타원곡선 암호 및 응용

세종사이버대학교

박영호

2021.06.14

한성대학교
HANSUNG UNIVERSITY

세종사이버대학교

0 목차

I 타원곡선 암호 소개

II 타원곡선암호 구현 및 응용

1 타원곡선 암호 소개

1) 타원곡선암호(Elliptic Curve Cryptosystem)

- 타원곡선 암호란?
  - 타원곡선 위의 타원곡선군에 대한 이산대수문제를 기반으로 한 공개키 암호
  - 1985년 Koblitz와 Miller에 의해 독립적으로 제안

- 타원곡선 암호의 장점
  - 작은 키 크기(메모리, 전력 측면에서 우수)
  - 빠른 속도
  - 높은 안전성 : 해독에 지수승 시간이 걸림
  - 응용 분야: 키 교환, 서명, 인증, 암호화

- 타원곡선 암호의 단점
  - 구현의 어려움(or 복잡함) (유한체 이론 및 정수론에 기반)

1) 타원곡선암호(Elliptic Curve Cryptosystem)

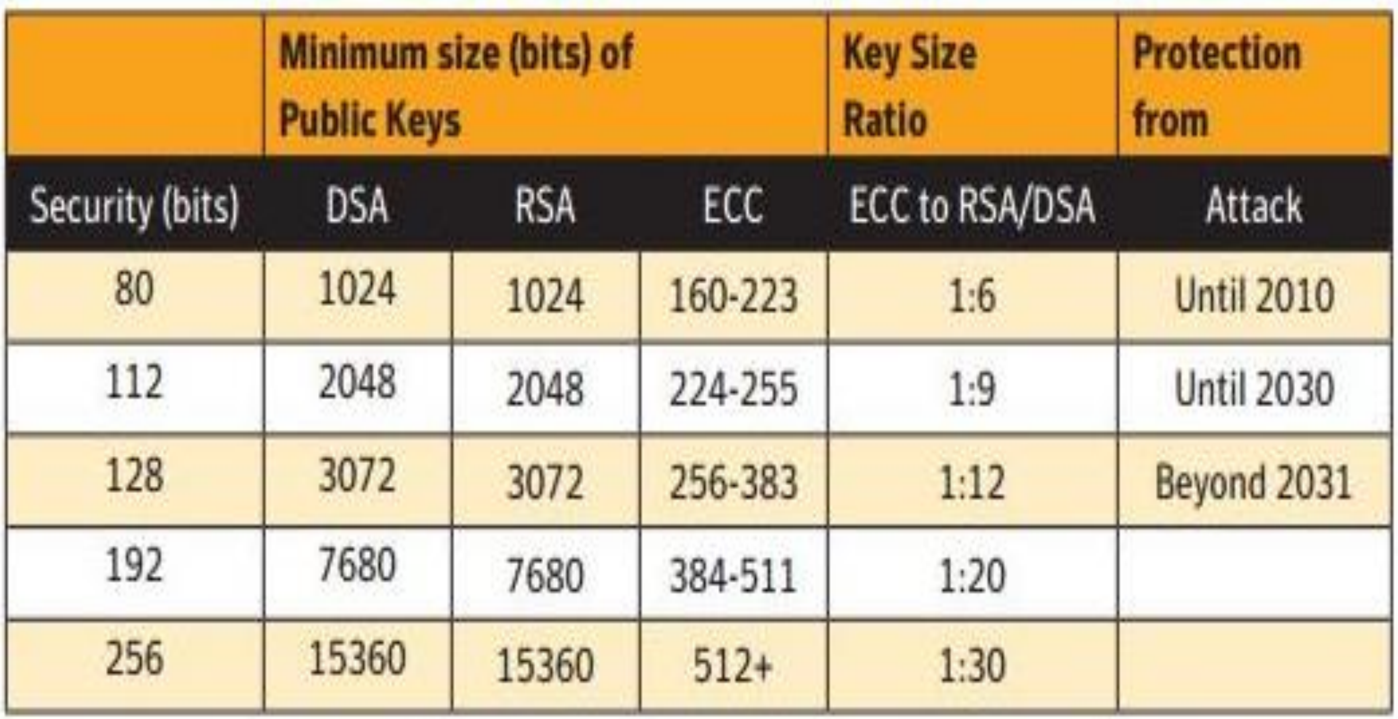
ECC is particularly beneficial for applications where:

장점

- **Computational power is limited**
  (smart cards, wireless devices, smart phone, PC Cards)
- **Integrated circuit space is limited**
  (smart cards, wireless devices, PC Cards)
- **Bandwidth is limited**
  (wireless communications)
- **Intensive use of signing & authenticating is required**
  (electronic commerce)

1) 타원곡선암호(Elliptic Curve Cryptosystem)

보안강도에 따른 공개키 암호 알고리즘 분류



	Minimum size (bits) of Public Keys			Key Size Ratio	Protection from
Security (bits)	DSA	RSA	ECC	ECC to RSA/DSA	Attack
80	1024	1024	160-223	1:6	Until 2010
112	2048	2048	224-255	1:9	Until 2030
128	3072	3072	256-383	1:12	Beyond 2031
192	7680	7680	384-511	1:20	
256	15360	15360	512+	1:30	

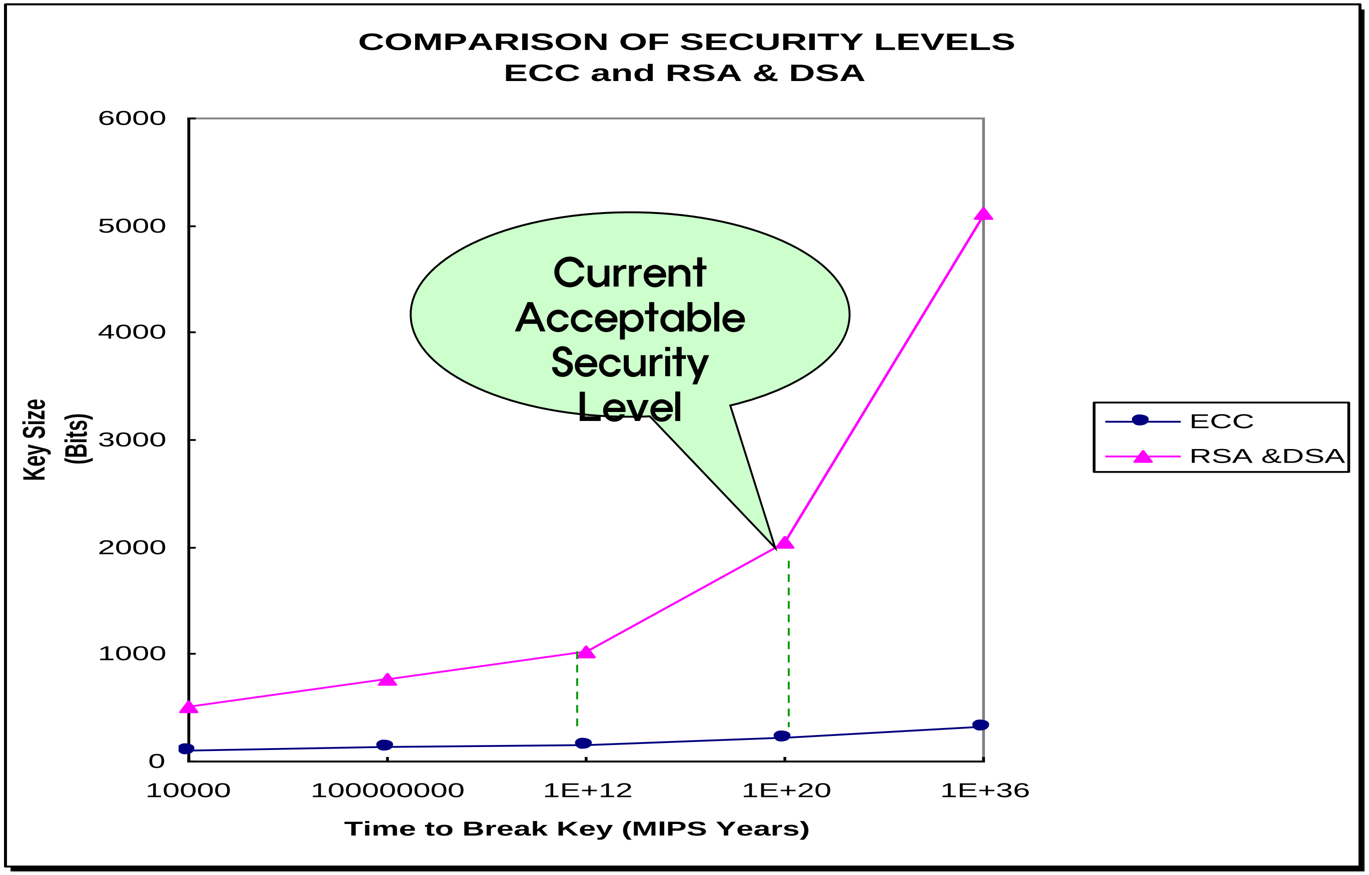
1) 타원곡선암호(Elliptic Curve Cryptosystem)

ECC 키길이 비교

ECC Key Size	RSA/DSA Key Size	Time to Break Mips/Yeas	RSA/ECC Key Size Ratio
106	512	10^{4}	4.83 : 1
132	768	10^{8}	5.82 : 1
160	1024	10^{12}	6.40 : 1
224	2048	10^{20}	9.14 : 1
600	21000	10^{78}	35.0 : 1

