



**Exponentiation:  $y = a^e \bmod n$**

<p><b>Right-to-left binary exponentiation</b></p> <p style="text-align: center;"><math>e = (e_{L-1}, e_{L-2}, \dots, e_1, e_0)_2</math></p> <pre> y = 1; s = a; for i=0 to L-1 {   if (e_i == 1)     y = y · s mod n;   s = s<sup>2</sup> mod n; }           </pre>	<p><b>Left-to-right binary exponentiation</b></p> <pre> y = 1; for i=L-1 downto 0 {   y = y<sup>2</sup> mod n;   if (e_i == 1)     y = y · a mod n; }           </pre>
---	--

---

---

---

---

---

---

---

---

**Scalar Multiplication:  $Y = k \cdot P$**

<p><b>Right-to-left binary scalar multiplication</b></p> <p style="text-align: center;"><math>k = (k_{L-1}, k_{L-2}, \dots, k_1, k_0)_2</math></p> <pre> Y = O; S = P; for i=0 to L-1 {   if (k_i == 1)     Y = Y + S;   S = 2S; }           </pre>	<p><b>Left-to-right binary scalar multiplication</b></p> <pre> Y = O; for i=L-1 downto 0 {   Y = 2Y;   if (k_i == 1)     Y = Y + P; }           </pre>
---	--

---

---

---

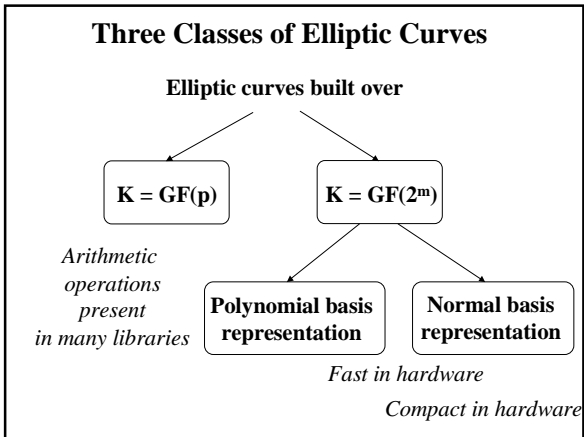
---

---

---

---

---




---

---

---

---

---

---

---

---

### Elliptic Curve over GF(p)

Set of solutions  $(x, y)$  to the equation

$$y^2 = x^3 + ax + b$$

where  $x, y \in \text{GF}(p)$

$$a, b \in \text{GF}(p) \quad 4a^3 + 27b^2 \neq 0 \pmod{p}$$

+ a special point called *the point at infinity*  $\mathcal{O}$

---

---

---

---

---

---

---

---

### Elliptic Curve over GF(2<sup>n</sup>)

#### Non-supersingular

Set of solutions  $(x, y)$  to the equation

$$y^2 + xy = x^3 + a_2x^2 + a_6$$

where  $x, y \in \text{GF}(2^n)$

$$a_2 \in \{0, 1\}, a_6 \in \text{GF}(2^n)$$

+ a special point called *the point at infinity*  $\mathcal{O}$

---

---

---

---

---

---

---

---

### Elliptic Curve over GF(2<sup>n</sup>)

#### Supersingular

Set of solutions  $(x, y)$  to the equation

$$y^2 + a_3y = x^3 + a_4x + a_6$$

where  $x, y \in \text{GF}(2^n)$

$$a_3, a_4, a_6 \in \text{GF}(2^n), a_3 \neq 0$$

+ a special point called *the point at infinity*  $\mathcal{O}$

---

---

---

---

---

---

---

---

**MOV (Menezes-Okamoto-Vanstone) attack**

- The *elliptic curve discrete logarithm problem* on  $E(\text{GF}(q))$  can be reduced to the *logarithm problem* over  $\text{GF}(q^k)$
- The *logarithm problem* over  $\text{GF}(q^k)$  can be solved in subexponential time using the **index calculus method**
- Value of  $k$ 
  - small ( $< 7$ ) for supersingular curves
  - large for non-supersingular curves
- **Non-supersingular curves more suitable for cryptographic transformations**

---

---

---

---

---

---

---

---

**Addition of two points on the elliptic curve over  $\text{GF}(p)$  (1)**

$$P = (x_1, y_1) \quad Q = (x_2, y_2)$$
$$R = P + Q = (x_3, y_3)$$

Case 1:

$$P + O = O + P = P$$

Case 2:

$$x_2 = x_1 \text{ and } y_2 = -y_1$$
$$P + Q = O$$
$$Q = -P$$

---

---

---

---

---

---

---

---

**Addition of two points on the elliptic curve over  $\text{GF}(p)$  (2)**

Case 3:

