Tagungsband zum 7. Kryptotag

Workshop der Fachgruppe Kryptographie in der Gesellschaft für Informatik

Bonn-Aachen International Center for Information Technology

© 2007 Daniel Loebenberger, Michael Nüsken

Version: 8. November 2007

Programm

09^{30} Kaffee und Gebäck.

09^{50} Begrüßung (Joachim von zur Gathen, Daniel Loebenberger, Michael Nüsken).

10^{00} - 11^{00} Session I: Kryptographische Primitive.

- **10^{00}** Jens Zumbrägel (Universität Zürich). *Einfache Halbringe und ihre kryptographischen Anwendungen.* 4
- **10^{20}** Anna Perschl (FH Hagenberg). *Attacken auf RSA durch Lösen von univariaten modularen Polynomgleichungen.* 5
- **10^{40}** Jeremie Detrey (b-it). *Arithmetic operators for pairing-based cryptography.* 6

11^{00} - 11^{20} Kaffeepause.

11^{20} - 12^{20} Session II: Datenschutz.

- **11^{20}** Heiko Stamer (Universität Kassel). *Kryptographische Missbrauchssicherung für die Voratsdatenspeicherung.* 7
- **11^{40}** Martin Keßler, Sefan Lucks, Emin Islam Tatli (Bauhaus-Universität Weimar). *Tracking Dog: A Privacy Tool against Google Hacking.* 8
- **12^{00}** Denise Doberitz, Sebastian Gajek (Ruhr-Universität Bochum). *Visual Mutual Authentication - an approach to secure online banking.* 9

12^{20} - 13^{40} Mittagessen in der Kantine der Deutschen Welle.

13^{40} - 13^{50} Rump Session (Ankündigung anderer Tagungen etc).

13^{50} - 14^{40} Gastvortrag:

Werner Schindler (BSI):
Für jedes Problem das richtige Werkzeug: Stochastische Methoden für Seitenkanalangriffe. 3

14^{40} - 15^{00} Kaffeepause.

15^{00} - 16^{00} Session III: Kryptanalyse von Stromchiffren.

- **15^{00}** Andrea Röck (INRIA). *Entropieberechnung des inneren Zustandes eines FCSR's.* 10
- **15^{20}** Tobias Eibach, Enrico Pilz (Universität Ulm). *Ein Angriff auf Bivium mittels SAT Solver.* 11
- **15^{40}** Deike Priemuth-Schmid, Alex Biryukov (University of Luxembourg). *Auf der Suche nach schwachen Schlüsseln bei Trivium.* 12

16^{00} - 16^{05} Verabschiedung.

16^{30} - 18^{00} Fachgruppensitzung.

ab 18^{00} Ausklang des Kryptotages.

Teilnehmer

Martin Goldack	M.Goldack@tuvit.de
Mathias Herrmann	
Tina Lößle	tina.loessle@web.de
Deike Priemuth-Schmid . .	
Daniel Reinert	Daniel.Reinert@ruhr-uni-bochum.de
Patrick Renz	Patrickrenz@web.de
Maike Ritzenhofen	maike.ritzenhofen@ruhr-uni-bochum.de
Christopher Wolf	Chris@christopher-wolf.de

Für jedes Problem das richtige Werkzeug: Stochastik bei Seitenkanalangriffen

Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn

Die Evaluierung kryptographischer Algorithmen und Protokolle erfordert den Einsatz zum Teil tiefliegender Techniken aus unterschiedlichen mathematischen Gebieten. Besondere Bedeutung besitzen u.a. die Zahlentheorie wie auch algebraische und komplexitätstheoretische Ansätze. Stochastik und Statistik spielen dagegen eine eher untergeordnete Rolle.

Starke kryptographische Algorithmen und Protokolle sind jedoch nur eine notwendige, aber keineswegs eine hinreichende Voraussetzung für sichere IT-Systeme. Ebenso wichtig ist ihre sichere Implementierung und dabei insbesondere das Zusammenspiel mit den kryptographischen Mechanismen und ihrer algorithmischen Umsetzung. Die Chipkartenindustrie und universitären Forschungsgruppen verfolgen daher vor allem Seitenkanalangriffe mit großer Aufmerksamkeit und entwickeln sie weiter. Seitenkanalangriffe richten sich meist gegen Chipkarten, aber in den letzten Jahren sind auch Softwareimplementierungen verstärkt in den Fokus geraten.

