

Tagungsband zum 9. Kryptotag

Workshop der Fachgruppe Kryptographie in der Gesellschaft für Informatik

Institut für Internet-Sicherheit

Fachhochschule Gelsenkirchen

Fachbereich Informatik

10. November 2008



Programm

- 10:00 Begrüßungskaffee
- 10:30 Begrüßung
- 10:45 **Session 1:**
- 10:45** Ewan Fleischmann, Christian Forler, Michael Gorski, Stefan Lucks
Twister - A new hash function proposal
- 11:10** Martin Schmidt
KronCrypt; Der Approximationssatz von Kronecker in der symmetrischen Kryptographie
- 11:35 Pause
- 11:50 **Invited Talk:** Sibylle Hick secunet
Kryptographie in der Praxis - Der elektronische Reisepass
- 12:30 Mittagspause¹
- 14:00 Rump Session
- 14:10 Rundtour: Selbstvorstellung der Teilnehmer
- 14:40 **Session 2:**
- 14:40** Denise Doberitz
Complete Codings for Visual Cryptography
- 15:05** Christian Dietrich
Extended Access Control – neuer Zugriffsmechanismus für elektronische Ausweisdokumente
- 15:30** Dominique Petersen
Reale Nutzung kryptografischer Verfahren innerhalb von TLS/SSL
- 15:55 Ende der Vorträge
- 17:00 Ausklang des Kryptotages

¹Mensa der Fachhochschule

Inhaltsverzeichnis

TWISTER- A New Hash Function Proposal <i>Ewan Fleischmann</i> ^{*,†} and <i>Christian Forler</i> ^{*,‡} and <i>Michael Gorski</i> ^{*,†} and <i>Stefan Lucks</i> ^{*,†}	4
KronCrypt: Der Approximationssatz von Kronecker in der symmetrischen Kryptographie <i>Carsten Elsner</i> [*] und <i>Martin Schmidt</i> [†]	6
Complete Codings for Visual Cryptography <i>Denise Doberitz</i>	7
Extended Access Control – neuer Zugriffsmechanismus für elektronische Ausweisdokumente <i>Christian J. Dietrich, Prof. Dr. Norbert Pohlmann</i>	8
Reale Nutzung kryptografischer Verfahren innerhalb von TLS/SSL <i>Dominique Petersen</i>	9

TWISTER- A New Hash Function Proposal

Ewan Fleischmann ^{*,†} and Christian Forler ^{*,‡} and Michael Gorski ^{*,†} and Stefan Lucks ^{*,†}

^{*,†}Bauhaus-University Weimar ^{*,‡}Sirrix AG security technologies

Introduction

One of the most used primitives in modern cryptography are hash functions. A hash function $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ is used to compute an n -bit

fingerprint out of an arbitrarily-sized input. Established security requirements for cryptographic hash functions are collision-, pre-image and 2nd pre-image resistance – but ideally, cryptographers expect a good hash function to *behave like a random function*. Nearly all iterative hash functions are designed using the MERKLE-DAMGÅRD construction. A MERKLE-DAMGÅRD hash function is an iterated hash function that uses a fixed length compression function $C : \{0, 1\}^{n_c} \times \{0, 1\}^m \rightarrow \{0, 1\}^{n_c}$ where n_c is the size of the chaining value and m the size of a message block. We have $n = n_c$ for hash functions using the MERKLE-DAMGÅRD construction. By assuming a padded message $M = (M_1, \dots, M_l)$, $|M_i| = m$, $1 \leq i \leq l$ and an internal chaining value $h_i \in \{0, 1\}^{n_c}$ (h_0 is called the initial value) the computation of the hash value for such a message M is as follows:

```
FOR  $i$  FROM 1 TO  $l$  do
   $h_i = C(h_{i-1}, M_i)$ 
RETURN  $h_l$ 
```

The main benefit of the MERKLE-DAMGÅRD transformation is that it preserves collision resistance: if the compression function C is collision resistant, then so is the hash function. Unfortunately, this result does not extend to 2nd pre-image resistance. Recent results highlight some intrinsic limitations of the MERKLE-DAMGÅRD approach. This includes being vulnerable to multicollision attacks, long second-pre-images attacks, and herding. Even though the practical relevance of these attacks is unclear, they highlight some security issues which designers are well advised to avoid or take care of.

