A Systematization of Knowledge on Biomarker Based Encryption Keys

Matthew Gaber[1], Mohiuddin Ahmed[2] and Al-Sakib Khan Pathan[3]
[1]Sirindhorn International Institute of Technology, Thammasat University, Pathum Thani, Thailand
[2]School of Computer Science and Information Technology, Adelaide University, Australia
[3]Department of Computer Science and Engineering, United International University, Bangladesh

m.gaber@siit.tu.ac.th
m.ahmed.au@ieee.org
spathan@ieee.org

Abstract: Encryption keys require careful management, they must be securely stored, and if stolen or compromised, the consequences can be catastrophic. Ephemeral keys are created, used and then deleted, reducing the attack surface. As the tactics, techniques and procedures of threat actors continue to evolve, implementing an ephemeral encryption key would enhance the protection of critical infrastructure systems, sensitive data and communication systems. This research investigates the feasibility of generating a repeatable, unique, yet transient encryption key from human biomarkers. By deriving cryptographic keys directly from bioelectrical and biochemical markers, key management overhead and long-term exposure risks can be minimized. This Systematization of Knowledge (SoK) addresses two primary challenges. Firstly, determining the viability and limitations of deriving consistent keys from inherently variable biomarkers. Secondly, we propose a manifold encryption key derivation scheme using context dependent signals drawn from the network, device and environment to overcome the limitations of biometric based key generation, including irrevocability, noise, and entropy deficiency.

Keywords: Biomarker, Cryptography, Data security, Encryption keys

1. Introduction

Cryptography, commonly referred to as encryption, constitutes the systematic process of transforming information into a secure form such that its content remains unintelligible to unauthorized parties. With the continual escalation of cybercrime, the development of increasingly robust encryption methods is imperative to mitigate potential security breaches (Diffie et al, 1976; Rivest et al, 1978; Lutsenko et al, 2021). According to IBM, the global average cost of a data breach as of 2025 is USD 4.44 million, as shown in Figure 1 (Kessem, 2025).

Given the pervasive integration of digital technologies, encryption underpins a wide array of everyday activity, including financial transactions, authentication protocols, electronic commerce, numerous communication apps, and social networking platforms (Ozer et al, 2024; Marappan et al, 2025; Qiu et al, 2020; Talwar et al, 2022). The protection of such data is typically achieved through the application of cryptographic algorithms designed to ensure confidentiality and integrity.

Traditional authentication schemes rely on tokens or secret knowledge to establish identity but cannot distinguish a legitimate user from an adversary who has obtained those credentials (Uludag et al., 2004; Sheng et al., 2012). Biometric authentication addresses this by leveraging unique physiological and behavioural characteristics, including fingerprints, face, iris, or voice, that are inherently tied to the individual rather than to a possession or secret (Pahuja et al., 2024; Alrawili et al., 2024). In practice, systems operate in two phases: enrolment, where biometric data is captured and stored as a reference template, and verification, where subsequent inputs are matched against that template within a defined threshold. Systems may be unimodal or multimodal, the latter combining multiple traits to improve accuracy and robustness (Pahuja et al., 2024; Sheng et al., 2012). Despite these advantages, biometric systems remain vulnerable to template theft, presentation and replay attacks, side-channel exploits, and insider misuse, while system accuracy is further sensitive to factors such as age, illness, injury, illumination, and noise (Alrawili et al., 2024).

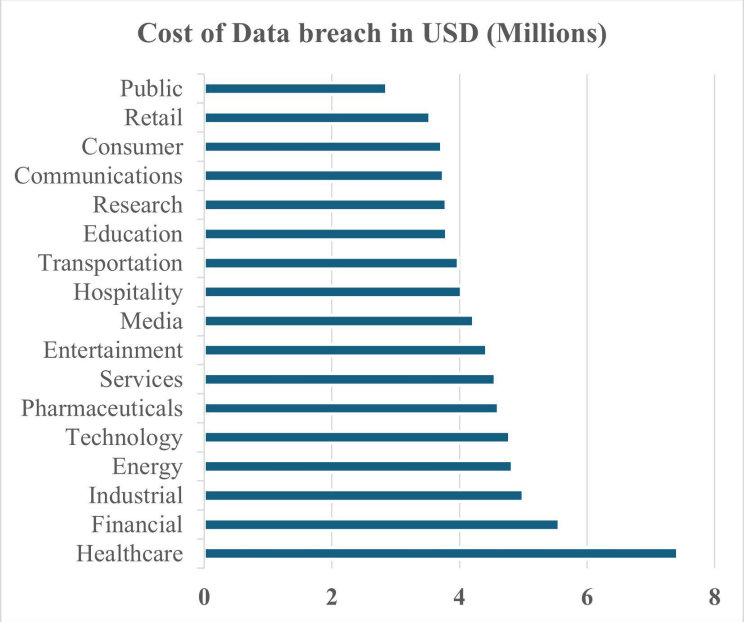

Figure 1: Cost of data breaches as of 2025 by IBM (Kessem et al)

