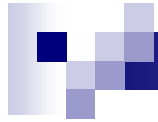


Zero-Value Point Attacks on Elliptic Curve Cryptosystems

Toru Akishita, Sony Corporation
Tsuyoshi Takagi, TU Darmstadt



Overview

- Elliptic Curve Cryptosystems (ECC)
- Power Analysis against ECC
- Goubin's Attack
- Zero-Value Point Attack
- Smart's Isogeny Defense

Elliptic Curve

- Elliptic curve on binary field

$$E : y^2 + xy = x^3 + ax^2 + b \quad (a, b \in GF(2^n), b \neq 0)$$

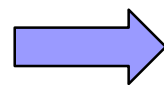
- Elliptic curve on prime field

$$E : y^2 = x^3 + ax + b \quad (a, b \in GF(p), 4a^3 + 27b^2 \neq 0)$$

$$x, y \in GF(p)$$

All points satisfying E
and infinity point O

$$E(GF(p))$$



Abelian group
by the following addition

O : group identity

Addition Formulae on EC

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

■ EC Doubling (ECDBL)

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

$$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1 \\ y_3 = \left(\frac{3x_1^2 + a}{2y_1} \right) (x_1 - x_3) - y_1 \end{cases}$$

■ EC Addition (ECADD)

$$P_3 = P_1 + P_2 \quad (P_1 \neq P_2)$$

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \\ y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) - y_1 \end{cases}$$

Affine coordinate (x, y) \Rightarrow Jacobian coordinates $(X : Y : Z)$

$$x = X/Z^2, y = Y/Z^3$$

Addition Formulae on EC (Jacobian Coordinates)

$$P_1 = (X_1 : Y_1 : Z_1), P_2 = (X_2 : Y_2 : Z_2), P_3 = (X_3 : Y_3 : Z_3)$$

■ ECDBL

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

$$\begin{cases} X_3 = T, \\ Y_3 = -8Y_1^4 + M(S - T), \\ Z_3 = 2Y_1Z_1, \end{cases}$$

$$S = 4X_1Y_1^2, M = 3X_1^2 + aZ_1^4$$

$$T = -2S + M^2$$

■ ECADD

$$P_3 = P_1 + P_2 \quad (P_1 \neq P_2)$$

$$\begin{cases} X_3 = -H^3 - 2U_1H^2 + R^2, \\ Y_3 = -S_1H^3 + R(U_1H^2 - X_3), \\ Z_3 = Z_1Z_2H, \end{cases}$$

$$U_1 = X_1Z_2^2, U_2 = X_2Z_1^2, S_1 = Y_1Z_2^3$$

$$S_2 = Y_2Z_1^3, H = U_2 - U_1, R = S_2 - S_1$$

Scalar Multiplication on EC

■ Scalar Multiplication dP

□ Binary Method $P \in E$, $d = (d_{n-1} \Lambda d_0)_2$, $d_{n-1} = 1$

1. $Q \leftarrow P$

binary representation

2. For $i = n-2$ downto 0

$Q \leftarrow 2Q$

ECDBL

if $d_i = 1$, $Q \leftarrow Q + P$

ECADD

3. Return Q

Ex. $51P = (110011)_2 P$

$P \xrightarrow{D} 2P \xrightarrow{A} 3P \xrightarrow{D} 6P \xrightarrow{D} 12P \xrightarrow{D} 24P \xrightarrow{A} 25P$
 $\xrightarrow{D} 50P \xrightarrow{A} 51P$



Power Analysis

- **Simple Power Analysis (SPA)**

Observe the power consumption of devices in a single computation and detect the secret key

- **Differential Power Analysis (DPA)**

Observe many power consumptions and analyze these information together with statistic tools

SPA against ECC (Coron 1999)

Binary method

1. $Q \leftarrow P$
2. For $i = n-2$ downto 0
 $Q \leftarrow 2Q$ ECDBL
 $\text{if } d_i = 1, Q \leftarrow Q + P$ ECADD
3. Return Q