1) 타원곡선암호(Elliptic Curve Cryptosystem)

Security Levels



1) 타원곡선암호(Elliptic Curve Cryptosystem)

Implementation of ECC

- ECC vs RSA 8-bit Atmega 구현 결과 (Gura et al. 2004)

Algorithm	Time(s)	Data memory	Size (bytes)
ECC secp160r1	0.81	282	3,682
ECC secp192r1	1.24	336	3,979
ECC secp224r1	2.19	422	4,812
RSA-1024 public-key	0.43	543	1,073
RSA-1024 private-key	10.99	930	6,292
RSA-2048 public-key	1.94	1,332	2,854
RSA-2048 private-key	83.26	1,853	7,736

- 현재 ECC는 8/16/32 비트별 디바이스 최적화 구현하는 추세
  - 디바이스에서 제공하는 하드웨어 곱셈기 사용
  - 메모리를 적게 사용하면서 고속화 구현

2) 타원곡선(Elliptic Curve)

Elliptic Curve

[Def] **An Elliptic Curve over a field K is defined by an equation :**

$$E\ :\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Weierstrassen equation

where $a_i \in K$ **and the discriminant of E** $\Delta \neq 0$ **.**

$$\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6$$

$$d_2 = a_1^2 + 4a_2$$

$$d_4 = 2a_4 + a_1 a_3$$

$$d_6 = a_3^2 + 4a_6$$

$$d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

2) 타원곡선(Elliptic Curve)

Elliptic Curve

An Elliptic Curve over a field K is defined by an equation :

$$E\ :\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

By the admissible change of variables

1) **Char(K)=2**

$$E\ :\ y^2 + xy = x^3 + ax^2 + b,\ \ where\ \ a, b \in K,\ \ \Delta = b$$

2) **Char(K) ≠ 2 or 3**

$$E\ :\ y^2 = x^3 + ax\ \ + b,\ \ where\ \ a, b \in K,\ \ \Delta = -16(4a^3 + 27b^2)$$

2) 타원곡선(Elliptic Curve)

Elliptic Curve

Constructing an Elliptic Curve over a finite field requires two basic steps:

1. Selecting a finite field F_q

➔ typically q=p, a prime or q $=2^m$

2.Select an equation of the form

➔ Non-supersingular Curves

$p>3$	$y^2 = x^3 + ax + b, \quad a,b \in F_p, \quad \Delta = 4a^2 + 27b^2 \neq 0,$
$p = 2$	$y^2 + xy = x^3 + ax^2 + b, \quad a,b \in F_{2^m}, \quad \Delta = b \neq 0.$

2) 타원곡선(Elliptic Curve)

Elliptic Curve

[타원곡선의 정의]

- $E(F_p) = \{(x,y) \mid y^2 = x^3 + ax + b\} \cup \{O\}, p > 3$
- $E(F_{2^m}) = \{(x,y) \mid y^2 + xy = x^3 + ax^2 + b\} \cup \{O\}$

O (∞)는 무한원점(the point at infinity)

Example

$E(F_5) = \{(x,y) \mid y^2 = x^3 + 2x + 3\} \cup \{O\}$

➔ 곡선상의 점들은 { (1,1) (1,4) (2,0) (3,1) (3,4) (4,0), O}

2) 타원곡선(Elliptic Curve)

Elliptic Curve Addition

The points on an EC over a field form

an abelian group under the operation +.

1. Commutativity. $P_1 + P_2 = P_2 + P_1$

2. Existence of identity. $P + O = P$

3. Existence of inverses. $P + (-P) = O$

4. Associativity. $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$

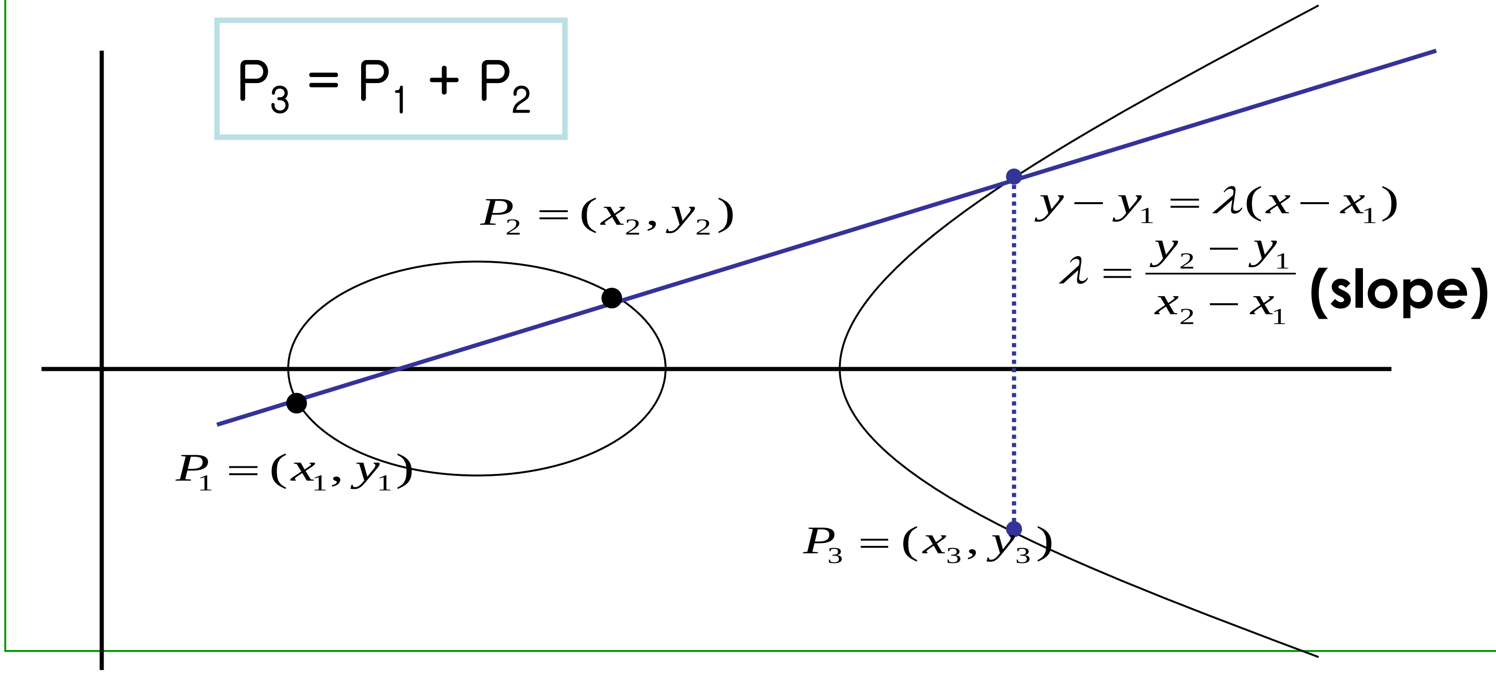
2) 타원곡선(Elliptic Curve)

Elliptic Curve Addition

The points on an EC over a finite field form an abelian group

under the following operation.

$P_3 = P_1 + P_2$

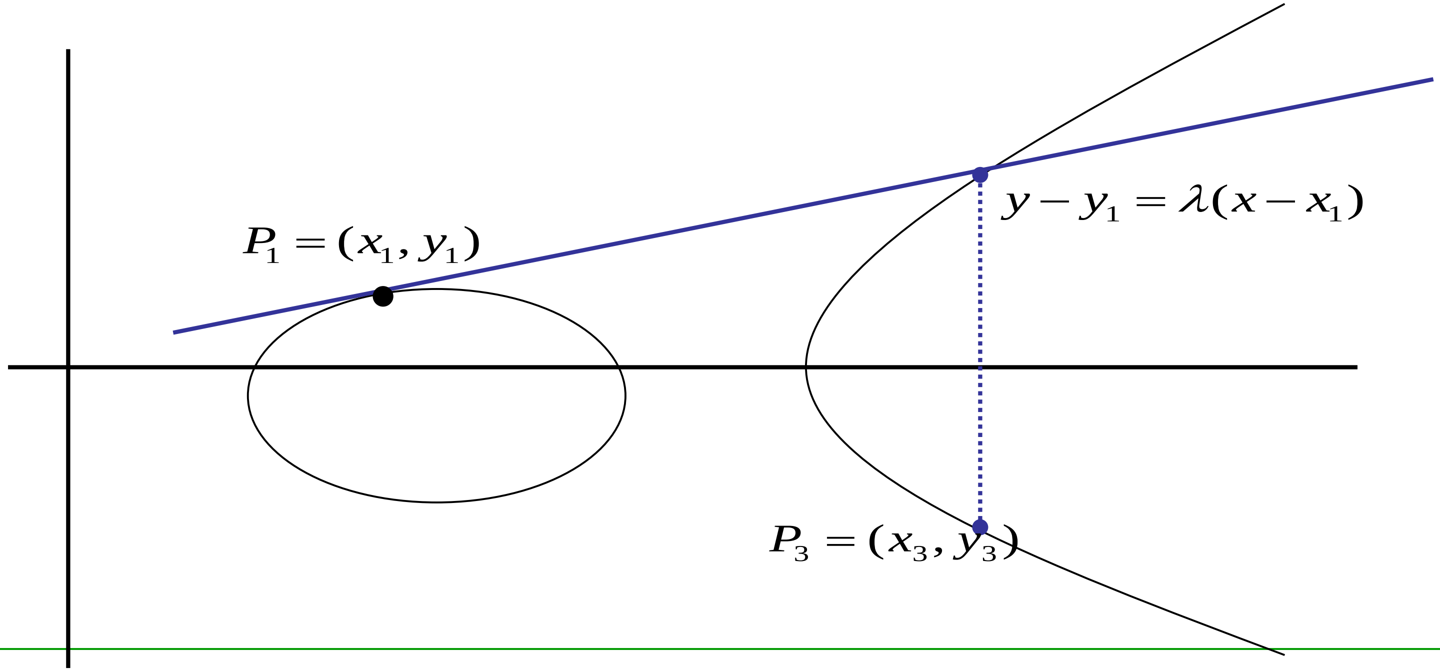


$P_2 = (x_2, y_2)$
$y - y_1 = \lambda(x - x_1)$
$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ (slope)
$P_1 = (x_1, y_1)$
$P_3 = (x_3, y_3)$

