.

[7] A. A. S. Raj, N. Dheetsith, S. S. Nair, and D. Ghosh, "Auto analysis of ECG signals using artificial neural network," in *Proc. IEEE Int. Conf. Sci. Eng. Manag. Res. (ICSEMR)*, 2014, pp. 1–4.

[8] H. P. Da Silva, A. Fred, A. Lourenço, and A. K. Jain, "Finger ECG signal for user authentication: Usability and performance," in *Proc. IEEE 6th Int. Conf. Biometr. Theory Appl. Syst. (BTAS)*, 2013, pp. 1–8.

[9] *Data Breaches in Healthcare Totaled Over 112 Million Records in 2015*. Accessed: Dec. 16, 2016. [Online]. Available: https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015

[10] M. S. Thaler, *The Only EKG Book You'll Ever Need*. Philadelphia, PA, USA: Lippincott Williams & Wilkins, 2010.

[11] J. R. Pinto, J. S. Cardoso, A. Lourenço, and C. Carreiras, "Towards a continuous biometric system based on ECG signals acquired on the steering wheel," *Sensors*, vol. 17, no. 10, p. 2228, 2017.

[12] R. Sameni, G. D. Clifford, C. Jutten, and M. B. Shamsollahi, "Multichannel ECG and noise modeling: Application to maternal and fetal ECG signals," *EURASIP J. Appl. Signal Process.*, vol. 2007, no. 1, p. 94, 2007.

[13] G. H. Golub and C. Reinsch, "Singular value decomposition and least squares solutions," *Numerische Mathematik*, vol. 14, no. 5, pp. 403–420, 1970.

[14] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends® Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.

[15] S. Eberz, N. Paoletti, M. Roeschlin, M. Kwiatkowska, I. Martinovic, and A. Patané, "Broken hearted: How to attack ECG biometrics," in *Proc. NDSS Symp.*, 2017, pp. 1–15.

[16] R. Kottath, P. Narkhede, V. Kumar, V. Karar, and S. Poddar, "Multiple model adaptive complementary filter for attitude estimation," *Aerosp. Sci. Technol.*, vol. 69, pp. 574–581, Oct. 2017.

[17] E. Fortune, V. A. Lugade, and K. R. Kaufman, "Posture and movement classification: The comparison of tri-axial accelerometer numbers and anatomical placement," *J. Biomech. Eng.*, vol. 136, no. 5, 2014, Art. no. 051003.

[18] G. H. Golub and C. F. Van Loan, *Matrix Computations*, vol. 3. Baltimore, MD, USA: JHU Press, 2012.

[19] J. M. Joyce, "KullbackŰLeibler divergence," in *International Encyclopedia of Statistical Science*. Heidelberg, Germany: Springer, 2011, pp. 720–722.

[20] P. Huang, B. Li, L. Guo, Z. Jin, and Y. Chen, "A robust and reusable ECG-based authentication and data encryption scheme for eHealth systems," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, 2016, pp. 1–6.

[21] I. Khalil and F. Sufi, "Legendre polynomials based biometric authentication using QRS complex of ECG," in *Proc. IEEE Int. Conf. Intell. Sensors Sensor Netw. Inf. Process. (ISSNIP)*, 2008, pp. 297–302.

[22] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*, vol. 55. New York, NY, USA: Courier Corporat., 1965.

[23] V. Rastogi and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, 2010, pp. 735–746.

[24] B. Mohl, M. Wahlberg, and P. Madsen, "Ideal spatial adaptation via wavelet shrinkage," *J. Acoust. Soc. America*, vol. 114, no. 3, pp. 1143–1154, 2003.

[25] M. Bachmayr and R. Schneider, "Iterative methods based on soft thresholding of hierarchical tensors," *Found. Comput. Math.*, vol. 17, no. 4, pp. 1037–1083, 2017.

[26] A. L. Goldberger *et al.*, "PhysioBank, PhysioToolkit, and PhysioNet," *Circulation*, vol. 101, no. 23, pp. e215–e220, 2000.

[27] G. B. Moody and R. G. Mark, "The impact of the MIT-BIH arrhythmia database," *IEEE Eng. Med. Biol. Mag.*, vol. 20, no. 3, pp. 45–50, May/Jun. 2001.

