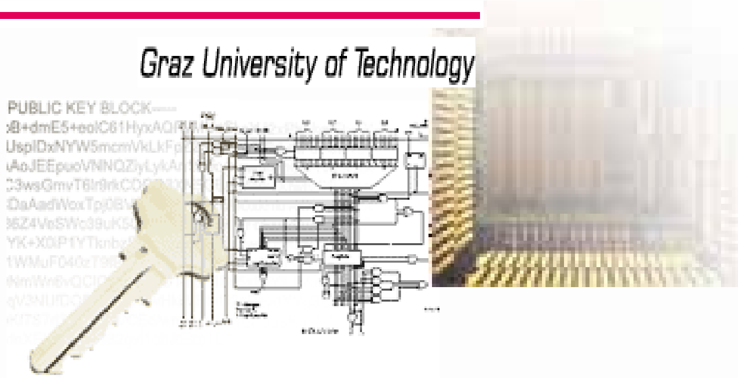
Enhancing Simple Power-Analysis Attacks on Elliptic Curve Cryptosystems

Elisabeth Oswald

Institute for Applied Information Processing and Communications

Graz University of Technology

KATHOLIEKE UNIVERSITEIT LEUVEN



Motivation

- ECC (especially ECDSA) are getting more and more popular (see for example Austrian Social Insurrance Smart Card).
- ECDSA and ephemeral DH are non-deterministic encryption schemes, thus DPA directly on the scalar point-multiplication is unlikely to work.
- SPA is a direct thread to the ephemeral key used in $Q = kP$.
- Recent paper by Römer et al. shows that the well known lattice-attack on the DSA can very efficiently also be applied to the ECDSA.
- $\Rightarrow$ the protection of the ephemeral key of the ECDSA is of greatest importance!

Types of SPA countermeasures in SW

- Rearrangment of the field operations in such a way that both EC-PD and EC-PA look alike.

- Make an efficient *always double and always add* algorithm. Use for example special curves (Montgomery form), another parametrization (Hessian form), special recoding, etc. . . .

- Conceal the actions of the bits of the ephemeral key (by recoding and/or randomization).

Assumptions

- Arithmetic of EC allows three operations (EC-PD,EC-PA,EC-PS), whereby EC-PA and EC-PS are essentially the same $\Rightarrow$ they power traces look alike.
- Classical SPA: passive attack, observation of one single EC-SPM, plus knowledge of input and output to EC-SPM.
- Bits of k are independently drawn and identically distributed.

Preliminaries

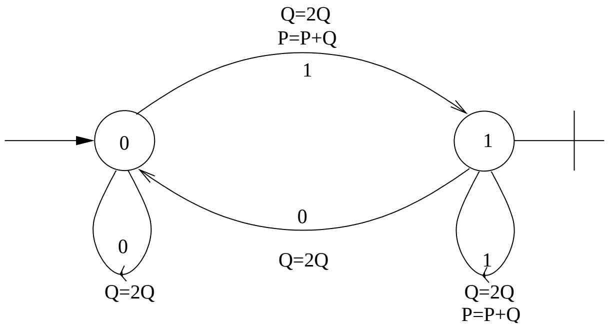


Figure 1: Transition graph of the standard binary algorithm

- Recoding techniques transform the ephemeral key k. Most simple case uses three digits instead of two.

- Obscuring means that there are more difficult relationships between the bits of the ephemeral key and the elliptic curve operations.

Attacker's Task

Attacker's Task

- Eve observes the sequence of EC-PA and EC-PD operations from the power trace: $ADADDDADADADDDADADADADDDADDDDAD$.

Attacker's Task

- Eve observes the sequence of EC-PA and EC-PD operations from the power trace: $ADADDDADADADDDADADADADDDADDDDAD$.

- Table consisting of all combinations of keys and sequences for all? $\Rightarrow$ much too large!

Attacker's Task

- Eve observes the sequence of EC-PA and EC-PD operations from the power trace: $ADADDDADADADDDADADADADDDADDDDAD$.

- Table consisting of all combinations of keys and sequences for all? $\Rightarrow$ much too large!

- X . . . sequence of EC operations. For example: $X = DDD$

- Y . . . sequence of bits. For example: $Y = 00$.

