NUMBER THEORY

A Cryptographic Idea Hidden in Ramanujan's Last Notebooks

By PAULINA ROWIŃSKA

An unusual class of functions—once considered an isolated curiosity—may point toward a different foundation for secure communication, one that depends less on computational hardness and more on the limits of mathematical identification.

Paulina Rowińska

Contributing Writer

March 6, 2026

VIEW PDF/PRINT MODE

combinatorics geometry mathematics number theory prime numbers

All topics →

In the final year of his life, writing from his sickbed in India, Srinivasa Ramanujan filled notebooks with formulas that seemed to resist classification. He called them *mock theta functions*. He offered no formal definitions, no proofs, and no clear indication of how they fit into the existing theory of modular forms. The expressions appeared precise, yet strangely incomplete—as if they belonged to a larger mathematical structure whose full form he had glimpsed but never fully described.

For decades, mathematicians treated these functions as isolated artifacts. They were studied, cataloged, and admired, but not understood in structural terms.

Only in the early 21st century did that begin to change. Work by Sander Zwegers and Don Zagier revealed that mock theta functions are not anomalies, but fragments—holomorphic components—of a broader class of objects known as *harmonic Maass forms*. Each admits a completion: an additional, non-holomorphic term that restores a deeper symmetry.

But the completion introduces a complication.

It is not uniquely determined by what we can see.

The Part That Doesn't Determine the Whole

A mock theta function, typically written as $f(\tau)$, behaves almost like a modular form but fails to satisfy its defining symmetries. That failure can be corrected by adding a second term:

$f^*(\tau) = f(\tau) + R(\tau)$

The added component $R(\tau)$, determined by an associated "shadow," restores modular behavior. The completed function transforms cleanly. The original function can then be understood as a projection—a partial view of a more symmetric object.

What makes this construction unusual is not the existence of the completion, but its ambiguity.

The holomorphic component does not uniquely determine the completion. Different choices of shadow produce globally distinct objects that, within any finite observational window, can appear indistinguishable.

From the perspective of analysis, this reflects hidden structure—degrees of freedom invisible to local evaluation.

From the perspective of information, it implies something more striking:

The observable data does not uniquely specify the underlying identity.

A Structural Form of Uncertainty

In most mathematical settings, such ambiguity is resolved. Additional constraints are imposed, canonical representatives are chosen, or symmetry principles eliminate degeneracy.

Here, none of that applies.

The ambiguity is not provisional. It is structural.

And that has begun to draw attention beyond pure mathematics.

The Familiar Logic of Cryptography

Modern cryptography rests on a simple premise: public data uniquely determines a secret, but recovering it is computationally difficult.

This is true for factoring in RSA, discrete logarithms in elliptic curves and lattice problems in post-quantum cryptography

Even as quantum computing has challenged specific assumptions—most notably through the work of Peter Shor—the underlying framework has remained intact.

Security still depends on difficulty.

But it also depends, more fundamentally, on something rarely stated explicitly:

that the problem is uniquely defined.

When the Problem Is Not Fully Defined

Mock theta functions suggest a different possibility.

If multiple underlying structures are consistent with the same observable data, then an attacker is not trying to invert a function. They are trying to select among many valid candidates.

There is no single object to recover.

In this setting, the problem is not merely difficult. It is ill-posed.

A computational system—classical or quantum—can accelerate the solution of a well-defined problem. But it cannot resolve ambiguity that is intrinsic to the structure itself.

A System Built on Ambiguity

One effort to translate this idea into a working cryptographic framework is underway at the Ramanujan Institute in São Paulo.

Led by Marcos Eduardo Elias, an engineer and mathematician, the group has developed what they describe as a third regime of cryptographic security—one based not on computational hardness, but on what they call *controlled non-identifiability*.

Their system departs from a premise shared by nearly all public-key cryptography: that public data uniquely determines the secret.

“In existing systems, the public key fixes the secret completely,” Elias said. “Security is only about how hard it is to recover it. We remove that premise entirely.”

Instead, the system constructs *transcripts*—finite, verifiable public data structures that are compatible with many distinct private identities. The private key does not invert the public data. It selects one valid completion among many.

The resulting framework, described in a detailed technical architecture , defines cryptographic primitives such as key exchange and digital signatures in terms of identification under ambiguity rather than inversion.

From Analysis to Engineering

Turning this idea into a functioning system introduces a different set of challenges.

Mock theta functions live in a continuous, analytic setting. Cryptography operates in finite, discrete environments. The task is not simply to approximate the mathematics, but to preserve its essential feature: non-identifiability.

In practice, this means constructing finite representations—truncated series, sampled evaluations, structured constraints—that remain compatible with multiple global completions.

If the discretization process introduces artifacts that distinguish one completion from another, the system collapses back into a conventional inversion problem.

Maintaining ambiguity is therefore not a limitation. It is the central engineering requirement.

What Computation Can—and Cannot—Resolve

Quantum algorithms are powerful when a problem has exploitable structure—periodicity, algebraic symmetry, or linear relations. But they rely on the assumption that the object of interest is uniquely defined.

In systems built on controlled ambiguity, that assumption fails.

The attacker's task is no longer to compute a hidden value, but to determine which of many valid values is correct.

That shifts the problem from computation to inference.

And inference, unlike computation, depends on what information is available—not just how efficiently it can be processed.

Open Questions

The approach remains exploratory, and significant questions remain.

Can non-identifiability be formalized in a way that supports rigorous security guarantees? Could statistical or machine-learning methods extract hidden structure from large datasets? Are there invariants that distinguish different completions in ways not yet understood?

Institutions such as NIST evaluate cryptographic systems through well-defined reductions and hardness assumptions. A framework based on ambiguity does not fit naturally into that model.

Its claims are not about difficulty, but about structure.

A Different Way to Think About Secrecy

For decades, cryptography has been guided by a single intuition: Secrecy depends on problems that are easy to state but hard to solve.

RELATED:

1. Smaller Is Better: Why Finite Number Systems Pack More Punch
2. A Master of Numbers and Shapes Who Is Rewriting Arithmetic
3. The Core of Fermat's Last Theorem Just Got Superpowered

Mock theta functions suggest a complementary idea:

Secrecy may also arise when a problem cannot be uniquely stated from the data available.

In Ramanujan's notebooks, these functions appeared as fragments of something larger—objects that hinted at structure without fully revealing it. A century later, they may be pointing toward a different way of thinking about information itself.

Not everything that is hidden is hidden by complexity.

Things remain inaccessible because they are not fully determined by what we can observe.