

3. Krypto-Tag – Workshop über Kryptographie Technische Universität Darmstadt

Ralf-Philipp Weinmann (Hg.)
Technische Universität Darmstadt, Fachbereich Informatik
Hochschulstr. 10, D-64289 Darmstadt

15. September 2005



Technical Report No. TI-1/05

Inhaltsverzeichnis

Fault Attacks on Combiners with Memory <i>Frederik Armknecht and Willi Meier</i>	3
Some Thoughts about Block Ciphers and Stream Ciphers <i>Erik Zenner</i>	4
Runners, Starting Lines and Mutual Distances: On the Security of Tree Parity Machine Key Exchange <i>Markus Volkmer and Florian Grewe</i>	5
A Framework for Computer Proofs in Probability Theory for Use in Cryptography <i>Markus Kaiser, Johannes Buchmann, and Tsuyoshi Takagi</i>	6
Hocheffiziente modulare Multiplikation für $\mathbb{GF}(P)$ <i>Rainer Blümel, Ralf Laue und Sorin A. Huss</i>	7
Angriffe auf RC4 <i>Andreas Klein</i>	8
Verifizierbares geheimes Mischen <i>Heiko Stamer</i>	9
Designing Secure Protocol Implementations <i>Philipp A. Baer</i>	10
Improved Boomerang Attack on Eight-Round-Serpent <i>Anne Schwalb</i>	11
Wiedererkennung anonymer Knoten <i>Stefan Schlott und Frank Kargl</i>	12
Strengthening the E_0 Keystream Generator against Correlation Attacks and Algebraic Attacks <i>Frederik Armknecht and Matthias Krause and Dirk Stegemann</i>	13
Elektronische Wahlen mit Observer <i>Jörn Schweisgut</i>	14
Kryptographisch t-private Auktionen <i>Nina Moebius</i>	15

Fault Attacks on Combiners with Memory

Frederik Armknecht* and Willi Meier†

* Universität Mannheim † FH Aargau
Germany Switzerland

Fault attacks are powerful cryptanalytic tools that are applicable to many types of cryptosystems. Recently, general techniques have been developed which can be used to attack many standard constructions of stream ciphers based on LFSR's. Some more elaborated methods have been invented to attack RC4. These fault attacks are not applicable in general to combiners with memory.

In this paper, techniques are developed that specifically allow to attack this class of stream ciphers. These methods are expected to work against any LFSR-based construction that uses only a small memory and few input bits in its output function. In particular, efficient attacks are described against the stream cipher E0 used in Bluetooth, either by inducing faults in the memory or in one of its LFSR's. In both cases, the outputs derived from the faulty runs finally allow to describe the secret key by a system of linear equations. Computer simulations showed that inducing 12 faults sufficed in most cases if about 2500 output bits were available. Another specific fault attack is developed against the stream cipher SNOW 2.0, whose output function has a 64-bit memory. Similar to E_0 , the secret key is finally the solution of a system of linear equations. We expect that one fault is enough if about 2^{12} output words are known.

References

- [1] Biham, Granboulan, Nguyen: Impossible Fault Analysis of RC4 and Differential Fault Analysis of RC4, FSE 2005, Springer, 2005.
- [2] Boneh, DeMillo, R.J. Lipton: *On the Importance of Checking Cryptographic Protocols for Faults*, Eurocrypt 1997, LNCS 1233, pp. 37-51, Springer, 1997.
- [3] Biham, Shamir: *Differential fault analysis of secret key cryptosystems*, Crypto 1997, LNCS 1294, pp. 513-525, Springer, 1997.
- [4] Hoch, Shamir: *Fault Analysis of Stream Ciphers*, CHES 2004, LNCS 3156, pp. 240-253, Springer, 2004.

Some Thoughts about Block Ciphers and Stream Ciphers

Erik Zenner

Cryptico A/S
ez@cryptico.com

Block ciphers and stream ciphers are well-known concepts in cryptography. They are encountered in almost all major textbooks, and they form the basis of all known symmetric encryption algorithms. Nonetheless, many misconceptions surround these concepts. Adi Shamir announced in early 2004 that stream ciphers were dead, just to revoke that statement on the SASC workshop and on Asiacrypt 2004. At the SKEW workshop that was held in May 2005 in Aarhus, it turned out that the specialists in stream cipher cryptography do not even agree on what a stream cipher actually is.