2) 타원곡선(Elliptic Curve)

Elliptic Curve Doubling

$$P_3 = P_1 + P_1 = 2P_1$$



2) 타원곡선(Elliptic Curve)

$$E(F_p) = \{(x, y) \mid y^2 = x^3 + ax + b\} \cup \{O\}, p > 3$$

$$P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = (x_3, y_3) \in E(F_p)$$

- $P + O = P, \quad P + (-P) = O,$
- $P = (x, y) \Rightarrow -P = (x, -y)$
- $P_3 = (x_3, y_3) = P_1 + P_2$

$P_1 \neq P_2$
$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$P_1 = P_2$
$$\begin{cases} x_3 = \lambda^2 - 2x_1 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \qquad \lambda = \frac{3x_1^2 + a}{2y_1}$$

2) 타원곡선(Elliptic Curve)

$$E(F_{2^m}) = \{(x, y) \mid y^2 + xy = x^3 + ax^2 + b\} \bigcup \{O\}, b \neq 0$$

$$P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = (x_3, y_3) \in E(F_{2^m})$$

- $P = (x, y) \Rightarrow -P = (x, x + y)$

- $P_3 = (x_3, y_3) = P_1 + P_2$

$$\left\{ \begin{array}{l} x_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + \dfrac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a, & P_1 \neq P_2, \\ x_1^2 + \dfrac{b}{x_1^2}, & P_1 = P_2 \end{cases} \\ y_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1, & P_1 \neq P_2, \\ x_1^2 + (x_1 + \dfrac{y_1}{x_1})x_3 + x_3, & P_1 = P_2 \end{cases} \end{array} \right.$$

2) 타원곡선(Elliptic Curve)

Example

$$E(F_5) = \{(x, y) \mid y^2 = x^3 + 2x + 3\} \cup \{O\}$$

- $P_1 = (1,4)$, $P_2 = (3,1)$, $P_3 = (x_3, y_3) = P_1 + P_2$?

- $\lambda = (1-4)/(3-1) = -3/2$

  $= 2(3) = 6 = 1 \pmod 5$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

- $x_3 = 1 - 1 - 3 = 2 \pmod 5$

- $y_3 = 1(1-2) - 4 = 0 \pmod 5$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

➔ $(1,4) + (3,1) = P_3 = (x_3, y_3) = (2,0)$

2) 타원곡선(Elliptic Curve)

The order of Elliptic Curve

[Theorem](Hasse) Let E be an elliptic curve defined over F_q.

$$\#E(F_q)=q+1-t, \qquad |t|\le 2\sqrt{q}$$

⇒ $$q+1-2\sqrt{q}\le \#E(F_q)\le q+1+2\sqrt{q}$$

[Def] Let Char(F_q)=p.

An elliptic curve E defined over F_q is supersingular if p divides t.

Ex) $$E(F_5)=\{(x,y)\,|\,y^2=x^3+2x+3\}\cup\{O\} \qquad \#E(F_5)=q+1-t=7$$

⇒ $$t=-1,\ \ \text{non}-\text{supersingu lar}$$

3) 타원곡선 이산대수문제(Elliptic Curve Discrete Log Problem)

Recall of DLP

- Let *G* be a cyclic subgroup $Z_p^* = \{1,2,\ldots,p-1\}$ of a modulo group Zp.

  Let *g* be a generator of *G*.

  Discrete Log Problem (DLP) : Given p, g, and y, find x such that

$$\boxed{y \equiv g^x \pmod{p}}$$

- Example:

$$G = Z_{11}^* = \{1,2,\ldots,10\} = < 2 > .$$

8

Given p=11, g=2 and 3, find x such that $3 \equiv 2^x \pmod{11}$.

3) 타원곡선 이산대수문제(Elliptic Curve Discrete Log Problem)

ECDLP

- Suppose that two points P and $Q \in < P >$ in $E(F_q)$.

The Elliptic Curve Discrete Logarithm Problem (ECDLP) is to find an integer m satisfying

$$Q = P + P + \cdots + P = m\,P.$$

- Scalar multiplication : $m\,P = P + P + \cdots + P$
- If the prime p is large, it is very difficult to find m.

3) 타원곡선 이산대수문제(Elliptic Curve Discrete Log Problem)

ECDHP

- Diffie-Hellman Problem (DHP)

  Given p, g, g^a, g^b → find g^{ab} (mod p).

- The Elliptic Curve Diffie-Hellman Problem (ECDHP) is to find

  Given P, sP, tP → find *stP*.

3) 타원곡선 이산대수문제(Elliptic Curve Discrete Log Problem)

DLP and ECDLP

	Regular DL (e.g. Diffie-Hellman)	ECC with prime field	ECC with binary field
Field	GF(p)	GF(p)	GF(2^m)
Field representation	0,1,…,p-1	0,1,…,p-1	Polynomial basis or normal basis
Field order (size)	p	p	2^m
Group elements	GF(p)*	E(Fp)	E(GF(2^m))
Basic operation	Multiplication in GF(p)	Addition of points on E	Addition of points on E
Base element	Generator g	Base point P	Base point P
Main operation	Exponentiation	Scalar multiplication	Scalar multiplication
Group order (size)	p-1	$p+1-2p^{1/2} \le \#E(Fp) \le p+1+2p^{1/2}$	$2^m+1-2^{m/2+1} \le \#E(GF(2^m)) \le 2^m+1+2^{m/2+1}$

4) 타원곡선암호 파라미터

NIST Recommended Elliptic Curves

1. Choice of Key Lengths

- The elliptic curve *E*, the base point *G on E* has order *n, which is a large prime.*
- #E = hn, *h is the cofactor.*
- it is desirable to have the cofactor be as small as possible
- the private and public keys for a curve are approximately the same length.

Public key : $Q = kG$ and Private key: k, $(1 \le k \le n)$

4) 타원곡선암호 파라미터

2. Choice of Underlying Fields

- Choice a *prime field* F_p or a *binary field* GF(2^m) = F_{2^m}

Bits of Security	Symmetric key algs.	Hash algs.	RSA	Prime field	Binary Field
80	SKIPJACK	SHA-1	*k* = 1024	*Len(p)*= 192	*m*= 163
112	TDES		*k* = 2048	*Len(p)*= 224	*m*= 233
128	AES-128	SHA-256	*k* = 3072	*Len(p)*= 256	*m*= 283
192	AES-192	SHA-384	*k* = 7680	*Len(p)*= 384	*m*= 409
256	AES-256	SHA-512	*k* = 15360	*Len(p)*= 512	*m*= 571

4) 타원곡선암호 파라미터

3. Choice of Basis for Binary Fields

- Polynomial Basis:
  - *an* irreducible *trinomial* $t^m + t^k + 1$ *over* $GF(2)$ *with the lowest-degree middle*
  - *an* irreducible *pentanomial* $t^m + t^a + t^b + t^c + + 1$
- Normal Basis: Choose low-complexity normal basis.

4. Choice of Curves

- *Pseudo-random curves* : from the output of a seeded cryptographic hash function.
- *Special curves* *: to* optimize the efficiency of the elliptic curve operations.

  → A special curve over $GF(2^m)$ *called a Koblitz curve or anomalous binary curve*

5. Choice of Base Points

- Any point $G = (Gx , Gy)$ of order n *can serve as the base point*

4) 타원곡선암호 파라미터

Elliptic curve domain parameters and their validation

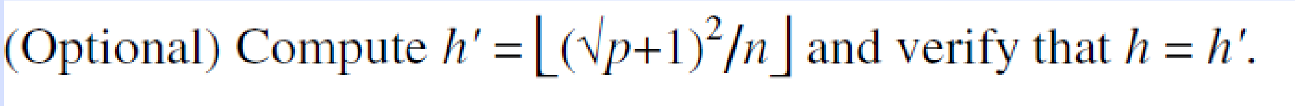
1. Elliptic curve domain parameters and their validation over F_p

$$E : y^2 = x^3 + ax + b \quad over \quad F_p$$

- Verify that p *is an odd prime number*
- Verify that *a, b, Gx and Gy are integers in the interval [0, p−1]*
- If the elliptic curve was randomly generated, verify that SEED is a bit string of length at least 160 bits that a and b were suitably derived from SEED
- Verify that $4a^3 + 27b^2 \neq 0 \pmod p$.
- Verify that *G=(Gx , Gy) is the point in E.*

4) 타원곡선암호 파라미터

$$E : y^2 = x^3 + ax + b \quad over \quad F_p$$

- Verify that *n is prime, and that len(n)>160 and n > 4√p* *(Security)*
- Verify that *nG = O*
- 
  (Optional) Compute $h' = \lfloor (\sqrt{p}+1)^2/n \rfloor$ and verify that $h = h'$.
- Verify that the MOV and Anomalous (#E≠p) conditions hold.
- If any of the above verifications fail then output "invalid".

