

Noise as Structure: From Exact Algebra to Adversarial Arithmetic

Xuan-Gottfried Yang

January 31, 2026

Noise as Structure: From Exact Algebra to Adversarial Arithmetic

1 Exact inversion problems in classical cryptography

Classical public-key cryptography is governed by exact algebraic inversion problems. Typical instances include:

- discrete logarithms in finite abelian groups,
- integer factorization,
- isogeny inversion between elliptic curves.

All these problems admit the abstract form

$$f: X \longrightarrow Y, \quad \text{given } y \in Y, \text{ recover } x \in X \text{ such that } f(x) = y.$$

Here X and Y are algebraic objects and f is an algebraic morphism. Hardness is algorithmic, not structural.

Quantum algorithms (notably Shor's algorithm) show that sufficient algebraic rigidity forces these inversion problems to collapse.

2 The post-quantum shift

Post-quantum cryptography replaces exact inversion by inversion under perturbation.

Instead of

$$y = f(x),$$

one studies equations of the form

$$y = f(x) + e,$$

where e is a structured error term.

The error is not accidental; it is part of the mathematical definition of the problem.

3 Formal model

[Noisy inversion problem] Let R be a ring, M, N finitely generated R -modules, and $f: M \rightarrow N$ an R -linear map. Let $E \subset N$ be a designated subset.

Given

$$y = f(x) + e \quad \text{with } x \in M, e \in E,$$

recover x .

The set E is chosen such that:

1. inversion is no longer unique,
2. semantic information is preserved,
3. worst-case recovery is computationally infeasible.

4 Noise as deformation

Exact algebra corresponds to the degenerate case $E = \{0\}$. Post-quantum hardness arises in the intermediate regime

$$\{0\}EN.$$

This resembles deformation phenomena in arithmetic geometry. However, the deformation here is discrete, adversarial, and worst-case, rather than geometric or analytic.

5 The LWE archetype

Let $A \in R^{m \times n}$, $s \in R^n$, and $e \in E \subset R^m$. The Learning With Errors distribution is given by

$$(A, As + e).$$

Mathematically, this defines a family of affine fibers whose canonical splitting is destroyed by noise. In the presence of admissible noise, the inverse of the linear map defined by A fails to be functorial.

[Sketch] Noise introduces nontrivial equivalence classes of preimages. Any inverse depends on arbitrary choices and is unstable under composition.

6 Failure of classical invariants

Classical invariants such as rank, determinant, or Smith normal form classify linear maps over Z .

These invariants persist algebraically under noise, but lose operational meaning. This separation between algebraic classification and computational recovery does not occur in classical public-key cryptography.

7 Categorical viewpoint

One may formalize noisy problems in a category where:

- objects are modules,
- morphisms are correspondences modulo bounded error,
- composition is non-strict.

In such a category, inverses rarely exist. Hardness appears as a categorical obstruction rather than an algorithmic one.

8 Loss of geometry

Elliptic-curve-based cryptography relies on low-dimensional geometric rigidity. Post-quantum constructions instead exploit high-dimensional arithmetic roughness.

Introducing noise systematically destroys the geometric structures on which classical cryptographic hardness relies.

9 Limits of unification

Although complex tori

$$C^g/\Lambda$$

relate lattices and abelian varieties formally, their cryptographic roles diverge.

Lattice-based cryptography exploits dimension and distortion, whereas isogeny-based cryptography exploits rigidity. Any unification must confront this structural mismatch.

10 Reductions as Morphisms and Functorial Obstructions

In cryptography, reductions are often described informally as algorithmic transformations between problems. From a structural point of view, however, a reduction may be understood as a morphism between *families of instances*.

Let \mathcal{P} and \mathcal{Q} be cryptographic problems, each modeled as a family of instances parameterized by public randomness. Abstractly, we regard such a problem as a structured object

$$\mathcal{P} = (I_{\mathcal{P}}, S_{\mathcal{P}}, R_{\mathcal{P}}),$$

where $I_{\mathcal{P}}$ denotes the space of public instances, $S_{\mathcal{P}}$ the corresponding secret space, and $R_{\mathcal{P}}$ the admissible relations between them.

