ERCIM "ALAIN BENSOUSSAN" FELLOWSHIP PROGRAMME

ERCIM
European Research Consortium for Informatics and Mathematics

Scientific Report

First name / Family name	Markku-Juhani Olavi Saarinen
Nationality	Finnish
Name of the *Host Organisation*	Department of Telematics, Norwegian University of Science and Technology (NTNU – Trondheim)
First Name / family name of the *Scientific Coordinator*	Prof. Colin Boyd
Period of the fellowship	14/02/2014 to 13/02/2015

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

As planned, my research focused on Authenticated Encryption algorithms and the related U.S. NIST – sponsored CAESAR competition. The activities mainly consisted of cryptographic design, engineering, and cryptanalysis (codebreaking) work.

CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) is a U.S. NIST (National Institute for Standards and Technology) -Sponsored international effort to find one or more algorithms to replace or complement the AES-GCM Authenticated Encryption standard.[1] The CAESAR competition runs from 2014 until 2017 and consists of four stages or "elimination rounds." By the March 2014 first round deadline, 57 candidate algorithms had been submitted.

I prepared two submissions to the CAESAR competition, CBEAM and STRIBOB. Creating submissions to such competitions is a rather laborious process, involving not only documenting the design and cryptographic strengths and features of the proposed

[1] CAESAR Competition: http://competitions.cr.yp.to/caesar.html

algorithms, but also creating optimized software and hardware implementations on various targets platforms. Most submission teams consisted of half a dozen people or more.

I withdrew my lightweight candidate CBEAM shortly after the start of the competition in April 2014 after Brice Minaud (French Information Security Agency ANSSI) found cryptographic weaknesses in it.

My efforts thereafter focused on further developing my other candidate, STRIBOB[2]. STRIBOB is based on Russian Streebog design, which allowed me to expand my understanding of Russian cryptography through cryptanalysis and by meeting the designers in person during the CTCrypt '14 conference in Moscow in June, where I gave a talk.

I further proposed another improvement, WhirBob, together with Billy Bob Brumley of Tampere University of Technology. This will be a CAESAR second round candidate.

Cryptanalysis**:** After the release of 57 CAESAR candidates in March 2014, I found serious cryptographic weaknesses in three algorithms:

1. PAES (China), structural weaknesses. Now withdrawn from competition.
2. HKC (Singapore), authentication broken. Now withdrawn from competition.
3. iFeed[AES] (China), shown to have weak authentication. Status unknown.

There are promising leads on more advanced attacks on some other candidates and these will be published on appropriate academic forums later.

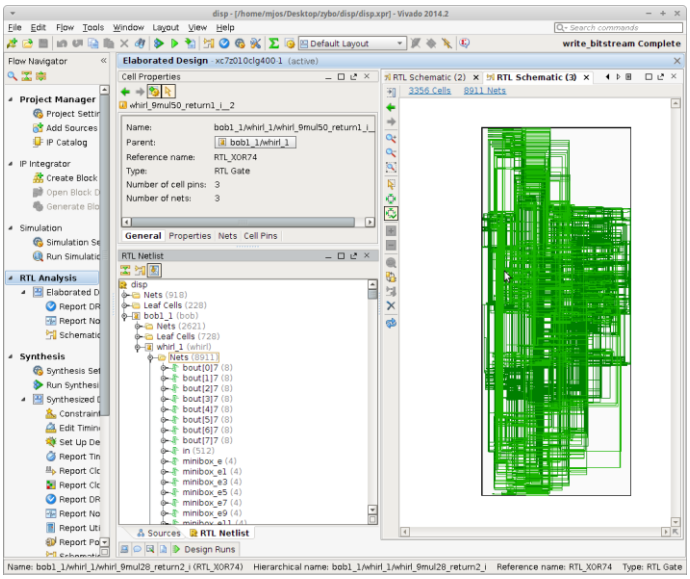
I authored the BRUTUS[3]. testing framework which allows statistical, compliance, and performance testing of all CAESR candidates via a standardized modular interface. A report on this work has been submitted for publication.

Implementation: In addition to optimized software implementations, I worked on hardware. I implemented the WhirlBob and Keccak AEAD transforms using Verilog and integrating them with the Artix-7 FPGA Logic Fabric that is available on the Xilinx Zynq 7000-series System-on-Chips. The Zynq SoC also houses a dual-core Cortex-A9 and is able to run full Linux (with Android), making it a realistic profiling tool for mobile, embedded, and IoT targets.

