Smart Cards

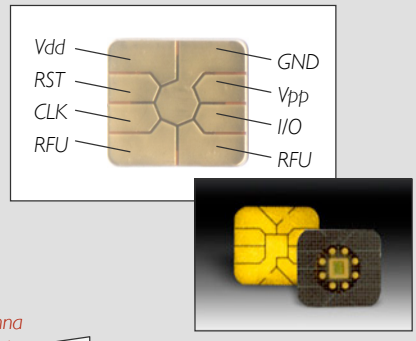
Towards a modern run-time platform

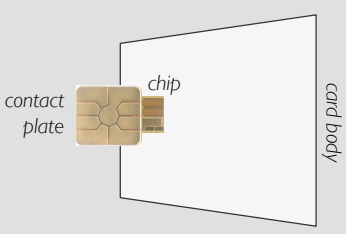
1. Introduction

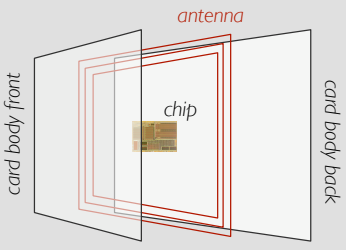
Thorsten Kramp & Michael Kuyper
IBM Zurich Research Laboratory

What is a Smart Card?

- Defined by ISO Joint Technical Committee 1 (JTC1): ISO 7816
  - *physical characteristics*
  - *physical contacts*
  - *electronic signals*
  - *transmission protocols*
- "Piece of plastic" with an embedded IC
  - *contact-based vs. contactless*







Smart "Card" Applications Domains

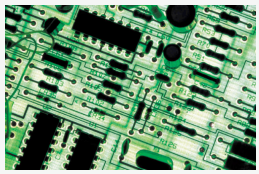
- Application Domains
  - *secure storage*
  - *payment*
  - *authentication*
  - *signing*
- Alternative form factors
  - *contact-based*
    - traditional plastic card
    - as USB token
  - *contactless*
    - embedded in jewelry (e.g., in a ring)
    - embedded in watches

DEMO

Overview

A. Hardware overview

CPUs, memory types, I/O, cryptographic co-processors, random number generators

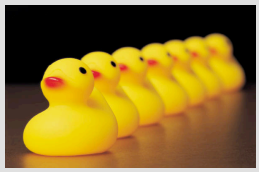


B. Communication modes and protocols

interaction model, contact-based vs. contact-less

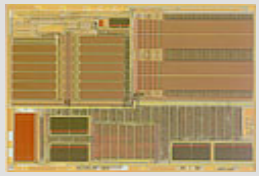
C. Classification of smart-card operating systems

static vs. dynamic, file-system-based vs. object-oriented



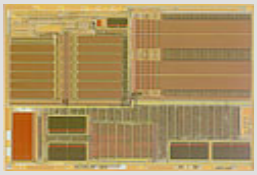
A. Smart Card Chips

- Chip Characteristica:
  - *physical:*
    - up to 25 mm^2 (typical 9-14 mm^2)
  - *power:*
    - external power only (no batteries)
    - 1-5V (typical: 1.8, 3V, 5V)
  - *clock:*
    - external clock only (internal clock multiplier)
    - clock-less design (a.k.a. "free running")
    - no "wall clock", only timers
  - *manufacturers*
    - Philips, Infineon, Atmel, ARM, STmicro, Samsung, Sharp, MIPS



A. Smart Card Chips

- Chip Components:



CPU *8-32 bit, CISC/RISC*	**ROM** *< 512 KB*
Crypto-Co *DES/AES, RSA/ECC*	**RAM** *< 8 KB*
RNG *true random*	**EEPROM, Flash** *< 256 KB, < 2 MB*
I/O *up to 848 Kbit/s*	**MMU**

A. Smart Card Chips: CPU

- 8-32 bits
  - *8 bits (still very common)*
    - smaller code size
    - small address range w/o instruction set extensions (cf. memory banking)
    - usually w/ extensions for 16 bits memory addressing and access
    - cheap (many chips per wafer)
  - *16-32 bits (upcoming)*
    - large(r) code size
    - large(r) linear address space
    - increasingly expensive (fewer chips per wafer)

CPU *8-32 bits, CISC/RISC*
Crypto-Co *DES/AES, RSA/ECC*
I/O *up to 848 Kbit/s*
RNG *true random*

