ISO/IEC-Compliant Match-on-Card Face Verification with Short Binary Templates

Abdelilah Ganmati[a,*], Karim Afdel[a], Lahcen Koutti[a]

[a] *Computer Systems & Vision Laboratory, Faculty of Sciences, Ibn Zohr University, BP 8106, Agadir 80000, Morocco*

Abstract

We present a practical match-on-card design for face verification in which compact 64/128-bit templates are produced off-card by PCA–ITQ and compared on-card via constant-time Hamming distance. We specify ISO/IEC 7816-4/14443-4 command APDUs with fixed-length payloads and decision-only status words (no score leakage), together with a minimal per-identity EEPROM map. Using real codes from a CelebA working set (55 identities, 412 images), we (i) derive operating thresholds from ROC/DET, (ii) replay enrol→verify transactions at those thresholds, and (iii) bound end-to-end time by pure link latency plus a small constant on-card budget. Even at the slowest contact rate (9.6 kbps), total verification time is 43.9 ms (64 b) and 52.3 ms (128 b); at 38.4 kbps both are < 14 ms. At FAR= 1%, both code lengths reach TPR= 0.836, while 128 b lowers EER relative to 64 b. An optional +6 B helper (symbol-level parity over empirically unstable bits) is latency-negligible. Overall, short binary templates, fixed-payload decision-only APDUs, and constant-time matching satisfy ISO/IEC transport constraints with wide timing margin and align with ISO/IEC 24745 privacy goals. Limitations: single-dataset evaluation and design-level (pre-hardware) timing; we outline AgeDB/CFP-FP and on-card microbenchmarks as next steps.

Keywords: Face verification, Binary templates, PCA–ITQ, Match-on-card, ISO/IEC 7816, ISO/IEC 14443, Hamming distance, APDU, Smart card

1. Introduction

Short, fixed-length binary face templates enable constant-time Hamming matching and tiny on-card storage—an excellent fit for contact and contactless smart cards. Classical hashing methods such as Spectral Hashing (SH) and Iterative Quantization (ITQ) compress high-dimensional embeddings into compact codes while preserving neighborhood structure; in practice, a PCA front-end plus ITQ rotation gives strong binarization quality at very low bit budgets [1, 2]. With modern identity-supervised backbones (e.g., MobileFaceNets) providing highly discriminative float features, 64–128 bit PCA–ITQ templates commonly support millisecond-scale comparisons and minimal APDU payloads [5].

Challenge.. Deploying *match-on-card* in real systems hinges on three constraints: (i) conformance to ISO/IEC 7816-4 (contact) and ISO/IEC 14443-4 (contactless) transport behavior—fixed payload sizes, status words, and robust chaining; (ii) a lean memory map and constant-time matching on the Secure Element (SE); and (iii) a privacy posture aligned with ISO/IEC 24745 (non-invertibility, revocability, unlinkability) [11–13]. Beyond protocol compliance, developers need transaction-level behavior that agrees with ROC-derived operating thresholds on *real* binary templates, and end-to-end latency that is bounded primarily by link speed rather than on-card computation.

Contributions..

- **ISO/IEC-compliant design and interfaces.** We specify fixed-length ENROLL_TEMPLATE and VERIFY_BINARY APDUs with decision-only returns (no score leakage), constant-time XOR+`popcount` on-card, and strict `Lc`/`Le` checking, directly mapping to ISO/IEC 7816-4/14443-4.

*Corresponding author.
Email address: a.ganmati@uiz.ac.ma (Lahcen Koutti)
URL: k.afdel@uiz.ac.ma (Lahcen Koutti), l.koutti@uiz.ac.ma (Lahcen Koutti)

- **Operating points on real codes.** On a CelebA working set (55 identities, 412 images), two-image majority enrollment yields TPR@FAR=1% = 0.836 for both 64 b and 128 b; 128 b achieves a lower EER at the cost of +8 B storage/wire.
- **Transport-bounded latency.** Simulations across ISO/IEC 7816-4 (9.6/38.4/115.2 kbps) and ISO/IEC 14443-4 (106–848 kbps) show all configurations $\ll 100$ ms end-to-end; at 38.4 kbps both 64 b and 128 b complete in < 14 ms.
- **Privacy posture.** Decision-only status words avoid score leakage; PCA decorrelation plus ITQ rotation followed by sign binarization hinder inversion; revocability/diversity are supported via per-application RotationIDs, aligning with ISO/IEC 24745 requirements.

