Universität Mannheim, Reihe Informatik, TR 2004-10

1. Kryptotag – Workshop über Kryptographie Universität Mannheim

Stefan Lucks
Universität Mannheim, Deutschland

Christopher Wolf
KU Leuven, Belgien

1. Dezember 2004

Beiträge

1. Sebastian Faust und Stefan Lucks: **Neue Wege des anonymen Datenaustausches in Peer-2-Peer-Netzwerken**
2. Stefan Lucks: **Ein neues Designprinzip für kryptographische Hashfunctionen**
3. Jörg Lässig, Stefanie Thiem and Matthias Baumgart: **The Deterministic AKS Primality Method in the PRAM-Model and a Parallel Implementation on a High Performance Cluster**
4. Christof Paar and Jan Pelzl and Thomas Wollinger: **Hyperelliptic Cryptosystems in Practice**
5. Heiko Stamer: **Oleshchuk's Public Key Cryptosystem**
6. Christopher Wolf: **Äquivalente Private Schlüssel in Systemen mit $\mathcal{M}$ultivariaten $\mathcal{Q}$uadratischen Öffentlichen Polynomgleichungen**
7. Frederik Armknecht: **Algebraische Angriffe auf LFSR-basierte Stromchiffren**
8. Magnus Daum: **Solving Systems of Equations with incompatible operations**
9. Dirk Stegemann: **BDD-basierte Kryptanalyse von Flusschiffren am Beispiel des A5/1 Schlüsselstromgenerators**
10. Philipp A. Baer: **Group Authentication and Encryption in Distributed Environments**
11. André Schaumburg: **Authentification within Tree Parity Machine Rekeying**
12. Elena Ivanova Andreeva : **Overview of Authenticated Encryption Modes of Operation**
13. André Adelsbach, Markus Rohe and Ahmad-Reza Sadeghi: **Improving The Security Of Watermarking Schemes With Cryptographic Techniques**
14. Stefan Katzenbeisser: **Cryptographic Watermarking**
15. Tobias Straub: **Bridging the Usability Gap of PKI**

Neue Wege des anonymen Datenaustausches in Peer-2-Peer-Netzwerken

Sebastian Faust* und Stefan Lucks*
* Universität Mannheim
Deutschland

P2P-Netzwerke erfreuen sich zunehmender Beliebtheit und sind bisher besonders im Bereich des direkten Austausches von Dateien und Dokumenten, dem so genannten File-Sharing, weit verbreitet. Aufgrund der hohen Flexibilität durch die Verwendung einer dezentralen Netzwerk-Infrastruktur, lassen sich jedoch auch viele weitere Probleme mit Hilfe von P2P-Netzwerken lösen, beispielsweise aus dem Gebiet des Distributed Computing oder dem Instant Messaging.

Diese Arbeit beschäftigt sich mit dem sicheren Datenaustausch in Peer-to-Peer-Netzwerken. Hierbei werden wir uns auf die Anonymität der Teilnehmer konzentrieren.

Wir werden die Sicherheit der Teilnehmer in einem formalen Modell spezifizieren und, darauf aufbauend, zwei Bedrohungsmodelle entwickeln. Wir werden die Begriffe der ("absoluten") Sicherheit und der ("t-Sicherheit") einführen. Bei ersterer kontrolliert ein aktiver, dynamischer, arbeitsamer Angreifer mit Ausnahme einer Partei das Verhalten aller am Datenaustausch teilnehmenden Benutzer. Wir weisen nach, dass diese größtmögliche ("absolute") Sicherheit in einem Peer-to-Peer Netzwerk nicht erreichbar ist. Im Sinne eines etwas abgeschwächten Bedrohungsmodells, der ("t-Sicherheit"), bei dem maximal t Teilnehmer vom Angreifer korrumpiert werden dürfen, kann jedoch die Sicherheit aller ehrlichen Teilnehmer gewährleistet werden. Wir geben ein Protokoll an, das die t-Sicherheit garantiert.

