Cryptographic Approach to Enhance the Security Against Recent Threats

Atsuko Miyaji

JAIST

Thank you very much for giving an opportunity to talk.
Hope this opportunity becomes the first step of good collaboration between Taiwan and Japan researchers.

Outline

This talk

Cryptographic Approach to Enhance the Security Against Recent Real Threats.

1. Information Security for Cloud Computing
2. Public key cryptosystems
   1. Elliptic Curve Cryptosystems (ECC)
   2. Dominant factor of ECC, security & efficiency
3. Scalar Multiplication
4. Side Channel Attack, real recent threats
5. Approach to Achieve a Secure and Efficient cryptosystems (our new results)
6. Conclusion

Information Security for Cloud Computing

Customers are both excited and nervous at the prospects of Cloud Computing.

Why?: Customers are also very concerned about the risks of Cloud Computing if not properly secured.

Cloud Security Alliance, Top Threats to Cloud Computing V1.0

How to reduce the risk?

Confidentiality: Protect a data from an outsider.
Integrity: Guarantee a data consistency.
Access control: Control data for users without right.

Information security

Encryption, Signature (Authentication)

Public Key Cryptosystems

In this talk, we focus on public key cryptosystems.

Outline 2

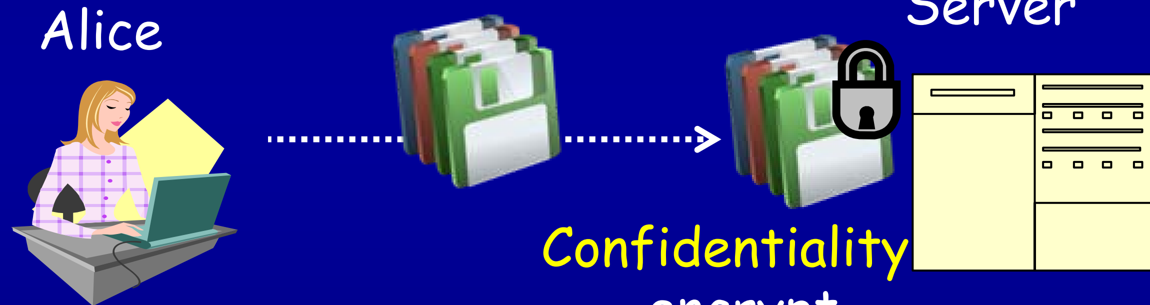
1. Information Security for Cloud Computing
2. Public key cryptosystems
    1. Elliptic Curve Cryptosystems (ECC)
    2. Dominant factor of ECC, security & efficiency
3. Scalar Multiplication
4. Side Channel Attack, real recent threats
5. Approach to Achieve a Secure and Efficient cryptosystems (our new results)
6. Conclusion

Principle of Public Key Cryptosystems

Main Features

・Encryption key≠Decryption key
⇒Encryption/Decryption key is published/ kept secretly (public key/secret key)

⇒encryption (confidentiality) + signature (integrity/access control) + are achieved.