Related Work

Most popular hash functions such as MD5, SHA-0 or SHA-1 possess weaknesses in their design, leading to a huge amount of attacks [1, 2, 5]. But also most new hash functions [3, 7] which try to take care for weaknesses in the MERKLE-DAMGÅRD -construction itself were broken soon after their publications [6, 8].

The concept of sponge functions [11] uses an i.e. big internal state that absorbs a message of infinite length and that later squeezes out an hash value of variable size. RADIOGATÚN with XOR sponges and GRINDAHL with truncate-overwrite sponges are the first hash function that use this framework. GRINDAHL was shown to be vulnerable [10].

Our contribution

The design of secure and practical hash functions is of great interest since most hash functions have been broken. Due to the SHA-3 competition many new proposals for hash function primitives will be published in the next months. Our proposal is based on a sponge construction as well as on the

wide-pipe approach [4]. It also includes randomized hashing as proposed in the Haifa framework [12]. The main goal of our approach is to present a fast, secure hash function which is flexible and simple to analyze. We can show that one cannot find a collision after one so called **Mini-Round** and that we obtain full diffusion after two application of a **Mini-Round**.

More precise, it uses XOR-sponges with a big internal state as proposed in [4]. The randomized hashing is built in via a salt value. This scheme was proposed in the HAIFA framework [12]. In some sense we learn from the GRINDAHL design, but our approach is different in many ways. We take advantage of the well studied basic operations of AES and adopt some of them, including some optimization techniques.

Due to recent breakdowns of many proposed hash functions we analyze the resistance of TWISTER against all known generic attacks on hash functions. We find, that TWISTER resists all of them if the size of the internal chaining value is at least double the size of the hash output.

References

- [1] Eli Biham and Rafi Chen. Near-Collisions of SHA-0.
- [2] Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet, and William Jalby. Collisions of SHA-0 and Reduced SHA-1.
- [3] Lars R. Knudsen, Christian Rechberger, and Søren S. Thomsen. The Grindahl Hash Functions.
- [4] Stefan Lucks. A Failure-Friendly Design Principle for Hash Functions. In Bimal K. Roy, editor, *ASIACRYPT*, volume 3788 of *Lecture Notes in Computer Science*, pages 474–494. Springer, 2005.
- [5] Florent Chabaud and Antoine Joux. Differential Collisions in SHA-0. In Hugo Krawczyk, editor, *CRYPTO*, volume 1462 of *Lecture Notes in Computer Science*, pages 56–71. Springer, 1998.
- [6] Krystian Matusiewicz, Thomas Peyrin, Olivier Billet, Scott Contini, and Josef Pieprzyk. Cryptanalysis of FORK-256
- [7] Jean-Philippe Aumasson, Willi Meier, and Raphael C.-W. Phan. The Hash Function Family LAKE. In *FSE*, page inproceeding, 2008.
- [8] Norbert Pramstaller, Christian Rechberger, and Vincent Rijmen. Breaking a New Hash Function Design Strategy Called SMASH. In Bart Preneel and Stafford E. Tavares, editors, *Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 233–244. Springer, 2005.
- [9] Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche. Sponge Functions. Ecrypt Hash Workshop, 2007. See <http://gva.noekeon.org/papers/bdvp07.html>.
- [10] Michael Gorski, Stefan Lucks, and Thomas Peyrin. Slide Attacks on Hash Functions. Cryptology ePrint Archive, Report 2008/263, 2008. <http://eprint.iacr.org/>.
- [11] Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche. Sponge Functions. Ecrypt Hash Workshop, 2007. See <http://gva.noekeon.org/papers/bdvp07.html>.
- [12] Eli Biham and Orr Dunkelman. A Framework for Iterative Hash Functions - HAIFA. Cryptology ePrint Archive, Report 2007/278, 2007.

KronCrypt: Der Approximationssatz von Kronecker in der symmetrischen Kryptographie

Carsten Elsner* und Martin Schmidt†

Fachhochschule der Wirtschaft (FHDW)

Freundallee 15

30173 Hannover

*carsten.elsner@fhdw.de, †martin.schmidt@fhdw.de

Immer wieder hat die Neuentdeckung schon lange bekannter mathematischer Ideen für die Kryptographie zu immensen Fortschritten dieser Wissenschaft geführt. Beispielhaft können hier die gesamte public-key Kryptographie oder auch die Verwendung endlicher Körper als Basis für den heutigen Verschlüsselungsstandard AES genannt werden.

