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. 09 Dienstag, 2. März 2004

VERANSTALTUNGEN DIESES MONATS / ACTIVITIES OF THIS MONTH

Montag / Monday HGI Kolloquium „Datenschutz“	31.03.2004 16.00 Uhr, IHK Bochum, Ostring 30-32, 44787 Bochum **Franz John**, Business Development Group, Gemplus mids GmbH „Datenschutzpraxis im Büroalltag“
Montag / Monday HGI Kolloquium „Datenschutz“	31.03.2004 16.30 Uhr, IHK Bochum, Ostring 30-32, 44787 Bochum **Prof. Dr. Helmut Siekmann**, Lehrstuhl für Öffentliches Recht, inbes. Staatsrecht, Ruhr-Universität Bochum „Neue Entwicklungen im Datenschutzrecht“

Sehr geehrte Damen und Herren,

wir freuen uns, Ihnen mitteilen zu können, dass am 31. März 2004 ein **Kolloquium zum Thema „Datenschutz“** stattfindet. Initiiert wird dieses Kolloquium vom Horst Görtz Institut für Sicherheit in der Informationstechnik, der IHK Bochum, RuhrSecure – Das Netzwerk für IT-Sicherheit – sowie dem Amt für Wirtschaft- und Beschäftigungsförderung der Stadt Bochum. Zu dieser Veranstaltung wollen wir Sie hiermit herzlich einladen.
Das Anmeldeformular finden Sie unter folgender URL: *www.bochum.ihk.de*
Das HGI-Kolloquium findet am 31. März 2004 um 16.00 Uhr in der IHK zu Bochum, Ostring 30–32 in 44787 Bochum, statt.
Als Referenten konnten wir gewinnen:
Franz John
Business Development Group, Gemplus mids GmbH
mit einem Vortrag zum Thema: „Datenschutzpraxis im Büroalltag“
Prof. Dr. Helmut Siekmann
Lehrstuhl für öffentliches Recht, insbesondere Staatsrecht, Ruhr-Universität Bochum
mit einem Vortrag zum Thema: „Neue Entwicklungen im Datenschutzrecht“

Nach den Vorträgen, die jeweils ca. 30 Minuten dauern, bietet sich für Sie die Möglichkeit, einer vertiefenden Diskussion mit den Referenten. Zusätzlich werden Sie sich nach der Veranstaltung im Foyer mit anderen Unternehmern und Spezialisten zum Thema austauschen können.

Workshop on
"Algebraic Methods in Cryptography"

University of Dortmund, March 11-12, 2004

Organizing Committee

Prof. Dr. H. Dobbertin, Ruhr-Universität Bochum
Prof. Dr. L. Gerritzen, Ruhr-Universität Bochum
Prof. Dr. M. Kreuzer, Universität Dortmund
Prof. Dr. G. Rosenberger, Universität Dortmund

The workshop takes place in the Hörsaal 6 of the Hörsaalgebäude II of the university of Dortmund.

Preliminary Program for Thursday:

9:00-9:30	Welcome by Prof. Dr. Eberhard Becker ('Rektor der Universität Dortmund'), and by Prof. Dr. Gerhard Rosenberger ('Dekan des Fachbereichs Mathematik')
9:30-10:30	Mina Teicher (Bar-Ilan University): "Braid group techniques and cryptography"
10:30-11:00	Coffee
11:00-12:00	Dorian Goldfeld (Columbia University): "Linear time encryption using braid groups"
12:00-13:00	Lunch
13:00-14:00	Patrick Dehornoy (University of Caen): "Fast methods for braid computing"
14:00-15:00	Vladimir Shpilrain (City College of New York): "Combinatorial group theory and public key" cryptography
15:00-15:15	Coffee
15:15-16:15	Alexei G. Myasnikov (City College of New York)

Preliminary Program for Friday:

9:00-10:00	Paolo Bellingeri (University of Grenoble): Conjugacy and related problems in surface braid groups
10:00-10:30	Coffee
10:30-11:30	Volker Gebhardt (University of Sydney): Additional structure in super summit sets of Garside group elements
11:30-12:30	Dimitri Grigoriev (University of Rennes): Homomorphic cryptosystems over groups and rings and encrypting boolean circuits
12:30-13:30	Lunch
13:30-14:10	Martin Kreuzer (University of Dortmund): Gröbner bases cryptosystems
14:10-14:30	Arkadius Kalka (Ruhruniversität Bochum): Computing preimage braids for the Burau representation
14:30-15:00	Coffee
15:00-16:00	Benjamin Fine (Fairfield University): Encryption Algorithms Using Linear Groups

Weitere Informationen finden Sie unter:
http://www. mathematik.uni-dortmund.de/tagungen/cryptoworkshop2004.html
und *http://www.exp-math.uni-essen.de/zahlentheorie/gkkrypto/index.html*

VORHERIGE VERANSTALTUNGEN / PAST ACTIVITIES

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

19.01.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Stefan Lucks, Universität Mannheim
„Practice and Theory of Related-Key Attacks"

Abstract
The "classical" attack scenarios for block ciphers allow the adversary to choose plaintexts and ask for ciphertexts, or additionally to choose ciphertexts and request plaintexts. "Related-key" attacks give the adversary the additional power to manipulate the secret key. Two practical reasons to study related-key attacks are:
1. Related key attacks have been found useful to evaluate the security of block ciphers (e.g. in the context of the AES-process).
2. Some cryptographic protocols actually allow the adversary to mount a related-key attack against an underlying block cipher. Thus, the security of the protocol can depend on the block cipher's related-key security.
The talk gives examples for related-key attacks against block ciphers and protocols. Also, it presents new theoretical constructions for ciphers provably secure against related-key attacks.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

26.01.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Johannes Ueberberg, SRC GmbH
„Sichere Zahlungsverkehrsmodelle im Internet“

Abstract
Kartengestützte elektronische Bezahlverfahren gibt es derzeit fast ausschließlich an einem Terminal (Kartenleser), das sich physisch beim Händler befindet.
Diese Systeme (insbesondere Kreditkarte, Debitkarte und GeldKarte) werden derzeit weiterentwickelt, um sie auch für Internet-Zahlungen nutzbar zu machen.
In dem Vortrag wird ein Überblick über den Stand der Entwicklungen gegeben.