■ ECDBL

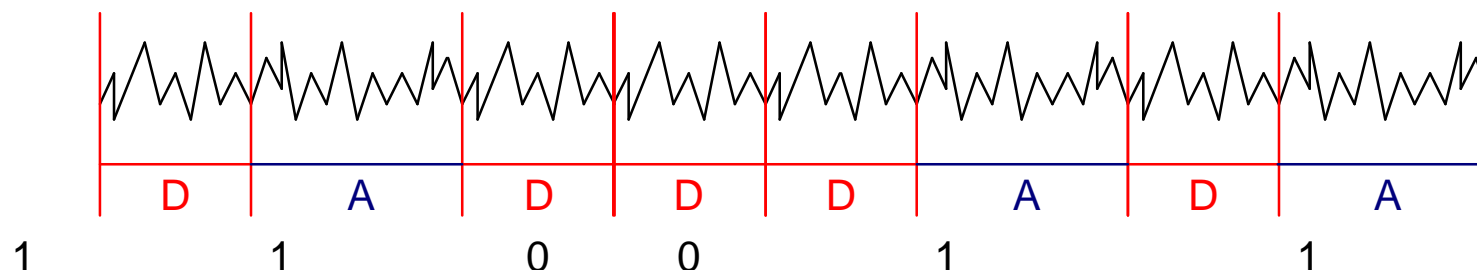


■ ECADD



Ex. $51P = (110011)_2 P$

Attacker can guess bit information



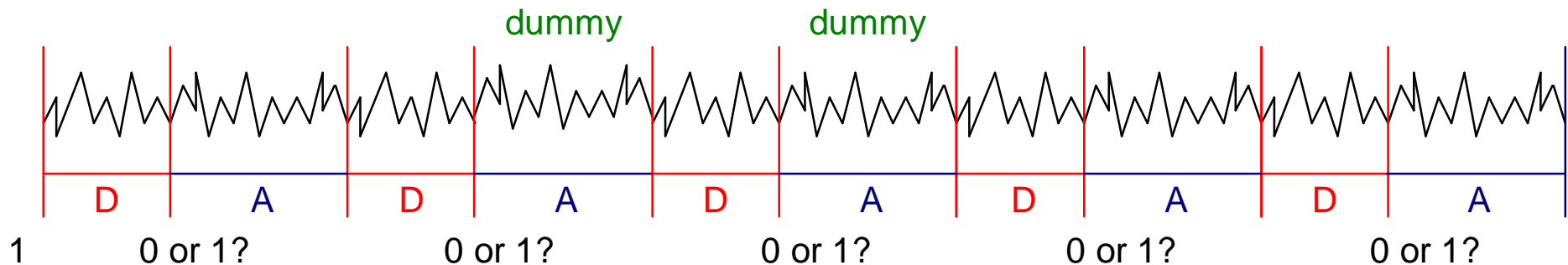
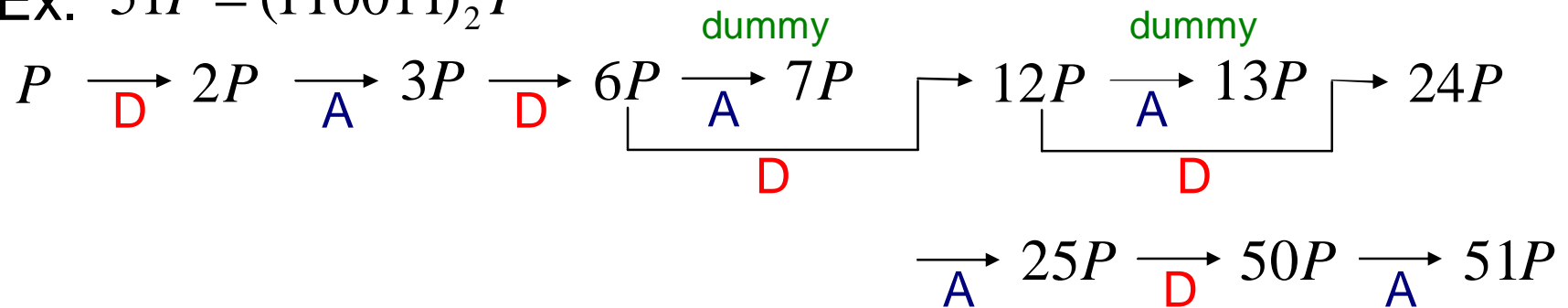


SPA Countermeasure (Coron 1999)


- Scalar Multiplication dP $P \in E, d = (d_{n-1} \Lambda d_0)_2$
 - Double-and-add-always method
 1. $Q \leftarrow P$
 2. For $i = n - 2$ downto 0
 - $Q[0] \leftarrow 2Q$ ECDBL
 - $Q[1] \leftarrow Q[0] + P$ ECADD
 - $Q \leftarrow Q[d_i]$
 3. Return Q

Double-and-add-always method (Coron 1999)

Ex. $51P = (110011)_2 P$

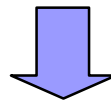


Attacker cannot guess bit information



DPA against Double-and-add-always method (Coron 1999)

- d is fixed and the attacker can choose P
ECIES, single-pass ECDH
- Power consumption of double-and-add-always method for each input looks same, but is slightly different.
- Power consumption is correlated to any bit of processing point.