Biometric authentication, as described above, ultimately reduces to a binary decision: a score is computed, compared against a threshold, and access is granted or denied. While effective for identity verification, this model does not generate cryptographic material, the biometric serves as a gate, not a key. The shift from authentication to cryptographic key generation is non-trivial. Where authentication tolerates variability through a soft threshold, key generation demands exact or near-exact reproducibility of a fixed bitstring across presentations. An active area of research pursues a more fundamental integration, where biometric traits are used to generate or protect encryption keys that underpin critical security services including confidential communication, ensuring the integrity of data, and enabling non-repudiation through digital signatures (Lutsenko et al, 2021; Cowley et al, 2025; Gorski and Wodo, 2024). The potential of this integration lies in producing cryptographic material that is user specific and challenging to replicate. Biometric key generation offers a major advantage, it removes the need to store or remember external keys or passwords as the key can be reconstructed as required (Lutsenko et al, 2021; Sheng et al, 2012). However, current frameworks often lack formal security proofs, rigorous entropy analysis, and practical mechanisms for error tolerance or revocability, leaving their robustness uncertain (Sheng et al, 2012; Uludag et al, 2004). These limitations motivate the need for a systematic study of biometric key generation approaches and the exploration of new frameworks that integrate biometrics with complementary signals for stronger, more adaptable cryptographic systems.

1.1 Key Contributions

Our main contributions are summarized as follows:

- We develop a comprehensive Systematization of Knowledge (SoK) on biometric based encryption key generation.
- We provide a structured critique of prior approaches, highlighting open challenges in entropy estimation, error tolerance, revocability, and compliance with Kerckhoffs's principle.
- We propose a novel manifold key generation framework that binds biometric traits with complementary context dependent signals from network, environmental, and device hardware markers to enhance resilience against attacks.

To the best of our knowledge, the use of environmental, hardware, and network markers in conjunction with biometric features for encryption key generation has not been previously examined, positioning this work as a foundation for future experimental validation and benchmarking.

2. Fundamentals and Background

Biometric cryptosystems are typically categorised into three main categories: Key Release, Key Binding, and Key Generation as shown in Figure 2.

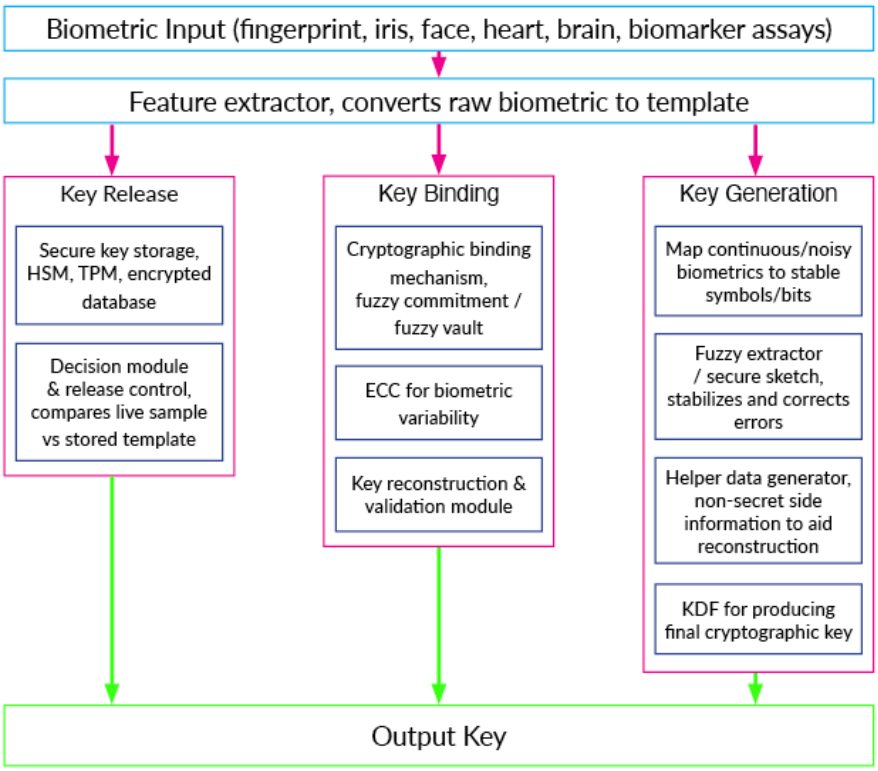

Figure 2: Biometric Encryption Key Systems

In Key Release systems, a conventional cryptographic key is stored securely, in a Hardware Security Module (HSM) or Trusted Platform Module (TPM) and only released after a successful biometric authentication (Lutsenko et al, 2021). Key Bindings systems mathematically bind a cryptographic key with biometric data using various error tolerant algorithms, where the key cannot be retrieved without the biometric data. This approach depends heavily on Error Correction Codes (ECC) for biometric variability (Lutsenko et al, 2021). In Key Generation systems, the key is directly generated from biometric features using a Key Derivation Function (KDF), that variously use fuzzy extractors and helper data (Lutsenko et al, 2021). Key generation systems regenerate cryptographic keys directly from biometric data, eliminating the need to store keys, but at the cost of easy revocation or rotation. To avoid ambiguity, we clarify the terminology used throughout this work.