In einer Vorarbeit entdeckte Elsner, dass der Approximationssatz von Kronecker aus der zahlen-theoretischen Disziplin der diophantischen Approximation die Basis für ein symmetrisches Kryptosystem bildet. Der Kronecker'sche Satz besteht in der folgenden Aussage (vgl. [HW79, Kap. 23]):

Für jedes $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, jedes $\eta \in \mathbb{R}$, jedes $n > 0$ und jedes $\delta \in \mathbb{R}$ gibt es Zahlen p, q mit $q > n$ und

$$|q\alpha - p - \eta| < \left(\frac{1}{2} + \frac{1}{\sqrt{5}} + \delta \right) \cdot \frac{1}{q}.$$

Dabei wird der Klartext als Inhomogenität η aufgefasst und der Schlüssel geht in die zu approximierende Zahl α ein. Als Chiffretext wird der Nenner q der rationalen Approximation p/q der Zahl α verwendet. Der Verschlüsselungsschritt besteht also in dem Lösen einer inhomogenen diophantischen Ungleichung. Es lässt sich zeigen, dass ein mit Hilfe von Kettenbrüchen konstruierter Beweis neben einer Verschlüsselungsfunktion auch ein Verfahren zur Entschlüsselung liefert. Der Nutzen der Methoden und Sätze der diophantischen Approximation für die symmetrische Kryptographie war bis dato unentdeckt.

In der Diplomarbeit von Schmidt wurde diese Idee analysiert und das symmetrische Verschlüsselungsverfahren KronCrypt entwickelt, welches als zentrale Komponente eine auf dem konstruktiven Beweis des Approximationssatzes von Kronecker basierende schlüsselabhängige S-Box benutzt. Diese S-Box und das gesamte Kryptosystem wurden bzgl. ihrer Konfusions-, Diffusions- und Vollständigkeitseigenschaften analysiert. Des Weiteren wurden erste Ergebnisse bzgl. der Resistenz von KronCrypt gegen differentielle und lineare Kryptoanalysen ([BS90, Mat93]) erzielt.

Im Vortrag wird KronCrypt einschließlich der nötigen Grundlagen der diophantischen Approximation vorgestellt und es werden die genannten Analyseergebnisse skizziert.

Literatur

- [HW79] Hardy, G. H. ; Wright, E. M. *An Introduction to the Theory of Numbers*. Fünfte Auflage, Clarendon Press, 1979
- [BS90] Biham, E. ; Shamir, A. *Differential Cryptanalysis of DES-like Cryptosystems*. In: Menezes, A. J. (Hrsg.) ; Vanstone, S. A. (Hrsg.): *Advances in Cryptology - CRYPTO 90*, Springer-Verlag, 1991 (Lecture Notes in Computer Science 537), S. 2-21
- [Mat93] Matsui, M. *Linear Cryptanalysis Method for the DES Cipher*. In: Helleseht, T. (Hrsg.): *Advances in Cryptology - EUROCRYPT 93*, Springer-Verlag, 1994 (Lecture Notes in Computer Science 765), S. 386-397

Complete Codings for Visual Cryptography

Denise Doberitz

Institute for E-Business Security (ISEB)
Ruhr-Universität Bochum

In [DG07] we presented Visual Mutual Authentication, a Visual-Cryptography [NS94] based approach, which allows to establish a trusted channel between two parties and can be used for secure communication although the underlying system is untrusted. However, the approach contains the two main problems of Visual Cryptography, concerning the difficulty of a precise alignment of the key-transparency and the fact, that due to the one-time pad characteristic, a key-transparency can only be used once.

As a response to these problems, we introduce the concept of Complete Codings. In this context, we define a coding to be a homomorphic function, which transforms an information $i \in \mathcal{I}$ to a symbol $s \in \mathcal{S}$. If all symbols $s \in \mathcal{S}$ are related to an information $i \in \mathcal{I}$, the set of all symbols in \mathcal{S} can also be denoted as an alphabet \mathcal{A} . In the basic concept of Visual Cryptography, the message is coded as an image, composed of black and white pixels as smallest elements, which leads to the problem, that the transparencies have to be aligned with a precision of one pixel.

