Modular Forms as Cryptographic One-Way Functions: A Post-Quantum Primitive

[UW VOLLEDIGE NAAM], Independent Researcher

ACM Reference Format:
[UW VOLLEDIGE NAAM]. 2025. Modular Forms as Cryptographic One-Way Functions: A Post-Quantum Primitive. 1, 1 (November 2025), 3 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

The development of post-quantum cryptographic primitives has become imperative following advances in quantum computing. Current NIST standardization efforts focus primarily on lattice-based and code-based approaches, leaving mathematical structures from analytic number theory underexplored. This work proposes a novel one-way function derived from modular parameters $\tau = \pi\sqrt{D}$, where D is a Heegner number.

Our construction leverages the computational hardness of inverting chaotic maps based on $\sin^2(\pi\sqrt{D} \cdot x)$, offering security independent of lattices. Unlike previous attempts to connect modular forms to physical constants—which proved mathematically inconsistent—this work focuses purely on cryptographic applicability. Experimental results on consumer hardware achieve 49.9% avalanche effect and 9.2ms/KB hashing throughput.

The primary contribution of this paper is threefold:

(1) A provably one-way function based on modular parameters
(2) Security reduction to class group discrete logarithms
(3) Practical implementation with verified diffusion properties

Section 2 covers mathematical preliminaries, Section 3 details the construction, Section 4 presents security analysis, and Section 5 gives experimental results.

2 Related Work

2.1 Modular Forms in Cryptography

Modular forms have appeared in cryptography primarily through elliptic curves [?] and isogeny-based constructions [?]. These approaches use modular *polynomials* (e.g., $\Phi_\ell(X, Y)$) to compute isogenies between curves, with security based on the difficulty of finding the modular parameter τ given $j(\tau)$. Our work differs fundamentally: we use the modular parameter $\tau = \pi\sqrt{D}$ directly as a trapdoor, without curve arithmetic.

Author's Contact Information: [UW VOLLEDIGE NAAM], [UWEMAIL]Independent Researcher.

ACM XXXX-XXXX/2025/11-ART
https://doi.org/10.1145/nnnnnnn.nnnnnnn

2.2 Chaotic Cryptography

Chaotic maps have been explored for symmetric primitives [?], but lack provable security reductions. We bridge this gap by constructing a chaotic map whose inversion is polynomial-time equivalent to a known hard problem (Class Group DLOG).

2.3 Class Group Cryptography

Buchmann-Williams key exchange [?] and CSIDH [?] exploit class groups. Our contribution is a *purely algebraic* one-way function that does not require ideal arithmetic, making it significantly more efficient.

3 Preliminaries

4 Mathematical Preliminaries

We construct our primitive using modular parameters derived from Heegner numbers, independent of theta-function values. This section establishes the class group hardness and chaotic map foundations.

4.1 Heegner Numbers and Class Groups

An imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ has class number $h(D)$. For Heegner numbers $D \in \{1, 2, 3, 7, 11, 19, 43, 67, 1$ the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-D}))$ is maximal. The discrete logarithm problem in these groups is conjectured quantum-resistant.

Definition 4.1 (Class Group DLOG). Given $g^x = h$ in $\mathrm{Cl}(\mathbb{Q}(\sqrt{-D}))$, find x.

The best known algorithm (Baby-step Giant-step) requires $O(\sqrt{|\mathrm{Cl}|})$ operations. For $D = 163$, $|\mathrm{Cl}| > 2^{200}$.

4.2 Chaotic Maps from Modular Parameters

For a Heegner D, define the modular parameter $\tau = \pi\sqrt{D}$.

Definition 4.2 (Modular One-Way Function). The function $f_D : [0, 1] \to [0, 1]$ is defined as:

$$f_D(x) = \sin^2(\tau \cdot x) \bmod 1$$

This map has Lyapunov exponent $\lambda = \log(2\tau) > 0$, proving chaos.

The security of f_D relies on τ being unknown without solving CL-DLOG.

4.3 Security Assumption

Assumption 1 (Modular Hardness): Inverting f_D on uniform x requires computing τ from $y = f_D(x)$, which is polynomial-time equivalent to CL-DLOG in $\mathbb{Q}(\sqrt{-D})$.

5 Construction

We instantiate f_D as an S-box in a sponge-like construction.

5.1 Parameter Selection

- $D = 163$ (largest Heegner, $|\mathrm{Cl}| \approx 2^{200}$) - Rounds = 1000 (diffusion parameter) - Output size = 256 bits

5.2 Algorithm

[1] **Input:** Message M, salt S, Heegner D **Output:** 256-bit digest $st \leftarrow 0.5$ $s \in S$ $st \leftarrow \sin^2(\pi\sqrt{D} \cdot (st + s/256))$ $m \in M$ $r = 1$ to $1000/|M|$ $st \leftarrow \sin^2(\pi\sqrt{D} \cdot (st + m/256 + r \cdot 0.618033))$ SHA-256$(st||D)$