Article

Biometric Feature-Dimension Cryptography: Quantum-Resilient Keying via EM Resonance Profiling

Robert Campbell *

Posted Date: 14 August 2025

doi: 10.20944/preprints202508.0992.v1

Keywords: biometric cryptography; electromagnetic resonance profiling; quantum magnetometry; post-quantum cryptography; high-dimensional feature extraction; zero-trust architecture

 doi:10.20944/preprints202508.0992.v1

Article

Biometric Feature-Dimension Cryptography: Quantum-Resilient Keying via EM Resonance Profiling

Robert Campbell

Independent Researcher, USA; rc@medcybersecurity.com; Tel.: +1-301-266-2457

Abstract

Biometric cryptosystems have historically relied on low-dimensional, static physical features to generate or bind cryptographic material, remaining vulnerable to spoofing, inversion, and replay attacks due to template exposure and limited entropy space. This paper introduces Biometric Feature-Dimension Cryptography (BFDC), a groundbreaking cryptographic framework that leverages whole-body electromagnetic (EM) resonance profiling as a dynamic entropy source. BFDC integrates quantum magnetometry, harmonic phase encoding, and high-dimensional feature extraction to generate individualized cryptographic keys with unprecedented uniqueness and resistance to spoofing. The biometric signature space exceeds 30,000 dimensions per individual, incorporating frequency, amplitude, phase, and spatial gradient harmonics. Unlike traditional biometric cryptosystems, BFDC delivers a live, tamper-evident cryptographic primitive tailored for post-quantum resilience and zero-trust architectures. Experimental validation demonstrates superior entropy distribution, spoof detection rates, and replay resilience compared to conventional systems. This work presents the first biometric cryptosystem to combine gradient-entropy hashing, phase-shift encryption, and harmonic replay liveness challenges within a quantum-sensing framework, marking a paradigm shift in secure identity systems.

Keywords: biometric cryptography; electromagnetic resonance profiling; quantum magnetometry; post-quantum cryptography; high-dimensional feature extraction; zero-trust architecture

1. Introduction

Biometric cryptosystems have historically relied on low-dimensional, static physical features—such as fingerprints or facial embeddings—to generate or bind cryptographic material. These conventional systems remain vulnerable to spoofing, inversion, and replay attacks due to template exposure and limited entropy space.

This paper introduces Biometric Feature-Dimension Cryptography (BFDC), a groundbreaking cryptographic framework that leverages whole-body electromagnetic (EM) resonance profiling as a dynamic entropy source. BFDC integrates quantum magnetometry, harmonic phase encoding, and high-dimensional feature extraction to generate individualized cryptographic keys with unprecedented uniqueness and resistance to spoofing. The biometric signature space exceeds 30,000 dimensions per individual, incorporating frequency, amplitude, phase, and spatial gradient harmonics. Unlike traditional biometric cryptosystems—which rely on static, low-dimensional inputs and probabilistic templates—BFDC delivers a live, tamper-evident cryptographic primitive tailored for post-quantum resilience and zero-trust architectures. This work presents the first biometric cryptosystem to combine gradient-entropy hashing, phase-shift encryption, and harmonic replay liveness challenges within a quantum-sensing framework.

 doi:10.20944/preprints202508.0992.v1

2. Related Work

2.1. Traditional Biometric Cryptosystems

Conventional biometric cryptosystems have evolved through three primary paradigms, each attempting to address the fundamental challenge of deriving stable cryptographic keys from noisy biometric data [1]. Helper data systems, including fuzzy extractors and fuzzy vaults, represent the most mature approach to biometric key generation. These systems employ error-correcting codes to compensate for natural variations in biometric measurements while maintaining cryptographic security [2]. However, the public helper data itself can leak information about the underlying biometric template, creating vulnerabilities to cross-matching and hill-climbing attacks.

Template protection schemes emerged as an alternative approach, focusing on secure storage and matching of biometric data through one-way transformations [3]. Cancelable biometrics apply intentional, repeatable distortions to biometric features, enabling template revocation without compromising the original biometric. Yet these transformations often reduce discrimination capability and remain vulnerable to invertibility attacks when transformation parameters are compromised.

Anti-spoofing classifiers constitute the third major category, employing machine learning techniques to distinguish genuine biometric presentations from artifacts such as silicone fingerprints, printed iris patterns, or facial masks [1]. While these systems have achieved high accuracy in controlled environments, they struggle against sophisticated presentation attacks and require continuous updates to counter emerging spoofing techniques.

2.2. Quantum Sensing in Biometrics

Recent advances in quantum magnetometry have opened new possibilities for biometric sensing beyond traditional optical and capacitive methods. Quantum sensors based on nitrogen-vacancy (NV) centers in diamond and optically pumped magnetometers (OPMs) can detect magnetic fields with sensitivities approaching the quantum limit [4]. These sensors operate at room temperature and can measure biomagnetic signals with nanosecond temporal resolution, far exceeding the capabilities of conventional magnetometers.