Attacker's Task

IAIK TUG

- Eve observes the sequence of EC-PA and EC-PD operations from the power trace: $ADADDDADADADDDADADADADDDADDDDAD$.
- Table consisting of all combinations of keys and sequences for all? $\Rightarrow$ much too large!
- X ... sequence of EC operations. For example: $X = DDD$
- Y ... sequence of bits. For example: $Y = 00$.
- $$P(Y = y|X = x) = \frac{P(Y = y \cap X = x)}{P(X = x)} \qquad (1)$$

Markov Process - 1

- Point multiplication algorithm $\Leftrightarrow$ Markov process.
- Markov process:

Markov Process - 1

IAIK TUG

- Point multiplication algorithm $\Leftrightarrow$ Markov process.
- Markov process:
  - The next state (event) is only dependent on the present state,

Markov Process - 1

- Point multiplication algorithm $\Leftrightarrow$ Markov process.

- Markov process:
  - The next state (event) is only dependent on the present state,
  - but is independent of the state before the present state.

Markov Process - 1

- Point multiplication algorithm $\Leftrightarrow$ Markov process.

- Markov process:
  - The next state (event) is only dependent on the present state,
  - but is independent of the state before the present state.
  - Transitions are determined by a random variable (probability is known or has to be estimated).

Markov Process - 1

- Point multiplication algorithm ⇔ Markov process.

- Markov process:
  - The next state (event) is only dependent on the present state,
  - but is independent of the state before the present state.
  - Transitions are determined by a random variable (probability is known or has to be estimated).
  - Several possible states ⇔ random variables are entries in a *transition matrix*.

Markov Process - 1

- Point multiplication algorithm ⇔ Markov process.
- Markov process:
  - The next state (event) is only dependent on the present state,
  - but is independent of the state before the present state.
  - Transitions are determined by a random variable (probability is known or has to be estimated).
  - Several possible states ⇔ random variables are entries in a *transition matrix*.
  - The transition matrix is used to forecast future states.

Markov Process - 1

IAIK TUG

- Point multiplication algorithm $\Leftrightarrow$ Markov process.

- Markov process:
  - The next state (event) is only dependent on the present state,
  - but is independent of the state before the present state.
  - Transitions are determined by a random variable (probability is known or has to be estimated).
  - Several possible states $\Leftrightarrow$ random variables are entries in a *transition matrix*.
  - The transition matrix is used to forecast future states.
  - A steady state exists for a large class of Markov processes!

Markov Process - 2

Analysis of a double-add-and-subtract algorithm. Details are in the paper.

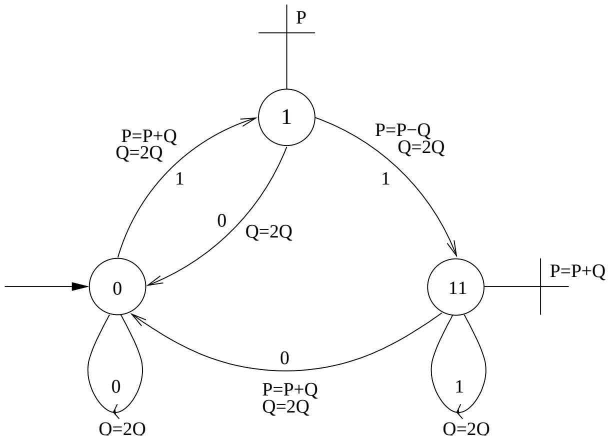


Figure 2: Transition graph of the algorithm.

Markov Process - 2

Analysis of a double-add-and-subtract algorithm. Details are in the paper.

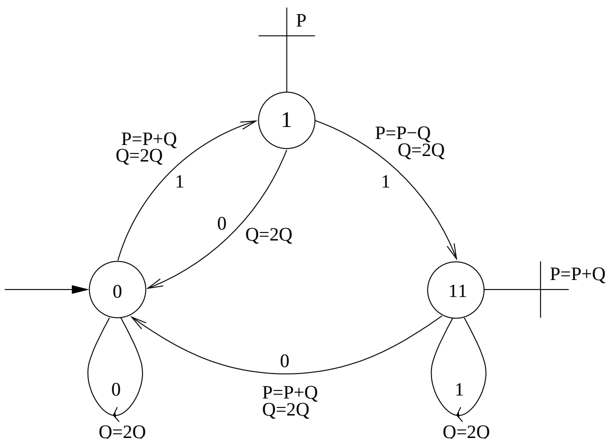


Figure 2: Transition graph of the algorithm.

$$M = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

Figure 3: Transition matrix. The steady state vector is $(\frac{1}{2}, \frac{1}{4}, \frac{1}{4})$

The Attack

The Attack

1. **Precomputation phase:** Find the Markov model. Calculate the conditional probabilities for a lot of combinations of realizations of X and Y.

