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. 01 Donnerstag, 26. Juni 2003

VERANSTALTUNGEN DIESES MONATS / ACTIVITIES OF THIS MONTH

Montag / Monday, HGI Seminar Kryptographie und Datensicherheit	30.06.2003,13.00 Uhr, IC 4/39 **Jan Pelzl,** COSY Group, Ruhr-Universität Bochum „HECC on embedded microprocessors“
Montag / Monday, HGI Seminar Kryptographie und Datensicherheit	23.06.2003, 13.15 Uhr, NA 1/51 **Svetlana Nikova**, ESAT/COSIC, K. U. Leuven, Belgium “(Proactive) Verifiable Secret Sharing and DKDC schemes”
Mittwoch / Wednesday, Institut für Sicherheit im E-Business	18.06.2003, Haus für IT-Sicherheit, Bochum **Prof. Dr. Christof Paar,** Lehrstuhl für Kommunikationssicherheit, RUB „IT-Sicherheit und Kryptographie in ‚Pervasive Computing' Szenarien“
Montag / Monday, HGI Seminar Kryptographie und Datensicherheit	16.06.2003, 13.15 Uhr, IC 4/39 **Marcus Schumacher,** Department of Computer Science, TU Darmstadt “Security Patterns – Get It Right The 1st Time…”

VORHERIGE VERANSTALTUNGEN / PAST ACTIVITIES

TREFFEN DES FORSCHUNGSVERBUNDES DATENSICHERHEIT NRW

08.05.2003
Prof. Dr. Christof Paar, Lehrstuhl für Kommunikationssicherheit

„Eingebettete Sicherheit“

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

12.05.2003, 13.00 Uhr
IC 4/39, Ruhr-Universität Bochum
Willi Stein, BSI Bonn

„Schutz kritischer Infrastrukturen und Informationssicherheit: Ansätze zur Bewältigung der neuen Herausforderung"

Abstract
Naturwissenschaftlich-technische Zivilisationen sind verletzlich, das wird uns täglich vor Augen geführt. Das Skelett dieser Zivilisationen bilden die Infrastrukturen, z.B. Energie, Telekommunikation, Medien, Transport- und Verkehr, Notfall- und Rettungswesen etc., die sich aus physischen Anteilen und IT-Anteilen zusammensetzen. Der Weg in die IT-Gesellschaft bringt zwangsläufig neue Verletzlichkeiten und Abhängigkeiten mit sich. Wenn in Staat, Wirtschaft und Gesellschaft von traditionellem Handeln zu
IT-gestütztem Handeln in einem gemeinsamen "Datenraum" übergegangen wird, dann werden alle Lebensbereiche von einem zuverlässigen und sicheren Funktionieren der Informations- und Kommunikationstechnik (IKT) abhängig. In dem Vortrag wird ein Überblick über das im Entstehen befindliche Arbeitsfeld "Critical Infrastructure Protection (CIP)" bzw. "Schutz kritischer Infrastrukturen (KRITIS)" gegeben. Ziel des Infrastrukturschutzes ist es, Bedrohungen, Verletzlichkeiten und Risiken von Staat, Wirtschaft und Gesellschaft durch umfassende landesweite sowie staatenübergreifende Maßnahmen, auch zwischen Staat und Privatwirtschaft, zu reduzieren, z.B. durch einen Mehr-Säulen-Ansatz mit informationstechnischem Schutz, Prävention, Lagebeurteilung und Frühwarnung sowie Entscheidungsunterstützung und Beratung im Rahmen von Dienstnetzwerken. Infrastrukturschutz ist auf Informationssicherheit angewiesen, will aber darüber hinausgehen. Die bislang vorgeschlagenen Infrastrukturschutzkonzepte lassen einen erheblichen - vor allem interdisziplinären - Forschungsbedarf erkennen.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

19.05.2003, 14.00 Uhr
NA 1/51 (Friedrich Sommer Raum), Ruhr-Universität Bochum
Gary McGuire, Department of Mathematics, NUI Maynooth, Co. Kildare, Ireland

„A Case when Three Weights in a Cyclic Code is Impossible"

Abstract
We show that the dual code of the cyclic code C with two zeros, alpha and alpha^t, cannot have three weights in the case that m is even, t= 0 (mod 3), and d(C) > 3. The proof involves the partial calculation of a coset weight distribution.

