A Precoding Perturbation Method in Geometric Optimization: Exploring Manifold Structure for Privacy and Efficiency

Azadeh Pourkabirian, *Member, IEEE*, Wei Ni, *Fellow, IEEE*, Xiaolin Zhou, *Senior Member, IEEE,* Kai Li, *Senior Member, IEEE,* and Mohammad Hossein Anisi, *Senior Member, IEEE*

***Abstract*— Inherent broadcast characteristics can raise privacy risks of wireless networks. The specifics of antenna ports, antenna types, orientation, and beamforming configurations of a transmitter can be susceptible to manipulation by any device within range when the signal is transmitted wirelessly. Personal and location information of users connected to the transmitter can be intercepted and exploited by malicious actors to track user movements and profile behaviors or launch targeted attacks, thus compromising user privacy and security. In this paper, we propose a novel precoding perturbation approach for privacy preservation in wireless communications. Our approach perturbs the precoding matrix of the transmitter using a Riemannian manifold (RM) structure that adaptively adjusts the magnitude and direction of perturbation based on the geometric properties of the manifold. The approach ensures robust privacy protection while minimizing the distortion of the transmitted signals, thus balancing privacy preservation and data utility. Privacy can be preserved without relying on additional cryptographic mechanisms, resulting in the computational and communication overhead reduction. Our approach operates directly on the transmission of signals, making them inherently secure against eavesdropping and interception. Simulation results underscore the superiority of the approach, showing a 17.21% improvement in privacy preservation while effectively maintaining data utility.**

***Index Terms*— Privacy preservation, precoding perturbation, Riemannian manifold, wireless communication.**

I. Introduction

As the modern world embraces digitization and connectivity, the importance of privacy preservation [1],[2] has ever been more pronounced. The fifth-generation (5G) systems often use massive multiple input multiple output (MIMO) configurations with a large number of antennas (e.g., 64x64) to improve spectral efficiency and coverage. These configurations, while beneficial for performance, increase the surface area for potential eavesdroppers to exploit. 5G systems often use channel state information (CSI) feedback and precoding techniques to optimize signal transmission and enhance communication reliability.

The information contained in the precoding matrix derived from CSI can be exploited by adversaries to infer sensitive information, such as user locations or network topology. By analyzing the precoding matrix, an adversary can potentially infer the number of users and their directions relative to the base station, which can be used to triangulate the users. On the other hand, CSI contains detailed information about the channel gains between the transmitter and receiver. In a time-varying radio propagation environment, CSI needs to be shared between the transmitter and receiver for effective transmission. The phase of the CSI can expose information about the relative distances and angles between the transmitter and receiver, which can be used for localization. The changes in CSI can reveal movement patterns of users, enabling adversaries to track their locations. Adversaries can also use these vectors to infer the spatial location of users, see Fig.1.

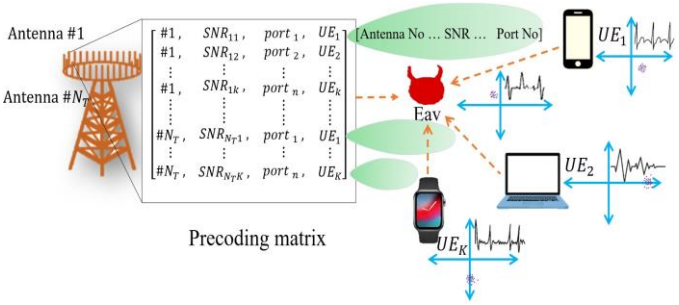


Fig.1. Potential risks of privacy distortion - This figure illustrates how sensitive information transmitted over networks can be intercepted by eavesdroppers or unauthorized entities, leading to the inference of private details about users.

This raises privacy concerns about sensitive information within the networks. In response to privacy concerns, existing literature employs different methods in wireless communications. Secure multi-party computation (SMPC) [3]-[5] enables multiple parties to jointly compute a function over their inputs without revealing individual inputs, thereby preserving privacy. Homomorphic encryption [6],[7] allows

This work was supported in part by the Natural Science Foundation of Shanghai under Grant 24ZR1407100, and in part by the National Natural Science Foundation of China under Grant 61571135. This work was also supported by the CISTER Research Unit (UIDP/UIDB/04234/2020), financed by National Funds through FCT/MCTES (Portuguese Foundation for Science and Technology), and by project Aero.Next Portugal (ref. C645727867-00000066), funded by the EU/Next Generation, within call n.º 02/C05-i01/2022 of the Recovery and Resilience Plan (RRP).

A. Pourkabirian and K. Li are with the Real-Time and Embedded Computing Systems Research Centre (CISTER), 4249015 Porto, Portugal. E-mail: {azadeh.pourkabirian@cister-labs.pt, kai@isep.ipp.pt}

W. Ni is with Data61, CSIRO, Sydney, NSW 2122, Australia. E-mail: wei.ni@data61.csiro.au.

X. Zhou is with the School of Information Science and Technology, Fudan University, Shanghai 200433, China. E-mail: zhouxiaolin@fudan.edu.cn.

M. H. Anisi is with the School of Computer Science and Electronic Engineering, University of Essex, CO4 3SQ Colchester, U.K. E-mail: m.anisi@essex.ac.uk.

Corresponding author: X. Zhou

computations to be performed on encrypted data without decrypting it, enabling privacy-preserving data analysis. Advanced authentication techniques such as eye tracking [8] and Swift-eye [9] leverage biometric data to enhance security while incorporating advanced encryption and anonymization methods to prevent re-identification of individuals. Furthermore, methods such as obfuscation [10] and perturbation [11] were proposed to protect users' location privacy in location-based services and applications. Techniques to counter traffic analysis attacks, such as mix networks [12], onion routing [13], and traffic padding [14], aim to obfuscate communication patterns and protect user privacy. Randomized response [15], noise injection [16], and data masking [17] are examples of data perturbation techniques that introduce randomness or distortion to data to protect privacy.

Differential privacy (DP) [18], another notable technique, provides a rigorous framework for privacy guarantees. DP adds noise to data to obscure it, ensuring that sensitive information cannot be accurately inferred. Although there exist rich works on data privacy [19]-[22] for wireless networks, only a few works have addressed the privacy issue in physical-layer signal processing [23],[24]. The DP technique can be applied to protect CSI by adding controlled noise to the precoding matrix derived from CSI, a method known as precoding perturbation. This ensures that the precise channel characteristics are obscured, preventing attackers from gaining accurate insights while still allowing the system to perform effectively. The authors of [23],[24] developed privacy-preserving channel estimation schemes that inject noise into the channel matrix to protect data. However, these perturbation mechanisms inherently introduce a trade-off between privacy protection and data utility. The presence of perturbation/noise can alter the statistical properties of the data, posing challenges for accurate and reliable statistical analysis of the precoding matrix. Motivated by this challenge, we propose a novel precoding matrix perturbation method that considers the trade-off between privacy protection and data utility within the DP framework.

This paper focuses on an eavesdropping adversary capable of passively monitoring communications between the transmitter and users [25]. This adversary aims to extract sensitive information—such as user locations and network topology—by analyzing the precoding matrix derived from CSI [26]. To protect against this threat, we utilize the *Riemannian manifold* (RM) structure, a mathematical framework in differential geometry, to introduce controlled variations into the precoding matrix. The RM structure ensures that these variations respect the geometric properties of the precoding matrix, such as maintaining orthogonality, symmetric positive definiteness (SPD), or unitarity. This preserves communication quality, such as the signal-to-interference-plus-noise ratio (SINR) or channel capacity, while making it difficult for the adversary to infer the original matrix. As the SPD property of the precoding matrix could potentially be exploited by the adversary, we employ the DP mechanism to carefully calibrate the smooth variations injected into the precoding matrix. The privacy budget of DP controls the amount of variation imposed, ensuring that the adversary's ability to infer sensitive information is mathematically bounded. A smaller privacy budget provides stronger privacy guarantees, making reconstruction of the original matrix more difficult for the adversary. Conversely, a larger privacy budget allows for better utility, enabling more accurate communication and improved system performance. We address this trade-off between privacy and utility for secure and efficient 5G communication systems.

The contributions of this study are summarized as follows:

- We propose a novel approach to protecting sensitive information of precoding matrices. The approach does not preserve the privacy of data, since data can be protected using cryptographic methods. Instead, it protects the sensitive information of the precoding matrix during transmission, which cryptographic methods cannot safeguard. Our approach strikes a balance between privacy and data utility through calibrated perturbations.
- We develop an RM structure to introduce controlled variations in precoding matrices. To the best of our knowledge, this is the first work that leverages RM for privacy preservation in wireless communications. We consider the space of analog precoding matrices as a manifold to analyze the relationships between different precoding matrix configurations, identifying regions of interest for perturbation based on the geometric properties of the manifold. Utilizing tangent vectors within each tangent space, we effectively navigate through the manifold and accurately measure the distances between points on the manifold. This approach maintains the geometric integrity of the data.
- We calculate the geodesic of the proposed RM, which are curves on the manifold representing the shortest paths between points, to find neighbors of each element of the precoding matrix with similar characteristics of the original point, which correspond to a perturbed precoding matrix. The neighborhoods around each point in the precoding matrix are located to apply controlled perturbations along geodesics for precoding information modification. This ensures that the variations introduced to the analog precoding matrix are small while safeguarding the precoding matrix information.
- Numerical simulations along with theoretical analysis validate the substantial enhancement achieved by our approach in preserving privacy and efficient signal transmission.

The remainder of the paper is organized as follows: We describe the problem statement and system model in Section 2. The fundamental concept of privacy is elucidated in Section 3. In Section 4, we formulate the optimization problem and develop an RM structure to solve it. In Section 5, we develop a Riemannian gradient method to solve the optimization problem and then design a precoding perturbation algorithm to find the optimal perturbed precoding matrix. Section 6 provides simulation results and performance evaluation of the proposed approach. We conclude our work in Section 7.

Notation: Bold lowercase $\boldsymbol{a}$ and uppercase $\boldsymbol{A}$ letters denote vectors and matrices, respectively. $|\cdot|$ denotes the absolute value of a number, $\|\cdot\|_2$ indicates the Euclidean norm of a

vector, $\|\cdot\|_2^2$ represents the squared Euclidean norm of a vector, and $\|\cdot\|_F$ and $\|\cdot\|_F^2$ represent the Frobenius norm and squared Frobenius norm, respectively, which measure the magnitude of a matrix. $\boldsymbol{A}^H$, $tr(\boldsymbol{A})$, $diag(\boldsymbol{A})$, and $\boldsymbol{A}^{1/2}$ respectively denote the conjugate transpose of a matrix $\boldsymbol{A}$, the trace of a square matrix $\boldsymbol{A}$, the diagonal matrix formed from the elements of a vector or a matrix $\boldsymbol{A}$, and the square root of a matrix $\boldsymbol{A}$. The key notation of this paper is presented in Table 1.

Table 1. The key notation

Notation	Definition
N_T	The number of transmitter antennas
N_S	The number of data streams
N_{RF}	The number of RF chains
K	The number of wireless users
$\boldsymbol{F}_{BB} \in \mathbb{C}^{N_S \times N_{RF}}$	The digital precoding matrix
$\boldsymbol{F}_{RF} \in \mathbb{C}^{N_{RF} \times N_T}$	The analog precoding matrix
$\widetilde{\boldsymbol{F}}_i \in \mathbb{C}^{N_{RF} \times N_T}$	The perturbed precoding matrix
$\overline{\boldsymbol{F}}_{RF} \in \mathbb{C}^{N_{RF} \times N_T}$	The Riemannian geometric mean matrix
$\boldsymbol{s} \in \mathbb{C}^{N_S \times 1}$	The signal vector
$\boldsymbol{P}^{tr} \in \mathbb{C}^{K \times K}$	The transmit power
P^{min}	The minimum transmit power
P^{max}	The maximum transmit power
$\mathbf{x} \in \mathbb{C}^{N_{RF} \times 1}$	The transmitted signal
X	The input signal space
$\hat{\boldsymbol{y}}$	The output signal
$\mathbf{y}$	The desired output signal
Z	The output signal space
τ	The BER threshold
ε	The privacy budget
δ	The privacy risk
Δ_f	The sensitivity
σ_n^2	The noise variance
λ_i	The eigenvalues of the precoding matrix $\boldsymbol{F}_{RF}$
$\boldsymbol{v}_i$	The *i*-th tangent vector of the space
N	The number of points on the tangent space
$d_{\mathcal{M}_{RF}}$	The Riemannian distance
g_p	The Riemannian metric tensor at point p
T_P	The tangent space at point p in $\mathcal{M}$
γ	The geodesic distance
$\boldsymbol{A}$, $\boldsymbol{B}$	The arbitrary SPD matrices
$\boldsymbol{X} \in \mathbb{C}^{N_T \times N_T}$	The invertible matrix
$\boldsymbol{U} \in \mathbb{C}^{N_T \times N_T}$	The unitary matrix
$\boldsymbol{V} \in \mathbb{C}^{N_T \times N_T}$	The orthogonal matrix containing eigenvectors
$\boldsymbol{\Lambda} \in \mathbb{C}^{N_T \times N_T}$	The diagonal matrix containing positive eigenvalues
$\boldsymbol{\Lambda}^{1/2} \in \mathbb{C}^{N_T \times N_T}$	The diagonal matrix containing the square root of the eigenvalues
$\boldsymbol{\Lambda}_{\boldsymbol{RF}} \in \mathbb{C}^{N_T \times N_T}$	The diagonal matrices containing the eigenvalues of $\boldsymbol{F}_{RF}$
$\boldsymbol{\Lambda}_i \in \mathbb{C}^{N_T \times N_T}$	The diagonal matrices containing the eigenvalues of $\widetilde{\boldsymbol{F}}_i$
p and q	The arbitrary points on the tangent space
η_t	The step size

II. Problem Description

A. System Model

Consider downlink communications of a multi-user multiple input multiple output (MU-MIMO) system in which a hybrid transmitter equipped with N_T antennas and $N_{RF} \leq N_T$ radio frequency (RF) chains convey N_S data streams for K single-antenna users. The transmitter first performs the digital precoding technique. Digital precoding is especially useful in multi-user/multi-antenna (i.e., multi-stream) scenarios where multiple data streams can be transmitted simultaneously over the same frequency band. The data stream vector $\boldsymbol{s} \in \mathbb{C}^{N_S \times 1}$ is multiplied by the digital precoding matrix $\boldsymbol{F}_{BB} \in \mathbb{C}^{N_S \times N_{RF}}$ to produce the precoded signal $\mathbf{x} = \boldsymbol{F}_{BB}\boldsymbol{s}$.