Randomize the representation of points

- Coron's 3rd countermeasure
- Joye-Tymen countermeasure



DPA Countermeasure (Coron 1999)

- Randomize point representation in Jacobian coordinates
- Scalar Multiplication dP
 1. Choose randomly $r \in [1, p-1]$
 2. $Q \leftarrow (r^2 x_p : r^3 y_p : r)$
 3. Compute $Q = dP$
 4. Return Q



DPA Countermeasure (Joye-Tymen 2001)

- Use a random isomorphic curve to the original curve
- Scalar multiplication dP
 1. Choose randomly $r \in [1, p-1]$
 2. $a' = r^4 a, b' = r^6 b$ and $P' = (r^2 x_p, r^3 y_p)$
 3. Compute $Q' = dP'$ on $E' : y^2 = x^3 + a'x + b'$
 4. $x_Q = r^{-2} x_{Q'}, y_Q = r^{-3} y_{Q'}$
 5. Return $Q = (x_Q, y_Q)$

Goubin's Attack (Goubin 2003)

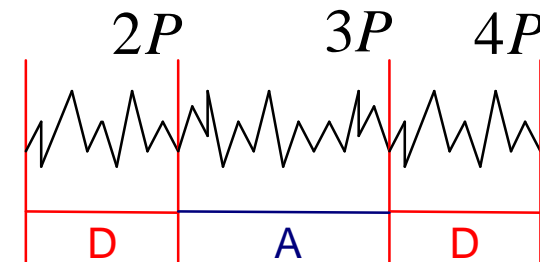
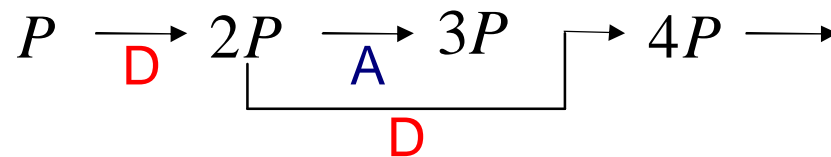
- Cannot randomize the points $(x,0)$ and $(0,y)$

- $(x,0) \rightarrow (r^2x : 0 : r)$, $(0,y) \rightarrow (0 : r^3y : r)$

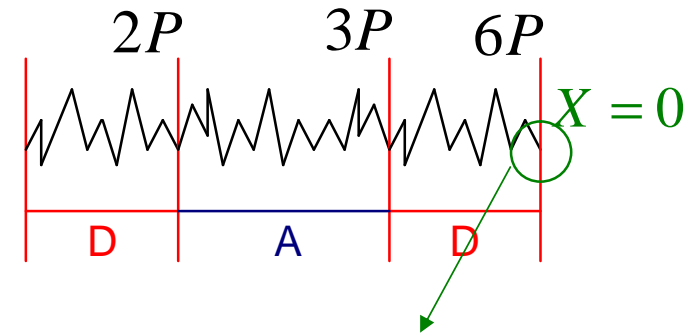
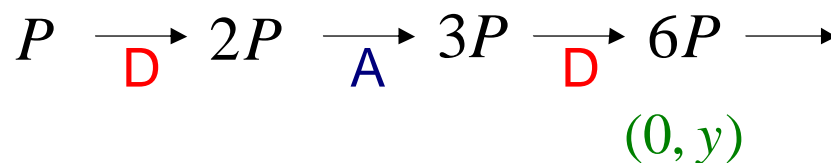
- Assume $d_{n-2} = 1$

- Input $P = (6^{-1} \bmod \#E)(0, y)$

$d_{n-2} = 0$



$d_{n-2} = 1$



irregular power consumption



Condition of Goubin's Attack

- point $(x, 0)$ **Order is 2**
 - Not exist in elliptic curve $E : y^2 = x^3 + ax + b$ of prime order.
 - If exist, the input can be discarded.
- point $(0, y)$
 - $y^2 = b \Rightarrow b$ is quadratic residue modulo p

If b is random, this probability is about 50%



Goubin's Points on Standard Curves

■ SECG Curves

	$(0, y)$
SECG secp112r1	-
SECG secp128r1	0
SECG secp160r1	0
SECG secp160r2	0
SECG secp192r1	0
SECG secp224r1	-
SECG secp256r1	0
SECG secp384r1	0
SECG secp521r1	0



ZVP Attack

- Zero-value point attack
- Generalization of Goubin's attack
 - Goubin's attack pays attention to only representation of processing points.
 - We consider that intermediate values of addition formulae are equal to 0.
 - If the point has no zero-value coordinate, the intermediate values might take zero.

