2. Krypto-Tag – Workshop über Kryptographie Universität Ulm

Wolfgang Lindner (Hg.)
Universität Ulm

Christopher Wolf (Hg.)
K.U.Leuven

31. März 2005

Ulmer Informatik-Berichte Nr. 2005-02
K.U.Leuven, Technical Report ESAT-COSIC 2005-CW-1

Inhaltsverzeichnis

Multicast-Security – Simulation logischer Schlüsselbäume unter Berücksichtigung unterschiedlichen Benutzerverhaltens

Alexander Heese, Luigi Lo Iacono, Christoph Ruland

Institut für Digitale Kommunikationssysteme
Universität Siegen

In Multicast-Umgebungen werden Nachrichten von einem Sender an mehrere Empfänger geschickt. Durch Verschlüsselung der Kommunikation und durch kontrolliertes Verteilen der kryptographischen Schlüssel zur Entschlüsselung wird der Zugang zu den Kommunikationsinhalten kontrolliert. Die Verteilung und Verwaltung der kryptographischen Schlüssel ist hierbei von grundlegender Bedeutung und stellt eines der Hauptprobleme bei der Realisierung vertraulicher Multicast-Kommunikation dar. Insbesondere große Gruppen mit häufigen Ein- und Austritten der Mitglieder sind hinsichtlich der Skalierbarkeit und Sicherheit in diesem Zusammenhang zu betrachten. Zur Lösung dieser Problemstellung wurden logische Schlüsselbäume vorgeschlagen, die zur Verwaltung des Gruppenschlüssels dienen [WGL98, WHA99].

Die Vorteile dieser Verfahren gehen offensichtlich verloren, sobald die zugrundeliegende Baumstruktur entartet. Gegenstand dieser Arbeit ist die Veränderungen der Schlüsselbäume anhand des Verhaltens von Benutzergruppen zu simulieren und hieraus den durchschnittlichen Aufwand für die verschiedenen Schlüsselverteilstrategien zu ermitteln. Als Grundlage für die Simulationen werden Untersuchungsergebnisse zum Benutzerverhalten in Multicast-Gruppen herangezogen [Al00, HB01]. Aus dem beobachteten Benutzerverhalten sowohl im MBone als auch bei Netzwerk-Spielen werden Verhaltensmuster herausgearbeitet und darauf aufbauend Szenarien definiert, die die Basis für die Simulationen bilden.

Literatur

[WGL98] C. K. Wong, M. Gouda, and S. S. Lam. Secure Group Communication using Key Graphs. *In Proceedings of ACM SIGCOMM '98*, 1998.

[WHA99] D. M. Wallner, E. G. Harder, and R. C. Agee. Key Management for Multicast: Issues and Architectures. *IETF RFC 2627*, 1999.

[Al00] Kevin C. Almeroth. A Long-Term Analysis of Growth and Usage Patterns in the Multicast Backbone (MBone). *IEEE Infocom*, 2000.

[HB01] Tristan Henderson and Saleem Bhatti. Modelling User Behaviour in Networked Games. *In Proceedings of the 9th ACM international conference on Multimedia*, Ottawa, Canada, pp. 212-220, 2001.

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.

Mental Poker in practice: An extended implementation of Schindelhauer's Toolbox for Mental Card Games

Heiko Stamer

University of Kassel, Department of Mathematics/Computer Science
Heinrich-Plett-Straße 40, D-34132 Kassel, Germany
stamer@theory.informatik.uni-kassel.de

A lot of cryptographic research has been carried out on *Mental Poker* during the last decades. But efficient implementations are still very rarely.

Few years ago Schindelhauer [Sc98] introduced a general toolbox which extends previous work of Crépeau [Cr87]. Roughly speaking, the type of a card is shared among the players through bitwise representation by quadratic (non-)residues. Thus the security relies on the well known *Quadratic Residuosity Assumption (QRA)*. Unfortunately, the size of a card grows linearly in the number of players and logarithmically in the number of different cards. Recently a more efficient solution [BS03] was proposed, whose security can be based on the *Decisional Diffie-Hellman Assumption (DDH)*. Moreover, the encoding is independent of the number of players respectively cards.

My talk presents the technical details of a extended implementation for the open source library `libTMCG` [St05]. Further we discuss the practicability while considering as example the german card game *Skat* [St04].

References

[Sc98] Christian Schindelhauer. *Toolbox for Mental Card Games*. Technical Report A-98-14, University of Lübeck, 1998.

[Cr87] Claude Crépeau. *A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or how to achieve an electronic poker face*. In *Advances in Cryptology: CRYPTO '86 Proceedings*, Lecture Notes in Computer Science **263**, pp. 239-247, 1987.

