Ed448-Goldilocks

A new high-strength curve and implementation

Mike Hamburg
Rambus Cryptography Research

Goal

- Design a modern high-strength curve
- Complete formulas, constant time
- Better performance than NIST P-384, P-521
- One curve — no “overkill” and “more overkill” levels

Desiderata

- “Overkill”: ~384+ bit field size
- Good tradeoff of size vs performance
- Simple implementation
- Implementation flexibility, good on multiple arch’s
- Conservative: prime field, no endomorphisms
- Safecurves criteria

Prime choice: $2^{448} - 2^{224} - 1$

- Best performance for its size on many platforms
- Best Solinas prime shape
- Vectorizable: 448 = 16x28 = 8x56
- Fast Karatsuba multiplication
- Designed for 32- and 64-bit
    - On 64-bit, could use $2^{480} - 2^{240} - 1$

Ed448-Goldilocks

$$y^2 + x^2 = 1 - 39081x^2y^2$$

- Minimum |d| with 4q curve and 4q’ twist
- Order 4q, q just under 2^{446}

Implementation

http://sourceforge.net/p/ed448goldilocks/code/ci/decaf/tree/

- x86-64, ARM32 scalar, ARM NEON, generic 32/64
- C and asm
- Constant-time (except verify)
- Control and indexing don’t depend on secrets
- Complete formulas using extended coords

Implementation

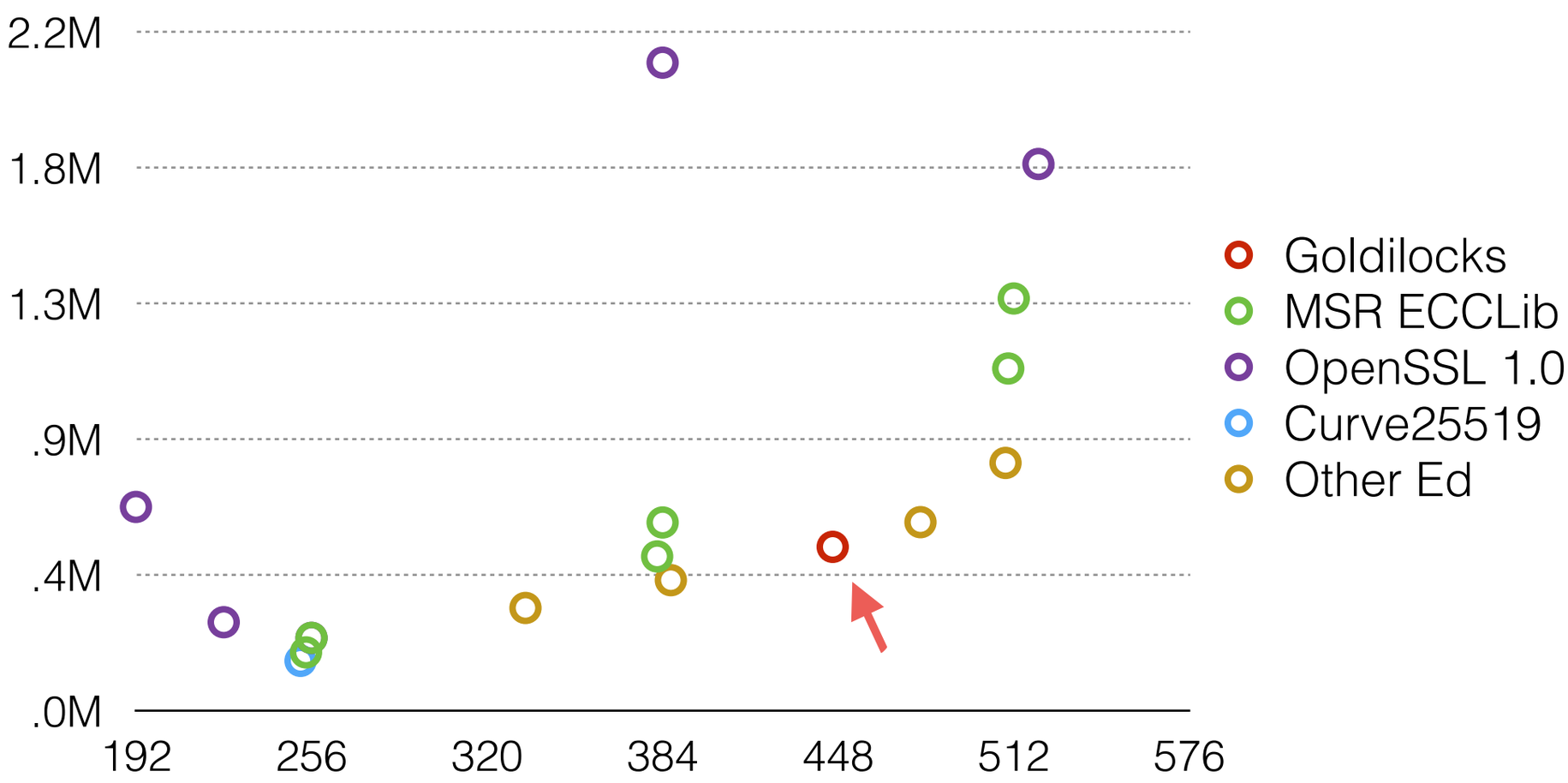
http://sourceforge.net/p/ed448goldilocks/code/ci/decaf/tree/

