



Background: The deployment of elliptic curve cryptosystems is gaining speed and popularity especially in the wireless arena.

Objective: Investigate critical issues concerning foundational security of elliptic curve cryptography.

Approach: A unified approach using the theory of global duality is developed to study the discrete-log problem that lies at the heart of discrete-log based cryptosystems including ECC.



Approach and Impact

New approach

- A unified framework using global duality
- Signature calculus generalizing classical index calculus

Research Impact

- Provide evidence for the relative hardness of elliptic curve discrete-log compared to discrete-log over finite fields
- Relate foundational security of d-log based cryptography to arithmetic duality theory

Discrete logarithm problem is the basis of many public-key cryptosystems used today. We develop a unified framework for studying the discrete logarithm problem in abelian algebraic groups over finite fields. This is done by lifting the group to an algebraic number field and using global duality. Two of the most important examples of finite abelian groups that are used in public-key cryptography are the multiplicative group of a finite field and the group of points on an elliptic curve over a finite field.

Results:

(1) Develop *Signature calculus method*, which generalizes and refines the index calculus

method, and relates the discrete logarithm problem to some well-known problems in algebraic number theory and arithmetic geometry.

(3) Address an important aspect of index calculus for elliptic curve discrete-log, namely, the plausibility of leveraging small primes to tackle a computational problem that involves large primes.