Vereinfacht gesagt, versuchen Seitenkanalangriffe, aus physikalischen Messwerte (z.B. Laufzeiten, Stromaufnahme oder elektromagnetische Abstrahlung) teilschlüsselabhängige Informationen zu extrahieren, um den gesuchten Schlüssel in kleinen Portionen (z.B. bit- oder byteweise) zu bestimmen. Diese teilschlüsselabhängigen Nutzinformationen werden jedoch in aller Regel durch weitere arithmetische Operationen und / oder gezielte algorithmische oder Hardware-Gegenmaßnahmen überdeckt und damit verschleiert. Ein gemeinsames Ziel von Angreifern und Designern von Kryptosystemen besteht darin, einen Angriff bzw. einen Klasse von Angriffen zu optimieren, wenngleich aus völlig unterschiedlichen Gründen. Während ein Angreifer schlicht seine Erfolgsaussichten optimieren möchte, ermöglicht dies dem Designer, das wahre Risikopotential auszuloten und zuverlässige und vertrauenswürdige Gegenmaßnahmen zu entwickeln.

Fortgeschrittene stochastische und statistische Ansätze haben sich bei vielen unterschiedlichen Problemstellungen als die geeigneten Werkzeuge erwiesen, dieses Ziel zu erreichen. Gerade bei hardwarenahen Kryptographietagungen besitzen konkrete experimentelle Resultate, etwa das Brechen einer Testimplementierung samt einer ad-hoc Gegenmaßnahme, häufig einen höheren Stellenwert als die verwendeten mathematischen Methoden und eine tiefer gehende Analyse der Situation, um die eigentliche Ursache für den Angriff herauszuarbeiten und in einem zweiten Schritt zuverlässige Gegenmaßnahmen auch für modifizierte Angriffsvarianten zu entwickeln. Zudem erreichen Erkenntisse von hardwareorientierten Fachtagungen Softwareentwickler oft nur mit großer zeitlicher Verzögerung, obwohl ähnliche stochastische Ansätze teilweise auch Seitenkanalangriffe gegen Softwareimplementierungen ermöglichen (auch wenn die Angriffe im Detail sehr verschieden sein können). Diese beiden Effekte haben in der Vergangenheit verschiedentlich (z.B. bei OpenSSL) dazu geführt, dass Schutzmaßnahmen schrittweise nachgebessert werden mussten, nämlich als Antwort auf neue Angriffe.

Im Vortrag werden verschiedene Angriffe gegen Chipkarten und Softwareimplementierungen besprochen. Gemeinsamkeiten und Unterschiede werden herausgearbeitet, die angewandten stochastischen Methoden dargestellt und Implikationen aufgezeigt.

Einfache Halbringe und ihre kryptographische Anwendung

Jens Zumbrägel · jzumbr@math.uzh.ch

Institut für Mathematik, Universität Zürich
Winterthurerstr. 190, CH - 8057 Zürich

Halbringe sind verallgemeinerte Ringe, in denen negative Elemente nicht zu existieren brauchen. Formal ist ein *Halbring* eine Struktur $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+$, $\cdot$, so dass $(R, +)$ eine kommutative Halbgruppe ist, $(R, \cdot)$ eine Halbgruppe, und dass beide Distributivgesetze gelten. Wir nehmen weiterhin die Existenz eines Elements $0 \in R$ an, welches sich neutral in $(R, +)$ und absorbierend in $(R, \cdot)$ verhält.

Halbringe sind beispielsweise die natürlichen Zahlen $(\mathbb{N} = \{0, 1, 2, 3, \dots\}, +, \cdot)$, der boolesche Halbring $(\{0, 1\}, \texttt{or}, \texttt{and})$, und der Endomorphismenhalbring $(\mathrm{End}(M), +, \circ)$ eines kommutativen Monoids $(M, +, 0)$. Die Halbringstruktur ist im Wesentlichen die schwächste, für die noch eine sinnvolle Matrixmultiplikation definiert werden kann.

Endliche Halbringe und Matrizen über diesen können in der Public-Key Kryptographie angewendet werden, um Operationen von kommutativen Halbgruppen auf Mengen zu konstruieren, die effizient berechenbar sind, jedoch im Allgemeinen schwierig zu invertierende Bahnenabbildungen besitzen. Solche Operationen bieten einen natürlichen Rahmen, um DL-basierte Kryptosysteme zu verallgemeinern, bei denen die Halbgruppe $(\mathbb{Z}, \cdot)$ durch Exponentiation auf einer zyklischen Gruppe operiert, siehe [MMR05].