Security-wise, things do not look much better. The common perception is that block ciphers (like AES) are more secure than stream ciphers - but are they? In fact, such a statement is comparing apples with oranges, since block ciphers are not used directly for encryption. Instead, they are used in a mode of operation, which is usually a stream cipher that often turns out to be cryptographically weaker than the dedicated stream ciphers themselves.

In this talk, we attempt to clear up some of the conceptual muddle around block and stream ciphers. We will review some definitions and notions of security, point out the true advantages of block and stream ciphers, and advocate a clear use of terminology.

Runners, Starting Lines and Mutual Distances: On the Security of Tree Parity Machine Key Exchange

Markus Volkmer and Florian Grewe

Hamburg University of Technology, Computer Engineering VI
Schwarzenbergstraße 95, D-21073 Hamburg, Germany

Attacks on key exchange by Tree Parity Machines (TPMs) [1] exist that also employ one or more TPMs (e.g. [2]). An attacker tries to learn the internal state of the interacting parties from observing the publicly communicated outputs of their synchronisation process. The security of the principle has so far only been accessed experimentally in terms of success probabilities of an attacker with respect to the chosen TPM parameters.

This contribution suggests to take a different view on the key exchange and the related attacks. The interacting as well as the attacking TPMs are considered to be runners that start a race at different starting lines chosen at random. Although the finish is determined by the choice of the interacting runners, it is unknown to all the runners. The attacking runner has the disadvantage of being slower than the two interacting runners, because he can only chase them and does not interact. In this unusual race, the starting lines can be chosen freely and neither runner knows the starting line of the other runners. A slower attacking runner can thus win by chance, if he picks an advantageous starting line relative to one of the other two runners. In particular, the initial mutual distances between the runners and the attacking runner determine who will win.

This perspective still leaves one with success probabilities, after all. Yet it allows for fundamental insights in terms of the relation between the initial mutual distances, synchronisation times, success probabilities and thus the discussion of security. Countermeasures against attacks are also motivated: increase the interaction of your runners, slow down the attacking runner or choose close starting lines.

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] Klimov, A., Mityagin, A., and Shamir, A.: *Analysis of neural cryptography*, In Proc. of AsiaCrypt 2002, volume **2501** of LNCS, pages 288–298, Queenstown, New Zealand, December 1-5 2002, Springer Verlag.

A Framework for Computer Proofs in Probability Theory for Use in Cryptography ¹

Markus Kaiser*, Johannes Buchmann*, and Tsuyoshi Takagi**

* Darmstadt University of Technology
Germany

** Future University - Hakodate
Japan

Mathematical proofs are often complex and hard to verify by their readers. Consequently, the application of formal proof systems are a useful approach in the area of verification. We present a framework for computer proofs in probability theory. Therefore we describe formalized probability distributions and fundamental lemmata concerning σ -algebras, probability spaces and conditional probabilities. These are given in the formal language of the formal proof system Isabelle/HOL. Besides we describe an application of the presented formalized probability distributions and fundamental lemmata to cryptography.

Our achievements are a step towards computer verification of cryptographic primitives. They describe a basis for computer verification in probability theory for interactive proof constructions within the formal proof system mentioned above. Computer verification can be applied to further problems in cryptographic research, if the corresponding basic mathematical knowledge is available in a database.

References

- [BR93] M. Bellare and P. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In *proceedings of the First ACM Conference on Computer and Communication Security*, 1993.
- [Hur01] Joe Hurd. *Formal Verification of Probabilistic Algorithms*. PhD thesis, Trinity College University of Cambridge, 2001.
- [Ric03] Stefan Richter. Formalizing Integration theory, with an Application to Probabilistic Algorithms. Diplomarbeit, Technische Universität München, 2003.
- [Sho01] V. Shoup. OAEP Reconsidered. In *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes of Computer Science*, pages 239–259. Springer-Verlag, 2001.

¹This work was partially funded by the German Federal Ministry of Education and Technology (BMBF) in the framework of the Verisoft project under grant 01 IS C38. The responsibility for this article lies with the authors.

Hocheffiziente modulare Multiplikation für $\mathbb{GF}(P)$

Rainer Blümel*, Ralf Laue† und Sorin A. Huss†

* cv cryptovision GmbH † Integrierte Schaltungen und Systeme
Gelsenkirchen TU Darmstadt

Die Leistungsfähigkeit heutiger Public-Key-Systeme beruht hauptsächlich auf der Effizienz der modularen Körper-Multiplikation. Wir stellen einen Algorithmus für $\mathbb{GF}(P)$ mit nur $n^2 + 7n$ Wort-Multiplikationen vor.