TREFFEN DES FREUNDESKREISES LEHRSTUHLS FÜR SOFTWARETECHNIK

20.05.2003
Prof. Dr. Christof Paar, Lehrstuhl für Kommunikationssicherheit

„Datensicherheit und Pervasive Computing"

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

16.06.2003, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Marcus Schumacher, Department of Computer Science, TU Darmstadt

„Security Patterns – Get It Right The 1st Time…"

Abstract
Wir können heute eine stetig zunehmende Zahl an Sicherheitsvorfällen beobachten. Um diese unbefriedigende Situation zu verbessern, müssen wir die Lücke zwischen der Theorie und der Praxis im Bereich der IT Sicherheit schließen. Gleichfalls müssen wir darauf hinarbeiten, dass Lücken in dem Sicherheitslernprozess geschlossen werden, um zumindest die bekannten Fehler zukünftig zu verhindern, bevor es zu einem Vorfall kommt.
Als Lösung bieten sich Security Patterns an. Diese sind insbesondere dann hilfreich, wenn die Verantwortlichen für Sicherheit keine entsprechende Erfahrung haben oder Sicherheitsaspekte nicht mit hoher Priorität berücksichtigt werden.

INSTITUT FÜR SICHERHEIT IM EBUSINESS

18.06.2003
Haus für IT-Sicherheit, Bochum
Prof. Dr. Christof Paar, Lehrstuhl für Kommunikationssicherheit, RUB

„IT-Sicherheit und Kryptographie in ‚Pervasive Computing' Szenarien"

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

23.06.2003, 13.15 Uhr
NA 1/51 (Friedrich Sommer Raum), Ruhr-Universität Bochum
Svetlana Nikova, ESAT/COSIC, K. U. Leuven, Belgium

„(Proactive) Verifiable Secret Sharing and DKDC schemes"

Abstract
In 1979 Shamir introduced the concept of secret sharing schemes (SSS) as a tool to protect a secret simultaneously from exposure and from being lost. It allows a so called dealer to share the secret among a set of entities, usually called players, in such a way that only certain specified subsets of the players are able to reconstruct the secret while smaller subsets have no information about it. Since an SSS neither guarantees reconstructability when some shares are incorrect (e.g. in presence of adversary), nor verifiability of a shared value a stronger primitive Verifiable Secret Sharing (VSS) has been introduced in 1985 by Chor et al. In a VSS a dealer distributes a secret value among the players, where the dealer and/or some of the players may be cheating. It is guaranteed that if the dealer is honest, then the cheaters obtain no information about the secret, and all honest players will later be able to reconstruct it, without the help of the dealer. Even if the dealer cheats, a unique value will be determined and is reconstructable without the cheaters help. When the secret value needs to be maintained for a long period of time we need a proactive security. Proactive security refers to security and availability in the presence of a mobile adversary. Proactive security for secret sharing was first suggested by Ostrovski and Yung in 1991 and further specialized by Herzberg et al. 1995 and the corresponding notions of Proactive SSS were introduced.
vThe objective of this talk is to give an elementary introduction to fundamental concepts, techniques and results of verifiable secret sharing. We also introduce such concepts as security against malicious attacks, proactive secret sharing and for some of these important primitives we discuss realization. Topics covered include these classical results and their applications e.g. distributed key distribution center. A Key Distribution Center of a network is a server enabling private communications within groups of users. A new approach to the key distribution was introduced by Naor et al. in 1999. A Distributed Key Distribution Center (DKDC) is a set of n servers of a network that jointly realize the function of a Key
Distribution Center. A user who needs to participate in a conference sends a key-request to a subset of his own choosing of the n servers, and the contacted servers answer with some information enabling the
user to compute the conference key. In such a model, a single server by itself does not know the secret keys, since they are shared between the n servers. We will show how can be built a robust Distributed Key Distribution Center Scheme secure against active and mobile adversary. For this talk a general background in cryptography is required.

ANKÜNDIGUNG / ANNOUNCEMENT

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

07.07.2003, 13.00 Uhr
IC 4/39, Ruhr-Universität Bochum
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.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

14.07.2003, 13.00 Uhr
IC 4/39, Ruhr-Universität Bochum
Thomas Wollinger, COSY Group Ruhr-Universität Bochum

„FPGAs as cryptographic modules"

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

21.07.2003, 13.00 Uhr
Tanja Lange, ITSC Ruhr-Universität Bochum, TBA

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

Abstract
Curve-endomorphisms allow to obtain further speed-up. We shortly present Koblitz curves, the generalized GLV method and trace zero subvarieties.
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. Hans Dobbertin. "Nonlinear Boolean Functions: Recent Progress, Methods, and Perspectives". Proceeding von: International Workshop on Coding and Cryptography, WCC 2003.

Prof. Dr. Christof Paar. „IT-Sicherheit für Kühlschränke und Milchkartons". RubBITS, Ausgabe 11, S.4.