- Example crypto: Schnorr, ECDH/3DH, MQV, PAKE
- Hash to curve, steg encoding with Elligator 2
- C library with C++ wrapper

“Decaf” point compression

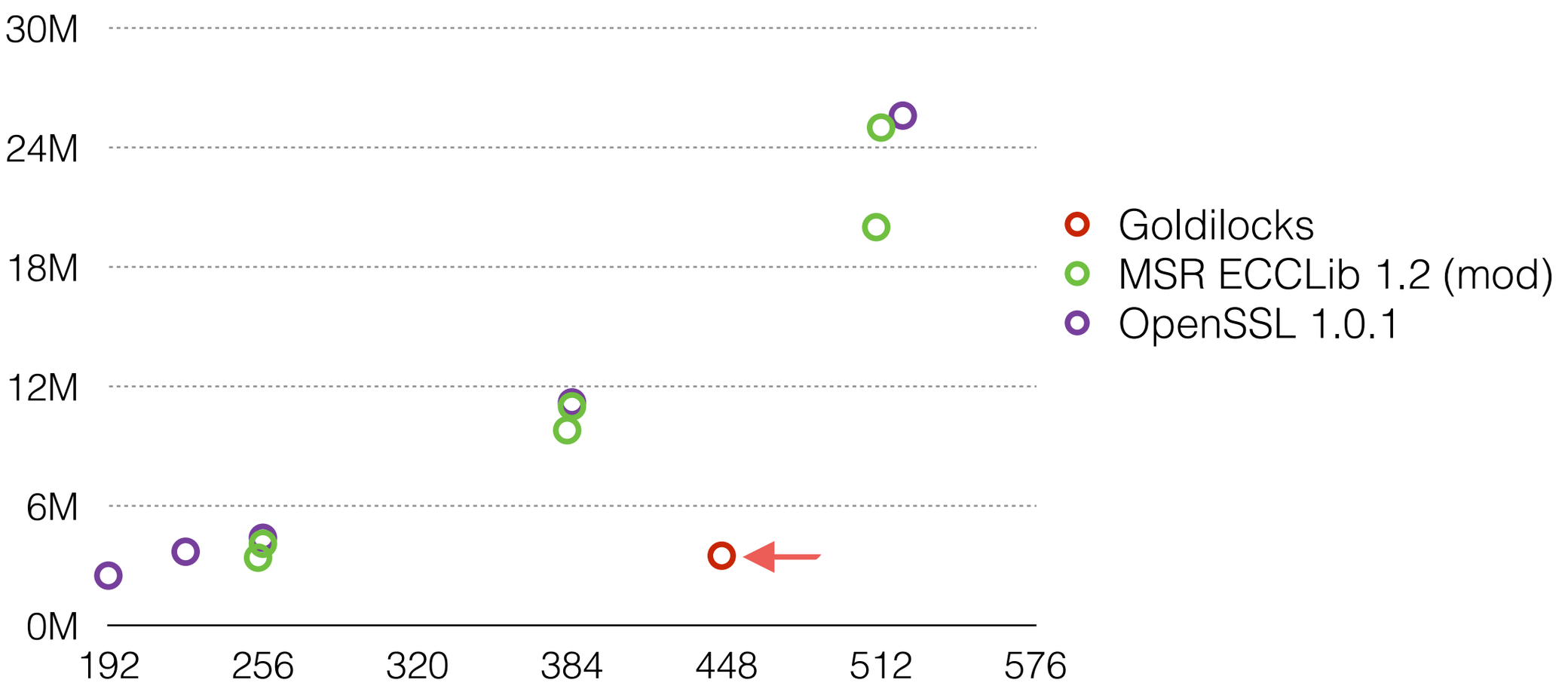
- Remove cofactor of 4 with subgroup/quotient
- Transparently use isogenous curves
  - Remove points at infinity on twisted curve
  - Compatible with Montgomery ladder
- Performs the same as other point compression
- CRYPTO 2015

