Symposium “20 Years of Cryptography and Security at WPI“
October 19, 2015
Christof Paar
Ruhr University Bochum & UMass Amherst
Table of Content

1. Teaching

2. Research
Table of Content

1. Teaching

2. Research
1991 – 1994

beautiful University of Essen, Germany
lucky me – Institute for Experimental Mathematics
July 1994

Han Vinck, my *Doktorvater*

Ph.D. in applied coding

also in Essen: Gerhard Frey
famous number theorist
Summer 1994 – visit to Philips Research
Eindhoven, The Netherlands

Dr. Kees-Immink, Philips Research
(co-inventor of CD disk coding)

Christof, nice work, except nobody in industry will ever use it.
Dr. John A. Orr  
Head, ECE Department  
Worcester Polytechnic Institute  
100 Institute Road  
Worcester, MA 01609-2280  
USA

Dr.-Ing. Christof Paar  
Arnimstr. 6a  
50825 Cologne, Germany  
phone: +49 201 32064 46  
after October 20:  
11 Winter St.  
Northampton, MA 01060  
phone: 413 584 6230

Dear Dr. Orr,  

I am writing in response to your advertisement in the August issue of the IEEE Spectrum magazine. I am very interested in the prospect of a faculty position at an educational institution in Massachusetts and in the strong research and teaching involvement which this would entail.  

As you can see from my enclosed resume, I have an extensive educational and practical background in the field of Electrical Engineering, with an empha-
January 1995
The most unlikely event – WPI hired me! (?)
January 1995
The most unlikely event – WPI hired me! (?)

Special thanks (for taking the risk) go to

John Orr  David Cyganski  Reinhold Ludwig
ca. May 1995
First Crypto Course Announcement

Prerequisites
Working knowledge of “C”. An interest in discrete mathematics and algorithms is highly desirable. Students interested in a further study of the underlying mathematics, can register for MA 4891 (B term) where topics in modern Algebra relevant to cryptography will be treated.

Textbook
September 1995
The first crypto course at WPI (20 years ago)!!

My first TA – Jorge Guajardo
& my first MS student
& my first PhD student
September 1995

... and the first crypto course at GTE Government Systems

---

Course Information

Cryptography and Data Security

General Information

The course gives a comprehensive introduction into the field of cryptology. We will cover the theoretical aspects as well as practical ones. The mathematical background will be developed throughout the course as needed.

Students are expected to have a working knowledge of the C programming language for some of the homework assignments. If you do not have the background, please consult immediately with me.
Before we look at crypto research...

... I had the pleasure to also teach...

- Computer Networks (1995)
- Introduction to VLSI Design (1996)
- Continuous-Time Signal and System Analysis (1998)
- Technical German (2000, 2001)

### MQPs Advised

<table>
<thead>
<tr>
<th>Year Finished</th>
<th># Students</th>
<th>Project Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>3</td>
<td>Coprocessor Board for Cryptographic Applications¹</td>
</tr>
<tr>
<td>1996</td>
<td>3</td>
<td>Secure Transmission System for SNMP⁵</td>
</tr>
<tr>
<td>1996</td>
<td>1</td>
<td>VLSI Implementation of Cryptographic Schemes</td>
</tr>
<tr>
<td>1997</td>
<td>2</td>
<td>Reconfigurable Cryptography Coprocessor Board</td>
</tr>
<tr>
<td>1997</td>
<td>2</td>
<td>Data Link Encryption with DES</td>
</tr>
<tr>
<td>1998</td>
<td>3</td>
<td>Cryptographic Coprocessor with Algorithm Agility</td>
</tr>
<tr>
<td>1998</td>
<td>2</td>
<td>A Parallel Implementation of Pollard’s Rho Method</td>
</tr>
<tr>
<td>1998</td>
<td>1</td>
<td>FPGA-Based Massively Parallel Keysearch Machine</td>
</tr>
<tr>
<td>1998</td>
<td>1</td>
<td>Optimal Extension Fields (CS Dept.)²</td>
</tr>
<tr>
<td>1999</td>
<td>3</td>
<td>Smart Card Based Implementation of an Electronic Wallet</td>
</tr>
<tr>
<td>1999</td>
<td>2</td>
<td>Interface for High-Speed Network Encryption⁶</td>
</tr>
<tr>
<td>1999</td>
<td>3</td>
<td>Cryptographic Coprocessor With Algorithm Agility³</td>
</tr>
<tr>
<td>2000</td>
<td>1</td>
<td>A Random Generator Test Suite⁷</td>
</tr>
<tr>
<td>2000</td>
<td>3</td>
<td>Advanced Encryption Standard (AES) Algorithm Library⁴,⁷</td>
</tr>
<tr>
<td>2000</td>
<td>1</td>
<td>Point Counting on Elliptic Curves with the CM Method (CS Dept.)⁶</td>
</tr>
</tbody>
</table>
Table of Content