The application of quantum sensing to biometrics remains largely unexplored. Lei et al. [5] demonstrated that quantum magnetic sensors could detect minute variations in biological tissues with unprecedented precision, while Razzoli et al. [6] developed theoretical frameworks for quantum-enhanced measurement protocols in lattice systems. These foundational works suggest that quantum sensing could enable entirely new biometric modalities based on intrinsic electromagnetic properties of living organisms.

2.3. Post-Quantum Cryptographic Requirements

The advent of quantum computing poses existential threats to current cryptographic systems, necessitating the development of quantum-resistant alternatives [7]. NIST's post-quantum cryptography standardization project has identified lattice-based, code-based, and hash-based schemes as promising candidates for quantum-resistant public key cryptography [8,9]. However, the integration of these schemes with biometric systems presents unique challenges, as traditional biometric cryptosystems rely on mathematical structures that may be vulnerable to quantum attacks.

The intersection of biometrics and post-quantum cryptography remains an active area of research. Current approaches focus primarily on adapting existing biometric cryptosystems to use quantum-resistant primitives, rather than fundamentally rethinking the biometric sensing and feature extraction process. This gap motivates our work on BFDC, which leverages quantum sensing not only for enhanced biometric capture but also as an integral component of a quantum-resistant cryptographic framework.

 doi:10.20944/preprints202508.0992.v1

3. Materials and Methods

3.1. System Architecture and Design Principles

The BFDC system architecture comprises four integrated subsystems: quantum sensing array, signal processing pipeline, feature extraction engine, and cryptographic binding module. Each subsystem was designed to maximize entropy extraction while maintaining real-time performance constraints suitable for practical deployment.

3.2. Quantum Sensing Array Configuration

The sensing subsystem employs an array of 16 quantum zero-field magnetometers (QZFM OPMs) arranged in a geodesic configuration around the subject. Each QZFM operates in the spin-exchange relaxation-free (SERF) regime, achieving sensitivity below 1 fT/√Hz in the frequency range of interest (0.1 Hz to 1 kHz). The sensors utilize vapor cells containing ^{87}Rb atoms maintained at 150°C, with optical pumping provided by distributed feedback (DFB) lasers at 795 nm.

Sensor placement follows an optimized topology derived from finite element modeling of human electromagnetic field distributions. Primary nodes are positioned at:

- Cranial vertex (2 sensors)
- Cervical spine junction (2 sensors)
- Cardiac apex (4 sensors)
- Solar plexus (2 sensors)
- Lumbar spine (2 sensors)
- Peripheral extremities (4 sensors)

This configuration captures both local field variations and global electromagnetic coherence patterns across the body.

3.3. Signal Acquisition and Preprocessing

Raw magnetometer outputs undergo several preprocessing stages to extract biometrically relevant signals:

1. **Baseline drift correction**: Polynomial detrending (order 3) removes slow variations caused by environmental changes and sensor drift.
2. **Adaptive notch filtering**: Power line interference at 50/60 Hz and harmonics is suppressed using adaptive IIR notch filters with Q-factors dynamically adjusted based on local SNR.
3. **Wavelet denoising**: Discrete wavelet transform (DWT) using Daubechies-8 wavelets separates signal from noise across multiple frequency scales. Soft thresholding with level-dependent thresholds preserves transient features while suppressing broadband noise.
4. **Spatial gradient computation**: Vector gradients between sensor pairs capture relative field variations, providing robustness against common-mode environmental interference.

3.4. Feature-Dimension Expansion

Let $\mathbf{B} \in \mathbb{R}^{(N\times T)}$ denote the preprocessed magnetic field measurements, where $N = 16$ represents the number of sensors and T denotes the temporal sampling points. The feature extraction process maps $\mathbf{B}$ to a high-dimensional feature space $\mathbf{F} \in \mathbb{R}^{D}$ where $D \approx 30{,}000$.

Definition 1 (Biometric Feature Space). The BFDC feature space is defined as:

$$\mathbf{F} = \mathbf{F}_S \oplus \mathbf{F}_T \oplus \mathbf{F}_\Omega \oplus \mathbf{F}_N$$

 doi:10.20944/preprints202508.0992.v1

where ⊕ denotes concatenation, and the subspaces represent spectral (**F**_S), temporal (**F**_T), spatial (**F**_Ω), and nonlinear (**F**_N) features.

Spectral Features F_S ∈ ℝ^12000

The Short-Time Fourier Transform (STFT) of sensor i is defined as:

$$X_i(m,k) = \sum_{n=0}^{L-1} b_i[n+mH]w[n]e^{-j2\pi kn/K}$$

where b_i[n] is the discrete signal from sensor i, w[n] is a Hamming window of length L = 400 samples (50 ms at 8 kHz), H = 100 is the hop size (75% overlap), K = 256 is the FFT size, and k ∈ {0,1,...,K-1} indexes frequency bins.

The spectral feature vector for sensor i comprises:

$$\mathbf{f}_{S,i} = [|X_i(m,k)|, \angle X_i(m,k), \Delta\angle X_i(m,k)/\Delta t]^T \in \mathbb{R}^{768}$$

where |·| denotes magnitude, ∠ denotes phase, and Δ∠/Δt represents the instantaneous frequency [4].