A. Smart Card Chips: CPU

- CISC vs. RISC
  - *CISC (complex instruction set computer)*
    - complex opcodes (many cycles)
    - more complex CPU design
    - smaller code
    - comparatively easy to hand-optimize (less error-prone compilers)
  - *RISC (reduced instruction set computer)*
    - simple opcodes (usually only one cycle)
    - simpler CPU design
    - larger code
    - comparatively difficult to hand-optimize (better compiler logic for optimization)

A. Smart Card Chips: Crypto Co-processor

- Symmetric cryptography
  - *shared key used for both encryption and decryption*
  - *fully hardware-implemented*
  - *DES (Data Encryption Standard)*
    - key length: 8-24 bytes (DES, 2DES, 3DES)
    - block length: 8 bytes
    - modes: encryption/decryption, MAC
  - *AES (Advanced Encryption Standard)*
    - key length: 128-256 bits
    - block length: 16, 24, 32 bytes
    - modes: encryption/decryption, MAC

A. Smart Card Chips: Crypto Co-processor

- Public-key cryptography
  - *public/private key pair*
    - public key: encryption, signature verification
    - private key: decryption, signature generation
  - *partially hardware-implemented*
    - support for large-number modular arithmetic
    - support for modular polynomial arithmetic
    - often w/ extra crypto RAM
  - *RSA (Rivest, Shamir, Adelmann)*
    - key length: 256-4096 bits on-card
  - *ECC (elliptic curve cryptography)*
    - key length: 112-576 bits on-card

A. Smart Card Chips: I/O

- Contact-based
  - *serial communication*
  - *via smart-card reader (ISO 7816)*
    - 9,6-115 Kbits/sec
    - half duplex
  - *USB 1.1 low-speed*
    - up to 1,5 Mbits/sec
    - half duplex, full duplex
  - *I^2C (inter-integrated circuit)*
    - up to 100 Kbits/sec
    - half duplex

A. Smart Card Chips: I/O

- Contact-less
  - *serial communication*
  - *half duplex*
  - *13.56 Mhz*
  - *proximity (ISO 14443)*
    - up to 15cm
    - up to 848 Kbits/sec
  - *long range (ISO 15693)*
    - up to 1.5m
    - long distance mode: 6,62 Kbit/sec
    - fast mode: 26,48 Kbit/sec

CPU
8-32 bit, CISC/RISC

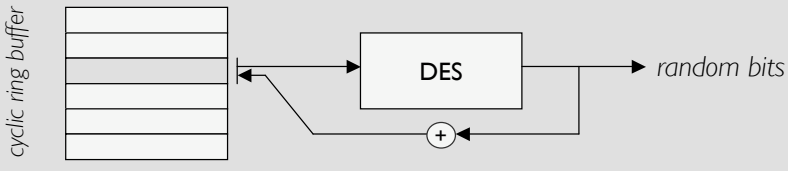
Crypto-Co
DES/AES, RSA/ECC

I/O
up to 848 Kbit/s

RNG
true random

A. Smart Card Chips: RNG

- Random number generator
  - *must pass statistical tests (e.g., χ^2 or FIPS 140-2)*
  - *Software random number generator*
    1. some logical CPU states
    2. using a crypto algorithm such as DES



  - *Hardware random number generator*
    - exploits physical characteristics
    - performance varies depending upon how long it takes to build up a sufficient level of entropy

CPU
8-32 bit, CISC/RISC

Crypto-Co
DES/AES, RSA/ECC

I/O
up to 848 Kbit/s

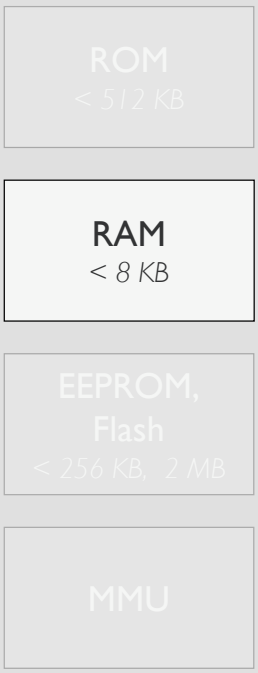
RNG
true random

A. Smart Card Chips: Memory

- ROM
  - *read-only memory*
  - *"masking" during chip fabrication*
  - *read latency: ~70ns*