Die grundlegende Idee ist von Karatsuba abgeleitet: Je zwei Wort-Multiplikationen werden zu einer Wort-Multiplikation zusammengefasst, allerdings ohne Einsatz von Rekursion. Die beschleunigte Multiplikationsformel ermöglicht es, eine Mehr-Wort-Multiplikation mit nur $\frac{n \cdot (n+1)}{2}$ Wort-Multiplikationen zu berechnen.

Die Reduktion lässt sich auch als Multiplikation darstellen: $0 \leq X \odot Y \ominus P \odot Z < P$. So kann die beschleunigte Multiplikation auch für die Reduktionsphase eingesetzt werden. Sortiert man die Terme in Reihenfolge absteigender Wertigkeit, ergibt sich $X \odot Y \ominus P \odot Z =$

$$\sum_{i=n-1}^0 \left\{ \sum_{j=0}^{i-1} ((x_i + x_j) \cdot (y_i + y_j) + p_i \cdot z_i - x_i \cdot y_i) \cdot 2^{(i+j)b} \right. \\ \left. - (p_i \cdot z_i - x_i \cdot y_i) 2^{2ib} \right. \\ \left. + \sum_{j=i+1}^{n-1} (p_i \cdot z_i - x_i \cdot y_i - (p_i + p_j) \cdot (z_i + z_j)) \cdot 2^{(i+j)b} \right\}.$$

In jedem Schritt wird nur je ein neues z_i benötigt, welches zu Beginn jedes Schrittes mit einem *Look Ahead*-Mechanismus abgeschätzt wird: Die höchstwertigen Terme des i -ten Schrittes – mit Ausnahme der z_i enthaltenden Teilterme – werden ausgewertet. Aus dem Ergebnis lässt sich z_i mit einer Division durch P errechnen. Als Ersatz für die Division wird eine Multiplikation mit dem Kehrwert der führenden Wörter von P verwendet (ähnlich zu Barrett).

Ungenaue z_i werden durch Korrekturberechnungen ausgeglichen. Geschickte Parameterwahl ermöglicht es, die Genauigkeit soweit zu erhöhen, dass der Aufwand zur Korrektur ignoriert werden kann (Fehlerwahrscheinlichkeit $\approx 10^{-5}$). Für jeden Schritt werden 2 Wort-Multiplikationen für $(p_i \cdot z_i - x_i \cdot y_i)$ und weitere $n - 1$ für die Summen benötigt. Unsere Implementierung benötigt weiterhin 3 Wort-Multiplikationen für die Auswertung der höchstwertigen Terme und 3 für die Multiplikation mit dem Kehrwert. Als Summe ergibt sich die oben erwähnte Komplexität von $n^2 + 7n$.

Angriffe auf RC4

Andreas Klein*

*Arbeitsgruppe Computational Mathematics, Universität Kassel

RC4 ist eine Stromchiffre die 1987 von Ron Rivest erfunden wurde. Die Chiffre ist sehr schnell und wird daher in Anwendungen wie SSL und WEP eingesetzt. Damit gehört sie zu den populärsten Stromchiffren. Der Algorithmus wurde als Firmengeheimnis von RSA Data Security Inc. behandelt. Die Beschreibung des Algorithmus wurde erst 1994 anonym auf der Mailing-Liste Cypherpunks veröffentlicht.

Die Struktur des Verfahrens ist recht einfach. Der Algorithmus arbeitet mit einer Permutation S_0, \dots, S_{255} der Zahlen von 0 bis 255. In jedem Schritt wird auf folgende Weise eine Pseudozufallszahl erzeugt.

$$\begin{aligned} i &= (i + 1) \pmod{256} \\ j &= (j + S_i) \pmod{256} \\ &\text{vertausche } S_i \text{ und } S_j \\ t &= (S_i + S_j) \pmod{256} \\ &\text{gebe } S_t \text{ aus} \end{aligned}$$

In meinem Vortrag möchte ich eine Schwäche der von RC4 erzeugten Pseudozufallsfolge vorstellen und zeigen wie diese zu einem Angriff ausgenutzt werden kann.

