Automatic Generation of HCCA Resistant Scalar Multiplication Algorithm by Proper Sequencing of Field Multiplier Operands

Poulami Das, **Debapriya Basu Roy** and, Debdeep Mukhopadhyay
Indian Institute of Technology Kharagpur

Outline

- Introduction

Outline

- Introduction
- Motivation

Outline

- Introduction
- Motivation
- Horizontal Collision Correlation Analysis (HCCA)

Outline

- Introduction
- Motivation
- Horizontal Collision Correlation Analysis (HCCA)
- Asymmetric Leakage of Long Integer Field Multiplication

Outline

- Introduction
- Motivation
- Horizontal Collision Correlation Analysis (HCCA)
- Asymmetric Leakage of Long Integer Field Multiplication
- Countermeasure Design

Outline

- Introduction
- Motivation
- Horizontal Collision Correlation Analysis (HCCA)
- Asymmetric Leakage of Long Integer Field Multiplication
- Countermeasure Design
- Conclusion

Introduction

- Cryptography has emerged as the practice or study of securing communications against third parties called adversaries.

Introduction

- Cryptography has emerged as the practice or study of securing communications against third parties called adversaries.
- Public Key Cryptography (PKC) was introduced to address key issues of Key Distribution Problem and Digital Signature Verification problems.

Introduction

- Cryptography has emerged as the practice or study of securing communications against third parties called adversaries.
- Public Key Cryptography (PKC) was introduced to address key issues of Key Distribution Problem and Digital Signature Verification problems.
- The two most widely used primitives of PKC are RSA and Elliptic Curve Cryptography.

Introduction

- Cryptography has emerged as the practice or study of securing communications against third parties called adversaries.
- Public Key Cryptography (PKC) was introduced to address key issues of Key Distribution Problem and Digital Signature Verification problems.
- The two most widely used primitives of PKC are RSA and Elliptic Curve Cryptography.
- Elliptic Curve Cryptography (ECC) has emerged as a strong alternative to RSA due to its property of more security per key bit.

- ECC scalar multiplication algorithm is mathematically secure against the ECDLP problem.

- ECC scalar multiplication algorithm is mathematically secure against the ECDLP problem.
- However ECC algorithms once implemented, the implementations suffer from side-channel leakage such as power (EM) leakage, timing leakage, acoustic leakage etc.

- ECC scalar multiplication algorithm is mathematically secure against the ECDLP problem.
- However ECC algorithms once implemented, the implementations suffer from side-channel leakage such as power (EM) leakage, timing leakage, acoustic leakage etc.

Motivation

- ECC scalar multiplication algorithm is mathematically secure against the ECDLP problem.
- However ECC algorithms once implemented, the implementations suffer from side-channel leakage such as power (EM) leakage, timing leakage, acoustic leakage etc.
- Ladder, Unified Algorithm, Atomic formula: Countermeasure against Simple Power Analysis

Motivation

- ECC scalar multiplication algorithm is mathematically secure against the ECDLP problem.
- However ECC algorithms once implemented, the implementations suffer from side-channel leakage such as power (EM) leakage, timing leakage, acoustic leakage etc.
- Ladder, Unified Algorithm, Atomic formula: Countermeasure against Simple Power Analysis
- Scalar Blinding, Point Coordinate Randomization: Countermeasure against Differential Power Analysis

Motivation

- Horizontal Attacks are special attacks which threatens a SPA as well as DPA resistant implementation.

Motivation

- Horizontal Attacks are special attacks which threatens a SPA as well as DPA resistant implementation.
- It involves few (single) number of traces to break the entire secret key.

Motivation

- Horizontal Attacks are special attacks which threatens a SPA as well as DPA resistant implementation.
- It involves few (single) number of traces to break the entire secret key.
- Thus imposes a serious threat to ECC implementations.

Horizontal Collision Correlation Analysis (HCCA)

- First seminal work in Horizontal Attacks was Big Mac Attack by Walter et. al.

- First seminal work in Horizontal Attacks was Big Mac Attack by Walter et. al.
- Big Mac Analysis followed several flavors of Horizontal attacks on the RSA-based exponentiation algorithms.