2.1 Helper Data

A string, data, or a system that is extra information produced at enrolment to enable reliable reconstruction of a secret from a noisy source such as biometrics (Gebali et al, 2022). However, many works deviate, treating helper data as confidential or hardware-protected, or omitting it entirely in favour of direct mappings, trusted hardware, or a user secret such as a PIN. In this paper, we use *helper data* to mean any auxiliary string intended to aid reproducibility.

2.2 Secure Sketch

A primitive with two algorithms: Sketch(w) → s and Rec(w′, s) → w, where w is the enrolment biometric, w′ is the verification sample, and s is the helper data, with w and w′ within a threshold under a chosen distance metric. Correctness: if w′ is within that threshold of w, Rec recovers w with high probability. Security: s reveals only bounded information about w and typically preserves most of w's minimum entropy (Dodis et al, 2008). A secure sketch enables reproducibility from noisy inputs but does not itself ensure that the final key is uniformly random.

2.3 Information Reconciliation

This follows the classical noisy-channel key agreement paradigm, where information reconciliation uses ECC to resolve correlated but noisy values into an identical string, with the side-channel communication serving as helper data (Gorski and Wodo, 2024).

2.4 Fuzzy Extractor

A fuzzy extractor is a pair of algorithms Generate and Reproduce that derive a stable cryptographic key from a noisy biometric measurement. A fuzzy extractor can be viewed as a *secure sketch* for reproducibility plus privacy amplification for uniformity (Dodis et al, 2008). Generation: *(R, P)* ← Gen*(w),* where *R* is the secret key and *P* is public helper data that may be stored or transmitted. Reconstruction: Given any fresh sample *w′* that is sufficiently *close* to *w* under a chosen metric, the algorithm Rep reproduces the same key: Rep(*w′, P*) = R. Correctness: If *w′* is within the tolerated noise radius of *w*, reconstruction succeeds with high probability. Security: For any source *W* with sufficient minimum entropy, the key *R* is *nearly* indistinguishable from a uniform ℓ bit string and independent of *P*.

2.5 Security Analysis

In a biometric key generation system, security can be assessed across four principal layers: the Sensor Layer, the Preprocessing Layer, the Feature Extraction Layer, and the Key Derivation Layer, each introducing unique attack vectors and corresponding defences, as shown in Figure 3.

At the sensor layer, where raw biometric signals are captured, attacks include presentation spoofing, replay injection, and environmental manipulation. Defences include Presentation Attack Detection (PAD), multi-spectral or 3D sensing, cryptographically authenticated sensor links to prevent MITM attacks, and hardware attestation to protect sensor firmware.

The preprocessing layer, which cleans and normalizes raw data, may be targeted through adversarial perturbations, calibration tampering, or parameter rollback. Defences include robust normalization, cryptographic integrity protection of configuration parameters, and execution within a Trusted Execution Environment (TEE).

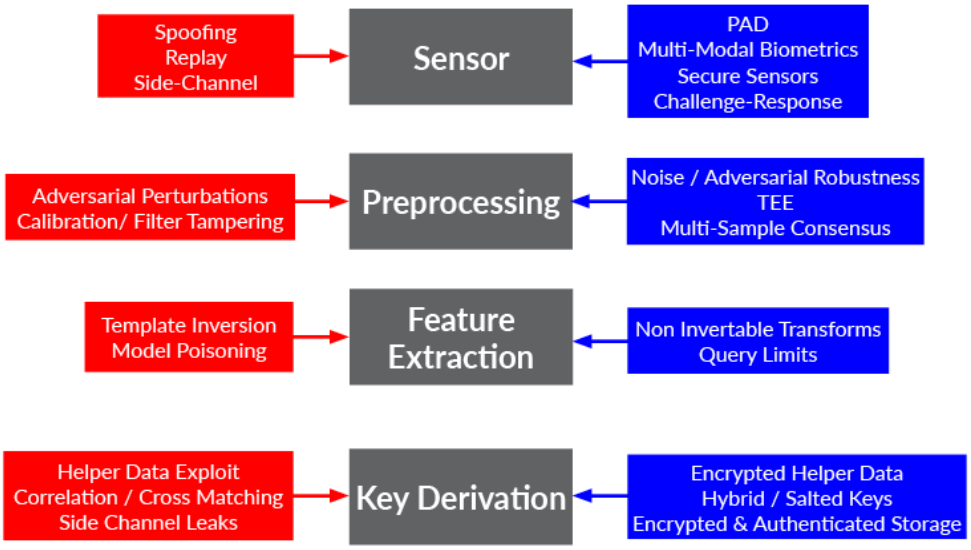

Figure 3: Biometric Key Generation showing potential attack vectors and defences at each stage

At the feature extraction layer, threats include template inversion and hill-climbing attacks exploiting repeated queries. Defences focus on non-invertible feature transforms, restricted query access, and hardening models against poisoning.

