

Book of Abstracts

# 6. KRYPTOTAG

Workshop der Fachgruppe Kryptografie  
in der Gesellschaft für Informatik

Ammar Alkassar, Michael Backes (Hrsg.)

*Sirrix* AG  
security technologies



Sirrix AG security technologies,  
Im Stadtwald, Geb. D3 2,  
66123 Saarbrücken

Sirrix Technical Report 07/342

# Inhaltsverzeichnis

Automated derivation of public key authenticity using a formal model of certificate based security infrastructures <i>Thomas Wölfel</i> .....	3
Untersuchung von NTRUsign <i>Richard Lindner</i> .....	4
A Cryptographic model for branching time security properties – the case of contract signing <i>Ralf Küsters</i> .....	5
Concealed data aggregation in wireless sensor networks <i>Frederik Armknecht</i> .....	6
Netzwerksicherheit: Mit Kryptographie gegen DDoS <i>Ulrich Kühn und Roger Karrer</i> .....	7
Neuste Ergebnisse des SASC Stream Cipher Workshops/eStream <i>Dirk Stegemann</i> .....	8
Sicherheit der Random-Oracle-Methodik: Ein neuer Ansatz <i>Björn Fay</i> .....	9
Beweisbare Sicherheit in der physikalischen Welt <i>Sebastian Faust</i> .....	10

# Automated derivation of public key authenticity using a formal model of certificate based security infrastructures

Thomas Wöflf

University of Regensburg

The authenticity of public keys is a well-known prerequisite for the applicability of asymmetric cryptography. Formal models of public key infrastructures (PKI) provide a theoretical foundation for the validation of public key certificates with the goal to derive the required key authenticity. A significant example is Maurer's PKI model [2]. However, existing models neglect validity periods and revocations of public key certificates.

This work presents the formal model [1] which covers these temporal aspects. It allows the derivation of public key authenticity for a certain point in time. Additionally, it enables the authentication of attributes different from public keys, such as biometric reference templates, access privileges or liability commitments.

The core of the model consists of eight axioms formulated in first order logic. It takes the perspective of the user Alice who represents her knowledge about digital certificates by means of two logical statements. After this, Alice verifies if public key (or attribute) authenticity is a logical consequence of the completion [3] of her knowledge and the model's axioms.

Because of the complexity of the modeled scenarios, a manual derivation can be long and time consuming. Therefore, a PROLOG program is presented as an automated derivation method. It can be used in an interactive way (using e.g. SWI-PROLOG [4]) or it can be encapsulated in software and serve as module for the decision about public key (or attribute) authenticity. The latter has the advantage that soundness, completeness and termination of the logic program are formally shown which are crucial aspects for the software system or a cryptographic algorithm relying on the decision about authenticity.

Another task of the program is the detection of revocation cycles. Consider the following paradox situation: A revocation  $r$  for digital certificate  $c$  exists which is used for the authentication or the authorization of the revocation  $r$ . It cannot be decided if either  $c$  or  $r$  is valid. For example, the validity of  $r$  implies the invalidity of  $c$  which implies the invalidity of  $r$ . The logic program detects these revocation cycles and delivers a warning.

All in all, the formal model and the logic program can be used for the authentication of public keys and other attributes. This allows the reliable application of asymmetric cryptographic methods.

## References

- [1] T. Wöflf, Formale Modellierung von Authentifizierungs- und Autorisierungsinfrastrukturen, Deutscher Universitäts-Verlag, 2006.
- [2] U. Maurer, Modelling a public-key infrastructure, in: E. Bertino (Ed.), Proceedings of 1996 European Symposium on Research in Computer Security (ESORICS96), no. 1146 in Lecture Notes in Computer Science, Springer, 1996, pp. 325–350.
- [3] U. Nilsson, J. Maluszynski, Logic, Programming and PROLOG, 2nd Edition, John Wiley and Sons, 2000.
- [4] <http://www.swi-prolog.org/>

# Untersuchung von NTRUsign

Richard Lindner\*

\* Technische Universität Darmstadt  
Kryptographie und Computeralgebra  
Hochschulstr. 10, 64289 Darmstadt

Das neue Signaturverfahren NTRUsign[1] basierend auf NTRU[3], dem bekanntesten gitterbasierten Public-Key Verfahren von der gleichnamigen Firma aus Amerika, wurde in der Diplomarbeit „Current Attacks on NTRU“ kritisch unter die Lupe genommen und auf Schwächen geprüft. Dabei geht es insbesondere um 4 Angriffsarten, die bei der NTRUsign Variante mit Störung (engl. perturbations) beachtet werden müssen. Die Variante von NTRUsign ohne Störungen wurde ja sowohl von NTRU selber[1], als auch etwas solider von Nguyen und Regev als sehr unsicher entlarvt[5].