Security Bases

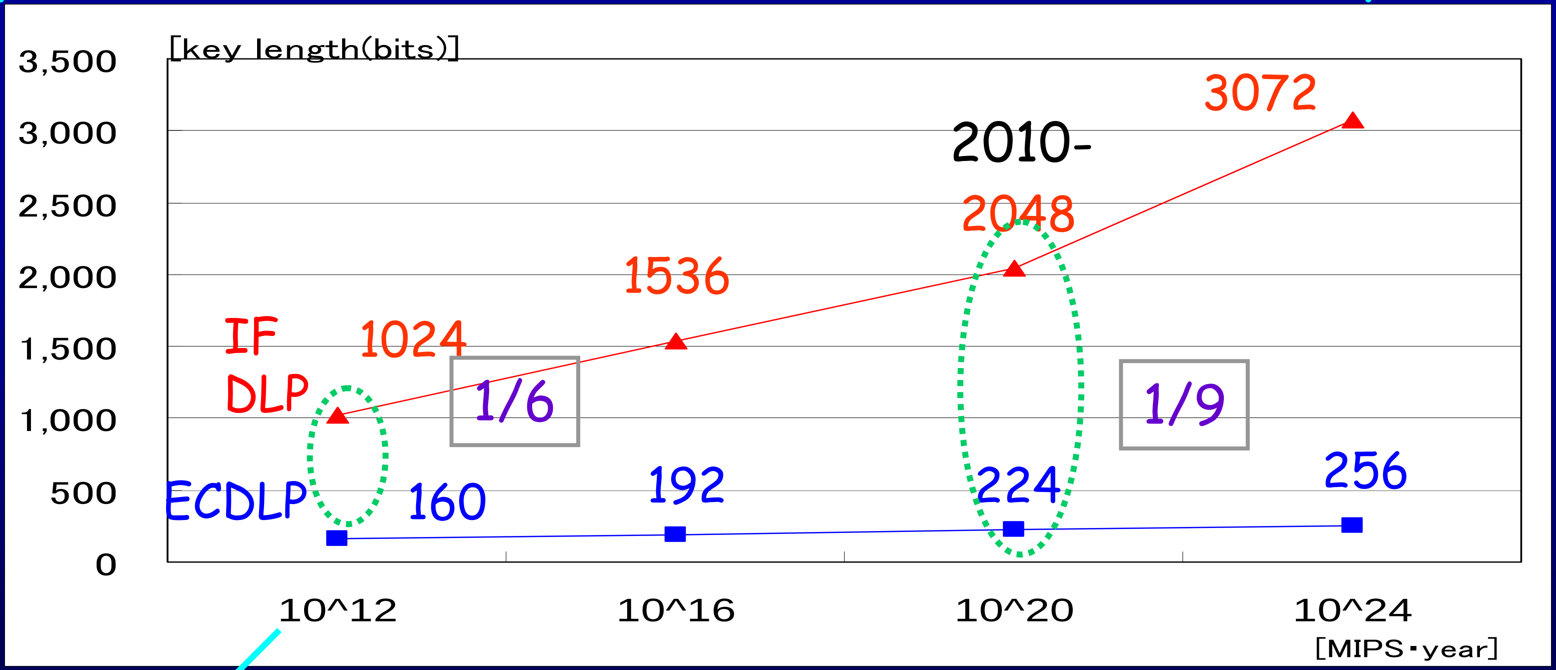
Integer Factorization Problem (IF, '78)
Discrete Logarithm Problem (DLP, '85)
Elliptic Curve Discrete Logarithm Problem (ECDLP, '86)

Security Comparison between IF, DLP, and ECDLP

- DLP&IF: a sub-exponential time faster than exhaustive search $O(\exp\{(\log\log p)^{2/3}(\log p)^{1/3}\})$
- ECDLP: a square-root time (exhaustive search), $O(p^{1/2})$

→ ECDLP is more efficient than DLP/IF. (more and more)

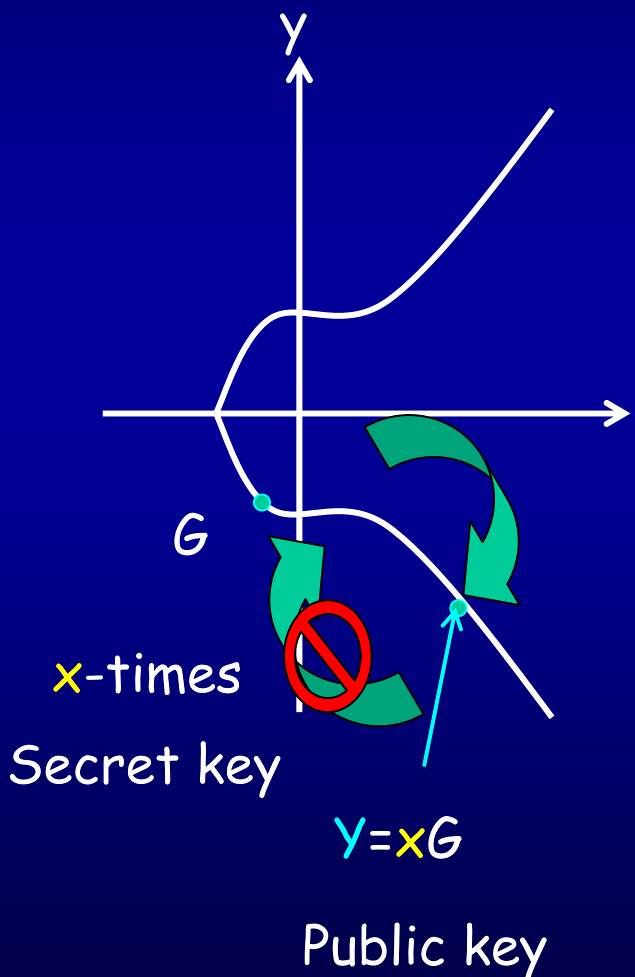
Key size for IF, DLP, ECDLP to achieve a security level.