Literatur

[ASF01] Dmitri Asonov, Markus Schaal and Johann-Christoph Freytag. *Absolute Privacy in Voting. LNCS – ISC2001, 2001.*

[DJN03] I. Damgard, M. Jurik and J. Nielsen. *A generalization of paillier's public-key system with applications to electronic voting*, 2003.

[Ste98] Julien P. Stern. *A New Efficient All-Or-Nothing Disclosure of Secrets Protocol.* LNCS vol. 1514 / 1998 – ASIACRYPT'98 , 1998.

Ein neues Designprinzip für kryptographische Hashfunctionen

Stefan Lucks

Universität Mannheim
http://th.informatik.uni-mannheim.de/people/lucks

Die Grundstruktur aller aktuell in der Praxis verwendeten Hashfunktionen stammt von Merkle [3] und Damgård [1]. Eine Kompressionsfunktion fester Eingabelänge wird so lange iteriert, bis der gesamte Input für die Hashfunktion verarbeitet wurde.

Um das Sicherheitsziel "Kollisionsresistenz" für die Hashfunktion zu erreichen, genügt schon die Kollisionsresistenz der Kompressionsfunktion. Verfehlt die Kompressionsfunktion dieses Ziel allerdings, sind auf die Hashfunktion sogar verheerende K-fache Kollisionsangriffe möglich. Dies zeigte Joux [2] auf der Crypto 2004.

Der Vortrag gibt eine Übersicht über

- verschiedene Sicherheitsziele für Hashfunktionen,
- das Designprinzip von Merkle und Damgård und
- den Angriff von Joux.

Des weiteren wird eine Verbesserung des Konstruktionsprinzips von Merkle und Damgård eingeführt, die nachweisbar Sicherheit gegen Angriffe wie den von Joux gewährleistet.

Literatur

[1] I. Damgård. A design principle for hash functions. Crypto 89.

[2] A. Joux. Multicollisions in iterated hash functions, application to cascaded constructions. Crypto 04.

[3] R. Merkle. One-way hash functions and DES. Crypto 89.

The Deterministic AKS Primality Method in the PRAM-Model and a Parallel Implementation on a High Performance Cluster

Jörg Lässig, Stefanie Thiem and Matthias Baumgart

Chemnitz University of Technology
09366 Chemnitz
Germany

In August 2002 the three Indian researchers Manindra Agrawal, Neeraj Kayal & Nitin Saxena at the Indian Institute of Technology in Kanpur published the manuscript "PRIMES is in $\mathcal{P}$" [Ag02] and presented a deterministic, polynomial time algorithm to determine whether a given integer is prime or composite.

Later on a series of variations of the original algorithm, has been published (e.g. [Br02]), the so-called AKS-class of algorithms. The improvements over the original AKS breakthrough are orders of magnitude, referring to Daniel J. Bernstein, one of the major protagonists [Be03].

The objective of these studies is to present a completely deterministic AKS instance with conjectured running time $T^{\infty}(n) = \tilde{O}(\log^4 n)$ in the PRAM Model, including all available speedups. Additionally, we present its parallel implementation and some experimental results besides a practical comparison to standard methods.

Key Words and Phrases: PRIMES, AKS-class, PRAM-model, Deterministic primality method

References

[Ag02] M. Agrawal and N. Kayal and N. Saxena. PRIMES is in P (revised version). Preprint, Indian Institute of Technology Kanpur. http://www.cse.iitk.ac.in/news/primality.html, December 2002.

[Br02] P. Berrizbeitia. Sharpening 'Primes is in P' for a Large Family of Numbers. Preprint, Universidad Simón Bolívar. http://arxiv.org/abs/math.NT/0211334, November 2002.

[Be03] D. J. Bernstein. Proving Primality after Agrawal-Kayal-Saxena. Preprint, University of Illinois at Chicago. http://cr.yp.to/papers.html, January 2003.