[28] G. B. Moody, W. Muldrow, and R. G. Mark, "A noise stress test for arrhythmia detectors," *Comput. Cardiol.*, vol. 11, no. 3, pp. 381–384, 1984.

[29] S. Marcus, C. Chang, and S. Baskerville, "Wireless ECG sensor system and method," U.S. Patent Appl. 15 839 941, Apr. 12 2018.

[30] A. K. M. F. Haque, M. H. Ali, M. A. Kiber, and M. T. Hasan, "Detection of small variations of ECG features using wavelet," *ARPN J. Eng. Appl. Sci.*, vol. 4, no. 6, pp. 27–30, 2009.

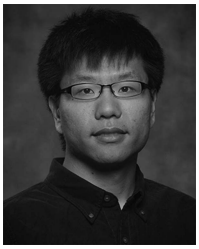
[31] Z. Wang *et al.*, "Muscle and electrode motion artifacts reduction in ECG using adaptive Fourier decomposition," in *Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC)*, 2014, pp. 1456–1461.

[32] *Toolbox-for-Adaptive-Fourier-Decomposition*. Accessed: May 27, 2019. [Online]. Available: https://github.com/pikipity/Toolbox-for-Adaptive-Fourier-Decomposition

[33] M. Varanini, G. Tartarisco, L. Billeci, A. Macerata, G. Pioggia, and R. Balocchi, "An efficient unsupervised fetal QRS complex detection from abdominal maternal ECG," *Physiol. Meas.*, vol. 35, no. 8, p. 1607, 2014.
[34] F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, and K. Ren, "Cardiac scan: A non-contact and continuous heart-based user authentication system," in *Proc. ACM 23rd Annu. Int. Conf. Mobile Comput. Netw.*, 2017, pp. 315–328.
[35] M. Abo-Zahhad, A. F. Al-Ajlouni, S. M. Ahmed, and R. J. Schilling, "A new algorithm for the compression of ECG signals based on mother wavelet parameterization and best-threshold levels selection," *Digit. Signal Process.*, vol. 23, no. 3, pp. 1002–1011, 2013.
[36] P. A. Regis, A. N. Patra, and S. Sengupta, "Unmanned aerial vehicles positioning scheme for first-responders in a dynamic area of interest," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, 2018, pp. 1–5.
[37] C.-K. Chen, C.-L. Lin, S.-L. Lin, Y.-M. Chiu, and C.-T. Chiang, "A chaotic theoretical approach to ECG-based identity recognition [application notes]," *IEEE Comput. Intell. Mag.*, vol. 9, no. 1, pp. 53–63, Feb. 2014.
[38] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Adv. Cryptol. (Eurocrypt)*, 2004, pp. 523–540.
[39] R. Canetti, B. Fuller, O. Paneth, L. Reyzin, and A. Smith, "Reusable fuzzy extractors for low-entropy distributions," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2016, pp. 117–146.
[40] J. C. Sriram, M. Shin, T. Choudhury, and D. Kotz, "Activity-aware ECG-based patient authentication for remote health monitoring," in *Proc. Int. Conf. Multimodal Interfaces*, 2009, pp. 297–304.
[41] R. Chauhan, R. Dahiya, and P. Bansal, "Optimal choice of thresholding rule for denoising ECG using DWT," in *Proc. IEEE 4th Int. Conf. Signal Process. Comput. Control (ISPCC)*, 2017, pp. 288–292.
[42] G. U. Reddy, M. Muralidhar, and S. Varadarajan, "ECG DE-noising using improved thresholding based on wavelet transforms," *Int. J. Comput. Sci. Netw. Security*, vol. 9, no. 9, pp. 221–225, 2009.

Pei Huang (S'17) received the B.Sc. degree from Xidian University, Xi'an, China, in 2015 and the M.Sc. degree from the State University of New York (SUNY) at Binghamton, Binghamton, NY, USA, in 2017. She was a Ph.D. candidate at SUNY at Binghamton and is currently pursuing her doctorate degree at Clemson University, Clemson, SC, USA.

Her current research interests include security and privacy in eHealth/mHealth system, wireless networks, and crowdsensing, with a focus on the security problems regarding physical layer properties in Internet of Things.



