FEL ČVUT

Security of RFID in pracitce

Electronic Passports

Jiří Buček, Róbert Lórencz, Tomáš Rosa

May 22, 2008

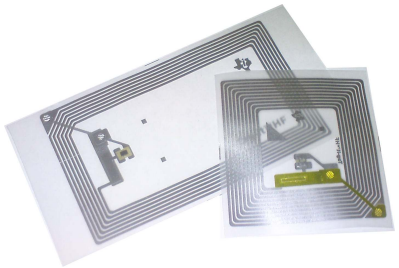
1. RFID Principles
   - Physical Principles
2. RFID Applications
   - Applications
3. Electronic Passports
   - Standards
   - Security
   - Measurements

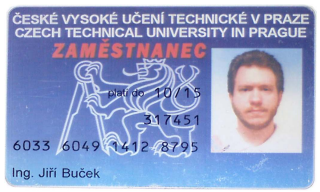
Radio Frequency Identification

- Frequency categories
  - LF chips/cards (125–150 kHz)
  - HF proximity cards – ISO/IEC 14443 (13.56 MHz)
  - HF vincity cards – ISO/IEC 15693 (13.56 MHz)
  - UHF chips (868–928 MHz)
- Physical principles
  - LF, HF – inductive coupling
  - UHF – radiation coupling
- RFID – Application of RF technology for identification

Applications

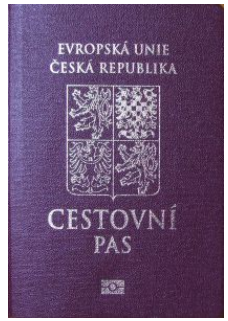
- Theft protection – one-bit transponders
- Product labels
- Entrance systems – LF, HF
- Transportation tickets
- Recreational service tickets
- Payment systems
- **Electronic passports**





Electronic Passports

- ICAO (International Civil Aviation Organization)
  - MRTD – Machine Readable Travel Document
  - MRP – Machine Readable Passport
  - Electronically readable MRP – ePassport
- ISO/IEC 14443 – Physical layer, low-level communication
- ISO/IEC 7816 – Communication protocol
  - Application ID A0 00 00 02 47 10 01
  - File system



Information stored in the chip

- File system (ISO/IEC 7816-4)
  - EF.DG1 – Machine Readable Zone (mandatory)
  - EF.DG2 – Encoded face – photograph (mandatory)
  - EF.DG2 – Encoded fingers (optional)
  - EF.DG3 – Encoded eyes (optional)

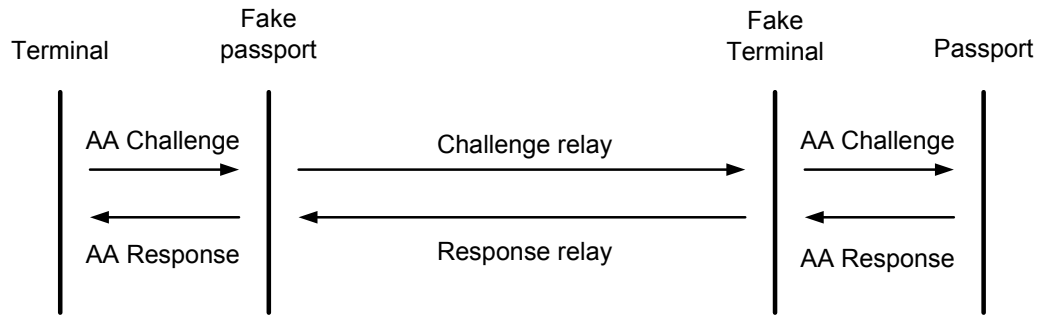
  ...
  - EF.DG15 – Public key for active authentication (optional)
  - EF.COM – Version information, tag list (mandatory)
  - EF.SO_D – Document Security Object (mandatory)
- K_{ENC}, K_{MAC} – Document Basic Access Keys (optional)
- KPr_{AA} – Active Authentication Private Key (optional)

Security Measures

1. Data groups 1-15 are write-protected
2. Each data group is digitally signed (hashes and signature stored in EF.SO_D)
3. Basic Access Control – Access restriction
   - Symmetrical encryption and authentication, keys derived from information in the Machine Readable Zone (MRZ)
   - Secure Messaging
   - Mandatory in European Union
4. **Active Authentication** – Prevention of chip substitution
   - Asymmetrical authentication, private key stored in protected (non-readable) space, public key stored in EF.DG15
   - Optional in European Union
   - **Czech Passports** (as of 2007) – RSA-CRT 1024 bit