Wenn man nun Operationen unter Verwendung von Halbringen konstruiert, welche sich homomorph auf kleinere Halbringe abbilden lassen, dann ist das Kryptosystem anfällig für Angriffe, die vom verkleinerten homomorphen Bild ausgehen. Diese Angriffe sind vergleichbar mit dem Pohlig-Hellman-Algorithmus zur Berechnung diskreter Logarithmen in zyklischen Gruppen von Nichtprimzahl-Ordnung. Daher ist es für kryptographische Zwecke wichtig, dass der Halbring *einfach* d. h. kongruenz-frei ist, da in diesem Fall kein kleineres homomorphes Bild existiert.

Die vollständige Klassifikation von endlichen einfachen Halbringen in [Zu07] (siehe auch [Mo04]) liefert zahlreiche Beispiele, nämlich gewisse Teilhalbringe von Endomorphismenhalbringen endlicher kommutativer idempotenter Monoide, welche bijektiv den endlichen Verbänden entsprechen. Es ist dadurch mit wenig Computer-Ressourcen möglich, auch sehr große Halbringe und deren Verknüpfungen zu erzeugen. Diese Vielfalt von einfachen Endomorphismenhalbringen bieten zahlreiche Möglichkeiten, Halbgruppenoperationen zu konstruieren, die unter anderem aufgrund der Effizienz für Public-Key Kryptographie potenziell interessant sind. Die Konstruktion von kryptographisch geeigneten Operationen ist Gegenstand meiner aktuellen Forschung.

Literatur

[Mo04] Chris Monico. On finite congruence-simple semirings. *J. Algebra* 271 (2004), no. 2, 846–854 arXiv:math.RA/0205083, Mai 2002.

[MMR05] Gérard Maze, Chris Monico, Joachim Rosenthal. Public Key Cryptography based on Semigroup Actions. arXiv:cs.CR/0501017v2, Januar 2005, erscheint in *Adv. Math. Commun.*.

[Zu07] Jens Zumbrägel. Classification of finite congruence-simple semirings with zero. arXiv:math.RA/0702416, Feburar 2007.

Attacken auf RSA durch Lösen von univariaten modularen Polynomgleichungen

Anna Perschl

FH Oberösterreich - Campus Hagenberg
Softwarepark 11, 4232 Hagenberg, Österreich

Don Coppersmith stellte in [1] eine Methode vor, die eine univariate Polynomgleichung mit Modul N und Grad δ in polynomialer Zeit löst, wenn die gesuchte Lösung kleiner als $N^{1/\delta}$ ist. Auf diesen Ergebnissen aufbauend, präsentierte Nicholas Howgrave-Graham in [2] eine weitere Methode.

Mit Hilfe dieser Methoden kann RSA kompromittiert werden, z.B. wenn ein Teil der Nachricht bekannt ist, die Nachricht zwei Mal mit gleichem Schlüssel und unterschiedlichem Padding oder die Nachricht mehrmals mit unterschiedlichen Schlüsseln und bekannten Paddings verschlüsselt wird. In diesen Fällen sind Angriffe dann möglich, wenn ein kleiner öffentlicher Exponent e verwendet wird und die Unbekannte kleiner als $N^{1/e}$ ist. Die Methoden ermöglichen auch das Faktorisieren von N, wenn genügend höchstwertige Bits eines Teilers bekannt sind. Eine aktuelle Übersicht der Anwendungen findet sich in [3], ein aktueller Faktorisierungsalgorithmus in [4].

Die beiden Methoden lösen univariate modulare Polynomgleichungen in Zeit polynomiell in $\log N$ und δ. Da dies jedoch keine konkrete Aussage über die tatsächlichen Laufzeiten zulässt, haben wir beide Methoden im Rahmen der Diplomarbeit in Java implementiert und auf ihren Einsatz in drei Attacken getestet.

Eine Gleichung dritten Grades mit einer Lösung von höchstens 256 Bit und einem Modul von 1024 Bit löst die implementierte Coppersmith-Methode in 55 Sekunden, die implementierte Howgrave-Graham-Methode in 22 Sekunden. Bei einem Modul von 2048 Bit benötigen die Methoden 340 bzw. 150 Sekunden. Wird also eine Nachricht mit öffentlichem Exponent 3 und einem 1024-Bit-Modul verschlüsselt, so kann ein Angreifer, der 3/4 der Nachricht kennt, das unbekannte Viertel der Nachricht in 22 Sekunden ermitteln. Dem Angreifer kann theoretisch bis zu 1/3 der Nachricht unbekannt sein, allerdings ist dann der benötigte Zeitaufwand deutlich größer.

