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. 10 Mittwoch, 09. Juni 2004

Der Vorstand des Horst Görtz Instituts hat in seiner Sitzung am 10.02.2004 folgende neuen Mitglieder aufgenommen:

Prof. Dr. Brigitte Werners, LS für BWL, insbes. Unternehmensforschung und Rechnungswesen
Prof. Dr. Stephan Paul, LS für Finanzierung und Kreditwirtschaft
Prof. Dr. Ahmad-Reza Sadeghi, LS für Kommunikationssicherheit

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

VERANSTALTUNGEN DIESES MONATS / ACTIVITIES OF THIS MONTH

Montag / Monday
HGI Seminar Kryptographie und Datensicherheit

14.06.2004
13.15 Uhr, IC 4/39, Ruhr-Universität Bochum
Kerstin Lemke, Lehrstuhl für Kommunikationssicherheit, Ruhr-Universität Bochum
„DPA on n-bit sized Boolean and Arithmetic Operations and its application to IDEA, RC6 and the HMAC-Construction "

Mittwoch / Wednesday
HGI Seminar Kryptographie und Datensicherheit

16.06.2004
13.30 Uhr, NA 1/58 (Friedrich Sommer Raum), Ruhr-Universität Bochum
Eike Kiltz, Lehrstuhl Mathematik und Informatik, Ruhr-Universität Bochum
„Secure Constant Round Multi-Party Computation for Equality, Comparison and Bits"

Montag / Monday
HGI Seminar Kryptographie und Datensicherheit

21.06.2004
13.15 Uhr, IC 4/39, Ruhr-Universität Bochum
Howon Kim, Lehrstuhl für Kommunikationssicherheit, Ruhr-Universität Bochum
Der Titel wird noch bekannt gegeben.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Kerstin Lemke, Lehrstuhl für Kommunikationssicherheit, Ruhr-Universität Bochum

„ DPA on n-bit sized Boolean and Arithmetic Operations and its application to IDEA, RC6 and the HMAC-Construction "

Abstract

Differential Power Analysis (DPA) has turned out to be an efficient method to attack the implementations of cryptographic algorithms and has been well studied for ciphers that incorporate a nonlinear substitution box as e.g. in DES. Other product ciphers and message authentication codes are based on the mixing of different algebraic groups and do not use look-up tables. Among these are IDEA, the AES finalist RC6 and HMAC-constructions such as HMAC-SHA-1 and HMAC-RIPEMD-160. These algorithms restrict the use of the selection function to the Hamming weight and Hamming distance of intermediate data as the addresses used do not depend on cryptographic keys. Because of the linearity of the primitive operations secondary DPA signals arise.

This presentation gives a deeper analysis of the characteristics of DPA results obtained on the basic group operations XOR, addition modulo 2^n and modular multiplication using multi-bit selection functions. The results shown are based both on simulation and experimental data.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Eike Kiltz, Lehrstuhl für Kommunikationssicherheit, Ruhr-Universität Bochum

„ Secure Constant Round Multi-Party Computation for Equality, Comparison and Bits "

Abstract

In this presentation we give efficient and secure constant round multi-party protocols to compute shares of the bit indicating if a shared input value $x \in \Z_q$ is zero or not providing a missing building stone for many constant round linear algebra protocols from a paper from Cramer and Damgaard [CD01]. Furthermore, we present a secure and efficient constant round protocol for computing shares of the binary representation of a shared input value $x \in \Z_q$ improving on a result from [ACS02].

Our techniques can also be used to securely compute in constant rounds shares of the bit indicating which of two shared inputs is bigger. The main building stone of our protocols is a protocol to convert fromadditives shares over $\Z_q$ to additive shares over the integers that works for all shared inputs from $\Z_q$. We also present a constant round protocol to efficiently compute a secure approximation of the value $1/p$ for a given shared p. This enables us to do efficient computation modulo a shared secret in a constant number of rounds. Until now, for all the above mentioned problems, there were in general no constant round protocols known. The main tools to obtain our protocols are the Chinese Remainder Representation (CRR) and Lagrange Interpolation.