Possible attacks

- Protocols and implementations
  - Asymmetrical decryption/signing is time-consuming
  - Delays in communication tolerated – relay attacks

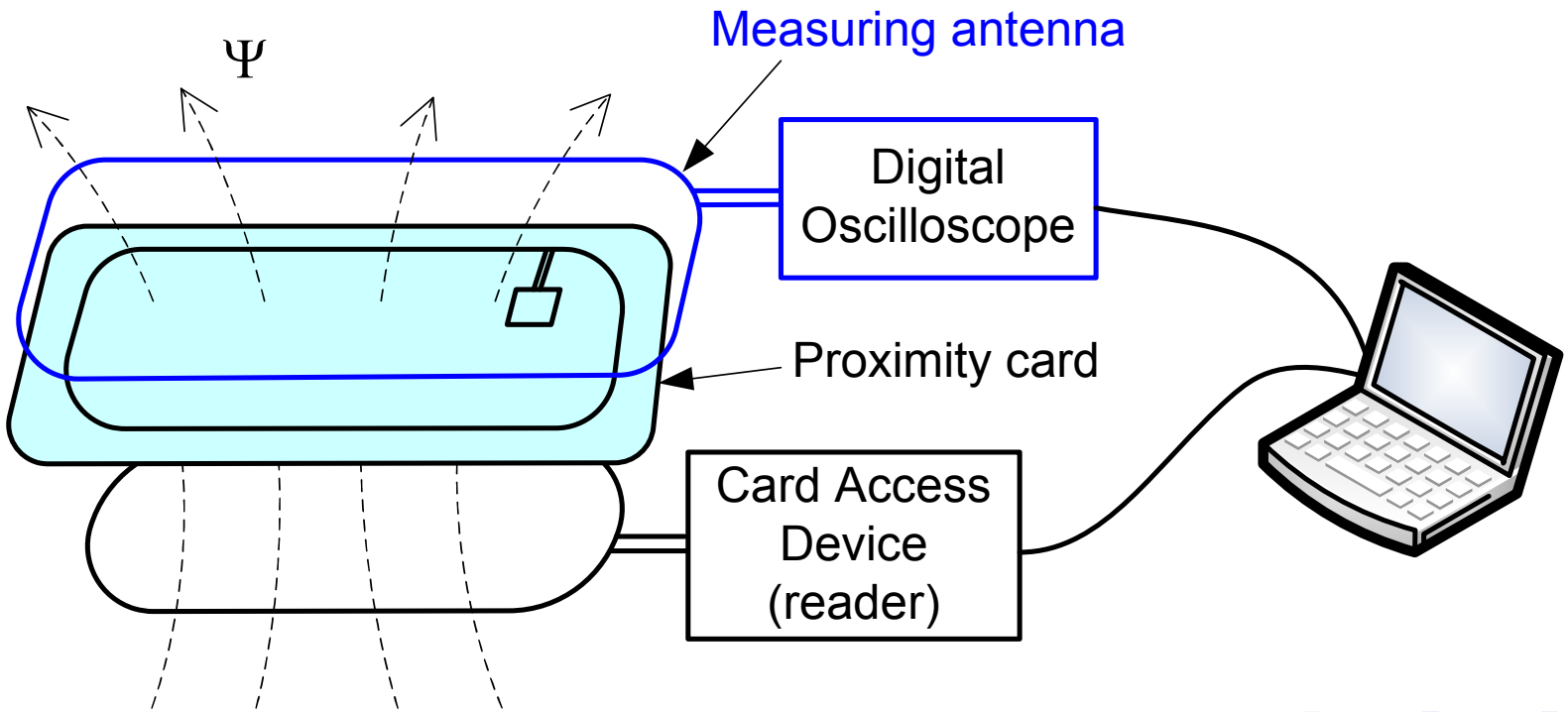


- Power supply and communications
  - Sensitive operations – symmetrical encryption/decryption, asymmetrical decryption/signing
  - Card uses the magnetic field both for its power and for communication – potential **RF power side channel** – that is what we examine now $\longrightarrow$