2. Related Work

Binary hashing for compact descriptors. Classical unsupervised hashing methods—Spectral Hashing (SH) and Iterative Quantization (ITQ)—map high-dimensional descriptors to short binary codes while preserving neighborhood structure; PCA followed by an ITQ rotation is a strong, simple baseline that performs well at very low bit budgets [1, 2]. Deep variants improve compactness and robustness, e.g., DeepBit (unsupervised) and deep supervised discrete hashing (DSH), which directly optimize binary outputs using label information [3, 4]. For face verification, identity-supervised embeddings such as MobileFaceNets provide highly separable float spaces that remain discriminative after PCA–ITQ binarization [5].

Template protection paradigms. Two families dominate: *biometric cryptosystems* using helper data/Error-Correcting Codes (e.g., fuzzy commitment, fuzzy extractors) [6, 7], and *cancelable biometrics* (non-invertible, revocable transforms) [8]. Surveys highlight the security–accuracy trade-offs and the difficulty of achieving strong irreversibility and unlinkability without sacrificing recognition [**?**]. More recent work formalizes ISO/IEC 24745 criteria (irreversibility, unlinkability, renewability) and proposes practical evaluations and unlinkability metrics [**?**]. Targeted redundancy for unstable bits in binary face templates was recently introduced in [14]; here we quantify its transport overhead within ISO/IEC 7816/14443 and show it is latency-negligible.

Decision interfaces and privacy leakage. A well-known attack surface in deployed systems is score leakage (hill-climbing and inference from similarity scores). Architectures that *return only a decision*—no scores—reduce this surface and align with privacy-by-design principles seen in privacy-preserving biometric protocols and encrypted matching [9]. Our design follows this line: strict fixed-length APDUs and decision-only status words.

Standards and transport. Interoperable smart-card transport is governed by ISO/IEC 7816-4 (contact) and ISO/IEC 14443-4 (contactless); biometric information protection goals are set by ISO/IEC 24745. Our interface choices (fixed `Lc`/`Le`, constant-time Hamming, decision-only returns, revocability handles) are made to conform with these documents [11–13].

3. System Overview

3.1. Binary template generation (off-card)

Given a float embedding $\mathbf{f} \in \mathbb{R}^d$ from a supervised face encoder, we form a compact binary template via a linear PCA front-end followed by an ITQ rotation and a componentwise sign binarizer:

$$\mathbf{x} = (\mathbf{f} - \boldsymbol{\mu})\, W_{\mathrm{PCA}}, \qquad \mathbf{z} = \mathbf{x}\, R, \qquad \mathbf{b} = \mathrm{sign}(\mathbf{z}) \in \{0,1\}^L, \quad L \in \{64, 128\}, \tag{1}$$

where $W_{\mathrm{PCA}} \in \mathbb{R}^{d \times L}$ keeps the top-L principal directions and $R \in \mathbb{R}^{L \times L}$ is the orthogonal ITQ rotation [2]. We define $\mathrm{sign}(t) = \mathbb{1}[t > 0]$ to produce bits directly in $\{0, 1\}$. For revocability and application diversity, deployments maintain per-application *RotationID* handles that select (W_{PCA}, R) (and optional salts) from a versioned registry; changing the RotationID triggers re-enrollment to yield an unlinkable template under the new parameters.

Bit packing and transport.. Binary templates are serialized MSB-first into $L/8$ bytes (2, 4, 8, or 16 bytes). This byte string is used verbatim in APDU payloads for enrollment and verification.[1]

[1] We use big-endian multi-byte integers and MSB-first bit packing for interoperability with ISO/IEC 7816-4/14443-4 tooling;