The digital precoding matrix contains complex different weights that are assigned to each stream in such a way that each data stream can be transmitted over the same frequency band but along different spatial paths, allowing for effective spatial multiplexing and interference management. We consider that the data streams are uncorrelated and have equal average transmit power, given by $\mathbb{E}\{\boldsymbol{s}\,\boldsymbol{s}^H\} = \frac{\|\boldsymbol{P}^{tr}\|_F}{K}\mathbf{I}$. Here, $\boldsymbol{P}^{tr}$ represents the transmit power matrix and $\mathbf{I}$ is the identity matrix. Next, analog precoding is applied in the RF domain using an analog precoding matrix $\boldsymbol{F}_{RF} \in \mathbb{C}^{N_{RF} \times N_T}$. This stage focuses on beamforming and directional signal transmission, which is crucial for overcoming high path loss and interference. The analog precoding matrix contains phase shifts and amplitude adjustments that are applied to the RF signals to adjust the phases and amplitudes of the transmitted signals. These adjustments help in steering the signal beams towards the intended directions.

We impose a normalization constraint $|\boldsymbol{F}_{RF}(i,j)| = 1/\sqrt{N_T}, \forall i \in N_{RF}, \forall j \in N_T$ to balance the power distribution across all transmitting antennas, avoiding certain signals from overpowering others that contribute to interference, where $|\boldsymbol{F}_{RF}(i,j)|$ is the magnitude of the (i,j)-th element of $\boldsymbol{F}_{RF}$. We also impose $\|\boldsymbol{P}^{tr}\|_F \leq P^{max}$ to ensure that the total transmit power $\boldsymbol{P}^{tr}$ does not exceed a predefined maximum limit P^{max} for energy conservation and interference mitigation purposes, where $\|\cdot\|_F$ denotes the Frobenius norm. The hybrid precoding matrix $\boldsymbol{F} \in \mathbb{C}^{N_S \times K}$ is the product of the analog precoding matrix and the digital precoding matrix i.e., $\boldsymbol{F} = \boldsymbol{F}_{BB}\boldsymbol{F}_{RF}$.

Hybrid precoding combines the benefits of digital and analog precoding, enhancing spectral efficiency and beamforming capabilities while reducing hardware complexity and power consumption. To ensure the total transmit power is distributed uniformly across all subcarriers and data streams, we set $\|\boldsymbol{F}_{RF}\boldsymbol{F}_{BB}\|_F^2 = N_S N_T$, maintaining signal quality and avoiding excessive power in any subcarrier or stream.

B. Threat Model and Precoding Privacy

Although precoding techniques improve signal quality and enhance data transmission rates in wireless communication systems, they also introduce potential privacy risks. The precoding matrix, which contains critical information about the transmitter and connected users, can become a target for malicious actors. This information, including the number of connected users, number and arrangement of antennas, power levels, modulation schemes, and coding techniques, can be used to infer sensitive details about the communication system and

its users, such as their location, movement patterns, network topology, and potentially the content of their communications.

Assume an eavesdropping adversary, an external entity who passively observes communication between the transmitter and users. The adversary in our model is passive and can only observe the perturbed precoding matrix. It cannot actively corrupt users or the system. When the adversary accesses the original precoding matrix components, such as channel gain or phase, it can approximate distances between devices, triangulate positions, and potentially deduce the content of communications, see Fig.2. For instance, by measuring the received signal strength (RSS), the adversary can approximate the distance between a transmitter and the signal receiver. Combining RSS readings from multiple points can help triangulate the device's position. Therefore, safeguarding this information is crucial for ensuring the privacy and security of wireless communication systems.

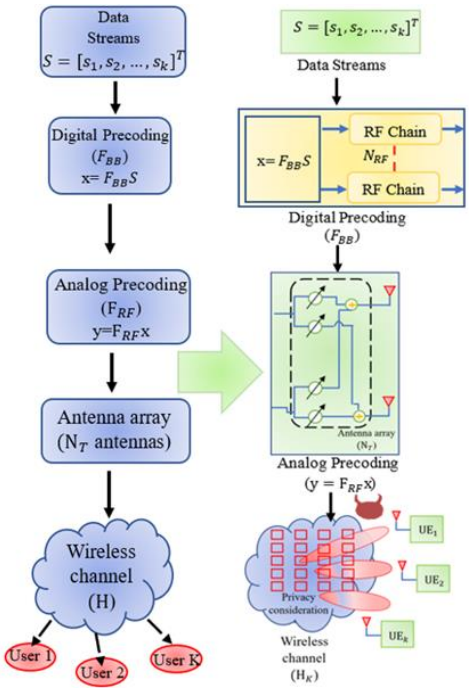


Fig 2. System model diagram illustrating the steps of the precoding algorithm with precoding matrix perturbation the channel matrix, which is a critical component from a privacy perspective, is highlighted as the primary concern for ensuring privacy preservation.

One way to address these challenges is by perturbing the precoding matrix to obfuscate the details and making it difficult for malicious actors to extract meaningful insights. By introducing small variations to the precoding matrix, sensitive information can be concealed, protecting it during transmission. This approach helps maintain the integrity and confidentiality of the communication system, ensuring that the transmitted data remains secure even if intercepted. However, the precoding matrix modification may lead to a degradation in signal quality at the receiver, resulting in inaccuracies or errors in data analysis and interpretation. When the precoding matrix is perturbed, a transmitted signal is altered or disturbed from its intended configuration, making it harder to detect at the receiver, increasing the bit error rate (BER), and potentially degrading communication quality. Therefore, it is indispensable to find a perturbation precoding matrix with a minimum distance from the original precoding matrix for data utility. With careful design, the perturbation can be minimized to ensure BER within acceptable limits while still providing sufficient obfuscation to protect sensitive information.

III. Privacy Considerations in Precoding Techniques

A. Essential Principles of Precoding Privacy

To perturb the precoding matrix, we inject small variations into the precoding matrix $\widetilde{\boldsymbol{F}}_{RF} = \boldsymbol{F}_{RF} + \boldsymbol{W}_{RF}$, where $\widetilde{\boldsymbol{F}}_{RF}$ is the perturbed precoding matrix, and $\boldsymbol{W}_{RF} \in \mathbb{C}^{N_{RF} \times N_T}$ represents a perturbation weights matrix containing controlled variations that are injected into the original precoding matrix $\boldsymbol{F}_{RF}$.

Remark 1. *While $\widetilde{\boldsymbol{F}}_{RF}$ retains the SPD property, we ensure that the added variations satisfy DP guarantees. This ensures that the adversary cannot accurately reconstruct the original precoding matrix $\boldsymbol{F}_{RF}$ or infer individual user inputs, even with knowledge of the SPD structure.*

This process generates a perturbed signal vector $\hat{\mathbf{x}}$ that closely approximates the original signal vector $\mathbf{x}$ at the transmitter. Define $\mathbf{x}$ and $\hat{\mathbf{x}}$ as

$$\mathbf{x} = \boldsymbol{F}_{BB}\boldsymbol{F}_{RF}\boldsymbol{P}^{tr} \tag{1}$$

and

$$\hat{\mathbf{x}} = \boldsymbol{F}_{BB}\widetilde{\boldsymbol{F}}_{RF}\boldsymbol{P}^{tr}\boldsymbol{s}. \tag{2}$$

To ensure data utility, we wish to minimize the mean squared error (MSE) of the perturbed signal $\hat{\mathbf{x}}$ with respect to the original signal $\mathbf{x}$ as $\lim_{N_{RF}\to\infty} \frac{1}{N_{RF}} \sum_{i=0}^{N_{RF}} \mathbb{E}[\|\mathrm{x}_i - \hat{\mathrm{x}}_i\|_2^2]$, where $\mathrm{x}_i \in \mathbf{x}, \forall i \in N_{RF}$.

As a result of perturbation, a valid signal can be converted to another valid signal that is adjacent to it; in this regard, we define adjacency between two signals to identify their similarity. The adjacency measure helps us identify pairs of signals that are close to each other. Adjacency between signals refers to the similarity or closeness of two signals in the signal space (i.e., both the magnitude and direction of the differences between the signals). The adjacency between two signals can be measured as:

$$\mathrm{Adj}(\mathbf{x}, \hat{\mathbf{x}}) = \sqrt{\sum_{i=1}^{n} \left|\mathrm{x}_i - \mathrm{x}_i'\right|^2}. \tag{3}$$

where x_i and x_i' are the i-th elements of $\mathbf{x}$ and $\hat{\mathbf{x}}$, respectively. By considering the adjacency, we apply the perturbation selectively to signals that are sufficiently close, ensuring that perturbing one would not convert to another one, thereby preserving data utility.

Definition 1 (ℓ_2-sensitivity). Suppose that $\mathrm{f}(\mathbf{x})$ is a perturbation function on the signal space $\mathrm{X} = \{\mathbf{x}_1, \dots, \mathbf{x}_{\mathrm{N_{RF}}}\}$. The ℓ_2-Sensitivity can be defined as the maximum (ℓ_2-norm) of the difference in the function outputs for any two arbitrary signals that should be less than or equal to the adjacency between two signals, as follows:

$$\Delta_f = \max_{\mathbf{x},\hat{\mathbf{x}}} \|f(\mathbf{x}) - f(\hat{\mathbf{x}})\|_2 < \mathrm{Adj}(\mathbf{x}, \hat{\mathbf{x}}). \tag{4}$$

The ℓ_2-sensitivity quantifies how much the output of function f can change for adjacent signals when the precoding matrix is perturbed. Ensuring the ℓ_2-sensitivity is less than the adjacency

measure, we can control the extent of perturbation applied to the signal, ensuring it does not convert to another one (i.e., its adjacent signal) and preserving data utility.

Definition 2 (Differential privacy). Consider two adjacent signals $\mathbf{x}, \acute{\mathbf{x}} \in X$, and let Z be the output space from perturbation, and ε and δ be positive real numbers. A mechanism $M: X \to Z$ is said to satisfy (ε, δ)-differential privacy, if for any pair of adjacent signals $Adj(\mathbf{x}, \acute{\mathbf{x}})$, the following condition holds:

$$Pr[M(\mathbf{x}) \in Z] \leq e^{\varepsilon} Pr[M(\acute{\mathbf{x}}) \in Z] + \delta, \quad (5)$$

where ε is the privacy budget controlling the level of privacy, and δ is the acceptable risk of privacy loss. When $\delta = 0$, the mechanism is described as being ε-differentially private.

The choice of ε and δ in the defined differential privacy mechanism is crucial in balancing privacy protection and data utility. A smaller ε implies stronger privacy guarantees. When ε is small, the probability distributions of the mechanism's outputs for adjacent signals (x and x') are very similar. This makes it harder for an adversary to distinguish between them, thereby protecting the privacy of the individual signal. However, a smaller ε often results in more noise being added to the output to achieve the desired level of privacy. This can degrade the utility of the data, making it less accurate or less useful for analysis. δ is a parameter that allows for a small probability of the differential privacy guarantee being violated. A smaller δ means that the privacy guarantee holds with higher probability, thus offering better privacy protection. Lowering δ also typically requires adding more noise to the data. This can reduce the accuracy and utility of the data, similar to the effect of a smaller ε. In contrast, large values of ε and δ maintain higher data utility by adding less noise, thus preserving the accuracy and usefulness of the data. However, they provide weaker privacy guarantees, making it easier for an adversary to distinguish between adjacent signals and potentially infer sensitive information.

Lemma 1. For a perturbation function f with sensitivity Δ_f, there exist an upper bound for the privacy budget ε in ε-differential privacy, as follows:

$$\varepsilon \leq \frac{\Delta_f}{(2\sigma_n^2)\ln\frac{1}{\delta}}, \quad (6)$$

where σ_n^2 is the noise variance.

Proof. See Appendix A. ■

IV. Privacy Preservation Optimization Problem

We here formulate the privacy preservation optimization problem as follows:

$$\begin{aligned} &\min_{\boldsymbol{F}_{RF} \neq \widetilde{\boldsymbol{F}}_i} \max \left\| \boldsymbol{F}_{RF} - \widetilde{\boldsymbol{F}}_i \right\|_F^2 \\ &s.t. \quad C_1: \sup \left\| \boldsymbol{F}_{RF} - \widetilde{\boldsymbol{F}}_i \right\|_F^2 \leq \varepsilon \\ &\quad C_2: \left\| \boldsymbol{P}^{tr} \right\|_F \leq P^{max} \\ &\quad C_3: \left\| \widetilde{\boldsymbol{F}}_i(i,j) \right\|_F = 1 \Big/ \sqrt{N_T} \\ &\quad C_4: BER\left(\widetilde{\boldsymbol{F}}_i\right) \leq \tau, \end{aligned} \quad (7)$$

where $\widetilde{\boldsymbol{F}}_i$ denote specific perturbations, i represents the i-th perturbed precoding matrix that exhibits the maximum similarity to the original matrix. Constraint C_1 defines the privacy budget of the problem limiting the perturbation magnitude. By setting an upper bound (ε) on the Frobenius norm of the difference between the original and perturbed precoding matrices, it ensures that the perturbation does not deviate too much from the original, hence maintaining data utility while masking the transmission characteristics. C_2 ensures that the total transmit power does not exceed a specified maximum value, P^{max}. By capping the transmit power, the power levels remain within a safe and efficient range and help maintain good signal quality. This prevents adversaries from inferring sensitive information caused by excessive power such as signal distortion or interference. C_3 enforces normalization of the elements of the perturbed precoding matrix $\widetilde{\boldsymbol{F}}_i$. This helps balance the signal power distribution across all elements, preserving the signal's integrity and quality. C_4 limits the BER to a maximum threshold (τ) ensuring that the perturbed signal remains within an acceptable error margin, preventing adversaries from easily decoding or interpreting the signal.

Without loss of generality, we define the following BER function to measure data accuracy:

$$BER\left(\widetilde{\boldsymbol{F}}_i\right) = \frac{1}{N_s}\sum_{i=1}^{N_s} \mathbb{I}(y_i \neq \hat{y}_i), \quad (8)$$

where y_i is the actual received signal; $\hat{y}_i$ is the estimated signal obtained through the perturbed beamforming matrix; $\mathbb{I}(\cdot)$ is the indicator function, which returns 1 if the condition inside the parentheses is true, and 0 otherwise. The BER function calculates the average number of symbol errors per symbol due to the perturbation in the precoding matrix.

Constraints C_1 to C_4 work together to balance the dual goals of privacy preservation and data utility. The parameters ε, P^{max}, and $\tau$are crucial in fine-tuning this balance, influencing how much privacy protection is achieved at the expense of data utility and vice versa. ε controls the maximum allowable perturbation. A smaller ε means stricter control over how much the precoding matrix can be altered, which tends to preserve data utility but might weaken privacy. Conversely, a larger ε allows more significant perturbations, enhancing privacy but potentially degrading data utility. Setting P^{max} determines the upper limit of the transmit power. A higher P^{max} can improve signal strength and quality, which is good for data utility but may reveal more about the transmission setup and user data. A lower P^{max} enhances privacy by limiting the power, making it harder for adversaries to extract information from the power levels. τsets the maximum allowable BER. A lower τensures high data quality by minimizing errors, which is beneficial for data utility. However, it might require less perturbation, potentially compromising privacy. A higher τ allows for more errors, enhancing privacy by making the signal harder to decode accurately, but at the cost of data utility.