The key derivation layer converts noisy biometric features into reproducible cryptographic keys via feature quantization, error correction using secure sketches or fuzzy extractors, and a KDF to produce the final key.

3. Analysing the State-of-the-Art

This section surveys recent biometric key derivation schemes, with Table 1 providing a structured comparison. The analysis follows the framework established in Section 2 and evaluates each work along two axes. First, which of the four key-generation building blocks, namely helper data, secure sketches, information reconciliation, and fuzzy extractors, are instantiated, how explicitly, and whether their security properties are formally or empirically justified. Second, security coverage across the sensor, pre-processing, feature

extraction, and key derivation layers, with attention to presentation attacks, replay, template inversion, and offline guessing.

A key evaluative criterion throughout is Kerckhoffs's Principle, that system security must rest solely on the secrecy of the key, not on obscured parameters, undisclosed feature selection, or protected helper data (Petitcolas, 2025). Section 3.5 synthesises the resulting research gaps.

Table 1: Summary and comparison of biometric key derivation methods

Note. Filled circles indicate level: ○ None, ◔ Low, ◑ Moderate, ● High

Paper	Data Source	Key Size (bits)	Estimated Entropy	Error Tolerance	Revocable	Kerckhoffs	Replay Spoof Res.	Helper Data	Secure Sketch	Info. Recon.	Fuzzy Ext.
Cowley et al, (2025)	Immunoassay	128	~27 bits	○	✗	✗	✗	✗	✗	✗	✗
Gorski &Wodo (2024)	Finger, Eye	256	≪128 bits	◔	✗	✗	✗	✓	✓	✓	✓
Kocak et al, (2025)	ECG	256	~1 bit/bit	◑	✗	✗	✗	✗	✗	✗	✗
Sulavko et al, (2025)	Voice	1024	~1 bit/bit	◑	✗	✗	✗	✗	✓	✓	✓
Oktay et al, (2024)	ECG	256	~1 bit/bit	◔	✗	✗	✗	✗	✗	✗	✗
Kuznetsov et al, (2024)	Face	37	≪37 bits	◑	✗	~	✗	✓	✓	✓	✓
Szymoniak et al, (2025)	Face	256	30-40 bits	○	✗	✗	✗	~	✗	✗	✗
Hoque et al, (2008)	Handwriting	~93	~40 bits	◑	~	✓	~	~	✗	✗	✗
Mohd et al, (2025)	Fingerprint	NA	NA	◑	✓	✓	~	✓	✗	✗	✗
Ballard et al, (2008)	Handwriting	256	~2^30	◔	✓	✓	✗	✗	~	~	✗
Rathgeb & Uhl (2011)	Iris	280	~200	●	~	✓	✗	✓	~	✗	~

3.1 Reproducibility Versus Leakage in Helper Data and Kerckhoffs Compliance

A persistent tension across the literature is that reliable key reconstruction from noisy biometrics requires auxiliary information, yet auxiliary information risks leakage and is often handled in ways that undermine Kerckhoffs compliance. Cowley et al. (2025) sidestep the problem entirely by mapping immunoassay absorbance values directly into an AES-compatible string with no secure sketch, reconciliation, or fuzzy extraction. This avoids helper-data leakage but shifts the burden onto experimental repeatability and parameter secrecy, making key reproduction fragile and Kerckhoffs compliance weak. Ballard et al. (2008) take a different approach, explicitly addressing the problem that biometrics alone can be too predictable or too noisy for key generation. Their Randomized Biometric Templates (RBTs), evaluated on handwriting, add entropy by introducing uncertainty in the measurement process rather than relying solely on biometric randomness. A key design objective is that decrypting a stored template under an incorrect password still yields a plausible output, preventing offline password-checking and obscuring which features are in use. This is a more cryptographically deliberate handling of auxiliary information than in many applied schemes. However, no information-theoretic leakage bound is provided, the construction sits outside the fuzzy extractor paradigm rather than instantiating it, and a non-trivial minority of users remain susceptible to rapid key recovery by search.

Rathgeb and Uhl (2011) follow the classical public helper-data model, storing a bit mask of stable iris code positions alongside cyclic error-correcting redundancy, which allows a fresh noisy sample to be decoded back to the original representation, to enable repeatable reconstruction. The design moves closer to a reproducible-key pipeline, but residual entropy is not tightly bounded, and the security analysis rests on iris code bit independence assumptions known to be imperfect. Kuznetsov et al. (2024) similarly publish a helper string in a code based pipeline without fully accounting for what it reveals about residual entropy under realistic feature distributions. Across these works, helper data is either omitted, which weakens reproducibility, or introduced without complete leakage accounting, sometimes with implicit secrecy assumptions filling the gap. This

pattern highlights the need to consider whether helper data is public, what it leaks, and how it can be revoked as fundamental design requirements rather than implementation details.

3.2 Error Tolerance and Effective Entropy Under Noise Correction

The relationship between noise tolerance and effective key strength presents its own complications. Many papers report AES-length outputs, but key length is not a security guarantee when the mapping from biometrics to bits is biased, redundant, or requires substantial correction. In schemes that attempt deterministic reconstruction, error correction and redundancy unavoidably trade off against entropy. That is, selecting stable bits, partitioning continuous features into tolerance bands, and publishing ECC redundancy can all reduce the attacker's search space, especially if bit distributions are non-uniform or correlated.