Performance – Intel



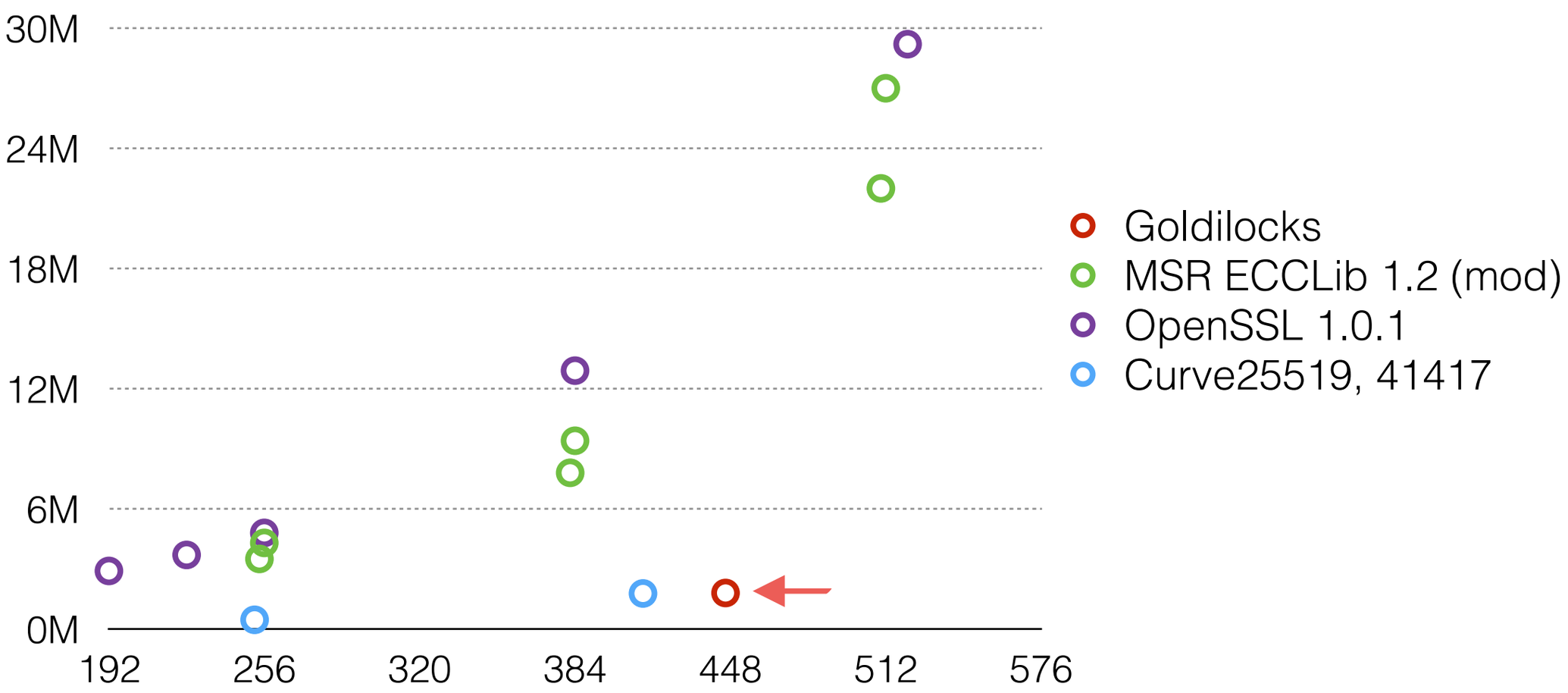
ECDH, Haswell cycles

Performance – ARM



ECDH, Cortex-A9 cycles

Performance – NEON



ECDH, Cortex-A8 cycles

Conclusion

- Goldilocks has conservative design
- Edwards replacement for NIST “overkill” curves
- Fast on many platforms
- Featureful implementation
- Selected by CFRG for TLS
- Good choice for NIST standardization

Questions?