1. Teaching

2. Research
Crypto Research Community in the mid-1990s

... was quite manageable

- 2 important conferences (competitive!)
- 2 x 30 research papers per year
- a few 100 participants worldwide
Recall that my Ph.D. was in coding
= no clue about cryptography
... luckily I had really smart graduate students


Pedro Soria-Rodriguez, CP: *Fast Arithmetic Architectures for Public-Key Algorithms over Galois Fields GF((2^n)^m)*. EUROCRYPT 1997

1998: CRIS (CRyptography and Information Security) Labs

... and the first larger research grants arrived

Cryptography on Reconfigurable Hardware: Algorithmic and System Aspects

Cryptographic Library for DSPs
... but very few researchers were working on crypto implementation

Why don’t we organize a workshop on crypto hardware?

Good idea, but what about a name?

Cetin Koc
Oregon State Univ.

me
(bad photo)
Cetin,

The web page is up. Please check ece.wpi.edu/Research/crypt/che

For instance, perhaps there are better abbreviations than "CHE" (for Cryptography Hardware and Embedded systems) for the workshop, but for now it's short and easy to use.

Regards, Christof
Christof,

Let's use the acronym: **CHWES Workshop**. It is better to say either "CHWES Workshop" or "CHWES Workshop 1999". I prefer CHWES Workshop

**Long Name:** Cryptographic Hardware and Embedded Systems Workshop.

Cetin
Cetin,

I think it would be much better to have an acronym that can be pronounced more easily. What do you think about "CHES"?

CHES would mean that we have the first letter of each noun in "Cryptography Hardware and Embedded Systems" used. I try to call you later today,

Christof
Israeli Scientist Reports Discovery of Advance in Code Breaking

By JOHN MARKOFF
Published May 2, 1999

An Israeli computer scientist is expected to shake up the world of cryptography this week when he introduces a design for a device that could quickly unscramble computer-generated codes that until now have been considered secure enough for financial and government communications.
… but CHES wouldn’t have been possible

without Adam Woodbury

Linda Looft

all CRIS Lab members
... and CHES continued

CHES 2000 @ WPI
... and continued
CHES has become largest intern. Cryptography conference!

CHES Attendance

- Year: 1999 to 2015
- Participants: 0 to 400
- Line chart showing attendance over time.
Late 1990s
Many exciting developments in cryptography

Abstracts of AES-related Papers from the Fast Software Encryption
Workshop (FSE) 2000 ................................................................. 9

Day 1 - Thursday, April 13, 2000

Session 1: “FPGA Evaluations”

An FPGA Implementation and Performance Evaluation of the
AES Block Cipher Candidate Algorithm Finalists ............................ 13
A.J. Elbert, W. Yip, B. Chetwynd, C. Paar

A Comparison of the AES Candidates Amenability to FPGA
Implementation ............................................................................ 28
Nicholas Weaver, John Wawrzynek

Comparison of the hardware performance of the AES candidates
using reconfigurable hardware ...................................................... 40
Kris Gaj, Pawel Chodowiec

Session 2: “Platform-Specific Evaluations”

AES Finalists on PA-RISC and IA-64:
Implementations & Performance ............................................... 57
John Worley, Bill Worley, Tom Christian, Christopher Worley

A comparison of AES candidates on the Alpha 21264 .................. 75
Richard Weiss, Nathan Bonkert

Performance Evaluation of AES Finalists on the High-End
Smart Card .................................................................................. 82
Fumihiko Sano, Masanobu Kozue, Shinichi Kawamura,
Masato Shiba

How Well Are High-End DSPs Suited for the AES Algorithms?
AES Algorithms on the TMS320C6x DSP ................................. 94
Thomas J. Wollinger, Min Wang, Jorge Guajardo, Christof Damm
2000 – finally not alone anymore

Bill Martin
Math Dept.

Berk Sunar
ECE Dept.
2 Ph.D. theses

Gerardo Orlando
Efficient Elliptic Curve Processor Architecture for Field Programmable Logic

Adam J. Elbirt
Reconfigurable Computing for Symmetric-Key Algorithms
2001 – after 7 years at WPI
... beautiful Bochum was calling
3 Students went with me to Bochum

Thoma Wollinger, PhD 2004
CEO Escrypt GmbH

André Weimerskirch, PhD 2004
UMich (2:50pm talk today)

Jorge Guajardo, PhD 2004
Bosch Research Pittsburgh
Some of the things we did at U Bochum

Built a large research center in IT Security

... and I am still teaching a lot of cryptography
... and this is what happened at WPI
WPI Faculty in Security 2015

... and much success with research
What have we learned from the last 20 years?

If you want to grow a large research program in security – get rid of Christof.
Thank you for your attention!

1999

2015