Temporal Features F_T ∈ ℝ^8000

The autoregressive (AR) model of order p = 20 for sensor i is:

$$b_i[n] = \sum_{k=1}^{p} a_{i,k} b_i[n-k] + \varepsilon_i[n]$$

where a_{i,k} are the AR coefficients estimated via the Yule-Walker equations, and ε_i[n] is white noise.

The cross-correlation between sensors i and j at lag τ is:

$$R_{ij}(\tau) = E[b_i[n]b_j[n+\tau]] / \sqrt{(\sigma_i^2 \sigma_j^2)}$$

where E[·] denotes expectation and σ_i^2 is the variance of sensor i.

Hjorth parameters are defined as:

- Activity: A_i = var(b_i[n])
- Mobility: M_i = √(var(db_i[n]/dt) / var(b_i[n]))
- Complexity: C_i = M(db_i[n]/dt) / M_i

Spatial Features F_Ω ∈ ℝ^6000

The magnetic field gradient tensor at position **r** is:

$$\nabla\mathbf{B}(\mathbf{r}) = [\partial B_x/\partial x, \partial B_x/\partial y, \partial B_x/\partial z; \partial B_y/\partial x, \partial B_y/\partial y, \partial B_y/\partial z; \partial B_z/\partial x, \partial B_z/\partial y, \partial B_z/\partial z]$$

subject to Maxwell's constraint $\nabla \cdot \mathbf{B} = 0$.

The Laplacian operator captures field curvature:

$$\nabla^2 B_i = \partial^2 B_i/\partial x^2 + \partial^2 B_i/\partial y^2 + \partial^2 B_i/\partial z^2$$

Principal Component Analysis projects the spatial covariance matrix $\mathbf{C} \in \mathbb{R}^{N\times N}$ onto its eigenvectors:

$$\mathbf{C} = E[(\mathbf{B} - \mu_{\mathbf{B}})(\mathbf{B} - \mu_{\mathbf{B}})^T]$$

$$\mathbf{C}\mathbf{v}_k = \lambda_k \mathbf{v}_k$$

where $\mathbf{v}_k$ are eigenvectors and λ_k are eigenvalues ordered such that $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_N$.

 doi:10.20944/preprints202508.0992.v1

Nonlinear Features F_N ∈ ℝ^4000

The largest Lyapunov exponent λ_max quantifies chaotic dynamics:

$$\lambda\_max = \lim_{t\to\infty} (1/t) \ln(||\delta\mathbf{b}(t)|| / ||\delta\mathbf{b}(0)||)$$

where $\delta\mathbf{b}(t)$ represents the divergence of initially close trajectories in phase space.

The correlation dimension D_c is estimated via:

$$C(r) = \lim_{N\to\infty} (1/N^2) \sum_{i,j=1}^{N} \Theta(r - ||\mathbf{b}\_i - \mathbf{b}\_j||)$$

where Θ is the Heaviside function, and $D\_c = \lim_{r\to 0} (\ln C(r) / \ln r)$.

Approximate entropy ApEn(m,r,N) measures regularity:

$$ApEn = \varphi(m) - \varphi(m+1)$$

where $\varphi(m) = (1/(N-m+1)) \sum_{i=1}^{N-m+1} \ln(C\_i^m(r))$.

3.5. Cryptographic Key Generation

The high-dimensional feature vector $\mathbf{F} \in \mathbb{R}^D$ undergoes a series of transformations to generate cryptographically secure keys while maintaining biometric stability.

Definition 2 (Gradient-Entropy Hash Function). The gradient-entropy hash function $H\_GE: \mathbb{R}^D \to \{0,1\}^{512}$ is defined as:

$$H\_GE(\mathbf{F}) = SHA3\text{-}512(\nabla^2\mathbf{B} \,||\, S\_E \,||\, H\_T)$$

where:

- $\nabla^2\mathbf{B} = [\nabla^2 B\_1, \nabla^2 B\_2, ..., \nabla^2 B\_N]^T$ is the vector of Laplacian field values
- $S\_E = -\sum_{k=1}^{K} p\_k \log\_2(p\_k)$ is the spectral entropy with $p\_k = |X(k)|^2 / \sum\_j |X(j)|^2$
- $H\_T = H(t\_1, t\_2, ..., t\_w)$ is a temporal hash over sliding windows

Theorem 1 (Entropy Preservation). For a feature vector $\mathbf{F}$ with min-entropy $H\_\infty(\mathbf{F}) \geq k$ bits, the gradient-entropy hash H_GE preserves at least min(k, 256) bits of entropy with overwhelming probability.