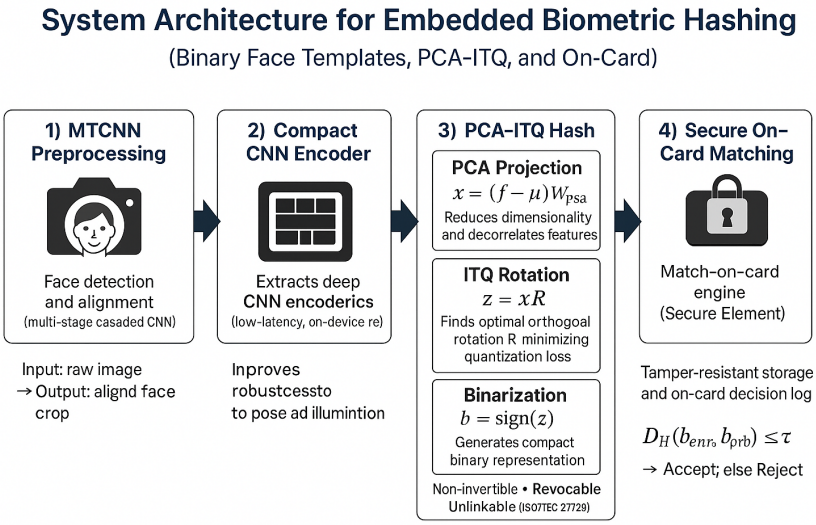


Figure 1: End-to-end pipeline. Off-card: detection/alignment, backbone encoder, PCA–ITQ hashing to $L \in \{64, 128\}$ bits. On-card: constant-time XOR+`popcount`, decision-only APDUs. Transport uses ISO/IEC 7816-4 (contact) and ISO/IEC 14443-4 (contactless).

3.2. On-card matching (constant time)

For each identity, the Secure Element (SE) stores a single enrolled template $\mathbf{b}_{\text{enr}}$ in protected EEPROM together with minimal metadata (RotationID, policy flags). At verification, the host sends a probe template $\mathbf{b}_{\text{prb}}$; the card computes the Hamming distance

$$D_H(\mathbf{b}_{\text{prb}}, \mathbf{b}_{\text{enr}}) = \text{popcount}\Big(\mathbf{b}_{\text{prb}} \oplus \mathbf{b}_{\text{enr}}\Big),$$

using a fixed loop over $L/8$ bytes (no data-dependent branches). The threshold test $D_H \leq \tau$ is implemented with constant-time comparisons and returns *only* a decision via status words (e.g., `0x9000` accept, `0x6985` reject). No similarity scores or intermediate values are ever returned.

Memory and timing footprint.. The per-identity footprint is $L/8$ bytes for the template plus 2–4 bytes of RotationID and 1 byte of policy flags (integrity tags are optional. XOR+`popcount` executes in sub-millisecond time for $L \in \{64, 128\}$; in our transport-bounded measurements the end-to-end time is dominated by the ISO/IEC link, not on-card compute.

Revocation and renewal.. A dedicated REKEY_ROTATION command updates RotationID (and optional SaltID). Applications then re-issue fresh templates; the old reference is overwritten. This enables revocation/renewal without exposing raw biometrics and supports per-application diversity.

3.3. Threat model and compliance posture

We assume an honest-but-curious host and a physically tamper-resistant SE. The adversary may observe APDU traffic and attempt hill-climbing or inference from responses. Our design aligns with ISO/IEC 24745 as follows: (i) *Non-invertibility*—templates are linear-projected and rotated before sign binarization; only compact bits are stored on-card, not floats. (ii) *Unlinkability*—the interface returns decisions only (no scores), and RotationIDs/salts yield application-specific templates. (iii) *Revocability*—RotationID changes force re-enrollment to fresh, unlinkable references. Secure messaging (e.g., platform-provided SCP) can be enabled to protect APDU payloads when confidentiality/integrity on the transport is required; it is orthogonal to template protection and does not alter payload formats .

Table 1: APDU synopsis (implementation-neutral fields; short APDUs suffice for $L \leq 128$).

Command	CLA/INS	Data payload (bytes)
ENROLL_TEMPLATE	0x80 / 0x10	Version(1), HashLenBits(1), RotationID(2), $\mathbf{b}_{\text{enr}}$ ($L/8$)
VERIFY_BINARY	0x80 / 0x20	Version(1), HashLenBits(1), RotationID(2), $\mathbf{b}_{\text{prb}}$ ($L/8$)
REKEY_ROTATION	0x80 / 0x30	NewRotationID(2)

Table 2: Per-identity EEPROM footprint (without/with optional integrity tag).