[BS03] Adam Barnett and Nigel P. Smart. *Mental Poker Revisited*. In K.G. Paterson (Ed.): *Cryptography and Coding 2003*, Lecture Notes in Computer Science **2898**, pp. 370–383, 2003.

[St04] Heiko Stamer. *Kryptographische Skatrunde.* In Offene Systeme **4**, pp. 10–30, 2004. ISSN 1619-0114

[St05] Heiko Stamer. `http://savannah.nongnu.org/projects/libtmcg/`

MYSTERY-TWISTER – www.mystery-twister.com

Hans Dobbertin, Magnus Daum, Patrick Felke, Gregor Leander

CITS Research Group
Ruhr Universität Bochum

Die Forschungsgruppe Kryptologie und Informationssicherheit (CITS) der Universität Bochum organisiert im Jahr 2005 den internationalen Kryptographie-Wettbewerb MYSTERY-TWISTER. Es geht um Verschlüsselung, die jedem jeden Tag begegnet, meist unbemerkt. Der Wettbewerb richtet sich sowohl an Jedermann, der gerne verstehen möchte wie Verschlüsselung bei Online Banking, im Handy oder im Bankautomaten funktioniert, als auch an führende Forscher auf dem Gebiet der Kryptographie.

Im Laufe des Jahres 2005 werden 13 CryptoChallenges (CC1 bis CC13) mit steigendem Schwierigkeitsgrad veröffentlicht. Es geht unter anderem um das Entschlüsseln von Nachrichten, das Klonen von Mobil-Telefonen und das Fälschen von digitalen Signaturen.

Die Auswahl der Themen für die 13 Challenges werden dabei einen Überblick über viele Bereiche moderner Kryptographie liefern.

Einer der wichtigsten Gründe für MYSTERY-TWISTER ist es, auch Laien die nötigen Informationen und Einsichten zu vermitteln, die nötig sind, um die Prinzipien moderner kryptographischer Verfahren zu verstehen. Wichtig ist daß MYSTERY-TWISTER diese Einsichten spielerisch vermittelt.

Für Forscher auf dem Gebiet der Kryptographie sind die CryptoChallenges 9 bis 13 gedacht. Hier sind Profis gefragt und in den Aufgaben geht es zum Beispiel um AES und RSA, also die defacto Verschlüsselungs-Standards schlechthin. Wer hier Erfolg haben will, muss einen echten Beitrag zur aktuellen Forschung leisten.

Und nicht zuletzt lohnt sich die Teilnahme bei MYSTERY-TWISTER, da...

...es Spaß macht Codes zu knacken und Geheimnisse zu lüften.

Erweiterte visuelle Kryptographie

Andreas Klein

Fachbereich für Mathematik/Informatik, Universität Kassel

Visuelle Kryptographie wurde 1994 von Naor und Shamir [3] erfunden. Dabei wird ein Schwarz-Weiß-Bild so in zwei Bilder codiert, daß jedes der beiden Bilden wie ein zufälliges Punktmuster wirkt. Kopiert man jedoch diese Bilder auf Folien und legt diese übereinander, so erscheint wieder das ursprüngliche Bild.

Allgemeiner kann man visuelle Kryptographie als ein Shared-Secret-System auffassen, dabei wir das geheime Bild so auf n Folien verteilt, daß man es nur durch das Übereinanderlegen von mindestens k Folien rekonstruieren kann. Eine weitere Verallgemeinerung erzeugt n Folien, so daß man bei jeder der $2^n - 1$ möglichen Kombinationen von Folien ein anderes Bild sieht. Dabei sind alle Bilder voneinander unabhängig, d.h. man kann durch Untersuchen eines Teils der Bilder keine Rückschlüsse auf die anderen Bilder ziehen.

Die folgende Abbildung zeigt das Prinzip mit zwei Folien.

Das dies für jede natürliche Zahl n möglich ist wurde zu erst in [1] bewiesen. In meinem Vortrag werde ich nicht nur die Existenz dieser System beweisen, sondern auch das jeweils beste System charakterisieren.

Literatur

[1] S. Droste: *New results in visual cryptography.* In: *Advances in cryptology – CRYPTO '96*, Band 1109 von *Lect. Notes Comput. Sci.*, S. 401–415. Springer, Berlin, 1996.

[2] A. Klein und M. Wessler: *Extended visual cryptography schemes.* Information and Computation to appear.

