Timing Side-Channel Attack

Using linear correlation to reveal secrets

A. Anselmo, S.A. Chiaberto, F. Chiatante, G. Roggero

Supervisor: *Prof. Renaud Pacalet*

21st June, 2019

Outline

Introduction

- in several algorithms used for security purposes some optimizations are introduced
- these optimizations lead to a linear dependency between time and the data encrypted
- knowing information regarding the time-data pair, it is possible to find a correlation
- this correlation can be used to unveal part of the secret

Hypothesis

Our starting point

In order to successfully extract the secret through the correlation, we have to make a list of assumptions:

- timing for a sufficiently large number of cyphertexts is known
- cyphertexts are known
- secret is the same for all cyphertexts
- the HW/SW implementation is known to the attacker
- a timing model can be built

From the very beginning

BIGINT required

In order to operate with large integers, we decided to develop our own library of functions to operate over integers of arbitrary length, in particular with the following elementary instructions:

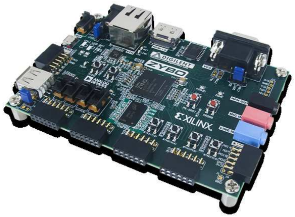
- addition and subtraction
- multiplication
- bitwise operation, such as `AND, OR, XOR, NOT`
- logical comparison

The least complex attack

Bare metal

We wanted to exploit the easiest possible attack. Since on a normal device an OS might cause interrupts, thus changing the total time of the enciphering, we decided to:

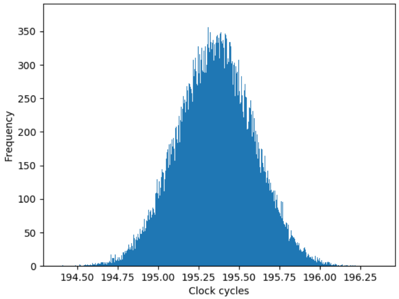
- compile our code for an ARM architecture
- add it to an *Eclipse* project
- used the MAKEFILE generated by Xilinx SDK
- copy the executable on the Zybo board



Finding correlations

PCC: our game changer

In order to find the linerar contribution of each sample in the overall time, we have used the *Pearson Correlation Coefficient* as an estimator. It has proved to be really effective for our needs, working on the realizations of a random variable.



WE JUST CORRELATE

Algorithm

Development

WE JUST CORRELATE

Algorithm

Development

1. Started in Python to allow better flexibility and library support (infinite precion, `scipy.stats`)

Algorithm

Development

1. Started in Python to allow better flexibility and library support (infinite precion, `scipy.stats`)
2. At firt, attacking conditional Montgomery Mult., 1 bit at-a-time, using fixed threshold

Algorithm

Development

1. Started in Python to allow better flexibility and library support (infinite precion, `scipy.stats`)
2. At firt, attacking conditional Montgomery Mult., 1 bit at-a-time, using fixed threshold
3. Move on to attack both MM to improve statistical relevance of 0 guesses

Algorithm

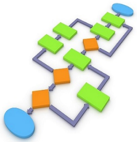
Development

1. Started in Python to allow better flexibility and library support (infinite precion, `scipy.stats`)
2. At firt, attacking conditional Montgomery Mult., 1 bit at-a-time, using fixed threshold
3. Move on to attack both MM to improve statistical relevance of 0 guesses
4. Get rid of fixed threshold by using multi bit analysis and the max of the accumulated PCCs on a common path

Algorithm

Final implementation

- Attack at the same time the two Montgomery moltiplications present in an RSA iteration
- Timing estimate based on a dummy Montgomery moltiplication which evaluates the number of taken branches
- Multi bit guessing
- Error-detection capabilities



Algorithm

Optimizations

- Completely rewritten in C with +10x speedup over Python
- Fully customizable number of bits considered and guessed in one attack iteration
- Tweakable filtering of input data with `#define` parameters

Just a simplification

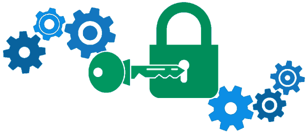
Works on computer also

Even if we mainly worked on the *Zybo* board, we can claim that:

- our attack works also when mounted for other devices, including different architectures (Intel x86, ..)
- with an OS, more tuples (cipher, timing) are needed
- the attack is still feasible

We have completely tested what is mentioned above.

Bigger keys



RSA on 512/1024/2048/4096

The algorithm is capable of handling larger keys on 512, 1024, 2048 and 4096 bits. However, the processing time is longer, and a more complex backtrack might be necessary in some cases.