A. Riemannian Manifold for Privacy Preservation

The precoding matrices in wireless communication systems are SPD matrices and exist in a non-Euclidean space [28], meaning that it does not follow the standard geometric rules of Euclidean space. Thus, to solve the optimization problem (7), we need appropriate mathematical tools of differential geometry that

accurately model this non-Euclidean space. An RM is a fundamental concept in differential geometry, offering a framework for studying the geometric properties of non-Euclidean spaces in which SPD matrices exist. By leveraging the RM framework, we can accurately model the geometric properties of the precoding matrices, e.g., distances, angles, and curvature, and find perturbations (i.e., small changes) to the matrices that align with the intrinsic geometry of the SPD matrix space, resulting in preserving data utility.

When we perturb the precoding matrices—introducing small changes to them—we need to ensure that these perturbations do not destroy the essential characteristics of the matrices. In the context of SPD matrices, this means maintaining their positive definiteness and symmetry. Positive definiteness ensures that the matrices have all positive eigenvalues, which is crucial for maintaining the stability and performance of the signal transmission. Symmetry ensures that the matrix remains unchanged when transposed, which is important for the mathematical operations used in signal processing. If perturbations do not respect the geometric structure of the SPD manifold, the resulting matrices might lose their positive definiteness or symmetry, leading to degraded signal quality and transmission errors. The RM allows us to define and follow geodesics, which are the shortest paths between points on the manifold. By perturbing the matrices along these geodesic paths, we can ensure the changes remain small and controlled, minimizing the distortion of the original matrix properties.

According to SPD matrices, the precoding matrix $\boldsymbol{F}_{RF}$ can be represented as follows:

$$\boldsymbol{F}_{RF} = \boldsymbol{V}\boldsymbol{\Lambda}_{RF}\boldsymbol{V}^{H}, \tag{9}$$

where $\boldsymbol{V}$ identifies the orthogonal matrix containing eigenvectors, and $\boldsymbol{\Lambda}_{RF}$ represents the diagonal matrix containing positive eigenvalues of $\boldsymbol{F}_{RF}$ as follows:

$$\boldsymbol{\Lambda}_{RF} = \mathrm{diag}(\lambda_i),\ \forall i = 1,2,\dots,N_T,\ \lambda_i > 0, \tag{10}$$

Remark 2. *Since $\boldsymbol{F}_{RF}$ is an SPD matrix, it must be square and Hermitian ($\boldsymbol{F}_{RF} = \boldsymbol{F}_{RF}^{H}$), implying $N_{RF} = N_T$.*

Designing a perturbation method based on the RM structure involves treating the space of precoding matrices as a manifold. The manifold represents the space of all possible precoding matrices. Each point on the manifold corresponds to a specific precoding matrix configuration. By identifying neighborhoods around the point that corresponds to the precoding matrix on the manifold, we can achieve small perturbations in matrices that are still close to the original matrix (i.e., with minimum distortion) and have similar characteristics.

Consider a differentiable RM, denoted as $\mathcal{M}_{RF}$, comprising all configurations of the analog precoding matrix $\boldsymbol{F}_{RF}$. The manifold is equipped with the tangent space $T_{F_{RF}}$, and the metric tensor $g_{F_{RF}}$. Each point on the manifold represents a unique configuration of $\boldsymbol{F}_{RF}$. For each point on the manifold (such as $\boldsymbol{F}_{RF}$), we have a tangent space containing all tangent vectors at that specific point. Tangent vectors represent the direction and rate of change of a curve or surface at a specific point on the manifold. The metric tensor [29] is a mathematical concept that defines the inner product of tangent vectors at each point on the manifold, e.g., $g_{F_{RF}}: T_{F_{RF}} \times T_{F_{RF}} \to R$, at $\boldsymbol{F}_{RF}$ point. Indeed, this determines how distances between points (precoding matrices) are measured. Therefore, we can measure how the precoding matrix changes as we move from one point to another on the manifold.

The aim is to find a perturbed precoding matrix $\widetilde{\boldsymbol{F}}_i$ nearby $\boldsymbol{F}_{RF}$ (i.e., introducing small variations in $\boldsymbol{F}_{RF}$) that has the minimum distance from $\boldsymbol{F}_{RF}$ (i.e., similar characteristics) for both privacy and data utility. For this purpose, we need to move along its tangent space $T_{F_{RF}}$, see Fig. 3, respecting the geometry defined by the RM tensor, as follows:

$$T_{F_{RF}} = \left\{ \boldsymbol{v}_i = upper\left(\boldsymbol{F}_{RF}^{-1/2}\ \log_{\boldsymbol{F}_{RF}}(\widetilde{\boldsymbol{F}}_i)\ \boldsymbol{F}_{RF}^{-1/2} \right) \in \mathbb{R}^{N(N+1)/2} \right\}, \tag{11}$$

where $\boldsymbol{v}_i$ denotes the i-th tangent vector of the space, N is the number of points on the tangent space, the $upper(\cdot)$ operator retains the upper triangular part of the matrix and transforms it into a vector $\log_{\boldsymbol{F}_{RF}}(\widetilde{\boldsymbol{F}}_i) : \widetilde{\boldsymbol{F}}_i \to \boldsymbol{v}_i$ where

$$\log_{\boldsymbol{F}_{RF}}(\widetilde{\boldsymbol{F}}_i) = \boldsymbol{F}_{RF}^{1/2}\ \log\left(\boldsymbol{F}_{RF}^{-1/2}\ \widetilde{\boldsymbol{F}}_i\ \boldsymbol{F}_{RF}^{-1/2} \right)\ \boldsymbol{F}_{RF}^{1/2}. \tag{12}$$

There is a logarithmic mapping operator $\log_{\boldsymbol{F}_{RF}}(\widetilde{\boldsymbol{F}}_i) : \widetilde{\boldsymbol{F}}_i \to \boldsymbol{v}_i$, mapping from the surface of the manifold to the tangent space, which is expressed as

$$\log_{\boldsymbol{F}_{RF}}(\widetilde{\boldsymbol{F}}_i) := \boldsymbol{V}\ diag\left(\log(\lambda_1), \dots, \log(\lambda_{N_{RF}})\boldsymbol{V}^{H}\right), \tag{13}$$

and the inverse operation $\exp_{\boldsymbol{F}_{RF}}(\boldsymbol{v}_i) :\ \boldsymbol{v}_i \to \widetilde{\boldsymbol{F}}_i$; the exponential mapping from the tangent space to the surface of the manifold, as follows:

$$\exp_{\boldsymbol{F}_{RF}}(\boldsymbol{v}_i) := \boldsymbol{V}\ diag\left(\exp(\dot{\lambda}_1), \dots, \exp(\dot{\lambda}_{N_{RF}})\boldsymbol{V}^{H}\right), \tag{14}$$

where $\dot{\lambda}_i = |\boldsymbol{v}_i|_{\boldsymbol{F}_{RF}}$ identifies the magnitude of the tangent vector $\boldsymbol{v}_i$.

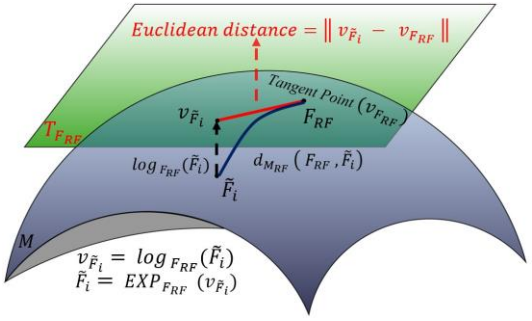


Fig. 3. Configurations of the analog precoding matrix $\boldsymbol{F}_{RF}$ and their corresponding tangent vectors on the differentiable RM, $\mathcal{M}_{RF}$, with tangent space $T_{F_{RF}}$ and metric tensor $g_{F_{RF}}$.

Remark 3. *An RM equipped with an affine-invariant Riemannian metric (AIRM) [30] ensures that the distance between two SPD (precoding) matrices is invariant under affine transformations (such as rotation, scaling, and shearing). The distance between two SPD matrices A and B in the RM is given by the AIRM:*

$$d_{AIRM}(A,B) = \left\| \log\left(A^{-1/2}\ B\ A^{-1/2} \right) \right\|_F. \tag{15}$$

This is particularly useful in maintaining the consistency of distance measures when the precoding matrices undergo transformations during the perturbation process.

Following the AIRM, we rewrite the perturbation optimization problem as follows:

$$\widetilde{\boldsymbol{F}}_i = \arg\min_{\widetilde{\boldsymbol{F}}_i} \sum_{i=1}^{N} \left\| \log\left(\boldsymbol{F}_{RF}^{-1/2}\ \widetilde{\boldsymbol{F}}_i\ \boldsymbol{F}_{RF}^{-1/2} \right) \right\|_F. \tag{16}$$

The perturbation is achieved along geodesic curves [31], which are the shortest paths between points on a manifold. Given two points p and q on the RM, the Riemannian distance is $d_{\mathcal{M}_{RF}}(p,q) = \sqrt{g_p(\boldsymbol{v_p}, \boldsymbol{v_q})}$, where g_p is the tangent vector from tangent points $\boldsymbol{v_p}$ to $\boldsymbol{v_q}$.

The Riemannian distance between two SPD matrices $\boldsymbol{F}_{RF}$ and $\widetilde{\boldsymbol{F}}_i$ on the RM can be calculated using the logarithmic mapping $\log_{\boldsymbol{F}_{RF}}(\widetilde{\boldsymbol{F}}_i)$, as given by

$$d_{\mathcal{M}_{RF}}(\boldsymbol{F}_{RF}, \widetilde{\boldsymbol{F}}_i) := \left\| \log(\boldsymbol{F}_{RF}) - \log(\widetilde{\boldsymbol{F}}_i) \right\|_F. \quad (17)$$

The logarithmic mapping maps $\boldsymbol{F}_{RF}$ and $\widetilde{\boldsymbol{F}}_i$ to the tangent space $T_{F_{RF}}$, where all tangent vectors of $\boldsymbol{F}_{RF}$ can be captured. The tangent vectors represent the direction and magnitude of the smallest change needed to move from $\boldsymbol{F}_{RF}$ to $\widetilde{\boldsymbol{F}}_i$ within the manifold. In this way, we can accurately measure and control the distance between the original $\boldsymbol{F}_{RF}$ and perturbed $\widetilde{\boldsymbol{F}}_i$ precoding matrices, ensuring that perturbations preserve essential characteristics and maintain data utility.

B. Geodesic Distance Analysis for Precoding Perturbation on the Riemannian Manifold

In the Riemannian structure, the geodesic distance between two SPD matrices represents the shortest path between them within the manifold.

Definition 3 (Geodesic). A geodesic is a fundamental path that connects points on the manifold in a way that minimizes the distance according to the metric structure of the manifold. For a pair of points on the manifold $\mathcal{M}$, denoted as p and q, and considering the set of all curves $\dot{\gamma} : [a,b] \to \mathcal{M}$ with $\dot{\gamma}(a) = p$ and $\dot{\gamma}(b) = q$, the geodesic γ is the curve that minimizes the total length $L(\gamma)$:

$$L(\gamma) := \inf\{L(\dot{\gamma}) | \dot{\gamma} : [a,b] \to \mathcal{M}, with\, \dot{\gamma}(a) = p, \dot{\gamma}(b) = q\}. \quad (18)$$

In the context of a perturbed precoding matrix, the geodesic represents the path of minimal distortion between the original matrix $\boldsymbol{F}_{RF}$ and the perturbed matrix $\widetilde{\boldsymbol{F}}_i$ within the RM. This distance can be calculated using logarithmic mapping, which translates the points into the tangent space where the Euclidean norm can be applied.

To construct the geodesic path between $\boldsymbol{F}_{RF}$ and $\widetilde{\boldsymbol{F}}_i$, we first use the logarithmic map to project $\widetilde{\boldsymbol{F}}_i$ onto the tangent space at $\boldsymbol{F}_{RF}$. This gives us a tangent vector $v_i = \log_{\boldsymbol{F}_{RF}}(\widetilde{\boldsymbol{F}}_i)$. The Riemannian distance from $\boldsymbol{F}_{RF}$ to the nearby $\widetilde{\boldsymbol{F}}_i$ closely resembles the Euclidean distance between their corresponding points in the tangent spaces $\boldsymbol{v}_{RF}$ and $\boldsymbol{v}_i$, i.e., $d_{\mathcal{M}_{RF}}(\boldsymbol{F}_{RF}, \widetilde{\boldsymbol{F}}_i) \approx \|\boldsymbol{v}_{RF} - \boldsymbol{v}_i\|_F$. In the tangent space, the shortest path between the origin ($\boldsymbol{v}_{RF}$) and the point v_i is simply a straight line. To map this straight-line path back into the manifold, we use the exponential map.

For a point tv_i (where t is a scalar parameter representing how far along the path we are), the corresponding point on the manifold is $exp_{\boldsymbol{F}_{RF}}(tv_i)$. Considering $v = \log(\boldsymbol{F})$, the geodesic can be expressed as

$$\gamma(t) = \exp\left((1-t)\log(\boldsymbol{F}_{RF}) + t\log(\widetilde{\boldsymbol{F}}_i)\right). \quad (19)$$

where $\gamma(t)$: $[0,1] \to \mathcal{M}$. As t varies from 0 to 1, it determines the linear combination of the logarithms, tracing a path that smoothly transitions from the logarithm of matrix $\boldsymbol{F}_{RF}$ to the logarithm of matrix $\widetilde{\boldsymbol{F}}_i$. When $t = 0$, $\gamma(t) = \log(\boldsymbol{F}_{RF})$; when $t = 1$, $\gamma(t) = \log(\widetilde{\boldsymbol{F}}_i)$. By following geodesics, we can ensure that the perturbations to the precoding matrices are minimal, resulting in preserving data utility.

V. Optimization of Multifaced Precoding Matrices

In the perturbation process by the RM technique, the precoding matrix projects from the manifold to the tangent space and vice versa, which involves intricate transformations. If the projections are not handled carefully, there is a risk that the SPD property could be lost, rendering the matrices invalid in the wireless communication system. To ensure that the intrinsic properties of the matrices (i.e., SPD property- positive definiteness and symmetry) are preserved, we apply congruence transformations, leveraging the congruence invariance property [32] of the Riemannian metric, which guarantees that the geometric properties of the matrices are preserved during these projections.

A. Privacy-Aware Optimization Framework

During the perturbation process, the distance between the original precoding matrix $\boldsymbol{F}_{RF}$ and its perturbed version $\widetilde{\boldsymbol{F}}_i$must be accurately measured to ensure minimal impact on data utility. Congruence invariance guarantees that these distances remain consistent even after transformations, which is vital for maintaining the integrity of the system's performance. Furthermore, this ensures the precoding matrices remain valid (i.e., still SPD) during perturbation in communication systems.

Definition 4 (Congruence transformation). If $\boldsymbol{A}$ is an SPD matrix and $\boldsymbol{X}$ is an invertible matrix, the congruence transformation is expressed as $\boldsymbol{A}' = \boldsymbol{X}^H \boldsymbol{A}\, \boldsymbol{X}$.