Measuring assembly

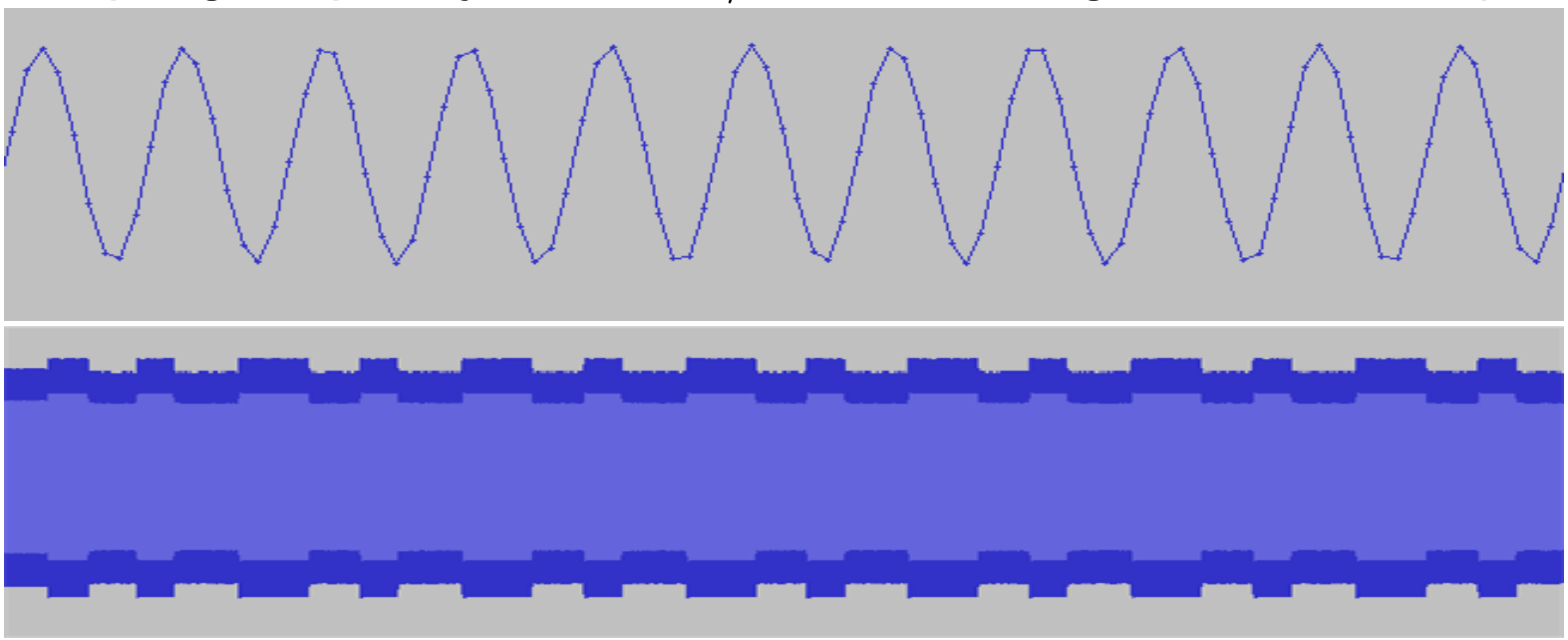
RF power side channel – voltage induced in measuring antenna