ANKÜNDIGUNG / ANNOUNCEMENT

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

05.07.2004, 13.15 Uhr

IC 4/39, Ruhr-Universität Bochum

Mark Manulis, Lehrstuhl für Netz- und Datensicherheit, Ruhr-Universität Bochum

„Pseudonym Generation Scheme for Ad-Hoc Group Communication based on IDH"

INSTITUT FÜR SICHERHEIT IM E-BUSINESS (ISEB)
VERANSTALTUNG IM RAHMEN DER VORTRAGSREIHE DES ISEB IM SS 04

06.07.2004, 17.30 – 19.00 Uhr

IHK im mittleren Ruhrgebiet zu Bochum, Ostring 30-32, 44787 Bochum

Jörg Grosche, Experte Produktmanagement, Deutsche Telekom

„ENX® Solution - Sichere, flexible und vertrauensvolle Datenkommunikation für die Zusammenarbeit zwischen Unternehmen"

INSTITUT FÜR SICHERHEIT IM E-BUSINESS (ISEB)
GEMEINSCHAFTSVERANSTALTUNG DES CCEC UND DES ISEB

13.07.2004, 16.00 – 17.30 Uhr

GC 4/50, Ruhr-Universität Bochum

Dr. Hans-Dieter Zimmermann, Universität Münster, Institut für Wirtschaftsinformatik/Universität St. Gallen, Schweiz

„Die Rolle des Vertrauens in der Digitalen Ökonomie"

VORHERIGE VERANSTALTUNGEN / PAST ACTIVITIES

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“

Prof. Dr. Helmut Siekmann, Lehrstuhl für Öffentliches Recht, insbes. Staatsrecht, Ruhr-Universität Bochum
„Neue Entwicklungen im Datenschutzrecht“

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

19.04.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Marc Stevens, Lehrstuhl für Informationssicherheit und Kryptologie, Ruhr-Universität Bochum
„Arithmetic on Hyperelliptic curves of genus 1 and 2“

Abstract
The talk is about arithmetic on hyperelliptic curves of genus 1 and 2 over finite fields of even characteristic. It discusses the group operations for these curves and presents new doubling formulas for some cases. Furthermore it presents the comparison we've made between different implementations of calculating scalar multiples on Koblitz curves and with different bases for the field.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

26.04.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Jonathan Hammell, COSY Group, Ruhr-Universität Bochum (University of Waterloo Co-op)
„Recognition in a Low-Power Environment"

Abstract
Extremely low-power devices, such as those involved in sensor networks, are becoming more prevalent as ubiquitous computing scenarios descend from the theoretical into realistic applications. Building security into such applications from the beginning is important and requires inventive new techniques since traditional protocols are designed for much more powerful environments.
This talk contrasts traditional security definitions with some proposed, intending to provide a basis on which to examine protocols designed for such restrictive environments. Some previously proposed protocols are examined according to their ability to satisfy both the security and low-power requirements.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

03.05.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Kai Schramm, Lehrstuhl für Kommunikationssicherheit, Ruhr-Universität Bochum
„Internal Collisions in AES“

Abstract
Recently a new class of collision attacks which was originally suggested by Hans Dobbertin has been introduced. These attacks use side channel analysis to detect internal collisions and are generally not restricted to a particular cryptographic algorithm. As an example, a collision attack against DES was proposed which combines internal collisions with side channel information leakage. It had not been obvious, however, how this attack applies to non-Feistel ciphers with bijective S-boxes such as the Advanced Encryption Standard (AES).
This contribution takes the same basic ideas and develops new optimized attacks against AES. Our major finding is that the new combined analytical and side channel approach reduces the attack effort compared to all other known side channel attacks. We develop several versions and refinements of the attack. First we show that key dependent collisions can be caused in the output bytes of the mix column transformation in the first round. By taking advantage of the birthday paradox, it is possible to cause a collision in an output with as little as 20 measurements. Each collision will reveal at least 8 bits of the secret key. Furthermore, in an optimized attack, it is possible to cause collisions in all four output bytes of the mix column transformation with an average of only 31 measurements, which results in knowledge of all 32 key bits. Finally, if collisions are caused in all four columns of the AES in parallel, it is possible to determine the entire 128-bit key with only 40 measurements, which a is a distinct improvement compared to DPA and other side channel attacks.