In Gegensatz zur bekannten FMS-Attacke [1] braucht der neue Angriff keine schwachen Schlüssel. Daher reichen jetzt bereits etwa 25000 statt 1000000 abgefangener Sitzungen zur Analyse aus. Mit der neuen Technik ist es auch dann möglich den Schlüssel zu rekonstruieren, wenn die ersten 256 Byte des Schlüsselstroms für eine Analyse nicht zu Verfügung stehen.

Literatur

- [1] S. Fluhrer, I. Mantin, and A. Shamir. Weakness in the Key Scheduling Algorithm of RC4. In *Selected areas in cryptography*, volume 2259 of *LNCS*, pages 1–24, Berlin, 2001. Springer.

Verifizierbares geheimes Mischen

Heiko Stamer

Universität Kassel, Fachbereich Mathematik/Informatik
Heinrich-Plett-Straße 40, D-34132 Kassel
stamer@theory.informatik.uni-kassel.de
<http://www.theory.informatik.uni-kassel.de/~stamer>

Geheimes Mischen hat vielfältige Anwendungsmöglichkeiten. Beispielsweise ist es ein wichtiger Bestandteil von sicheren Mix-Netzen, welche wiederum für elektronische Wahlen oder Online-Auktionen benötigt werden. Weitere Einsatzgebiete sind Anonymisierungsdienste, datenschutzfreundliche Statistikabfragen sowie elektronische Bezahlssysteme. Fast alle der genannten Anwendungen erfordern jedoch neben einer unbedingten Geheimnisbewahrung der Permutation zusätzlich deren Verifizierbarkeit, d. h. unter vernünftigen kryptographischen Annahmen soll die Korrektheit des Mischens „beweisbar“ sein. Seit kurzem wird dieser Bereich intensiv untersucht [Ne01, Gr03, Fu04, Wi05, Gr05]. Infolgedessen gibt es mittlerweile auch effiziente und praxistaugliche Protokolle.

Der Vortrag stellt kurz die bekannten Techniken für verifizierbares geheimes Mischen gegenüber und vergleicht sie hinsichtlich ihrer Berechnungs- und Kommunikationskomplexität. Weiterhin werden die Grundlagen sowie die praktische Umsetzung eines aktuellen Verfahrens [Gr05] diskutiert.

Literatur

- [Fu04] J. Furukawa. Efficient, Verifiable Shuffle Decryption and Its Requirement of Unlinkability. In *Public Key Cryptography - PKC 2004 Proceedings*, Lecture Notes in Computer Science 2947, pp. 319–332, 2004.
- [Gr03] J. Groth. A Verifiable Secret Shuffle of Homomorphic Encryptions. In *Public Key Cryptography - PKC 2003: Proceedings*, Lecture Notes in Computer Science 2567, pp. 145–160, 2003.
- [Gr05] J. Groth. A Verifiable Secret Shuffle of Homomorphic Encryptions. Cryptology ePrint Archive, Report 2005/246.
- [Ne01] C.A. Neff. A Verifiable Secret Shuffle and its Application to E-Voting. 8th ACM Conference on Computer and Communications Security, pp. 116–125, 2001.
- [Wi05] D. Wikström. A Sender Verifiable Mix-Net and a New Proof of a Shuffle. Cryptology ePrint Archive, Report 2005/137.

Designing Secure Protocol Implementations

Philipp A. Baer*

*University of Kassel, FB 16, FG Distributed Systems, Germany

Security network protocols specified in only a formal language normally cannot be translated into software right away, mostly due to missing implementation details. Furthermore, a naïve implementation is often error-prone because of the variety of environmental configurations. We propose the *interactive assisted modeling* (IAM) architecture for security protocol specification. Its objective is to improve the quality of protocol implementations and portability.

The IAM architecture offers detail level-filtered modeling, support for group communication, and optimized code generation. An abstract and platform-independent *representation language* is introduced to guarantee portability of protocol specifications.

The AIM modeling interface provides an abstract view on the communication scenario and the environment. It furthermore supports specification of environmental properties such as characteristics of the communication media. Third-party tools for protocol and security analysis will also be supported. Projects like [1] follow a similar approach.

Cryptographic or communication primitives and common networking parameters are directly mapped into our representation language. It is similar to MuCAPSL [2] which is primarily targeted towards specification of multicast authentication protocols. The objective of MuCAPSL is protocol analysis whereas our language was explicitly designed for automatic code generation.