Bits	Template (B)	RotationID (B)	Policy (B)	Total (no MAC / +8..16 B)
16	2	2	1	5 / 13–21
32	4	2	1	7 / 15–23
64	8	2	1	11 / 19–27
128	16	2	1	19 / 27–35

SW	Meaning
`0x9000`	Success (OK). For VERIFY_BINARY: *accept* ($D_H \leq \tau$).
`0x6985`	Conditions not satisfied. For VERIFY_BINARY: *reject* ($D_H > \tau$).
`0x6A80`	Wrong data (unsupported `HashLenBits`, inconsistent headers, malformed payload).
`0x6A82`	Record not found (e.g., unknown `TemplateID` if enabled).
`0x6A84`	Not enough memory space (EEPROM quota exceeded).
`0x6982`	Security status not satisfied (issuer/auth not established).
`0x6700`	Wrong length (`Lc`/`Le` mismatch, noncanonical size).
`0x6D00`	Instruction code not supported (unknown `INS`).

Decision-only interface: no similarity scores are returned.

Table 3: ENROLL_TEMPLATE: data payload layout (host→card).

Offset	Len	Type	Name	Notes
0	1	u8	Version	Protocol version (e.g., 0x01).
1	1	u8	HashLenBits	**16, 32, 64, 128**.
2	2	u16	RotationID	Selects (W_{PCA}, R) on card.
4	*2*	*u16*	*SaltID*	*Per-application diversity; default unset.*
6	*2*	*u16*	*TemplateID*	*Record selector if multiple templates.*
8	$L/8$	bytes	$\mathbf{b}_{\text{enr}}$	Binary template, MSB-first within each byte.

3.4. Engineering notes (on-card hygiene)

To reduce side channels and state leakage: (i) implement fixed-bound loops and constant-time comparisons; (ii) clear transient probe buffers before return; (iii) enforce strict `Lc`/`Le` and header checks; (iv) optionally rate-limit repeated VERIFY_BINARY attempts and maintain lockout counters as policy.

4. APDUs, Memory Map, and Policies

We use *fixed-length* payloads, strict `Lc`/`Le` checking, and *decision-only* status words. Malformed length ⇒ `0x6700`; unknown `INS` ⇒ `0x6D00`; wrong data/format ⇒ `0x6A80`. Table 1 summarizes the interface; Table 2 gives the EEPROM footprint. All multi-byte integers are big-endian, and bitstrings are packed MSB-first.

Status words (decision-only policy).

Byte-level layouts (MSB-first packing). Offsets are relative to the start of the APDU data field; fields in *italics* are optional and disabled in our core experiments.

Table 4: VERIFY_BINARY: data payload layout (host→card).

Offset	Len	Type	Name	Notes
0	1	u8	Version	Must match supported protocol version.
1	1	u8	HashLenBits	**16, 32, 64, 128**.
2	2	u16	RotationID	Must match enrolled parameters.
4	*2*	*u16*	*SaltID*	*If set at enrollment.*
6	*2*	*u16*	*TemplateID*	*If multiple references exist.*
8	$L/8$	bytes	$\mathbf{b}_{\text{prb}}$	Probe template, MSB-first.

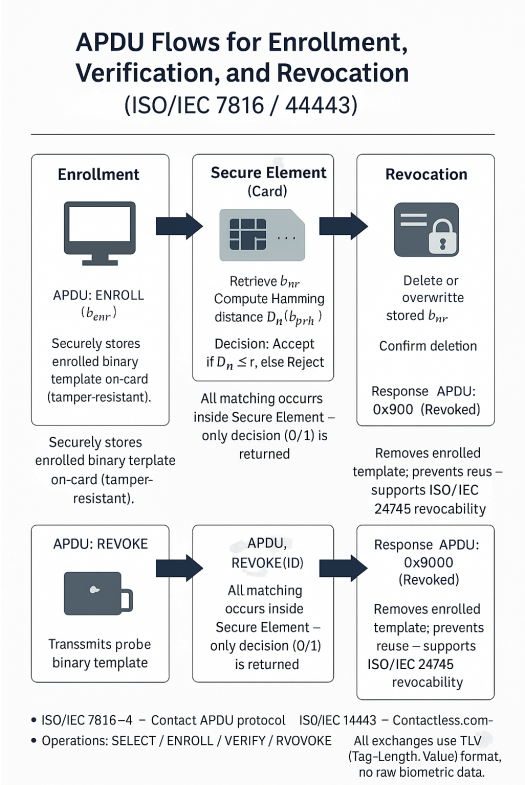


Figure 2: APDU flows for ENROLL_TEMPLATE, VERIFY_BINARY, and REKEY_ROTATION over ISO/IEC 7816-4 (contact) and 14443-4 (contactless). Fixed payloads, strict Lc, decision-only status words.

