Sicherheit im E-Commerce durch Kryptographie on-the-chip

Dirk Timmermann

Institut für
Angewandte Mikroelektronik und Datentechnik
FB Elektrotechnik u. Informationstechnik
Universität Rostock

Agenda

- **Projekt Mobilität und spontane Vernetzung**
- **Motivation für hardwaregestützte Kryptographie**
- **Kryptographische Systeme und Operatoren**
- **Anwendungsbeispiele**

Sicherheitsarchitektur für mobile spontan vernetzte Geräte

Prof. Dr. Clemens Cap
FB Informatik
Institut für Technische Informatik

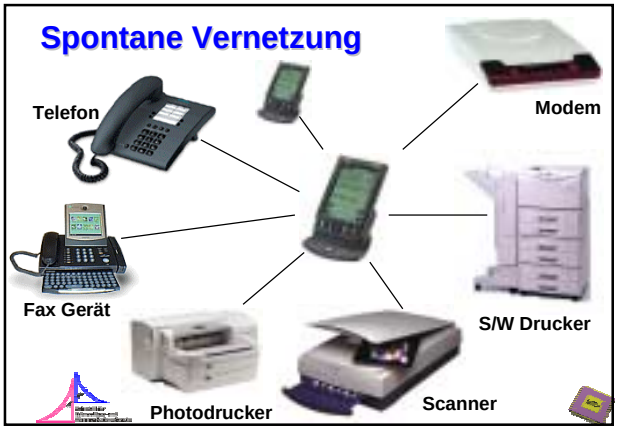
Prof. Dr. Dirk Timmermann
FB Elektrotechnik u. Informationstechnik
Institut für Angewandte Mikroelektronik und Datentechnik

Deutsche Forschungsgemeinschaft
DFG

Projektziele

- Untersuchung der *ungelösten Sicherheitsprobleme* im Bereich *mobiler* Systeme bei *spontaner* Vernetzung über *drahtlose* Verbindungen
- Ganzheitliche theoretische und praktische Untersuchungen im Soft- *und* Hardwarebereich
- Sichere Authentifizierung, Verschlüsselung und Zugriffssteuerung trotz geringerer Prozessorleistung und niedriger Stromaufnahme auf mobilen Systemen
- Entwicklung von Techniken der *Anonymisierung* und der individuellen Konfiguration durch den Anwender
- Prototypische Implementierung eines
  - gestuften Client-Server Systems, bestehend aus
    - mobilem PersonalCard-Client aus Javaprozessor + Kryptofähigkeit + drahtloser Schnittstelle
    - PC-basiertem Server
  - Beispielanwendung als Referenzszenario, z.B. Info-Badge, digitaler Assistent

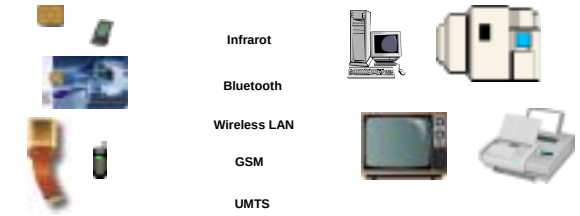
Spontane Vernetzung



Gedanken zur Applikation

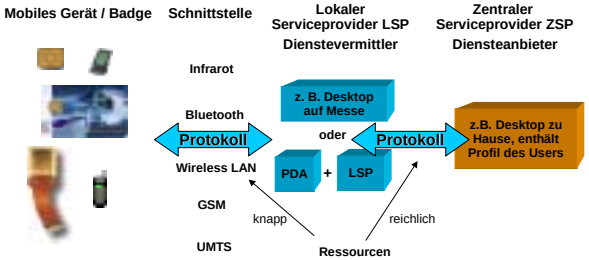
- **Einfache Nutzung eines Dienstes**
  - Anonym / Persönlich bei Autorisierung, Bezahlung, Profilerstellung
  - Bsp: Nachrichtendienst, Zutrittskontrolle (Mitbestimmungs-konform)
- **Multicast von Informationen**
  - Identitätsabhängiger Zugang ohne Roaming
  - Bsp: Börsenticker
- **Koppelung mehrerer Nutzer**
  - Profilabhängige Kommunikation, bidirektional, Multicast oder Konferenz
  - Durch Vermittlung von zentralem Server
  - Server lernt aus Kommunikation möglichst wenig
  - Bsp: Messe, active badge, drahtlose Abstimmungen und Auktionen, Verkehrskoordinationssystem (Taxi-Sharing)

