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. 03 Donnerstag, 14. August 2003

ANNOUNCEMENT

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 (Algebraic Structures in the Design of AES - Cryptographically Strong or Risky?)*, *Adi Shamir (RSA Security Analysis)*, and *Frank Stajano (The Security Challenges of Ubiquitous Computing)*.

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

VORHERIGE VERANSTALTUNGEN / PAST ACTIVITIES

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.

VERÖFFENTLICHUNGEN / PUBLICATIONS

Prof. Dr. Christof Paar und Thomas Wollinger. „Eingebettete Sicherheit und Kryptographie im Automobil: Eine Einführung". Informatik 2003, Workshop: Automotive SW Engineering & Concepts, 33. Annual Meeting of the GI, Frankfurt/M., 29.09.-02.10.2003.

Jan Pelzl, Thomas Wollinger, Prof. Dr. Christof Paar. "Low Cost Security: Explicit Formulae for Genus-4 Hyperelliptic Curves". Selectec Areas in Cryptography – SAC, 14.-15.08.2003.

Jan Pelzl, Thomas Wollinger, Jorge Guarjardo, Prof. Dr. Christof Paar. Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves. Workshop on Cryptographic Hardware and Embedded Systems – CHES, 07.-10.09.2003.

Thomas Wollinger und Prof. Dr. Christof Paar. „How Secure are FPGAs in Cryptographic Applications? ". The International Conference of Field Programmable Logic and Applications – FPL 2003, Lissabon, Portugal, 01.-03.09.2003.

André Weimerskirch (mit Douglas Stebila und Sheueling Chang Shantz). „Generic GF (2^m) Arithmetic in Software and ist Application to ECC2. The Eighth Australasian Conference on Information Security and Privacy (ACISP 2003), Wollongong, Australien, 09.-11.07.2003

Jörg Lange. "Sicherheit als notwendige Eigenschaft computergestützter Informationssysteme - Rechtliche Rahmenbedingungen und gesellschaftliche Aspekte". Arbeitsbericht Nr. 1 des Instituts für Sicherheit im E-Business, Bochum 2003.

Jochen Hundsdörfer und Olaf Siegmund. „ELSTER - Vorteile, Nachteile und IT-Sicherheitsrisiken der elektronischen Einkommensteuererklärung". Arbeitsbericht Nr. 2 des Instituts für Sicherheit im E-Business, Bochum 2003. (Der Bericht entstand in wissenschaftlicher Zusammenarbeit mit dem Rechenzentrum der Finanzverwaltung NRW)

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

Prof. Dr. Paar war am 16.07.2003 auf der „communicate! 2003"-Messe in Köln und hielt dort ein Impulsreferat mit dem Titel „IT-Sicherheit in kleineren und mittleren Unternehmen – (K)ein Thema für den Mittelstand?".

Prof. Dr. Paar und **Tanja Lange** besuchten vom 11.-13.08.2003 den 7th Workshop Elliptic Curve Cryptography (ECC 2003) an der University of Waterloo, Ontario, Kanada. **Prof. Paar** hielt dort einen Invited Talk mit dem Titel "Hyperelliptic Curve Cryptosystems for Embedded Applications". **Tanja Lange** wurde eingeladen, zum Thema „Efficient Arithmetic on (Hyper-)Elliptic Curves over Infinite Fields" zu sprechen.

Jan Pelzl und **André Weimerskirch** besuchten vom 14.-15.08.2003 den Tenth Annual Workshop on Selected Areas in Cryptography (SAC 2003). **Jan Pelzl** hielt dort einen Vortrag mit dem Titel "Low Cost Security – Explicit Formulae for Genus-4 Hyperelliptic Curves". **André Weimerskirch** sprach über das Thema „Zero Common-Knowledge Authentication for Pervasive Networks".

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.

Thomas Wollinger besucht vom 01.-03.09.2003 die „International Conference on Field Programmable Logic and Applications – FPL 2003" in Lissabon, Portugal. Er hält dort den Vortrag "How Secure are FPGAs in Cryptographic Applications?"

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 auf dem Workshop „Mathematics of Cryptology" einen Invited Talk mit dem Titel „Some Mathematics Behind the Design of Block Ciphers".

Der Vorstand des Horst Görtz Instituts hat in seiner Sitzung am 09.07.2003 folgende neuen Mitglieder aufgenommen:

Prof. Dr. Lothar Gerritzen, Lehrstuhl IV: Algebra/Geometrie
Prof. Dr. Peter Hammann, LS BWL - Marketing
Prof. Dr. Marion Steven, LS BWL - Produktionswirtschaft
Dipl.-Ök. Christian Einhaus, Lehrstuhl für Finanzierung und Kreditwirtschaft
Dipl.-Ök. Sandra Grunewald, Lehrstuhl Wirtschaftspolitik II
Dipl.-Ing. Philip Klempt, Lehrstuhl für BWL insb. Unternehmensforschung und Rechnungswesen
Dipl.-Ök. Susanne Neuber, Lehrstuhl für Angewandte BWL IV - Marketing
Dipl.-Ök. Klaus Rüdiger, Lehrstuhl für Wirtschaftsinformatik
Dipl.-Ök. Olaf Siegmund, Lehrstuhl für Betriebswirtschaftslehre
Dipl.-Ök. Sebastian Tengler, Lehrstuhl für Produktionswirtschaft

Der Vorstand und die Geschäftsführung heißen die neuen Mitglieder willkommen und hoffen auf eine gute Zusammenarbeit.

Redaktionsschluß für
„HGI – News" Nr. 04
Freitag, 29. 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.