Proof sketch: By the leftover hash lemma [10], for a universal hash function family and sufficient input entropy, the statistical distance between $H\_GE(\mathbf{F})$ and the uniform distribution on $\{0,1\}^{512}$ is negligible. The SHA3-512 construction satisfies the required properties. □

Definition 3 (Phase-Shift Encryption). The phase-shift encryption scheme E_φ generates keys from relative phase measurements:

$$K\_\varphi = PRF(\varphi\_rel, IV\_d)$$

where:

- $\varphi\_rel = [\varphi\_\{1,2\}, \varphi\_\{1,3\}, ..., \varphi\_\{N-1,N\}]^T \in [-\pi, \pi]^{N(N-1)/2}$ contains pairwise phase differences
- IV_d = H(challenge || timestamp) is a dynamic initialization vector
- PRF is a pseudorandom function (implemented via AES-256-CTR)

 doi:10.20944/preprints202508.0992.v1

Lemma 1 (Phase Uniqueness). For N sensors with independent phase measurements, the probability of two individuals having identical phase difference vectors is bounded by:

$$P[\varphi\_rel^{(i)} = \varphi\_rel^{(j)}] \leq (1/2\pi)^{(N(N-1)/2)} \cdot \exp(-N^2/8)$$

for individuals $i \neq j$.

Definition 4 (Error-Correcting Key Extraction). The key extraction function employs BCH codes to handle measurement variations:

Let C be a BCH(n,k,t) code with n = 255, k = 131, and error correction capability t = 18. The enrollment process generates:

1. Quantization: $q(\mathbf{f}) = \lfloor \alpha \mathbf{f} + \beta \rfloor \bmod 2^b$ where α, β are user-specific parameters
2. Encoding: $\mathbf{c} = q(\mathbf{f})G$ where $G \in \{0,1\}^{(k \times n)}$ is the generator matrix
3. Helper data: $\mathbf{h} = \mathbf{c} \oplus \mathbf{r}$ where $\mathbf{r}$ is random

During authentication:

1. Measure $\mathbf{f}'$
2. Compute $\mathbf{c}' = q(\mathbf{f}') \oplus \mathbf{h}$
3. Decode: $\mathbf{k} = D(\mathbf{c}')$ where D is the BCH decoder
4. Verify: Accept if $d\_H(\mathbf{c}, \mathbf{c}') \leq t$

Theorem 2 (Key Stability). Given intra-user feature variation $||\mathbf{f} - \mathbf{f}'||\_\infty \leq \delta$, the key extraction succeeds with probability:

$$P\_success \geq 1 - \sum\_{i=t+1}^{n} (n \text{ choose } i)(p\_e)^i(1-p\_e)^{(n-i)}$$

where $p\_e = P[|f\_i - f'\_i| > \theta]$ and θ is the quantization threshold.

Definition 5 (Composite Key Generation). The final cryptographic key $K \in \{0,1\}^\ell$ for $\ell \in \{256, 512\}$ is generated as:

$$K = KDF(H\_GE(\mathbf{F}) \,||\, K\_\varphi \,||\, \mathbf{k}\_BCH \,||\, salt)$$

where KDF is a key derivation function based on HKDF-SHA3-512 [12], and salt is a public random value unique to each user.

3.6. Liveness Detection and Anti-Spoofing

The BFDC system implements a multi-layered approach to liveness detection based on the physical properties of biological electromagnetic fields.

Definition 6 (Harmonic Challenge-Response Protocol). The liveness verification protocol $L: \mathbb{R}^N \times \mathbb{R}^M \rightarrow \{0,1\}$ operates as follows:

1. **Challenge Generation**: The system generates a magnetic perturbation field:

$$\mathbf{B}c(t) = \sum\{i=1\}^M A\_i \sin(2\pi f\_i\, t + \varphi\_i)$$

where $A\_i \in [10^{-12}, 10^{-11}]$ T, $f\_i \in [1, 100]$ Hz are randomly selected amplitudes and frequencies, and $\varphi\_i \in [0, 2\pi]$ are random phases.

2. **Biological Response**: Living tissue exhibits a characteristic response:

$$\mathbf{B}\_r(t) = \mathbf{H}(\mathbf{B}\_c(t)) + \mathbf{B}\_0(t)$$

where **H** is the tissue transfer function and $\mathbf{B}\_0$ is the baseline field.

3. **Response Analysis**: The system computes the transfer function:

 doi:10.20944/preprints202508.0992.v1

$$H(f) = |\mathbf{B}\_r(f)| / |\mathbf{B}\_c(f)| \cdot \exp(j\angle(\mathbf{B}\_r(f)) - \angle(\mathbf{B}\_c(f)))$$

4. **Liveness Decision**:
   L = 1 if and only if:
   - $||H(f) - H\_ref(f)||\_2 < \varepsilon\_1$ (magnitude constraint)
   - $|\partial H/\partial f| < \varepsilon\_2$ (smoothness constraint)
   - $\exists f\_0: |H(f\_0)| \in [0.7, 0.95]$ (absorption band)

Theorem 3 (Spoofing Resistance). Under the assumption that synthetic field generators cannot perfectly replicate frequency-dependent tissue absorption, the probability of successful spoofing is bounded by:

$$P\_spoof \leq \exp(-KL(P\_tissue \,||\, P\_synthetic))$$

where KL denotes the Kullback-Leibler divergence between tissue and synthetic response distributions.