In another transformation process a protocol specification is translated into intermediate or native code. The intermediate code target is similar to Microsoft's *Intermediate Language* (MSIL). An optimized interpreter executes this code (*communication sandboxing*).

Literatur

- [1] E. Saul, A.C.M. Hutchison. SPEAR II: The Security Protocol Engineering and Analysis Resource. 2nd Annual South African Telecommunications, Networks and Applications Conference, 1999.
- [2] J. Millen, G. Denker. CAPSL and MuCAPSL. Journal of Telecommunications and Information Technology 4, 2002.

Improved Boomerang Attack on Eight-Round-Serpent

Anne Schwalb

Mathematisches Institut
Justus-Liebig-Universität Giessen, Germany
a.schwalb@gmx.de

One of the five AES finalists is the block cipher Serpent (see [ABK98]) which is a 32-round SP-network.

In the beginning of this talk a short introduction to this cipher is given. Then the boomerang attack on 8-round-Serpent is presented as an extension of the differential cryptanalysis. The boomerang attack is a key-recovery attack which needs chosen-plaintexts and adaptive-chosen-ciphertexts.

Both, the differential cryptanalysis and the boomerang attack, use characteristics. Since for the efficiency of the attack it is important that the used characteristics have a probability as high as possible, an introduction to differential characteristics is also given as a component of the boomerang attack.

As a novel contribution, the attack on the 8-round-Serpent as given in [KKS00] is improved by using a characteristic with a probability higher than the one used there. This better characteristic is taken from [BDK01].

The attack presented in [KKS00] requires 2^{128} chosen plaintexts and ciphertexts (which means the entire codebook), 2^{133} bytes of memory and time equivalent to approximately 2^{163} 8-round-Serpent-encryptions. The new attack which uses the better characteristic from [BDK01] also works with the entire codebook, which means it also requires 2^{128} chosen plaintexts and ciphertexts and 2^{133} bytes of memory but it decreases the required time to approximately 2^{159} 8-round-Serpent-encryptions. To the best of our knowledge this new attack is the best published attack on 8-round-Serpent.

References

- [ABK98] R. J. Anderson, E. Biham, L. R. Knudsen. Serpent: A Proposal for the Advanced Encryption Standard. *NIST AES Proposal*, 1998.
- [KKS00] T. Kohno, J. Kelsey, B. Schneier. Preliminary Cryptanalysis of Reduced-Round Serpent. *Third AES Candidate Conference*, 2000.
- [BDK01] E. Biham, O. Dunkelman, N. Keller. The Rectangle Attack - Rectangling the Serpent. *Proceedings of EUROCRYPT 2001, Advances in Cryptology*, LNCS 2045, Springer 2001, S. 340-357.

Wiedererkennung anonymer Knoten

Stefan Schlott und Frank Kargl

Universität Ulm {stefan.schlott|frank.kargl}@uni-ulm.de

Die Privatsphäre ist ein wichtiger Aspekt des Ubiquitous Computings. Um das Erstellen von Personenprofilen zu verhindern, werden die Knoten solcher Netze anonymisiert. Dies kann beispielsweise über ständig wechselnde Identitäten oder Kommunikation über Mixkaskaden geschehen. In bestimmten Situationen soll es jedoch möglich sein, einen Knoten wiederzuerkennen. Beim erfolgreichen Wiedererkennen soll ein Knoten auf entsprechende gespeicherte Werte (z.B. der letzte Sitzungsschlüssel) zurückgreifen können; falls jedoch keine passende Kommunikationsbeziehung besteht, soll durch den Erkennungsversuch keiner der Knoten zusätzliche Informationen erlangen. Das Abhören der Kommunikation darf ebenfalls keine Informationen preisgeben.

Wiedererkennung anhand des ausgetauschten Schlüssels: Bei einer ersten Verbindung werden ein gemeinsamer Schlüssel k sowie ein Token T (String) vereinbart. Will A nun B wiedererkennen, so sendet A zunächst eine Nonce N_A . B sendet nun für alle gespeicherten Verbindungen $E_k(T, N_A, N_B)$. A versucht nun, jedes der Pakete mit allen ihm bekannten Schlüsseln zu dechiffrieren. Erhält er hierbei T und N_A , so war die Erkennung erfolgreich. Um die Suche nach dem richtigen Schlüssel bei A einzugrenzen, kann zusätzlich ein Index ID übertragen werden; der Indexraum darf aber nicht so groß sein, daß anhand von ID eine Identifizierung möglich ist. Bei Verwendung des Indexes ist die Reihenfolge, in der B seine Pakete überträgt, zufällig zu wählen; sonst wäre eine u.U. Identifizierung anhand der ID-Reihenfolge möglich. Nach einer erfolgreichen Wiedererkennung wird ein neues ID vereinbart.

