

## Das Institut für Digitale Kommunikationssysteme

An unserem Institut sind 10 – 15 Mitarbeiterinnen und Mitarbeiter beschäftigt. Wir sind aktiv beteiligt an der nationalen und internationalen Normung (DIN und ISO) auf dem Gebiet der kryptographischen Sicherheit. In den vergangenen fünf Jahren haben wir mehr als 10 Forschungs- und Drittmittelprojekte im Auftrag des Landes Nordrhein-Westfalen, der DFG, von Bundesbehörden, der Industrie sowie folgende EU-Projekte im ISIS, Crafts, 4., 5. und 6. Rahmenprogramm durchgeführt:

- WEBSIG (Digital Signatures for Web-Contents)
- ELIAS (Elliptic Curve Cryptography Standards Reference Implementation)
- NEWTRON (New Transponder Generation)
- SCARAB (Smart Card and Agent Enabled Reliable Access to Telecommunication Services)
- GNIUS (GSM Network for Improved Access and Universal Services)
- USB\_CRYPT (Crypto Module with USB-Interface)
- eMAYOR (Electronic and Secure Municipal Administration for European Citizens)

Bisher wurden am Institut über 100 Diplomarbeiten angefertigt und 19 Promotionen abgeschlossen, davon 14 in den vergangenen fünf Jahren. Unsere Forschungs- und Arbeitsgebiete konzentrieren sich auf

## Sicherheit in realzeitorientierten Kommunikationssystemen

- Industrieanwendungen
- Satellitenkommunikation und drahtlose Systeme
- Multimedia-Übertragung und -Verteilung in heterogenen Multicast-Umgebungen
- Kryptographie in RFID-Chips
- Grid-Security
- Sicherer Download eichpflichtiger bzw. kritischer Software

sowie die

## Kombination von Kanalcodierung und Kryptographie

## Sicherheit in realzeit- und multimedia-orientierten Kommunikationssystemen

Während der Gesichtspunkt der Vertraulichkeit durch die Anwendung von Verschlüsselungsverfahren weitgehend gelöst ist, beschäftigen wir uns besonders mit dem Nachweis des Ursprungs der Daten (Authentikation) bei der Übertragung in Hochgeschwindigkeitsnetzen, für realzeitorientierte Anwendungen und die Informationsverteilung in Broadcast- und Multicastumgebungen. Dazu gehören unter anderem multimediale und industrielle Anwendungen. Die Überprüfung der Vertrauenswürdigkeit erfolgt während des Sendens bzw. des Empfangs der Daten, sodass sie ohne wesentliche Verzögerung weiterverarbeitet oder ausgegeben werden können. Wichtig ist für uns auch die Untersuchung der Auswirkungen der Sicherheitsmechanismen auf die Dienstgüte der Übertragung (Quality of Service), z.B. auf Verzögerung, Durchsatz, Fehlerfortpflanzung und (Selbst-)Synchronisation, indem wir uns intensiv mit den Betriebsarten (Modes of Operation) der kryptographischen Algorithmen beschäftigen.

## Industrieanwendungen

In industriellen Anwendungen kommt es besonders auf die Zuverlässigkeit der Informationen an, die an Maschinen oder Steuereinheiten gesendet werden bzw. von Maschinen, Steuereinheiten, Überwachungseinrichtungen und Messgeräten empfangen werden. Als Beispiel für unsere Arbeiten auf diesem Gebiet sollen unsere nationalen und internationalen Projekte dienen, die den Messdatenaustausch mit Energiezählern (Strom und Gas) gesichert haben. Alle Auslese- und Managementkommandos an Messgeräte werden mit digitalen Signaturen versehen, die mit nach dem Signaturgesetz für qualifizierte Signaturen zugelassenen Signaturerstellungseinheiten (Chipkarten) erstellt werden. Ein Rechtekmanagement gewährleistet, dass nur jeweils befugte Stellen Kommandos ausführen dürfen. Dies ist insbesondere auf Grund der Liberalisierung des Energiemarktes und des Energiewirtschaftsgesetzes erforderlich, das zahlreiche Partner auf dem Energiemarkt vorsieht, die je nach ihrer zugeordneten Aufgabe auf bestimmte Funktionen der Messgeräte zugreifen dürfen. Als Beispiel sei das Projekt SELMA genannt ([www.selma.eu](http://www.selma.eu)). Die für Energiemessgeräte erarbeitete Lösung kann leicht auf andere Industrieapplikationen übertragen werden, z.B. auf Pumpen, Waagen, Taxameter, Kassen, Spielautomaten.

