CRT Walls: Isomorphism Encoding

CRT Walls for Product-Functorial Isomorphism Encodings of Semiprime Factorization

Abstract. We investigate whether integer factorization of an RSA semiprime $N = pq$ can be encoded as a small group or matrix-space isomorphism problem solvable by Babai's quasi-polynomial algorithm. The encoding would need to have size $\text{poly}(\log N)$ and to recover p, q from an isomorphism witness. We prove that this is impossible via product-functorial algebraic encodings: any such encoding either remains CRT-symmetric (carrying no p/q-distinguishing information) or already generates a factoring certificate before the isomorphism algorithm applies. We extend this to matrix-space invariants (adjoint algebra, centroid, radical) and to singular matrix spaces. The singular case exhibits a genuine boundary: publicly constructible singular matrix spaces can have locally asymmetric rank structure without containing an immediate factoring witness (Theorem 16.2, counterexample $\mathcal{S}_d$). However, any constructive witness for the asymmetry is polynomial-time equivalent to QR-witness extraction, which is factoring-equivalent under standard reductions (Theorem 16.3). The conclusion is a dichotomy: *no small explicit Babai encoding factors N, and the only remaining route — forced singular witness extraction — is equivalent to the known hardness of quadratic residuosity witness computation.*

---

1. Introduction

Babai's quasi-polynomial graph isomorphism algorithm [Babai 2016] runs in time $n^{O(\log n)}$ for graphs on n vertices. For $n = \text{poly}(\log N)$, this gives complexity

$$\exp(O((\log \log N)^2)),$$

which beats $L_N[1/3]$ asymptotically and would constitute a significant breakthrough for RSA factorization. This raises the question: can factorization of $N = pq$ be encoded as a small explicit group, graph, or matrix-space isomorphism problem of size $\text{poly}(\log N)$?

The natural candidates are algebraic constructions over $R = \mathbb{Z}/N\mathbb{Z}$: unit groups, torsion subgroups of elliptic curves, matrix spaces arising from R-module structure. All of these are *product-functorial* — they decompose as $F(R) \cong F(\mathbb{F}_p) \times F(\mathbb{F}_q)$ via the Chinese Remainder Theorem. This product structure is the source of the obstruction.

Main result (informal). Every product-functorial Babai-compatible construction either (a) preserves the CRT symmetry and carries no p/q-distinguishing information, or (b) produces an effectively CRT-separating witness that already factors N before Babai is invoked. Babai's algorithm is never the critical step.

This negative result is sharp. We exhibit a family $\mathcal{S}_d$ of singular matrix spaces with publicly verifiable local rank asymmetry between $\mathbb{F}_p$ and $\mathbb{F}_q$, without any coefficient being a zero-divisor modulo N. This shows the strong wall ("existence implies factoring") is false. The weak wall ("witness implies factoring") is true and tight: extracting a concrete rank-1 element of $\mathcal{S}_d$ is equivalent to producing a QR-witness for d modulo N, which is polynomial-time interreducible with factoring.

Limits of claims. This paper does not prove that no classical factoring algorithm below $L[1/3]$ exists, nor that factoring is hard in any complexity-theoretic sense. It proves that a specific class of Babai-encoding approaches — product-functorial ones — cannot avoid the CRT wall. The "factoring-equivalent" claims are under standard randomized polynomial-time reductions and concern QR-*witness* extraction, not QR-*decision* (which is easy via the Jacobi symbol).

Organization

§2 collects preliminaries (CRT structure, Idempotent–Factor Lemma, QR-witness). §3 defines product-functorial and Babai-compatible encodings. §4 states and proves the CRT-Wall Theorem. §5 analyzes specific algebraic candidates. §6 extends to matrix-space invariants and identifies the non-central projector gap. §7 proves the singular matrixspace boundary results. §8 makes the QR-witness interreduction explicit. §9 concludes.

---

2. Preliminaries

Throughout, $N = pq$ is an RSA semiprime with p, q distinct odd primes, and $R = \mathbb{Z}/N\mathbb{Z}$.