Hyperelliptic Cryptosystems in Practice

Christof Paar and Jan Pelzl and Thomas Wollinger

Communication Security Group — COSY
Ruhr Universität Bochum
Germany

The Hyperelliptic curve cryptosystem is one of the emerging cryptographic primitives of the last years. This system offers the same security as established public-key cryptosystems, such as those based on RSA or elliptic curves, with much shorter operand length. However, until recently the common belief in industry and in the research community was that hyperelliptic curves are out of scope for any practical application.

We were able to show the practical use of hyperelliptic curve cryptosystems (HECC) by narrowing the performance gap between elliptic curve (EC) and hyperelliptic curve cryptosystems. The complexity of the group operation for small genus hyperelliptic curves was reduced and efficient algorithms have been proposed [PWGP03, PWP03]. We developed a new metric to compare different cryptographic primitives based on the atomic operations of a processor and our theoretical comparison between elliptic curve and hyperelliptic curve cryptosystems, as well as our software and hardware implementations show that the performance of both cryptographic primitives are in the same range [P02]. Surprisingly, the hyperelliptic curve cryptosystems even outperform elliptic curves using certain curve parameters. We implemented these cryptosystems on general purpose processor and on a variety of different embedded processors, and build even a prototype implementation of a hyperelliptic curve coprocessor on FPGAs [WPWPSK04, Wol04].

References

[Wol04] Thomas Wollinger. Software and Hardware Implementation of Hyperelliptic Curve Cryptosystems Ph.D., Ruhr-University Bochum, Bochum, Germany July 2004.

[PWGP03] Jan Pelzl and Thomas Wollinger and Jorge Guajardo and Christof Paar. Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves *Workshop on Cryptographic Hardware and Embedded Systems - CHES 2003* September 2003.

[PWP03] Jan Pelzl and Thomas Wollinger and Christof Paar. Low Cost Security: Explicit Formulae for Genus-4 Hyperelliptic Curves *Tenth Annual Workshop on Selected Areas in Cryptography - SAC 2003* August 2003.

[P02] Jan Pelzl. Hyperelliptic Cryptosystems on Embedded Microprocessors Diplomarbeit, Ruhr-Universitt Bochum September 2002.

[WPWPSK04] Thomas Wollinger and Jan Pelzl and Volker Wittelsberger and Christof Paar and Gokay Saldamli and Cetin Koc. Elliptic and Hyperelliptic Curves on Embedded uP *Special issue on Embedded Systems and Security of the ACM Transactions in Embedded Computing Systems (TECS)*

Oleshchuk's Public Key Cryptosystem

Heiko Stamer

Universität Kassel, Fachbereich Mathematik/Informatik
Heinrich-Plett-Straße 40, D-34132 Kassel, Germany
stamer@theory.informatik.uni-kassel.de

Vor etwa zehn Jahren stellte VLADIMIR A. OLESHCHUK [Olk95] ein neues asymmetrisches Verschlüsselungsverfahren vor, dessen Sicherheit auf der Unentscheidbarkeit des Wortproblems für endliche Wortersetzungssysteme basiert. Zur Konstruktion der Falltürfunktion verwendet er dabei eingeschränkte Systeme mit *Church-Rosser Eigenschaft*, für die das Wortproblem in linearer Zeit lösbar ist. Diese grundsätzliche Strategie wurde später auch auf Baumersetzungssysteme [Sa03] übertragen.

Ein motivierender Entwicklungsaspekt solcher Verfahren ist sicherlich die beweisbare Schwierigkeit des zugrundeliegenden Problems. Leider ist damit noch keinerlei Aussage über die praktische Sicherheit getroffen, denn alle bekannten Ansätze leiden unter anderen Verwundbarkeiten. Insbesondere spielt hier die Problematik „schwacher Schlüssel" eine große Rolle, d. h. die bekannte Lücke zwischen *average-* und *worst-case Komplexität* von Instanzen tritt hier verstärkt zutage. Hinsichtlich Oleshchuks Verfahren hat sich beispielsweise herausgestellt, daß viele der möglichen Schlüssel (Wortersetzungssysteme) durch *Vervollständigung* [StO04] angreifbar sind.