Rathgeb and Uhl (2011) make this trade off explicit by using ECC to correct bit flips in selected iris-code positions. Kuznetsov et al. (2024) likewise analyse FRR/FAR trade-offs under code parameters in a code-based fuzzy extractor setting. These schemes are stronger than direct mappings because they use a correction mechanism, but their security interpretation still hinges on how much uncertainty remains after feature selection and redundancy publication. In contrast, Cowley et al. (2025) highlight a different failure mode, an AES compatible string can be produced without explicit correction, yet small measurement deviations can render reconstruction infeasible, and the usable uncertainty can be far below the nominal key size. Szymoniak et al. (2025) illustrate a related risk of overstating key strength. Their IoT oriented scheme derives a nominal 256-bit key from a facial triangle using the eye corners and chin. However, the effective uncertainty is constrained by the low-dimensional geometry of the underlying biometric signal and by acquisition conditions including pose, lighting, expression, that alter coordinates without any ECC or secure-sketch mechanism to stabilise them. Consequently, the reported key length primarily reflects output formatting rather than a quantified entropy guarantee.

A related strategy appears in several Machine Learning (ML) based bio-key papers where rather than enforcing deterministic reconstruction, they relax the success condition to similarity under a threshold. This improves apparent robustness with lower rejection but transforms the problem into verification rather than cryptographic key generation, as the output is not guaranteed to be identical across sessions. The literature repeatedly confronts the same issue where the robust handling of noise is essential, but it must be evaluated together with the entropy cost of tolerance mechanisms and the gap between output length and effective security.

3.3 Distinguishing Biometric Verification from Cryptographic key Generation

A substantial portion of recent work, particularly ML systems, implicitly adopts a verification paradigm even when describing outputs as keys. In these designs, bitstrings produced from different sessions are not required to match exactly; instead, authentication is decided by Hamming distance or related similarity scores, against an optimised threshold. This is legitimate and often effective for authentication, but it does not directly produce encryption ready keys because encryption requires absolute key agreement.

Kocak et al. (2025) use this pattern using ECG heart prints. Their Siamese neural network produces 256-bit outputs designed to be consistent within user and different across users, and ECG is argued to be intrinsically harder to spoof than external traits. However, the system is evaluated as a matcher. Keys are close rather than identical, and no reconciliation or extraction layer is provided to convert noisy outputs into stable shared secrets. Oktay et al. (2024) similarly generate ECG-derived 256-bit outputs for digital watermarking and validate them with a reliability metric rather than requiring exact reproduction. This is compatible with watermark verification tolerance but underscores the mismatch with cryptographic key agreement. Hoque et al. (2008) also faces this limitation. Signature subspace partitioning concatenates the components into a bitstring and does show some resistance to forgery, but the absence of error correction leads to high false rejection and divergence between sessions, limiting its application as a cryptographic key generator.

Mohd et al. (2025) illustrates a different problem, while the work is strong as cancellable template protection, emphasising revocability, non-invertibility, and unlinkability, but the output remains an authentication decision rather than a reproducible secret key, and helper-data leakage is not characterised in the formal secure-sketch sense. In contrast, Sulavko et al. (2025) are closer to an explicit key-generation framing, the authors present a neural fuzzy extractor for voice and report long outputs of 1024 bits, with robust matching performance. However, the deliberate avoidance of stored helper data, motivated by inversion concerns, substitutes one risk for another. The burden of reproducibility shifts to learned stability and system assumptions rather than a standard public helper data with bounded leakage model.

Across these works, the field repeatedly uses the language of key generation while evaluating systems as matchers. However, there is a categorical distinction, verification systems can be valuable, but without an explicit reconciliation or extraction stage they do not satisfy the functional requirements for a cryptographic key.

3.4 Primitive Security Versus end-to-end Security in Biometric key Generation

Even when a design includes strong cryptographic primitives at the key derivation layer, system level assumptions often determine real security. Gorski and Wodo (2024) make this point in their security evaluation of biometric AKE protocols (BAKE/BRAKE). While BRAKE incorporates substantial cryptographic structure including template obfuscation, OPRF-based protections, and a KDF for session keys, the authors identify residual vulnerabilities rooted in key compromise and enforceability. Compromise of evaluator side secrets can enable offline attacks, and assumptions that sensitive values remain only in volatile memory cannot be guaranteed against a rogue client who persists credentials and bypasses biometric presentation. The results emphasise that protocol soundness must be evaluated together with key management, client behaviour, and adversary capabilities.