  If all the verifications pass then output "valid".

4) 타원곡선암호 파라미터

2. Elliptic curve domain parameters and their validation over *GF(2^m)*

$$E: y^2 + xy = x^3 + ax^2 + b \quad over \quad F_{2^m}$$

- Verify that q = *2^m* and a reduction polynomial of degree m over F_2
  - If the basis used is a TPB,

    verify that the reduction polynomial is an irreducible trinomial over F_2
  - If the basis used is a PPB,

    verify that the reduction polynomial is an irreducible pentanomial over F_2
  - If the basis used is a Gaussian Normal Basis, verify that m is not divisible by 8.
- Verify that *a, b, Gx and Gy are* bit strings of length *m* bits.
- Verify that b$\neq$ *0*

5) 타원곡선암호 응용분야

Signature Schemes	ECDSA	ANSI X9.62, FIPS 186-2, IEEE 1363-2000, ISO/IEC 15946-2
	EC-KCDSA	ISO/IEC 15946

Public Key Encryption	ECIES	ANSI X9.63, IEEE 1363a, ISO/IEC 15946-3
	PSEC	ISO 18033-2

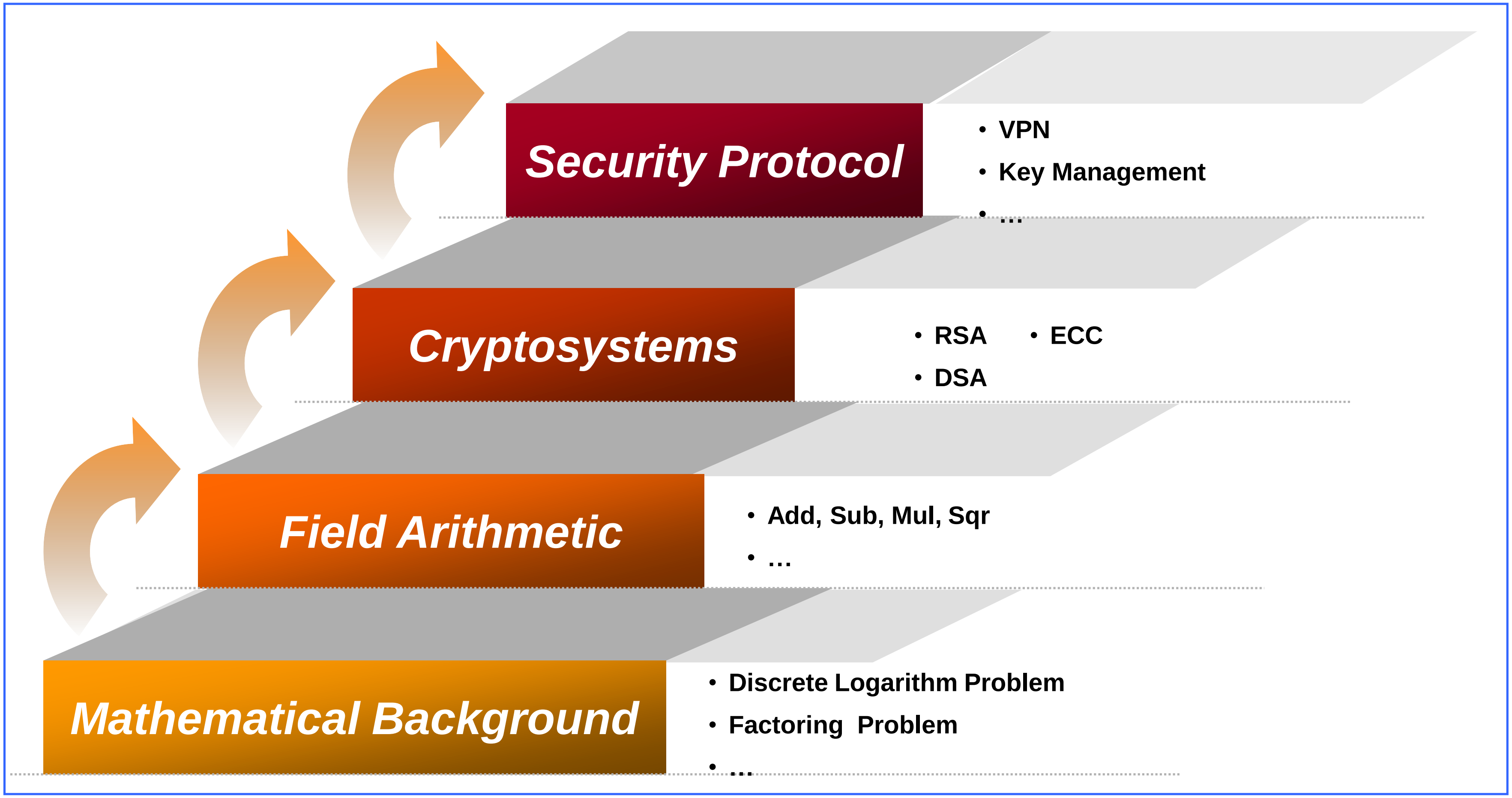
Key Establishment	ECDH	ANSI X9.63, IPSec, IEEE 1363, ISO/IEC 15946
	ECMQV	ANSI X9.63, IEEE 1363, ISO/IEC 15946

5) 타원곡선암호 응용분야

Standard	Schemes included
ANSI X9.62	ECDSA
ANSI X9.63	ECIES, ECDH, ECMQV
FIPS 186−2	ECDSA
IEEE 1363−2000	ECDSA, ECDH, ECMQV
IEEE 1363A	ECIES
IPSec	ECDSA, ECDH
ISO 14888-3	ECDSA
ISO/IEC 15946	ECDSA, ECDH, ECMQV

2 타원곡선암호 구현 및 응용

1) 암호시스템 구현



Security Protocol

- VPN
- Key Management
- …

Cryptosystems

- RSA
- ECC
- DSA

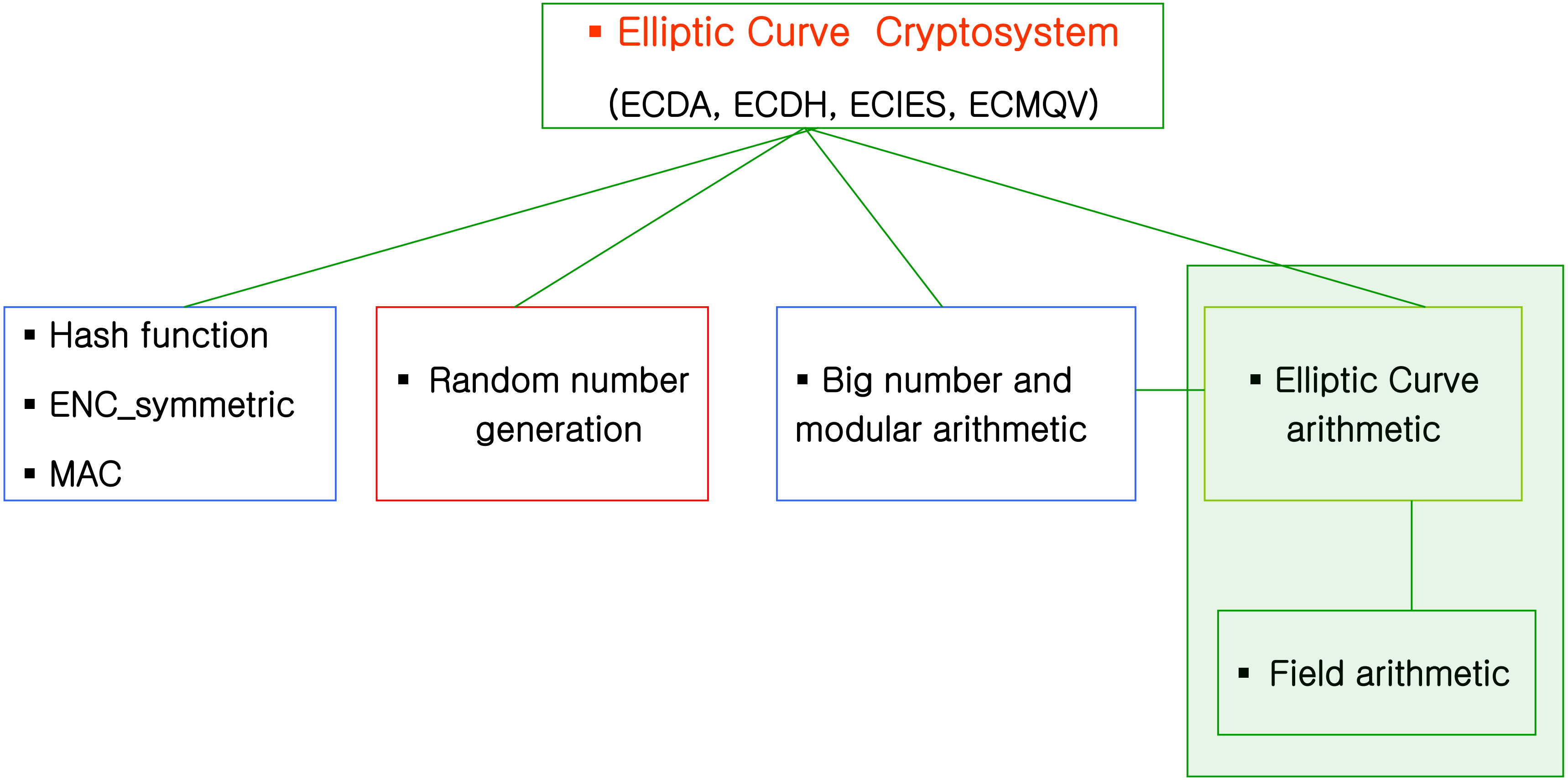
Field Arithmetic

- Add, Sub, Mul, Sqr
- …

Mathematical Background

- Discrete Logarithm Problem
- Factoring Problem
- …

1) 암호시스템 구현



- Elliptic Curve Cryptosystem

(ECDA, ECDH, ECIES, ECMQV)