Der Vortrag führt anfangs die notwendigen theoretischen Grundlagen von Wortersetzungssystemen ein. Im Hauptteil wird das oben erwähnte Kryptosystem vorgestellt. Schließlich betrachten wir einige Ideen zur Kryptoanalyse und untersuchen praktische Implementierungsfragen.

Literatur

[Olk95] Vladimir A. Oleshchuk: *On Public-Key Cryptosystem Based on Church-Rosser String-Rewriting Systems*, Proc. COCOON'95, Lecture Notes in Computer Science **959**, pp. 264–269, 1995

[Sa03] S.C. Samuel, D.G. Thomas, P.J. Abisha, K.G. Subramanian: *Tree Replacement and Public Key Cryptosystem*, INDOCRYPT 2002, Lecture Notes in Computer Science **2551**, pp. 71–78, 2002

[StO04] Heiko Stamer, Friedrich Otto: *On Oleshchuk's Public Key Cryptosystem*, Cryptology ePrint Archive, Report 2004/220, 2004, http://eprint.iacr.org/2004/220/

Äquivalente Private Schlüssel in Systemen mit $\mathcal{M}$ultivariaten $\mathcal{Q}$uadratischen Öffentlichen Polynomgleichungen

Christopher Wolf

ESAT-COSIC, K.U. Leuven, Belgien
http://www.esat.kuleuven.ac.be/cosic/
Christopher.Wolf@esat.kuleuven.ac.be
oder chris@Christopher-Wolf.de

Seit dem Artikel von Matsumoto und Imai [MI88] über asymmetrische Systeme mit multivariaten Polynomgleichungen als öffentlichem Schlüssel wurden eine Reihe solcher Systeme vorgeschlagen, z.B. [Pat96] und [KPG99]. Die Variante HFE- bildet die Grundlage einer verbesserten Version des Signaturverfahrens Quartz während C^{*--} im Signaturschema $Sflash^{v3}$ Verwendung findet.

In diesem Vortrag beleuchten wir die Struktur des privaten Schlüsselraums in diesen Systemen. Insbesondere zeigen wir, dass sowohl in HFE- als auch in C^{*--} für jeden privaten Schlüssel eine große Anzahl äquivalenter Schlüssel existiert, die alle auf den selben öffentlichen Schlüssel abgebildet werden.

Des weiteren stellen wir einen effizienten Algorithmus vor, mit dessen Hilfe eine Normalform für private Schlüssel in diesen Systemen berechnet werden kann.

Literatur

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *EUROCRYPT 1999*, volume 1592 of *LNCS*, pages 206–222.

[MI88] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature verification and message-encryption. In *EUROCRYPT 1988*, volume 330 of *LNCS*, pages 419–545.

[Pat96] Jacques Patarin. Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In *EUROCRYPT 1996*, volume 1070 of *LNCS*, pages 33–48. Extended Version: http://www.minrank.org/hfe.pdf.

Algebraische Angriffe auf LFSR-basierte Stromchiffren

Frederik Armknecht

Universität Mannheim

Durch ihre hohen Effizienz haben LFSR[1]-basierte Stromchiffren ihre Anwendung in der Praxis gefunden (bspw. im Bluetooth- oder GSM-Standard). LFSRs sind endliche Automaten, die auf einfache Art und Weise Bitstrme beliebiger Lnge produzieren knnen, welche sehr gute statistische Eigenschaften besitzt. Mit der Zeit entwickelten Kryptographen Techniken, um die Resistenz solcher Stromchiffren gegen eine Reihe von Angriffen (bspw. Fast Correlation Attacks) zu erhhen.