Zweistufige Architektur für Mobilität



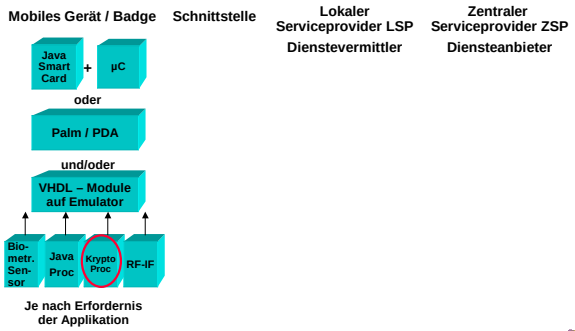
- **Eigenschaften**
  - Knappe Ressourcen: Größe, Performance, Stromverbrauch, Bandbreite, Reichweite
  - Jini zu „schwer“
  - Konsequenzen für Konfigurierbarkeit, Anonymität, Sicherheit

Mehrstufige Architektur für Mobilität

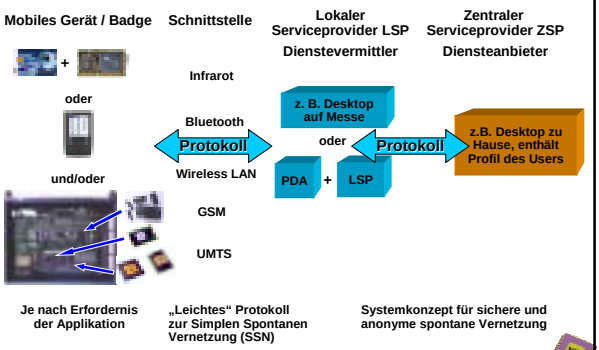


- Mobilgerät (intell. Badge) sehr einfach
- Enthält nur IP- # oder URL und 'etwas' Kryptofähigkeit
- Systemarchitektur für mobile Sicherheit
- mehrstufiges Konzept nutzt jeweils verfügbare Ressourcen
- vgl. NINJA, UC Berkeley, Prof. Katz

Zu entwickeln



Zu entwickeln



Gründe *für* HW-Kryptographie

- **Software auf Standard-Prozessoren**
  - Zu langsam
  - Zu teuer
  - Zu groß
  - Zu energiehungrig
  - Zu unsicher
- **Warum ?**
  - Datenpfadbreite (max. 64 Bit) nicht ausreichend für sichere Kryptographie
  - Architektur angepasst an Std.-Programme, Caches unnötig
  - Befehlssatz nicht adäquat für kryptotypische Bitoperationen
    - Floating Point, aber keine modulare Multiplikation u. Exponentiation
  - Großteil der Chipfläche nicht ausgelastet
  - Extern gespeicherte Programme verletzlicher gegen Ausspähung u. Angriffe, Private Keys on Chip relativ sicher

Gründe *gegen* HW-Kryptographie

- **Hardware extrem schnell, aber**
  - Zu entwicklungsintensiv
  - Zu schlechtes Time-to-Market (a.k.a. Time-to-Money)
  - Zu unflexibel gegen ECO, HW-Patches unrealistisch
  - Software substituiert dedizierte Hardware ohnehin wg. Moore in 3 Jahren
  - Höhere Performance = höhere Leistungsaufnahme
- **Wirklich ?**
  - Aktuell: HW-Entwicklung mit Hochsprachen und Komponenten (IP)
  - Aktuell: HW-Entwicklung prinzipiell nicht aufwendiger
  - Aktuell: ECO und „Bananen“-Hardware durch REKONFIGURIERBARE LOGIK
  - Aktuell: Neues FPGA behält Leistungsvorsprung
- **Mix aus SW, dedizierter HW und rekonfigurierbarer Logik realisiert anwendungsspezifisches Optimum an Performance, Entwicklungszeit, Leistungsaufnahme und Flexibilität**