[3] M. Naor und A. Shamir: *Visual cryptography.* In: *Advances in Cryptology – EUROCRYPT '94* (Herausgegeben von A. D. Santis), Band 950 von *Lect. Notes Comput. Sci.*, S. 1–12. Springer, Berlin, 1994.

Fair DRM – Fair Use by Secret Sharing

André Adelsbach, Ulrich Greveler, Jörg Schwenk

Horst Görtz Institute for IT security
Ruhr-Universität Bochum, Germany
www.nds.rub.de

We present a *fair* DRM environment, where each user can act pseudonymously and is entitled to make a fixed number of copies for private purposes (*e.g.*, a maximum of 7 copies) but where the user can be identified and prosecuted when more copies are produced.

Our system constitutes three central authorities (pseudonymization, licensing, issuer) in order to protect the user agains malicious providers and uses secret-sharing schemes in a way that a central authority can only reconstruct the secret (the user's identity) when a number of shares is transmitted by the media players. The user's identity will not be known to this authority as long as the user limits the number of private copies to the maximum (being a parameter in the system).

The set-up phase of the DRM system let each user choose a pseudonym that is a key pair (sk_P, pk_P) and let him send a request for a certificate on this pseudonym

$$Req_{Pseud} = Sign(sk_B, pk_P||terms)$$

to a pseudonymization authority, where $terms$ is a description of the contractual conditions regarding liability and depseudonymization.

The users may obtain a licence for an object identified by DOI when he sends a signed request

$$Req = Sign(sk_P, < DOI||cert_P||terms >)$$

to the licensing agency. This licence can then be of the form

$$Licence = Sign(sk_L, DOI||Pol||Rights||Enc(pk_P, key))$$

where Pol is a random polynom of the same degree as the number of allowed copies so that Shamir's secret-sharing scheme may be used here. We will also present other forms with different performance characteristics. The media player evaluates Pol at position $i := Hash(Licence||player - ID)$ and transmit share

$$S := DOI||Hash(Licence)||i||Pol(i)$$

so each time the object is played the same share is computed but different players will compute different shares with high probability.

Klassifizierung von Public Key Systemen mit Multivariaten Quadratischen Polynomen

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 den frühen 1980er Jahren werden multivariate quadratische Gleichungen für die Konstruktion von Public Key Kryptosystemen eingesetzt. Diese Gleichungen sind im Gegensatz zu linearen Gleichungen schwer zu lösen — Stichwort $\mathcal{NP}$-Vollständigkeit.

Bisher wurden eine Reihe von grundlegenden Klassen vorgeschlagen — 1988 das System MIA von Matsumoto-Imai (Schema A), 1996 die HFE (Hidden Field Equations) von Jacques Patarin, und 1997 die Essig und Öl Systeme von Patarin, die 1999 von Kipnis, Goubin und Patarin zu den UOV (Unbalenced Oil and Vinegar) Systemen verallgemeinert wurden. Als letzte Klasse seien noch die 1993 von Shamir als Birational Permutations vorgeschlagenen Systeme genannt, die 2000 von Goubin und Courtois zu TPM (Triangular Plus Minus) spezialisiert wurden und letztere 2004 von Wolf, Braeken und Preneel zu STS (Stepwise Trianguar Systems) in eine andere Richtung verallgemeinert wurden. Diese Grundklassen können in eine einfache Taxonomie gebracht werden.

Neben diesen Grundklassen sind auch eine Reihe von generischen Modifikatoren bekannt, wie z.B. die Minus Modifikation, die Plus Modifikation, das Fixieren von Variablen, das Aufspalten in verschiedene Äste, dünn besetzte Polynome für den geheimen Schlüssel sowie das interne Stören der Gleichungen.

Darüber hinaus wurden seit Beginn 2000 verschiedene *Mischsysteme* vorgeschlagen, die jeweils versuchen aus bekannten Bausteinen neue Systeme zu entwickeln. Analog dem Design-Prinzip von Blockchiffren werden dabei (einzeln) schwache Komponenten verbunden, um damit ein stärkeres Gesamtsystem zu erhalten. Vertreter sind die *enhanced Tame Transformation Signatures* von Chen und Yang sowie die *Tractable Rational Maps* von Wang und Chang. Beide benutzen als Grundgerüst STS. Während Chen und Yang hier dünn besetzte UOV Systeme einbetten, verwenden Wang und Chang dünn besetzte Monome über einem Erweiterungskörper und sind damit relativ nahe an der MIA Konstruktion.