2.1 CRT structure

By the Chinese Remainder Theorem,

$$R \cong \mathbb{F}_p \times \mathbb{F}_q.$$

The two projections $\pi_p : R \to \mathbb{F}_p$ and $\pi_q : R \to \mathbb{F}_q$ are the *CRT components*. An element $a \in R$ is a *nontrivial zero-divisor* if $a \neq 0$ and a is not a unit; equivalently, $\pi_p(a) = 0$ or $\pi_q(a) = 0$ but not both. Such elements satisfy $1 < \gcd(a, N) < N$.

2.2 Idempotent–Factor Lemma

Lemma (Idempotent–Factor). Let $e \in R$ with $e^2 \equiv e \pmod{N}$ and $e \not\equiv 0, 1 \pmod{N}$. Then $\gcd(e, N)$ or $\gcd(e-1, N)$ is a nontrivial factor of N.

Proof. Under CRT, idempotents in $\mathbb{F}_p \times \mathbb{F}_q$ are componentwise 0 or 1. The only nontrivial idempotents are $(1, 0)$ and $(0, 1)$, divisible by exactly one of p, q. □

2.3 QR-Decision vs QR-Witness

For $d \in R^*$:

- **QR-Decision:** Compute $(\frac{d}{N})$ (the Jacobi symbol). *Easy:* polynomial-time algorithm, no factoring required.
- **QR-Witness:** Find (x, y) with $x^2 \equiv dy^2 \pmod{N}$, (x, y) nontrivial (i.e., $xy \not\equiv 0$ and x/y is not a square root of d modulo both p and q simultaneously). *Hard:* factoring-equivalent under standard reductions (see §8).

These two problems must not be conflated. All "factoring-equivalent" claims in this paper refer to QR-*Witness*, not QR-Decision.

---

3. Product-functorial Babai encodings

Definition 3.1 (Babai-compatible instance). A family $I(N)$ of group/graph/permutation instances is Babai-compatible if it is computable in time $\mathrm{poly}(\log N)$ and has size $n(N) = \mathrm{poly}(\log N)$.

For Babai-compatible instances, the algorithm runs in time

$$n^{O(\log n)} = \mathrm{poly}(\log N)^{O(\log \mathrm{poly}(\log N))} = \exp(O((\log \log N)^2)),$$

beating $L_N[1/3]$.

Definition 3.2 (Product-functorial encoding). An encoding F is product-functorial if $F(A \times B) \cong F(A) \times F(B)$ canonically. Typical examples: $R \mapsto R^*$, $R \mapsto R^*/(R^*)^k$, $R \mapsto E[\ell](R)$ for elliptic E, Cayley graphs on functorially defined generators.

Definition 3.3 (Effectively CRT-separating witness). A witness w output by an algorithm on input N is *effectively CRT-separating* if it enables the computation, in polynomial time, of a nontrivial idempotent or ring projector $e \in R$ with $e \neq 0, 1$.

4. The CRT-Wall Theorem

Lemma 4.1 — Effectively CRT-separating witnesses imply factoring

Let F be a product-functorial encoding with $F(R) \cong F(\mathbb{F}_p) \times F(\mathbb{F}_q)$. Let $G = F(R)$ and suppose an algorithm outputs a witness w that is effectively CRT-separating (Definition 3.3). Then N can be factored in polynomial time.

Proof. By Definition 3.3, w enables computation of $e \in R$ with $e^2 = e$, $e \neq 0, 1$. By the Idempotent–Factor Lemma, $\gcd(e, N)$ is a nontrivial factor of N. □

Remark. The content of the lemma is not tautological: it identifies the *effectively CRT-separating* condition as the right hypothesis, and rules out two spurious strengthenings — (a) that every isomorphism witness is CRT-separating (false: CRT-symmetric witnesses are not), and (b) that the construction needs to proceed through Babai (false: the idempotent is extracted before isomorphism is needed). More concretely: if w contains an element $g \in G$ whose order divides $|F(\mathbb{F}_p)|$ but not $|F(\mathbb{F}_q)|$, set $k = |F(\mathbb{F}_p)|$. Then $g^k \equiv 1 \pmod{p}$ and $g^k \not\equiv 1 \pmod{q}$, so $g^k - 1$ is a nontrivial zero-divisor and $\gcd(g^k - 1, N)$ factors N.