Security level 10^2MIPS PC × 10^{10} year

What is Elliptic Curve Cryptosystems -Elliptic Curve Discrete Logarithm Problem-

A non-degenerate cubic curve
$E: y^2 = x^3 + ax + b \ (a, b \in F_p (p>3),\ 4a^3+27b^2 \neq 0)$



Easily-executed addition is defined.
→ E is a group. $\infty = (\infty, \infty)$ is a zero.

$A + B = (x_3, y_3) \quad (A \neq B)$
$x_3 = ((y_2-y_1)/(x_2-x_1))^2 - x_1 - x_2$
$y_3 = (y_2-y_1)(x_2-x_1)(x_1-x_3)-y_1$

Finite abelian group.

$E(F_p)$, F_p-rational points,
$=\{(x,y) \in F_p \times F_p \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$

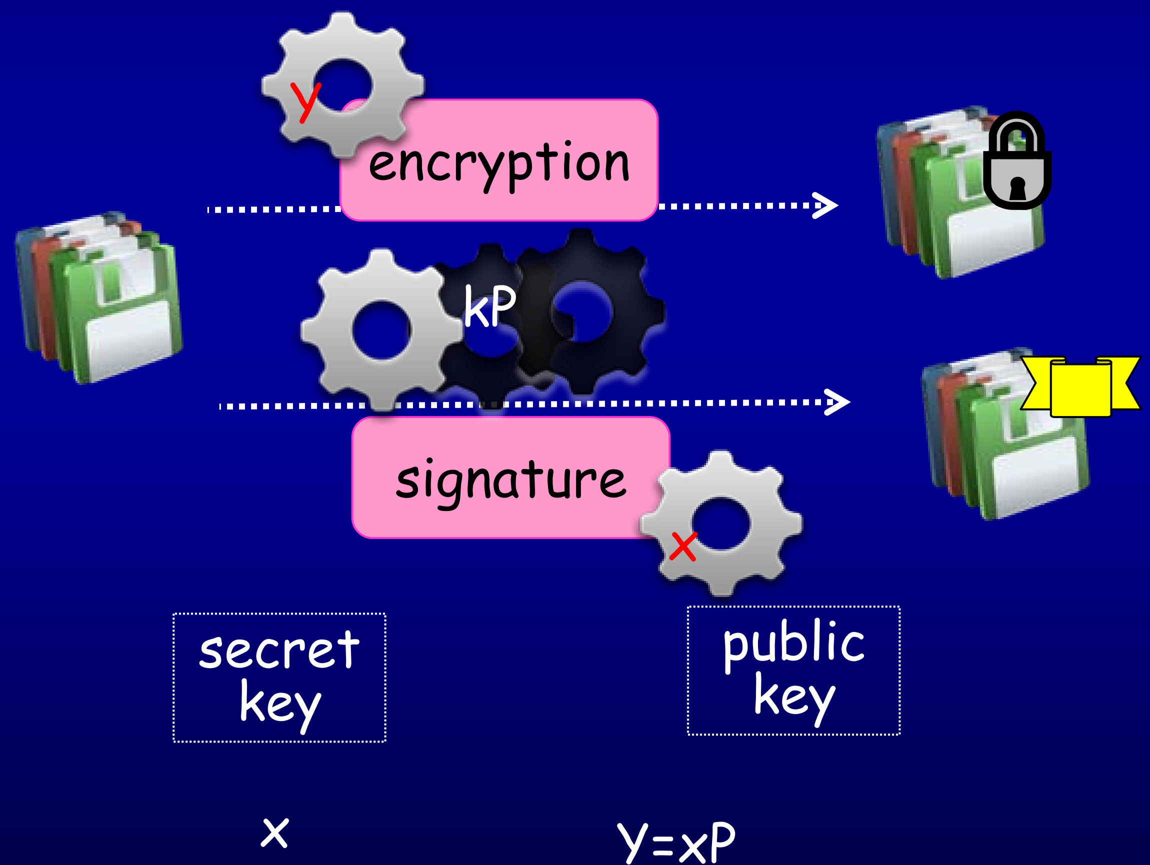
ECDLP

For given $G, Y \in E(F_p)$, find x such that $Y = G + \cdots + G = xG$

ECC (Elliptic Curve Cryptosystems) is based on ECDLP.

Dominant Computation of ECC

- Dominant security/computation of ECC is a scalar multiplication of kP for a secret k and given P.



