

Innovation and Technology Fund (ITF) - Tier 3

Elliptic Curve Scalar Multiplier (ECSM) IP Core

Demonstration

Project Investigator: **Prof. Xiaotie Deng** (Deputy Project Coordinator)

Project Coordinator: **Dr. Duncan S. Wong**

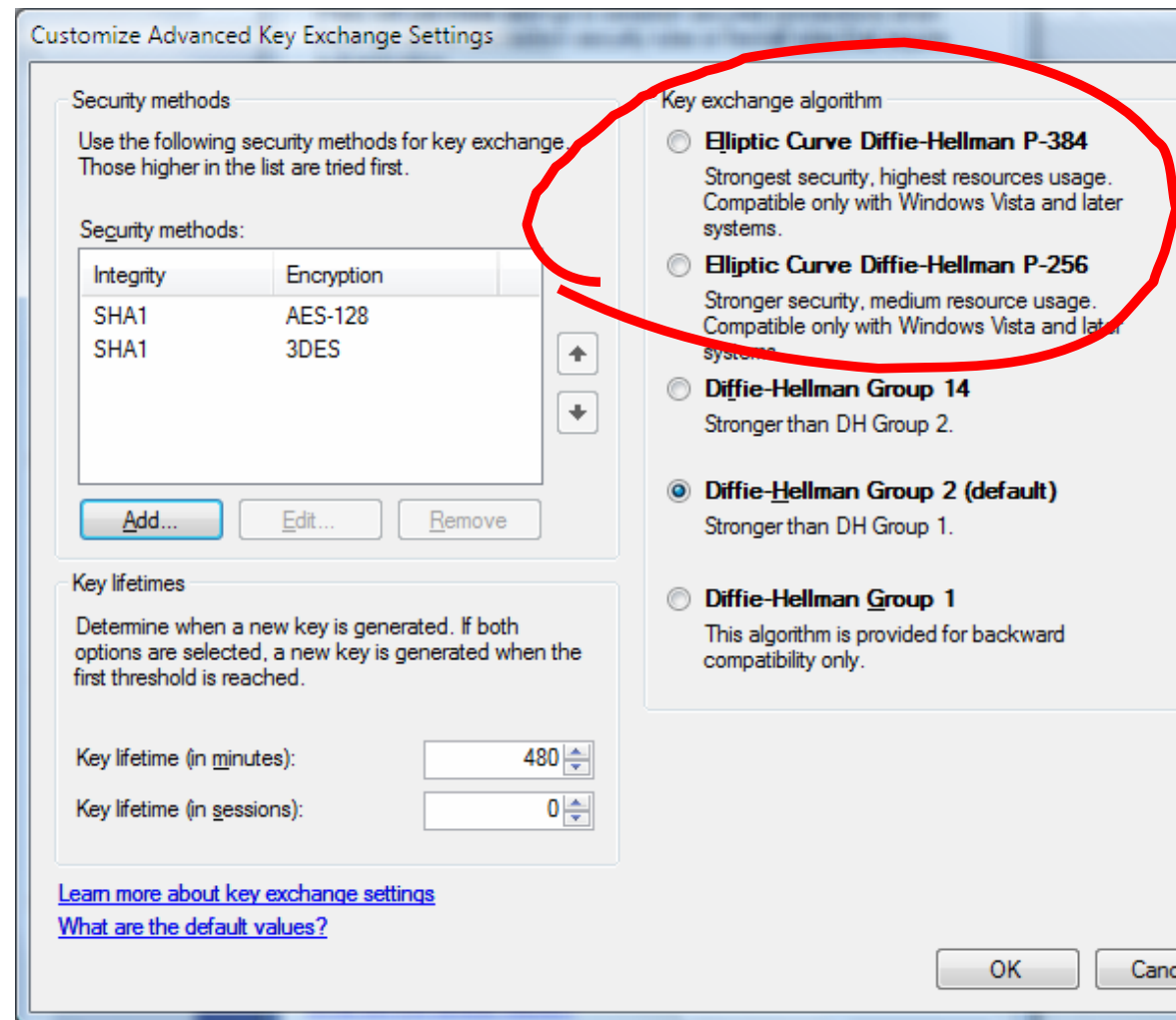
Principal Applicant Organization: **City University of Hong Kong**