Wir präsentieren die Testergebnisse der Methoden im Detail, zeigen theoretische und praktische Grenzen auf und treffen eine Aussage über ihre Relevanz im Bezug auf die Sicherheit von RSA.

Literatur

[1] Don Coppersmith: Finding a Small Root of a Univariate Modular Equation. In *Advances in Cryptology – EUROCRYPT '96*, Bd. 1070 d. Reihe *Lecture Notes in Computer Science*, S. 155–165, Springer-Verlag, 1996.

[2] Nicholas Howgrave-Graham: Finding Small Roots of Univariate Modular Equations Revisited. In *Crytography and Coding – IMA 1997*, Bd. 1355 d. Reihe *Lecture Notes in Computer Science*, S. 131–142, Springer-Verlag, 1997.

[3] Alexander May: Using LLL-Reduction for Solving RSA and Factorization Problems: A Survey. *LLL+25 Conference in honour of the 25th birthday of the LLL algorithm*, 2007.

[4] Mathias Herrmann, Alexander May: On Factoring Arbitrary Integers with Known Bits. In *INFORMATIK 2007 - Informatik trifft Logistik, Band 2*, Bd. P-110 d. Reihe *Lecture Notes in Informatics*, S. 195–199, 2007.

Arithmetic operators for pairing-based cryptography

Jérémie Detrey*

*Computer Security group, B-IT, Bonn, Germany

Since their introduction in constructive cryptographic applications, pairings over (hyper)elliptic curves are at the heart of an ever increasing number of protocols. Software implementations being rather slow, the study of hardware architectures became an active research area. In this talk, I will first describe an accelerator for the η_T pairing over $\mathbb{F}_3[x]/(x^{97} + x^{12} + 2)$. Our architecture is based on a unified arithmetic operator which performs addition, multiplication, and cubing over $\mathbb{F}_{3^{97}}$. This design methodology allows us to design a compact coprocessor (1888 slices on a Virtex-II Pro 4 FPGA) which compares favorably with other solutions described in the open literature.

References

[1] Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, and Eiji Okamoto. Arithmetic operators for pairing-based cryptography. In P. Paillier and I. Verbauwhede, editors, *9th International Workshop on Cryptographic Hardware and Embedded Systems (CHES'07)*, pages 239–255, Vienna, Austria, September 2007. Springer-Verlag.

Kryptographische Missbrauchssicherungen für die Vorratsdatenspeicherung

Heiko Stamer

Universität Kassel, Fachbereich Elektrotechnik/Informatik
Wilhelmshöher Allee 71-73, D-34109 Kassel
stamer@theory.informatik.uni-kassel.de

Auf Grundlage der EU-Richtlinie 2006/24/EG hat die Bundesregierung im April 2007 einen umstrittenen Gesetzentwurf [BT07a] vorgelegt, welcher alle Telekommunikations- und Internetanbieter verpflichtet, die Kommunikationsverbindungsdaten ihrer Kunden für mindestens 6 Monate auf Vorrat zu speichern. Bei der Sachverständigenanhörung im Rechtsausschuss des Deutschen Bundestages [BT07b] ist kürzlich sehr deutlich geworden, dass nicht nur verfassungs- und datenschutzrechtlich *große Bedenken* bestehen, sondern das auch viele technische Fragen noch ungeklärt sind.

Zwar gab es auf europäischer Ebene bereits verschiedene Expertentreffen [AKV1] und das Europäische Institut für Telekommunikationsnormen (ETSI) hat mittlerweile ebenfalls in Form von Standardisierungsbestrebungen [ETSI1, AKV2, ETSI2] reagiert, jedoch sind bisher kaum *datenschutzfreundliche Lösungen* für die Speicherung der sensiblen Verbindungsdaten öffentlich bekannt geworden. Das ist im Zusammenhang mit der Brisanz von Telekommunikationsverbindungsdaten mehr als erstaunlich, da diese Daten ein *enormes Missbrauchspotential* in sich bergen.