Definition 5 (Congruence invariance). Given two SPD matrices $\boldsymbol{A}, \boldsymbol{B} \in \mathcal{M}$, and an invertible matrix $\boldsymbol{X}$, the congruence transformations are defined as:

$$\boldsymbol{A}' = \boldsymbol{X}^H \boldsymbol{A}\, \boldsymbol{X}, \quad (20)$$

and

$$\boldsymbol{B}' = \boldsymbol{X}^H \boldsymbol{B}\, \boldsymbol{X}. \quad (21)$$

The congruence invariance property ensures that the distance between $\boldsymbol{A}$ and $\boldsymbol{B}$ remains unchanged under congruence transformation as follows:

$$d_{AIRM}(\boldsymbol{A}, \boldsymbol{B}) = d_{AIRM}(\boldsymbol{A}', \boldsymbol{B}'), \quad (22)$$

where d_{AIRM} is the distance given by ARIM in (14).

According to Definition 5, the perturbation process maintains the properties of $\boldsymbol{F}_{RF}$ as the SPD matrix if there exists an invertible matrix $\boldsymbol{X}$, so that $d_{AIRM}(\boldsymbol{F}_{RF}, \widetilde{\boldsymbol{F}}_i) = d_{AIRM}(\boldsymbol{X}^H \boldsymbol{F}_{RF}\, \boldsymbol{X}, \boldsymbol{X}^H \widetilde{\boldsymbol{F}}_i\, \boldsymbol{X})$.

Theorem 1. For two SPD precoding matrices $\boldsymbol{F}_{RF}, \widetilde{\boldsymbol{F}}_i \in \mathcal{M}$, there exists a non-singular (invertible) matrix $\boldsymbol{X} \in R^{N_{RF} \times N_{RF}}$ providing the congruence invariance property under the congruence transformation, so that

$$\boldsymbol{X}^H \boldsymbol{F}_{RF}\, \boldsymbol{X} = \mathbf{I}, \quad (23)$$

and

$$\boldsymbol{X}^H \widetilde{\boldsymbol{F}}_i\, \boldsymbol{X} = \boldsymbol{\Lambda_i}, \quad (24)$$

where $\boldsymbol{\Lambda_i} \in \mathbb{F}^{N_{RF} \times N_{RF}}$ states the diagonal matrix containing eigenvalues of $\boldsymbol{F}_{RF}^{-1} \widetilde{\boldsymbol{F}}_i$. $\boldsymbol{F}_{RF}^{-1} \widetilde{\boldsymbol{F}}_i$is a scalar transformation of $\boldsymbol{F}_{RF}$,

which represents the scaling factor applied to the eigenvalues of $\boldsymbol{F}_{RF}$to obtain $\widetilde{\boldsymbol{F}}_i$.

Proof. See Appendix B. ■

Corollary 1. Suppose that $\boldsymbol{F}_{RF}$ and $\widetilde{\boldsymbol{F}}_i$ are nonsingular. For any invertible matrix $\boldsymbol{X}$, we have

$$d_{\mathcal{M}_{RF}}\left(\boldsymbol{X}^H\boldsymbol{F}_{RF}\,\boldsymbol{X},\boldsymbol{X}^H\widetilde{\boldsymbol{F}}_i\,\boldsymbol{X}\right)=d_{\mathcal{M}_{RF}}\left(\boldsymbol{F}_{RF},\widetilde{\boldsymbol{F}}_i\right). \tag{25}$$

Proof. See Appendix C. ■

To simplify the analysis and complex operations, such as logarithmic and exponential mappings, we apply the identity matrix $\mathbf{I}\in\mathbb{C}^{N_{RF}\times N_{RF}}$ as the tangent space basis in our analysis. With the identity matrix as the basis, perturbations can be interpreted as deviations from the identity, making it easier to understand and control the nature and extent of these perturbations, ensuring that the perturbed matrices remain close to the original matrices. Based on the congruence invariance property, the Riemannian distance between the perturbed precoding matrix $\boldsymbol{F}_{RF}$ and the original precoding matrix $\widetilde{\boldsymbol{F}}_i$ with the identity matrix $\mathbf{I}\in\mathbb{C}^{N_{RF}\times N_{RF}}$ as the tangent space can be calculated as follows:

$$\begin{aligned}d_{\mathcal{M}_{RF}}\left(\boldsymbol{F}_{RF},\widetilde{\boldsymbol{F}}_i\right)&=d_{\mathcal{M}_{RF}}\left(\mathbf{I},{\boldsymbol{F}_{RF}}^{-1/2}\,\widetilde{\boldsymbol{F}}_i{\boldsymbol{F}_{RF}}^{-1/2}\right)=\left\|\log(\mathbf{I})-\log\left({\boldsymbol{F}_{RF}}^{-1/2}\,\widetilde{\boldsymbol{F}}_i{\boldsymbol{F}_{RF}}^{-1/2}\right)\right\|_F=\left\|\log\left({\boldsymbol{F}_{RF}}^{-1/2}\,\widetilde{\boldsymbol{F}}_i{\boldsymbol{F}_{RF}}^{-1/2}\right)\right\|_F=\\&\left(\sum_{i=1}^{N_{RF}}\log^2\lambda_i\left({\boldsymbol{F}_{RF}}^{-1}\widetilde{\boldsymbol{F}}_i\right)\right)^{1/2},\end{aligned} \tag{26}$$

where $\boldsymbol{F}_{RF}={\boldsymbol{F}_{RF}}^{-1/2}\,{\boldsymbol{F}_{RF}}^{-1/2}$, and $\lambda_i\left({\boldsymbol{F}_{RF}}^{-1}\widetilde{\boldsymbol{F}}_i\right)$ collect the eigenvalues of ${\boldsymbol{F}_{RF}}^{-1}\widetilde{\boldsymbol{F}}_i$.

Using the geodesic concept, we can calculate the minimum distance the matrices $\mathbf{I}$ and ${\boldsymbol{F}_{RF}}^{-1/2}\,\widetilde{\boldsymbol{F}}_i{\boldsymbol{F}_{RF}}^{-1/2}$ as

$$\begin{aligned}\gamma_0(t)&=\exp\left(\log\left({\boldsymbol{F}_{RF}}^{-1/2}\,\widetilde{\boldsymbol{F}}_i{\boldsymbol{F}_{RF}}^{-1/2}\right)t\right)\\&=\left({\boldsymbol{F}_{RF}}^{-1/2}\,\widetilde{\boldsymbol{F}}_i{\boldsymbol{F}_{RF}}^{-1/2}\right)^t,\end{aligned} \tag{27}$$

where $\gamma_0(t)$ states the geodesic on the RM between $\mathbf{I}$ and ${\boldsymbol{F}_{RF}}^{-1/2}\,\widetilde{\boldsymbol{F}}_i{\boldsymbol{F}_{RF}}^{-1/2}$.

We use the congruence invariance property to ensure that the SPD property of the perturbed matrix is maintained during transformations and perturbations. Therefore, the geodesic path based on the congruence invariance property can be rewritten as follows:

$$\begin{aligned}\gamma(t)&={\boldsymbol{F}_{RF}}^{1/2}\left(\gamma_0(t)\right){\boldsymbol{F}_{RF}}^{1/2}\\&={\boldsymbol{F}_{RF}}^{1/2}\left({\boldsymbol{F}_{RF}}^{-1/2}\,\widetilde{\boldsymbol{F}}_i{\boldsymbol{F}_{RF}}^{-1/2}\right)^t{\boldsymbol{F}_{RF}}^{1/2},\end{aligned} \tag{28}$$

where $\gamma(0)=\boldsymbol{F}_{RF}$ and $\gamma(1)=\widetilde{\boldsymbol{F}}_i$.This ensures that the geodesic is independent of the chosen tangent space basis and provides a smooth transition between the two matrices while preserving their geometric properties.

To move between the manifold and the tangent space, the exponential/logarithmic map for matrices $\boldsymbol{F}_{RF},\widetilde{\boldsymbol{F}}_i$ and $T_{\widetilde{\boldsymbol{F}}_i}\in T_{\boldsymbol{F}_{RF}}$ with $T_{\boldsymbol{F}_{RF}}\subset\boldsymbol{F}_{RF}$ is expressed as follows:

$$\begin{aligned}\widetilde{\boldsymbol{F}}_i&=\exp_{\boldsymbol{F}_{RF}}\left(T_{\widetilde{\boldsymbol{F}}_i}\right)\\&={\boldsymbol{F}_{RF}}^{1/2}\exp\left({\boldsymbol{F}_{RF}}^{-1/2}\,T_{\widetilde{\boldsymbol{F}}_i}{\boldsymbol{F}_{RF}}^{-1/2}\right){\boldsymbol{F}_{RF}}^{1/2},\end{aligned} \tag{29}$$

where

$$T_{\widetilde{\boldsymbol{F}}_i}=\log_{\boldsymbol{F}_{RF}}\left(\widetilde{\boldsymbol{F}}_i\right)={\boldsymbol{F}_{RF}}^{1/2}\log\left({\boldsymbol{F}_{RF}}^{-1/2}\,\widetilde{\boldsymbol{F}}_i{\boldsymbol{F}_{RF}}^{-1/2}\right){\boldsymbol{F}_{RF}}^{1/2}. \tag{30}$$

Theorem 2. On a complete RM $\mathcal{M}$, there exists a unique geodesic between any pair of points, $p,q\in\mathcal{M}$.

Proof. See Appendix D. ■

B. Multifaceted Precoding Matrices

With these newly established geodesics and mappings, we can assess relationships between SPD matrices with minimal distortions in the tangent space. However, when dealing with a substantial dataset containing multiple SPD precoding matrices, determining the appropriate tangent space basis may not be straightforward. Using the identity matrix $\mathbf{I}$ as the tangent space basis may lead to distortions when projecting to the tangent space $T_{\boldsymbol{F}_{RF}}\mathbf{I}$, particularly if the data points are located in regions of the manifold that are far from $\mathbf{I}$. In this case, the geometric mean of the matrices on the manifold can be identified and employed as a reference point.

The Riemannian geometric mean matrix, e.g., $\overline{\boldsymbol{F}}_{RF}$, is the matrix that minimizes the sum of squared Riemannian distances to each of the matrices in the given SPD precoding matrices set. Unlike the arithmetic mean, the geometric mean considers the manifold's curvature. It is affine-invariant, preserving intrinsic properties of SPD matrices such as positive definiteness and symmetry during transformations and projections. Therefore, we construct a tangent space at the geometric mean, $T_{\overline{\boldsymbol{F}}_{RF}}$, and project the SPD precoding matrix onto the tangent space $T_{\overline{\boldsymbol{F}}_{RF}}=\log_{\boldsymbol{F}_{RF}}(\overline{\boldsymbol{F}}_{RF})$.

Given a set of SPD precoding matrix $\{\boldsymbol{F}_{RF,1},\dots,\boldsymbol{F}_{RF,K}\}$ on the RM, a Riemannian geometric mean matrix $\overline{\boldsymbol{F}}_{RF}$ can be expressed as

$$\overline{\boldsymbol{F}}_{RF}=\arg\min_{\overline{\boldsymbol{F}}_{RF}}\sum_{k=1}^{K}d_{AIRM}\left(\overline{\boldsymbol{F}}_{RF},\boldsymbol{F}_{RF,k}\right)^2. \tag{31}$$

The goal is to find the matrix $\overline{\boldsymbol{F}}_{RF}$ within this space that minimizes the sum of squared Riemannian distances to each of the precoding matrices in the set and this is the optimal precoding perturbation matrix. The Riemannian distance $d_{AIRM}\left(\overline{\boldsymbol{F}}_{RF},\boldsymbol{F}_{RF,k}\right)$ is a measure of dissimilarity between the matrices $\overline{\boldsymbol{F}}_{RF}$ and $\boldsymbol{F}_{RF,k}$ on the RM. Based on the AIRM, the optimization problem (31) can be reformulated as follows:

$$\overline{\boldsymbol{F}}_{RF}:=\arg\min_{\overline{\boldsymbol{F}}_{RF}}\sum_{k=1}^{K}\left\|\log\left((\overline{\boldsymbol{F}}_{RF})^{-1/2}\,\boldsymbol{F}_{RF,k}\,(\overline{\boldsymbol{F}}_{RF})^{-1/2}\right)\right\|_F. \tag{32}$$

To compute $\overline{\boldsymbol{F}}_{RF}$, we use an iterative method. We start with an initial point $\overline{\boldsymbol{F}}_{RF}(0)=\boldsymbol{F}_{RF,j}$, selecting one of the matrices randomly, $\boldsymbol{F}_{RF,j},j\in K$. We update $\overline{\boldsymbol{F}}_{RF}$ as follows:

$$\overline{\boldsymbol{F}}_{RF}(t+1)=\overline{\boldsymbol{F}}_{RF}(t)\exp\left(\frac{1}{K}\sum_{k=1}^{K}\log\left((\overline{\boldsymbol{F}}_{RF}(t))^{-1/2}\,\boldsymbol{F}_{RF,k}\,(\overline{\boldsymbol{F}}_{RF}(t))^{-1/2}\right)\right)^{\overline{\boldsymbol{F}}_{RF}(t)} \tag{33}$$

We repeat (33) until convergence, i.e., $\|\overline{\boldsymbol{F}}_{RF}(t+1)-\overline{\boldsymbol{F}}_{RF}(t)\|_F\le\varepsilon$.

By constructing the tangent space at the geometric mean, $T_{\overline{\boldsymbol{F}}_{RF}}$, the projection and analysis are centered around the most representative point. This approach minimizes the overall projection errors and distortions for the entire dataset of SPD matrices. When perturbing the precoding matrices, starting from the geometric mean ensures any changes or optimizations are balanced and less likely to introduce significant deviations. For large datasets of SPD matrices, using the geometric mean simplifies the process of choosing a tangent space basis. Instead of evaluating multiple potential bases, the geometric mean

provides a natural and efficient starting point that is computationally tractable and robust.

VI. Incentive Riemannian Gradient Method

A. Gradient Descent Approach

To solve problem (7), we apply the Riemannian gradient descent algorithm as follows:

$$\widetilde{\boldsymbol{F}}_i(t+1) = \exp_{\widetilde{F}_i}\left(-\eta_t \nabla_{\mathcal{M}} \mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right)\right), \tag{34}$$

where η_t is the step size at iteration t, $\nabla_{\mathcal{M}} \mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right)$ denotes the Riemannian gradient of the objective function in which $\mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right) = \min\limits_{\boldsymbol{F}_{RF} \neq \widetilde{\boldsymbol{F}}_i} \max \left\|\boldsymbol{F}_{RF} - \widetilde{\boldsymbol{F}}_i\right\|_F^2$ is the objective function.

Taking partial derivatives with respect to the elements of $\widetilde{\boldsymbol{F}}_i$ obtains the optimal perturbation precoding matrix for privacy preservation and data utility (see Fig.4). These derivatives guide the iterative update process within the Riemannian gradient descent, allowing for the fine-tuning of the perturbation matrix to strike a balance between minimizing the distance from the original precoding matrix $\boldsymbol{F}_{RF}$ while satisfying the constraints imposed by the privacy budget.