More broadly, across the surveyed literature the sensor layer is frequently excluded or treated as future work. Voice systems remain exposed to replay and synthesis without liveness or PAD. Face systems evaluated on static datasets lack threat modelling during capture. Iris systems often acknowledge presentation attacks but defer defences and ECG systems sometimes claim inherent spoof resistance without implementing or evaluating formal PAD. Preprocessing layers are typically treated as engineering steps rather than attack surfaces, despite their potential vulnerability to manipulation. Consequently, many schemes concentrate their security reasoning in feature extraction and key derivation while leaving the most deployment relevant attack classes including presentation, replay, and adversarial capture, outside the evaluated system boundary.

3.5 Critical Analysis

Across the surveyed approaches, a common pipeline emerges. Starting from a biometric, a noisy numeric feature vector is extracted. Then an ECC, that ensures small intra-subject variations do not break reproducibility, is applied. Lastly, the corrected vector is hashed to obtain a fixed-length cryptographic key. However, these works generally fall short of Kerckhoffs's principle and do not rigorously evaluate resilience to replay or spoofing attacks. A more formal approach replaces direct mapping b → K with a secure sketch S(b) → s. Given a fresh sample b' close to b, the pair (b', s) reliably reconstructs the same keying material. The helper string s can be stored or made public while leaking only bounded information about b. A fuzzy extractor strengthens this by coupling sketch reconciliation with randomness extraction, ensuring K is both reproducible across noisy measurements and statistically close to uniform (Kuznetsov et al., 2024). Using biometrics as the sole key source faces deeper structural problems. Many biometrics, including biochemical assays, yield only a few dozen bits of entropy, leaving derived keys vulnerable to offline search, population-level inference, and quantum attacks. Biometrics are also not secret, a latent fingerprint, a blood sample, or an intercepted wearable stream exposes the same underlying features. Finally, compromise is permanent: any key deterministically derived from a biometric remains reproducible forever, regardless of how well spoofing is mitigated.

4. Manifold Encryption Key Derivation

The idea of deriving cryptographic keys directly from biometric markers such as bioassays, ECG, fingerprints, and iris prints, is appealing but currently fraught with challenges presented in Section 3. In practice, most systems use biometrics merely as a gate to securely generated keys rather than as the keys themselves.

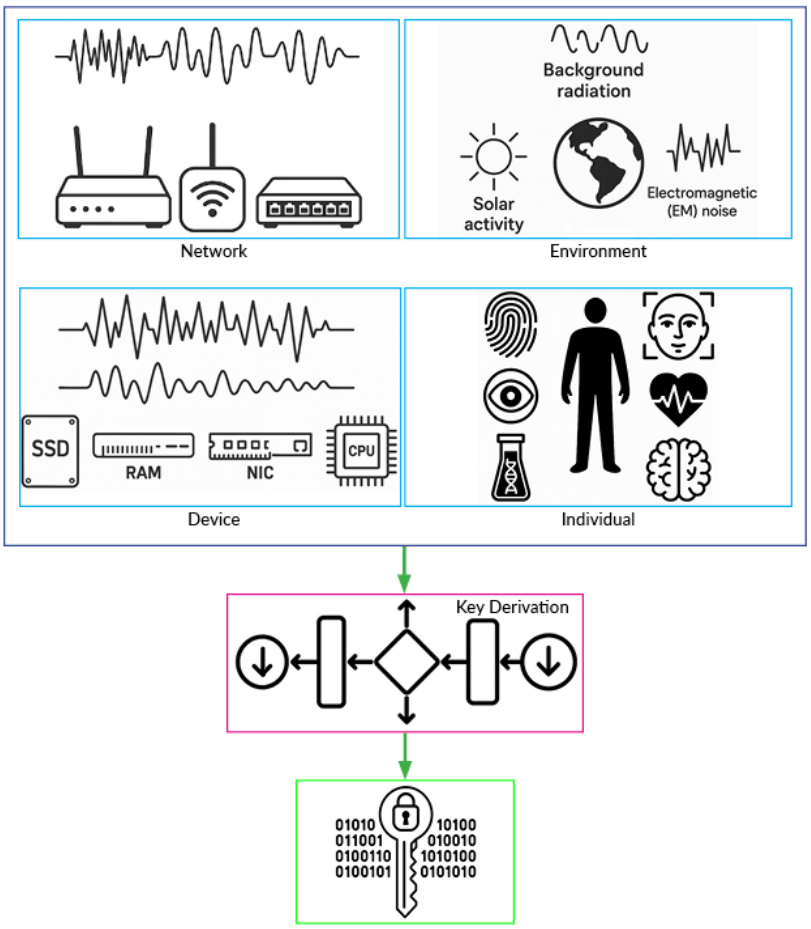

Figure 4: Manifold Encryption Key Derivation

A practical path beyond single modality biometric key generation is to bind biometric traits to signals drawn from the network, environment, and device hardware. For instance, network markers may be derived from topology or hardware identifiers. Environmental markers may include background RF, ambient audio and lighting, temperature, and location. Hardware markers such as CPU, RAM, or SSD fingerprints could be incorporated through challenge-response protocols to further strengthen the binding between identity, device, and context. This proposed manifold encryption key derivation framework is conceptual, but not without precedent. Location has been investigated in continuous authentication architectures for location-based services (Alamleh et al, 2020). Further, beacon frame based two-factor authentication demonstrates how environmental RF signals can serve as an unobtrusive second factor with minimal user involvement (AlQahtani et al, 2020). Additionally, DeMiCPU introduced a robust challenge–response hardware fingerprinting method that leverages magnetic induction signals emitted from CPU modules to capture unique device level discrepancies (Ji et al, 2021).