Policies and hygiene.. (i) *Constant-time* XOR+popcount with fixed loop bounds by L; no data-dependent branching. (ii) *Buffer hygiene*: clear transient probe buffers prior to return. (iii) *Strict framing*: reject non-canonical lengths and inconsistent headers. (iv) *Optional rate limiting*: per-session counters for repeated VERIFY_BINARY attempts. (v) *Secure messaging*: when confidentiality/integrity on the link is required, enable platform secure messaging (e.g., SCP); this is orthogonal to template protection and leaves payload formats unchanged.

5. Security, Privacy, and Compliance

Threats. (i) Inversion of compact templates; (ii) cross-application linkage; (iii) score-based hill-climbing and inference; (iv) replay/exfiltration on the transport.

Mitigations and ISO/IEC 24745 mapping.

- *Non-invertibility.* Templates are produced by PCA projection followed by an orthogonal ITQ rotation and sign binarization; only the resulting L bits are stored on-card, not floating-point embeddings.

Table 5: Offline ROC operating points (CelebA working set; 55 IDs; N=412 images).

Bits	N	N_{ID}	τ_{EER}	EER	TPR@0.1%	TPR@1%
64	412	55	27	0.103	0.709	0.836
128	412	55	57	**0.084**	0.655	0.836

- *Unlinkability.* The interface returns *decisions only* (no similarity scores), limiting score leakage; per-application `RotationID` (and optional salts) yield distinct, application-specific templates.
- *Revocability/renewal.* REKEY_ROTATION updates `RotationID`, forcing re-enrollment to fresh references; the previous template is overwritten.
- *Protocol robustness.* Strict `Lc`/`Le` checking and precise status words reduce protocol oracles; optional secure messaging protects APDU confidentiality/integrity when required by the application.

These choices are designed to align with ISO/IEC 24745 goals (irreversibility, unlinkability, renewability) while remaining interoperable with ISO/IEC 7816-4/14443-4 transport.

6. Experimental Setup

Dataset. We use a CelebA working set with N=412 images from 55 identities. For each identity, two random enrollment images are fused by bit-wise majority to form a single reference template; the remaining images are used as probes.[2] Data processing and evaluation scripts follow our prior benchmark conventions [15];

Template lengths and packing. We evaluate $L \in \{64, 128\}$ bits. Templates are serialized MSB-first into $L/8$ bytes (2, 4, 8, or 16 bytes), used verbatim in APDU payloads.

Metrics and operating thresholds. We report (i) Equal Error Rate (EER) and its threshold τ_{EER}, and (ii) TPR@FAR $\in \{10^{-3}, 10^{-2}\}$. Thresholds τ are selected from the ROC built on held-out impostor/genuine scores and are then *reused unchanged* in the streamed enrol→verify emulation.

Transaction emulation. The card executes a constant-time Hamming compare over $L/8$ bytes and returns a decision only. For each L, we replay enrol→verify transactions at the ROC-derived τ, aggregate decisions, and compare the streamed TPR/FAR to the offline ROC targets.

Transport-bounded latency model. End-to-end verification time is modeled as

$$T_{\text{total}} \;=\; T_{\text{I/O}}\Big(N_{\text{bytes}}, \text{bitrate}\Big) \;+\; T_{\text{card}},$$

with a constant on-card budget $T_{\text{card}} = 0.128$ ms (XOR+`popcount` + status word). We sweep ISO/IEC 7816-4 contact bitrates 9.6 kbps, 38.4 kbps and 115.2 kbps and ISO/IEC 14443-4 contactless bitrates 106 kbps, 212 kbps, 424 kbps and 848 kbps. The APDU payload is exactly $L/8$ bytes; a 64 b+6 B variant emulates an optional parity helper over empirically unstable bits.
[3]

