CERIAS

the center for education and research in information assurance and security

Explicit formulas for real hyperelliptic curves of genus 2 in affine representation

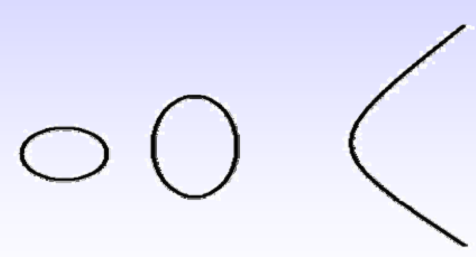
S. Erickson[1], M.J. Jacobson, Jr.[2], N. Shang[3], S. Shen[3], A. Stein[4]
Colorado College[1], Univ. of Calgary[2], Purdue University[3], Univ. of Wyoming[4]

Motivation

- To extend elliptic curve based cryptographic protocols and cryptosystems
- To find faster arithmetic to compete with elliptic curves and imaginary hyperelliptic curves while obtaining the same security level

Real hyperelliptic curve of genus 2 over finite fields *GF(q)*

C: $y^2+h(x)y=f(x)$



- $y^2+h(x)y-f(x)$ absolutely irreducible, non-singular
- If q odd: $f(x)$ monic, $deg(f)=6$, $h(x)=0$
- If q even: $h(x)$ monic, $deg(h)=3$, either $deg(f)<6$ or $deg(f)=6$ and $f(x)$ has leading coefficient of form e^2+e for some $e \in GF(q)$*

Diffie-Hellman Key Exchange with real hyperelliptic curves

- Key space: subset of reduced principal ideals in the ring of regular function of C with infrastructure; one-to-one correspondence to a subset of divisor class groups of C
- Mumford representation and Cantor's algorithm
- Main steps of divisor arithmetic:

  - giant step: divisor/ideal composition and reduction
  - baby step: output adjustment

Explicit Formulas Developed

- Baby step
- Divisor addition
- Divisor doubling

Comparison of operation counts for explicit formulas

Notation for operations in finite fields:
I: inversion, S: squaring, M: multiplication

	Imaginary	**Real**
Baby Step	NA	1I, 2S, 4M
Addition	1I, 2S, 22M	1I, 2S, 26M
Doubling	1I, 5S, 22M	1I, 4S, 28M

Experimental result

Scalar multiplication and key exchange timings over GF(q) (in seconds)

Security Level (Bits)	**Imag**	**Fixed**	**Var**	**DH Imag**	**DH Real**
80	0.0048	0.0050	0.0056	0.0097	0.0106
112	0.0083	0.0085	0.0096	0.0166	0.0180
128	0.0103	0.0106	0.0117	0.0206	0.0223
192	0.0220	0.0230	0.0256	0.0442	0.0485
256	0.0403	0.0411	0.0452	0.0806	0.0863

PURDUE UNIVERSITY

CERIAS

Discovery Park
e-Enterprise Center