Theorem 4.2 — CRT-Wall for product-functorial Babai encodings

Let F be a product-functorial algebraic encoding and $N = pq$ squarefree. Suppose a Babai-compatible GI instance $I(N)$ of size $\mathrm{poly}(\log N)$ is constructed from $F(R)$. Then:

1. (Symmetric case.) If the construction is invariant under swapping the two CRT components, every canonically computable isomorphism witness carries at most Jacobi-type symmetric information and cannot separate p and q.
2. (Separating case.) If the construction or extracted isomorphism witness is effectively CRT-separating, it generates a nontrivial CRT projector, which by Lemma 4.1 immediately yields a factor of N.

In particular, Babai's algorithm cannot serve as the "missing last step": either the construction is factorization-blind, or it has already factored N before the isomorphism step.

Proof. Product-functoriality gives $F(R) \cong F(\mathbb{F}_p) \times F(\mathbb{F}_q)$. Any canonical operation on $F(R)$ either (a) treats both components symmetrically, preserving the swap-invariance, in which case no p/q-distinguishing projection exists; or (b) produces an element with asymmetric CRT behavior, which is by definition an effectively CRT-separating witness. By Lemma 4.1, case (b) factors N. □

5. Candidate analysis

We apply Theorem 4.2 to the natural algebraic candidates.

Unit group R^*. Size $\approx N$; not Babai-compatible. Small quotients $R^*/(R^*)^k$ are again product-functorial and CRT-decomposed. *Closed.*

Nontrivial square roots of 1 in R. A perfect extraction mechanism: $\xi^2 \equiv 1$, $\xi \not\equiv \pm 1$ gives $\gcd(\xi - 1, N)$. But constructing such ξ is factoring-equivalent. *Closed.*

Elliptic ℓ-torsion $E[\ell](R)$. By Hensel lifting, $E[\ell](R) \cong E[\ell](\mathbb{F}_p) \times E[\ell](\mathbb{F}_q)$. Product-functorial; separated Frobenius data require CRT. *Closed.*

Galois groups of N-dependent polynomials (e.g. $x^m - N$). These detect Kummer/root structure of N as a single integer, not the factorization $N = pq$: the group $\mathrm{Gal}(\mathbb{Q}(\zeta_m, N^{1/m})/\mathbb{Q})$ depends only on m and N, not on p and q individually. *Closed.*

Cayley/automorphism graphs on $N \bmod m$ generators. Babai-compatible and computable from N alone, but carry only public residue data, not CRT-separating information: the construction depends only on $N \bmod m$, which is publicly computable and CRT-blind. *Closed.*

---

6. HPMI and matrix-space invariants

The Hidden Product Matrix-space Isometry (HPMI) problem asks whether factorization can be encoded in a singular matrix space $\mathcal{M} \leq \mathrm{Mat}_m(R)$ that admits a natural isometry decomposition exploiting local rank asymmetry.

Theorem 6.1 — Extension to matrix-space invariants. Let $\mathcal{M}$ be a matrix space over R and let $\Phi(\mathcal{M})$ be a product-compatible algebraic invariant (adjoint algebra, centroid, endomorphism ring, radical, determinantal ideals):

$$\Phi(\mathcal{M}_R) \cong \Phi(\mathcal{M}_p) \times \Phi(\mathcal{M}_q).$$

Then the same CRT dichotomy applies: the output is either CRT-symmetric, or it generates a central CRT-separating idempotent that factors N by the Idempotent–Factor Lemma.

6.2 Non-central projectors — the residual gap

Not every idempotent in $\mathrm{Adj}(\mathcal{M})$ factors N. A matrix idempotent such as

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{F}_p)$$

is a nontrivial projector but carries no CRT information about p vs. q. Factorization follows only from a *central scalar* idempotent eI with $e \in Z(R)$, $e^2 \equiv e \pmod N$, $e \notin \{0, 1\}$.