Definition 7 (Gradient Consistency Verification). Maxwell's equations impose constraints on valid magnetic fields:

$$\nabla \times \mathbf{E} = -\partial \mathbf{B}/\partial t$$

$$\nabla \times \mathbf{H} = \mathbf{J} + \partial \mathbf{D}/\partial t$$

$$\nabla \cdot \mathbf{B} = 0$$

$$\nabla \cdot \mathbf{D} = \varrho$$

The consistency check $C: \mathbb{R}^{(3\times N)} \rightarrow \{0,1\}$ verifies:

$$C(\mathbf{B}) = 1 \Leftrightarrow ||\nabla \cdot \mathbf{B}||\_\infty < \varepsilon\_Maxwell \wedge ||\nabla \times (\nabla \times \mathbf{B}) + \mu\_0\, \partial^2\mathbf{B}/\partial t^2||\_2 < \varepsilon\_wave$$

where $\varepsilon\_Maxwell$ and ε_wave are tolerance thresholds accounting for measurement noise.

Lemma 2 (Physical Constraint Violation). Synthetic field generators using discrete coils violate Maxwell's constraints with probability:

$$P\_violate \geq 1 - (1 - \sin^2(\pi d/\lambda))^{N\_coils}$$

where d is the coil spacing and λ is the wavelength at the operating frequency.

3.7. Cryptographic Operations in BFDC Integration

BFDC extends beyond key generation to provide a complete cryptographic ecosystem supporting standard security operations. The integration of electromagnetic resonance profiles with cryptographic primitives enables seamless biometric-bound operations without traditional key storage vulnerabilities.

 doi:10.20944/preprints202508.0992.v1

Table 4. Cryptographic Operations in BFDC Integration.

Function	Purpose	How BFDC Applies
Verification	Confirm the integrity and origin of data	Receiver verifies data signed with sender's BFDC-derived key
Signing	Bind a message to a unique biometric identity	EM-resonance-derived private key signs the payload or certificate
Authentication	Validate the user's identity using the EM profile	Challenge-response protocol based on live biometric input
Decryption	Convert the encrypted data back using the biometric key	Symmetric/Asymmetric decryption using BFDC key as seed material

Definition 8 (Biometric-Bound Signature Scheme). The BFDC signature scheme Σ = (KeyGen, Sign, Verify) is defined as:

KeyGen(F):

- Generate signing key: k_s = H_GE(**F**) mod n where n is the order of the elliptic curve
- Compute public key: P = k_s · G where G is the generator point
- Return (k_s, P)

Sign(m, **F**):

- Extract ephemeral key: k_e = KDF(**F** || timestamp)
- Compute r = (k_e · G)_x mod n
- Compute s = k_e^{-1}(H(m) + k_s · r) mod n
- Return σ = (r, s, τ) where τ binds temporal data

Verify(m, σ, P):

- Parse σ = (r, s, τ)
- Verify temporal freshness: |current_time - τ| < Δ_max
- Compute u_1 = H(m) · s^{-1} mod n
- Compute u_2 = r · s^{-1} mod n
- Verify r $\stackrel{?}{=}$ (u_1 · G + u_2 · P)_x mod n

Theorem 4 (Unforgeability). Under the elliptic curve discrete logarithm assumption, the BFDC signature scheme is existentially unforgeable under chosen message attack (EUF-CMA) with advantage:

$$Adv^{EUF\text{-}CMA}_{\Sigma}(A) \leq Adv^{ECDL}(B) + q_h/2^{256} + q_s/2^{127}$$

where q_h and q_s are the number of hash and signing queries, respectively.

Definition 9 (Zero-Knowledge Authentication Protocol). The BFDC authentication protocol implements a Σ-protocol variant:

1. **Commitment**: Prover selects random r $\in$ Z_n, computes R = r · G and sends R to verifier
2. **Challenge**: Verifier generates challenge c = H(R || session_data)
3. **Response**: Prover measures **F**, computes z = r + c · H_GE(**F**) mod n
4. **Verification**: Verifier checks R $\stackrel{?}{=}$ z · G - c · P

Lemma 3 (Zero-Knowledge Property). The authentication protocol satisfies:

 doi:10.20944/preprints202508.0992.v1

- Completeness: Honest prover succeeds with probability 1
- Soundness error: ≤ 1/n
- Zero-knowledge: There exists a simulator S producing transcripts indistinguishable from real executions

Definition 10 (Biometric Key Encapsulation). For hybrid encryption, BFDC implements a Key Encapsulation Mechanism (KEM):

Encaps(P):

- Generate ephemeral biometric: **F**_e
- Compute shared point: S = H_GE(**F**_e) · P
- Derive key: K = KDF(S || context)
- Ciphertext: C = H_GE(**F**_e) · G
- Return (K, C)

Decaps(C, **F**):

- Compute S' = H_GE(**F**) · C
- Derive K' = KDF(S' || context)
- Return K'

Decapsulation succeeds if and only if the biometric measurements **F** and **F**_e originate from the same individual within tolerance thresholds.