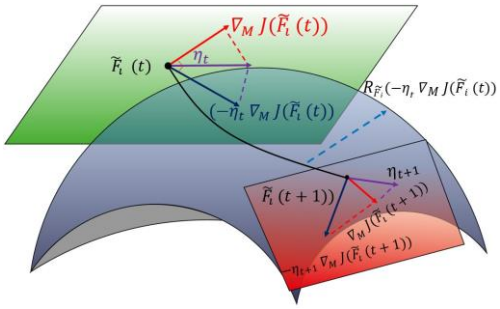


Fig.4. Riemannian gradient descent optimization

Theorem 3. The proposed precoding perturbation method is (ε, δ)-differential privacy.

Proof. See Appendix E. ■

B. Precoding Perturbation Algorithm

We develop a robust precoding perturbation algorithm to find the optimally perturbed precoding matrix that minimizes data distortion, with the pseudo-code presented in Algorithm 1.

Algorithm 1 iteratively adjusts the elements of $\boldsymbol{F}_{RF}$ along the conjugate directions on the RM, using the Riemannian gradient. It efficiently navigates the solution space, utilizing conjugate directions to avoid unnecessary steps and accelerate convergence. The computational complexity of the algorithm is primarily driven by the matrix operations involved in each iteration. Logarithmic and exponential maps and gradient computation, involving matrix operations, have a complexity of $O(N_{RF}^3)$ for $N_{RF} \times N_{RF}$ matrices. Each geodesic update also involves matrix operations and eigen decomposition, $O(N_{RF}^3)$. Suppose that T is the number of iterations until convergence, the overall complexity is $O(N_{RF}^3 T)$.

Algorithm 1. Perturbation Algorithm

1. **Initialize** $\boldsymbol{P}^{tr}$, $\boldsymbol{F}_{RF}$, $\overline{\boldsymbol{F}}_{RF}$, $\boldsymbol{s}$.
2. **Output**: Perturbed precoding matrix $\widetilde{\boldsymbol{F}}_i$.
3. **Set** N_T, N_{RF}, N_s, and K, ε, τ.
4. **Compute** a Riemannian geometric mean matrix
$$\overline{\boldsymbol{F}}_{\boldsymbol{RF}} = \arg\min_{\overline{F}_{RF}} \sum_{k=1}^{K} d_{AIRM}\left(\overline{\boldsymbol{F}}_{RF}, \boldsymbol{F}_{RF,i}\right)^2$$
5. **Construct** the tangent space $T_{\overline{\boldsymbol{F}}_{\boldsymbol{RF}}}$ at $\overline{\boldsymbol{F}}_{\boldsymbol{RF}}$
6. **Set** step size η_t, and $t = 0$.
7. **For** all RF precoding matrices
8. **Repeat**
9. **Project** $\boldsymbol{F}_{RF,i}$ onto the $T_{\overline{\boldsymbol{F}}_{\boldsymbol{RF}}}$:
$$\log_{\overline{\boldsymbol{F}}_{\boldsymbol{RF}}}(\boldsymbol{F}_{RF,i}) = \log\left((\overline{\boldsymbol{F}}_{RF})^{-1/2} \boldsymbol{F}_{RF,i} (\overline{\boldsymbol{F}}_{RF})^{-1/2}\right)$$
10. **Find** $\mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right) := \arg\min \max \left\|\log_{\overline{\boldsymbol{F}}_{\boldsymbol{RF}}}(\boldsymbol{F}_{RF,i}) - \log_{\overline{\boldsymbol{F}}_{\boldsymbol{RF}}}(\widetilde{\boldsymbol{F}}_i)\right\|_F^2$ **so that** $\|\boldsymbol{P}^{tr}\|_F \leq P^{max}$, $\left\|\widetilde{\boldsymbol{F}}_i(i,j)\right\|_F = 1/\sqrt{N_T}$, and $\widetilde{\boldsymbol{F}}_i = \arg\min_{\widetilde{\boldsymbol{F}}_i} \sum_{i=1}^{N} \left\|\log_{\overline{\boldsymbol{F}}_{\boldsymbol{RF}}}(\boldsymbol{F}_{RF,i})\right\|_F$
11. **Compute** the search direction $v_i(t) = \nabla_{\mathcal{M}} \mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right)$
12. **Update** the perturbed precoding matrix $\widetilde{\boldsymbol{F}}_i(t+1) = \mathrm{Exp}_{\boldsymbol{F}_{\boldsymbol{RF}}}\left(-\eta_t \nabla_{\mathcal{M}} \mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right)\right)$
13. **Update** the search direction: $v_i(t+1) = -\nabla_{\mathcal{M}} \mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right)$
14. $t = t + 1$
15. **Until** $\left((BER(\widetilde{\boldsymbol{F}}_i) \leq \tau) \text{ and } (sup\|\boldsymbol{F}_{\boldsymbol{RF}} - \widetilde{\boldsymbol{F}}_i\|_F \leq \varepsilon)\right)$
16. **Update** the precoding matrix $\boldsymbol{F}_{RF,i}$
17. **End for**

VII. Numerical Results

In this section, we evaluate the proposed approach against a privacy-preserving channel estimation scheme labeled as PPCE [21] and a privacy-preserving distributed optimization scheme known as PPDO [22] method. We consider a MIMO network consisting of a BS equipped with $N_T = 16$ antenna elements and $N_{RF} = 8$ RF chains conveying $N_S = 4$ data streams and serves $K = 4$ single-antenna users. We assume each user receives one data stream, and generate random complex-valued vectors for each data stream following a Gaussian distribution. All experiments are conducted over 3000 runs, where each run comprises 1800 random sets of the RF precoding matrix $\boldsymbol{F}_{RF}$ and digital precoding matrix $\boldsymbol{F}_{BB}$. The elements of these matrices are set using the Gaussian random number generation function numpy.random.normal. The bound of the BER is $\tau = 0.01$, the maximum transmission power is $P^{max} = 33$ dB, and the noise variance is $\sigma_n^2 = 0.03$ for all antennas. The key numerical values used in the simulation setup are summarized in Table 2.

Table 2. Simulation parameters

Number of transmitter antennas	$N_T = 64$
Number of RF chains	$N_{RF} = 8$
Number of data streams	$N_S = 4$
Number of users	$K = 4$
Minimum transmit power	$P^{min} = 11\ dB$
Noise variance	$\sigma_n^2 = 0.03$
BER threshold	$\tau = 0.01$
Maximum transmit power	$P^{max} = 33\ dB$
Scaling factor	$0 \leq \alpha \leq 1$
Step size	$0 \leq \eta \leq 1$

We also employ the DeepMIMO dataset for CSI-based precoding matrices and compare the results with those obtained

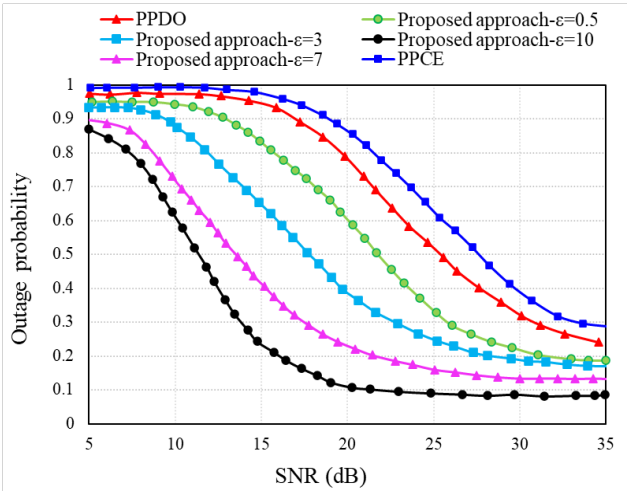
from randomly generated RF precoding matrices. While the random precoding matrix serves as a worst-case scenario since it lacks adaptation to actual channel conditions, the DeepMIMO dataset provides real-world channel characteristics, including spatial correlations, multipath effects, and realistic propagation conditions.

In Fig. 5, we evaluate the outage probability of the proposed method for a random set of RF precoding matrices and CSI-based RF precoding from the DeepMIMO dataset. In the case of random RF precoding matrices, we set the minimum power for reliable communication as $P^{min} = 11$ dB and generate 900 random values for the RF precoding matrix under a Gaussian distribution with zero mean and a standard deviation of 1. We conduct simulations under four different privacy budgets $\varepsilon = 0.5$, $\varepsilon = 3$, $\varepsilon = 7$, and $\varepsilon = 10$. Higher privacy budgets indicate less noise added to the data, and the RF precoding matrix retains more of its original structure and properties, reducing the outage probability, see Fig. 5(a). Furthermore, the superiority of our method is demonstrated in reliability, with the outage probability close to zero in the presence of perturbations to the RF precoding matrix. Two other methods, however, experience a higher outage probability, ranging from 0.2 to 0.6. For instance, with $SNR = 25$ dB, the outage probability is 0.54 for the PPCE and 0.37 for the PPDO, whereas the proposed method with $\varepsilon = 10$ experiences an outage probability of almost 0.15. The near-zero outage probability observed in our method compared to the other methods is from the use of geodesic perturbation in the RM.

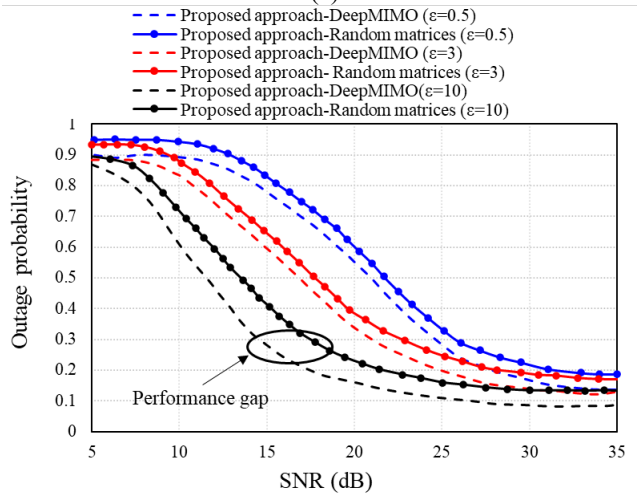
Additionally, the results demonstrate that CSI-based precoding significantly enhances system performance, reducing the outage probability and improving spectral efficiency compared to random RF precoding (see Fig. 5(b)). The DeepMIMO dataset offers precoding matrices derived from realistic CSI, a more structured and realistic representation of the channel, enabling better beamforming and alignment with the channel conditions. This allows for more effective precoding and reduced outages.

In Fig. 6, we evaluate the impact of ℓ_2-sensitivity on the BER of all benchmarks. Fig. 6(a) analyzes the BER using a Gaussian random precoding matrix, where the elements of the RF precoding matrix $\boldsymbol{F}_{RF}$ and digital precoding matrix $\boldsymbol{F}_{BB}$ are generated following a standard normal distribution. We define the ℓ_2-sensitivity based on the adjacency relation of two input signals (3), which imposes stringent conditions to maintain data utility. To measure Δ_f, we set an upper bound for $\mathrm{Adj}(\mathbf{x}, \hat{\mathbf{x}})$ as αs_0 where $s_0 = min_i|x_i - x_i'|$ represents the minimum difference between the input signal components, and $0 \leq \alpha \leq 1$ is a scaling factor. Therefore, according to Definition 1, the ℓ_2-sensitivity should be as $\Delta_f \leq \alpha s_0$. We run the experiments for three adjacency values with $s_0 = 3$, $s_0 = 5$, and $s_0 = 8$.

We also vary α from 0.1 to 0.95. When the scaling factor is small ($\alpha = 0.12$), the perturbations may not effectively preserve the privacy of the wireless users, resulting in compromised performance. Conversely, excessively large scaling factors ($\alpha = 0.83$) can lead to overly aggressive perturbations, causing distortion in the transmitted signals and consequently higher BER. The findings show that the proposed method exhibits a BER of 0.0053 for $\alpha = 0.48$ and $s_0 = 8$, while the PPCE and PPDO schemes suffer higher BER of 0.054 and 0.031, respectively. Our method uses geodesic distances, guiding the perturbations in directions that preserve signal characteristics and minimize information loss. This ensures that the transmitted signals remain closer to their original states, reducing the likelihood of errors and resulting in a lower BER compared to methods that neglect the manifold's geometry.



(a)



(b)

Fig.5. The outage probability versus different SNRs under four different privacy budgets $\varepsilon = 0.5$, $\varepsilon = 3$, $\varepsilon = 7$, and $\varepsilon = 10$. (a) Outage probability under a random set of RF precoding matrices. (b) Comparison of outage probability between random RF precoding matrices and CSI-based RF precoding using the DeepMIMO dataset.

In Fig. 6(b), we investigate the BER using the real-world DeepMIMO dataset and compare the results with those obtained from random precoding matrices. Without leveraging CSI, the system operates blindly, leading to inefficient resource allocation, degraded communication performance, and increased BER. In contrast, the DeepMIMO dataset allows for CSI-aware precoding, enabling more effective beamforming, reduced interference, and improved signal alignment, improving overall system reliability. By leveraging real CSI,

we assess how our approach adapts to practical deployment conditions. The results highlight the robustness of our method, showing that CSI-based precoding achieves significantly lower BER than the randomly generated RF precoding matrices, particularly at lower SNR levels.

We also investigate the impact of the privacy budget on the BER performance of all methods in Fig.7. We consider four various privacy budgets: $\varepsilon = 0.5$, $\varepsilon = 3$, $\varepsilon = 7$, and $\varepsilon = 10$, respectively, and perform simulations under different transmission rates ranging from 0.5×10^5 bit to 3×10^5 bit. The results show that our privacy preservation mechanism significantly experiences lower BER compared to alternative methods. As the transmission rate increases, the BER of PPCE and PPDO schemes significantly increases, whereas our approach shows a steady increase. Additionally, increasing the privacy budget leads to an increase in BER. The primary reason for this is the privacy-preserving mechanism introduces noise that degrades the quality of the transmitted signal, making it more susceptible to errors.

Fig. 8 extends the analysis of Fig. 7 to higher transmission rates, ensuring a comprehensive evaluation of the privacy budget's impact across a broader range of operating conditions. In Fig. 7, the transmission rate is varied from 0.5×10^5 to 3×10^5 bits. This range is relatively low and focuses on understanding BER performance at lower transmission rates. In Fig. 8, the transmission rate is increased to a much higher range, from $2 * 10^5$ to $12 * 10^5$ bits. This expansion allows for a broader analysis of how BER behaves at higher transmission rates, which is critical for evaluating the robustness and scalability of the methods under more demanding conditions. The BER of our method increases with the transmission rate, consistently demonstrating lower values compared to other benchmarks. This is because the method effectively balances privacy with communication reliability, resulting in lower BER across a range of transmission rates.