Encryption keys require careful management, they must be securely stored and if stolen or compromised, the effects can be catastrophic. Ephemeral keys are created, used and then deleted, reducing the attack surface. As the tactics, techniques and procedures of threat actors continue to evolve, implementing ephemeral encryption keys could enhance the protection of mission critical systems, sensitive intelligence and military communication systems.

This multi-domain fusion mitigates the classic weaknesses of unimodal biometrics by binding key derivation to multiple independent contexts. Network and environmental binding limits out-of-context misuse of compromised biometric templates, while hardware anchoring ties key derivation to trusted devices, raising the bar against insider abuse and template attacks. The result is a context-aware, revocable, and device-, location-, and individual-bound key generation scheme, in which compromise of any single domain is insufficient to reconstruct the cryptographic key.

5. Conclusions and Future Research Direction

Security and privacy challenges limit large scale adoption of biometric key generation. Compared with conventional key management, biometric derivation reduces the attack surface associated with stored keys as material is generated on demand rather than persisted, and ties possession to the individual rather than a token or password. However, several fundamental limitations constrain the approach. Measurement noise and intra-subject variability undermine the bit-for-bit reproducibility that cryptographic keys require, and error correction techniques introduced to compensate, reduce effective entropy while the resulting helper data introduces new leakage vectors. Further, many biometric signals carry insufficient entropy to begin with, weakening collision resistance and enabling offline search. Irrevocability compounds this, unlike passwords, biometric traits cannot be rotated, so a deterministically derived key remains reproducible by any adversary who captures the underlying signal. Finally, without robust liveness detection, recorded or synthetic samples enable replay and presentation attacks. These limitations are frequently understated in the literature. Proposed schemes often demonstrate promising entropy or brute-force resistance in controlled settings but lack evaluation under realistic threat models, and the absence of standardised benchmarks makes it difficult to assess robustness and scalability. Without formal proofs and rigorous cryptographic engineering, biometric key generation risks being operationally fragile and in the worst case, a liability rather than an improvement over the approaches it seeks to replace. A practical path beyond biometric key generation is to bind biometrics with complementary, context dependent signals drawn from the network, environment, or device hardware to generate ephemeral encryption keys which dramatically reduces the vulnerabilities of biometrics alone.

Ethics Declaration: No ethics clearance required.

AI Declaration: No AI tools were used in the creation of this paper.

References

Alamleh, H. and AlQahtani, A. (2020) 'Architecture for continuous authentication in location-based services', *2020 3ICT*, https://doi.org/10.1109/3ICT51146.2020.9311972

AlQahtani, A.A.S., Alamleh, H. and Gourd, J. (2020) 'BF2FA: Beacon frame two-factor authentication', *IEEE Comnetsat*, pp. 357–361. https://doi.org/10.1109/Comnetsat50391.2020.9328965

Alrawili, R., AlQahtani, A.A.S. and Khan, M.K. (2024) 'Comprehensive survey: Biometric user authentication application, evaluation, and discussion', *Computers and Electrical Engineering*, 119, 109485. https://doi.org/10.1016/j.compeleceng.2024.109485

Ballard, L., Kamara, S., Monrose, F., and Reiter, M. (2008). 'Towards practical biometric key generation with randomized biometric templates'. *In Proceedings of the 15th ACM conference on Computer and communications security (CCS '08). Association for Computing Machinery*. https://doi.org/10.1145/1455770.1455801

Cowley, A., Newland, A., Halámková, L., Manson, R., Morales, J. and Halámek, J. (2025) 'Utilizing encryption keys derived from immunoaffinity interactions as a basis for potential security enhancements', *ACS Omega*, 10, pp. 6119–6123. https://doi.org/10.1021/acsomega.4c10568

Diffie, W. and Hellman, M. (1976) 'New directions in cryptography', *IEEE Trans Information Theory*, 22(6), pp. 644–654. https://doi.org/10.1109/TIT.1976.1055638

Dodis, Y., Ostrovsky, R., Reyzin, L. and Smith, A. (2008) 'Fuzzy extractors: How to generate strong keys from biometrics and other noisy data', *SIAM Journal on Computing*, 38(1), pp. 97–139. https://doi.org/10.1137/060651380

Gebali, F. and Mamun, M. (2022) 'Review of physically unclonable functions (PUFs): Structures, models, and algorithms', *Frontiers in Sensors*, 2, 751748. https://doi.org/10.3389/fsens.2021.751748

Gorski, M. and Wodo, W. (2024) 'Analysis of biometric-based cryptographic key exchange protocols-BAKE and BRAKE', *Cryptography*, 8(2), 14. https://doi.org/10.3390/cryptography8020014