Sponsoring Organization: **HXBC Technology Co., Ltd**

<http://www.cs.cityu.edu.hk/~ecc>

Recent Deployments of ECC and Bilinear Pairings

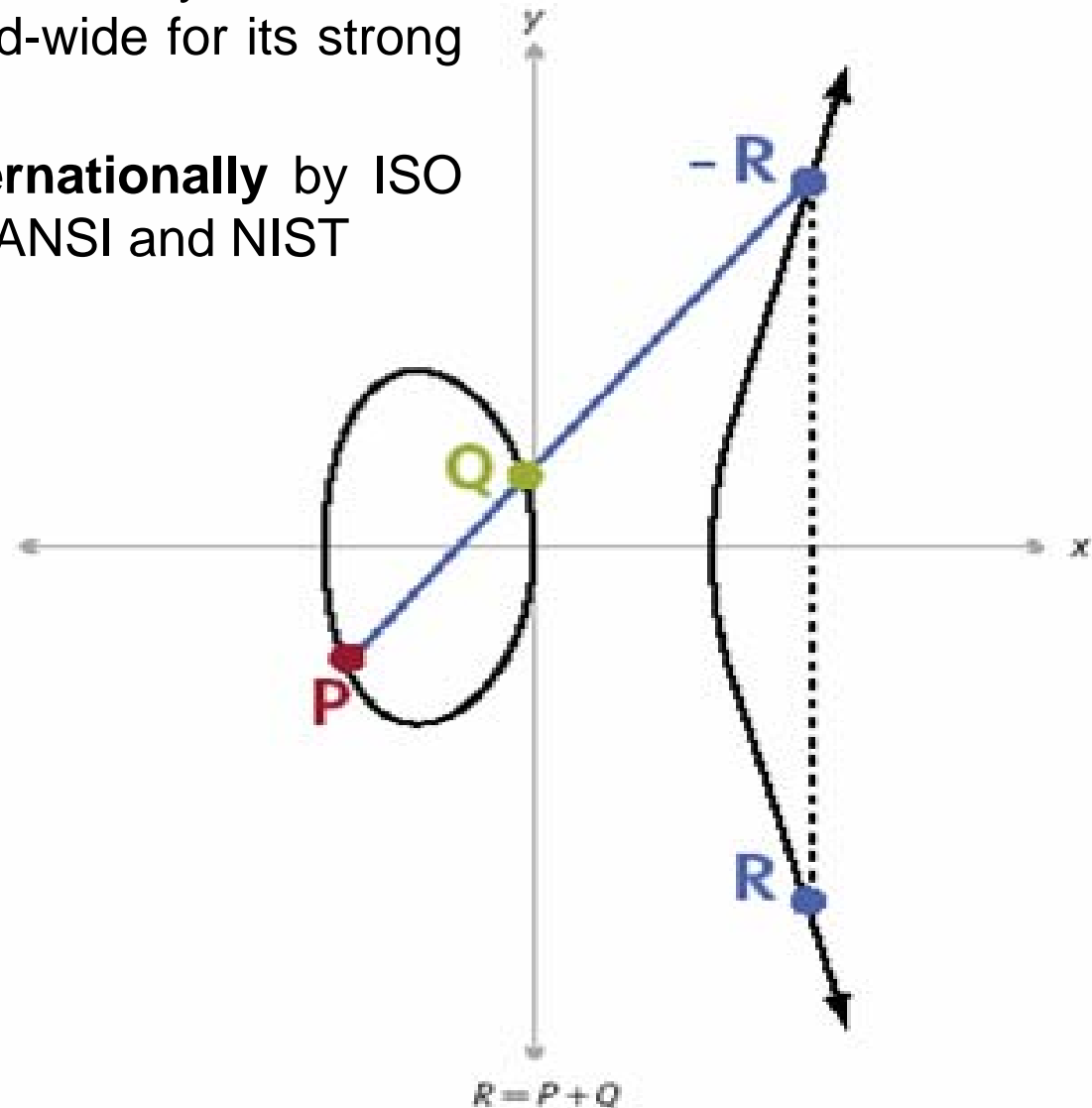
- Microsoft implemented ECC based key exchange algorithms in Windows Vista.
- Philips Electronics uses ECC Authentication in DisplayPort, a new digital display interface standard for Content Protection.
- Motorola implemented ECC in their mobile devices.
- US Government, NATO and some in Financial sector are adopting **Suite-B** (an ECC based set of cryptographic algorithms) – NSA announced Suite-B at RSA Conference 2005.
 - for classified applications up through **Top Secret**
- Three components in Suite-B:
 - **ECC**
 - **AES**
 - **SHA-2**



Introduction to ECC

- Invented by Neil Koblitz and Victor Miller in 1985, eight years after RSA
- ECC has been studied extensively for 20+ years and is well recognized and accepted world-wide for its strong number-theoretic foundation.
- ECC has been **standardized internationally** by ISO and the IETF and within the US by ANSI and NIST

- Point multiplication $Q=kP$
- Repeated point addition and doubling:
 $9P=2(2(2P)) + P$
- Public key operation: $Q(x,y) = kP(x,y)$
 Q = public key
 P = base point (curve parameter)
 k = private key
 n = order of P
- Elliptic curve discrete logarithm
Given public key kP , find private key k
- Best known attack: Pollard's rho method with running time: $\frac{(\pi n)^{1/2}}{2}$



Introduction to ECC

- NIST has defined several sets of curves, the most important of which are generated by the equations of the form

$$Y^2 = x^3 - 3x + b \text{ modulo } p$$

- Three curves in $GF(p)$ are particularly important:
 - P-256, with a 256-bit key, equivalent to AES-128
 - P-384, with a 384-bit key, equivalent to AES-192
 - P-512, with a 512-bit key, equivalent to AES-256

Performance

- ECC is much stronger **per bit** than RSA and is less computationally intensive
 - P-163 is equivalent to RSA-1024, equivalent to 80-bit symmetric key
 - P-256 is equivalent to RSA-3,072
 - P-384 is equivalent to RSA-7,680
 - P-521 is equivalent to RSA-15,380
- The performance of ECC is also proportional to the cube of the key size, but the keys are much smaller and more efficient in strength.

