riscure

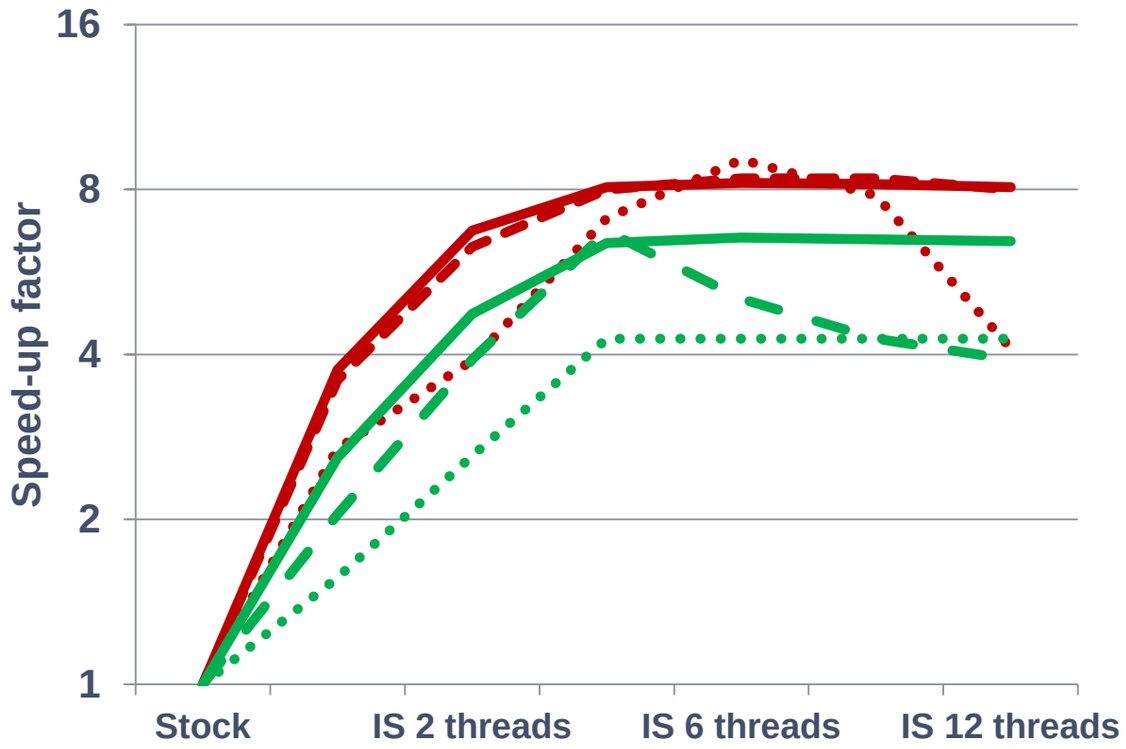
RnD topics in side channel analysis

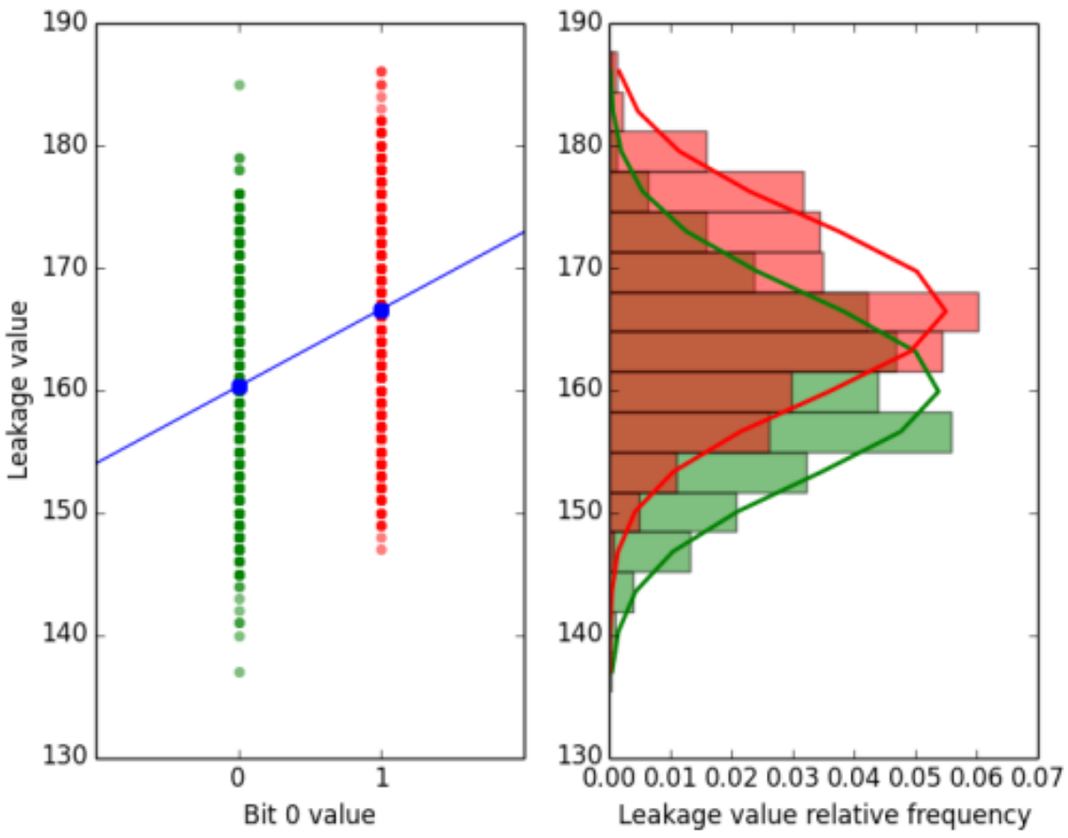
Ilya Kizhvatov, Riscure

Uni.Lu 9 December 2014

General RnD directions

1. Speed up existing methods

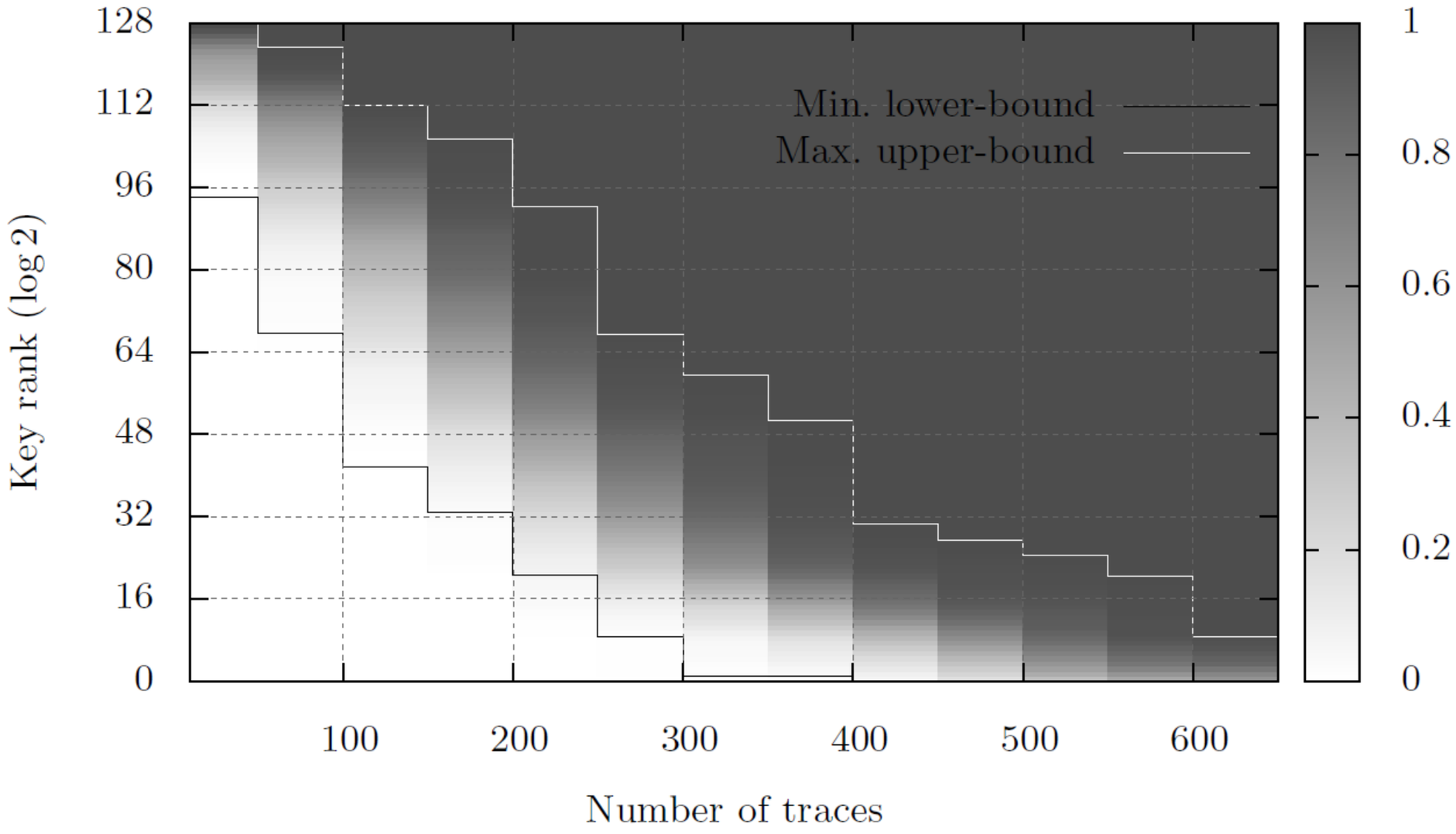




2. Put advanced methods into practice