Im Vortrag werden verschiedene Speicher- und Zugriffsszenarien sowie entsprechende Implementierungsansätze diskutiert, die mit Hilfe von Kryptographie (Verschlüsselung, PIR u. ä.) eine „datenschutzfreundlichere Vorratsdatenspeicherung“ ermöglichen könnten. Diese *konstruktive* Herangehensweise soll jedoch nicht darüber hinweg täuschen, dass ich persönlich *jegliche* Vorratsspeicherung prinzipiell für unverhältnismäßig, ineffizient und datenschutzrechtlich gefährlich halte.

Literatur

[BT07a] Gesetzentwurf der Bundesregierung. *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG.* BT-Drucksache 16/5846. Online verfügbar unter http://www.bundestag.de/ausschuesse/a06/anhoerungen/24_tkue_vorratsdatenspeicherung/01_Bundestagsdrucksachen/1605846.pdf

[BT07b] Zusammenfassung der Stellungnahmen der Sachverständigen im Rechtsausschuss. *Telefonüberwachung und Datenspeicherung umstritten.* Online verfügbar unter http://www.bundestag.de/aktuell/archiv/2007/telekom_kw38/index.html

[AKV1] Arbeitskreis Vorratsdatenspeicherung. *Protokoll des Expertentreffens zu Implementierungsfragen der Vorratsdatenspeicherung vom 16. Mai 2007.* Online verfügbar unter: http://wiki.vorratsdatenspeicherung.de/Protokoll_des_Expertentreffens_zu_Implementierungsfragen_der_Vorratsdatenspeicherung_vom_16._Mai_2007

[AKV2] Arbeitskreis Vorratsdatenspeicherung. *ETSI-Dokumente.* Online verfügbar unter: http://wiki.vorratsdatenspeicherung.de/ETSI-Dokumente

[ETSI1] European Telecommunications Standards Institute. *Retained data requirements law enforcement.*

[ETSI2] European Telecommunications Standards Institute. *Security framework in Lawful Interception and Retained Data environment.* Ref. DTR/LI-00044, Start of work on 2007-04-25.

Tracking Dog - A Privacy Tool against Google Hacking

Martin Keßler, Stefan Lucks and Emin Islam Tatlı

Bauhaus Universität Weimar, Medien Fakultät
Bauhausstraße 11, 99423 Weimar
{martin.kessler, stefan.lucks, emin-islam.tatli}@medien.uni-weimar.de

Protection of personal data is a privacy right from both ethical and legislation perspectives. Internet users require safeguarding their privacy against misuses and exploits. On the other hand, internet search engines and especially the most popular Google threaten user privacy. Google Hacking is a general term describing how Google can be used to find out vulnerable servers, files and web applications, unauthenticated programs, various online devices, etc.[Ghdb]. As threats to privacy, Google indexes and reveals sensitive and confidential user data that include names, addresses, CVs, files containing usernames-passwords, confidential emails and forum postings, private directories, chat log files, secret and private keys, etc. to unauthorized persons [Tatli06, Tatli07]. As a countermeasure, the users should be equipped with privacy enhancing tools to protect their privacy.

In this talk, we present *Tracking Dog* [Kessler07], a penetration testing tool for searching cryptographic secrets and personal private data for a given host and/or given person name. The tool helps the individuals to detect if any of their confidential data have become public over the internet via Google. *Tracking Dog* supports both English and German language-specific queries and enables the users to edit raw search queries.

References

[Tatli06] Emin Islam Tatlı. Google Reveals Cryptographic Secrets. 1. Kryptowochenende, Kloster Bronbach, July 2006.

[Tatli07] Emin Islam Tatlı. Google Hacking Against Privacy. 3. International IFIP Privacy Summer School, Karlstad-Sweden, August 2007.

[Kessler07] Martin Keßler. Bachelorarbeit: Tracking Dog - Implementation of a penetration testing tool for searching cryptographic secrets and personal secrets with Google. Bauhaus Universität Weimar, Fakultät Medien, Oktober 2007.

[Ghdb] Google Hacking Database. http://johnny.ihackstuff.com/ghdb.php.

Visual Mutual Authentication - an approach to secure online banking

Denise Doberitz and Sebastian Gajek

Horst Görtz Institut für IT-Sicherheit
Ruhr-Universität Bochum

Today, most applications are only as secure as their underlying system. Since the design and technology of malware has improved steadily, their dectection is a difficult problem. As a result it is nearly impossible to be sure whether a computer, that is connected to the internet, can be considered trustworthy and secure or not. The question is, how to handle applications, that require a high level of security, such as online banking. In consequence we are interested in a solution, that allows us to establish a secure and trusted communication, although the underlying system is untrusted.