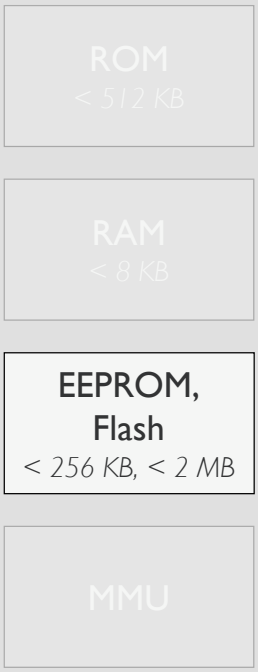
A. Smart Card Chips: Memory

- RAM
  - *random-access memory, loses content w/o power*
  - *scarcest memory resource*
  - *single cell: ~4 x size of EEPROM*
  - *read/write latency: ~70ns*



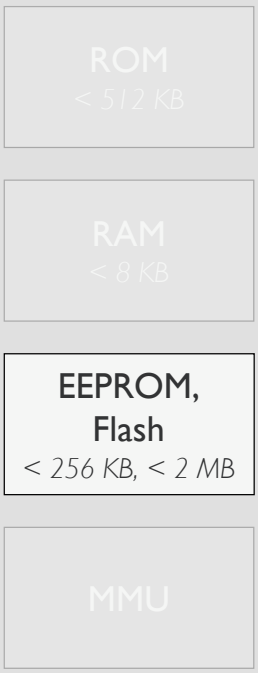
A. Smart Card Chips: Memory

- EEPROM
  - *electrical erasable persistent read-only memory*
  - *maintains state even w/o power (up to 10 years)*
  - *single cell: ~4 x size of ROM*
  - *write latency: ~3-10ms*
  - *read latency: ~70ns*
  - *limited number of write cycles per cell*



A. Smart Card Chips: Memory

- Flash
  - *flash electrial erasable read-only memory*
  - *maintains state even w/o power*
  - *write latency: ~10µs*
  - *read latency: ~70ns*
  - *limited number of write cycles per cell*
  - *write operations can only erase bits*
  - *erase operations in blocks only (e.g., 8 KB or 64 KB)*



A. Smart Card Chips: Memory

- Memory Management Unit
  - *memory banking/mapping*
    (8 bits CPUs w/ limited address range)
  - *restrict read/write operations to certain address ranges*
  - *user mode vs. supervisor mode*
    - restrict access to some address ranges
    - restrict access to certain special function registers

A. Smart Card Chips: Examples

- Philips SmartMX
  - *8 bits CISC CPU (80C51 derivative w/ extended 24 bits addressing)*
  - *1-10 Mhz (up to 40 Mhz internally)*
  - *communication*
    UART
    ISO 7816, ISO 14443, USB 1.1
  - *crypto co-processors*
    DES, AES
    32 bits FameXE crypto co-processor
  - *hardware random number generator*
  - *ROM: 160KB, RAM: 4KB, EEPROM: 72KB*

PHILIPS

A. Smart Card Chips: Examples

- Samsung SC3CC9
  - *16 bits CalmRISC CPU*
  - *Harvard architecture*
  - *1-5 Mhz*
  - *communication*
    - UART
    - ISO 7816
  - *crypto co-processors*
    - DES
    - SuperMAP II crypto co-processor
  - *hardware random number generator*
  - *ROM: 128-160KB, RAM: 4-6 KB, EEPROM: 32-64 KB*

SC3CC9
16 bits RISC

A. Smart Card Chips: Examples

- Infineon SLE88
  - *32 bits RISC CPU*
  - *1-10 Mhz (up to 66 Mhz internally)*
  - *communication*
    - UART
    - ISO 7816
  - *crypto co-processors*
    - DES
    - crypto co-processor
  - *hardware random number generator*
  - *ROM: 192-240KB, RAM: 6-8 KB, EEPROM: 72-80 KB*

SLE88
32 bits RISC

A. Smart Card Chips

- Compare to: Apollo 11 Guidance Computer
  - *2 Mhz CPU*
  - *16 bits word length*
  - *4 KB RAM*
  - *72 KB ROM*

`www.apollosaturn.com/gnc.htm`
`www.digitalmist.com/plethorama/apollogc.htm`

DEMO

A. Smart Card Chips: Tamper Resistance

- Run-time mechanisms
  - *randomized clock or "free running"*
  - *unified power consumption*
  - *memory encryption (EEPROM/RAM)*
  - *bus randomization*
  - *voltage, clock, temperature sensors*
- Static mechanisms
  - *shielding against micro-probing*
  - *light sensors*
  - *randomized chip layout*