INSTITUT FÜR SICHERHEIT IM E-BUSINESS (ISEB)
VERANSTALTUNG IM RAHMEN DER VORTRAGSREIHE DES ISEB IM SS 04

04.05.2004, 17.00 Uhr
GC 4/50, Ruhr-Universität Bochum
Dr. Haio Röckle, Geschäftsführer der Röckle IT-Sicherheit GmbH, Bochum
„Praktische und unpraktische Ansätze zum Umgang mit IT-Sicherheit in kleinen und großen Unternehmen"

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

17.05.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Christian Tobias, JLU Gießen
„Design und Analyse kryptografischer Bausteine auf nicht-abelschen Gruppen "

Abstract
Die Public-Key Kryptografie ermöglicht es Teilnehmern, kryptografische Protokolle auszuführen (z.B. vertrauliche Nachrichten zu versenden), ohne dass sie dazu vorher über ein gemeinsames Geheimnis verfügen müssen. Die heutzutage gebräuchlichen Verfahren beruhen dabei meist auf abelschen Gruppen. In letzter Zeit werden jedoch erhebliche Anstrengungen unternommen, kryptografische Verfahren auf nicht-abelschen Gruppen zu konstruieren. Dabei wird die Schwierigkeit des Konjugationsproblems oder einer Variante als zugrundeliegende Sicherheitsannahme verwendet.
Eines dieser neuen Verfahren ist das MOR System, das auf der Schwierigkeit der Berechnung diskreter Logarithmen in der Gruppe der inneren Automorphismen Inn(G) einer nicht-abelschen Gruppe beruht. Das MOR System wird zunächst vorgestellt und die Schwierigkeit des Problems der Berechnung diskreter Logarithmen in Inn(G) diskutiert. Anschließend werden notwendige Bedingungen für die Nutzbarkeit nicht-abelscher Gruppen im MOR System formuliert und die Sicherheit von MOR bei Benutzung einer der bisher vorgeschlagenen Gruppen analysiert.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

24.05.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Jamshid Shokrollahi, Universität Paderborn
„Unifying structures for polynomial and normal bases"

Abstract
We develop an efficient circuit for multiplication of elements in a binary finite field represented with respect to a normal basis of type II. The circuit uses an efficient transformation from the normal basis into a suitable polynomial basis, and performs polynomial multiplication concurrently with polynomial reduction and the back-transformation into the normal basis in an efficient manner.
The transformation circuit uses $n+2\mu(n)+\mu(2n)$ XOR gates, and has a propagation delay of $2\lceil \log_2(n)\rceil$, wherein n is the degree of the field extension over $\F_2$, and $\mu(n)$ is a function that is majorized by $n\log_2(n)$. Our multipliers achieve the advantages of both normal and polynomials bases at the same time. The small size of our multipliers makes them attractive for hardware implementations in situations where area is a limited resource, or in situations where pipelining strategies are desired.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

07.06.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Lars Pontow, Lehrstuhl für Kommunikationssicherheit, Ruhr-Universität Bochum
„Elliptic Curve Cryptography as a Case Study for Hardware/Software Codesign"

Abstract
Embedded systems, like Personal Digital Assistants (PDA) and mobile phones, are ubiquitous nowadays. With newer applications, like e-commerce, securing the vulnerable communication in these systems has become extremely important. For accomplishing this kind of security, asymmetric cryptography is required. But a major challenge when implementing asymmetric cryptographic algorithms on embedded systems is the limited CPU power and memory size. Hence dedicated hardware support to accelerate these algorithms is highly desirable. FPGAs are an attractive platform to implement such dedicated hardware in an inexpensive and uncomplicated way.
In this thesis, we analyze performance gain versus the hardware cost for elliptic and hyperelliptic curve cryptosystems, when a certain amount of special hardware is added to the system. For our implementation, we use a typical embedded processor, the ARM 7TDMI. Directly connected to the ARM processor is a XILNX VirtexE XCV2000E FPGA on which the special dedicated hardware is implemented. We implement ECC over $\mathbb{F}_{2^{167}}$ and HECC of genus 2 over $\mathbb{F}_{2^{81}}$. Thus, HECC provides about the same level of security as the ECC.