Immediate Rekeying by Tree Parity Machines in a WLAN-System

Nazita Behroozi

Hamburg University of Technology, Distributed Systems,
Schwarzenbergstraße 95, D-21073 Hamburg – Germany
E-mail: nazita_behroozi@hotmail.com

WPA and IEEE802.11i provide the Pre-Shared-Key (PSK) for key establishment in Wireless LAN (WLAN) in the case that no 802.1x authentication server (RADIUS) is available. Recent research shows the risk of using PSK because the security depends on the length and quality of the pass phrase used [2].

We investigate secure key exchange in WLAN via Tree Parity Machines (TPMs) [1]. In order to evaluate the capability and suitability of an integrated key exchange via TPM, a system was developed which allows the transfer of encrypted data between two WLAN clients. One WLAN client is an embedded system that includes a hardware- and a software-part. It was developed on an embedded ARM processor based development kit with a FPGA device. The other WLAN client was implemented in software running on a Personal Computer.

In this work an *immediate rekeying* scenario was implemented to study frequent key exchange via TPMs in parallel to the encrypted data transmission in WLAN. The immediate rekeying technique allows exchange a new key as soon as the previous key has been exchanged. We measured the number of keys exchanged and used for encryption of different amounts of data to be transferred. The evaluation shows that each Ethernet packet with a maximum length of 1500 byte can be encrypted with a new key in the best case. In Temporal Key Integrity Protocol which is used in WPA and IEEE802.11i, a rekeying message will be sent around every 10000 packets to request for a new key [3].

References

[1] Kanter, I., Kinzel, W. and Kanter, E.: *Secure exchange of information by synchronisation of neural networks* Europhysics Letters **57** (1), pp, 141-147 (2002)

[2] Moskowitz, R.: *WLAN Testing Reports, PSK as the Key Establishment Method*, ICSA Labs, 2003

[3] Walker, J.: *802.11 Security Series, PartII: The Temporal Integrity Protocol (TKIP)*, Network Security Intel Corporation, 2003

Security Challenges of Location-Aware Mobile Business

Emin Islam Tatli, Dirk Stegemann, Stefan Lucks

Department of Computer Science, University of Mannheim
{tatli,stegemann,lucks}@th.informatik.uni-mannheim.de

In addition to mobility, the ability of context awareness and especially location awareness has enhanced mobile businesses to support context-aware services. Today, many different kinds of context-aware services, ranging from finding nearby restaurants [FR] to sending ambulances to people in emergency [LP], have already taken their places in the business.

The m-business research group at the University of Mannheim [MB04] aims at building a generic framework that is able to execute any kind of context-aware service. Our talk presents the security challenges of this mobile business framework with special focus on location as a context property.

Our analysis shows that, in addition to privacy and confidentiality, other security challenges, especially anonymous and unlinkable services, usability with security, integrity and authenticity of services, secure payment, fair exchange, location-based spamming, rogue access points and forged GPS-signals would directly affect the user acceptance of the m-business framework.

Having specified the challenges and possible solutions, our next step is to design an open and flexible security architecture that can be integrated into the application framework.

References

[MB04] The Mobile Business Research Group
URL: http://www.m-business.uni-mannheim.de

[LP] Locating people in emergency
URL: http://www.sintrade.ch

[FR] Location-based services for mobile communities
URL: http://www.mobiloco.de

Secure Group Communication in WLAN Ad-Hoc Networks with Tree Parity Machines

Björn Saballus

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

Most portable customer devices, such as laptops and PDA's, have the ability to communicate via Wireless Local Area Networks (WLAN). These are described in the IEEE 802.11 standard which also allows to set up self-configuring and self- organising ad-hoc networks without a central server.

This work investigates a method to allow secure group communication in ad-hoc networks using symmetric key exchange by Tree Parity Machines (TPMs) [KKK02].

A main problem in secure group communication is the need to establish and distribute a shared, secret key between the members in the group, especially on join- or leave-actions [HD03]. With TPMs, multiparty key exchange is inherently possible based on multiparty synchronisation. A group of TPMs, all sharing one key, can perform a synchronisation with another group of TPMs sharing another key. Once the synchronisation process is finished, all TPMs will share the same key. The suggested chained synchronisation has a runtime-complexity of $O(n)$, with n being the group size. Another concurrent synchronisation has a runtime-complexity of $O(\log(n))$.

This Work-in-Progress presents some preliminary experimental results on the usability of TPMs in secure group communication.

References

[KKK02] Kanter, I., Kinzel, W. and Kanter, E.: *Secure exchange of information by synchronisation of neural networks*, Europhysics Letters **57** (1), pp, 141-147, 2002

[HD03] Hardjono, T. and Dondeti, L.R.: *Multicast and Group Security*, Artech House Inc, 2003