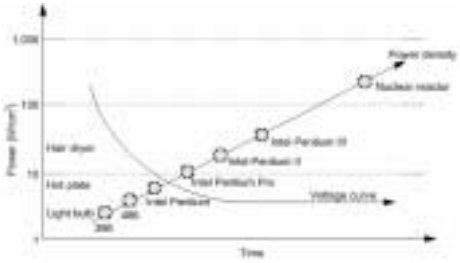
Mobilitätsszenario

- Rechner
  - Rechnerperformance und –leistungs-verbrauch steigt exponentiell nach Moore
- Kommunikation
  - Sendeleistung steigt mit zunehmender Entfernung und Bitrate exponentiell an

- Batteriekapazität steigt aber in 5 Jahren nur um 30-50%

Außerdem
- Kosten, Größe, Kühlung, ...
- Umwelt (Elektronikanteil derzeit 10% am Gesamtenergieverbrauch)

Trend Leistungsdichte



[Hoering, MICROPROCESSORS, MICROCONTROLLERS, AND SYSTEMS IN THE NEW MILLENNIUM, IEEE Micro, vol. 20, no. 6, Nov/Dez. 2000]

Energieverbrauch und Performance

Energieeffizienz [MOPS/mW]

Flexibilität

In eingebetteten System ist rekonfigurierbare HW genauso flexibel wie SW, nur leistungsfähiger und sparsamer !

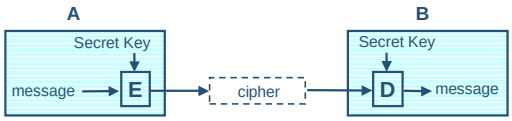
[UC Berkeley Rabaey]

Kryptographische Systeme

- **Private key (DES, AES)**
- **Public key (RSA, ECC)**
- **Hybride Systeme**
- **Digitale Signatur**

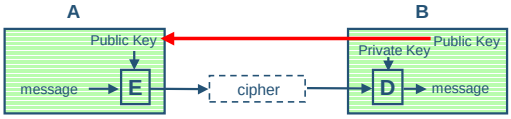
Überblick: Symmetrische Systeme

- **Ein geheimer Schlüssel auf beiden Seiten**
  - Verschlüsselung : $c = f(m, k)$
  - Entschlüsselung : $m = f^{-1}(c, k)$



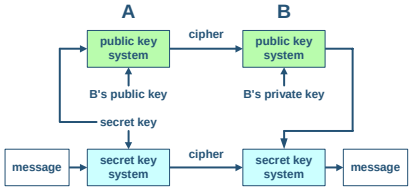
Überblick: Asymmetrische Systeme

- **Verschiedene Schlüssel auf jeder Seite**
  - Verschlüsselung : $c = f(m, \text{public key})$
  - Entschlüsselung : $m = f^{-1}(c, \text{private key})$
- **Langsamer als symmetrische Systeme (~ 100 mal)**

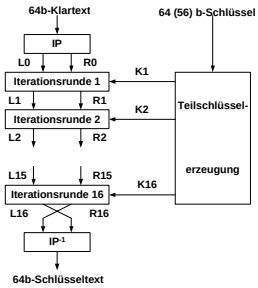


Überblick: Hybride Systeme

- **Benutzung des asymm. Systems für den Sitzungsschlüssel**
  - Während des Verbindungsaufbaus
  - Unkritische Geschwindigkeitsanforderung
- **Benutzung des symm. Systems für den Datenstrom**



DES - Ablaufstruktur



- **Ablauf**
  - IP (initial permutation) teilt Klartext in L0 und R0 auf
  - Iteration (1 .. 16)

    $L_i = R_{i-1}$

    $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

    unabhängig vom Vorgänger
  - IP^{-1} mischt L16 und R16 zu Schlüsseltext
- **Grundoperationen**
  - Transposition, Substitution
  - d.h. *Bitoperationen, XOR*