Formally: if $e \in \mathrm{Adj}(\mathcal{M})$ is a non-central idempotent, it gives a direct-sum decomposition of the $\mathcal{M}$-action but **not** a CRT decomposition of R itself. Such non-central idempotents do not automatically yield $\gcd(e, N) \in \{p, q\}$.

This creates a narrow residual gap: a non-central idempotent in $\mathrm{Adj}(\mathcal{M})$ might exist without factoring N. Whether any such idempotent can be constructed from N alone, without factoring-equivalent data, is not ruled out by Theorem 6.1. All known natural constructions from R-data collapse to central decompositions or QR-witnesses; but we acknowledge this gap rather than silently closing it.

---

7. The singular matrix-space boundary

7.1 Constructive witness wall (Theorem 16.1)

Theorem 7.1 — Constructive witness wall. Let $\mathcal{M} \leq \mathrm{Mat}_m(R)$ be publicly given. If an algorithm outputs a concrete matrix $M \in \mathcal{M}$ with $\mathrm{rank}_p(M_p) \neq \mathrm{rank}_q(M_q)$, or equivalently (after computing minors) a minor Δ with $\Delta \equiv 0 \pmod p$, $\Delta \not\equiv 0 \pmod q$, then $\gcd(\Delta, N)$ is a nontrivial factor.

Proof. If $\mathrm{rank}(M_p) < \mathrm{rank}(M_q)$, there exists a $(k+1)$-minor of M_p that vanishes while the corresponding minor of M_q does not. Its lift $\Delta \in R$ satisfies $\Delta \equiv 0 \pmod p$, $\Delta \not\equiv 0 \pmod q$, giving $1 < \gcd(\Delta, N) < N$. □

7.2 The strong wall is false — counterexample $\mathcal{S}_d$

Theorem 7.2 — Strong wall is false. The statement "every publicly constructible locally asymmetric singular matrix space already contains a factoring witness" is false.

Counterexample. Choose public $d \in R^*$ with Jacobi symbol $\left(\frac{d}{N}\right) = -1$, computable in polynomial time without factorization. This forces $\left(\frac{d}{p}\right) \neq \left(\frac{d}{q}\right)$. Define

$$\mathcal{S}_d = \left\{ \begin{pmatrix} x & dy & 0 \\ y & x & 0 \\ 0 & 0 & 0 \end{pmatrix} : x, y \in R \right\} \subseteq \mathrm{Mat}_3(R).$$

Every element is singular. The 2×2 upper block has determinant $x^2 - dy^2$. Over $\mathbb{F}_r$, a nonzero rank-1 element exists iff d is a quadratic residue mod r. Therefore

$$\mathrm{minrank}_{\mathbb{F}_p}(\mathcal{S}_d) \neq \mathrm{minrank}_{\mathbb{F}_q}(\mathcal{S}_d),$$

yet no coefficient in the definition of $\mathcal{S}_d$ is a nontrivial zero-divisor modulo N. Local rank asymmetry exists publicly without an immediate factor. □

7.3 The singular matrixspace boundary (Theorem 16.3)

Theorem 7.3 — Singular Matrixspace Boundary. There exist publicly constructible singular matrix spaces over R whose local low-rank structure is asymmetric at p and q. This existence information does not immediately factor N. However, any constructive witness for the asymmetry — a rank-reducing matrix, minor, or pivot — generates a nontrivial zero-divisor and factors N via gcd. In the minimal family $\mathcal{S}_d$, the gap between existence and construction is equivalent to QR-Witness extraction for d modulo the prime factors of N (not QR-Decision; see §8). More general singular matrix spaces may encode stronger or different witness problems, but no natural construction outside this witness paradigm is found in this work.

---

8. QR-Witness interreduction

We make explicit the interreduction between factoring and QR-Witness extraction for the families studied.

QR-Witness problem. Given $N = pq$ and $d \in R^*$, find $(x, y) \in R^2$ nontrivially satisfying $x^2 \equiv dy^2 \pmod{N}$.