A Complete Coding maps the information to a set of symbols $\mathcal{S} = \{0, 1\}^n$, whereas a symbol $s = (s_1, \dots, s_n) \in \mathcal{S}$ is composed of n visual elements, whereas 1 denotes, that the element is visible and 0 denotes, that the element is not visible. With the help of a visualization mapping function \mathcal{D} , all possible combinations of the elements of a Complete Coding are mapped to an information and thus can be used as valid symbols resulting in the complete set \mathcal{S} being an alphabet \mathcal{A} .

Applied to Visual Cryptography, it can be shown, that a modified version of a Visual Cryptography System using a Complete Coding allows the multiple use of the key-transparencies, when the plaintexts are selected randomly and are not predictable by an adversary. Due to the fact, that the elements of a Complete Coding are not restricted to the size of one pixel, but can be larger, a simplified aligning of the transparencies can be provided.

In the talk we show an example for a Complete Coding, a so-called Dice-Coding. Additionally, a corresponding Visual Cryptography System is presented which can be applied to a protocol for the transmission of TANs in internet banking.

References

- [DG07] Denise Doberitz and Sebastian Gajek. Visual Cryptography - an approach to secure online banking. 7. *Kryptotag*, November 2007.
- [NS94] Adi Shamir and Moni Naor. Visual cryptography. In *EUROCRYPT*, pages 1-12, 1994.

Extended Access Control – neuer Zugriffsmechanismus für elektronische Ausweisdokumente

Christian J. Dietrich, Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
FH Gelsenkirchen

Seit den Terroranschlägen des 11. Septembers 2001 ist die Sicherheit von Ausweisdokumenten auf internationaler Ebene breit diskutiert worden. Diese Diskussion führte in Deutschland letztlich zur Einführung des elektronischen Reisepasses mit biometrischen Merkmalen. Seit November 2007 ist der elektronische Reisepass vollständig eingeführt und bietet aufgrund des biometrischen Merkmals in Form eines Fingerabdrucks ein erhöhtes Maß an Sicherheit in Bezug auf die Identifikation des Dokumenteninhabers. Im Rahmen der Modernisierung der Bundesverwaltung soll nun nach Vorstellung der Bundesregierung vermutlich ab 2010 der elektronische Personalausweis (ePA) eingeführt werden. Im Gegensatz zum elektronischen Reisepass gibt es derzeit jedoch auf internationaler oder europäischer Ebene noch keine gesetzlichen Rahmenbedingungen.

Das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) spezifizierte Verfahren EAC sichert die Authentizität und Integrität der Daten sowohl in gespeicherter Form als auch während der Übertragung. Es besteht aus den 3 Protokollen Password Authenticated Connection Establishment (PACE), Terminal Authentication und Chip Authentication. Kernbestandteile von Extended Access Control sind symmetrische und asymmetrische Kryptographie, eine globale Public Key Infrastruktur sowie die Verwendung von abstreitbaren Challenge-Response-Verfahren. Dieser Beitrag wird den Ablauf sowie die 3 Verfahren PACE, Terminal Authentication und Chip Authentication im Detail darstellen.

PACE ist ein Verfahren zur Freischaltung des Chips durch ein Lesegerät. Mit Hilfe einer PIN, die als Passwort fungiert, wird einem Lesegerät der Zugriff auf den Funkkanal zu einem Chip, z.B. dem ePA, gestattet. Aus kryptographischer Perspektive handelt es sich dabei um eine verschlüsselte Diffie-Hellman-Schlüsseleinigung. Im Rahmen der sog. **Terminal Authentication** prüft der Chip mit Hilfe eines Challenge-Response-Verfahrens die Zugriffsberechtigungen des Lesegeräts (Terminal). Die **Chip Authentication** ist ein Verfahren, das genutzt wird, um die Authentizität des Chips zu prüfen. Hierbei werden implizit die Daten, die ein Chip liefert authentisiert. Aus kryptographischer Sicht handelt es sich um eine Diffie-Hellman-Schlüsseleinigung mit statischem Chip-Schlüssel. Nach Abschluss der Chip Authentication ist ein verschlüsselter Ende-zu-Ende-Kanal etabliert.