In der Diplomarbeit ging es hauptsächlich darum einen Algorithmus der 'sichere' Parametervorgaben für NTRUsign bestimmt[2] zu prüfen. Dabei sind einige behebbare Mängel aufgefallen. Und diese werden zusammen mit einem überraschenden und nicht so leicht behebbaren Mangel vorgestellt.

## Literatur

- [1] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. NTRUsign: Digital signatures using the NTRU lattice. *Lecture Notes in Computer Science*, 2612:122–140, 2003.
- [2] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. Performance improvements and a baseline parameter generation algorithm for NTRUsign. <http://grouper.ieee.org/groups/1363/lattPK/submissions.html>, 2005.
- [3] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Buhler [4], pages 267–288.
- [4] Joe P. Buhler, editor. *Algorithmic Number Theory, ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*. Springer-Verlag, 1998.
- [5] Phong Q. Nguyen. A note on the security of NTRUsign. Cryptology ePrint Archive, Report 2006/387, 2006. <http://eprint.iacr.org/>.

# A Cryptographic Model for Branching Time Security Properties – the Case of Contract Signing Protocols

Ralf Küsters

ETH Zürich

`ralf.kuesters@inf.ethz.ch`

Some cryptographic tasks, such as contract signing and other related tasks, need to ensure complex, branching time security properties. When defining such properties one needs to deal with subtle problems regarding the scheduling of non-deterministic decisions, the delivery of messages sent on resilient (non-adversarially controlled) channels, fair executions (executions where no party, both honest and dishonest, is unreasonably precluded to perform its actions), and defining strategies of adversaries against all possible non-deterministic choices of parties and arbitrary delivery of messages via resilient channels. These problems are typically not, or not all, addressed in cryptographic models and these models therefore do not suffice to formalize branching time properties, such as those required of contract signing protocols.

In this talk, a cryptographic model that deals with all of the above problems is proposed. One central feature of this model is a general definition of fair scheduling which not only formalizes fair scheduling of resilient channels but also fair scheduling of actions of honest and dishonest principals. Based on this model and the notion of fair scheduling, a definition of a prominent branching time property of contract signing protocols, namely balance, is provided, along with the first cryptographic proof that the Asokan-Shoup-Waidner two-party contract signing protocol is balanced. The cryptographic models and notions proposed here provide a basis for relating cryptographic and formal definitions of branching time security properties.

Joint work with Veronique Cortier and Bogdan Warinschi.

# Netzwerksicherheit: Mit Kryptographie gegen DDoS

Roger Karrer und Ulrich Kühn  
Deutsche Telekom Laboratories  
Technische Universität Berlin  
`roger.karrer@telekom.de, ukuehn@acm.org`

Distributed Denial of Service (DDoS) – diese Art von Angriffen stellt im Internet ein großes Problem für ISPs und Serverbetreiber dar. Diese Angriffe existieren in einer Reihe von Varianten, z.B. kann man nach dem Angriffsziel unterscheiden: Endsysteme oder Netzwerke. So unterschiedlich die Angriffsziele, so unterschiedlich sind auch die nötigen Verteidigungsstrategien.

Hier betrachten wir den Fall von DDoS-Angriffen auf die Bandbreite im Zugangsnetz von Rechnern. Typischerweise schickt dabei eine große Zahl von *Bots* gleichzeitig und koordiniert Daten an einen Server, so dass letztlich legitime Anfragen nicht mehr durchkommen. Diese Art von Angriffen führt in der Praxis zu erheblichen Schäden.

In diesem Vortrag befassen wir uns mit der Frage, wie man dieses Problem angehen kann, und wie kryptographische Methoden dabei helfen können. Die Herausforderung besteht hier darin, dass Netzwerkelemente die Pakete des Datenstroms weiterleiten, während das Endsystem über die Legitimität urteilen kann. Auf der anderen Seite besitzen Netzelemente aber keine Möglichkeit der Unterscheidung von legitimen und unerwünschten Daten, während ein Endsystem keine Chance mehr hat, unerwünschten Datenverkehr und die dadurch entstehenden Engpässe zu verhindern.