Dipl.-Wirt.Inform. Sibylle Hick  
☎ 0271/740-2516    ✉ [sibylle.hick@uni-siegen.de](mailto:sibylle.hick@uni-siegen.de)

## Multimediaübertragung und -verteilung in heterogenen Multicast-Umgebungen

Die multimediale Kommunikationswelt ist durch Heterogenität gekennzeichnet: es gibt viele verschiedene Endgeräte, die sich durch ihre Verarbeitungs- und Darstellungsmöglichkeiten voneinander unterscheiden, sowie fixe und mobile Netzzugänge, die stark durch Übertragungsraten und -qualitäten voneinander abweichen. Es kann nicht für jeden Gerätetyp und aktuellen Netzzustand unterschiedliche Versionen des von der Quelle erzeugten Datenstroms geben! Neue hierarchische Audio- und Videokompressionsverfahren liefern die Basis, um Lösungen für dieses Problem zu entwickeln. Unsere Forschungsaktivitäten auf diesem Gebiet beschäftigen sich mit dem Problem, die Möglichkeiten, die moderne Quellkompressionsverfahren bieten, für mobile, heterogene Geräte zu nutzen. Dabei werden die (mobilen) Geräte dynamisch je nach Darstellungskapazität und aktueller Übertragungssituation – und gewünschter bzw. vertraglich verabredeter Qualitätsstufe – Multicast-Gruppen zugeordnet, für die jeweils ein entsprechender Datenstrom aus dem Quelldatenstrom gefiltert wird. Da nicht mehr Information übertragen wird als das Endgerät tatsächlich verarbeiten oder darstellen kann, erreicht man zudem eine Reduktion der Netzbelastung.

## Security bei VoIP und Multimedia-Übertragung

Weiterhin arbeiten wir an kryptographischen Konzepten, die den hierarchischen Kompressionsverfahren entsprechen. Auch wenn bestimmte Benutzergruppen nur die Information bestimmter Kompressionsstufen erhalten, sollen sie mit nur einem Entschlüsselungsschritt den für sie vorgesehenen Datenstrom in Klartext überführen können. Das Schlüsselmanagement wird für Multicast-Szenarien optimiert.

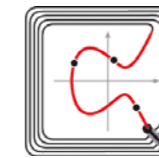
Weitere Arbeiten auf dem Gebiet der Sicherheit von Multimedia-Anwendungen betreffen die Erweiterung des SIP-Protokolls als Sicherheitsmanagementprotokoll, die Einbindung von Sicherheitsdiensten in H.323- sowie SIP-Umgebungen und die Realisierung von SRTP (Secure RTP). Die bei SRTP vorgesehenen Standard-Sicherheitsmechanismen werden um realtime Authentikation auf Basis digitaler Signaturen erweitert.

Dipl.-Ing. Markus Dunte  
☎ 0271/740-2516    ✉ [markus.dunte@uni-siegen.de](mailto:markus.dunte@uni-siegen.de)

## RFID-Kryptographie

Die RFID-Technologie und die damit verbundenen Sicherheitsaspekte sind ein heiß diskutiertes Thema. In den damit verbundenen Forschungsfragen konzentrieren wir uns auf die grundlegenden elektrotechnischen, nachrichtentechnischen und kryptographischen Aspekte: wie viel Energie kann zu einem passiven RFID-Tag über das Speisefeld des Readers drahtlos übertragen werden? Welche Verarbeitungskapazitäten lassen sich auf einem RFID-Chip realisieren? Welche kryptographischen Methoden sind in einen RFID-Tag integrierbar? Welche Sicherheitsstufe kann man damit erreichen? Unter welchen Voraussetzungen können digitale Signaturen generiert werden?