- Hash function
- ENC_symmetric
- MAC

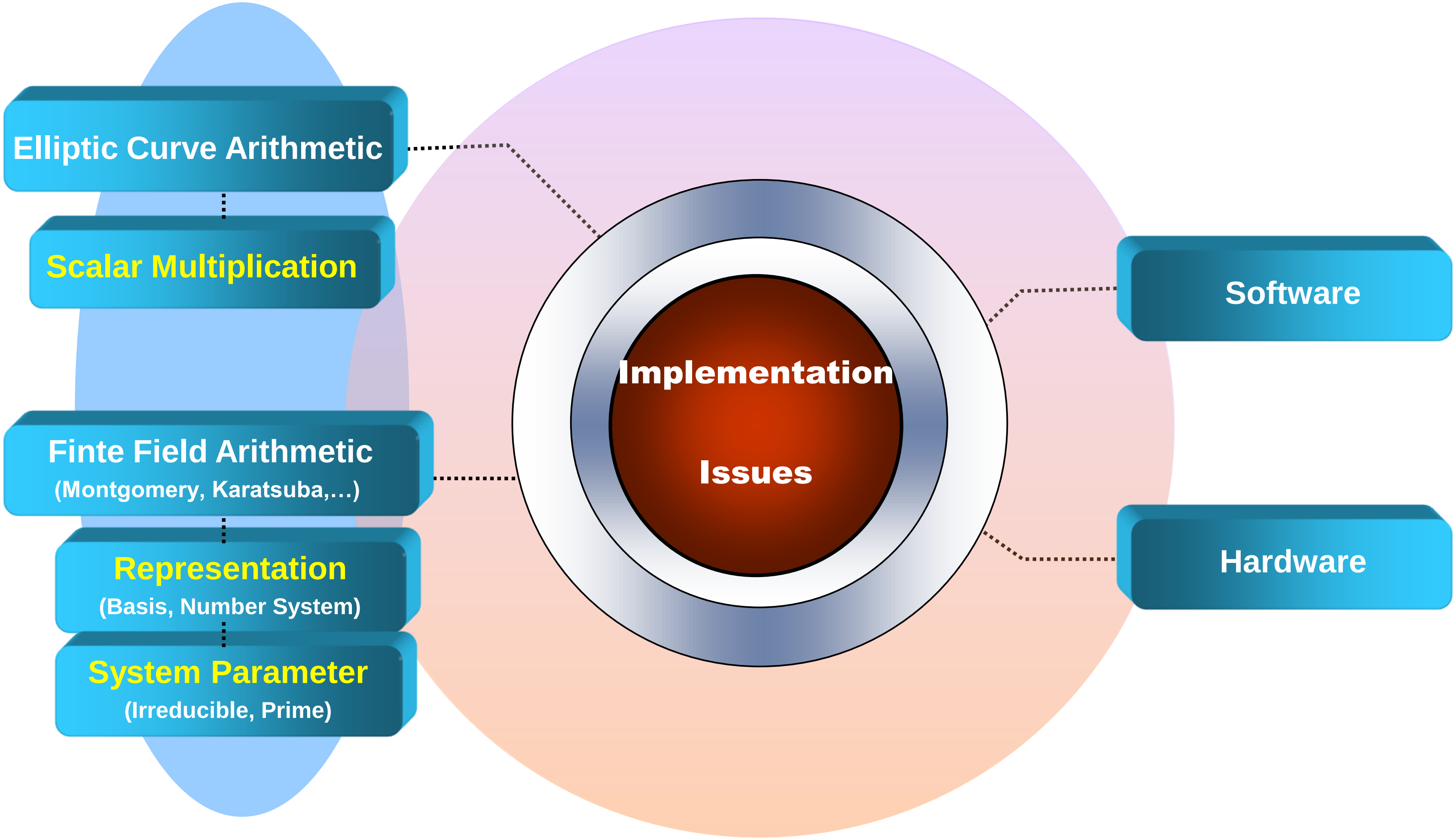
- Random number generation

- Big number and modular arithmetic

- Elliptic Curve arithmetic

- Field arithmetic

1) 암호시스템 구현


Elliptic Curve Arithmetic

Scalar Multiplication

Finte Field Arithmetic

(Montgomery, Karatsuba,…)

Representation

(Basis, Number System)

System Parameter

(Irreducible, Prime)

Implementation

Issues

Software

Hardware

1) 암호시스템 구현

효율적인 구현을 위한 고려사항

1. 기본 유한체를 선택
2. 선택된 유한체 원소의 표현 방법 선택
3. 유한체 상에서의 연산의 구현
4. 안전하고 효율적인 타원곡선 선택
5. 타원곡선상의 연산의 구현

2) Finite Field Arithmetic

Finite Field Arithmetic

- **Addition**
- **Subtraction**
- **Multiplication**
  - SchoolBook
  - Karatsuba-Ofman
- **Squaring**
  - SchoolBook
  - Karatsuba-Ofman
- **Inversion, GCD**
  - Extended Euclidean
  - Extended Binary
  - Almost Inversion

2) Finite Field Arithmetic

Finite Field Arithmetic

❍ **Reduction**

- Division
- Montgomey
- **Special Reduction**

❍ **Exponentiation**

- Binary(LtoR,RtoL)
- K-ary
- Modefied k-ary
- Sliding window

2) Finite Field Arithmetic

Prime Finite Field 에서 Special Reduction 을 위한 소수 p선택

❒ Mersenne 소수로 선택하거나 reduction이 효율적인 소수 선택

- ❖ *Special Prime (Nist Prime FIPS 186-2)*

$$p_{192} = 2^{192} - 2^{64} - 1$$

$$p_{224} = 2^{224} - 2^{96} + 1$$

$$p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$$

$$p_{384} = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$$

$$p_{521} = 2^{521} - 1.$$

2) Finite Field Arithmetic

Binary Finite Field 에서 Special Reduction 을 위한 소수 p선택

❒ Special Irreducible Polynomial (NIST Polynomial)