Fig. 9 investigates privacy loss against sensitivity under different noise variances. We run the experiments under four different noise variances: $\sigma_n^2 = 0.01$, $\sigma_n^2 = 0.1$, $\sigma_n^2 = 0.5$, and $\sigma_n^2 = 0.8$. We vary sensitivity from 0.01 to 0.06. The results show that increasing the noise variance generally leads to a decrease in privacy loss, especially at higher sensitivities. For example, the proposed method incurs a privacy loss of 0.39 under $\sigma_n^2 = 0.01$ and $\Delta_f = 0.045$ whereas it only experiences a privacy loss of 0.18 when $\sigma_n^2 = 0.8$ and $\Delta_f = 0.045$. This is because higher noise variances result in greater perturbations to the output of our proposed privacy function, making it more difficult to infer sensitive information about individual data points. Two PPCE and PPDO schemes suffer privacy losses of 0.58 and 0.41 under $\sigma_n^2 = 0.8$ and $\Delta_f = 0.045$ which is much more than that of the proposed approach. The reason is that these schemes do not adequately perturb the data, resulting in greater privacy loss. Our method does not provide much additional privacy protection at extremely high levels of noise variance. This is because the added noise reaches a point of saturation where further increases in sensitivity have diminishing effects on privacy loss reduction.

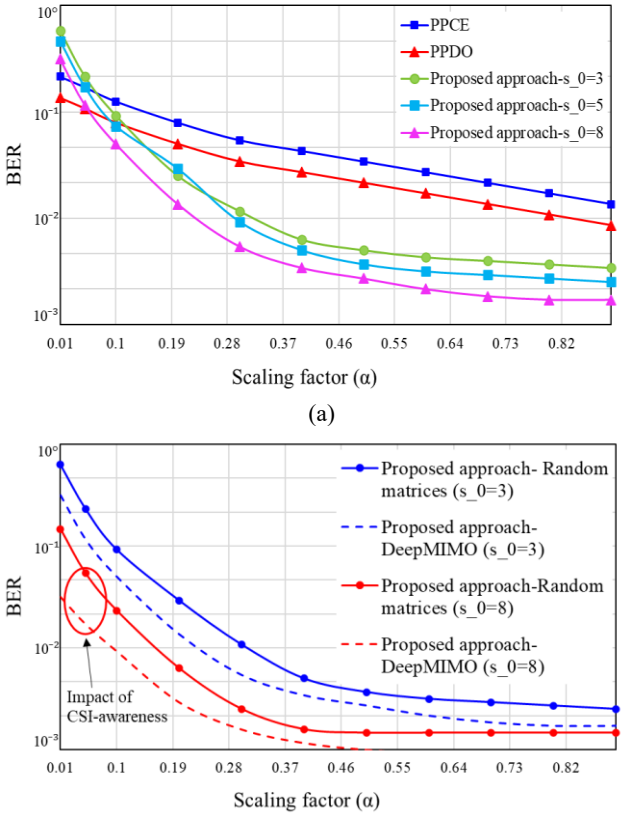


Fig. 6. BER under different scaling factors α for three different adjacency values with $s_0 = 3$, $s_0 = 5$, and $s_0 = 8$. (a) BER analysis using Gaussian random RF precoding matrices. (b) Comparison of BER between random RF precoding matrices and CSI-based RF precoding using the DeepMIMO dataset.

In Fig. 10, we evaluate the privacy loss of our method under both the randomly generated precoding matrix (Fig. 10(a)) and the realistic DeepMIMO dataset (Fig. 10(b)). We quantify privacy risk using a probabilistic scale ranging from 0 to 1, with 0 indicating no risk and 1 indicating certainty of risk. We conduct the simulation for four different privacy risks: $\delta = 0$, $\delta = 0.1$, $\delta = 0.5$, and $\delta = 1$ under noise variance $\sigma_n^2 = 0.5$ over the same sensitivity values in previous experiments. It is shown that the privacy risk directly influences the level of privacy loss experienced in all methods.

As the privacy risk increases, the potential for privacy loss also increases. Factors such as sensitivity and noise variance all contribute to the overall privacy risk. For instance, the privacy loss of our approach is 0.13 under $\Delta_f = 0.01$ and $\delta = 0.5$, while it is 0.29 when $\Delta_f = 0.06$ and $\delta = 0.5$. The results indicate that randomly generated RF precoding matrices exhibit lower privacy loss compared to the DeepMIMO dataset-based scenario. This difference arises because, while randomly generated precoding matrices introduce a high degree of diversity, they may not fully capture the complex spatial dependencies and structural correlations present in real-world channels. Consequently, this can lead to an overestimation or underestimation of privacy loss due to the lack of structured

interference patterns.

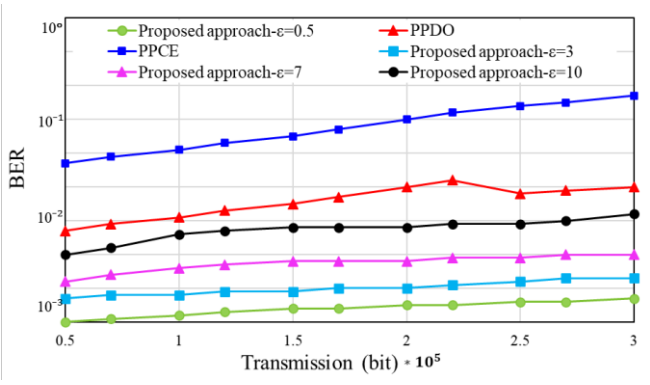


Fig 7. The BER performance under different transmission rates at various privacy budgets: $\varepsilon = 0.5$, $\varepsilon = 3$, $\varepsilon = 7$, and $\varepsilon = 10$.

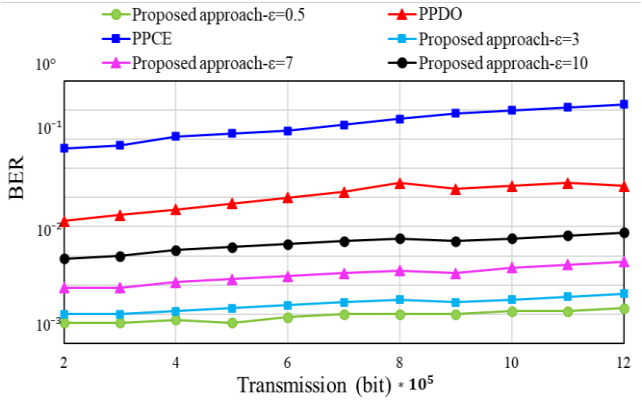


Fig 8. The BER performance for various transmission rates.

Fig. 11 analyzes the impact of the privacy budget on privacy loss under different values of sensitivity for all benchmarks. Four various privacy budgets are set as $\varepsilon = 0.5$, $\varepsilon = 3$, $\varepsilon = 7$, and $\varepsilon = 10$ for $\delta = 0.3$ and $\sigma_n^2 = 0.6$. Our method demonstrates superior performance compared to PPCE and PPDO approaches even in a wide range of privacy budgets, from smaller to larger values. This is because of its robustness and adaptability to varying privacy budgets and sensitivity levels. The results illustrate how our method minimizes privacy loss even in scenarios with high sensitivity, where other approaches may struggle to strike a balance between privacy preservation and data utility.

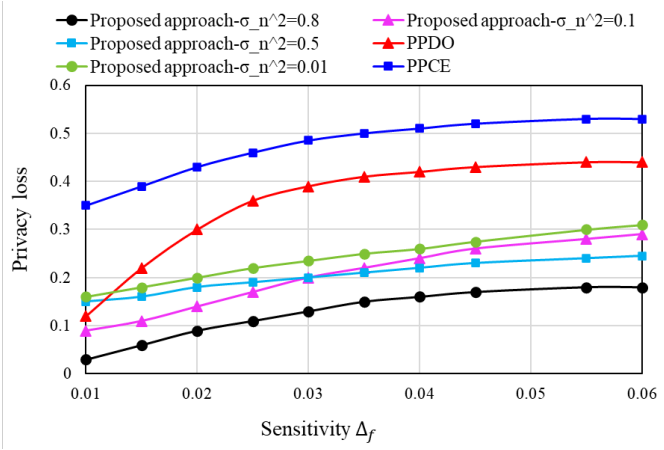
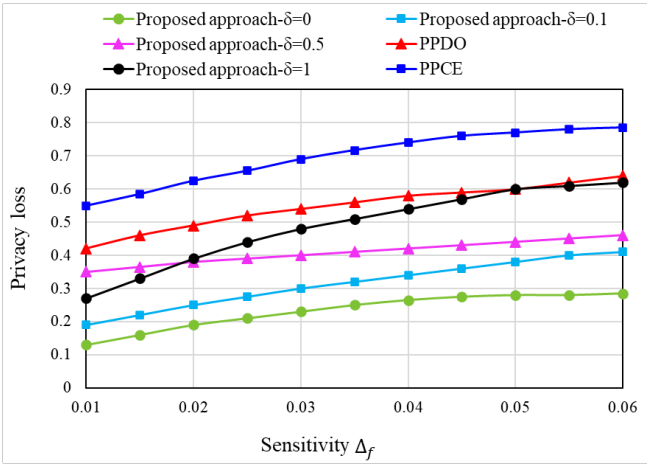
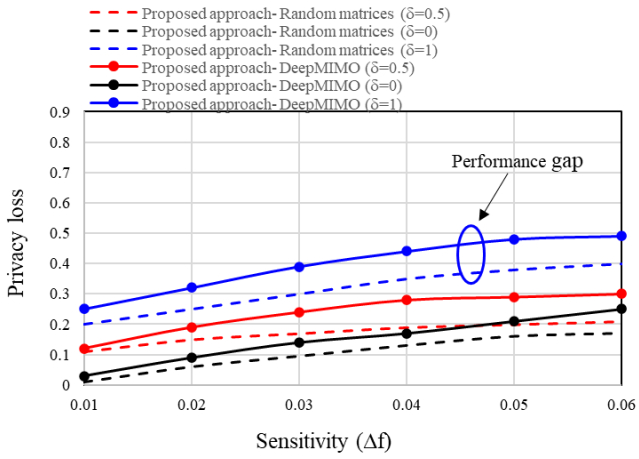


Fig. 9. The impact of sensitivity on privacy loss under different noise variances.



(a)



(b)

Fig. 10. Impact of sensitivity on privacy loss under different privacy risks with noise variance $\sigma_n^2 = 0.5$. (a) Privacy loss analysis using Gaussian random RF precoding matrices. (b) Comparison of privacy loss between random RF precoding matrices and CSI-based RF precoding using the DeepMIMO dataset.

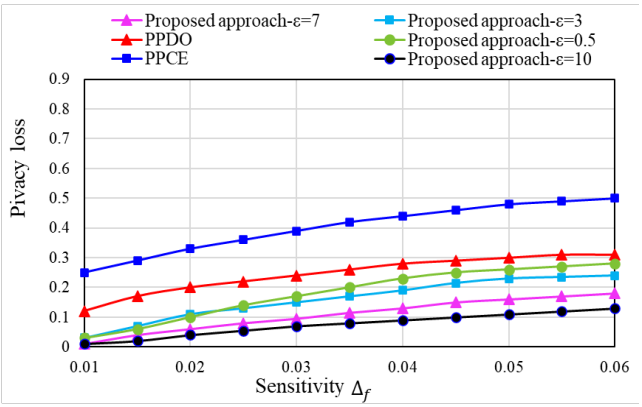


Fig.11. The impact of privacy budget on the privacy loss under different values of sensitivity at $\delta = 0.3$ and $\sigma_n^2 = 0.6$.

VII. CONCLUSION

In this study, we designed a privacy preservation approach for wireless communications that leverages the concept of RM to introduce perturbations to the precoding matrix of the transmitted signals. We analyzed the relationships between different precoding matrix configurations and identified regions of interest for perturbation through an understanding of the geometric properties of the manifold. By following geodesics, we were able to find neighborhoods around each point in the precoding matrix, representing regions where nearby points have similar properties or characteristics. Subsequently, we applied controlled perturbations along geodesics to introduce privacy-preserving modifications. This approach enabled us to modulate the magnitude and direction of perturbations in the precoding matrix, ensuring effective privacy preservation while minimizing distortion to the data space. Through extensive simulations, we demonstrated the efficacy of our proposed approach in achieving robust privacy preservation while maintaining the integrity and utility of the transmitted signals. In future work, we plan to extend the usage of RM techniques to other aspects of wireless communication systems, such as channel estimation, privacy protection and system performance enhancement. An intriguing future direction is to explore how the proposed precoding approach performs in the presence of internal corruption. In particular, we will investigate how to handle internal corruptions effectively and elegantly by leveraging the proposed geometric optimization.

APPENDIX A
PROOF OF LEMMA 1

Suppose f is a deterministic function and σ_n^2 is known. According to (5), we define $p = Pr[f(\mathbf{x}) \in Z]$ and $\acute{p} = Pr[f(\acute{\mathbf{x}}) \in Z]$. From Definition 2, we can write

$$p \leq e^{\varepsilon}. \tag{35}$$

We want to find the maximum value of ε so that (35) holds for all possible subsets X and adjacent signals $\mathbf{x}$ and $\acute{\mathbf{x}}$. Rearranging (35), we have

$$\varepsilon \geq \ln\left(\frac{p}{\acute{p}}\right). \tag{36}$$

Given that p and $\acute{p}$ are probabilities, $\frac{p}{\acute{p}}$ lies in the range [0,1]. So, $\ln\left(\frac{p}{\acute{p}}\right) \leq 0$. To bound ε, we maximize $\ln\left(\frac{p}{\acute{p}}\right)$. This maximum occurs when p is the maximum ($p = 1$) and $\acute{p}$ is the minimum ($\acute{p} = 0$). This means that $f(\mathbf{x})$ is deterministic and always outputs Z for $\mathbf{x}$, and $f(\acute{\mathbf{x}})$ is deterministic and never outputs Z for $\acute{\mathbf{x}}$. In this case, $\ln\left(\frac{p}{\acute{p}}\right) = \ln\left(\frac{1}{0}\right)$, which is undefined. However, $\ln\left(\frac{p}{\acute{p}}\right) \to \infty$ as $\frac{p}{\acute{p}} \to \infty$. Thus, the maximum of $\ln\left(\frac{p}{\acute{p}}\right)$ is infinity. Therefore, the maximum of ε is infinity, which is not meaningful.

To make ε meaningful, we need to bound it. For this purpose, we introduce a noise with variance σ_n^2. According to the Gaussian distribution, for a given sensitivity Δ_f, the added noise should have a standard deviation $\sigma = \frac{\Delta_f}{\left(2\ln\left(1/\delta\right)\right)}$. Now, ε can be bounded by the ratio of the sensitivity to the noise standard deviation as follows:

$$\varepsilon \leq \frac{\Delta_f}{\left(2\sigma_n^2 \ln\left(1/\delta\right)\right)}. \tag{37}$$

This completes the proof. ■

APPENDIX B
PROOF OF THEOREM 1

Since $\boldsymbol{F}_{RF}$ and $\widetilde{\boldsymbol{F}}_i$ are SPD matrices, they can be diagonalized by a unitary matrix. Let $\boldsymbol{U}$ be a unitary matrix such that:

$$\boldsymbol{F}_{RF} = \boldsymbol{U}\boldsymbol{\Lambda}_{RF}\boldsymbol{U}^H, \tag{38}$$

and

$$\widetilde{\boldsymbol{F}}_i = \boldsymbol{U}\boldsymbol{\Lambda}_i\boldsymbol{U}^H, \tag{39}$$

where $\boldsymbol{\Lambda}_{RF}$ and $\boldsymbol{\Lambda}_i$ are diagonal matrices with positive eigenvalues of $\boldsymbol{F}_{RF}$ and $\widetilde{\boldsymbol{F}}_i$, respectively; $\boldsymbol{U}$ is the unitary matrix.