Linke Guo (M'14) received the B.E. degree in electronic information science and technology from the Beijing University of Posts and Telecommunications, Beijing, China, in 2008, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2011 and 2014, respectively.

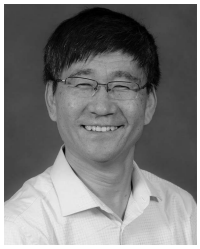
From August 2014 to August 2019, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Binghamton University (State University of New York), Binghamton, NY, USA. Since August 2019, he has been an Assistant Professor with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, USA. His current research interests include network security and privacy, social networks, and applied cryptography.

Prof. Guo was a co-recipient of the Best Paper Award of Globecom 2015, Symposium on Communication and Information System Security. He is currently serving as an Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He also serves as the Poster/Demo Chair of the IEEE INFOCOM 2020. He was the Publication Chair of the IEEE Conference on Communications and Network Security in 2016 and 2017. He was the Symposium Co-Chair of Network Algorithms and Performance Evaluation Symposium, ICNC 2016. He has served as the Technical Program Committee Member for several conferences, including IEEE INFOCOM, ICC, GLOBECOM, and WCNC. He is a member of ACM.

Ming Li (M'14) received the B.E. degree in electrical engineering from Sun Yat-sen University, Guangzhou, China, in 2007, the M.E. degree in electrical engineering from the Beijing University of Posts and Communications, Beijing, China, in 2010, and the Ph.D. degree in electrical and computer engineering from Mississippi State University, Starkville, MS, USA, in 2014.

She is currently an Assistant Professor with the Department of Computer Science and Engineering, University of Texas at Arlington, Arlington, TX, USA. Her current research interests include mobile computing, Internet of Things, security, and privacy-preserving computing.

Dr. Li was a recipient of the Best Paper Award in the IEEE Global Communications Conference 2015 and the IEEE Digital Avionics Systems Conference 2017.



Yuguang Fang (F'08) received the M.S. degree from Qufu Normal University, Shandong, China, in 1987, the first Ph.D. degree from Case Western Reserve University, Cleveland, OH, USA, in 1994, and the second Ph.D. degree from Boston University, Boston, MA, USA, in 1997.

He joined the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA, in 2000, where he has been a Full Professor since 2005. He holds a University of Florida Research Foundation Professorship in 2006–2009 and in 2017–2020; a University of Florida Term Professorship in 2017–2019; a Changjiang Scholar Chair Professorship with Xidian University, Xi'an, China, in 2008–2011 and Dalian Maritime University, Dalian, China, in 2015–2018; an Overseas Academic Master with the Dalian University of Technology, Dalian, in 2016–2018, and has been an Overseas Advisor with the School of Information Science and Technology, Southwest Jiao Tong University, Chengdu, China, since 2014.

Dr. Fang was a recipient of the U.S. National Science Foundation Career Award in 2001, the Office of Naval Research Young Investigator Award in 2002, the 2018 IEEE Vehicular Technology Outstanding Service Award, the 2015 IEEE Communications Society CISTC Technical Recognition Award, the 2014 IEEE Communications Society WTC Recognition Award, the Best Paper Award from IEEE ICNP in 2006, the 2010–2011 UF Doctoral Dissertation Advisor/Mentoring Award, the 2011 Florida Blue Key/UF Homecoming Distinguished Faculty Award, and the 2009 UF College of Engineering Faculty Mentoring Award. He was the Editor-in-Chief of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY from 2013 to 2017 and the IEEE WIRELESS COMMUNICATIONS from 2009 to 2012. He serves/served on several editorial boards of journals, including PROCEEDINGS OF THE IEEE since 2018, *ACM Computing Surveys* since 2017, the IEEE TRANSACTIONS ON MOBILE COMPUTING from 2003 to 2008 and from 2011 to 2016, the IEEE TRANSACTIONS ON COMMUNICATIONS from 2000 to 2011, and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2002 to 2009. He has been actively participating in conference organizations, such as serving as the Technical Program Co-Chair for IEEE INFOCOM'2014 and the Technical Program Vice-Chair for IEEE INFOCOM'2005. He is a fellow of the American Association for the Advancement of Science.