- ❍ Trinomial
- ❍ Pentanomial

❖ ***Special Prime (Nist Prime)***

$$f(z) = z^{163} + z^{7} + z^{6} + z^{3} + 1$$

$$f(z) = z^{233} + z^{74} + 1$$

$$f(z) = z^{283} + z^{12} + z^{7} + z^{5} + 1$$

$$f(z) = z^{409} + z^{87} + 1$$

$$f(z) = z^{571} + z^{10} + z^{5} + z^{2} + 1 .$$

2) Finite Field Arithmetic

Binary Field Arithmetic Comparison

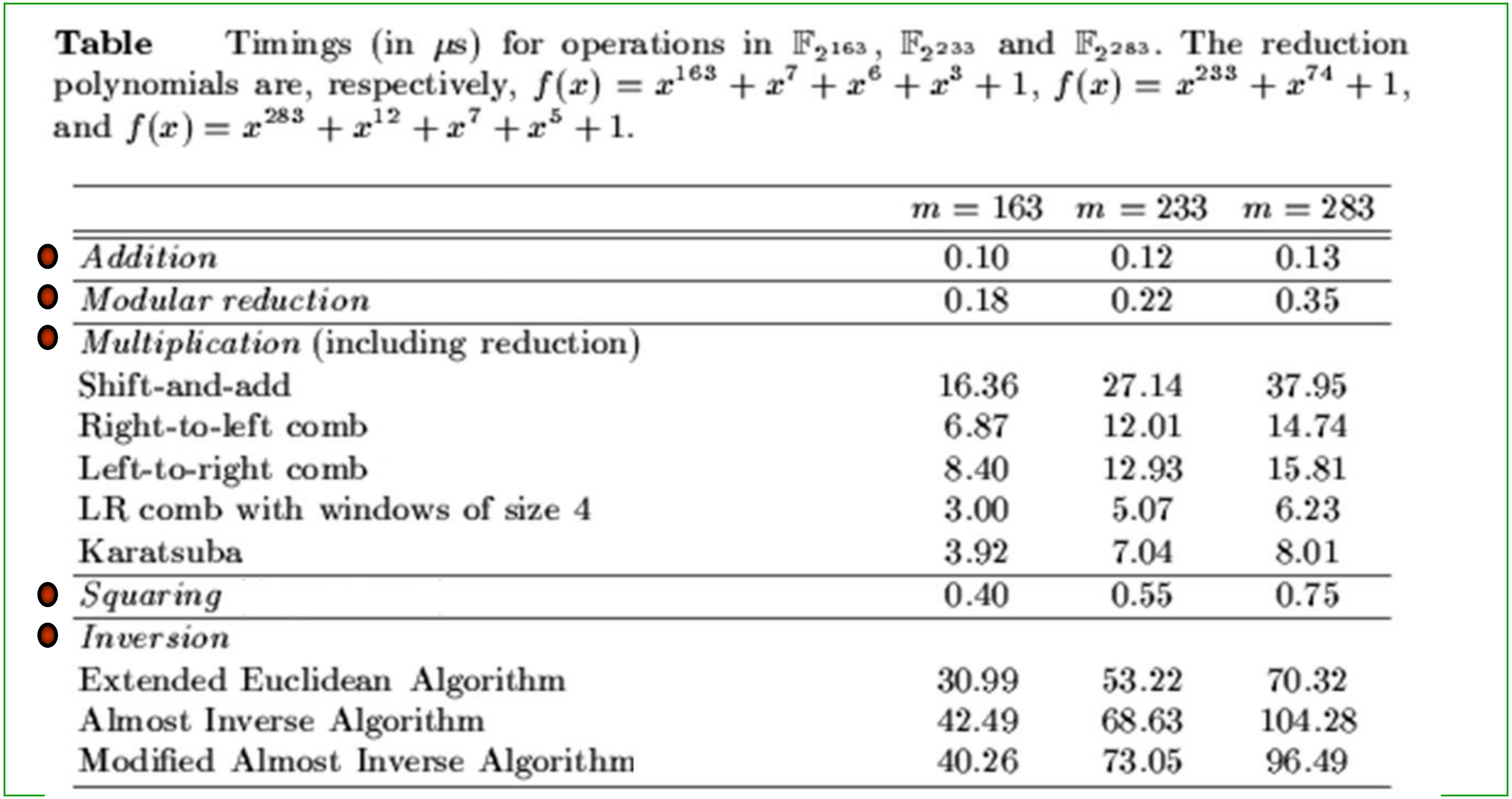


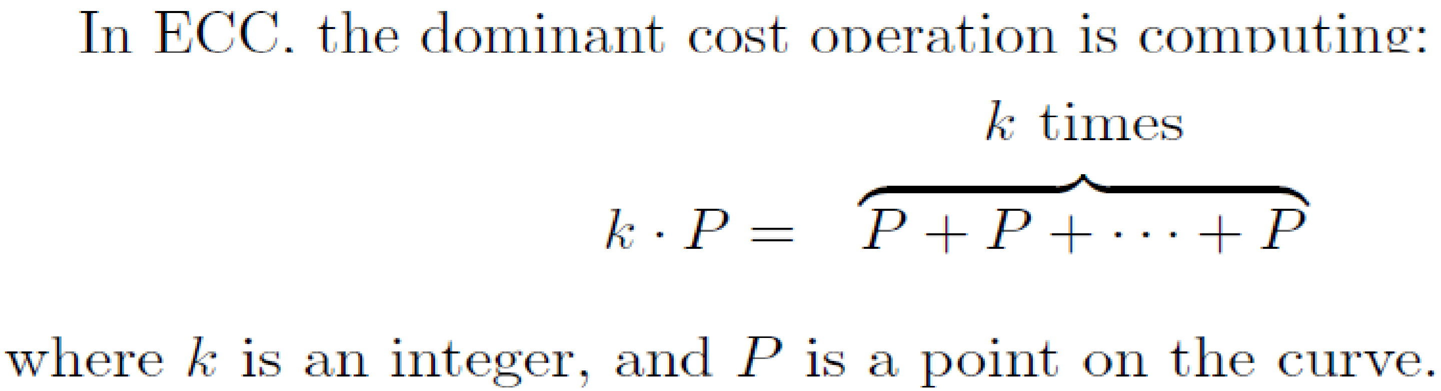
Table Timings (in μs) for operations in $\mathbb{F}_{2^{163}}$, $\mathbb{F}_{2^{233}}$ and $\mathbb{F}_{2^{283}}$. The reduction polynomials are, respectively, $f(x) = x^{163} + x^7 + x^6 + x^3 + 1$, $f(x) = x^{233} + x^{74} + 1$, and $f(x) = x^{283} + x^{12} + x^7 + x^5 + 1$.

	$m = 163$	$m = 233$	$m = 283$
● *Addition*	0.10	0.12	0.13
● *Modular reduction*	0.18	0.22	0.35
● *Multiplication* (including reduction)			
Shift-and-add	16.36	27.14	37.95
Right-to-left comb	6.87	12.01	14.74
Left-to-right comb	8.40	12.93	15.81
LR comb with windows of size 4	3.00	5.07	6.23
Karatsuba	3.92	7.04	8.01
● *Squaring*	0.40	0.55	0.75
● *Inversion*			
Extended Euclidean Algorithm	30.99	53.22	70.32
Almost Inverse Algorithm	42.49	68.63	104.28
Modified Almost Inverse Algorithm	40.26	73.05	96.49

3) Elliptic Curve Arithmetic

Elliptic Curve Arithmetic

- ❍ **Coordinate**
- ❍ **Addition and Doubling**
- ❍ **Scalar Multiplication**



In ECC, the dominant cost operation is computing:

$$k \cdot P = \overbrace{P + P + \cdots + P}^{k \text{ times}}$$

where k is an integer, and P is a point on the curve.

3) Elliptic Curve Arithmetic

Elliptic Curve Coordinates

$$E : y^2 + xy = x^3 + ax^2 + b \quad over \quad F_{2^m}$$

- Affine coordinates;
  - $E(F_{2^m}) = \{(x, y) \mid y^2 + xy = x^3 + ax^2 + b\}$
- Standard projective coordinates;
  - $Y^2Z + XYZ = X^3 + aX^2Z + bZ^3 \quad (X : Y : Z) \;\; Z \neq O \rightarrow (X/Z, Y/Z)$
- Jacobian projective coordinates;
  - $Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6 \quad (X : Y : Z) \;\; Z \neq O \rightarrow (X/Z^2, Y/Z^3)$
- Lopez-Dahab projective coordinates;
  - $Y^2 + XYZ = X^3Z + aX^2Z^2 + bZ^4 \quad (X : Y : Z) \;\; Z \neq O \rightarrow (X/Z, Y/Z^2)$

3) Elliptic Curve Arithmetic

Elliptic Curve Coordinates

❍ Doubling for Binary Field (Jacobian projective coordinates)

$P=(X_1:Y_1:Z_1)\in E$ ⇨ $P=[X_1/Z_1^2 : Y_1/Z_1^3 : 1]$ ⇨ $2P=(X_3:Y_3:Z_3)$

$x = X_1/Z_1^2, \quad y = Y_1/Z_1^3$

Affine Doubling
공식에 대입

→

$$\begin{aligned} X_3 &= (3X_1^2 + aZ_1^4)^2 - 8X_1Y_1^2 \\ Y_3 &= (3X_1^2 + aZ_1^4)(4X_1Y_1^2 - X_3) - 8Y_1^4 \\ Z_3 &= 2Y_1Z_1. \end{aligned}$$

→

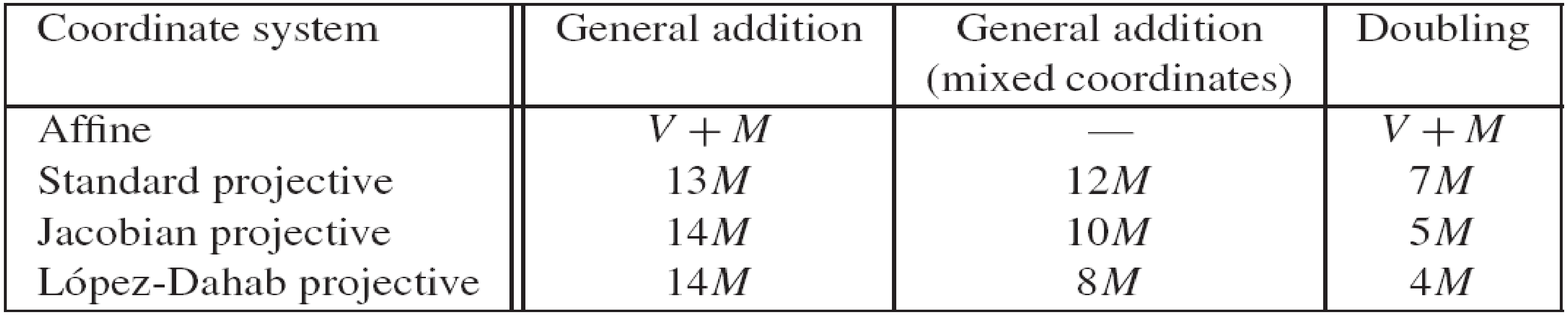
$$\begin{array}{llll} A \leftarrow Y_1^2, & B \leftarrow 4X_1 \cdot A, & C \leftarrow 8A^2, & D \leftarrow 3X_1^2 + a \cdot Z_1^4, \\ X_3 \leftarrow D^2 - 2B, & Y_3 \leftarrow D \cdot (B - X_3) - C, & Z_3 \leftarrow 2Y_1 \cdot Z_1. & \end{array}$$