In this paper we present an approach, that is based on Visual Cryptography. In [NaorS94] Shamir and Naor presented the concept of Visual Cryptography, that handles the plaintext to be encrypted as a graphic, that is processed pixel by pixel and thus implies interesting characteristics concerning security and fault tolerance. In [NaorP97] Naor and Pinkas demonstrated how to use Visual Cryptography for the authentication of one party without trusting the underlying system. Based on this, we develope a scheme for mutual visual authentication of a user and a server, that allows us to establish a trusted channel between the two parties, and can be used for secure communication.

We describe the Visual Mutual Authentication - Scheme and demonstrate its application as a protocol on the example of online-banking. The protocol provides a practical and user-friendly approach to secure online banking, that is not only resilient to malware, but also resistant to phishing.
Using Visual Cryptography, the user's key is a transparency that has to be applied on the computer monitor. With the tansparency, the decrypted message can simply be read from the monitor by the user. We transfer this application to a TAN-scheme and integrate a one-time pad structure. As a result, we achieve a user friendly scheme with a high level of secrecy.

References

[NaorS94] Moni Naor and Adi Shamir. Visual Cryptography, EUROCRYPT '94, *Volume 950 of Lecture Notes in Computer Science*, pp. 112. Springer-Verlag, 1995.

[NaorP97] Moni Naor and Benny Pinkas. Visual Authentication and Identification. CRYPTO '97, *Volume 1294 of Lecture Notesin Computer Science*, pp. 322-336. Springer-Verlag, 1997.

Entropieberechnung des inneren Zustandes eines FCSR's

Andrea Röck

Projet CODES, INRIA Paris-Rocquencourt, France

Lineare rückgekoppelte Schieberegister (LFSR) sind weitverbreitete Primitive in der Kryptographie. Um deren Linearität zu vermeiden, kann auf die nichtlineare Variante des rückgekoppelten Schieberegisters mit Übertrag (engl. Feedback with Carry Shift Register, kurz FCSR) ausgewichen werden, wie z.B. im Fall des eSTREAM Kandidaten F-FCSR [AB05] für eine Stromchiffre.

Ein FCSR ist ein endlicher Automat, welcher unabhängig von Klapper und Goresky [KG97], Marsaglia und Zamand [MZ91] und Couture und L'Ecuyer [CL94] eingeführt wurde. Er ist ähnlich aufgebaut wie ein LFSR, jedoch wird für die Rückkopplung nicht ein XOR, sondern eine Addition mit Übertrag angewandt. Daher benötigen wir an jeder Rückkopplungsposition einen zusätzlichen Speicherplatz für den Übertrag. Im Folgenden betrachten wir binäre FCSR's.

Wir interessieren uns für die Entropie des inneren Zustandes des FCSR's. Eine verringerte Entropie erleichtert es einem Angreifer, den Wert des Zustandes und somit die nachfolgende Ausgangssequenz des FCSR's zu erraten. Nehmen wir an, der innere Zustand des FCSR's bestehe aus einem Hauptregister der Länge n und ℓ Übertragsbits an den Rückkopplungspositionen. Unter der Vorraussetzung, dass der Anfangszustand jeden der $2^{n+\ell}$ möglichen Werte mit der gleichen Wahrscheinlichkeit annimmt, hat dieser FCSR eine Anfangsentropie von $n+\ell$ Bits. Da die Iteration des FCSR's keine bijektive Funktion ist, wird die Entropie mit jeder Iteration solange verringert, bis der FCSR einen periodischen Kreislauf erreicht. Ab diesem Zeitpunkt verhält sich eine Iteration wie die Anwendung einer Permutation, und die Entropie bleibt konstant.

Im Allgemeinen sinkt die Entropie des inneren Zustandes relativ schnell. Arnault, Berger und Minier zeigen in [ABM07], dass ein FCSR mit maximaler Periode seinen periodischen Kreislauf und somit seine endgültige Entropie nach maximal $n+3$ Iterationen erreicht. Indem wir betrachten, von wie vielen Zuständen ein bestimmter Zustand erzeugt werden kann, können wir zeigen, dass schon nach einer Iteration die Entropie auf $n+\frac{\ell}{2}$ Bits absinkt. Zusäztlich können wir einen Algorithmus angeben, welcher die endgültige Entropie für einen beliebigen FCSR berechnet. Dieser Algorithmus kann auch verwendet werden, um zu zeigen, dass die Entropie immer größer als n Bits ist, und dass die Verschiebung einer Rückkopplungsposition um eine Stelle in Richtung des höchstwertigen Bits die Entropie erhöht.