Wir werden hier einen Architektur-Ansatz aufzeigen und die zugehörigen Protokolle beschreiben, mit denen diese Herausforderung gelöst werden kann. Der Ansatz vereint dabei Sicherheit gegen Angriffe, Effizienz und auch Anreize zum Einsatz. Die zentrale Idee ist, dass legitimer Datenverkehr durch den Sender mit einer kryptographischen Marke versehen wird. Diese Marke kann effizient durch ein neuartiges Netzelement "*Gate*" an geeigneter Stelle im Netzwerk überprüft werden kann. Aufbauend auf dieser Prüfung kann dann eine Entscheidung zur Ausfilterung getroffen werden.

Darüber hinaus zeigen wir, wie ein effizienter und sicherer Informationsaustausch in dem sich ergebenden verteilten System realisiert werden kann. Bei den verwendeten Kommunikationsprotokollen ergeben sich eine Reihe von Herausforderungen, bei deren Lösung kryptographische Methoden zum Einsatz kommen: Sicheres Schlüsselmanagement, effiziente kryptographische Markierung, und nicht zuletzt ein Schlüsseltransport, der mit hoher Wahrscheinlichkeit menschliche Nutzer von Bots unterscheiden kann.

# Sicherheit der Random-Oracle-Methodik: Ein neuer Ansatz

Björn Fay\*

\* Justus-Liebig-Universität Gießen  
Mathematisches Institut  
Arndstraße 2  
35392 Gießen

Spätestens seit dem Artikel [BR93] von Bellare und Rogaway gehört die Random-Oracle-Methodik zu den Standard-Beweistechniken in der Kryptologie. Dabei behandelt man während des Sicherheitsbeweises eines Protokolls auftretende Hashfunktionen als wären sie echte Zufallsfunktionen, sogenannte Random-Oracles oder kurz RO. Man hofft dabei, dass beim Austausch des Random-Oracles durch eine Hashfunktion der Sicherheitsbeweis intakt bleibt. Hierzu gab es allerdings schon mehrere Gegenbeispiele, u. a. der Artikel [MRH04] von Maurer, Renner und Holenstein, der mit Hilfe eines allgemeinen Modells zeigte, dass sich ein Random-Oracle im Allgemeinen nicht durch eine Hashfunktion ersetzen lässt. Da die Gegenbeispiele sehr künstlich sind, geht man auch weiterhin davon aus, dass bei Anwendung der Random-Oracle-Methodik auf „normale“ Protokolle diese sicher sind, auch wenn dies kein Sicherheitsbeweis im Standard-Modell ist.

Protokolle bei denen die Random-Oracle-Methodik häufig benutzt wird, sind z. B. digitale Signaturen. Oft wird dabei erst ein Hashwert von der zu signierenden Nachricht gebildet und dann dieser Hashwert anstatt der ganzen Nachricht signiert, sogenanntes „hash & sign“.

Es gibt bisher allerdings keine allgemeinen Bedingungen unter denen sich die Random-Oracle-Methodik sicher anwenden lässt. Mittels einer neuen Art von Hashfunktionen, den unvorhersehbaren Hashfunktionen (für eine genaue Definition fehlt hier leider der Platz), lässt sich das zumindest ein wenig ändern. Es ist allerdings noch unklar, ob sich solche Hashfunktionen durch Standard-Annahmen konstruieren lassen, man die Existenz einfach annehmen muss oder vielleicht solche Hashfunktionen gar nicht existieren können.

Bei diesen neuen Hashfunktionen hat man auf den Hashwert nicht mehr Einfluss als auf den Rückgabewert eines Random-Oracles. D. h. für einen Algorithmus  $A$ , der Urbilder für die Hashfunktion erzeugt, gibt es einen Algorithmus  $B$ , der Urbilder für das Random-Oracle erzeugen kann, so dass es einem dritten Algorithmus  $D$  nicht möglich ist, zwischen den beiden Ausgaben zu unterscheiden, auch wenn er noch weitere (genau spezifizierte) Zusatzinformationen hat.

Es lässt sich damit eine Bedingung an ein „hash & sign“-Protokoll stellen unter der das Protokoll mit einer unvorhersehbaren Hashfunktion unter einem Angriff ohne Nachrichten nicht existentiell fälschbar ist, wenn das Protokoll mit einem Random-Oracle unter dem gleichen Angriff nicht existentiell fälschbar ist. Für Angriffe mit gewählten Nachrichten lässt sich eine solche Aussage noch nicht treffen. Allerdings lassen die bisherigen Ergebnisse hoffen, dass auch dies im Bereich des Möglichen liegen könnte. Evtl. lassen sich die Ergebnisse auch auf andere Protokolle anwenden.