Vor knapp zwei Jahren wurde eine neue Angriffsmethode vorgestellt, die sogenannten algebraischen Angriffe. Die Idee ist es, den geheimen Schlssel durch Lsen eines (ggf. nichtlinearen) Gleichungssystems zu rekonstruieren. Whrend das Lsen von nichtlinearen Gleichungssystemen im Allgemeinen schwierig ist, ist es aus mancherlei Grnden in diesem speziellen Fall einfacher. Es stellte sich heraus, dass die algebraischen Angriffe in vielen Fllen die schnellsten (theoretischen) Angriffe darstellen.

Der Vortrag gibt eine Einfhrung in die obige Thematik und bietet einen Einblick in den aktuellen Stand der Forschung.

Literatur

[1] Frederik Armknecht, Matthias Krause: *Algebraic attacks on Combiners with Memory*, Proceedings of Crypto 2003, LNCS 2729, pp. 162-176, Springer, 2003.

[2] Nicolas Courtois, Willi Meier: *Algebraic attacks on Stream Ciphers with Linear Feedback*, Proceedings of Eurocrypt 2003, LNCS 2656, pp. 345-359, Springer, 2003. An extended version is available at http://www.cryptosystem.net/stream/

[3] Nicolas Courtois: *Fast Algebraic Attacks on Stream Ciphers with Linear Feedback*, Proceedings of Crypto 2003, LNCS 2729, pp. 177-194, Springer, 2003.

[1] LFSR = Linear Feedback Shift Register

Solving Systems of Equations with incompatible operations

Magnus Daum

CITS Research Group, Ruhr University Bochum

In many cryptographic algorithms, which are aimed at being efficiently implementable rather than having some formal proof of security (e.g. in many dedicated hash functions or block ciphers), a mixture of very different kinds of operations is used. These operations include GF(2)-linear operations, additions modulo 2^n, bitwise applied Boolean functions and bit shifts and rotations. As these operations are not very compatible from a mathematical point of view, it is hard to analyse these structures theoretically and you need sophisticated algorithms to solve equations in which some different of these operations are involved.

In his attacks on various hash functions (see for example [Do97]) Dobbertin had to solve large systems of equations of this kind. We analyse the algorithms used by Dobbertin and describe improvements which lead to directed graphs, which represent the sets of solutions of such equations quite efficiently.

These graphs are related very closely to binary decision diagrams (see [We03]). Thus from the theory of decision diagrams many algorithms can be adopted. For example, it is possible to efficiently compute the number of solutions or to combine two such graphs to compute the intersection of two sets of solutions.

T-functions, as proposed by Klimov and Shamir (see [Kl04]), are another topic for which these algorithms could be of some interest, because due to their defining property, equations which only include T-functions should be solvable quite efficiently with such algorithms.

References

[Do97] H. Dobbertin (1997). *RIPEMD with two-round compress function is not collision-free.* Journal of Cryptology 10, pp. 51-68.

[We03] I. Wegener (2003). *Branching Programs and Binary Decision Diagrams–Theory and Applications.* SIAM.

[Kl04] A. Klimov (2004). *Applications of T-functions in Cryptography.* PhD Thesis, Weizmann Institute of Science.
(available from `http://www.wisdom.weizmann.ac.il/~ask/`)

BDD-basierte Kryptanalyse von Flusschiffren am Beispiel des A5/1 Schlüsselstromgenerators

Dirk Stegemann

Universität Mannheim

Viele praktisch eingesetzte Flusschiffren basieren auf einer kleinen Zahl linear rückgekoppelter Schieberegister (*Linear Feedback Shift Registers*, kurz LFSRs), deren Ausgabebitströme mit Hilfe einer nichtlinearen Kompressionsfunktion zu einem Schlüsselstrom $y \in \{0,1\}^*$ verdichtet werden.