Horizontal Collision Correlation Analysis (HCCA)

- First seminal work in Horizontal Attacks was Big Mac Attack by Walter et. al.
- Big Mac Analysis followed several flavors of Horizontal attacks on the RSA-based exponentiation algorithms.
- Horizontal Collision Correlation Analysis or HCCA by Bauer et. al. put forward the idea of Horizontal Attacks in case of elliptic curve cryptography.

Horizontal Collision Correlation Analysis (HCCA)

- First seminal work in Horizontal Attacks was Big Mac Attack by Walter et. al.
- Big Mac Analysis followed several flavors of Horizontal attacks on the RSA-based exponentiation algorithms.
- Horizontal Collision Correlation Analysis or HCCA by Bauer et. al. put forward the idea of Horizontal Attacks in case of elliptic curve cryptography.
- HCCA threatens an atomic scheme ECC algorithm or unified ECC algorithm (Edward curve) with SPA, DPA resistance.

- HCCA is based on underlying field multiplications that constitute ECC point addition and doubling.

- HCCA is based on underlying field multiplications that constitute ECC point addition and doubling.
- It is based on the following assumption: *The adversary can detect when a pair of field multiplications have at least one operand in common*

Horizontal Collision Correlation Analysis (HCCA)

- HCCA is based on underlying field multiplications that constitute ECC point addition and doubling.
- It is based on the following assumption: *The adversary can detect when a pair of field multiplications have at least one operand in common*
- If A, B, C and D be field multiplications considered without loss of generality, then following pairs can be defined

Horizontal Collision Correlation Analysis (HCCA)

- HCCA is based on underlying field multiplications that constitute ECC point addition and doubling.
- It is based on the following assumption: *The adversary can detect when a pair of field multiplications have at least one operand in common*
- If A, B, C and D be field multiplications considered without loss of generality, then following pairs can be defined
- $(A \times B, A \times B)$: sharing both operands

- HCCA is based on underlying field multiplications that constitute ECC point addition and doubling.
- It is based on the following assumption: *The adversary can detect when a pair of field multiplications have at least one operand in common*
- If A, B, C and D be field multiplications considered without loss of generality, then following pairs can be defined
- $(A \times B, A \times B)$: sharing both operands
- $(A \times B, C \times B)$: sharing one operand

Horizontal Collision Correlation Analysis (HCCA)

- HCCA is based on underlying field multiplications that constitute ECC point addition and doubling.
- It is based on the following assumption: *The adversary can detect when a pair of field multiplications have at least one operand in common*
- If A, B, C and D be field multiplications considered without loss of generality, then following pairs can be defined
- $(A \times B, A \times B)$: sharing both operands
- $(A \times B, C \times B)$: sharing one operand
- $(A \times B, C \times D)$: sharing no operand

- Following properties have been defined:

- Following properties have been defined:
- *property* 1*:* When a pair of multiplications (m_i, m_j) share one (two) common operand (s).

- Following properties have been defined:
- *property* 1*:* When a pair of multiplications (m_i, m_j) share one (two) common operand (s).
- *property* 1*a:* When a pair of multiplications (m_i, m_j) share one common operand. For example: ($A \times B$, $C \times B$)

- Following properties have been defined:
- *property* 1*:* When a pair of multiplications (m_i, m_j) share one (two) common operand (s).
- *property* 1*a:* When a pair of multiplications (m_i, m_j) share one common operand. For example: $(A \times B,\ C \times B)$
- *property* 1*b:* When a pair of multiplications (m_i, m_j) share two common operands. For example: $(A \times B,\ A \times B)$

Horizontal Collision Correlation Analysis (HCCA)

- Following properties have been defined:
- *property* 1*:* When a pair of multiplications (m_i, m_j) share one (two) common operand (s).
- *property* 1*a:* When a pair of multiplications (m_i, m_j) share one common operand. For example: $(A \times B, C \times B)$
- *property* 1*b:* When a pair of multiplications (m_i, m_j) share two common operands. For example: $(A \times B, A \times B)$
- *property* 2*:* When a pair of multiplications (m_i, m_j) share no common operand among themselves. For example: $(A \times B, C \times D)$

Horizontal Collision Correlation Analysis (HCCA)

- Following properties have been defined:
- *property* 1*:* When a pair of multiplications $(m_i,\ m_j)$ share one (two) common operand (s).
- *property* 1*a:* When a pair of multiplications $(m_i,\ m_j)$ share one common operand. For example: $(A \times B,\ C \times B)$
- *property* 1*b:* When a pair of multiplications $(m_i,\ m_j)$ share two common operands. For example: $(A \times B,\ A \times B)$
- *property* 2*:* When a pair of multiplications $(m_i,\ m_j)$ share no common operand among themselves. For example: $(A \times B,\ C \times D)$
- *property* 3*:* Given a set S of n field multiplications $(m_1,\ m_2,\ \ldots,\ m_n)$, if there exists at least one pair $(m_i,\ m_j)$, where m_i and $m_j \in S$, $i \neq j$, sharing property 1.