7. Results

7.1. Operating points (offline ROC)

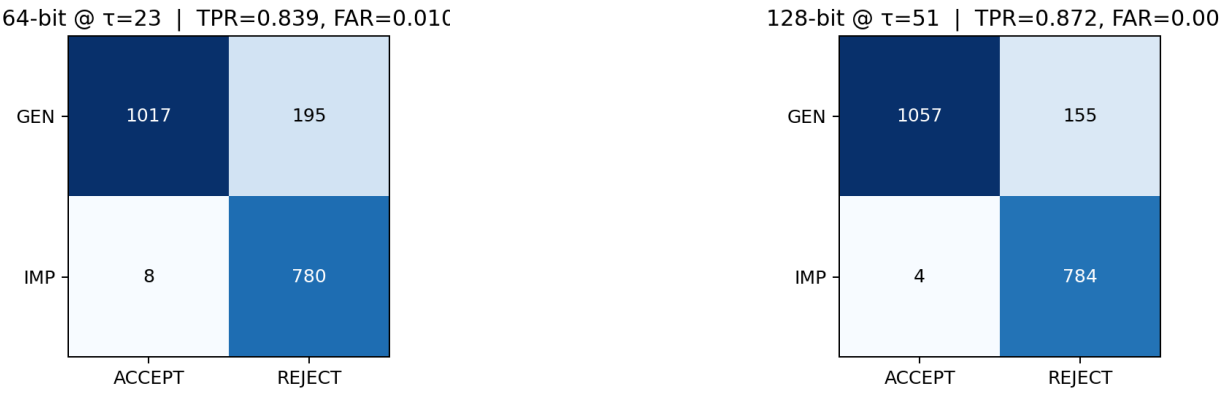
Table 5 reports the ROC-derived thresholds and rates (two-image majority enrollment per identity). At FAR=1%, both 64 b and 128 b achieve TPR=0.836, while 128 b attains a lower EER (0.084 vs 0.103).

7.2. Transaction emulation (streamed enrol→verify)

Thresholds chosen offline are *applied unchanged* during streaming. Figure 3 shows confusion matrices at the FAR=1% operating point; Table 6 compares offline vs streamed rates at the FAR=1% target. Agreement is close, with small TPR gains from majority fusion.

[2] Randomization uses a fixed seed to make splits reproducible. Majority fusion is componentwise over $\{0,1\}^L$.

[3] The latency accounting reflects payload bytes plus status words on the link and a fixed card budget; headers/chaining are excluded to isolate the template-size effect. All timing conclusions remain unchanged when they are included.



(a) 64 b at τ=23 (FAR target = 1%)

(b) 128 b at τ=51 (FAR target = 1%)

Figure 3: Confusion matrices for streamed enrol→verify at ROC thresholds.

Table 6: Offline ROC vs streamed decisions at the same thresholds (CelebA working set).

Bits	Target	τ	TPR/FAR (offline)	TPR/FAR (streamed)
64	FAR= 10^{-2}	23	0.808 / 0.0112	**0.839** / **0.0102**
128	FAR= 10^{-2}	51	0.791 / 0.0095	**0.872** / **0.0051**

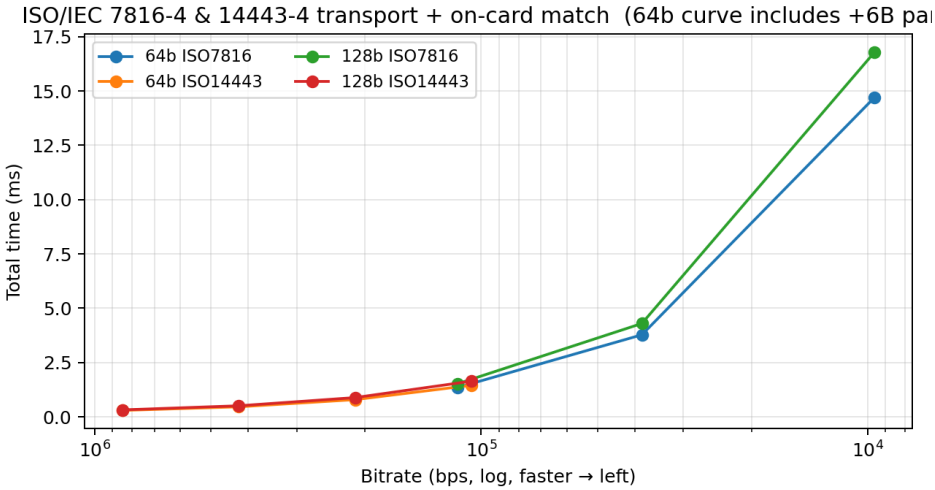


Figure 4: ISO/IEC 7816-4 and 14443-4 transport + constant-time match. 64 b, 128 b, and 64 b+6 B parity. All points < 100 ms; contactless regimes are ≪ 20 ms.