[Kra02] identifiziert die *best case* Kompressionsrate γ und die durchschnittliche Informationsrate α der Kompressionsfunktion als entscheidende Sicherheitsparameter und beschreibt einen Angriff auf LFSR-basierte Flusschiffren, der den geheimen Initialzustand $x \in \{0,1\}^n$ in einer Laufzeit von $n^{O(1)}2^{\frac{1-\alpha}{1+\alpha}n}$ aus den ersten $\lceil \gamma\alpha^{-1}n \rceil$ aufeinanderfolgenden Bits des Schlüsselstroms y rekonstruiert. Die Grundlage dieses Angriffs bildet die Repräsentation der Zwischenergebnisse in Binären Entscheidungsdiagrammen (*Binary Decision Diagrams*, kurz BDDs), die bisher vor allem zur formalen Schaltkreisverifikation im VLSI-Design eingesetzt wurden. Von [Sch02] und [Ste04] durchgeführte Experimente mit verschiedenen Flusschiffren scheinen die theoretischen Resultate zu bestätigen, zeigen jedoch gleichzeitig die durch hohen Speicherbedarf bedingten Grenzen der praktischen Durchführbarkeit von BDD-basierten Angriffen auf. Am Beispiel des A5/1 Schlüsselstromgenerators [BGW99] aus dem GSM-Standard soll die BDD-basierte Kryptanalyse vorgestellt und auf Implementationsaspekte und experimentelle Resultate eingegangen werden.

Literatur

[Kra02] M. Krause. BDD-based cryptanalysis of keystream generators. In *EUROCRYPT 2002*, Band 2332 der Reihe *Lecture Notes in Computer Science*, Seiten 222–237. Springer Verlag, Heidelberg, 2002.

[BGW99] M. Briceno, I. Goldberg, and D. Wagner. *A pedagogical implementation of A5/1*, May 1999. http://jya.com/a51-pi.htm.

[Sch02] F. Schleer. Einsatz von OBDDs zur Kryptanalyse von Flusschiffren. Diplomarbeit, Universität Mannheim, 2002.

[Ste04] D. Stegemann. Fbdd-basierte Kryptanalyse des A5/1 Schlüsselstromgenerators. Diplomarbeit, Universität Mannheim, 2004.

Group Authentication and Encryption in Distributed Environments

Philipp A. Baer

University of Ulm
Department of Theoretical Computer Science
Germany

Security is not always considered an important issue for groups of distributed systems. Message authentication and encryption are often disregarded, sometimes just because of missing implementations. Nevertheless, especially in the context of communication, control and monitoring, security is an extremely important issue.

This paper discusses techniques that address some of the basic security requirements for unreliable group communication scenarios. It combines existing security technologies (DH, GDH [STW96], DSA, AES) and communication protocols/schemes (IPv6, Multicast) for group collaboration scenarios in unreliable environments. Message authentication and message stream encryption for groups, to only mention the most important ones, are considered exemplary. The architecture and its communication primitives are tailored to the needs of unreliable environments. This is mostly due to its intended field of application: groups of autonomous mobile systems.

The architecture is designed for a wide variety of systems and open in the sense of extensibility. For the proposed techniques, i.e. key agreement, authentication and encryption, very simple yet extensible protocols are used. Because of the many unsolved problems in the area of secure ad-hoc communication, and due to the wide variety of involved scientific subjects, only a superficial solution can be presented.

References

[Bae04] Philipp A. Baer. *Group Authentication and Encryption in Distributed Environments*. University of Ulm, July 2004.

[STW96] Michael Steiner, Gene Tsudik, and Michael Waidner. Diffie-Hellman key distribution extended to group communication. In *ACM Conference on Computer and Communications Security*, pages 31–37, March 1996.