ECC Algorithms

- ECDSA (FIPS 186-3) is the elliptic curve equivalent of the DSA signature algorithm and is standardized in FIPS 186-2
- EC Diffie-Hellman (NIST SP 800-56A) is a key exchange algorithm
- ECMQV (NIST SP 800-56A) is another, stronger, key exchange algorithm (patented by Certicom)
- ECIES is an ECC encryption algorithm that is standardized by ISO, but has been rejected by NIST

AES and SHA-2

- AES-128 is significantly faster and stronger than triple-DES
- SHA-256/384/512 (FIPS 180-2) hash functions are much stronger than SHA-1, although somewhat slower

Customize Advanced Key Exchange Settings

Security methods

Use the following security methods for key exchange. Those higher in the list are tried first.

Security methods:

Integrity	Encryption
SHA1	AES-128
SHA1	3DES

Key exchange algorithm

- Elliptic Curve Diffie-Hellman P-384
Strongest security, highest resources usage. Compatible only with Windows Vista and later systems.
- Elliptic Curve Diffie-Hellman P-256
Stronger security, medium resource usage. Compatible only with Windows Vista and later systems.
- Diffie-Hellman Group 14
Stronger than DH Group 2.
- Diffie-Hellman Group 2 (default)
Stronger than DH Group 1.
- Diffie-Hellman Group 1
This algorithm is provided for backward compatibility only.

Key lifetimes

Determine when a new key is generated. If both options are selected, a new key is generated when the first threshold is reached.

Key lifetime (in minutes): 480

Key lifetime (in sessions): 0

[Learn more about key exchange settings](#)

[What are the default values?](#)

Performance Comparison Between ECC and RSA

- **ECC** vs. RSA

- **Security**

The security level of ECC on $GF(2^{163})$ is commonly considered to be comparable with 1024-bit RSA^[1]

- **Efficiency**

	Comparable security	Comparable operation	Time	Memory
ECC	163-bit	Scalar multiplication	1.05 ms	76KB
RSA	1024-bit	Modular exponentiation	13.33 ms	64KB

- *MIRACL*: a well-known multiple-precision arithmetic C/C++ library, running on 3GHz Pentium IV
- ECC is at least 12 times faster than RSA
- Both ECC and RSA require very little memory for storing their executables (compiled using VC6.0 on Win32) – contributor: *Xiaokang Xiong*

[1] Standards of Efficient Cryptography (SEC) 1: Elliptic Curve Cryptography, Certicom Research, Version 1.5, Feb 18, 2005

Previous Results

Performance of ECC Scalar Multiplication

Software Implementation:

- **1.05ms** over $GF(2^{163})$
- 3GHz Pentium IV
- MIRACL: a well-known multiple-precision arithmetic C/C++ library

Hardware Implementation:

- **41 μ s** over $GF(2^{163})$
- Xilinx Virtex-2 XCV2000 FPGA, with max achievable freq: **100MHz**
- B. Ansari, M. Anwar Hasan, High Performance Architecture of Elliptic Curve Scalar Multiplication, . CACR Research Report 2006-01, 2006

Our Result

- *at least 26% improvement in speed to the previous result*

Finite Field: $GF(2^{163})$

Irreducible Polynomial: $f(x)=x^{163}+x^7+x^6+x^3+1$

Elliptic Curve: sect163r1

Device: 4vlx200ff1513-11 (Xilinx Virtex-4 LX200 FPGA)

Software Version: ISE, 9.1i

Performance

Cycles: **8097**

Time: **32.3 μ s**

Min Period: **3.991ns**

Max Achievable Freq: **250.564MHz**

Device Utilization summary

Available

Occupied Slices: **38,753** (43%)

89,088

4 input LUTs: **72,147** (40%)

178,176

Flip Flops: **25,848** (15%)

178,176

Bonded IOBs: **819** (85%)

960

Equivalent ASIC Gates: **650,420**

Power Consumption: **1.469W**

Demonstration

- **ECIES (Elliptic Curve Integrated Encryption Scheme)**
 - an ECC encryption algorithm specified in ANSI X9.63 and the IEEE P1363a Draft
 - Included in Suite-B (a de facto standard for data encryption and authentication)
 - Combines elliptic curve asymmetric encryption, a block cipher (e.g. AES) and a message authentication algorithm
 - To provide data confidentiality and message authentication

P: a point generator on an elliptic curve E over $GF(2^{163})$

Q: a public key where $Q = xP$ and x is the private key

M: plaintext

Encryption

1. Randomly generate a 163-bit integer r
2. Compute $K = rQ$. (use K_x to represent the x-coordinate of K)
3. Compute $c = m \oplus K$
4. Compute $R = rP$
5. Set ciphertext to (c, R)

Decryption

1. Compute $K = xR$
2. Compute $c \oplus K$

Demonstration

- The core technology of ECIES
- Simplified for ease of illustration