- HCCA can be launched in two scenarios.

Horizontal Collision Correlation Analysis (HCCA)

- HCCA can be launched in two scenarios.
- *HCCA scenario* 1*:*

- HCCA can be launched in two scenarios.
- *HCCA scenario* 1*:*
- ECC point doubling can be considered as a set set_d of n_d underlying field multiplications $(d_1, d_2, \ldots, d_{n_d})$

- HCCA can be launched in two scenarios.
- *HCCA scenario* 1*:*
- ECC point doubling can be considered as a set set_d of n_d underlying field multiplications (d_1, d_2, ..., d_{n_d})
- ECC point addition can be considered as a set set_a of n_a underlying field multiplications (a_1, a_2, ..., a_{n_a})

Horizontal Collision Correlation Analysis (HCCA)

- HCCA can be launched in two scenarios.
- *HCCA scenario* 1*:*
- ECC point doubling can be considered as a set set_d of n_d underlying field multiplications $(d_1, d_2, \ldots, d_{n_d})$
- ECC point addition can be considered as a set set_a of n_a underlying field multiplications $(a_1, a_2, \ldots, a_{n_a})$
- HCCA scenario 1 is based on condition 1 defined below:

- HCCA can be launched in two scenarios.
- *HCCA scenario* 1*:*
- ECC point doubling can be considered as a set set_d of n_d underlying field multiplications $(d_1, d_2, \ldots, d_{n_d})$
- ECC point addition can be considered as a set set_a of n_a underlying field multiplications $(a_1, a_2, \ldots, a_{n_a})$
- HCCA scenario 1 is based on condition 1 defined below:
- *condition* 1*:* Only one of the sets set_a and set_d satisfies property 3.

HCCA scenario 1

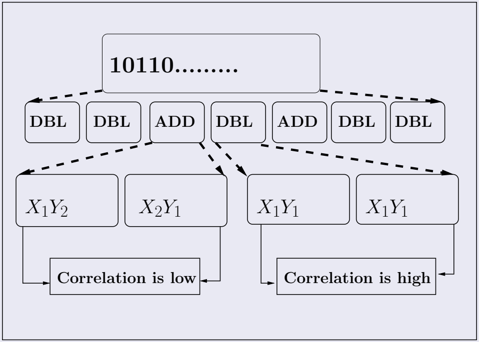


Figure: HCCA scenario 1

- *HCCA scenario 2:*

- *HCCA scenario 2:*
- Scenario 2 is based on the fact: *In point addition operation one of the point parameter is always the base point.*

Horizontal Collision Correlation Analysis (HCCA)

- *HCCA scenario 2:*
- Scenario 2 is based on the fact: *In point addition operation one of the point parameter is always the base point.*
- It holds irrespective of the curve equation or the unified formula steps involved in the scalar multiplication.

Horizontal Collision Correlation Analysis (HCCA)

- *HCCA scenario 2:*
- Scenario 2 is based on the fact: *In point addition operation one of the point parameter is always the base point.*
- It holds irrespective of the curve equation or the unified formula steps involved in the scalar multiplication.

HCCA scenario 2

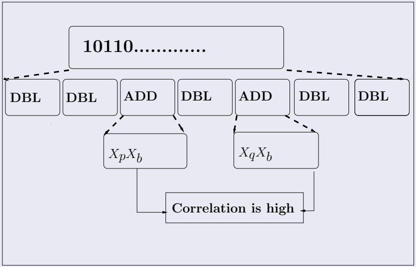


Figure: HCCA scenario 2

Long Integer Multiplication

Algorithm 1: Long Integer Multiplication algorithm(LIM)