Authentification within Tree Parity Machine Rekeying

André Schaumburg

Hamburg University of Science and Technology, Distributed Systems
Schwarzenbergstraße 95, 21073 Hamburg - Germany

Interaction of Tree Parity Machines (TPMs) has been discussed as an alternative secure key exchange concept and attacks have been proposed [KKK02]. Authentication is at least as important as a secure exchange of keys. Adding an authentication *e.g.* via hashing is straightforward but outside the concept named *Neural Cryptography*. The here presented is a consequent formulation of an implicit Zero-Knowledge authentication from within the key exchange concept and another alternative, integrating an explicit Zero-Knowledge authentication into the already interactive protocol. A Man-In-The-Middle attack and even all currently known attacks can so be averted. This in turn allows to securely exploit the trajectory in key space along with rapid key exchange and an efficient increase of key length.

Another benefit of the here presented authentication method is that all currently known findings concerning Neural Cryptography are untouched and still valid - even with the extension of authentication. Further on there is no need to reimplement the interface, it only gets extended by an authentication control unit.

The general trade-off in applied cryptography between available resources and the required level of security also applies using the TPM principle. In many practical embedded security solutions it is often admissive to provide a system safe enough for the particular application, and given certain attack scenarios. The TPM principle extended with the proposed authentication is very attractive for such embedded applications due to its hardware-friendly basic operations, particularly not operating on large numbers.

References

[KKK02] Kanter, I., Kinzel, W. and Kanter, E.: *Secure exchange of information by synchronization of neural networks* Europhysics Letters **57** (2002), pp. 141–147

[VS04] Volkmer, M. and Schaumburg, A.: *Authenticated tree parity machine key exchange* Preprint cs.CR/0408046 (2004), submitted to Europhysics Letters

Overview of Authenticated Encryption Modes of Operation

Elena Ivanova Andreeva

Saarland University

Traditional block cipher modes of operation, namely CBC, CFB, OFB and CTR, provide encryption with achieving the confidentiality goal without any integrity guarantees. On the other hand, there exist authentication modes that are custom-made to ensure integrity. However, they do not provide a secure encryption.

A conventional way to satisfy both security properties, confidentiality and integrity, is to make two separate passes on the data. One encryption pass for the encrypting of the data block cipher-wise, and a second authentication pass for checking the data integrity.

Recently, new unconventional integrity-aware modes of operation for block ciphers have been proposed. They provide confidentiality and integrity by combining authentication modes with the traditional block ciphers making only a single pass on the data. These modes are called authenticated encryption modes. In our presentation we give an overview on some of these newly proposed authenticated encryption modes, like IACBC, IAPM[JU01], XCBC[GD01] and OCB[RBBK01], their properties and advantages for a future use.

References

[GD01] V. Gligor, P. Donescu. Fast encryption and authentication: XCBC Encryption and XECB Authentication modes. *Proceedings of the Fast Software Encryption Workshop - FSE '01. Springer-Verlag*, October 2001.

[JU01] C. Jutla. Encryption Modes with Almost Free Message Integrity. *Advances in Cryptology-EUROCRYPT 2001.*

[RBBK01] P. Rogaway, M. Bellare, J. Black and T. Krovetz. OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption *ACM Transactions on Information and System Security (TISSEC)*, vol. 6, no. 3, pp. 365-403, August 2001.

Improving The Security Of Watermarking Schemes With Cryptographic Techniques

André Adelsbach*, Markus Rohe† and Ahmad-Reza Sadeghi*

†Universität des Saarlandes
Saarbrücken
mail@markus-rohe.de

*Ruhr-Universität Bochum
andre.adelsbach@nds.rub.de
sadeghi@crypto.rub.de

Standard information hiding schemes, such as watermarking schemes suffer from a major problem: They require to reveal security critical information to potentially untrusted parties, when proving the presence of a watermark to these parties. Zero-knowledge watermark detection is a promising means to overcome this problem:

The embedded information is concealed from the verifying party while the proving party is committed to it. A prover and a verifier perform a zero-knowledge detection protocol after which the verifier is convinced that the committed information is imperceptibly present in the given digital content without gaining any new knowledge on the security critical information.