Example proposal 1

Better metrics for SCA: explore an algorithm for full key rank estimation

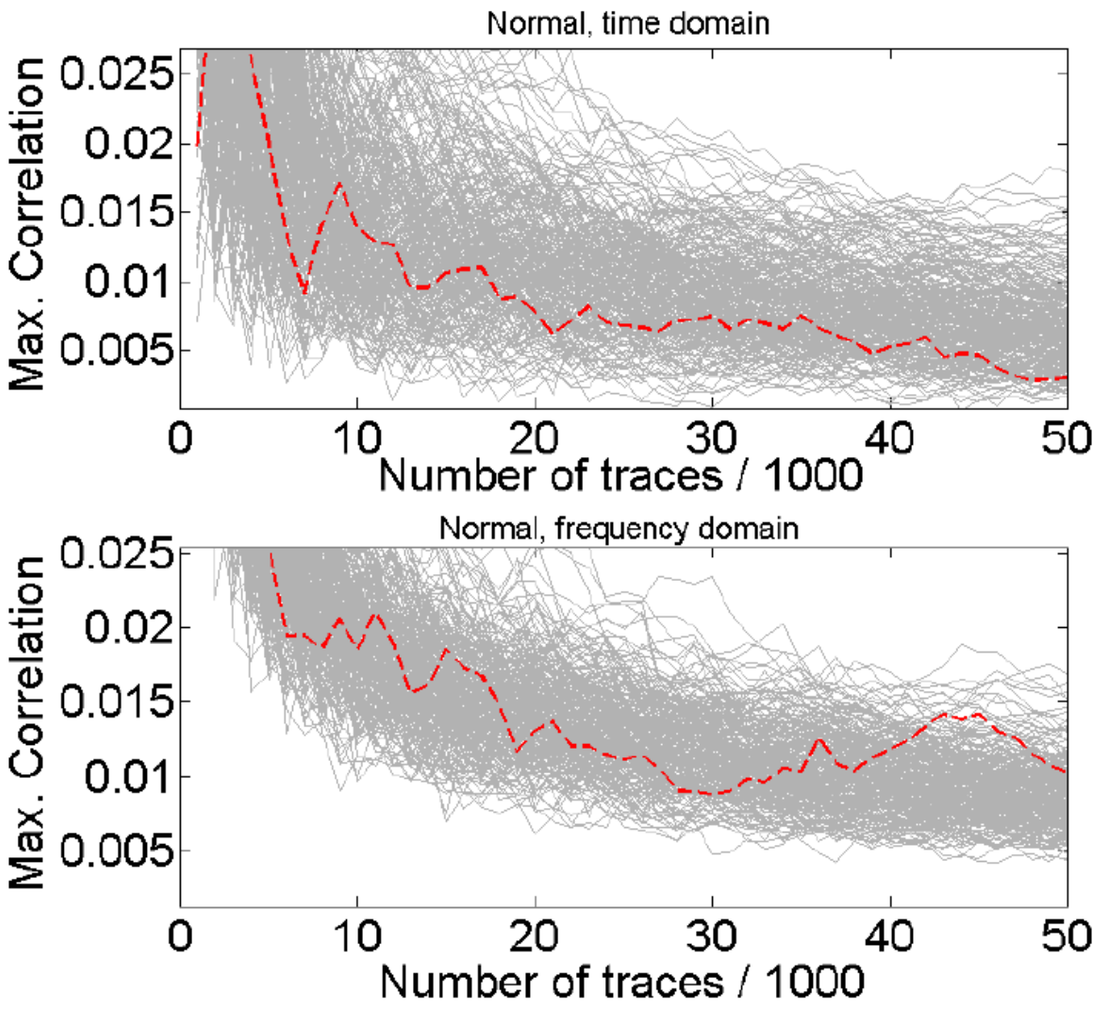


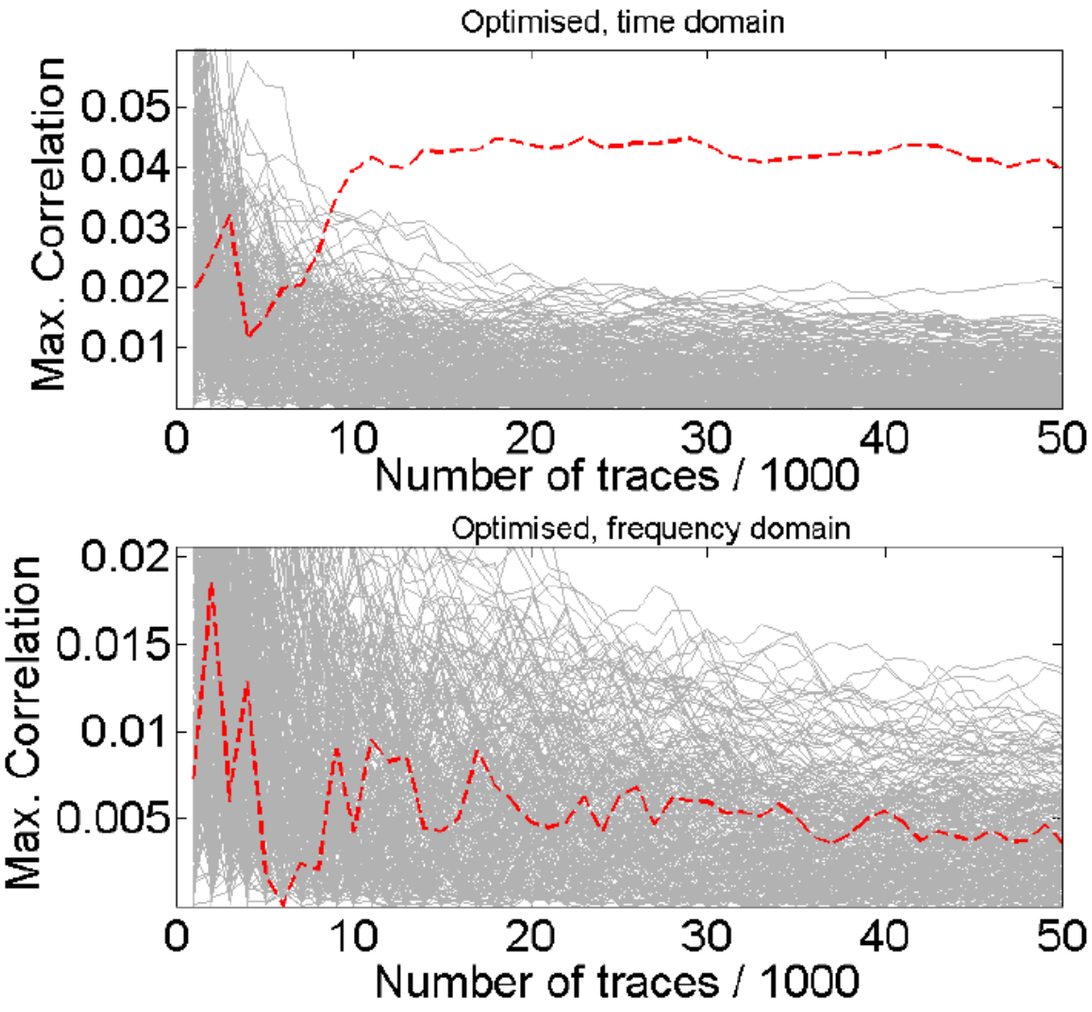
eprint 2012/578, eprint 2014/920

Example proposal 2

riscure

Apply optimal filtering techniques to different targets





cardis.iaik.tugraz.at/proceedings/cardis_2012/CARDIS2012_16.pdf
cosade.org/cosade14/presentations/session7_a.pdf

Good to have

- familiarity with statistics and/or signal processing
- strong programming skills (Java, scientific Python, MATLAB)
- familiarity with embedded devices, e.g. microcontrollers
- desire to implement practical tools and learn how security evaluations are performed

riscure

Challenge your security

Contact: Ilya Kizhvatov
ilya@riscure.com

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90

www.riscure.com

Riscure North America
71 Stevenson Street, Suite 400
San Francisco, CA 94105
USA
Phone: +1 650 646 99 79

inforequest@riscure.com