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda (x_1 - x_3) - y_1$$

where

Case 3a: if  $P \neq Q$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = (y_2 - y_1) (x_2 - x_1)^{-1}$$

Case 3b: if  $P = Q$

$$\lambda = \frac{3x_1^2 + a}{2y_1} = (3x_1^2 + a) (2y_1)^{-1}$$

---

---

---

---

---

---

---

---

**Addition of two points on the elliptic curve over GF(p) (3)**

Case 3a: if  $P \neq Q$

- 2 multiplications in GF(p)
- 1 squaring in GF(p)
- 1 inverse in GF(p)
- 6 subtractions in GF(p)

Case 3b: if  $P = Q$

- 2 multiplications in GF(p)
- 2 squarings in GF(p)
- 1 inverse in GF(p)
- 6 additions/subtractions in GF(p)

---

---

---

---

---

---

---

---

**Addition of two points on the non-supersingular elliptic curve over GF(2<sup>n</sup>)**

$$P = (x_1, y_1) \quad Q = (x_2, y_2)$$

$$R = P + Q = (x_3, y_3)$$

Case 1:

$$P + O = O + P = P$$

Case 2:

$$x_2 = x_1 \text{ and } y_2 = y_1 + x_1$$

$$P + Q = O$$

$$Q = -P$$

---

---

---

---

---

---

---

---

**Addition of two points on the non-supersingular elliptic curve over GF(2<sup>n</sup>)**

Case 3a: if  $P \neq Q$

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a_2$$

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

where

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2} = (y_1 + y_2) (x_1 + x_2)^{-1}$$

**Number of field operations:**

- 1 inversion in GF(2<sup>n</sup>)
- 2 multiplications in GF(2<sup>n</sup>)
- 1 squaring in GF(2<sup>n</sup>)

---

---

---

---

---

---

---

---

**Addition of two points on the non-supersingular elliptic curve over GF(2<sup>n</sup>)**

**Case 3b:** if P = Q

$$x_3 = a_6 (x_1^{-1})^2 + x_1^2$$

$$y_3 = x_1^2 + (x_1 + y_1 x_1^{-1}) x_3 + x_3$$

**Number of field operations:**

- 1 inversion in GF(2<sup>n</sup>)
- 3 multiplications in GF(2<sup>n</sup>)
- 2 squarings in GF(2<sup>n</sup>)

---

---

---

---

---

---

---

---

**Notation**

a	Multiplicand	$a_{k-1} a_{k-2} \dots a_1 a_0$
x	Multiplier	$x_{k-1} x_{k-2} \dots x_1 x_0$
p	Product (a · x)	$p_{2k-1} p_{2k-2} \dots p_2 p_1 p_0$

---

---

---

---

---

---

---

---

**Basic Multiplication Equations**

$$p = a \cdot x \quad x = \sum_{i=0}^{k-1} x_i \cdot 2^i$$

$$p = a \cdot x = \sum_{i=0}^{k-1} x_i \cdot 2^i =$$

$$= x_0 a 2^0 + x_1 a 2^1 + x_2 a 2^2 + \dots + x_{k-1} a 2^{k-1}$$

---

---

---

---

---

---

---

---

**Shift/Add Algorithms**

**Right-shift algorithm**

$$p = a \cdot x = x_0 a 2^0 + x_1 a 2^1 + x_2 a 2^2 + \dots + x_{k-1} a 2^{k-1} =$$

$$= (\dots((0 + \underbrace{x_0 a 2^k / 2 + x_1 a 2^k / 2 + \dots + x_{k-1} a 2^k / 2}_{k \text{ times}}) / 2 =$$

$$p^{(0)} = 0$$

$$p^{(j+1)} = (p^{(j)} + x_j a 2^k) / 2 \quad j=0..k-1$$

$$p = p^{(k)}$$

---

---

---

---

---

---

---

---

**Shift/Add Algorithms**

**Right-shift algorithm: multiply-add**

$$p^{(0)} = y 2^k$$

$$p^{(j+1)} = (p^{(j)} + x_j a 2^k) / 2 \quad j=0..k-1$$

$$p = p^{(k)}$$

$$= (\dots((y 2^k + \underbrace{x_0 a 2^k / 2 + x_1 a 2^k / 2 + \dots + x_{k-1} a 2^k / 2}_{k \text{ times}}) / 2 =$$

$$= y + x_0 a 2^0 + x_1 a 2^1 + x_2 a 2^2 + \dots + x_{k-1} a 2^{k-1} = y + a \cdot x$$