However, concealing the embedded information prevents the verifying party from performing additional checks on this data, e.g., on its probability distribution, which may be required for certain applications. We overcome this limitation by proposing concrete and practical protocols, which pursue two promising strategies:

The first one is to prove in zero-knowledge that a concealed information suffices a certain predicate, whereas the second strategy is to interactively and verifiably generate committed information that suffices the desired predicate, e.g., matches a certain probability distribution.

Moreover, we have designed an efficient implementation of a zero-knowledge watermark detection protocol to demonstrate its applicability in practice.

Cryptographic Watermarking

Stefan Katzenbeisser

Institut für Informatik, Technische Universität München
D-85748 Garching bei München
katzenbe@in.tum.de

The rapid growth of the Internet as a distribution medium for digital goods increased the risk of copyright infringements. From an economic point of view, this risk makes the commercialization of digital works difficult, if not impossible. Therefore, the need for technical copyright protection solutions has increased steadily over the last years. Robust digital watermarking became a promising technology in the context of copyright protection and was proposed as a central building block in various e-Commerce protocols (such as dispute-resolving, copy protection and traitor tracing schemes or DRM applications). Traditionally, the design of watermarking schemes was seen as a signal-processing problem and concentrated on issues such as the imperceptibility of the watermark or its resistance against unauthorized removal. However, when a watermark is to be used in an e-Commerce system, its properties may become critical to the security of the overall scheme. It is therefore necessary to gain a thorough and mathematically precise understanding of the essential security properties of watermarks.

In this talk, I review recent results [1, 2] that establish the security of two cryptographic protocols that employ watermarking operations as basic primitives. The first protocol can be used in dispute-resolving schemes in order to assure their resistance against an important class of attacks. The second protocol allows to detect forgeries in image files or video streams by embedding a watermark carrying a cryptographic signature. Both constructions are provably secure under standard cryptographic assumptions.

References

[1] A. Adelsbach, S. Katzenbeisser, H. Veith, "Watermarking Schemes Provably Secure Against Copy and Ambiguity Attacks", in *ACM Workshop on Digital Rights Management (DRM'2003)*, Proceedings, Washington DC, 2003, pp. 111-119.

[2] J. Dittmann, S. Katzenbeisser, C. Schallhart, H. Veith, "Provably Secure Authentication of Digital Media Through Invertible Watermarks", to appear as IACR ePrint report, 2004.

Bridging the Usability Gap of PKI

Tobias Straub
tstraub@gkec.tu-darmstadt.de
Computer Science Department
Technische Universitaet Darmstadt

From a user's viewpoint, security in general and PKI (public key infrastructure) in particular are complex matters. According to a recent study [kes04], the majority of security incidents still can be traced back to user errors or carelessness, although users' troubles with PKI-enabled applications are known since the study of Whitten and Tygar investigating the handling of secure e-mail [WT99].

Unfortunately, due to the nature of PKI, user interaction cannot be avoided entirely, e.g. when an unknown certificate has to be imported as a trust anchor. In my work, I am proposing several measures to face the usability challenges of PKI.

One of them is a generic framework to comprehensively evaluate usability and utility of PKI-enabled applications [SB04]. Apart from being a tool to detect usability problems and assess applications, it may as well serve as a requirements specification for application designers.

Another idea is to delegate complex and security-critical tasks to skilled personnel or a service provider. For instance, the protocol described in [Str04] allows an organization to outsource the task of maintaining a PKI in a way that it retains full control and does not have to trust the service provider.

References

[kes04] Lagebericht zur Informationssicherheit. In: kes 4/2004 and 5/2004.

[Str04] T. Straub. A Method for Strengthening Certificate Enrollment. WartaCrypt, 2004.

[SB04] T. Straub and H. Baier. A Framework for Evaluating the Usability and the Usefulness of PKI-enabled Applications. European PKI-Workshop, 2004. (Springer LNCS 3093)

[WT99] A. Whitten, J.D. Tygar. Why Johnny Can't Encrpyt: A Usability Evaluation of PGP 5.0. USENIX Security Symposium, 1999.