

# **Beyond Elliptic Curve Cryptosystems**

**Andreas Stein  
ICCIP**

University of Illinois, Urbana-Champaign

2000 Fall CEPS Conference,  
Urbana-Champaign

# Outline

- Motivation
- Hyperelliptic Curves (HCC)
- Koblitz Curves
- Superelliptic Curves
- Abelian Varieties (AVC)
- NTRU
- NICE
- XTR ?

## Why searching beyond ECC?

- Create **alternatives** to conventional public-key cryptosystems. Ideally, find systems whose security relies on different mathematical problems.
- Improve and speed up existing schemes.
- Investigate hyperelliptic curves or, more generally, algebraic curves to obtain results on **elliptic curves**.  
(e.g. **Weil descent**, Frey et. al.)
- Explore **interactions** with other areas: computational, algorithmic, and analytic number theory; algebraic geometry; applications to coding theory.

# Hyperelliptic Curves

(Koblitz 1989)

A hyperelliptic curve  $C$  of genus  $g$

$$C : y^2 + h(x)y = f(x) = x^{2g+1} + \dots$$

$h(x), f(x) \in \mathbb{F}_{q^n}[x]$ ,  $\deg h \leq g$ ,  $C$  nonsingular

- **Jacobian Group**  $J(\mathbb{F}_{q^n})$  of  $C$  is of size

$$J(\mathbb{F}_{q^n}) \sim q^{ng}$$

- Elements of  $J(\mathbb{F}_{q^n})$  are represented by two polynomials

$$D = [a(x), b(x)]; a(x), b(x) \in \mathbb{F}_{q^n}[x],$$

$\deg b < \deg a \leq g$  and  $a(x)$  monic.

- Arithmetic of reduced divisors in  $J(\mathbb{F}_{q^n})$ .  
(Cantor)

**Plus:** Hyperelliptic curves of genus 2, 3, (4)

- There exists an effective arithmetic over smaller finite fields.
- Same level of security as elliptic curves with parameters of the same size!
- The HCDLP appears to be difficult. Thus, the **strength-per-key-bit** is substantially greater than in conventional discrete logarithm and integer factoring systems.

**Minus:**

- Slower arithmetic than for elliptic curves.
- Computing the order  $\#J(\mathbb{F}_{q^n})$  of the Jacobian of hyperelliptic curves seems to be difficult. (Avoid **Pohlig-Hellman** attack!)

## Koblitz Curves

(Günther, Lange, Stein 2000)

$$C : y^2 + h(x)y = f(x) = x^{2g+1} + \dots$$

$h(x), f(x) \in \mathbb{F}_q[x]$ . Consider  $C$  over  $\mathbb{F}_{q^n}$ .

**Example:**  $C : y^2 + xy = x^5 + x^2 + 1$ ,  
hyperelliptic curve of genus 2 over  $\mathbb{F}_2$

### Advantages

- Computing  $\#J(\mathbb{F}_{q^n})$  is easy
- Arithmetic can be sped up considerably

### Disadvantages

- They might be weaker than random products.

## Superelliptic Curves

(Galbraith, Paulus, Smart 1999)

$$C : y^n = f(x) = x^l + \dots$$

where  $f(x) \in \mathbb{F}_{q^n}[x]$ ,  $\gcd(n, l) = 1 = \gcd(n, q)$ .

**Plus:** Superelliptic curves of genus 2, 3, (4)

- Effective ideal arithmetic in the divisor class group of  $C$  with LLL-type techniques.
- Same level of security as elliptic curves with parameters of the same size!

**Minus:**

- Slower arithmetic than for elliptic and hyperelliptic curves.
- Computing the order of the key space seems to be difficult. (**Pohlig-Hellman**)

## Purely Cubic Curves

(Bauer, Scheidler, Stein 2000)

$$C : y^3 = f(x) = x^l + \dots$$

- Cubic curves of genus 2, 3, (4) offer the same level of security as elliptic curves with parameters of the same size!
- The arithmetic of superelliptic cubic curves can be sped up considerably by using explicit techniques.
- The arithmetic of cubic curves of **unit rank** 1 can be sped up by making use of Voronoi's algorithm and **baby step** ideas.
- Still slower arithmetic than for elliptic and hyperelliptic curves.
- These curves are currently investigated for use in efficient implementations.

## **Abelian Varieties (AVC)**

(Frey, Murty 1998/1999)

### **Plus:**

- “Sufficiently” effective arithmetic of higher-dimensional objects.
- If the dimension is “small”, they offer the same level of security as elliptic curves with parameters of the same size!

### **Minus:**

- Abstract arithmetic is far slower than elliptic and hyperelliptic curve arithmetic except in some special curves.
- Computing the order of the key space seems to be very difficult.

## NTRU

(Hoffstein, Pipher, Silverman 1998)

**Plus:** With “current” parameter choice

- Very fast encryption and decryption time. Complexity is of order  $N^2$  for keys of size  $N$ . (RSA, El Gamal, ECC require  $N^3$ .)
- Arithmetic involves the manipulation of very small numbers.
- Security is based on the problem of finding sufficiently “short” vectors in a lattice, and **not** on DLP or integer factorization.

**Minus:**

- Broken in the first version. Really secure parameter choice is not yet known.

## **XTR**

(Lenstra, Verheul 2000)

- Idea of the digital signature scheme.
- Security is based on the DLP in  $\mathbb{F}_{q^6}$ , but the arithmetic is performed in  $\mathbb{F}_{q^2}$  via the trace function.
- Performance is comparable to random elliptic curves over prime fields.

## **NICE**

(Hartmann, Paulus, Takagi 1999)

- Ideal arithmetic in quadratic number fields. With proper parameter choice comparable to RSA.
- Security is based on the DLP in quadratic orders which is at least as difficult as factoring.