Data: : $\{X = (X[t], X[t-1], ..., X[1])_{2^w}\}$, $\{Y = (Y[t], Y[t-1], ..., Y[1])_{2^w}\}$
Result: : $\{X.Y\}$

begin
  for $i \leftarrow 1$ **to** $2t$ **do**
    $R[i] = 0$
  end
  for $i \leftarrow 1$ **to** t **do**
    $C = 0$;
    for $j \leftarrow 1$ **to** t **do**
      $(U, V)_{2^w} = X[i] \times Y[j]$;
      $(U, V)_{2^w} = (U, V)_{2^w} + C$;
      $(U, V)_{2^w} = (U, V)_{2^w} + R[i + j - 1]$;
      $R[i + j - 1] = V$;
      $C = U$;
    end
    $R[i + t] = C$;
  end
  return R ;
end

- Let C_i be the operation leaking information at each iteration.

Asymmetric Leakage of Field Multiplications

- Let C_i be the operation leaking information at each iteration.
- The output of the calculation C_i is denoted as O_i

Asymmetric Leakage of Field Multiplications

- Let C_i be the operation leaking information at each iteration.
- The output of the calculation C_i is denoted as O_i
- At each iteration output O_i leaks an information $I(O_i)$

Asymmetric Leakage of Field Multiplications

- Let C_i be the operation leaking information at each iteration.
- The output of the calculation C_i is denoted as O_i
- At each iteration output O_i leaks an information $I(O_i)$
- The leakage $I(O_i)$ is approximated by the Hamming Weight power model.

Asymmetric Leakage of Field Multiplications

- Let C_i be the operation leaking information at each iteration.
- The output of the calculation C_i is denoted as O_i
- At each iteration output O_i leaks an information $l(O_i)$
- The leakage $l(O_i)$ is approximated by the Hamming Weight power model.
- A long integer multiplication LIM(A, B) leads to a leakage vector $< l_{(a_0 b_0)}, l_{(a_0 b_1)}, \ldots, l_{(a_i b_j)}, \ldots, l_{(a_{t-1} b_{t-1})} >$

Asymmetric Leakage of Field Multiplications

- $\rho_1 = Corr(LIM(A, B), LIM(C, B))$

Asymmetric Leakage of Field Multiplications

- $\rho_1 = Corr(LIM(A, B), LIM(C, B))$
- $\rho_2 = Corr(LIM(A, B), LIM(B, C))$

Asymmetric Leakage of Field Multiplications

- $\rho_1 = Corr(LIM(A, B), LIM(C, B))$
- $\rho_2 = Corr(LIM(A, B), LIM(B, C))$
- $\rho_3 = Corr(LIM(A, B), LIM(C, D))$

Asymmetric Leakage of Field Multiplications

- $\rho_1 = Corr(LIM(A, B), LIM(C, B))$
- $\rho_2 = Corr(LIM(A, B), LIM(B, C))$
- $\rho_3 = Corr(LIM(A, B), LIM(C, D))$
- *Lemma* 1: $std(LIM(A, B)) = std(LIM(B, A))$

Asymmetric Leakage of Field Multiplications

- $\rho_1 = Corr(LIM(A, B), LIM(C, B))$
- $\rho_2 = Corr(LIM(A, B), LIM(B, C))$
- $\rho_3 = Corr(LIM(A, B), LIM(C, D))$
- *Lemma* 1*:* $std(LIM(A, B)) = std(LIM(B, A))$
- *Lemma* 2*:* $cov(LIM(A, B), cov(LIM(C, B)) \neq cov(LIM(A, B), LIM(B, C))$.

- With the help of the Lemmas following observations are made:

Asymmetric Leakage of Field Multiplications

- With the help of the Lemmas following observations are made:
- *Observation* 1*:* $\rho_1 \neq \rho_2$

Asymmetric Leakage of Field Multiplications

- With the help of the Lemmas following observations are made:
- *Observation* 1*:* $\rho_1 \neq \rho_2$
- *Observation* 2*:* $\rho_2 \approx \rho_3$

Asymmetric Leakage of Field Multiplications

- With the help of the Lemmas following observations are made:
- *Observation 1:* $\rho_1 \neq \rho_2$
- *Observation 2:* $\rho_2 \approx \rho_3$
- *Observation 3:* $\rho_1 > \rho_2$, when C=A (i.e. both the operands are shared).