Define $\boldsymbol{X} = \boldsymbol{U}\boldsymbol{\Lambda}^{-1/2}$, where $\boldsymbol{\Lambda}^{-1/2}$ is a diagonal matrix containing the square root of the eigenvalues of $\boldsymbol{F}_{RF}^{-1}\widetilde{\boldsymbol{F}}_i$. $\boldsymbol{X}$ is invertible because $\boldsymbol{\Lambda}$ has positive eigenvalues. Thus,

$$\boldsymbol{X}^H\boldsymbol{X} = \boldsymbol{U}^H\left(\boldsymbol{\Lambda}^{-1/2}\right)^H\boldsymbol{\Lambda}^{-1/2}\boldsymbol{U} = \boldsymbol{U}^H\boldsymbol{U} = \mathbf{I}. \tag{40}$$

We now apply the congruence transformation to $\boldsymbol{F}_{RF}$:

$$\boldsymbol{X}^H\boldsymbol{F}_{RF}\,\boldsymbol{X} = \left(\boldsymbol{U}\boldsymbol{\Lambda}^{-1/2}\right)^H\boldsymbol{F}_{RF}\left(\boldsymbol{U}\boldsymbol{\Lambda}^{-1/2}\right) = \left(\boldsymbol{\Lambda}^{-1/2}\right)^H\boldsymbol{U}^H\boldsymbol{U}\boldsymbol{\Lambda}_{RF}\boldsymbol{U}^H\left(\boldsymbol{U}\boldsymbol{\Lambda}^{-1/2}\right) = \left(\boldsymbol{\Lambda}^{-1/2}\right)^H\boldsymbol{\Lambda}_{RF}\boldsymbol{\Lambda}^{-1/2} = \boldsymbol{I} \tag{41}$$

As a result, $\boldsymbol{X}^H\boldsymbol{F}_{RF}\,\boldsymbol{X} = \boldsymbol{I}$.

Similarly, we imply the congruence transformation to $\widetilde{\boldsymbol{F}}_i$ as $\boldsymbol{X}^H\widetilde{\boldsymbol{F}}_i\,\boldsymbol{X} = \left(\boldsymbol{U}\boldsymbol{\Lambda}^{-1/2}\right)^H\widetilde{\boldsymbol{F}}_i\left(\boldsymbol{U}\boldsymbol{\Lambda}^{-1/2}\right)$. Since $\boldsymbol{F}_{RF}$ and $\widetilde{\boldsymbol{F}}_i$ are SPD matrices, we can define $\boldsymbol{F}_{RF}^{-1}\widetilde{\boldsymbol{F}}_i = \widetilde{\boldsymbol{U}}\boldsymbol{\Lambda}_i\widetilde{\boldsymbol{U}}^H$, where $\widetilde{\boldsymbol{U}}$ is the matrix of the eigenvalues of $\boldsymbol{F}_{RF}^{-1}\widetilde{\boldsymbol{F}}_i$.

On the other hand, we can write $\widetilde{\boldsymbol{F}}_i = \boldsymbol{F}_{RF}\widetilde{\boldsymbol{U}}\boldsymbol{\Lambda}_i\widetilde{\boldsymbol{U}}^H$, thus

$$\begin{aligned}\boldsymbol{X}^H\widetilde{\boldsymbol{F}}_i\,\boldsymbol{X} &= \left(\boldsymbol{U}\boldsymbol{\Lambda}^{-1/2}\right)^H\boldsymbol{F}_{RF}\widetilde{\boldsymbol{U}}\boldsymbol{\Lambda}_i\widetilde{\boldsymbol{U}}^H\left(\boldsymbol{U}\boldsymbol{\Lambda}^{-1/2}\right)\\ &= \left(\boldsymbol{\Lambda}^{-1/2}\right)^H\boldsymbol{U}^H\boldsymbol{U}\boldsymbol{\Lambda}_{RF}\boldsymbol{U}^H\widetilde{\boldsymbol{U}}\boldsymbol{\Lambda}_i\widetilde{\boldsymbol{U}}^H\boldsymbol{U}\left(\boldsymbol{\Lambda}^{-1/2}\right)\\ &= \left(\boldsymbol{\Lambda}^{-1/2}\right)^H\boldsymbol{\Lambda}_{RF}\widetilde{\boldsymbol{U}}\boldsymbol{\Lambda}_i\widetilde{\boldsymbol{U}}^H\left(\boldsymbol{\Lambda}^{-1/2}\right).\end{aligned} \tag{42}$$

Since $\widetilde{\boldsymbol{U}}$ diagonalizes $\boldsymbol{F}_{RF}^{-1}\widetilde{\boldsymbol{F}}_i$, we have

$$\left(\boldsymbol{\Lambda}^{-1/2}\right)^H\boldsymbol{\Lambda}_{RF}\widetilde{\boldsymbol{U}}\boldsymbol{\Lambda}_i\widetilde{\boldsymbol{U}}^H\left(\boldsymbol{\Lambda}^{-1/2}\right) = \widetilde{\boldsymbol{U}}\boldsymbol{\Lambda}_i\widetilde{\boldsymbol{U}}^H. \tag{43}$$

On the other hand, as $\boldsymbol{\Lambda}_{RF}$and $\boldsymbol{\Lambda}_i$ are diagonal, $\left(\boldsymbol{\Lambda}^{-1/2}\right)^H \boldsymbol{\Lambda}_{RF}\boldsymbol{\Lambda}^{-1/2}$ and $\left(\boldsymbol{\Lambda}^{-1/2}\right)^H \boldsymbol{\Lambda}_i\boldsymbol{\Lambda}^{-1/2}$ are also diagonal, and $\boldsymbol{\Lambda}$ is the diagonal matrix with these eigenvalues. Hence,

$$\boldsymbol{X}^H\widetilde{\boldsymbol{F}}_i\,\boldsymbol{X} = \boldsymbol{\Lambda}_i. \tag{44}$$

This demonstrates the existence of matrix $\boldsymbol{X}$ satisfying the specified conditions. This completes the proof.■

APPENDIX C
PROOF OF COROLLARY 1

We first imply the congruence transformation of the matrices by the invertible matrix $\boldsymbol{X}$, i.e., $\boldsymbol{X}^H\boldsymbol{F}_{RF}\,\boldsymbol{X}$ and $\boldsymbol{X}^H\widetilde{\boldsymbol{F}}_i\,\boldsymbol{X}$. Let $(\boldsymbol{X}^H\boldsymbol{F}_{RF}\,\boldsymbol{X})^{-1}$ be the inverse of the congruence transformation of $\boldsymbol{F}_{RF}$. Since $\boldsymbol{F}_{RF}$ is SPD, its inverse is also SPD. To investigate the relative relationship between the two transformed matrices after the transformation, we calculate $(\boldsymbol{X}^H\boldsymbol{F}_{RF}\,\boldsymbol{X})^{-1}\left(\boldsymbol{X}^H\widetilde{\boldsymbol{F}}_i\,\boldsymbol{X}\right)$, which simplifies to $\boldsymbol{X}^{-H}\boldsymbol{F}_{RF}^{-1}\boldsymbol{X}^{-1}\boldsymbol{X}^H\widetilde{\boldsymbol{F}}_i\,\boldsymbol{X} = \boldsymbol{X}^{-H}\left(\boldsymbol{F}_{RF}^{-1}\,\widetilde{\boldsymbol{F}}_i\right)\boldsymbol{X}$, where $\boldsymbol{X}^{-H}$ is the inverse of $\boldsymbol{X}^{-H}$. As a result, the eigenvalues of $\boldsymbol{F}_{RF}^{-1}\,\widetilde{\boldsymbol{F}}_i$are the same as those of $\boldsymbol{X}^H\left(\boldsymbol{F}_{RF}^{-1}\,\widetilde{\boldsymbol{F}}_i\right)\boldsymbol{X}$, i.e.,

$$\lambda_i\left(\boldsymbol{F}_{RF}\,\widetilde{\boldsymbol{F}}_i^{-1}\right) = \lambda_i\left((\boldsymbol{X}^H\boldsymbol{F}_{RF}\,\boldsymbol{X})\left(\boldsymbol{X}^H\widetilde{\boldsymbol{F}}_i\,\boldsymbol{X}\right)^{-1}\right),$$

where $\lambda_i(\cdot)$ denotes the i-th eigenvalue of the matrix. Because the eigenvalues, and thus the essential spectral properties, remain unchanged, the Riemannian distance $d_{\mathcal{M}_{RF}}$ calculated using these eigenvalues is invariant under the transformation. This completes the proof. ■

APPENDIX D
PROOF OF THEOREM 2

Let $p, q \in \mathcal{M}$ be any pair of points on a complete $\mathcal{M}$. We first show that there exists a geodesic connecting p and q. Given that $\mathcal{M}$ is complete, $\forall p \in \mathcal{M}$, there exists a neighborhood U_p containing p such that each pair of points within U_p can be connected by a unique geodesic segment. Now, let A_p be the set of all points in $\mathcal{M}$ that can be connected to p through minimizing geodesic as follows:

$$A_p = \left\{\begin{matrix} x \in \mathcal{M}: there\ is\ a\ minimizing \\ geodesic\ from\ p\ to\ x \end{matrix}\right\}. \tag{45}$$

in which A_p is non-empty since $p \in A_p$. Furthermore, A_p is an open set because geodesics are continuous curves. We now define a set B_p as follows:

$$B_p = \left\{\begin{matrix} x \in \mathcal{M}: there\ is\ a\ minimizing\ geodesic \\ from\ p\ to\ x\ contained\ in\ U_p \end{matrix}\right\}. \tag{46}$$

Similar to A_p, the set B_p is a non-empty open set. All open subsets of $\mathcal{M}$ are complete because $\mathcal{M}$ is complete. According to the Hopf-Rinow theorem [33], any locally compact, connected, and complete space that can connect any two points by minimizing geodesic is also a complete RM. Therefore, B_p is a complete RM. Thus, there exists a complete RM B_p containing p. As a result, there exists a minimizing geodesic connecting any pair of points in B_p (Hopf-Rinow theorem). Hence, there is a minimizing geodesic from p to q contained entirely within B_p, since $q \in B_p$. Consequently, there exists a geodesic connecting p and q in $\mathcal{M}$.

We now demonstrate the uniqueness of this geodesic. Assume two distinct geodesics γ_1 and γ_2 connecting p and q. Because of the characteristics of geodesics, γ_1 and γ_2 must coincide at their initial points, p [34]. In the same way, they have to line up at their terminal point, q, which is fully contained in p in B_p. Consequently, p and q in $\mathcal{M}$ are connected with a geodesic.

Let $L(\gamma)$ be the length function measuring the length of geodesic curves connecting two points p and q. For a smooth curve γ parameterized by t from p to q, the length function is

$$L(\gamma) = \int_p^q \|\dot{\gamma}(t)\|\,dt, \tag{47}$$

where $\dot{\gamma}(t)$ is the derivative (tangent vector) of γ at t, and $\|\dot{\gamma}(t)\|$ is the norm of the tangent vector, which is computed using the Riemannian metric g_p.

Geodesics are critical points of the length functional, meaning that they locally minimize the length among all possible curves connecting the same two points. Since γ_1 and γ_2 are geodesics, they are critical points of $L(\gamma)$. As geodesics are characterized by second-order ordinary differential equations (ODEs), there exists only a single solution that satisfies the equation. This means that if two curves (γ_1 and γ_2) satisfy the geodesic equation and share the same initial position and velocity, they must coincide across all values of the parameter. This uniqueness ensures that γ_1 and γ_2 are the same curve. There is only one geodesic connecting any two points p and q on $\mathcal{M}$. ■

APPENDIX E
PROOF OF THEOREM 3

Let $\widetilde{\boldsymbol{F}}_i$ represents a privacy mechanism implying that $M(\mathbf{x}) = \widetilde{\boldsymbol{F}}_i(t)$. $M(\mathbf{x}) \in Z$ verifies that the constraints are satisfied for $\boldsymbol{F}_{RF}$ and $\widetilde{\boldsymbol{F}}_i$. According to (34), we can express

$$p(M(\mathbf{x}) \in Z) = \widetilde{\boldsymbol{F}}_i(t+1), \tag{48}$$

and

$$p(M(\acute{\mathbf{x}}) \in Z) = \widetilde{\boldsymbol{F}}_i(t). \tag{49}$$

As a result, we have

$$\frac{p(M(\mathbf{x}) \in Z)}{p(M(\acute{\mathbf{x}}) \in Z)} = \frac{\widetilde{\boldsymbol{F}}_i(t+1)}{\widetilde{\boldsymbol{F}}_i(t)}$$
$$= \exp\left(-\eta_t\nabla_{\mathcal{M}}\mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right) + \eta_{t-1}\nabla_{\mathcal{M}}\mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t-1)\right)\right). \tag{50}$$

Based on the triangle inequality, the following is derived:

$$\left\|\eta_t\nabla_{\mathcal{M}}\mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right) + \eta_{t-1}\nabla_{\mathcal{M}}\mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t-1)\right)\right\|_F \leq$$
$$|\eta_t|\left\|\nabla_{\mathcal{M}}\mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right)\right\|_F + |\eta_{t-1}|\left\|\nabla_{\mathcal{M}}\mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t-1)\right)\right\|_F. \tag{51}$$

On the other hand, we have

$$\left\|\boldsymbol{F}_{RF} - \widetilde{\boldsymbol{F}}_i\right\|_F^2 = \sum_{n,k}\left(\boldsymbol{F}_{RF}(n,k) - \widetilde{\boldsymbol{F}}_i(n,k)\right)^2. \tag{52}$$

Differentiating (52) with respect to the eigenvalues yields:

$$\frac{\partial\|\boldsymbol{F}_{RF}-\widetilde{\boldsymbol{F}}_i(t)\|^2}{\partial\lambda_{n,k}} = 2\left(\left\|\boldsymbol{F}_{RF} - \widetilde{\boldsymbol{F}}_i(t)\right\|_F\right)\frac{\partial}{\partial\lambda_{n,k}}\left(\boldsymbol{F}_{RF} - \widetilde{\boldsymbol{F}}_i(t)\right). \tag{53}$$

Based on the function $\mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right)$, we can obtain

$$\|\nabla\boldsymbol{J}\|_F \leq \left(4\sum_{n,k}\left(\boldsymbol{F}_{RF}(n,k) - \widetilde{\boldsymbol{F}}_i(n,k)\right)^2\left(\frac{\partial}{\partial\lambda_{n,k}}\left(\boldsymbol{F}_{RF} - \widetilde{\boldsymbol{F}}_i(t)\right)\right)^2\right)^{1/2}. \tag{54}$$

Due to the constraint C_1, we have:

$$\left|\frac{\partial}{\partial\lambda_{n,k}}\left(\boldsymbol{F}_{RF} - \widetilde{\boldsymbol{F}}_i(t)\right)\right| < \epsilon, \tag{55}$$

Given that ϵ is a constant, from (51), we have

$$|\eta_t|\left\|\nabla_{\mathcal{M}}\mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t)\right)\right\|_F + |\eta_{t-1}|\left\|\nabla_{\mathcal{M}}\mathbf{J}\left(\widetilde{\boldsymbol{F}}_i(t-1)\right)\right\|_F$$

$$\leq 4\varepsilon\ (\varepsilon^2\ \epsilon^2\ N_{RF}\ K)^{1/2} = 4\varepsilon^2\epsilon(\ N_{RF}\ K)^{1/2}. \tag{56}$$

Let $C = 4\varepsilon^2\epsilon(\ N_{RF}\ K)^{1/2}$, thus, we can rewrite (50) as

$$\frac{p(M(\mathbf{x})\in Z)}{p(M(\acute{\mathbf{x}})\in Z)} \leq e^C. \tag{57}$$

Without loss of generality, we consider $e^C = \delta$, given the constancy of C. Therefore, (57) can be rewritten as

$$p(M(\mathbf{x}) \in Z) \leq e^{\varepsilon^2} p(M(\acute{\mathbf{x}}) \in Z) + \delta, \tag{58}$$

and this completes the proof. ■

ACKNOWLEDGMENT

This work was supported in part by the Natural Science Foundation of Shanghai under Grant 24ZR1407100, and in part by the National Natural Science Foundation of China under Grant 61571135.