6 sqr, 4 mul

3) Elliptic Curve Arithmetic

Elliptic Curve Coordinates

❍ Point operation for binary field



Coordinate system	General addition	General addition (mixed coordinates)	Doubling
Affine	$V + M$	—	$V + M$
Standard projective	$13M$	$12M$	$7M$
Jacobian projective	$14M$	$10M$	$5M$
López-Dahab projective	$14M$	$8M$	$4M$

M: Mul, V: division (a/b)

3) Elliptic Curve Arithmetic

Elliptic Curve Scalar Multiplication

$$k \cdot P = \overbrace{P + P + \cdots + P}^{k \text{ times}}$$

- Binary Method
- m-ary Method
- Sliding Window Method
- Simultaneous Method

Traditional exponentiation techniques

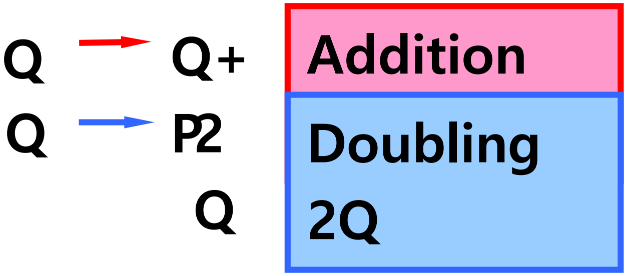
- NAF Method
- Montgomery Method
- Fronenius endomorphism (Koblitz curves)
- Efficiently computable endomorphism

3) Elliptic Curve Arithmetic

Elliptic Curve Scalar Multiplication

Binary Method

$d = 89 = (1011001)_2$



Q → Q+

Q → P2

Q

Addition

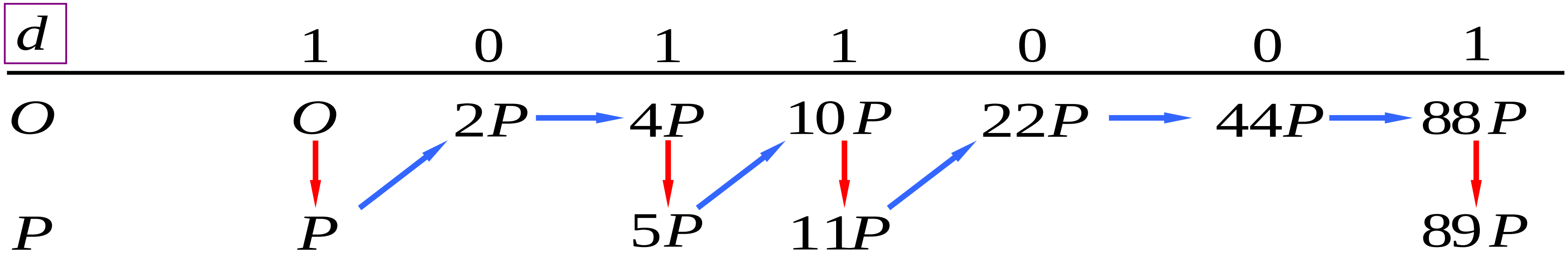
Doubling

2Q

Binary method (left-to-right)

```
INPUT: a point P, an n-bit d
OUTPUT: dP

1.   Q ← P
2.   For i=n-2 down to 0
 2.1. Q ← ECDBL(Q)
 2.2. If $d_i$ = 1
         then Q ← ECADD(Q,P)
3. Returen Q
```



d	1	0	1	1	0	0	1
O	O	$2P$	$4P$	$10P$	$22P$	$44P$	$88P$
P	P		$5P$	$11P$			$89P$

3) Elliptic Curve Arithmetic

Elliptic Curve Scalar Multiplication

● **NAF (Non-Adjacent Forms) Method**

$7 = (0111)_2$ ➔ $7 = (1\ 0\ 0\ -1)_{NAF}$

- ● −P : 계산이 쉬움
- ● Addition 연산

  m/2 => m/3

INPUT: A positive integer k.

OUTPUT: NAF(k).

```
1. $i \leftarrow 0$.
2. While $k \geq 1$ do
    2.1 If k is odd then: $k_i \leftarrow 2-(k \bmod 4)$, $k \leftarrow k-k_i$;
    2.2 Else: $k_i \leftarrow 0$
    2.3 $k \leftarrow k/2$ , $i \leftarrow i+1$
3. Return($(k_{i-1},k_{i-2},\cdots,k_1,k_0)$).
```

3) Elliptic Curve Arithmetic

Elliptic Curve Scalar Multiplication

NAF (Non-Adjacent Forms) Method

d=2004	T-representation	# of non-zeros
T={1} (binary)	$d = (11111010100)$	7
T={1,-1}	$d = (10\underline{1}111010100)$ $[\underline{1}=-1]$	7
	$d = (100\underline{1}11010100)$	6
	$d = (10000\underline{1}010100)$	4
	$d = (100000\underline{11}0100)$	4
	$d = (100000\underline{1}0\underline{11}00)$	4

3) Elliptic Curve Arithmetic

Elliptic Curve Scalar Multiplication

NAF (Non-Adjacent Forms) Method

d=2004	T-epresentation	# of non-zeros
Binary	d=(11111010100)	7
	(3d - d)/2 conversion	
T={1,-1}	3d=(1011101111100)	
	- d= (11111010100)	
	2d=(10000$\underline{1}$0101000) [$\underline{1}$=-1]	
NAF →	d= (10000$\underline{1}$010100)	4

3) Elliptic Curve Arithmetic

Elliptic Curve Scalar Multiplication

Montgomery Method

$$E : y^2 + xy = x^3 + ax^2 + b \quad over \quad F_{2^m}$$

$$P_1 = (x_1, y_1), P_2 = (x_2, y_2), \quad with \quad (P_1 \neq \pm P_2)$$

$$P_1 + P_2 = (x_3, y_3), P_1 - P_2 = (x_4, y_4)$$

⇒

$$x_3 = x_4 + \frac{x_2}{x_1 + x_2} + (\frac{x_2}{x_1 + x_2})^2$$

- x− coordinate of $P_1, P_2, P_1 - P_2$ ⇒ x− coordinate of $P_1 + P_2$

3) Elliptic Curve Arithmetic

Elliptic Curve Scalar Multiplication

Method	Addition	Doubling	Affine		Projective	
			A	D	A	D
			12M	12M	9M	4M
Binary	n/2	n	2940		1390	
m-ary	$n/r + 2^r$	n	2460		1165	
Sliding window	$n/(r+1)+2^{r-1}$	n	2488		994	
Binary NAF	n/3	n	2604		1138	
Window NAF	$n/(r+1)$ $+2^{r-2}-1$	n	2388		976	

4) ECC Implementation

8-bit AVR Atmega 구현 동향

Implementation	Year	Curve	Clock cycles	Size (bytes)	RAM usage (bytes)
Aranha et al.	2010	K-233	≈5,382,144	≈38,600	≈3,700
Aranha et al.	2010	B-233	≈13,934,592	≈34,600	≈2,200
Gura et al.	2004	P-224	≈17,520,000	4,815	422
Liu et al.	2014	256-bit Montgomery	≈21,078,200	14,700	556
Wenger et al.	2013	P-256	≈34,930,000	16,112	590
Hutter and Schwabe	2013	Curve25519	22,791,579	n/a	677
Dull et al.	2015	Curve25519	14,146,844	9,912	510
Dull et al.	2015	Curve25519	13,900,397	17,710	494

4) ECC Implementation

16-bit MSP430 구현 동향

Implementation	Year	CPU	Curve	Clock cycles @ 8MHz	Clock cycles @ 16MHz	Size (bytes)	Stack usage (bytes)
With 16-bit hardware multiplier							
Wenger and Werner	2011	MSP430	P-256	23,973,000	n/a	n/a	n/a
Wenger et al.	2013	MSP430	P-256	22,170,000	n/a	8,378	418
Gouvea et al.	2014	MSP430X	P-256	7,284,377	n/a	n/a	n/a
Hinterwalder et al.	2014	MSP430X	Curve25519	9,139,739	10,404,042	11,778	513
Dull et al.	2015	MSP430X	Curve25519	7,933,296	9,119,840	13,112	384
With 32-bit hardware multiplier							
Gouvea et al.	2014	MSP430X	P-256	5,321,776	n/a	n/a	n/a
Hinterwalder et al.	2014	MSP430X	Curve25519	6,513,011	7,391,506	8,956	495
Dull et al.	2015	MSP430X	Curve25519	5,301,792	5,961,784	10,088	382