Hoque, S., Fairhurst, M. and Howells, G. (2008) 'Evaluating biometric encryption key generation using handwritten signatures', *BLISS'08*, pp. 17–22, https://doi.org/10.1109/BLISS.2008.8

Ji, X., Cheng, Y., Zhang, J., Chi, Y., Xu, W. and Chen, Y.-C. (2021) 'Device fingerprinting with magnetic induction signals radiated by CPU modules', *ACM Trans Sensor Networks*, 18(2), https://doi.org/10.1145/3495158

Kessem, L. (2025) *2025 cost of a data breach report: Navigating the AI rush without sidelining security*. IBM. Available at: https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai

Kocak, O., Islam, S., Gumus, O. and Yilmaz, G.N. (2025) 'Using bio-cryptographic key extracted from heartprint signal by a deep neural network for authentication', *7th ICHORA*, pp. 1–6, https://doi.org/10.1109/ICHORA65333.2025.11017184

Kuznetsov, O., Zakharov, D. and Frontoni, E. (2024) 'Deep learning-based biometric cryptographic key generation with post-quantum security', *Multimedia Tools and Applications*, 83(19), pp. 56909–56938. https://doi.org/10.1007/s11042-023-17714-7

Lutsenko, M., Kuznetsov, A., Kiian, A., Smirnov, O. and Kuznetsova, T. (2021) 'Biometric cryptosystems: Overview, state-of-the-art and perspective directions', in Ilchenko, M., Uryvsky, L. and Globa, L. (eds.) *Advances in Information and Communication Technology and Systems*. pp. 66–84. https://doi.org/10.1007/978-3-030-58359-0_5

Marappan, K., Narani, S.R., R.C., I., M., A., S., M. and J., S. (2025) 'Blockchain-based financial systems using JPMorgan Liink network for secure transactions efficiently', *11th International Conference on Communication and Signal Processing (ICCSP)*, pp. 1749–1754, https://doi.org/10.1109/ICCSP64183.2025.11088723

Mohd, I., Umar, M.S. and Ahmad, F. (2025) 'A non-invertible secure template generation using AES-encrypted MCC and random triangle projection', *IEEE Access*, 13, pp. 78194–78213. https://doi.org/10.1109/ACCESS.2025.3562758

Oktay, U. and Islam, S. (2024) 'Biometrics-based image watermarking by heartprint signal', *ASYU*, pp. 1–6, https://doi.org/10.1109/ASYU62119.2024.10757151

Ozer, E. and Aydos, H. (2024) 'Utilizing hybrid encryption methods to ensure the security of financial transactions', *8th International Artificial Intelligence and Data Processing Symposium (IDAP),* https://doi.org/10.1109/IDAP64064.2024.10710781

Pahuja, S. and Goel, N. (2024) 'Multimodal biometric authentication: A review', *AI Communications*, 37(4), pp. 525–547. https://doi.org/10.3233/AIC-220247

Petitcolas, F.A.P. (2011) 'Kerckhoffs' Principle'. In: van Tilborg, H.C.A., Jajodia, S. (eds) *Encyclopedia of Cryptography and Security*. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-5_487

Qiu, H., Qiu, M., Liu, M. and Ming, Z. (2020) 'Lightweight selective encryption for social data protection based on EBCOT coding', *IEEE Trans Computational Social Systems*, 7(1), pp. 205–214, https://doi.org/10.1109/TCSS.2019.2952553

Rathgeb, C., & Uhl, A. (2011). 'Context-based biometric key generation for iris'. *IET Computer Vision*, 5(6), 389-397. https://doi.org/10.1049/iet-cvi.2010.0176

Rivest, R.L., Shamir, A. and Adleman, L. (1978) 'A method for obtaining digital signatures and public-key cryptosystems', *Communications of the ACM*, 21(2), pp. 120–126. https://doi.org/10.1145/359340.359342

Sheng, W., Howells, G., Fairhurst, M., Deravi, F. and Chen, S. (2012) 'Reliable and secure encryption key generation from fingerprints', *Information Management & Computer Security*, 20(3), pp. 207–221. https://doi.org/10.1108/09685221211247307

Sulavko, A., Panfilova, I., Inivatov, D., Lozhnikov, P., Vulfin, A. and Samotuga, A. (2025) 'Biometric-based key generation and user authentication using voice password images and neural fuzzy extractor', *Applied System Innovation*, 8(1), 13. https://doi.org/10.3390/asi8010013

Szymoniak, S. and Kubanek, M. (2025) 'Biometry-based verification system with symmetric key generation method for Internet of Things environments', *Scientific Reports*, 15, 5464. https://doi.org/10.1038/s41598-025-89226-3

Talwar, A., Chaudhary, A. and Kumar, A. (2022) 'Encryption policies of social media apps and its effect on users' privacy', 1*0th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),* https://doi.org/10.1109/ICRITO56286.2022.9964730

Uludag, U., Pankanti, S., Prabhakar, S. and Jain, A.K. (2004) 'Biometric cryptosystems: Issues and challenges', *Proc. IEEE*, 92(6), pp. 948–960. https://doi.org/10.1109/JPROC.2004.827372