REFERENCES

[1] X. S. Shen, C. Huang, D. Liu, L. Xue, W. Zhuang, R. Sun, and B. Ying, "Data Management for Future Wireless Networks: Architecture, Privacy Preservation, and Regulation," *IEEE Netw.*, vol. 35, no. 1, pp. 8-15, January/February 2021.

[2] M.M. Saeed, M.K. Hasan, A.J. Obaid, et al., "A comprehensive review on the users' identity privacy for 5G networks," *IET Commun.*, vol. 16, no. 5, pp.384-399, 2022.

[3] T. Peng, W. Zhong, G. Wang, et al., "Privacy-Preserving Truth Discovery Based on Secure Multi-Party Computation in Vehicle-Based Mobile Crowdsensing," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 7, pp. 7767-7779, July 2024.

[4] H.K. Alper, and A. Küpçü, "Optimally efficient multi-party fair exchange and fair secure multi-party computation," *ACM Trans. Privacy and Security*, vol. 25, no. 1, pp.1-34, 2021.

[5] R. Nieminen, and K. Järvinen, "Practical privacy-preserving indoor localization based on secure two-party computation," *IEEE Trans. Mobile Comput.*, vol. 20, no. 9, pp. 2877-2890, 2021.

[6] B. Alaya, L. Laouamer, and N. Msilini, "Homomorphic encryption systems statement: Trends and challenges," *Computer Sci. Review*, vol. 36, no. 8, p.100235, 2020.

[7] Z. Zhang, P. Cheng, J. Wu, and J. Chen, "Secure state estimation using hybrid homomorphic encryption scheme," *IEEE Trans. Control Syst. Technol.*, vol. 29, no. 4, pp. 1704-1720, July 2021.

[8] Y. Zhang, H. Wen, X. Weitao, C. Chun Tung, and H. Jiankun "Continuous authentication using eye movement response of implicit visual stimuli." P*roc. ACM Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, no. 4, pp.1-22, 2018.

[9] T. Zhang, Sh. Yiran Zh. Guangrong, W. Lin, Ch. Xiaoming, B. Lu, and Zh. Yuanfeng "Swift-eye: Towards anti-blink pupil tracking for precise and robust high-frequency near-eye movement analysis with event cameras," *IEEE Trans. Visualization Computer Graphics,* vol. 30, no. 5, pp. 2077-2086, May 2024.

[10] S.S. Albouq, A.A. Abi Sen, A. Namoun et al., "A double obfuscation approach for protecting the privacy of IoT location based applications," *IEEE Access*, *vol. 8, pp. 129415-129431, 2020.*

[11] B. Ma, X. Wang, W. Ni et al., "Personalized location privacy with road network-indistinguishability," *IEEE Trans. Intell. Transp. Syst.,* vol. 23, no. 11, pp. 20860 – 20872, 2022.

[12] N. Hrovatin, A. Tošić, M. Mrissa, and J. Vičič, "A general purpose data and query privacy preserving protocol for wireless sensor networks," *IEEE Trans. Info. Forensics Secur.*, vol. 18, pp. 4883-4898, 2023.

[13] A.V. Jambha, D. Swetchana, K. Sushrutha, et al, "Securing Layers: The Synergy of Mix Networks and Shamir's Secret Sharing in Onion Routing," *2nd Int'l Conf. Intelligent Data Commun. Technol. and Internet of Things (IDCIoT)*, Bengaluru, India, 2024, pp. 448-453.

[14] I. Karunanayake, N. Ahmed, R. Malaney, R. Islam, and S.K. Jha, "Darknet Traffic Analysis: Investigating the Impact of Modified Tor Traffic on Onion Service Traffic Classification," *IEEE Access,* vol. 11, pp. 70011-70022, 2023.

[15] Y.T. Tsou, H. Zhen, S.Y. Kuo, et al., "SPARR: Spintronics-based private aggregatable randomized response for crowdsourced data collection and analysis," *Computer Commun.*, vol. 152, pp.8-18. February 2020.

[16] S. Li, H. Xu, J. Wang et al., "Hierarchical Perceptual Noise Injection for Social Media Fingerprint Privacy Protection," *IEEE Trans. Image Proces.*, vol. 33, pp. 2714-2729, 2024.

[17] M. Yamac, M. Ahishali, N. Passalis, J. Raitoharju, B. Sankur, and M. Gabbouj, "Multi-level reversible data anonymization via compressive sensing and data hiding," *IEEE Trans. Info. Forensics Secur.*, vol. 16, pp. 1014-1028, 2021.

[18] T. Zhu, D. Ye, W. Wang, W. Zhou, and S.Y. Philip, "More than privacy: Applying differential privacy in key areas of artificial intelligence," *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 6, pp. 2824-2843, 1 June 2022,

[19] S.A. Soleymani, S. Goudarzi, M.H. Anisi, H. Cruickshank, A. Jindal, and N. Kama, "TRUTH: Trust and authentication scheme in 5G-IIoT," *IEEE Trans. Ind. Informatics*, vol. 19, no. 1, pp. 880-889, Jan. 2023.

[20] X. Yuan, W. Ni, M. Ding, et al., "Amplitude-varying perturbation for balancing privacy and utility in federated learning," *IEEE Trans. Info. Forensics Secur.*, vol. 18, pp. 4546-4560, 2023.

[21] B. Jiang, J. Li, H. Wang, and H. Song, "Privacy-preserving federated learning for industrial edge computing via hybrid differential privacy and adaptive compression," *IEEE Trans. Ind. Informatics*, vol. 19, no. 2, pp. 1136-1144, Feb. 2023.

[22] K. Wei, J. Li, M. Ding, et al., "User-level privacy-preserving federated learning: Analysis and performance optimization," *IEEE Trans. Mobile Comput.*, vol. 21, no. 9, pp. 3388-3401, 1 Sept. 2022.

[23] J. Xu, X. Wang, P. Zhu, and X. You, "Privacy-preserving channel estimation in cell-free hybrid massive MIMO systems," *IEEE Trans. Wirel. Commun.*, vol. 20, no. 6, pp. 3815-3830, June 2021.

[24] Q. Li, R. Heusdens, and M.G. Christensen, "Privacy-preserving distributed optimization via subspace perturbation: A general framework," *IEEE Trans. Signal Process.*, vol. 68, pp. 5983-5996, 2020.

[25] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1550-1573, Third Quarter 2014.

[26] D. A. Tubail, M. Alsmadi and S. Ikki, "Physical Layer Security in Downlink of Cell-Free Massive MIMO With Imperfect CSI," *IEEE Trans. Info. Forensics Secur.*, vol. 18, pp. 2945-2960, 2023.

[27] L. Hu, S. Tan, H. Wen, J. Wu, J. Fan, S. Chen, and J. Tang, "Interference Alignment for Physical Layer Security in Multi-User Networks With Passive Eavesdroppers," *IEEE Trans. Info. Forensics Secur.*, vol. 18, pp. 3692-3705, 2023.

[28] Xu, J. Xie, Y. Wu, L. Xu, and J. Huang, "Adaptive Precoding for Massive MIMO Systems with Non-linear Power Amplifiers," IEEE Trans. Wirel. Commun., vol. 20, no. 1, pp. 384-397, Jan. 2021.

[29] S.T. Smith, "Optimization techniques on Riemannian manifolds," *arXiv preprint arXiv:1407.5965*, 2014.

[30] Y. Thanwerdas, and X. Pennec, "O (n)-invariant Riemannian metrics on SPD matrices," *Linear Algebra and its Applications*, vol. *661*, pp.163-201, 2023.

[31] L. -H. Lim, R. Sepulchre and K. Ye, "Geometric Distance Between Positive Definite Matrices of Different Dimensions," *IEEE Trans. Info. Theory*, vol. 65, no. 9, pp. 5401-5405, Sept. 2019.

[32] M. Moakher, P.G. and Batchelor, "Symmetric positive-definite matrices: From geometry to applications and visualization," *Visualization and processing of tensor fields*, pp. 285-298, Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.

[33] I. Ekeland, "The Hopf-Rinow theorem in infinite dimension," *Journal of Differential Geometry*, vol. 13, no. 2, pp.287-301, 1978.

[34] D. Carmo, M. Perdigao, and J. Flaherty Francis, "*Riemannian geometry*," vol. 2. Boston: Birkhäuser, 1992.

Azadeh Pourkabirian received her Ph.D. in Computer Engineering from Science and Research Branch, Azad University, Tehran, Iran, in 2018. Currently, she is a Research Fellow with the School of Computer Science and Statistics at Trinity College Dublin, Ireland, and a Visiting Researcher with the Real-Time and Embedded Computing Systems Research Centre (CISTER) in Porto, Portugal. She was an Assistant Professor at Qazvin Azad University, Iran. Her research interests include wireless communications, signal processing, channel estimation, and game theory.

Wei Ni (M'09-SM'15-F'24) received the B.E. and Ph.D. degrees in Electronic Engineering from Fudan University, Shanghai, China, in 2000 and 2005, respectively. He is a Senior Principal Research Scientist at CSIRO and a Conjoint Professor at the University of New South Wales. He was a Postdoctoral Research Fellow at Shanghai Jiaotong University from 2005 -- 2008; Deputy Project Manager at the Bell Labs, Alcatel/Alcatel-Lucent from 2005 to 2008; and Senior Researcher at Devices R&D, Nokia from 2008 to 2009. He has co-authored five book chapters, more than 300 journal papers, more than 100 conference papers, 27 patents, and ten standard proposals accepted by IEEE. His research interests include machine learning, online learning, stochastic optimization, and their applications to system efficiency and integrity. Dr. Ni has been an Editor for IEEE Transactions on Wireless Communications since 2018, an Editor for IEEE Transactions on Vehicular Technology since 2022, an Editor for IEEE Transactions on Information Forensics and Security and IEEE Communications Surveys and Tutorials since 2025, and an Editor for IEEE Transactions on Network Science and Engineering since 2025. He served first as the Secretary, then the Vice-Chair and Chair of the IEEE VTS NSW Chapter from 2015 to 2022, Track Chair for VTC-Spring 2017, Track Co-chair for IEEE VTC-Spring 2016, Publication Chair for BodyNet 2015, and Student Travel Grant Chair for WPMC 2014.

Xiaolin Zhou (Senior Member, IEEE) received the B.S. degree from Xidian University, China, in 1996, and the Ph.D. degree in communications and information systems from Shanghai Jiaotong University, Shanghai, China, in 2003. From 2005 to 2006, he was a Visiting Researcher with Monash University, Australia. He is currently an Associate Professor with the Department of Communication Science and Engineering, Fudan University, China. His research interests include physical layer security, wireless precoding MIMO communications, wireless multi-user communications, and iterative detection.

Kai Li (S'09--M'14--SM'20) received the B.E. degree from Shandong University, China, in 2009, the M.S. degree from The Hong Kong University of Science and Technology, Hong Kong, in 2010, and the Ph.D. degree in computer science from The University of New South Wales, Sydney, NSW, Australia, in 2014. Currently, he is a Visiting Research Scholar with the School of Electrical Engineering and Computer Science, TU Berlin, Germany, and a Senior Research Scientist with the CISTER Research Centre, Porto, Portugal. He is also a CMU-Portugal Research Fellow, jointly supported by Carnegie Mellon University (CMU), Pittsburgh, PA, USA, and the Foundation for Science and Technology (FCT), Lisbon, Portugal. From 2023 to 2024, he was a Visiting Research Scientist with the Division of Electrical Engineering, Department of Engineering, University of Cambridge, UK. In 2022, he was a Visiting Research Scholar with the CyLab Security and Privacy Institute, CMU. Prior to this, he was a Post-Doctoral Research Fellow with the SUTD-MIT International Design Centre, Singapore University of Technology and Design, Singapore, from 2014 to 2016. He has also held positions as a Visiting Research Assistant with the ICT Centre, CSIRO, Brisbane, QLD, Australia, from 2012 to 2013, and a full-time Research Assistant with the Mobile Technologies Centre, The Chinese University of Hong Kong, Hong Kong, from 2010 to 2011. He has been an Associate Editor of journals, such as Internet of Things (Elsevier) since 2024, Nature Computer Science (Springer) since 2023, Computer Communications (Elsevier) and Ad Hoc Networks (Elsevier) since 2021, and IEEE ACCESS from 2018 to 2024.

Mohammad Hossein Anisi is currently a reader with the School of Computer Science and Electronic Engineering, University of Essex, U.K. and Head of Internet of Everything (IoE) Laboratory. Prior to that, he worked as a Senior Researcher with the University of East Anglia, U.K. and Senior Lecturer with the University of Malaya, Malaysia, where he received the Excellent Service Award for his achievements. His research interests include IoT, WSN, Vehicular Networks and Cybersecurity. He has published more than 150 articles in high-quality journals and received several international and national funding awards for his fundamental and practical research as PI and Co-I. He is an Associate Editor of IEEE Transactions on Cybernetics, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Automation Science and Engineering and IEEE Transactions on AgriFood Electronics. Moreover, he has been lead organizer of special sessions and workshops at IEEE conferences such as ICC, CAMAD, PIMRC, and VTC.