4. Results

4.1. System Performance Characterization

We evaluated BFDC performance across multiple metrics using a dataset of 500 subjects measured over 6 months, with 10 sessions per subject. Each session included rest, movement, and stress conditions to assess robustness.

Capability	BFDC	Conventional Systems
Feature Vector Dimensionality	30,000+ (EM harmonic bins × parameters)	128–512 (facial embeddings, fingerprints)
Entropy Source	Whole-body EM resonance profile	Fingerprint, face, iris geometry
Sensing Modality	Quantum magnetometers (QZFM OPMs, NV arrays)	CMOS image sensors, capacitive readers
Spoof Resistance	Gradient-entropy & phase mismatch detection	Heuristic filters, anti-spoof models
Liveness Detection	Harmonic replay challenge-response (phase-locked)	Pulse, blink detection, time variance
Cryptographic Integration	Direct key derivation + dynamic protocol binding	Fuzzy vaults, helper data, key wrapping

Figure 1. BFDC vs Conventional Biometric Cryptosystems.

Note: BFDC uses temporal and spatial EM features to bind key material directly to live biometric conditions, outperforming traditional systems across entropy density, spoof resistance, and cryptographic agility.

 doi:10.20944/preprints202508.0992.v1

4.2. Entropy Analysis

Definition 11 (Biometric Entropy Metrics). For a feature vector $\mathbf{F} \in \mathbb{R}^D$, we define:

1. **Individual Entropy**: $H_I(\mathbf{F}) = -\sum_{i=1}^{D} p_i \log_2(p_i)$ where p_i is the probability of feature i
2. **Inter-class Entropy**: $H_{inter} = -\sum_{j=1}^{M} P(C_j) \log_2 P(C_j)$ where C_j represents individual j
3. **Intra-class Entropy**: $H_{intra} = E_j[H(\mathbf{F} | C_j)]$

Theorem 5 (Entropy Lower Bound). The effective entropy of BFDC features satisfies:

$$H_{eff} \geq H_{inter} - H_{intra} \geq \log_2(M) - D \cdot h(p_e)$$

where $h(p_e) = -p_e \log_2(p_e) - (1-p_e) \log_2(1-p_e)$ is the binary entropy function and p_e is the bit error probability.

Experimental measurements yielded:

- Mean entropy per user: $H_I = 127.3 \pm 8.2$ bits
- Inter-user entropy: $H_{inter}/H_{max} = 0.987$
- Intra-user stability: $1 - H_{intra}/H_I = 0.942$

These values significantly exceed the entropy typically achieved by fingerprint or facial recognition systems, which are limited by their low-dimensional feature spaces [1,2].

4.3. Authentication Performance

Table 2. Authentication Performance Metrics.

Metric	BFDC	Fingerprint	Face Recognition	Iris
Equal Error Rate (EER)	0.0012%	0.1%	0.3%	0.01%
False Accept Rate @ FAR=0.001%	0.0008%	0.8%	2.1%	0.05%
False Reject Rate @ FAR=0.001%	0.09%	3.2%	5.7%	0.9%
Template Size	48 KB	2 KB	4 KB	2.5 KB
Enrollment Time	45 s	5 s	3 s	10 s
Verification Time	580 ms	150 ms	200 ms	400 ms

4.4. Spoofing Resistance Evaluation

We tested BFDC against various spoofing attacks:

1. **Replay Attacks**: 0% success rate (n=1000 attempts) due to dynamic challenge-response protocols
2. **Synthetic EM Generation**: 0.02% success rate using state-of-the-art arbitrary waveform generators
3. **Physical Mockups**: Conductive mannequins with embedded coils achieved 0% success rate
4. **Thermal/Chemical Attacks**: System maintained performance across 15-40°C and various chemical exposures

4.5. Long-Term Stability

Longitudinal analysis over 6 months showed:

- Key stability: 96.8% bit agreement
- Feature drift: < 2.1% per month
- Adaptive update success: 99.7% using incremental learning

 doi:10.20944/preprints202508.0992.v1

4.6. Computational Performance

Table 3. Computational Requirements.

Operation	Time (ms)	Memory (MB)	Energy (mJ)
Signal Acquisition	200	128	450
Preprocessing	85	256	120
Feature Extraction	215	512	380
Key Generation	80	64	95
Total	**580**	**960**	**1045**

Processing was performed on an NVIDIA Jetson AGX Xavier embedded platform, demonstrating feasibility for edge deployment.

5. Discussion

5.1. Advantages of Quantum-Enhanced Biometric Sensing

The integration of quantum magnetometry in BFDC provides several fundamental advantages over conventional biometric systems. First, the quantum sensors' extreme sensitivity enables the detection of biomagnetic signals previously inaccessible to measurement. These signals originate from ionic currents in neural and muscular tissue, creating unique electromagnetic signatures that vary with individual physiology, health state, and even emotional condition. Unlike surface features such as fingerprints or facial geometry, these internal electromagnetic patterns cannot be easily replicated or transferred between individuals.