Outline 3

1. Information Security for Cloud Computing
2. Public key cryptosystems
3. Elliptic Curve Cryptosystems
4. Scalar Multiplication
5. Side Channel Attack
6. Approach to Achieve a Secure and Efficient cryptosystems
7. Conclusion

Scalar Multiplications -how to efficient & secure-

ECC consists of
scalar multiplication kP.

$$kP = \underbrace{P + \cdots + P}_{k \text{ times}}$$

Performance of ECC: depends on (memory, comp) of kP

→efficient scalar multiplication is needed!

Security of ECC: also depends on a secrecy of k in kP

<Theoretically> Solve k from kP means "solve ECDLP".

<Practically> (side channel attack)
Solve k during execution of kP by side channel information.

→secure scalar multiplication is needed!

General Approach to compute kP

行政院國家科學委員會 National Science Council
科学技術振興機構 Japan Science and Technology Agency

kP = 1 0 1 1 0 0 ··· 1 P (in binary)

Scalar Multiplication

Left-to-Right binary Alg

L → R

k = 27 = 1 1 0 1 1

2(2(2(2P + P))+P) +P

Repeat: Y=2Y+P

Addition chains

Right-to-Left binary Alg

L ← R

k = 27 = 1 1 0 1 1

$((P + 2P) + 2^3P) + 2^4P$

Repeat: $2 \cdot 2^jP$, $Y = Y + 2^jP$

Addition formulae

Addition (Add), Doubling (Dbl)

Field Arithmetic

Multiplication (M), Inversion (S)

Layered Model for Scalar Multiplication

Addition-chains Binary, Signed binary, window method	# Dbl + # Add is different
Addition formulae Dbl Add	
Coordinates Affine (A) Jacobian (J)	#M+#I+#I is different.
Field arithmetic Multiplication (M) Square (S) Inversion (I)	Computation cost $I \gg M > S$

All layers have different methods with different computational cost.

→ We investigate secure and efficient scalar multiplication.

Outline 4

1. Information Security for Cloud Computing
2. Public key cryptosystems
3. Elliptic Curve Cryptosystems
4. Scalar Multiplication
5. Side Channel Attack
6. Approach to Achieve a Secure and Efficient cryptosystems
7. Conclusion

Scalar Multiplication

Left-to-Right binary algorithm

Input P, $k=(k_{n-1}, \cdots, k_0)$, Output kP

$R_0 = P$, $R_2 = P$
For i = n-2 to 0
  $R_0 = 2R_0$
  if $k_i = 1$ then $R_0 = R_0 + R_2$
Output R_0

Add only if k_i=1

Binary algorithm has branch instruction depends on secret-key bit k.

It is subject to side-channel attacks.

Side Channel Attack

Side channel attack

Obtain the secret of k by observing side channel info:
Computing time, power consumption traces, etc.

SPA (Single Power Analysis) :

Obtain the secret of k by observing the single power analysis.

→ regular execution without branch for a condition of k.

Safe error attack :

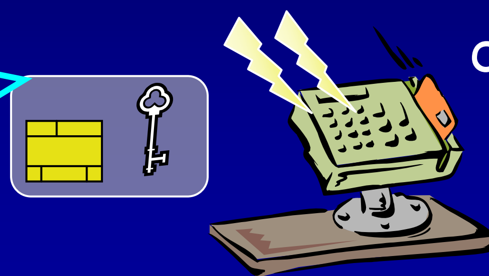
Obtain the secret by inducing a fault during the execution of kP and checking whether the targeted instruction is fake.

→ execution without dummy operation

Simple Power Analysis (SPA)

Use an instruction dependent of a secret k during kP
→ Eliminate any branch instruction of kP.

$E, E(F_p) \ni P$
x, k: secret key



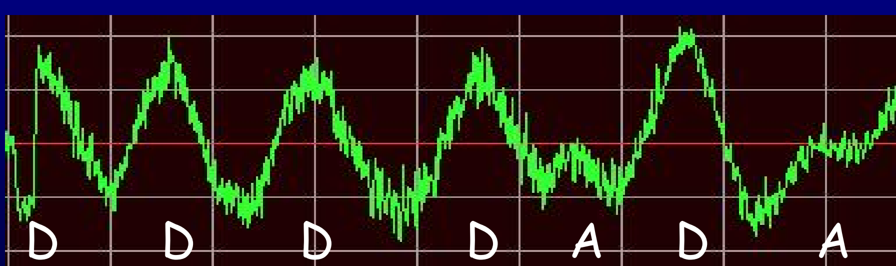
m → $R = kP = (R_x, R_y)$
$s = (m + x R_x)/k$

Signature generation

Binary algorithm ...ys algorithm

$R_0 = P, R_2 = P$
For i = n-2 to 0
$R_0 = 2R_0$
$b = {}^{c}k_i;\ R_b = R_b + R_2$
Output R_0

If power consumption is measured, then
branch instruction reveals the corresponding secret-key bit.



k = 1 0 0 0 1 0 1

Branch instruction dependent on each secret-key bit.