Literatur

[AB05] F. Arnault and T. P. Berger. F-FCSR: Design of a new class of stream ciphers. In *FSE*, Lecture Notes in Computer Science, pages 83–97. Springer, 2005.

[ABM07] F. Arnault, T. P. Berger, and M. Minier. On the security of FCSR-based pseudorandom generators. In *SASC 2007 - ECRYPT Workshop on stream ciphers*, January 2007.

[CL94] R. Couture and P. L'Ecuyer. On the lattice structure of certain linear congruential sequences related to AWC/SWB generators. *Math. Comput.*, 62(206):799–808, 1994.

[KG97] A. Klapper and M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory. *J. Cryptology*, 10(2):111–147, 1997.

[MZ91] G Marsaglia and A Zaman. A new class of random number generators. *Annals of Appl. Prob.*, 1(3):462–480, 1991.

Ein Angriff auf Bivium mittels SAT Solver

Tobias Eibach* and Enrico Pilz†

* Universität Ulm † Universität Ulm

Trivium (und damit auch die reduzierte Variante Bivium) ist ein aussichtsreicher Stufe 2 Kandidat in dem europäischen eSTREAM Projekt. Das Design der Stromchiffre ist schlicht und elegant, vorgestellt wurde die Chiffre 2005 von Cannière und Preneel [CB05]. Bislang wurde noch kein wirkungsvoller Angriff auf die Chiffre gefunden.

Zu den bekanntesten Angriffen auf Strom Chiffren zählen die Algebraischen Angriffe, die darauf abzielen ein Gleichungssystem aufzustellen und zu lösen. Bekannte Verfahren hierbei sind der F4- und F5-Algorithmus die auf Gröbner Basen basieren, die sich in Softwarepaketen wie Magma und Singular finden.

In [BCJ07] wird vorgeschlagen SAT Solver zum Lösen solcher (dünner) Gleichungssysteme zu verwenden und dieser Gedanke wird in [MCP07] speziell auf Bivium angewendet und durchgeführt. Hierin wurden auch erste interessante experimentelle Ergebnisse veröffentlicht.

SAT Solver sind seit langer Zeit Forschungsgegenstand der Theoretischen Informatik, es geht darum, die Erfüllbarkeit von Booleschen Formeln (in CNF) zu überprüfen und ggf. eine Lösung auszugeben. Das Erfüllbarkeitsproblem ist das kanonische NP-vollständige Problem, man geht davon aus, dass es keinen Algorithmus gibt, der das Problem in polynomieller Laufzeit lösen kann. Trotz dieser theoretisch nicht-effizienten Laufzeit ging viel Forschungsarbeit in die Entwicklung von möglichst effizienten SAT Algorithmen, die hoch optimiert sind und auf Teilklassen (hier: „industrial instances“) besonders schnell arbeiten.

Für den Angriff auf Stromchiffren bedeutet das: Zuerst muss das Problem in ein Gleichungssystem umgeformt werden (dessen Lösung der gesuchte interne Zustand der Chiffre ist). Das algebraische Gleichungssystem wird dann in eine äquivalente CNF transformiert, die dann als Eingabe für einen SAT Solver dient.

Den oben beschriebenen Angriff haben wir implementiert und damit die Ergebnisse aus [MCP07] überprüft und weitere Experimente durchgeführt. Teilweise konnten wir Ergebnisse bestätigen, teilweise nicht. Neue Ergebnisse betreffen Fragestellungen auf dem Weg zu einem möglichst effizienten Angriff und sollen in dem Vortrag vorgestellt werden. Zum Bsp. geben wir eine empirische Antwort darauf, welche Bits des internen Zustandes am 'wertvollsten' sind und somit am besten 'erraten' werden sollten. Auerdem haben wir untersucht welcher SAT solver am Besten für diese Problemklasse geeignet ist und ob mehr Redundanz im Gleichungssystem das Problem einfacher macht. Abschlieend wird noch vorgestellt welche Fragestellungen wir in den nchsten Wochen noch untersuchen werden.

Literatur

[CB05] Cannière and Preneel. *TRIVIUM - a stream cipher construction inspired by block cipher design principles*, 2005.