---

---

---

---

---

---

---

---

**Notation**

z Dividend  $z_{2k-1} z_{2k-2} \dots z_2 z_1 z_0$

d Divisor  $d_{k-1} d_{k-2} \dots d_1 d_0$

q Quotient  $q_{k-1} q_{k-2} \dots q_1 q_0$

s Remainder  $s_{k-1} s_{k-2} \dots s_1 s_0$   
( $s = z - dq$ )

---

---

---

---

---

---

---

---

### Basic Equations of Division

$$z = q d + s$$

$$s < d$$

---

---

---

---

---

---

---

---

### Unsigned Integer Division Overflow

Condition for no overflow:

$$z = q d + s < (2^k - 1) d + d = d 2^k$$

$$z = z_H 2^k + z_L < d 2^k$$

$$z_H < d$$

---

---

---

---

---

---

---

---

### Sequential Integer Division Basic Equations

$$s^{(0)} = z$$

$$s^{(j)} = 2 s^{(j-1)} - q_{k-j} (2^k d)$$

$$s^{(k)} = 2^k s$$

---

---

---

---

---

---

---

---

**Sequential Integer Division  
Justification**

$$\begin{aligned}
 s^{(1)} &= 2z - q_{k-1}(2^k d) \\
 s^{(2)} &= 2(2z - q_{k-1}(2^k d)) - q_{k-2}(2^k d) \\
 s^{(3)} &= 2(2(2z - q_{k-1}(2^k d)) - q_{k-2}(2^k d)) - q_{k-3}(2^k d) \\
 &\dots\dots\dots \\
 s^{(k)} &= 2(\dots 2(2(2z - q_{k-1}(2^k d)) - q_{k-2}(2^k d)) - q_{k-3}(2^k d) \dots \\
 &\quad - q_0(2^k d)) = \\
 &= 2^k z - (2^k d)(q_{k-1}2^{k-1} + q_{k-2}2^{k-2} + q_{k-3}2^{k-3} + \dots + q_02^0) = \\
 &= 2^k z - (2^k d)q = 2^k(z - dq) = 2^k s
 \end{aligned}$$

---

---

---

---

---

---

---

---

**Montgomery Modular Multiplication (1)**

$$C = A \cdot B \pmod{M} \quad A, B, M - k\text{-bit numbers}$$

Integer domain		Montgomery domain	
A	→	$A' = A \cdot 2^k \pmod{M}$	
B	→	$B' = B \cdot 2^k \pmod{M}$	
		$C' = \text{MP}(A', B', M) =$	
		$= A' \cdot B' \cdot 2^{-k} \pmod{M} =$	
		$= (A \cdot 2^k) \cdot (B \cdot 2^k) \cdot 2^{-k} \pmod{M} =$	
		$= A \cdot B \cdot 2^k \pmod{M}$	
$C = A \cdot B$	←	$C' = C \cdot 2^k \pmod{M}$	

---

---

---

---

---

---

---

---

**Montgomery Modular Multiplication (2)**

$$\begin{aligned}
 A &\longrightarrow A' \\
 A' &= \text{MP}(A, 2^k \pmod{M}, M) \\
 C &\longleftarrow C' \\
 C &= \text{MP}(C', 1, M)
 \end{aligned}$$

---

---

---

---

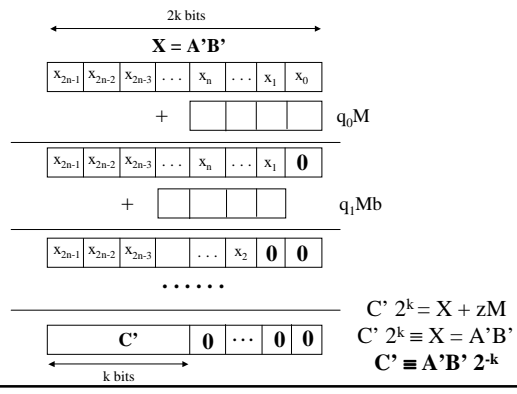
---

---

---

---

### Montgomery Modular Multiplication (3)




---



---



---



---



---



---



---