Safe sequence formation for Edward curve formula

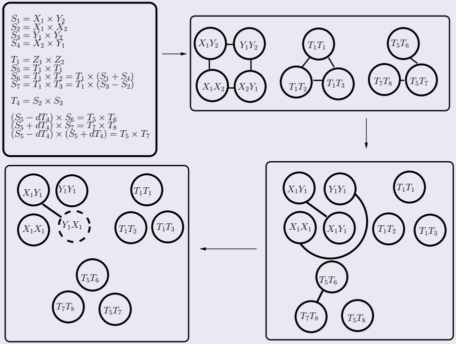


Figure: Safe sequence transformation of Edward unified formula

Countermeasure Design: Safe Sequence

Safe sequence formation for Brier-Joye unified formula

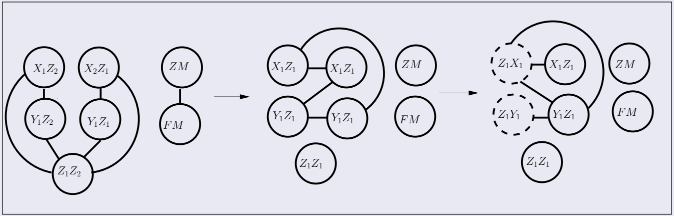


Figure: Safe sequence transformation of Brier-Joye unified formula

- Equipments:

Results

- Equipments:
  - SASEBO GII Board

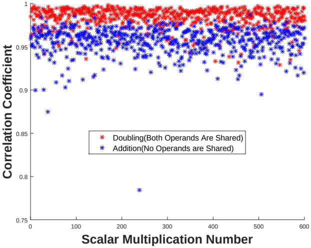
- Equipments:
  - SASEBO GII Board
  - Oscilloscope (DPO4034B)

- Equipments:
  - SASEBO GII Board
  - Oscilloscope (DPO4034B)
  - JTAG Cable

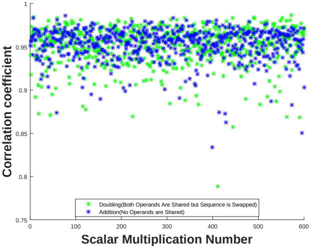
Results

- Equipments:
  - SASEBO GII Board
  - Oscilloscope (DPO4034B)
  - JTAG Cable
  - EM Probe

Results



(a) Evaluation of HCCA on Edwards Curve Scalar Multiplier



(b) Evaluation of proposed countermeasure on Edwards Curve Scalar Multiplier

HCCA Scenario 2 and Other Collision Attacks

- HCCA scenario 2: Same input point is used in all addition steps
- Re-randomization: Use randomize input point at each stage of addition steps
- After the end of scalar multiplication loop, de-randomize the results[1].
- Similar re-randomization can be used to mitigate other single trace collision attacks [2].

[1] Poulami Das, Debapriya Basu Roy, Debdeep Mukhopadhyay: Exploiting the Order of Multiplier Operands: A Low Cost Approach for HCCA Resistance. IACR Cryptology ePrint Archive 2015: 925 (2015)

[2] N. Hanley, H. Kim, and M. Tunstall, Exploiting collisions in addition chain-based exponentiation algorithm using a single trace, Cryptography ePrint Archive: Report 2012/485.

Conclusion

- We have shown how the property of asymmetric leakage of field multipliers can be utilized to construct a low-cost countermeasure which is able to defeat the powerful HCCA.

Conclusion

- We have shown how the property of asymmetric leakage of field multipliers can be utilized to construct a low-cost countermeasure which is able to defeat the powerful HCCA.
- We show how a unified addition (doubling) formula can be converted into a safe sequence where, the information leakage from sharing of operands among field multipliers have been hidden. Once the sequence have been determined through Algorithm 1 there is no runtime overhead requirement for the step 1 of our countermeasure.

Conclusion

- We have shown how the property of asymmetric leakage of field multipliers can be utilized to construct a low-cost countermeasure which is able to defeat the powerful HCCA.
- We show how a unified addition (doubling) formula can be converted into a safe sequence where, the information leakage from sharing of operands among field multipliers have been hidden. Once the sequence have been determined through Algorithm 1 there is no runtime overhead requirement for the step 1 of our countermeasure.
- We have validated HCCA and our proposed countermeasure scheme on a SASEBO platform.

Thank You