Dual-Curve Trapdoor Cryptography: A Novel Intersection-Based Hashing Scheme

AJAY CP

April 6, 2025

Abstract

This paper introduces a novel cryptographic concept that leverages the intersection of two mathematical curves to generate secure cryptographic outputs. The approach modifies traditional elliptic curve cryptography by introducing a secondary curve and utilizing the coordinates of their intersection, when approached via scalar multiplication from a random generator point. The resulting intersection coordinates are hashed using SHA-256, producing a unique and secure cryptographic hash.

1 Introduction

Elliptic Curve Cryptography (ECC) has become a cornerstone of modern cryptographic systems due to its efficiency and high level of security relative to key size. This proposal seeks to expand upon the ECC paradigm by introducing a second mathematical function or graph into the cryptographic process. This additional layer of complexity creates a new kind of cryptographic trapdoor function, one based on geometric interaction rather than purely algebraic relations.

2 Concept Overview

The core idea involves:

1. Selecting a primary elliptic curve:
$$E : y^2 = x^3 + ax + b$$
2. Selecting a secondary curve (arbitrary), such as:
   - $y = \sin(x)$
   - $y = \log(x)$
   - Another elliptic curve $y^2 = x^3 + cx + d$
3. Choosing a random generator point $G \in E$
4. Performing scalar multiplication:
$$P = k \cdot G$$
5. Observing when P intersects the secondary graph
6. Hashing the coordinates of that point with SHA-256:
$$H = \text{SHA-256}(x_P, y_P)$$

This process creates a cryptographic value based on both the algebraic properties of the elliptic curve and the geometric alignment with a second graph.

3 Visual Representation

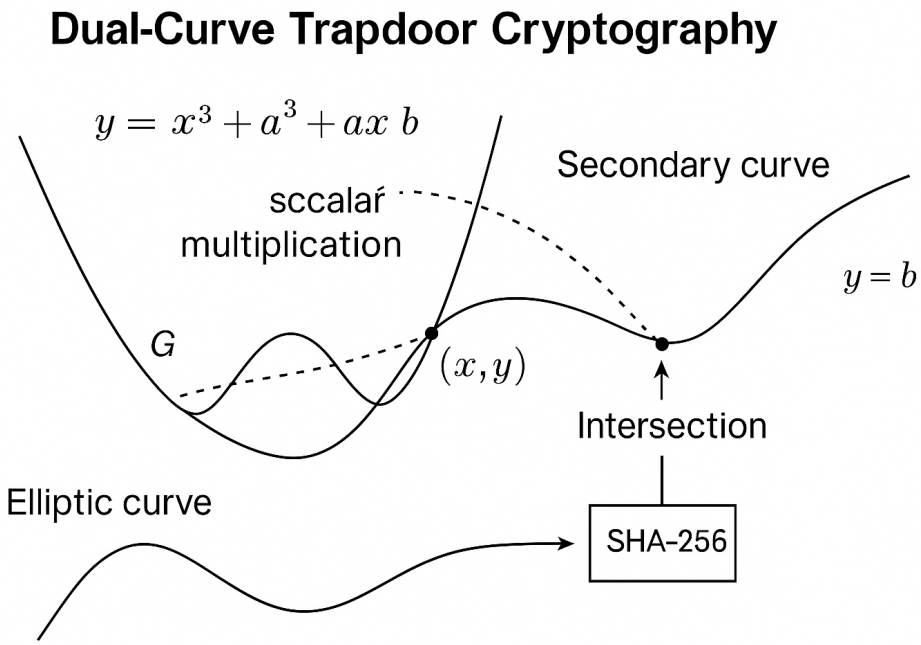

Figure 1: A scalar walk across an elliptic curve intersecting a secondary graph (e.g., sine wave). The intersection coordinates are hashed using SHA-256.

4 Security Implications

- **ECDLP Hardness Preserved:** The use of scalar multiplication retains the hardness of the Elliptic Curve Discrete Logarithm Problem.
- **Increased Entropy:** Random generator point selection and secondary curve behavior introduce unpredictability.
- **Trapdoor Design:** Only entities knowing the correct generator point and curves can recreate the correct hash.
- **Resistance to Brute Force:** The search space is vastly increased due to the dual-curve requirement.

5 Potential Applications

- Advanced Key Derivation Functions (KDFs)
- Novel Proof-of-Work Schemes
- Secure Hash-Based Message Authentication
- Decentralized Identity Systems with Custom Curve Logic

6 Future Work

- Formal mathematical modeling of intersection frequency and randomness.
- Exploration of finite-field adaptations.
- Development of a protocol or API around this method.
- Security analysis under quantum computing assumptions.

7 Conclusion

This document outlines a novel approach to cryptography that blends scalar multiplication with geometric intersection to produce unpredictable and secure hash values. It represents a new direction for cryptographic exploration, potentially offering strong resistance to future cryptographic threats.