Literatur

[BSI-TR-03110] BSI. Advanced Security Mechanisms for Machine Travel Documents - Extended Access Control (EAC), 2007

[BSI-TR-03116] BSI. Technische Richtlinien für die eCard-Projekte der Bundesregierung, 2007

Reale Nutzung kryptografischer Verfahren innerhalb von TLS/SSL

Dominique Petersen

Institut für Internet-Sicherheit - if(is)

FH Gelsenkirchen

Das Internet ist heutzutage zu einer allgegenwärtigen Selbstverständlichkeit geworden und nicht mehr aus unserem Leben wegzudenken. Wir kaufen die unterschiedlichsten Artikel zielsicher bei diversen Online-Shops, wickeln unsere Bankgeschäfte im Online-Banking ab, verwalten unsere elektronische Post und jonglieren mit Aktien und Wertpapieren auf verschiedenen Finanzportalen - sprich: Das Internet ist Teil unseres privaten und beruflichen Lebens geworden, und wir füttern es bereitwillig mit unseren persönlichen Daten wie Adressen, Passwörtern, Kontonummern und PINs.

Im gleichen Schritt wird es hierbei immer leichter, diese sensiblen Daten abzugreifen und zu missbrauchen. Längst interessieren sich nicht nur einzelne Hacker für diese Informationen, sondern vielmehr kriminelle Vereinigungen, die hier das groe Geld wittern. Wie die jüngst bekannt gewordenen Vorfälle illegalen Datenhandels mit Millionen Bankkontodaten erneut zeigen, ist dies ein blühendes und lukratives Geschäft. Firewall-Programme und Virens Scanner auf lokalen Rechnern bieten hierbei nicht den geringsten Schutz. Aus diesen Gründen ist es notwendiger denn je, auf eine verschlüsselte Kommunikation bei der Übertragung sensibler Daten zu achten.

Die verwendeten Verschlüsselungsverfahren unterscheiden sich jedoch stark in ihrer kryptographischen Leistungsfähigkeit. Zwar können alle Kryptosysteme mit genügend Rechenkraft geknackt werden, allerdings basiert der notwendige Aufwand für den Angreifer auf zwei beeinflussbaren Variablen. Zum einen ist das die verwendete Schlüssellänge, denn der theoretische Aufwand für das Ausprobieren aller möglichen Kombinationen berechnet sich aus dem Grad der Zweierpotenz. Zum anderen ist es das verwendete Verschlüsselungsverfahren, welches Schwachstellen im Algorithmus selbst aufweisen kann, so dass der theoretische Aufwand extrem verringert wird und schnell eine reale Bedrohung entsteht. Welche Kombination aus asymmetrischer und symmetrischer Verschlüsselung letztendlich gewählt wird, entscheiden die Clients (z.B. Web-Browser) und Server untereinander. Dazu schickt der Browser eine Liste seiner ihm zur Verfügung stehenden Verfahren an den Server, der wiederum aus diesem Angebot einen Algorithmus selektiert. Es wird bereits deutlich, dass beide Parteien sichere Algorithmen anbieten müssen.

Der Vortrag wird zeigen, wie die Verteilung aktueller Verschlüsselungsalgorithmen beim Surfen und Mailen mittels TLS/SSL-abgesicherten Verbindungen aussieht. Durch die Statistiken wird deutlich, ob derzeit wirklich sichere oder doch noch unsichere Verfahren verwendet werden.

Teilnehmer

Name

D. Hannemann
Johannes Lengler
Heiko Stamer
Sebastian Pape
Sabarnij Sergej
Christopher Wolf
Deike Priemuth-Schmid
Dirk Stegemann
Marco Smiatek
Sascha Bastke
Tibor Jager
Heiner Utz
Markus Linnemann
Christian Dietrich
Sibylle Hick
Denise Doberitz
Martin Schmidt
Christian Forler
Dominique Petersen
Andreas Speier
Oliver Achten
Michael Gröne
Malte Woelky

Einrichtung

Fachhochschule Gelsenkirchen
Universität des Saarlandes
Universität Kassel
Universität Kassel
Ruhr-Universität Bochum
Ruhr-Universität Bochum
University of Luxembourg
University of Mannheim
FH Gelsenkirchen, Institut für Internet-Sicherheit
FH Gelsenkirchen, Institut für Internet-Sicherheit
Ruhr-Universität Bochum
Universität Karlsruhe
FH Gelsenkirchen, Institut für Internet-Sicherheit
FH Gelsenkirchen, Institut für Internet-Sicherheit
secunet Security Networks AG
Ruhr-Universität Bochum
Leibniz Universität Hannover
Sirrix AG
FH Gelsenkirchen, Institut für Internet-Sicherheit
FH Gelsenkirchen, Institut für Internet-Sicherheit
FH Gelsenkirchen, Institut für Internet-Sicherheit
FH Gelsenkirchen, Institut für Internet-Sicherheit
FH Gelsenkirchen, Institut für Internet-Sicherheit