Wiedererkennung mit Hash Chains: Bei der ersten Verbindung wird neben dem Schlüssel k der Start von zwei Hashchains h_A, h_B ausgetauscht. Zum Wiedererkennen sendet A an B eine Nonce N_A . B sendet an A $N_B, H^k(h_B, N_A, N_B)$ (mit H^k dem k -ten Element der Hashchain und $k = k - 1$ bei jedem Versuch), k, N_B . A berechnet nun den k ten Wert von jedem gespeicherten h_B ; stimmt dieser mit dem übertragenen Wert überein, war die Erkennung erfolgreich. A sendet nun seinerseits $H^j(h_A, N_A, N_B)$ (mit $j = j - 1$ bei jedem Versuch), B erkennt A nach dem identischen Verfahren.

Strengthening the E_0 Keystream Generator against Correlation Attacks and Algebraic Attacks

Frederik Armknecht and Matthias Krause and Dirk Stegemann

University of Mannheim
Germany

Stream ciphers are widely used for online-encryption of arbitrarily long data. An important class of stream ciphers are combiners with memory, with the E_0 generator from the Bluetooth standard for wireless communication [2] being their most prominent example.

E_0 consists of 4 driving devices, a finite state machine (FSM) \mathcal{C} with a 4 bit state, an output function f and a memory update function δ . At each clock, one keystream bit z_t is produced from the output $X_t \in \{0, 1\}^4$ of the driving devices and the current state $C_t \in \{0, 1\}^4$ of the FSM according to $z_t = f(C_t, X_t)$, and the state of the FSM is updated to $C_{t+1} := \delta(C_t, X_t)$.

So far, the best publicly known attacks against combiners with memory are correlation attacks [4] and algebraic attacks [1]. Correlation attacks exploit linear equations $L(X_t, \dots, X_{t+r-1}, z_t, \dots, z_{t+r-1}) = 0$ that are true with some probability $\frac{1}{2} + \lambda$ with $\lambda \neq 0$. Algebraic attacks use valid non-linear equations of preferably low degree to describe the secret key by a system of equations.

We show how to avert a special class of correlation attacks [3] that is currently the most effective against E_0 and introduce a general design principle which guarantees that all valid equations have a degree not smaller than a certain lower bound. Combining these results, we construct a slightly modified version of E_0 with significantly improved resistance against correlation attacks and algebraic attacks.

References

- [1] Armknecht, Krause: *Algebraic Attacks on Combiners with Memory*, Crypto 2003.
- [2] Bluetooth specification Version 1.1. <http://www.bluetooth.com>
- [3] Lu, Vaudenay: *Faster Correlation Attack on the Bluetooth Keystream Generator*, Crypto 2004.
- [4] Salmasizadeh, Golić, Dawson, Simpson: *A Systematic Procedure for Applying Fast Correlation Attacks to Combiners with Memory*, SAC 1997.

Elektronische Wahlen mit Observer

Jörn Schweisgut

Mathematisches Institut,
Justus-Liebig-Universität Giessen
Joern.Schweisgut@math.uni-giessen.de

Im Herbst 2005 wird in Estland die Stimmabgabe zu den Kommunalwahlen über Internet möglich sein. Die Entscheidung des estnischen Parlamentes verdeutlicht den immer breiter werdenden Trend zu elektronischen Wahlen.

Ein großes Problem elektronischer Wahlen ist die Unüberprüfbarkeit (receipt-freeness). Selbst wenn ein Wähler mit einem Angreifer kooperiert, darf es ihm nicht möglich sein, beweisen zu können, wie er gewählt hat, da er sonst erpressbar oder bestechlich wird.

Das System, das bisher die Unüberprüfbarkeit (am besten) realisiert hat, ist das von Hirt und Sako [HS00]. Es hat sich jedoch herausgestellt, dass hier ein Angreifer einen Wähler zwingen kann zufällig oder gar nicht zu wählen.