ZVP in ECDBL

■ ECDBL $P_3 = 2P_1$

$$P_1 = (X_1 : Y_1 : Z_1), P_3 = (X_3 : Y_3 : Z_3)$$

$$3x_1^2 + a = 0$$

$$\begin{cases} X_3 = T, \\ Y_3 = -8Y_1^4 + M(S - T), \\ Z_3 = 2Y_1Z_1, \end{cases}$$

$$S = 4X_1Y_1^2, M = \underline{3X_1^2 + aZ_1^4}$$

$$T = -2S + M^2$$

$$\begin{aligned} & 3X_1^2 + aZ_1^4 \\ &= Z_1^4 \left(3(X_1/Z_1^2) + a \right) \\ &= Z_1^4 \underline{(3x_1^2 + a)} \\ & M = 0 \end{aligned}$$

ZVP Attack

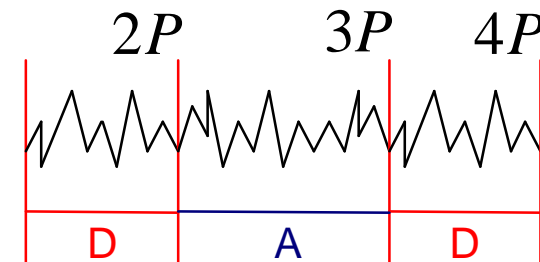
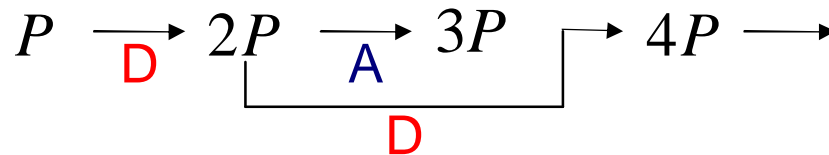
- $P_0 = (x, y)$ that satisfy $3x^2 + a = 0$
- Assume $d_{n-2} = 1$
 - Input $P = (3^{-1} \bmod \#E)P_0$

$$\begin{cases} X_3 = T, \\ Y_3 = -8Y_1^4 + M(S - T), \\ Z_3 = 2Y_1Z_1, \end{cases}$$

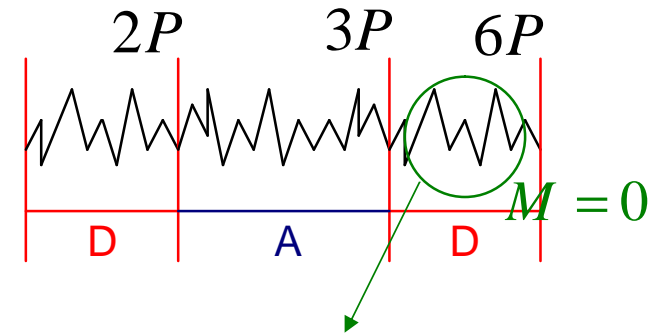
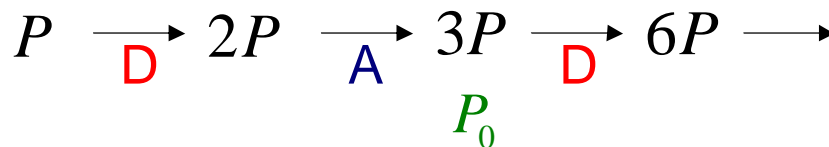
$$S = 4X_1Y_1^2, M = 3X_1^2 + aZ_1^4$$

$$T = -2S + M^2$$

$$d_{n-2} = 0$$



$$d_{n-2} = 1$$



irregular power consumption



ZVP in ECDBL

- (ED1) $3x^2 + a = 0$
- (ED2) $5x^4 + 2ax^2 - 4bx + a^2 = 0$
- (ED3) the order of P is equal to 3 trivial
- (ED4) $x = 0$
- (ED5) $y = 0$ Goubin's point

ZVP in ECADD[J]