Unsere Forschungsergebnisse haben gezeigt, dass beim Einsatz elliptischer Kurvenkryptographie die Erstellung und Verifikation digitaler Signaturen auch über Distanzen möglich sind, die deutlich größer als der Operationsradius von kontaktlosen Smart Cards sind. Ein besonderes Augenmerk wurde auf die Implementierung digitaler Signaturen



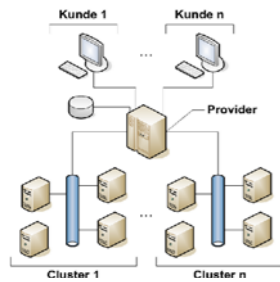
„giving message recovery“ gelegt. Bei diesen Verfahren werden kurze Nachrichten in die Signatur integriert und mit dieser übertragen. In RFID-Systemen kann davon ausgegangen werden, dass die im RFID-Tag gespeicherte und zu signierende Nachricht nur kurz ist, z.B. Passdaten, Geldschein-Identifikation, Fahrkarten- oder Eintrittskarten-Informationen. Diese Nachrichten können daher vollständig in die Signaturen vom Typ „giving message recovery“ integriert werden.

Dipl.-Ing. Tobias Lohmann  
☎ 0271/740-3322    ✉ [tobias.lohmann@uni-siegen.de](mailto:tobias.lohmann@uni-siegen.de)

## Grid Security

Grid-Anwendungen sind sehr sicherheitssensibel, weil firmeninterne Daten – hauptsächlich der Entwicklung und Fertigung – an fremde Dienstleister übertragen und ihnen zur Verarbeitung anvertraut werden. Derselbe Dienstleister kann auch für konkurrierende Kundenarbeiten. Daher können Grids nur verwendet werden, wenn entsprechende Sicherheitsmechanismen vorhanden sind. Unser Grid-Sicherheitskonzept geht von der Nutzung von WeBServices aus, um die Dienstleistungen des Grids in Anspruch zu nehmen. Es ist selbstverständlich, dass die Daten gegen das Abhören durch Dritte geschützt werden, aber auch der Grid-Provider, der den Zugang

zu den Grid-Diensten darstellt, erhält keine Kenntnisse über die Auftragsdaten und -ergebnisse. Jeder Systempartner erhält nur die Informationen, die er wirklich benötigt: für den Auftraggeber bleibt



der Grid-Applikationsdienstleister anonym, umgekehrt weiß dieser nicht, für wen er arbeitet. Trotzdem sind die ausgetauschten Daten authentisch. Dieses stellt der Grid-Provider sicher, der für die Authentizität von Auftraggeber und Auftragnehmer sorgt. Durch weitere Sicherheitsdienste, die ein

Leugnen der in Anspruch genommenen und erbrachten Dienste durch die Beteiligten verhindern, wird zudem für eine vertrauenswürdige Abrechnungsgrundlage gesorgt. Ein „Online Subscription Service“ ermöglicht zusätzlich den Abschluss von Online-Verträgen und somit die dynamische Registrierung von Grid-Serviceanbietern und -auftraggebern.

Dipl.-Wirt.Inform. André Groll

☎ 0271/740-2332 ✉ andre.groll@uni-siegen.de

### Sicherheits- und Zertifikatsmanagement

Die meisten Sicherheitsanwendungen, die asymmetrische kryptographische Verfahren verwenden, z.B. für digitale Signaturen, benötigen eine Public-Key-Infrastruktur. Hierzu zählen insbesondere Zertifikatsmanagementsysteme, die für alle Beteiligten Zertifikate ausstellen und verwalten. Im Rahmen von mehreren Projekten, in denen Chipkarten eingesetzt wurden, haben wir Zertifikatsmanagementsysteme entwickelt, die Zertifikate nach X.509v3 generieren und verwalten (LDAP Server). Dabei können wir auch Zertifikate ausstellen, die Schlüsselssysteme für elliptische Kurvenkryptographie berücksichtigen.

Neben einem Zertifikatsmanagement wird auch ein Sicherheitsmanagement benötigt, mit dem man auf Komponenten des Sicherheitssystems online zugreifen kann, um Schlüsselssysteme auszutauschen, Rechte zu verwalten, Logbücher auszulesen, Geräteparameter zu managen, Datum/Uhrzeit zu setzen, etc. An unserem Institut wurde ein Sicherheitsmanagementsystem entwickelt, mit dem Gerätebetreiber auf ihre Geräte zugreifen und Sicherheitsfunktionen ausführen können. Diese Funktionen, erweitert um den Software-Download zulassungspflichtiger Software, ermöglichen die komplette, sichere und

zugelassene Online-Administration sowie einen vertrauenswürdigen Datenaustausch.

