Horst Görtz Institut
für Sicherheit in der Informationstechnik

HGI-News

Horst Görtz Institut für Sicherheit in der Informationstechnik
Ruhr-Universität Bochum, Universitätsstr. 150, D-44780 Bochum
Tel.: +49 - (0)234 - 32 23262, Fax.: +49 – (0)234 – 32 14430
Web: http://www.hgi.ruhr-uni-bochum.de

Nr. 02 Dienstag, 8. Juli 2003

CALL FOR PARTICIPATION

5TH WORKSHOP ON CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS

CHES2003

Cologne, Germany
September 7 – 10, 2003

The focus of this workshop is on all aspects of cryptographic hardware and security in embedded systems. The workshop will be a forum of new results from the research community as well as from the industry. We hope that the workshop will help to fill the gap between the cryptography research community and the application areas of cryptography.

This will be the fifth CHES workshop. CHES '99 and CHES 2000 were held at WPI. CHES 2001 was held in Paris, and CHES 2002 in the San Francisco Bay Area. The number of participants has grown to more than 200, with attendees coming from industry, academia, and government organizations.

In addition to selected papers, there will be three invited presentations by *Hans Dobbertin*, *Adi Shamir*, and *Frank Stajano*.

The social program will include a reception on Sunday evening during registration, and a dinner and a banquet on Monday and Tuesday, respectively. Lunches on Monday through Wednesday are also included.

The preliminary program is available on the CHES web page at: www.chesworkshop.org

VERANSTALTUNGEN DIESES MONATS / ACTIVITIES OF THIS MONTH

Montag / Monday	07.07.2003
HGI Seminar Kryptographie und Datensicherheit	13.00 Uhr, Raum IC 4/39 **Marcus Miettinen**, COSY Group and Nokia Research Center, TBA „IT-Security in the Automobile Domain“
Mittwoch / Wednesday	09.07.2003
HGI Seminar Kryptographie und Datensicherheit	13.15 Uhr, Raum IC 4/39 **Jan Pelzl**, COSY Group Ruhr-Universität Bochum „HECC on Embedded Processors“
Montag / Monday	14.07.2003
HGI Seminar Kryptographie und Datensicherheit	13.15 Uhr, IC 4/39 **Christian Stueble,** Universität des Saarlands „Trusted Computing Platforms“
Mittwoch / Wednesday	23.07.2003
HGI Seminar Kryptographie und Datensicherheit	13.15 Uhr, Raum NA 1/51 (Friedrich Sommer Raum) **Tanja Lange**, ITSC Ruhr-Universität Bochum „Improved Algorithms for Efficient Arithmetic on Elliptic Curves Using Fast Endomorphisms“

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Jan Pelzl, COSY Group, Ruhr-Universität Bochum

„HECC on Embedded Processors“

Abstract
Embedded microprocessors in mobile phones or Personal Digital Assistants (PDAs) are becoming more and more part of our private and professional life. The supply of security for data exchange on basis of embedded systems is a very important objection to accomplish. Therefore we are faced with an increased demand for fast asymmetric algorithms especially for small devices.
Hyperelliptic curve cryptosystems (HECC) allow for shorter operands the same level of security than other public-key cryptosystems, such as RSA or Diffie-Hellman. These shorter operands make HECC well suited for the use in embedded systems which have shorter word lengths and less memory than common desktop systems. Hyperelliptic curves are a generalization of elliptic curves and can be used for building discrete logarithm public-key schemes.
The development and finally the implementation of explicit, fast formulae for group operations on hyperelliptic curves is a major part of our research. New results for genus 3 and genus 4 HECC will be presented

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Christian Stueble, Universität des Saarlands

„Trusted Computing Platforms“

Abstract
Microsoft Palladium (Pd) and TCPA are announced to be the next-generation computing platforms, and claimed to improve users' security. However, people are concerned about those capabilities of TCPA/Pd that may allow content providers to gain too much power and control over the use of digital content and users' private information.
In this talk, we argue that TCPA/Pd can be used to improve end-user security provided the controlling operating system is trustworthy. We propose a new architecture of a trustworthy security platform that uses TCPA/Pd hardware features in conjunction with an open-source security kernel we have developed. The design of the security kernel prevents the misuse of the "feared" Digital Rights Management (DRM) capabilities that might be provided by TCPA/Pd.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Tanja Lange, ITSC Ruhr-Universität Bochum

„Improved Algorithms for Efficient Arithmetic on Elliptic Curves Using Fast Endomorphisms"