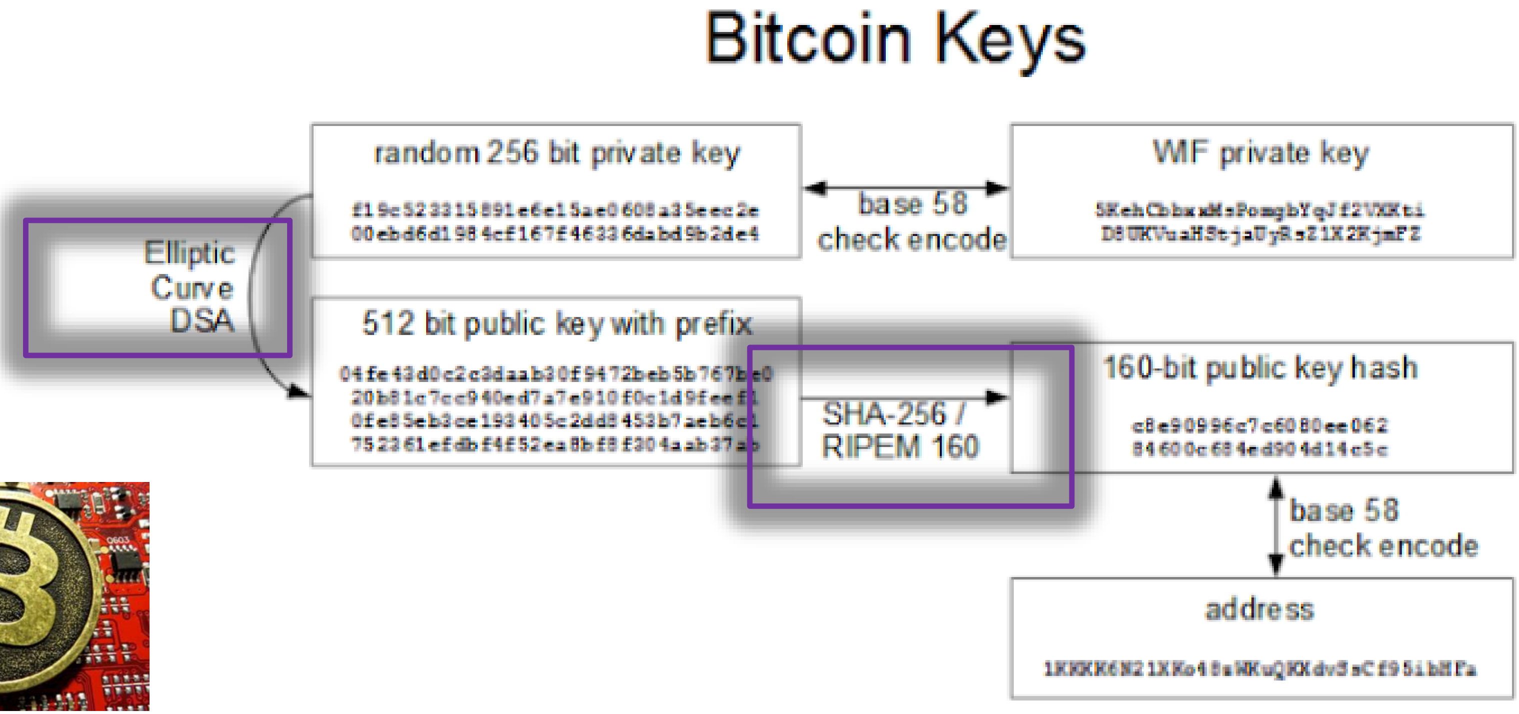
4) ECC Implementation

32-bit ARM Cortex-M0 구현 동향

Implementation	Year	Curve	Clock cycles	Size (bytes)	RAM usage (bytes)
De Clercq et al.	2014	K-233	2,762,000	n/a	n/a
Wenger et al.	2013	P-256	≈10,730,000	7,168	540
Dull et al.	2015	Curve25519	3,589,850	7,900	548

4) ECC 응용

⑩ 블록체인을 이용한 Bitcoin


Bitcoin Keys
random 256 bit private key
f19c523315891e6e15ae0608a35eec2e
00ebd6d1984cf167f46336dabd9b2de4
base 58
check encode
WIF private key
5KehCbbxxMsPomgbYqJf2VXKti
D8UKVuaHStjaUyRsZ1X2KjmFZ
Elliptic
Curve
DSA
512 bit public key with prefix
04fe43d0c2c3daab30f9472beb5b767be0
20b81c7cc940ed7a7e910f0c1d9feef1
0fe85eb3ce193405c2dd8453b7aeb6c1
752361efdbf4f52ea8bf8f304aab37ab
SHA-256 /
RIPEM 160
160-bit public key hash
c8e90996c7c6080ee062
84600c684ed904d14c5c
base 58
check encode
address
1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa

4) ECC 응용

⑩ Bitcoin 에 사용된 secp256k1

$$E(F_p) = \{(x, y) \mid y^2 = x^3 + 7\} \cup \{O\}$$

- *p* = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

  $= 2^{256} - 2^{32} - 2^{9} - 2^{8} - 2^{7} - 2^{6} - 2^{4} - 1$

- The base point G in compressed form is:

G = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

- The order *n* of *G* :

n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

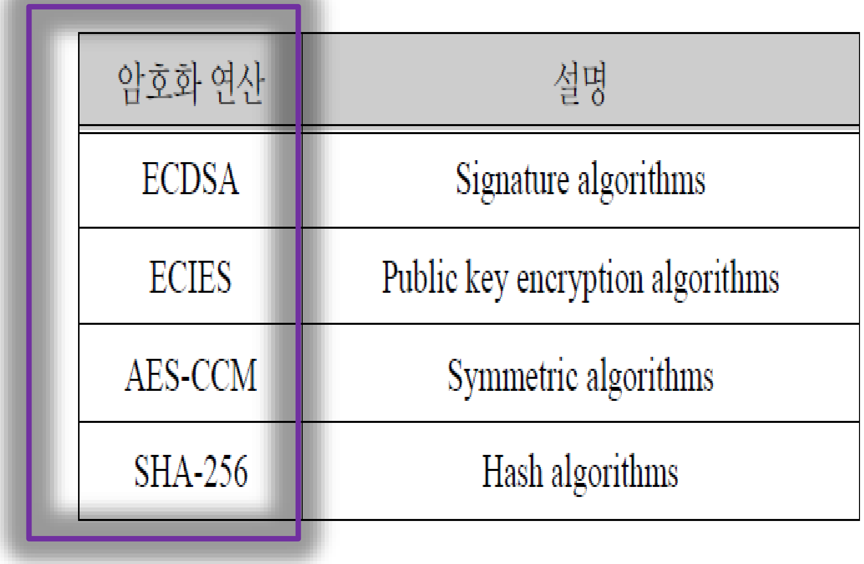
4) ECC 응용

⑩ 스마트자동차 (IEEE의 WAVE 1609.2)

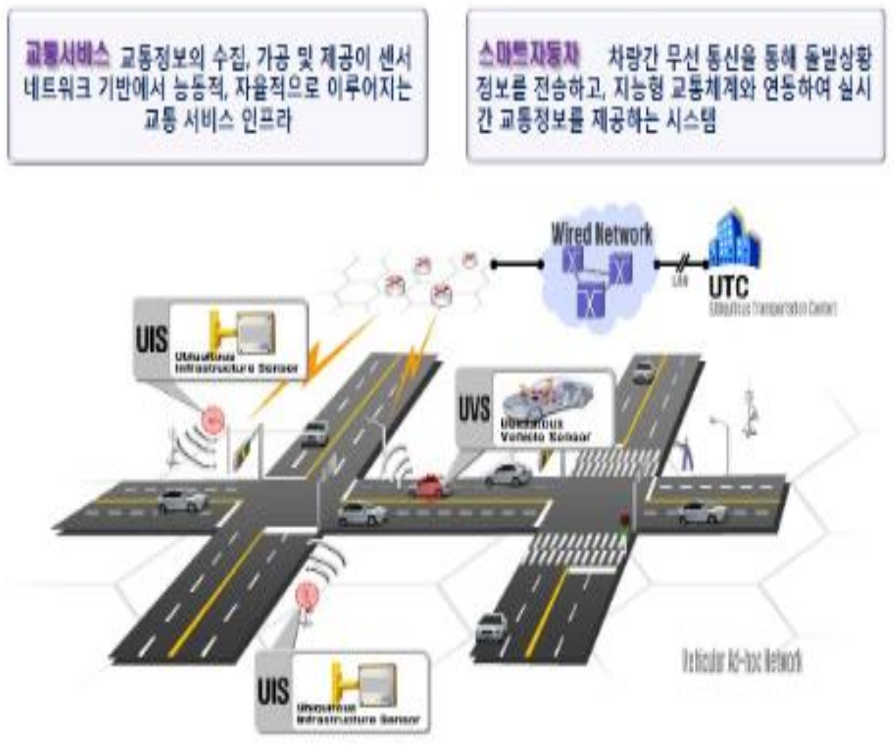
WAVE: Wireless Access in Vehicular Environment 약자의 IEEE 기술 표준

표 1. WAVE에서 사용되는 암호화 연산

Table. 1 Cryptographic operation in wave



암호화 연산	설명
ECDSA	Signature algorithms
ECIES	Public key encryption algorithms
AES-CCM	Symmetric algorithms
SHA-256	Hash algorithms



교통서비스 교통정보의 수집, 가공 및 제공이 센서 네트워크 기반에서 능동적, 자율적으로 이루어지는 교통 서비스 인프라

스마트자동차 차량간 무선 통신을 통해 돌발상황 정보를 전송하고, 지능형 교통체계와 연동하여 실시간 교통정보를 제공하는 시스템

Wired Network
LAN
UTC
Ubiquitous Transportation Center
UIS
Ubiquitous Infrastructure Sensor
UVS
Ubiquitous Vehicle Sensor
UIS
Ubiquitous Infrastructure Sensor
Vehicular Ad-hoc Network

Thank you