Safe Error Attach (SEA)

- One of fault attacks. Give just 1 fault.
- Distinguish the target bit = 0 or 1 by checking the output is correct or not.

double-and-add-always algorithm secure against SPA.

$R_0 = P$, $R_2 = P$
For $i = n-2$ to 0
  $R_0 = 2R_0$
  $b = \neg k_i$; $R_b = R_b + R_2$
Output R_0

Dummy instruction becomes safe error for 1 fault.

Addition in $k_i=0$ is dummy.

Safe error

$k_i=0$

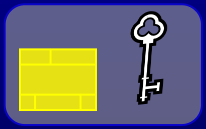
$R_0 = 2R_0$
$R_1 = R_1 + R_2$
Output R_0

Insert 1 error

Real error

$k_i=1$

$R_0 = 2R_0$
$R_0 = R_0 + R_2$
Output R_0



Outline 5

1. Information Security for Cloud Computing
2. Public key cryptosystems
3. Elliptic Curve Cryptosystems
4. Scalar Multiplication
5. Side Channel Attack
6. Approach to Achieve a Secure and Efficient cryptosystems
7. Conclusion

Secure Scalar Multiplication

Secure scalar multiplication algorithm against SPA (Single Power Analysis) and safe error attack are:

1. regular execution without branch for a condition of k.
2. do not insert any dummy operation

L→R Montgomery Algorithm

$R_0 = O, R_1 = P$
For i = n-2 to 0
  $b = k_i;\ R_{1-b} = R_{1-b} + R_b$
  $R_b = 2R_b$
Output R_0

R→L Joye's Algorithm

$R_0 = O,\ R_1 = P$
For i = 0 to n - 1 **do**
  $b = k_i$
  $R_{1-b} = 2R_{1-b} + R_b$
Output R_0

We have further improved those secure Montgomery & Joye's alg by introducing new formulae.

Improvement of addition formulae

行政院國家科學委員會 National Science Council

JST 科学技術振興機構 Japan Science and Technology Agency

Operation	|p|	Cost(S=0.8M)	
Co-Z Add	6	5M + 2S	6.6
(X, Y)-only co-Z Add	5	4M + 2S	5.6
Jacobian Add	7	11M + 5S	15
Our Conjugate co-Z Add	7	6M + 3S	8.4
(X, Y)-only conjugate co-Z Add	6	5M + 3S	7.4
Co-Z Dbl with update	6	1M + 5S	5
(X, Y)-only co-Z Dbl	5	1M + 5S	5
Jacobian Dbl	6	2M + 8S	8.4
Co-Z Tpl with update	6	6M + 7S	11.6
(X, Y)-only co-Z Tpl	5	5M + 7S	10.6
Jacobian Tpl	9	6M + 10S	14
Our Co-Z Dbl-Add	8	9M + 7S	14.6
(X, Y)-only co-Z Dbl-Add	6	8M + 6S	12.8
Co-Z conjugate-Add-Add	8	9M + 7S	14.6
(X, Y)-only co-Z conjugate-Add-Add with update	6	8M + 6S	12.8

15

Improvement of Scalar Multiplication

	Algorithm	Main op.	$\lvert p \rvert$	Comp cost/bit (M,S)	Comp cost/bit (M)	
R L	Basic Joye's double-add	DA	10	13M + 8S	19.4	
	Ours:Co-Z Joye's double-add	ZDAU	8	9M + 7S	14.6	75%
L ↓ R	Basic Montgomery	DBL+ADD	8	12M + 13S	22.4	
	Ours: co-Z Montgomery	ZDAU	8	9M + 7S	14.6	65%
	Ours:(X, Y)-only co-Z Montg	ZACAU′	6	8M + 6S	12.8	88%

Conclusion

1. We have investigated elliptic curve cryptosystems as the most attractive public key cryptosystems.
   1. A scalar multiplication is a dominant factor for both security and efficiency.
2. We have focused on Side Channel Attacks as recent threats and shown various attacks.
3. We have shown some secure ECC to avoid side channel attack.
4. Finally, we have presented our results that improve a secure scalar multiplication.