Abstract
In most algorithms involving elliptic curves, the most expensive part consists in computing multiples of points. This paper investigates how to extend the τ-adic expansion from Koblitz curves to a larger class of curves defined over a prime field having an efficiently-computable endomorphism φ in order to perform an efficient point multiplication with efficiency similar to Solinas' approach presented at CRYPTO '97.
Furthermore, many elliptic curve cryptosystems require the computation of $k_0P + k_1Q$. Following the work of Solinas on the Joint Sparse Form, we introduce the notion of Φ-Joint Sparse Form which combines the advantages of a φ-expansion with the additional speedup of the Joint Sparse Form. We also present an efficient algorithm to obtain the φ-Joint Sparse Form. Then, the double exponentiation can be done using the φ endomorphism instead of doubling, resulting in an average of *l* applications of φ and *l/2* additions, where *l* is the size of the k_i's. This results in an important speed-up when the computation of φ is particularly effective, as in the case of Koblitz curves.

VORHERIGE VERANSTALTUNGEN / PAST ACTIVITIES

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Marcus Miettinen, COSY Group and Nokia Research Center, TBA

„IT-Security in the Automobile Domain"

Abstract
The emergence of advanced wireless network technologies will have a considerable impact on IT applications in the future automobile environment. A whole new variety of applications and services will be made available to automobile users, when cars are hooked up to data communication networks like the Internet using broadband wireless connections.
The integration of these new applications in the automobile environment will introduce new hardware, software and communication protocols into the car. Because of this, new security threats may emerge and new attack paths against the car's IT infrastructure can open up. The objective of this talk is to give an overview of possible new applications in the automobile domain, to analyse the security problems that arise with them and to discuss some solution models suitable for tackling these problems.

VERÖFFENTLICHUNGEN / PUBLICATIONS

Prof. Dr. Hans Dobbertin (mit Donald Mills, Eva Nuria Müller, Alexander Pott, Wolfgang Willems). „APN functions in odd characteristic". Discrete Mathematics 267 (2003) 95 - 112.

KONGRESSE, TAGUNGEN, FORSCHUNGSAUFENTHALTE / CONGRESSES, MEETINGS, RESEARCH ABROAD

Prof. Dr. Dobbertin war am 09.05.2003 im Rahmen eines „Study Day" der Mathematical Society of the Flemish Community und der Katholieke Universiteit Leuven an der Universität Brüssel, Belgien. Er hielt dort einen Vortrag zum Thema „Optimality of the AES S-Box".

Prof. Dr. Dobbertin besucht vom 11.-13.08.2003 den 7th Workshop Elliptic Curve Cryptography (ECC 2003) an der University of Waterloo, Ontario, Kanada. Er hält dort einen Invited Talk mit dem Titel "Algebraic Structures in AES – Cryptographically Strong or Risky?".

Jan Pelzl besucht vom 14.-15.08.2003 den Tenth Annual Workshop on Selected Areas in Cryptography (SAC 2003). Er hält dort einen Vortrag mit dem Titel "Low Cost Security – Explicit Formulae for Genus-4 Hyperelliptic Curves".

Prof. Dr. Paar wird vom 17.-19.08.2003 auf der Hot Chips Conference an der Stanford University in Palo Alto, Kalifornien ein halbtägiges Tutorial zu dem Thema „Past and Future of Cryptographic Engineering" anbieten.

Prof. Dr. Dobbertin und **Jan Pelzl** besuchen vom 07.-10.09.2003 den Workshop on Cryptographic Hardware and Embedded Systems 2003 (CHES 2003) in Köln. **Prof. Dr. Dobbertin** hält dort einen Invited Talk mit dem Titel "Algebraic Structures in AES – Cryptographically Strong or Risky?". **Jan Pelzl** wird den Vortrag "Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves" halten.

Prof. Dr. Dobbertin ist vom 26.09.-02.10.2003 im Lorentz-Center der Leiden University, Niederlande. Er hält dort einen Invited Talk. Der Titel wird noch bekanntgegeben.

Redaktionsschluß für
„HGI – News" Nr. 03
Freitag, 01. August 2003
12.00 Uhr.

Redaktion:
Oliver Rausch
Email: oliver.rausch@ruhr-uni-bochum.de

Aleksandra Sowa (Geschäftsführerin, HGI)
Email: aleksandra.sowa@ruhr-uni-bochum.de

HGI – News by email
Senden Sie eine email an: hgi-news@lists.ruhr-uni-bochum.de
Zum Anmelden schreiben Sie „subscribe hgi-news" in den Body
Zum Abmelden schreiben Sie „unsubscribe hgi-news" in den Body

Das Archiv vorheriger Ausgaben ist unter http://www.hgi.ruhr-uni-bochum.de erreichbar.