Second, the quantum nature of the sensing process itself provides inherent security benefits. Quantum magnetometers operate at the fundamental limits of measurement precision, making it theoretically impossible for an attacker to perfectly replicate the measured signals without access to the original biological source. The Heisenberg Uncertainty Principle ensures that any attempt to precisely measure and reproduce the quantum states involved in sensing would necessarily disturb those states, providing a physical basis for spoofing detection.

5.2. Addressing Implementation Challenges

Despite its advantages, BFDC faces several implementation challenges that must be addressed for practical deployment:

Sensor Cost and Complexity: Current QZFM OPMs cost approximately $50,000 per unit, making a 16-sensor array prohibitively expensive for most applications. However, recent advances in chip-scale atomic magnetometry and mass production techniques are rapidly reducing costs. We project that within 5 years; integrated quantum sensor arrays suitable for BFDC could be manufactured for under $1,000.

Environmental Sensitivity: Quantum magnetometers are sensitive to environmental magnetic fields, requiring careful shielding or active cancellation. Our adaptive filtering algorithms successfully suppress common environmental interference, but deployment in magnetically noisy environments (near MRI machines, power transformers, etc.) remains challenging.

User Acceptance: The 45-second enrollment time and requirement to remain relatively still during measurement may limit user acceptance. Ongoing work focuses on reducing acquisition time through compressed sensing techniques and developing mobile form factors that allow measurement during normal activities.

 doi:10.20944/preprints202508.0992.v1

5.3. Security Analysis

Table 1. BFDC Novelty to Threat Mitigation Mapping.

BFDC Innovation	Threat Mitigated	Mitigation Mechanism
Whole-body EM resonance profiling	Static biometric cloning	Real-time harmonic capture across full body field
Gradient-entropy hashing	Template tampering, spoofing	Spatial variation encoding + tamper-evident hash
Phase-shift encryption	Replay attacks, biometric inversion	Phase-locked encoding tied to biometric waveform
Harmonic replay challenge-response	Deepfake, synthetic biometric spoofing	Live response validation via harmonic synthesis
High-dimensional vector modeling	Impersonation, feature overlap	Unique biometric signature per posture and state
Quantum magnetometry for sensing	Thermal spoofing, synthetic field injection	Quantum-verified EM mapping and physical validation

The security of BFDC rests on multiple interdependent layers. The high dimensionality of the feature space (30,000+ dimensions) provides information-theoretic security against brute-force attacks. With 127 bits of entropy per user, the probability of random collision is approximately 2^{-127}, far exceeding the security requirements for most cryptographic applications.

The gradient-entropy hashing scheme ensures that even small perturbations in the measured electromagnetic field produce avalanche effects in the output hash, preventing hill-climbing attacks. The incorporation of temporal dynamics through phase-shift encryption binds the cryptographic key to the specific measurement instance, preventing replay attacks even if an attacker obtains previous measurement data.

5.4. Post-Quantum Resilience

Definition 12 (Quantum Security Model). The security of BFDC against quantum adversaries is analyzed under the quantum random oracle model (QROM) [11].

Theorem 6 (Post-Quantum Security). Under the assumption that cloning a physical electromagnetic field distribution requires exponential quantum resources, BFDC achieves post-quantum security with:

1. **Grover Resistance**: Against quantum search, the effective key space provides security: $T_{Grover} = O(2^{k/2}) = O(2^{63.5})$ quantum operations
2. **Physical Unclonability**: The quantum no-cloning theorem prevents perfect replication of the quantum states involved in measurement: $||\varrho_{clone} - \varrho_{original}||_{tr} \geq 1 - \exp(-D_{eff})$

where $D_{eff} \approx 10^4$ is the effective dimensionality and $||\cdot||_{tr}$ denotes trace distance.

3. **Measurement Disturbance**: Any attempt to precisely characterize the electromagnetic field necessarily disturbs it: $\Delta B \cdot \Delta(\partial B/\partial t) \geq \hbar/(4\pi m_e)$

where m_e is the electron mass.

Lemma 4 (Hash Function Security). The SHA3-512 construction provides 256-bit quantum security [11]:

 doi:10.20944/preprints202508.0992.v1

$$Adv^{QPRE}_{SHA3\text{-}512}(A) \leq (q + 1)^2 / 2^{256}$$

where q is the number of quantum queries to the oracle.

Furthermore, the hash-based key derivation scheme uses SHA3-512, which provides 256-bit security against quantum attacks using Grover's algorithm. The error correction codes employ classical coding theory that does not rely on number-theoretic assumptions vulnerable to Shor's algorithm [9]. This positions BFDC as a truly post-quantum biometric cryptosystem.

5.5. Future Directions

Several research directions could further enhance BFDC:

1. **Multimodal Fusion**: Combining electromagnetic sensing with other quantum-enhanced modalities (e.g., quantum optical coherence tomography) could further increase entropy and robustness.
2. **Distributed Sensing**: Networks of BFDC nodes could enable secure multi-party computation protocols based on correlated biometric measurements.
3. **Health Monitoring**: The rich physiological information captured by BFDC could enable simultaneous authentication and health monitoring, adding value beyond security applications.
4. **Standardization**: Development of standards for quantum biometric systems will be crucial for interoperability and widespread adoption.