### Sicherer Download zulassungspflichtiger Software

In vielen Anwendungen darf nur Software eingesetzt werden, die zertifiziert, zugelassen oder geeicht worden ist. Häufig handelt es sich dabei um Software, die auf einer großen Anzahl von Endgeräten eingesetzt wird. Ein Austausch der Software, um Fehler zu beheben oder neue Funktionen anzubieten, durch zugelassenes Wartungspersonal vor Ort oder sogar im Rahmen einer Austauschaktion im Prüflabor, ist mit sehr hohen Kosten verbunden. Es ist daher wünschenswert auch derartige Software online nachladen zu können. Neue und europäisch harmonisierte Regelungen des Eichrechts machen dies erstmals auch für eichpflichtige Software möglich, wenn entsprechende Bedingungen eingehalten werden. Wir entwickeln ein Konzept, wie eichpflichtige und andere zulassungspflichtige Software online nachgeladen werden kann, und realisieren es als Prototyp. Dabei wird der gesamte Lebensweg der Software von der Softwareentwicklung beim Hersteller über die Prüfbehörde und den Betreiber der Geräte, deren Software ausgetauscht werden soll, bis zu Online-Prüfmöglichkeiten der Zulassungsstellen und Fehlermöglichkeiten beim Download betrachtet.

Dipl.-Wirt.Inform. Sibylle Hick

☎ 0271/740-2516 ✉ sibylle.hick@uni-siegen.de

### Kombination von Kanalcodierung und Kryptographie

Wir haben ein neues Forschungsgebiet gestartet, das kryptographische Verfahren mit neuen Entwicklungen der Kanalcodierung kombiniert. Moderne Kanalcodierungs- und -decodierungsverfahren, die für eine Fehlererkennung und automatische Fehlerkorrektur sorgen, verwenden mehr und mehr Softinput und Softoutput (SISO-Verfahren). Das bedeutet, dass an Stelle der Bits „0“ und „1“ reellwertige Zuverlässigkeitswerte verwendet werden, die ausdrücken, mit welcher Wahrscheinlichkeit ein empfangener Wert vor der Übertragung ein Bit „0“ oder „1“ gewesen ist. Wir lassen nun ebenfalls kryptographische Verfahren (Verschlüsselungs- und Signaturverfahren) mit diesen Zuverlässigkeitswerten arbeiten und können dadurch die Fehlerrate bei der Entschlüsselung und Verifikation von digitalen Signaturen wesentlich reduzieren. Nur ein einziges fehlerhaftes Bit macht einen verschlüsselten Text oder eine Signatur wertlos. Die automatische Korrektur

von fehlerhaften Signaturen oder gestörten verschlüsselten Texten ist daher besonders wichtig und interessant bei stark gestörten, realzeitorientierten oder Oneway-(simplex)-Übertragungen, wenn keine Wiederholung von fehlerhaft empfangenen Nachrichten möglich oder sinnvoll ist.

Dipl.-Ing. Natasa Zivic, Mag. ET

☎ 0271/740-3322 ✉ natasa.zivic@uni-siegen.de

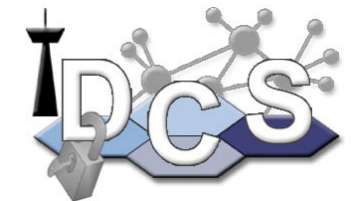
Ayyaz Mahmood, MSc

☎ 0271/740-2623 ✉ ayyaz.mahmood@uni-siegen.de



Oktober 2006

Institut für Digitale Kommunikationssysteme  
Lehrstuhl für Nachrichtenübermittlungstechnik



### Kontakt

Institut für Digitale Kommunikationssysteme  
Hölderlinstraße 3  
57076 Siegen  
☎ 0271/740-2522  
☎ 0271/740-2536  
✉ christoph.ruland@uni-siegen.de  
<http://www.dcs.uni-siegen.de>

Sekretariat:

Christine Haßler  
☎ 0271/740-2521  
✉ christine.hassler@uni-siegen.de

im Fachbereich Elektrotechnik und Informatik  
Univ.-Prof. Dr. Christoph Ruland, Institutsleiter