INSTITUT FÜR SICHERHEIT IM E-BUSINESS

02.02.2004, 16.00 – 18.00 Uhr
GC 4/50, Ruhr-Universität Bochum
Ansgar Heinen, Leiter Produktmarketing Utimaco Safeware AG, Aachen
„Marketing für IT-Sicherheitsprodukte im B2B Markt“
Die Veranstaltung fand in Kooperation mit der Bochumer Marketing Initiative e. V. (bomi) statt.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

02.02.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Thomas Groß, IBM Research Lab Zürich
„Emerging protocols in Federated Identity Management"

Abstract
Many influential industrial players are currently pursuing the development of new protocols for federated identity management. The Security Assertion Markup Language (SAML), Liberty, and WS Federation are the most important examples of this new protocol class and will be widely used in business-to-business scenarios to reduce user-management costs. All of them utilize constraint-based specifications and techniques of modular design, but do not include general security analyses. We analyze the security of the SAML Single Sign-on Browser/Artifact profile, which is the most important protocol of this class and already included in all major access control products. We demonstrate flaws of SAML Single Sign-on by mounting exemplary attacks on the protocol. Given this result, we also deduce the need for a methodology of Research to model, analyze and prove the security of this new protocol class.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

09.02.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Roger Oyon, Universität Essen
„Fast Arithmetic on Jacobians of Picard Curves

Abstract
In this paper we present a fast addition algorithm in the Jacobian of a Picard curve over a finite field $\mathbb F_q$ of characteristic different from 3. This algorithm has a nice geometric interpretation, comparable to the classic "chord and tangent" law for the elliptic curves. Computational cost for addition is $144M + 12SQ + 2I$ and $158M + 16SQ + 2I$ for doubling.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

16.02.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Bernhard Loehlein, T-Systems
„IP Multicast Security"

Abstract
T-Systems is currently developing a Multicast Security Gateway, called MuSeGa, which enables secure content distribution over multicast networks. The concept is compatible to the IETF MSEC architecture which is a general framework for multicast security at the IP layer.
IPSec is the well defined and accepted standard for security in unicast IP. In the step from unicast to multicast there arise several problems concerning security: group key agreement, key management, source authentication, ...
Our main focus in this talk is on the status of standardization in the IETF and an overview of efficient group key management algorithms for IP multicast.

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

Prof. Dobbertin wurde eingeladen, Mitglied im Programm Komitee der im Herbst stattfindenden „Conference on Countering Post Modern Terrorism, Cyber and Bio Terrorism, e-Crime History, Current Scenarios and Future Threats" zu werden. Veranstaltet wird diese Konferenz von der Heinrich-Heine-Universität, Düsseldorf, dem International Policy Institute for Counter-Terrorism, University Herzliya, Israel, dem Arbeitskreis Schutz kritischer Infrastrukturen, der Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. und der Gesellschaft für Informatik e.V.

CALL FOR PAPERS

Conference on Cryptographic Hardware and Embedded Systems 2004
(CHES 2004)

www.chesworkshop.org

Cambridge (Boston), USA
August 11-13, 2004

Second Call for Papers

The 6th CHES Conference will be held in Cambridge, Massachusetts (next to Boston.) Following the tradition of previous CHES conferences, it will take place on the Wednesday-Friday immediately preceeding CRYPTO 2004, which starts on Sunday, August 15.

The full Call for Papers is available on the CHES webpage at:
www.chesworkshop.org

CALL FOR CONTRIBUTIONS

Fourth Conference on the Advanced Encryption Standard (AES)
"AES – State of the Crypto Analysis"

AES4

www.aes4.org

Hilton Hotel Bonn, Germany
10-12 May, 2004

Besides several invited talks by various specialists in the field, the program of AES4 contains also slots to be filled in by submitted contributions. The programme committee invites submissions concerning different aspects of the AES cipher (Rijndael).

This includes, but is not limited to:

- cryptographic attacks on full or reduced versions
- observations about the design that may be relevant to the security
- protecting implementations against side-channel attacks
- comparisons with other block ciphers

All submissions will be reviewed.

Instructions for Authors

Authors who wish to present their results are invited to submit a paper of at most 15 pages describing their contribution. The submission should start with a title and a short abstract summarizing the paper. The submission must be **anonymous**, with no author names, affiliations, acknowledgements, or obvious references.

All submissions should be sent by email to sowa@hgi.ruhr-uni-bochum.de. Submissions should be in PostScript, Adobe PDF or Word format.

Important Dates

Submission deadline:	March 31st, 2004
Acceptance notification:	April 15th, 2004
Workshop:	10-12 May, 2004

Redaktionsschluß für
„HGI – News" Nr. 09
Freitag, 26. März 2004
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
Abonnement unter: http://lists.ruhr-uni-bochum.de/mailman/listinfo/hgi-news

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