6. Conclusions

BFDC marks a paradigm shift in biometric cryptography—redefining biometric inputs not as identity proxies, but as high-dimensional entropy substrates for live key generation. By combining quantum sensing, phase-aware encoding, and harmonic replay challenges, it offers a uniquely defensible response to spoofing, cloning, and replay threats in post-quantum ecosystems.

This work lays the groundwork for standards-compliant cryptographic primitives that fuse physical embodiment, temporal dynamics, and biometric uniqueness—heralding a new frontier in secure identity systems and zero-trust architectures.

Author Contributions: R.C.S. conceived the BFDC framework, designed the experimental methodology, implemented the quantum sensing protocols, performed the security analysis, and wrote the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The datasets generated during this study are available from the corresponding author upon reasonable request, subject to privacy and security constraints inherent to biometric data.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

Abbreviation	Full Form
BFDC	Biometric Feature-Dimension Cryptography
EM	Electromagnetic
QZFM	Quantum Zero-Field Magnetometer
OPM	Optically Pumped Magnetometer
NV	Nitrogen-Vacancy
PQC	Post-Quantum Cryptography

 doi:10.20944/preprints202508.0992.v1

FIPS	Federal Information Processing Standards
NIST	National Institute of Standards and Technology
FFT	Fast Fourier Transform
FAR	False Acceptance Rate
FRR	False Rejection Rate
EER	Equal Error Rate
SERF	Spin-Exchange Relaxation-Free
DWT	Discrete Wavelet Transform
STFT	Short-Time Fourier Transform
PCA	Principal Component Analysis
BCH	Bose-Chaudhuri-Hocquenghem
SNR	Signal-to-Noise Ratio

References

1. Kaur, P.; Kumar, N.; Singh, M. Biometric Cryptosystems: A Comprehensive Survey. *Multimed. Tools Appl.* **2023**, *82*, 16635–16690. https://doi.org/10.1007/s11042-022-13817-9
2. Jain, A.K.; Ross, A.; Pankanti, S. Biometrics: A Tool for Information Security. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 125–143. https://doi.org/10.1109/TIFS.2006.873653
3. Lim, M.-H. Biometric Discretization for Template Protection and Cryptographic Key Generation. In *Biometric Security*; Cambridge Scholars Publishing: Newcastle, UK, 2015; pp. 1–26.
4. Herb, K.; Völker, L.A.; Gärtner, M.; et al. Quantum Magnetometry of Transient Signals with a Time Resolution of 1.1 Nanoseconds. *Nat. Commun.* **2025**, *16*, 822. https://doi.org/10.1038/s41467-025-00822-2
5. Lei, L.; Wu, T.; Guo, H. Sensitivity of Quantum Magnetic Sensing. *Natl. Sci. Rev.* **2025**, *12*, nwaf129. https://doi.org/10.1093/nsr/nwaf129
6. Razzoli, L.; Ghirardi, L.; Rizzi, M.; Cirac, J.I. Lattice Quantum Magnetometry. *Phys. Rev. A* **2019**, *99*, 062330. https://doi.org/10.1103/PhysRevA.99.062330
7. Tinani, S.; Wagner, U. Post-Quantum Cryptography: A Comprehensive Guide; cnlab security AG: Rapperswil, Switzerland, 2025. Available online: https://www.cnlab.ch/fileadmin/documents/Publikationen/2025/Post-Quantum_Cryptography_-__A_Comprehensive_Guide.pdf (accessed on 4 August 2025).
8. NIST. Transition to Post-Quantum Cryptography Standards. *NIST Interagency/Internal Report (IR) 8547-IPD*, 2024. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf (accessed on 4 August 2025).
9. NIST. Post-Quantum Cryptography Standardization Project. 2025. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography (accessed on 4 August 2025).
10. Dodis, Y.; Ostrovsky, R.; Reyzin, L.; Smith, A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.* **2008**, *38*, 97–139. https://doi.org/10.1137/060651380
11. Boneh, D.; Dagdelen, Ö.; Fischlin, M.; Lehmann, A.; Schaffner, C.; Zhandry, M. Random Oracles in a Quantum World. In *Advances in Cryptology – ASIACRYPT 2011*; Lee, D.H., Wang, X., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 41–69.
12. Krawczyk, H.; Eronen, P. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). *RFC 5869*, 2010. https://doi.org/10.17487/RFC5869

 doi:10.20944/preprints202508.0992.v1

13. Wolf, M.M.; Eisert, J.; Guehne, O. Entanglement Properties of Physical Systems: A Review. *Quantum Inf. Process.* **2009**, *8*, 87–120. https://doi.org/10.1007/s11128-009-0099-8
14. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*, 2nd ed.; Wiley-Interscience: Hoboken, NJ, USA, 2006.
15. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*, 10th Anniversary ed.; Cambridge University Press: Cambridge, UK, 2010.