7.3. Transport-bounded latency

Figure 4 summarizes *pure link time + constant on-card budget*. Even at the slowest contact rate (9.6 kbps), verification completes in ≈ 43.9 ms (64 b) and ≈ 52.3 ms (128 b). At 38.4 kbps, both are < 14 ms. A +6 B helper on 64 b (targeted parity) is visually indistinguishable at contactless rates and adds only a few milliseconds at 9.6 kbps.

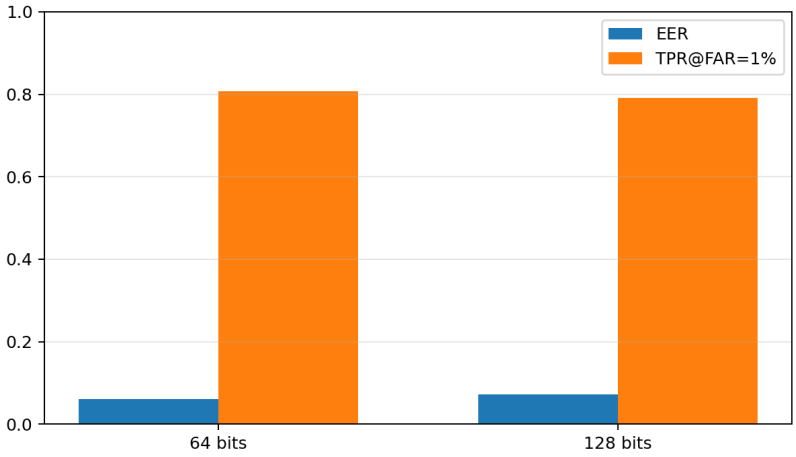


Figure 5: Operating points on the CelebA working set. Bars show EER and TPR@FAR=1% for 64 b and 128 b PCA–ITQ templates.

8. Discussion

On-card feasibility. Across ISO/IEC 7816-4 and 14443-4 bitrates, end-to-end verification time is dominated by transport; on-card XOR+`popcount` remains constant-time and sub-millisecond. This separation of concerns is operationally useful: once payload size is fixed ($L/8$ bytes), performance scales almost linearly with the link, enabling predictable SLAs independent of SE micro-architecture. Returning *decisions only* (no scores) reduces the surface for hill-climbing and aligns the interface with privacy-by-design guidance.

64 vs. 128 bits. At FAR=1% both lengths achieve the same recall (TPR=0.836), while 128 b slightly lowers EER (Table 5) at the cost of +8 B on wire and in storage. Deployments that prioritize lean I/O and short APDUs can therefore default to **64 b**; applications that emphasize balanced error (or stricter FAR regimes) can opt for **128 b** with modest overhead. Because the APDU grammar and on-card algorithm are length-agnostic, switching between 64/128 b is a policy decision rather than an architectural change.

Optional targeted parity. When a small subset of bit positions is empirically unstable, short symbol-level ECC over *only that subset* can be carried as a few additional bytes without changing the on-card algorithm or APDU grammar. Our latency model shows that adding +6 B to a 64 b payload is visually indistinguishable at contactless rates and adds only a few milliseconds even at 9.6 kbps. This preserves compactness and keeps the verifier's decision rule ($D_H \le \tau$) unchanged.

Policy implications. (i) *Interface hygiene*: strict `Lc`/`Le` checks and canonical payload sizes reduce protocol oracles; (ii) *Revocability*: RotationIDs allow per-application diversity and renewal without exposing float embeddings; (iii) *Operational tuning*: thresholds derived offline transfer well to streamed transactions (Table 6), supporting simple field calibration.