Our fastest ECC scalar multiplication is 1.9 ms at 25 MHz, which is 390.4 times faster than our implementation without dedicated hardware. We use 3220 slices on the FPGA for the dedicated hardware. The fastest HECC scalar multiplication takes 6.2 ms at 25 MHz using 1794 slices for the dedicated hardware, which is 248.4 times faster than the non-accelerated version.

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

Susanne Neuber und Marcus Heitmann vom Institut für Sicherheit im E-Business (ISEB) hielten auf der Paderborner Frühjahrstagung am 15.4.2004 den Vortrag "Chancen und Risiken des Web-EDI-Einsatzes im Supply Chain Management von Zulieferer-OEM-Beziehungen"

ANKÜNDIGUNGEN / ANNOUNCEMENTS

THE 8TH WORKSHOP ON ELLIPTIC CURVE CRYPTOGRAPHY (ECC 2004)

www.cacr.math.uwaterloo.ca/conferences/2004/ecc2004/announcement.html

Ruhr-University Bochum, Germany
September 20, 21 & 22, 2004

ECC 2004 is the eighth in a series of annual workshops dedicated to the study of elliptic curve cryptography and related areas. The main themes of ECC 2004 will be:

- The discrete logarithm problem.
- Efficient parameter generation and point counting.
- Provably secure cryptographic protocols.
- Efficient software and hardware implementation.
- Side-channel attacks.
- Deployment of elliptic curve cryptography.

It is hoped that the meeting will continue to encourage and stimulate further research on the security and implementation of elliptic curve cryptosystems and related areas, and encourage collaboration between mathematicians, computer scientists and engineers in the academic, industry and government sectors.
There will be approximately 15 invited lectures (and no contributed talks), with the remaining time used for informal discussions. There will be both survey lectures as well as lectures on latest research developments.

SPONSORS:

BSI - Bundesamt für Sicherheit in der Informationstechnik
DFG-Graduate School on Cryptography
ECRYPT - European Network of Excellence in Cryptography
Ruhr-University Bochum
University of Waterloo

ORGANIZERS:

Gerhard Frey (University of Duisburg-Essen)
Tanja Lange (Ruhr-University Bochum)
Alfred Menezes (University of Waterloo)
Christof Paar (Ruhr-University Bochum)
Scott Vanstone (University of Waterloo)

CONFIRMED SPEAKERS:

Roberto Avanzi (University of Duisburg-Essen, Germany)
Paulo Barreto (Scopus Tecnologia, Brazil)
Pierrick Gaudry (LIX Paris, France)
Marc Joye (Gemplus, France)
Norbert Luetkenhaus (University of Erlangen, Germany)
Kim Nguyen (Bundesdruckerei, Germany)
Alexander May (University of Paderborn, Germany)
Matt Robshaw (Royal Holloway University of London, UK)
Werner Schindler (BSI, Germany)
Jasper Scholten (KU Leuven, Belgium)
Hovav Shacham (Stanford University, USA)
Igor Shparlinski (Macquarie University, Australia)
Nigel Smart (University of Bristol, UK)
Thomas Wollinger (Ruhr-University Bochum, Germany)

CALL FOR PAPERS

Workskop on Cryptographic Hardware and Embedded Systems (CHES 2004)

www.chesworkshop.org
Cambridge (Boston), USA
August 11–13, 2004
sponsored by IACR

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. Of special interest
are contributions that describe new methods for e±cient hardware implementations and high-speed software for embedded systems, e.g., smart cards, microprocessors, DSPs, etc. We hope that the workshop will help to fill the gap between the cryptography research community and the application areas of cryptography. Consequently, we encourage submissions from academia, industry, and other organizations. All submitted papers will be reviewed.
This will be the sixth CHES workshop. CHES'99 and CHES 2000 were held at WPI. CHES 2001 was held in Paris, CHES 2002 in the San Francisco Bay Area, and CHES 2003 in Cologne. The number of participants has grown to more than 230, with attendees coming from industry, academia, and government organizations. The topics of CHES 2004 include but are not limited to:

** Computer architectures for public-key and secret-key cryptosystems*
** Reconfigurable computing in cryptography & FPGAs*
** Cryptography for pervasive computing*
** Cryptography in wireless applications (mobile phone, LANs, etc.)*
** Smart card attacks and architectures*
** True and pseudo random number generators*
** Embedded security*
** E±cient algorithms for embedded processors*
** Cryptographic processors and co-processors*
** Nonclassical cryptographic technologies*
** Security in pay-TV systems*
** Tamper resistance on the chip and board level*
** Special-purpose hardware for cryptanalysis*
** Device identification*

Instructions for Authors

Authors are invited to submit original papers. Electronic submission is strongly encouraged. A detailed description of the electronic submission procedure appears on the CHES webpages.
The submission must be anonymous, with no author names, a±liations, acknowledgements, or obvious references. It should begin with a title, a short abstract, and a list of keywords. The paper should be at most 12 pages (excluding the bibliography and clearly marked appendices), and at most 15 pages in total, using at least 11-point font and reasonable margins. Submissions not meeting these guidelines risk rejection without consideration of their merits. All submissions will be blind-refereed.
Only original research contributions will be considered. Submissions must not substantially duplicate work that any of the authors have published elsewhere or have submitted in parallel to any other conferences or workshops that have proceedings.

Important Dates

Submission deadline: March 2nd, 2004.
Acceptance notification: April 28th, 2004.
Final Version due: May 30th, 2004.
Workshop: August 11th – 13th, 2004 (just before CRYPTO 2004, August 15th –19th).

Mailing List

If you want to receive subsequent Call for Papers and registration information, please send a brief mail to mailinglist@chesworkshop.org.

ANKÜNDIGUNGEN DER HGI-PARTNER / ANNOUNCEMENTS BY CO-OPERATING ORGANISATIONS

1. esgeo Konferenz:
Sichere Geoinformationen
esgeo - Embedded IT-Security in der Geoinformation?
30.06.2004, 09.00 – 17.30 Uhr
Haus für IT-Sicherheit, Lise-Meitner-Allee 4, 44801 Bochum
Veranstalter: CeGi Center for Geoinformation GmbH, GITS Gesellschaft für IT-Sicherheit AG, escrypt GmbH

Wie schütze ich meine Geodaten vor mutwilliger oder fahrlässiger Manipulation/Modifikation?
Wie kann ein LBS-Anbieter für die Sicherheit meiner Daten garantieren?
Wie sichere ich meine Geodatenbestände vor unbefugter Weitergabe an Dritte?
Wie kann bei Großveranstaltungen die Sicherheit der Notfallsysteme gewährleistet werden?
Wer bedroht meine Geodaten?
Wie kann ich meine Geodaten sicher über das Internet vertreiben?

Diese und noch viele andere Fragen wollen wir am 30. Juni 2004 auf der Veranstaltung gemeinsam erarbeiten und beantworten.

Geoinformationen bilden einen wesentlichen Teil des in der modernen Informations- und Kommunikations-gesellschaft vorhandenen Wissens. Geoinformationen werden auf allen Ebenen in Politik, Verwaltung, Wirtschaft und Wissenschaft und vom Bürger benötigt. Geoinformationen müssen leicht auffindbar und jederzeit verfügbar sein. Fragen nach dem Schutz eigener oder fremder Geodaten treten immer häufiger in den Vordergrund. Daher ist Datensicherheit auch für den Geobereich ein aktuelles und wichtiges Thema.

Die von der Gesellschaft für IT-Sicherheit AG und der CeGi Center für Geoinformation GmbH * organisierte esgeo-Konferenz am 30. Juni 2004 möchte Fragen und Probleme rund um die Zusammenhänge zwischen Geodaten und Datensicherheit darstellen und diskutieren. Die ganztägige Konferenz im Haus für IT-Sicherheit in Bochum behandelt aktuelle Themen der Geobranche im Hinblick auf Datensicherheitsaspekte.

Die Veranstaltung richtet sich an Entscheidungsträger, Geschäftsführer und Mitarbeiter aus Wirtschaft, Verwaltung, Wissenschaft und Politik und möchte so als Kommunikationsplattform die Bereiche Geo und Datensicherheit zusammenbringen.

Weitere Informationen und Anmeldung unter: *http://www.gits-ag.de*

Redaktionsschluß für
„HGI – News“ Nr. 11
Mittwoch, 30. Juni 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.