RSA

- q, p sind große Primzahlen
- $n = p \cdot q$ (n > 1000 Binärstellen !)
- Wähle e, so dass e relativ prim zu $(p-1)\cdot(q-1)$ ist
- berechne d, so dass $d \cdot e = 1 \bmod ((p-1)\cdot(q-1))$ gilt
  - public key : e, n
  - message : m
  - private key : d
  - cipher : c

  Verschlüsseln : $E(m) = m^e \bmod n = c$

  Entschlüsseln : $D(c) = c^d \bmod n = m$
- Grundoperation ist *Modulare Exponentiation*
- Diese zurückgeführt auf $1{,}5 \log_2(n)$ [also > 1500 $2^{10} \cdot 2^{10}$ Bit]

  Modulare Multiplikationen $y = a \cdot b \bmod n$

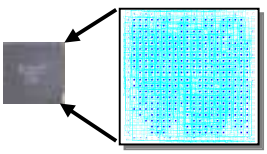
Beschleunigung

- **Algorithmisch**
  - Chinese Remainder Theorem, CRT
  - Montgomery Multiplikation, Sedlak
  - Barrett
  - MSD-First Algorithmen (Digit-on-line)
- **Architektur**
  - Optimales Mapping der Algorithmen
  - Parallelisierung
  - Pipelining
  - Redundante Zahlendarstellung
- **Schaltungstechnik**
  - z.B. Low Power dynamische Logik, asynchrone Logik

Realisierungsformen

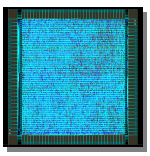
FPGA

Feldprogrammierbares Gate-Array



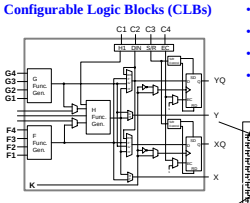
ASIC

Anwendungsspezifische integrierte Schaltung

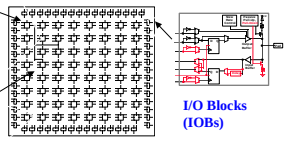


Rekonfig. Logik: Xilinx XC4000 FPGA

Configurable Logic Blocks (CLBs)



- Große Dichte → 1 Mio. System Gatter
- SRAM basierende LUT
- Array Struktur
- interne Tri-States
- beliebig rekonfigurierbar in wenigen ms



Programmable Interconnect

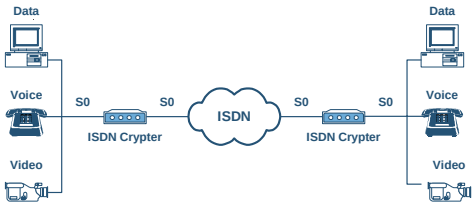
I/O Blocks (IOBs)

Laufende Arbeiten

- **Ziele:**
  - Hochgeschwindigkeitsverschlüsselung für multimediale Datenströme
  - Kleine Architekturen für den Bereich Smartcard / Personalcard
- **Weg:**
  - Optimierung von Algorithmen für den Hardwareeinsatz
  - Einsatz neuer Architekturen und Schaltungstechniken
- **Projekte:**
  - **SECOM mit Triple-DES für Daten und RSA für Schlüsselaustausch**
  - Online Festplattenverschlüsselung
  - **Smartcard RSA: Minimallösungen für modulare Exponentiation**
  - **GHz Kryptoprozessor durch massives Pipelining und dynamische Schaltungstechnik (TSPC)**

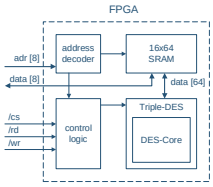
SECOM: ISDN Verschlüsselung

- **Benutzerfreundlich und transparent zu gängigen ISDN-Geräten**
- **Wiederverwendung von vorhandener Hardware**



Triple-DES in SECOM

- **FPGA: XC4010e-3**
  - 380 CLB von 400 = 95% Auslastung
  - Aber: 209 FF von 800 = 26%
- **TDES: 55 Takte**
  - Datenrate @ 8 MHz: 9.3 MBits/s