<http://KryptoTag.de>

Der Kryptotag ist eine zentrale Aktivität der GI-Fachgruppe „Angewandte Kryptologie“. Er ist eine wissenschaftliche Veranstaltung im Bereich der Kryptologie und von der organisatorischen Arbeit der Fachgruppe getrennt. Grundgedanke des Kryptotages ist, dass er inklusive Anreise wirklich nur einen Tag dauert und Nachwuchswissenschaftlern, etablierten Forschern und Praktikern auf dem Gebiet der Kryptologie die Möglichkeit bieten, Kontakte über die eigene Universität hinaus zu knüpfen.

Die Vorträge können ein breites Spektrum abdecken, von noch laufenden Projekten, die ggf. erstmals einem breiteren Publikum vorgestellt werden werden, bis zu abgeschlossenen Forschungsarbeiten, die zeitnah auch auf Konferenzen präsentiert wurden bzw. werden sollen oder einen Schwerpunkt der eigenen Diplomarbeit oder Dissertation bilden. Die eingereichten Abstracts werden gesammelt und als technischer Bericht veröffentlicht. Es handelt sich damit um eine zitierfähige Arbeit. Sie können von den Seiten der Fachgruppe herunter geladen werden.

Geplante Kryptotage

10. Kryptotag 20. März 2009, TU Berlin

Bisherige Kryptotage

9. Kryptotag am 10. November 2008 Institut für Internet-Sicherheit, Fachhochschule Gelsenkirchen. Kontakt: MMarkus Linnemann. 5 Einreichungen und 24 angemeldete Teilnehmer.

8. Kryptotag am 11. April 2008 Universität Tübingen, WSI für Informatik, Diskrete Mathematik. Kontakt: Michael Beiter, Claudia Schmidt, Anja Korsten. 7 Einreichungen und 36 angemeldete Teilnehmer.

7. Kryptotag am 9. November 2007 Bonn-Aachen International Center for Information Technology. Kontakt: Michael Nüsken und Daniel Loebenberger. 9 Einreichungen und 36 angemeldete Teilnehmer.

6. Kryptotag am 19. Februar 2007. Universität des Saarlandes, Information Security and Cryptography Group und Sirrix AG. Kontakt: Michael Backes und Ammar Alkassar. 8 Einreichungen und 30 angemeldete Teilnehmer.

5. Kryptotag am 11. September 2006. Universität Kassel, Fachbereich Mathematik/Informatik, Theoretische Informatik. Kontakt: Heiko Stamer. 8 Einreichungen und 22 angemeldete Teilnehmer.

1. Kryptowochenende am 1.–2. Juli 2006. Tagungszentrum Kloster Bronnbach der Universität Mannheim. Kontakt: Frederik Armknecht und Dirk Stegemann. 14 Einreichungen und 21 angemeldete Teilnehmer.

4. Kryptotag am 11. Mai 2006. Ruhr Universität Bochum, Horst-Görtz Institut. Kontakt: Ulrich Greveler. 10 Einreichungen und 32 angemeldete Teilnehmer.

3. Kryptotag am 15. September 2005. Technische Universität Darmstadt, Theoretische Informatik. Kontakt: Ralf-Philipp Weinmann. 13 Einreichungen und 35 angemeldeten Teilnehmer.

2. Kryptotag am 31. März 2005. Universität Ulm, Abteilung für Theoretische Informatik. Kontakt: Wolfgang Lindner und Christopher Wolf. 10 Einreichungen und 26 angemeldeten Teilnehmer.

1. Kryptotag am 1. Dezember 2004. Universität Mannheim, Theoretische Informatik. Kontakt: Stefan Lucks und Christopher Wolf. 15 Einreichungen und 37 angemeldeten Teilnehmer.

Innerhalb der Fachgruppe für Angewandte Kryptologie sind Stefan Lucks (Universität Mannheim) und Christopher Wolf (K.U.Leuven, Belgien) verantwortlich für die Organisation der Kryptotage. Für eventuelle Rückfragen bitte an sie wenden.