[BCJ07] Bard and Courtois and Jefferson. *Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariat Polynomials over GF(2) via SAT-Solvers*,2007.

[MCP07] Cameron McDonals and Chris Charnes and Josef Pieprzyk. *Attacking Bivium with MiniSat*, 2007.

Auf der Suche nach schwachen Schlüsseln bei Trivium

Deike Priemuth-Schmid und Alex Biryukov

Laboratory of Algorithmics, Cryptology and Security
University of Luxembourg
e-mail: deike.priemuth-schmid@uni.lu, alex.biryukov@uni.lu

Die Stromchiffre Trivium wurde als Kandidat für das eSTREAM-Projekt [ECR05] im Jahr 2005 von C. De Cannière und B. Preneel [CP05] entwickelt. Seit der Veröffentlichung von Trivium wurde das Design der Chiffre nicht geändert, denn auch nach $2\frac{1}{2}$ Jahren gibt es keine wirklichen Angriffe auf Trivium. Dies und seine sehr guten Eigenschaften im Bereich Performanz und das geringe Zeit-Flächen-Produkt machen Trivium zu einer interessanten Stromchiffre.

Trivium verwendet einen 80 Bit Schlüssel, einen 80 Bit Initialwert und eine nichtlineare Update-Funktion. Von den Designern wurde die Chiffre mit einem 288 Bit Register vorgestellt, welches jedoch auf natürliche Weise in drei Register der Länge 93, 84 und 111 Bit zerfällt. Mit jeder Taktung der Chiffre wird diese aktualisiert und ein Schlüsselstrombit ausgegeben. Die maximale Anzahl an Schlüsselstrombits pro Schlüssel-Initialwert-Paar wurde von den Designern mit 2^{64} Bits festgelegt. Im Key-Setup wird der Schlüssel in das erste und der Initialwert in das zweite Register geladen, jeweils beginnend mit den ersten 80 Bit. Alle restlichen Bits werden mit Null initialisiert, mit Ausnahme der letzten 3 Bit des dritten Registers, welche auf Eins gesetzt werden. Dieser Zustand mit Schlüssel, Initialwert und den fest gesetzten Bits ist der Startzustand. Nachdem alle Bits initialisiert sind, wird das Register 4×288 mal unter Verwendung der Update-Funktion getaktet, ohne dass Schlüsselstrombits produziert werden. Danach beginnt die Erzeugung des Schlüsselstroms.

Wir untersuchen die Fragestellung, ob es Paare von Schlüsseln und Initialwerten gibt, welche wieder einen Startzustand reproduzieren, wie erstmals von Jin Hong [JH05] erwähnt. Im Startzustand sind 128 Bits festgelegt. Nutzen wir diese festen Positionen, um den zweiten Startzustand als Gleichungssystem darzustellen, so erhalten wir 128 Gleichungen in 160 Variablen, davon jeweils 80 Schlüssel- und Initialwertbits. Der maximale Grad dieser Gleichungen beträgt entweder 3 oder 4. Da die Anzahl der Variablen größer ist, als die der Gleichungen, erhalten wir 2^{32} mögliche Lösungen für das Gleichungssystem. Unser Ziel ist die effiziente Beschreibung dieser Lösungen. Desweiteren wollen wir auch andere Chiffren auf solche schwachen Schlüssel untersuchen.

Literatur

[CP05] C. De Cannière and B. Preneel. *TRIVIUM - a stream cipher construction inspired by block cipher design principles.* eSTREAM, ECRYPT Stream Cipher Projekt, Report 2005/030, 2005. http://www.ecrypt.eu.org/stream

[ECR05] eSTREAM: The ECRYPT Stream Cipher Projekt, http://www.ecrypt.eu.org/stream/

[JH05] Jin Hong. Discussion Forum. *certain pairs of key-IV pairs for Trivium*, created September 13, 2005 05:11PM. http://www.ecrypt.eu.org/stream/phorum/read.php?1,152

http://www.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

8. Kryptotag am 11. April 2008: Wilhelm-Schickard-Institut für Informatik der Universität Tübingen. Kontakt: Michael Beiter, Claudia Kaesser und Anja Korsten.

Bisherige Kryptotage

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

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.

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

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 fÂ¨ur Theoretische Informatik. Kontakt: Wolfgang Lindner und Christopher Wolf. 10 Einreichungen und 26 angemeldeten Teilnehmer.

1. Kryptotag am 1. Dezember 2004: Universität Mannheim, Lehrstuhl für 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.