Titlepage settings

- by changing settings in

  `header_footer.sty`

  you can choose whether and where you want a second logo to be positioned on the titlepage:
  - small logo can be placed on the bottom right
  - big logo can be placed on the top right
- spaces and graphics dimensions will have to be adjusted depending on your logo

Outline

- divide the presentation, using the command `section` (as it is usually done in LaTeX)
- other divisions, just as chapter or part are not supported
- the sections are are listed on the top of each slide, the section the recent slide belongs to is highlighted
- you can automatically receive an outline out of this section by the command

  ```
  \tableofcontents
  ```

Itemize

- black circle is the default; other possibilities are:
    - ball
        - triangle
- the color of the items can also be changed
- all this settings have to be done in the preamble of the `presentation.tex` file

T S
C A
WE JUST CORRELATE

Overlays

Overlays

- its possible to build slides succesively

Overlays

- its possible to build slides succesively
- to do so use the command `onslide`

Overlays

- its possible to build slides succesively
- to do so use the command `onslide`
- other useful commands are `uncover` and `only`

Overlays

- its possible to build slides succesively
- to do so use the command `onslide`
- other useful commands are `uncover` and `only`
- this works also very nice to "develop" formulas:

Overlays

- its possible to build slides succesively
- to do so use the command `onslide`
- other useful commands are `uncover` and `only`
- this works also very nice to "develop" formulas:

$$f(x \mid \mu, \sigma^2) \; =$$

Overlays

- its possible to build slides succesively
- to do so use the command `onslide`
- other useful commands are `uncover` and `only`
- this works also very nice to "develop" formulas:

$$f(x \mid \mu, \sigma^2) = \frac{1}{\sigma\sqrt{2\pi}}$$

Overlays

- its possible to build slides succesively
- to do so use the command `onslide`
- other useful commands are `uncover` and `only`
- this works also very nice to "develop" formulas:

$$f(x \mid \mu, \sigma^2) \;=\; \frac{1}{\sigma\sqrt{2\pi}} \cdot \exp\left\{ \qquad\qquad\qquad \right\}$$

T S
C A
WE JUST CORRELATE

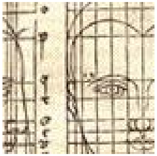
Overlays

- its possible to build slides succesively
- to do so use the command `onslide`
- other useful commands are `uncover` and `only`
- this works also very nice to "develop" formulas:

$$f(x \mid \mu, \sigma^2) \;=\; \frac{1}{\sigma\sqrt{2\pi}} \cdot \exp\left\{ -\frac{(x-\mu)^2}{2\sigma^2} \right\}$$

Pimp up your presentation

- an easy way to include pictures is by using `\includegraphics[width=...,height=...]{file}`
- in connection with `pdflatex` this supports a wider range of graphic formats, including GIF, PNG, JPG



Useful hints

- if you use a verbatim environment on a slide, declare that slide `fragile`:

  ```
  \begin{frame}[fragile]
  ```
- bibliography actually works as usual, just keep in mind that not all bibliography styles are supported by the *beamer* package, maybe you have to include some other packages to get your preferred style working

Possible solution

Blinding

The proposed countermeasure is the one given in Kocher (1996). It consists in blinding the message before the encryption using a couple of values v_f, v_i chosen in such a way that:

$$v_i^e \cdot v_f \, mod \, N = 1$$

This contermeasure, in all our tests, has proven to be really effective. Ciphers are completely masked, no correlation can be identified.

Possible solution

Blinding

Future expectations

What more

- porting the attack in C++ to keep class structure and speedup w.r. to Python
- find an optimal filter and explain the strange behavior of the implemented filter

References I

Bansal, M., Kumar, A., Devrari, A., Bhat, A., UTU, D., and Dehradun, U. (2015). Implementation of modular exponentiation using montgomery algorithms. *International Journal of Scientific & Engineering Research*, 6(11):1272–1277.

Crockett, L. H., Elliot, R. A., Enderwitz, M. A., and Stewart, R. W. (2014). *The Zynq Book: Embedded Processing with the Arm Cortex-A9 on the Xilinx Zynq-7000 All Programmable Soc*. Strathclyde Academic Media.

Kocher, P. C. (1996). Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Annual International Cryptology Conference*, pages 104–113. Springer.

Walter, C. D. (1999). Montgomery exponentiation needs no final subtractions. *Electronics letters*, 35(21):1831–1832.

Xilinx (2015). *Zynq-7000 All Programmable SoC Software Developers Guide*. Xilinx.