[Reduction as a morphism] A reduction from \mathcal{P} to \mathcal{Q} consists of maps

$$\Phi_I: I_{\mathcal{P}} \rightarrow I_{\mathcal{Q}}, \quad \Phi_S: S_{\mathcal{P}} \rightarrow S_{\mathcal{Q}},$$

compatible with the respective relations, such that solving \mathcal{Q} on $\Phi_I(i)$ yields a solution to \mathcal{P} on i .

In this formulation, a reduction is not a single algorithmic step, but a *structure-preserving transformation* between parameterized families. This perspective naturally suggests a categorical framework in which cryptographic problems form objects and reductions form morphisms.

In contrast to classical algebraic settings, these morphisms are generally neither invertible nor exact. Their failure to preserve algebraic structure reflects the presence of noise, randomness, and computational asymmetry.

This viewpoint clarifies why many reductions in post-quantum cryptography cannot be realized as homomorphisms of algebraic objects. Instead, they are obstructed by functorial incompatibilities: the reduction fails to commute with natural operations such as duality, decomposition, or base change.

[Functorial obstruction] A functorial obstruction arises when no morphism in the relevant category can simultaneously preserve the algebraic structure of instances and the distributional properties required for cryptographic hardness.

In particular, lattice-based and isogeny-based problems inhabit distinct categorical environments. Any reduction between them must necessarily break at least one layer of functoriality, explaining the absence of known structure-preserving translations between these domains.

11 Why supersingular isogeny graphs

11.1 Ordinary versus supersingular elliptic curves

Let E/F_q be an elliptic curve.

If E is ordinary, then

$$\text{End}(E) \otimes Q \cong K,$$

where K is an imaginary quadratic field. If E is supersingular and $q = p^2$, then

$$\text{End}(E) \otimes Q \cong B_{p,\infty},$$

the quaternion algebra ramified exactly at p and ∞ .

This dichotomy determines the global structure of the associated isogeny graphs.

11.2 Failure of ordinary isogeny graphs

Ordinary isogeny graphs exhibit:

- volcano structures,
- preferred directions,
- explicit class field theoretic parametrizations.

These properties permit efficient navigation and preclude cryptographic hardness.

Isogeny graphs of ordinary elliptic curves admit global algebraic coordinates.

[Sketch] The endomorphism ring embeds into a quadratic field, allowing parametrization via ideal class groups.

11.3 Supersingular isogeny graphs

For supersingular curves over F_{p^2} , the situation changes fundamentally.

- Endomorphism rings are noncommutative.
- Isogeny graphs are regular and highly connected.
- No global coordinates exist.

Supersingular ℓ -isogeny graphs over F_{p^2} are connected and exhibit strong expansion.

This expansion property is central to cryptographic security. It is absent in the ordinary case.

11.4 Categorical interpretation

Supersingular isogenies form a groupoid whose morphisms admit duals but no canonical inverses. Hardness arises from the non-functoriality of path inversion.

This explains why diagram chasing is possible only at the level of compositions and duals, but not via exact sequences or derived functors.

11.5 Exercises

Theoretical exercises

Show that the endomorphism ring of an ordinary elliptic curve over a finite field is commutative.

Let E be supersingular over F_{p^2} . Prove that $\text{End}(E) \otimes Q$ cannot be a field.

Explain why the existence of a global coordinate system on an isogeny graph would break cryptographic hardness.

Show that dual isogenies define an involution on the isogeny groupoid.

Computer exercises

[Isogeny graph exploration] Using **SageMath**, compute the ℓ -isogeny graph of supersingular elliptic curves over F_{p^2} for small p, ℓ . Visualize the graph and compare it to the ordinary case.

[Endomorphism ring experiment] Choose a supersingular elliptic curve E/F_{p^2} . Compute several isogenies and verify experimentally that their compositions fail to commute.

[Random walk mixing] Implement a random walk on a supersingular isogeny graph. Empirically study the mixing behavior and contrast it with an ordinary isogeny volcano.

[Path equivalence] Generate distinct isogeny paths with equal degree. Test whether they induce the same endomorphism up to isomorphism.

12 Conclusion

Post-quantum cryptography replaces exact algebraic inversion by adversarial arithmetic under deformation.

Noise is not a defect but the structural feature that replaces symmetry.