Prof. Dr. Christof Paar, C. Koc (Editoren). Special issue on cryptographic hardware and embedded systems. IEEE Transactions on Computers, April 2003.

Magnus Daum. „An Algorithm for Checking Normality of Boolean Functions". Proceeding von: International Workshop on Coding and Cryptography, WCC 2003.

Tanja Lange. "Koblitz Curve Cryptosystems". STJournal of System Research.

Tanja Lange (mit M. Ciet, F. Sica und J.-J. Quisquater). "Improved Algorithms for Efficient Arithmetic on Elliptic Curves using Fast Endomorphisms". Proceddings of EUROCRYPT 2003, LNCS 2656, 388-400.

Tanja Lange (mit A. Winterhof). "Interpolation of the Elliptic-Curve Diffie-Hellman Mapping". Proceedings of AAECC 2003, LNCS 2643, 51-60.

Gregor Leander. "Normal and Non-Normal Bent Functions". Proceeding von: International Workshop on Coding and Cryptography, WCC 2003.

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

Patrick Felke war vom 06.-08.01.2003 in Miami, Florida und nahm am „International Workshop on Practice and Theory in Public Key Cryptography 2003 (PKC 2003) " teil. **Magnus Daum** hielt dort einen Vortrag mit dem Titel "On the Security of HFE, HFEv- and Quartz"

Jan Pelzl, Kai Schramm und **Thomas Wollinger** waren vom 08.- 11.01.2003 in St. Etienne, Frankreich und nahmen dort am „International Workshop on Embedded Architectures for Applied Cryptography, CryptArchi" teil.

Jorge Guajardo, Sandeep Kumar, Kai Schramm und **Thomas Wollinger** waren am 20.01.2003 in Eindhoven, Niederlande und nahmen dort am Workshop „Can we trust networks?“ teil.

Jan Pelzl nahm am 29.01.2003 in Bonn am Seminar „Faktorisierung ganzer Zahlen“ teil.

Gregor Leander erhielt ein Stipendium der Marie Curie Fellowship Association und besuchte vom 01.02.-30.04.03 die Universität in Aarhus, Dänemark.

Tanja Lange war vom 11.-13.02.2003 in Tokio beim „2003 International Symposion on Next Generation Cryptography and Related Mathematics" und hielt den eingeladenen Vortrag über "Efficient arithmetic on (hyper-) elliptic curves".

Patrick Felke, Tanja Lange und **Gregor Leander** waren vom 24.-27.02.2003 in Lund, Schweden und nahmen am „Fast Software Encryption (FSE) Workshop“ und sowie am 2. Workshop des EU-Projektes STORK teil. **Kai Schramm** hielt auf dem FSE-Workshop den Vortrag „A New Class of Collision Attacks and its Application to DES".

Tanja Lange war vom 03.-07.03.2003 in Gainesville, Florida und hielt dort auf der Konferenz "Computational Aspects of Algebraic Curves“ einen Vortrag über „Efficient arithmetic on (hyper-) elliptic curves over finite fields".

Patrick Felke, Tanja Lange und **Aleksandra Sowa** waren vom 24.-27.03.2003 in Roquencourt, Frankreich und nahmen dort am „WCC – Workshop on Codingtheory and Cryptography“ teil. **Magnus Daum** hielt dort einen Vortrag zum Thema „An Algorithm for Checking Normality of Boolean Functions".
Gregor Leander hielt den Vortrag "Normal and Non-Normal Bent Functions". **Prof. Dr. Hans Dobbertin** hielt dort einen Invited Talk über „Nonlinear Boolean Functions: Recent Progress, Methods, and Perspectives".

Magnus Daum, Patrick Felke und **Aleksandra Sowa** waren vom 28.04.-03.05.2003 in Bedlewo, Polen und nahmen dort an der Konferenz „Cryptology – fundamentals and frontiers“ teil. **Prof. Dr. Dobbertin** hielt dort den Vortrag „Collisions – Why, when and how to avoid them".

Magnus Daum, Patrick Felke, Sandeep Kumar, Tanja Lange, Kai Schramm und **Thomas Wollinger** waren vom 05.-08.05.2003 in Warschau, Polen und nahmen dort an der „Eurocrypt 2003“ teil

Tanja Lange war vom 12.-16.05.2003 an der „Ecole Européenne Géométrie Algébrique et Théorie de l'Information“ in Luminy, Frankreich.

Prof. Dr. Christof Paar war am 11.06.2003 in Brüssel, Belgien bei einem „Hearing at the European Commission“ und einem STORK meeting.

Redaktionsschluß für
„HGI – News“ Nr. 02
Freitag, 04. Juli 2003
12.00 Uhr.

Redaktion:
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.