■ ECADD[J] $P_3 = P_1 + P_2$

$$P_1 = (X_1 : Y_1 : Z_1), P_2 = (X_2 : Y_2 : Z_2), P_3 = (X_3 : Y_3 : Z_3)$$

$$\begin{cases} X_3 = \underline{-H^3 - 2U_1H^2 + R^2}, \\ Y_3 = -S_1H^3 + R(U_1H^2 - X_3), \\ Z_3 = Z_1Z_2H, \end{cases}$$

$$U_1 = X_1Z_2^2, U_2 = X_2Z_1^2, S_1 = Y_1Z_2^3$$

$$S_2 = Y_2Z_1^3, H = U_2 - U_1, R = S_2 - S_1$$


$$\begin{aligned} P_1 &= cP, P_2 = P \\ &= -H^3 - 2U_1H^2 \\ &= -H^2(U_1 + U_2) \\ &= \underline{-H^2Z_1^2Z_2^2(x_1 + x_2)} \end{aligned}$$

division polynomial
(can solve for only small c)

ZVP on Standard Curves

■ SECG Curves

	$(0, y)$	(ED1)	(ED2)
SECG secp112r1	-	0	0
SECG secp128r1	0	-	-
SECG secp160r1	0	-	-
SECG secp160r2	0	-	0
SECG secp192r1	0	0	0
SECG secp224r1	-	-	0
SECG secp256r1	0	-	0
SECG secp384r1	0	0	-
SECG secp521r1	0	0	-



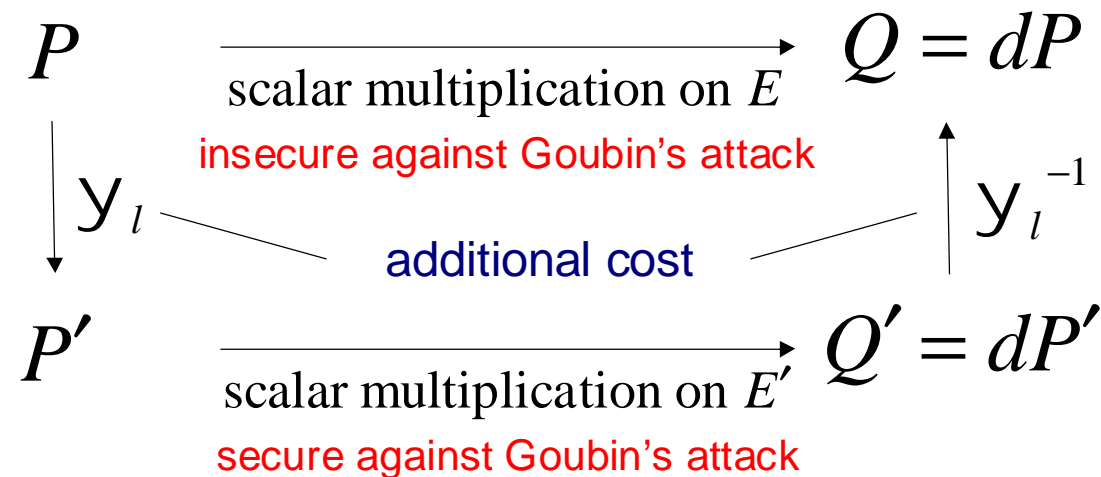
ZVP attack to other classes

- We can apply ZVP attacks to
 - Deterministic addition chain
 - Montgomery-type Method
Ex. $x^2 \pm a = 0$
 - Curves over $GF(2^n)$
- ZVP attack depends on implementation

Smart's Isogeny Defense (Smart 2003)

- Countermeasure against Goubin's attack

- Isogeny of degree l $y_l : E \rightarrow E'$
 E has $(0, y)$ E' has no $(0, y)$



additional cost depends on degree l



Smart's Isogeny Defense against Goubin's attack

efficient curve $a = -3$

	Minimal degree	Preferred degree
SECG secp112r1	1	1
SECG secp128r1	7	7
SECG secp160r1	13	13
SECG secp160r2	19	41
SECG secp192r1	23	73
SECG secp224r1	1	1
SECG secp256r1	3	11
SECG secp384r1	19	19
SECG secp521r1	5	5

Smart's Isogeny Defense against ZVP attack

■ (ED1) $3x^2 + a = 0$

efficient curve $a = -3$

	Minimal degree	Preferred degree
SECG secp112r1	7	> 107
SECG secp128r1	7	7
SECG secp160r1	13	13
SECG secp160r2	19	41
SECG secp192r1	23	> 107
SECG secp224r1	1	1
SECG secp256r1	3	23
SECG secp384r1	31	> 107
SECG secp521r1	5	5



Conclusion

- We propose ZVP attacks that is generalization of Goubin's attack.
- Our attack is applicable to EC that is secure against Goubin's attack.
- Smart's isogeny defense require higher isogeny degree for some curves.