The interreduction is stated for the $\mathcal{S}_d$ case where $(\frac{d}{N}) = -1$, so d is a QR mod exactly one of p, q.

Factoring ⇒ QR-Witness (asymmetric isotropic construction). Given p, q: WLOG $(\frac{d}{p}) = +1$ and $(\frac{d}{q}) = -1$. Set

$$x_p \equiv \sqrt{d} \pmod{p}, \quad y_p \equiv 1 \pmod{p}, \qquad x_q \equiv 0 \pmod{q}, \quad y_q \equiv 0 \pmod{q}.$$

CRT-lift to $(x, y) \in R^2$. Then $x^2 - dy^2 \equiv 0 \pmod{p}$ (since $x_p^2 = d$) and $x^2 - dy^2 \equiv 0 \pmod{q}$ (since $x_q = y_q = 0$), so $x^2 \equiv dy^2 \pmod{N}$. But $x \equiv 0 \pmod{q}$ while $x \not\equiv 0 \pmod{p}$, so x is a nontrivial zero-divisor and $\gcd(x, N) = q$.

QR-Witness ⇒ Factoring. Given any (x, y) with $x^2 \equiv dy^2 \pmod{N}$ and (x, y) nontrivial: since $(\frac{d}{N}) = -1$, no global solution with xy invertible modulo N exists — concretely, if $y \in R^*$ then $(x/y)^2 \equiv d \pmod{N}$ would give a global square root of d, contradicting the Jacobi condition; hence x or y must be a zero-divisor. Therefore at least one of $x, y, x^2 - dy^2$ is a nontrivial zero-divisor, and $\gcd(x, N)$, $\gcd(y, N)$, or $\gcd(x^2 - dy^2, N)$ factors N.

Consequence for $\mathcal{S}_d$. Finding a rank-1 element in $\mathcal{S}_d$ requires producing exactly such an asymmetric isotropic witness. Both directions of the interreduc-

tion hold, confirming polynomial-time equivalence to factoring under standard randomized reductions.

---

9. Conclusion

We have proved that product-functorial algebraic encodings cannot route factorization of $N = pq$ through Babai's isomorphism algorithm without first solving the factoring problem. The CRT-Wall Theorem (§4) gives the clean dichotomy: symmetric or already factored. The singular matrix-space analysis (§7) sharpens this: local asymmetry *can* exist publicly (Theorem 7.2), but its exploitation requires a constructive witness equivalent to QR-Witness extraction (Theorem 7.3), itself factoring-equivalent.

The resulting picture is:

Mechanism	Status
Product-functorial Babai encoding	**closed** — Theorem 4.2
Central idempotent in Adj/Cent/End	**closed** — Theorem 6.1
Non-central matrix projector	**open** — acknowledged residual gap (§6.2)
Singular matrix space: existence	**open** — $\mathcal{S}_d$ counterexample
Singular matrix space: witness	**closed** — witness = QR-witness = factoring (Theorem 7.3)

The only surviving candidate is forced singular witness extraction via non-central projectors or exotic matrix spaces outside the $\mathcal{S}_d$ paradigm. No natural construction achieving this is known. This constitutes a complete structural characterization of the Babai-encoding approach to semiprime factorization.

References

[**Babai 2016**] L. Babai. "Graph isomorphism in quasipolynomial time." *Proceedings of STOC 2016*, pp. 684–697. ACM. doi:10.1145/2897518.2897542

[**Goldwasser–Micali 1984**] S. Goldwasser, S. Micali. "Probabilistic encryption." *Journal of Computer and System Sciences* 28 (1984), no. 2, 270–299. doi:10.1016/0022-0000(84)90070-9

[**Kayal–Saxena 2006**] N. Kayal, N. Saxena. "Complexity of ring morphism problems." *Computational Complexity* 15 (2006), no. 4, 342–390. doi:10.1007/s00037-007-0219-8

[Kayal–Saxena 2005] N. Kayal, N. Saxena. "On the ring isomorphism and automorphism problems." *Proceedings of CCC 2005*, pp. 2–12. (Also ECCC TR04-109.)