In diesem Vortrag wird zunächst kurz ein Wahlsystem erläutert, das zur Stimmabgabe eine manipulationssichere Hardware, einen Observer, verwendet, der Unüberprüfbarkeit wie in [HS00] gewährleistet, jedoch effizienter ist. Das System wurde 2001 von Magkos et al. vorgestellt [MBC01].

Innerhalb des Protokolls wird ein honest-verifier Zero-Knowledge Beweis vom Observer gegenüber dem Wähler durchgeführt. Im Gegensatz zur Meinung der Autoren ist dieser Beweis übertragbar, wenn der Wähler *eine* Challenge wählt, die der Angreifer vorher festgelegt hat.

Im Rahmen des Vortrags wird daher beschrieben, wie dieses Problem mittels eines Designated-Verifier Beweises (siehe [JSI96]) gelöst werden kann.

Literatur

- [HS00] Martin Hirt, Kazue Sako. Efficient Receipt-Free Voting Based on Homomorphic Encryption. Band 1807 der LNCS, Springer-Verlag, Berlin. *Eurocrypt 2000 - Advances in Cryptology*, Seiten 539-554, 2000.
- [JSI96] Markus Jakobsson, Kazue Sako, Russel Impagliazzo. Designated-verifier proofs and their applications. Band 1070 der LNCS, Springer-Verlag, Berlin. *Eurocrypt 1996 - Advances in Cryptology*, Seiten 143-154, 1996.
- [MBC01] Emmanouil Magkos and Mike Burmester and Vassilis Chrissikopoulos. Receipt-freeness in Large-scale Elections without Untappable Channels. In B. Schmid et al., editor. *First IFIP Conference on E-Commerce, E-Business, E-Government (IEEE)*, Seiten 683-694, 2002.

Kryptographisch t -private Auktionen

Nina Moebius

Universität zu Lübeck

`nina.moebius@informatik.uni-luebeck.de`

Bei einer Auktion haben die Bieter, die ein Produkt ersteigern wollen, und der Verkäufer des Artikels gegensätzliche Interessen. Ein Bieter ist daran interessiert, das Produkt für einen möglichst geringen Preis zu erhalten, während der Verkäufer seinen Erlös maximieren möchte. Eine Gemeinsamkeit ist jedoch, dass beide Parteien sich einen für sie fairen Verlauf der Auktion wünschen. Das heißt, die Preisfindung muss so gestaltet sein, dass jeder Bieter den für ihn wahren Wert des Produktes bietet.

Das in dieser Arbeit präsentierte Protokoll fördert die Fairness einer Auktion dadurch, dass kein Wissen im kryptographischen Sinn über die Gebote der Bieter preisgegeben wird. Nach dem Ende der Auktion werden lediglich der Höchstbietende und sein Gebot veröffentlicht.

Dies gilt auch, wenn sich t Angreifer zu einer Koalition zusammenschließen und gemeinsam versuchen Wissen zu gewinnen. Die von uns betrachteten Angreifer sind passiv, d.h. sie folgen der Protokollspezifikation. Weiterhin ist es möglich, das Ergebnis der Auktion zu verifizieren.

Wir erweitern das in [NPS99] entwickelte 1-private Auktionsprotokoll unter Verwendung von Yaos garbled circuits ([Y82]).

Dabei stützen wir uns auf den in [HJS05, S05] vorgestellten Auktionsmechanismus. Dieser ist informationstheoretisch sicher, benötigt aber eine sehr große Zahl an zufälligen Bits, sodass eine praktische Umsetzung nicht möglich ist. In unserem Protokoll wird durch Zuhilfenahme von kryptographischen Primitiven die Anzahl der Zufallsbits eingeschränkt, sodass eine Implementierung möglich ist.

Literatur

- [HJS05] M. Hinkelmann, A. Jakoby, P. Stechert, *Dynamic t -Private Auctions*, Technical Report SIIM-TR-A-05-11, Universität zu Lübeck, 2005
- [NPS99] M. Naor, B. Pinkas, R. Sumner, *Privacy Preserving Auctions and Mechanism Design*, 1st ACM Conference on Electronic Commerce, pp. 129–139, 1999.
- [S05] P. Stechert, *Dynamic Private Auctions*, Diplomarbeit, Institut für Theoretische Informatik, Universität zu Lübeck, 2005
- [Y82] A. C. Yao. *Protocols for secure computations*, 23rd FOCS, pp. 160–164, 1982.