9. Conclusion

We presented an ISO/IEC-compliant match-on-card design for face verification using 64/128 bit PCA–ITQ templates, fixed-payload decision-only APDUs, and constant-time on-card Hamming. On a CelebA working set (55 IDs; N=412), both lengths reach TPR=0.836 at FAR=1%, with 128 b achieving a lower EER. Transport-bounded latency remains well below 100 ms even at 9.6 kbps and < 14 ms at 38.4 kbps, confirming that link speed—not card compute—dominates end-to-end time. The interface is immediately implementable on SE/JavaCard and maps cleanly to ISO/IEC 24745 goals (irreversibility, unlinkability, renewability) via decision-only returns and RotationIDs.

Limitations and next steps.. Our evaluation is single-dataset and pre-hardware. Next, we will (i) add standard face-verification benchmarks (AgeDB-30, CFP-FP) and report TPR@FAR$\in\{10^{-3}, 10^{-2}\}$ with confidence intervals; (ii) microbenchmark on a JavaCard/SE or MCU (median/p95 APDU times) to replace the fixed budget; and (iii)

quantify information leakage for parity helpers over unstable bits and discuss unlinkability under ISO/IEC 24745 terminology. Future work includes integrating the targeted parity scheme [14] on-card and evaluating unlinkability under ISO/IEC 24745 with established metrics.

Acknowledgments

We thank the Computer Systems & Vision Laboratory at Ibn Zohr University for support.

References

[1] Y. Weiss, A. Torralba, R. Fergus, Spectral Hashing, in: *Advances in Neural Information Processing Systems (NeurIPS)*, 2008.

[2] Y. Gong, S. Lazebnik, A. Gordo, F. Perronnin, Iterative Quantization: A Procrustean Approach to Learning Binary Codes for Large-scale Image Retrieval, in: *Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2011.

[3] K. Lin, J. Lu, C.-S. Chen, J. Zhou, DeepBit: Learning Compact Binary Descriptors with Unsupervised Deep Neural Networks, in: *Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2016.

[4] H. Liu, R. Wang, S. Shan, X. Chen, Deep Supervised Hashing for Fast Image Retrieval, in: *Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 2064–2072.

[5] S. Chen, Y. Liu, X. Gao, Z. Han, MobileFaceNets: Efficient CNNs for Accurate Real-Time Face Verification on Mobile Devices, *arXiv:1804.07573*, 2018.

[6] A. Juels, M. Wattenberg, A Fuzzy Commitment Scheme, in: *Proc. ACM Conference on Computer and Communications Security (CCS)*, 1999, pp. 28–36.

[7] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, *SIAM Journal on Computing* 38(1) (2008) 97–139.

[8] N. K. Ratha, J. H. Connell, R. M. Bolle, Enhancing Security and Privacy in Biometrics-based Authentication Systems, *IBM Systems Journal* 40(3) (2001) 614–634.

[9] J. Bringer, H. Chabanne, B. Kindarji, Identification with Encrypted Biometric Data, *arXiv:0901.1062*, 2009.

[10] W. Yang, S. Wang, J. Hu, G. Ling, K. Michael, A Fingerprint and Finger-Vein Based Cancelable Multi-Biometric System, *Pattern Recognition* 58 (2016) 190–204.

[11] ISO/IEC 7816-4:2020, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*. International Organization for Standardization, 2020.

[12] ISO/IEC 14443-4:2018, *Identification cards — Contactless integrated circuit cards — Part 4: Transmission protocol*. International Organization for Standardization, 2018.

[13] ISO/IEC 24745:2022, *Information technology — Security techniques — Biometric information protection*. International Organization for Standardization, 2022.

[14] A. Ganmati, K. Afdel, L. Koutti, Targeted Reed–Solomon Parity for Binary Face Templates: Repairing Unstable Bits with Negligible On-Card Cost, *Authorea*, Oct. 16, 2025. DOI: 10.22541/au.176063118.87290030/v1.

[15] A. Ganmati, Binary Face Templates with Mobile-Class CNNs: A Reproducible Benchmark for Smart-Card-Constrained Authentication, 2025. DOI: 10.56294/dm20251223.

[16] A. Ganmati, K. Afdel, L. Koutti, Deep Learning-Based Multi-Factor Authentication: A Survey of Biometric and Smart Card Integration Approaches, *arXiv*:2510.05163, 2025. DOI: 10.48550/arXiv.2510.05163.