## Literatur

- [BR93] Mihir Bellare, Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM Conference on Computer and Communications Security*, S. 62–73, 1993.
- [MRH04] Ueli M. Maurer, Renato Renner, Clemens Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In *TCC 2004, Proceedings*, Band 2951 von *Lecture Notes in Computer Science*, S. 21–39, Springer, 2004.

# Beweisbare Sicherheit in der physikalischen Welt

Sebastian Faust  
KU Leuven, ESAT/COSIC  
Kateelpark Arenberg 10  
3001 Heverlee

Seit den frühen 80ern beschäftigt sich die Kryptographie mit dem Themengebiet der beweisbaren Sicherheit [GM84, BR93]. Typischerweise wird hierbei zunächst ein allgemeines Angreifermodell definiert unter dem dann Protokolle auf ihre Sicherheitseigenschaften hin formal untersucht werden können. Für den formalen Beweis wird dann gezeigt, dass unter bestimmten Annahmen, z.B. die Schwierigkeit von zahlentheoretischen Problemen, kein effizienter Angreifer auf das Protokoll existieren kann.

Obwohl mittlerweile selbst für komplizierte Protokolle mathematische Sicherheitsbeweise existieren, werden immer häufiger praktische Angriffe auf Implementierungen der beweisbar sicheren Systeme gefunden. Nur sehr selten ist dies in einem Fehler des Sicherheitsbeweises begründet. Weitaus häufiger ist die Ursache für die Anfälligkeit des Systems im Modell zu suchen. Ein grundsätzliches Problem ist hierbei, dass Sicherheitsbeweise gegenwärtig im so genannten Black-Box Modell erbracht werden. Hier wird ein kryptographischer Algorithmus als Black-Box definiert, d.h. ein Angreifer erfährt nur eine Menge an Ein-/Ausgabepaaren, lernt jedoch nichts über interne Zustände während der Verarbeitung. In der Praxis kann ein Angreifer jedoch durchaus durch Beobachtung der physikalischen Welt, z.B. durch Messung des Stromverbrauchs oder des elektromagnetischen Feldes eines Chips, zusätzliche, so genannte Seiten-Kanal, Informationen sammeln. Diese Informationen werden im herkömmlichen Black-Box Modell nicht berücksichtigt, führen jedoch sehr häufig zum vollständigen Verlust der Sicherheit.

In diesem Vortrag wird das Modell von Silvio Micali und Leonid Reyzin [MR04] vorgestellt, das genau an dieser Stelle ansetzt und versucht, die offensichtliche Lücke zwischen Theorie und Praxis zu schließen. Hierzu führen die Autoren ein abstraktes Berechnungsmodell ein, in dem kryptographische Algorithmen durch eine Kombination von abstrakten Turing Maschinen und einer Leakage-Funktion modelliert werden. Erste Resultate zeigen, dass sich die physikalische Welt bereits bei einfachen Ergebnissen deutlich von dem traditionellen Modell unterscheidet. So ist beispielsweise die Äquivalenz von Nicht-Unterscheidbarkeit und Nicht-Vorhersagbarkeit nicht mehr gewährleistet. Abschließend werden wir einige offene Fragen diskutieren, u.a. ob das MR-Modell tatsächlich die Realität abbildet und inwieweit man durch eine Anpassung des Modells für die Praxis relevante Resultate erzielen kann.

## Literatur

- [BR93] Mihir Bellare and Phillip Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. ACM Conference on Computer and Communications Security, pages 62-73, 1993.
- [GM84] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption. J. Comput. Syst. Sci. (28), pages 270-299, 1984.
- [MR04] Silvio Micali and Leonid Reyzin. Physically Observable Cryptography. Theory of Cryptography Conference, TCC 2004. LNCS 2951, pages 278-296, 2004.

# <http://KryptoTag.de>

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

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

## Geplante Kryptotage

**7. Kryptotag** am 9. November 2007 (Einreichung: 2. Oktober 2007, Anmeldung: 1. November 2007). Bonn-Aachen International Center for Information Technology. Kontakt: Michael Nsken und Daniel Loebenberger

## Bisherige Kryptotage

**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 für 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.*