The Attack

1. **Precomputation phase:** Find the Markov model. Calculate the conditional probabilities for a lot of combinations of realizations of X and Y.

2. *Data collection phase:* Deduce the sequence of EC-PA and EC-PD operations.

The Attack

1. **Precomputation phase:** Find the Markov model. Calculate the conditional probabilities for a lot of combinations of realizations of X and Y.

2. *Data collection phase:* Deduce the sequence of EC-PA and EC-PD operations.

3. **Data analysis phase:** Split this sequence into a number of sub-sequences. Ensure a valid partitioning!

The Attack

1. **Precomputation phase:** Find the Markov model. Calculate the conditional probabilities for a lot of combinations of realizations of X and Y.

2. *Data collection phase:* Deduce the sequence of EC-PA and EC-PD operations.

3. **Data analysis phase:** Split this sequence into a number of sub-sequences. Ensure a valid partitioning!

4. **Key testing phase:** Check all possible keys by the known ciphertext.

A concrete example-Precomputation Phase

A concrete example-Precomputation Phase

IAIK TUG

Table 1: Non-zero conditional probabilities. In this table we use an abbreviated notation, i.e. we write $p(000|DDD)$ instead of $p(Y = 000|X = DDD)$. We use the LSB first representation.

$p(000\|DDD) = 1/2$	$p(01\|DAD) = 1/2$	$p(11\|ADAD) = 1/2$
$p(100\|DDD) = 1/4$	$p(10\|DAD) = 1/4$	$p(10\|ADAD) = 1/4$
$p(111\|DDD) = 1/4$	$p(11\|DAD) = 1/4$	$p(01\|ADAD) = 1/4$
$p(001\|DDAD) = 1/2$	$p(000\|ADDD) = 1/4$	$p(110\|ADADAD) = 1/2$
$p(101\|DDAD) = 1/4$	$p(100\|ADDD) = 1/2$	$p(101\|ADADAD) = 1/4$
$p(110\|DDAD) = 1/4$	$p(111\|ADDD) = 1/4$	$p(011\|ADADAD) = 1/4$

A concrete example-Data Analysis Phase

A concrete example-Data Analysis Phase

Table 2: Example : $k = 11110111101100010001$, LSB first representation

ADADDDADADADDDADADADADDDADDDDAD							
ADAD	DDAD	ADAD	DDAD	ADAD	ADDD	ADDD	DAD
11	001	**11**	001	**11**	100	**100**	**01**
10	101	10	101	10	**000**	000	10
01	**110**	01	**110**	01	111	111	11

- Worst Case . . . $3^{3n/2l}$ keys to test.
- Average Case . . . $2^{3n/2l}$ keys to test. Set $l = 16$.
- Average case for a 163-bit curve $\Rightarrow 2^{15.28}$ keys to test!

NAF-Method and Randomized Algorithms

NAF-Method and Randomized Algorithms

IAIK TUG

- **NAF-method:** $2^{n/3}$ possible keys need to be searched through. Would take approx. 2^{17} years with a single and not even optimized device.

NAF-Method and Randomized Algorithms

IAIK TUG

- **NAF-method:** $2^{n/3}$ possible keys need to be searched through. Would take approx. 2^{17} years with a single and not even optimized device.

- **Randomized Algorithms:**
  - The attack is not better than on the NAF-method.
  - The randomization does increase some of the conditional probabilities,
  - but, the number of combinations of possible bit-patterns and sub-sequences increases rapidly,
  - so that they are more resistant than the other algorithms.

Conclusions

- We presented a new and more efficient simple power-analysis attack on EC-SPM
- We used Markov models to calculate conditional probabilities for sequences of bits and sequences of elliptic curve operations.
- We could enhance attacks on double-add-and subtract algorithms (that only use a 3-digit encoding)
- The security margin of such algorithms when using 163-bit curves is rather small!

THE END

Thank you for your Attention!

Questions?

Elisabeth.Oswald@{iaik.at,esat.kuleuven.ac.be}
http://www.iaik.at
http://www.esat.kuleuven.ac.be/cosic