ISDN B-Kanal: 64 KBit/s pro Richtung

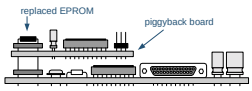
=> TDES-Core kann 8 ISDN B-Kanäle gleichzeitig verschlüsseln

Ausnutzen der Rekonfigurierbarkeit

- **Ziel: Vorhandene Hardwareressourcen besser ausnutzen**
- **Beobachtung: zeitlich getrennte Algorithmen**
- **Zwei Arbeitsphasen**
  - RSA nach dem Neustart
  - FPGA rebooten nach erfolgreichem Schlüsselaustausch
  - Triple DES für die Verschlüsselung des Datenstroms
- **Rebooten des FPGA mit neuem Inhalt in ungefähr 35 ms**

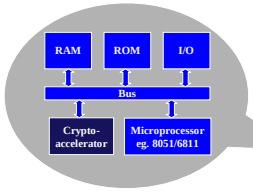
Prototyp

- **Basiert auf einem Least-Cost-Router mit 16bit CPU**
- **FPGA XC4010e-3**



Smartcard-Ressourcen

- **Mikroprozessor**
  - 8 .. 32 bit, 3.5 .. 5 MHz
- **Speicher**
  - ROM (16 - 32 KByte)
  - RAM (0,5 - 1 KByte)
  - EEPROM (8 - 16 KByte), NVRAM
- **Die Größe < 25 mm²**



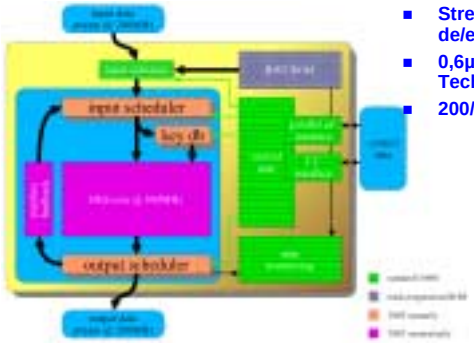
Performance Kryptoalgorithmen

- Benötigte Algorithmen: DES (Triple DES), RSA, SHA-1
- Hier als Beispiel: DES (RSA 100-1000 x langsamer)
- Typ | Clock | Durchsatz

Typ. Smartcard Prozessor	4 MHz	3,7	KBit/s
AMD-K6	266 MHz	3,6	MByte/s
XILINX FPGA rekursiv	**4 MHz**	**1,9**	**MByte/s**
XILINX FPGA pipelined	**4 MHz**	**30,7**	**MByte/s**

- Vorteile dedizierter Kryptoprozessoren
  - Performance ermöglich erst Anwendung !
  - skalierbar bezüglich Parallelität und Pipelinebarkeit
  - geringere Leistungsaufnahme

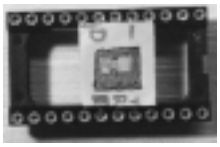
GHz Triple DES

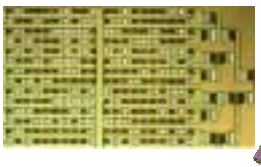


- Streaming data de/encryption
- 0,6µm@5V AMS Technologie
- 200/800 MHz

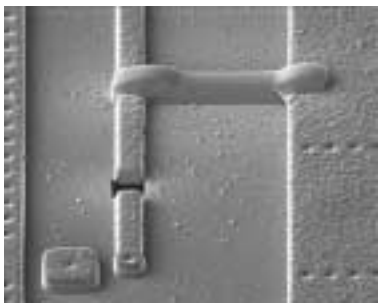
Sicherheit von HW-Kryptographie

- Sicherer als SW, aber .....



Focused Ion Beam - Beispiel

Fazit

"Was der eine Mensch sich ausdenken kann, kann ein anderer auch herausbekommen."

- Sherlock Holmes

"Was von einer Maschine chiffriert worden ist, lässt sich um so einfacher auf einer Maschine wieder dechiffrieren."

- Alan M. Turing