A report on this design (SÆHI) was published in TrustED 'TrustED '14, International Workshop on Trustworthy Embedded Devices. ACM CCS 2014 Workshop, 03 November 2014, Scottsdale, AZ, USA.

In our first experimental setup the SoCs on-chip FPGA not only implements the encryption coprocessor, but also display and networking interfaces. The demo runs single-chip Ubuntu Linux. Kernel drivers can be made available on other Linux-based platforms such as the market-leading Android OS.

[2] STRIBOB: http://www.stribob.com/ WhirlBob preprint: http://eprint.iacr.org/2014/501
[3] BRUTUS: https://github.com/mjosaarinen/brutus/ Preprint: http://eprint.iacr.org/2014/850



Left: Designing WhirlBob core for Artix-7. Right: The inexpensive Zybo evaluation board that houses the Xilinx Zynq 7010 SoC, with our first generation CAESAR coprocessor mapped to user space as /dev/xbob on the single-chip Linux system.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

1. M.-J. O. Saarinen: “BRUTUS: Identifying Cryptanalytic Weaknesses in CAESAR First Round Candidates” Submitted for publication. IACR ePrint 2014/850 (2014)
2. M.-J. O. Saarinen and B. B. Brumley: “Lighter, Faster, and Constant-Time: WHIRLBOB, the Whirlpool variant of STRIBOB.” Submitted for publication. IACR ePrint 2014/501 (2014)
3. M.-J. O. Saarinen: “Simple AEAD Hardware Interface (SÆHI) in a SoC: Implementing an On-Chip Keyak/WhirlBob Coprocessor.” TrustED '14, International Workshop on Trustworthy Embedded Devices, 03 November 2014, Scottsdale, AZ, USA. Part of ACM CCS Workshops. To appear. ACM (2014)
4. M.-J. O. Saarinen: “STRIBOB: Authenticated Encryption from GOST R 34.11-2012 LPS Permutation.” 3rd Workshop on Current Trends in Cryptology – CTCrypt 2014. 05-06 June 2014, Moscow, Russia. To appear in Journal “Математические вопросы криптографии” [Mathematical Aspects of Cryptography], Steklov Mathematical Institute of RAS (2014)

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

1. Finse Winter School in Cryptography. 4 – 9 May, 2014, Finse, Norway. I gave an invited lecture, "Developments in Authenticated Encryption." https://www.frisc.no/arrangementer/finse-winter-school-2014/
2. CTCrypt 2014: 3rd Workshop on Current Trends in Cryptology. 5 – 6 June 2014, Moscow, Russia. I gave a talk, "Authenticated Encryption from GOST R 34.11-2012 LPS Permutation." https://tc26.ru/en/CTCrypt/2014/
3. DIAC 2014: Directions in Authenticated Ciphers (CAESAR Workshop). 23 – 24 August 2014, Santa Barbara, USA. I Gave a workshop talk: "CAESAR candidate STRIBOB." http://2014.diac.cr.yp.to/
4. ACM CCS 2014: 21st ACM Conference on Computer and Communications Security, 3 – 7 November 2014, Scottsdale, Arizona, USA. http://www.sigsac.org/ccs/CCS2014/

   I gave workshop talk at the TrustED '14 Workshop – which was part of ACM CCS - on 03 November 2014: "Simple AEAD Hardware Interface (SÆHI) in a SoC: Implementing an On-Chip Keyak/WhirlBob Coprocessor." http://th.informatik.uni-mannheim.de/trusted-workshop/2014/

IV – RESEARCH EXCHANGE PROGRAMME (REP)

I visited the SECRET project-team at INRIA Paris-Rocquencourt for three weeks on 10 – 27 November 2014. The visit was hosted by the project team Director, Dr. Anne Canteaut.

I deeply recommend getting to know this group for anyone who is working cryptography and cryptanalysis. Furthermore Paris has one of the best concentrations of cryptographers anywhere in the world and researchers from different Universities and other facilities seem to frequently meet up at INRIA Paris offices for informal workshops (and to break codes). I gained valuable contacts and experience from this visit. https://www.rocq.inria.fr/secret/index.php?lg=en

I also had an opportunity to attend the NoSuchCon hacker event, which was held on 19 – 21 November 2014 in Paris. http://www.nosuchcon.org/