$$V = -N\frac{d\Psi}{dt}$$



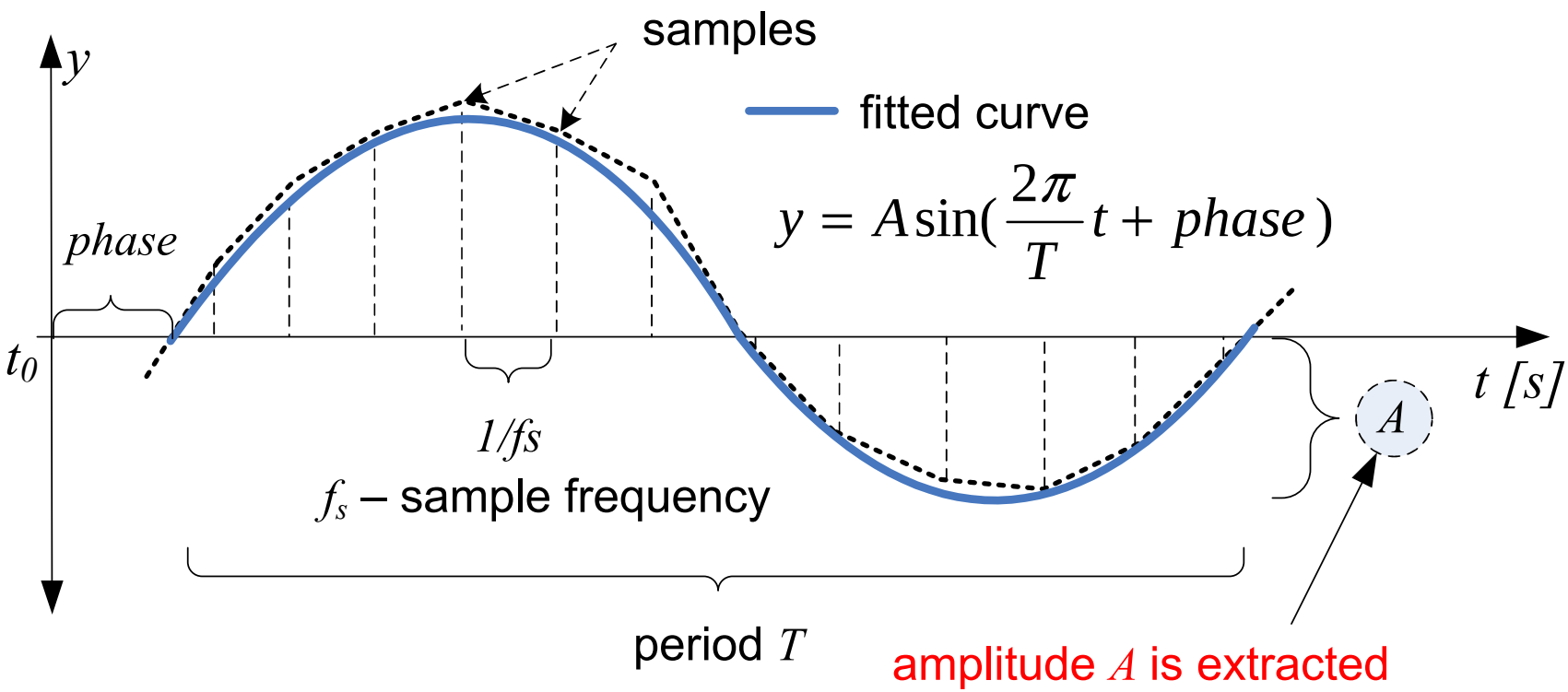
Measured signal

Measured RF signal: Load modulated sine wave, carrier frequency: 13.56 MHz
Sampling frequency: 125 MS/s, Record length: 128 MSamples



Extraction of amplitude

Method of extraction amplitude - filtering of carrier frequency



Extraction of amplitude I

Data acquisition:

1. Setting of measurement equipment
2. Adjusting of trigger and sample frequency (125 MS/s)
3. Measurement of RF side channel signal while waiting for Active Authentication response

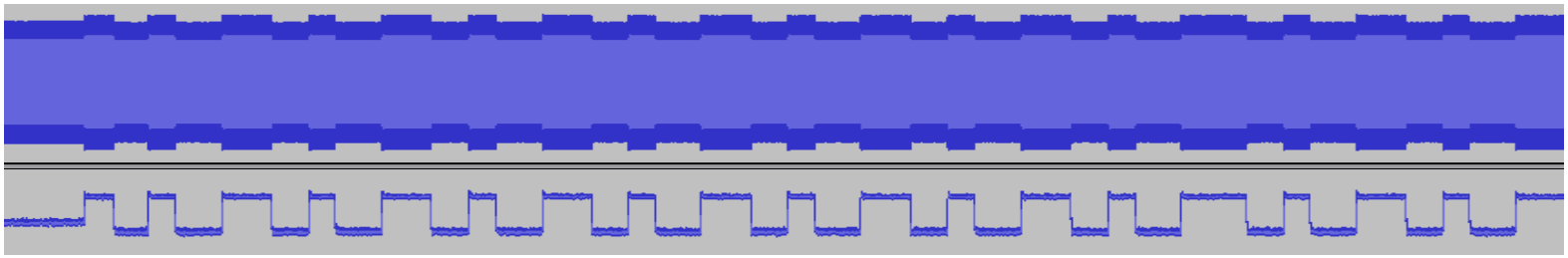
Steps of extraction:

1. Computing of average period
2. Fitting of samples with sine wave – Least Squares Method (LSM)
3. Extraction of amplitudes for each sample by 2-3 periods of sine wave
4. Adjusting of phase as needed during extraction

Extraction of amplitude II

Advantages of extraction method

- Simple (small complexity) and efficient method
- LSM is guarantee of good extraction of amplitude also in case of low sampling frequency
- Selection of fitted wave length – tradeoff between computational stability and loss of information
- Possibility of extraction en bloc – important for the following cryptanalysis

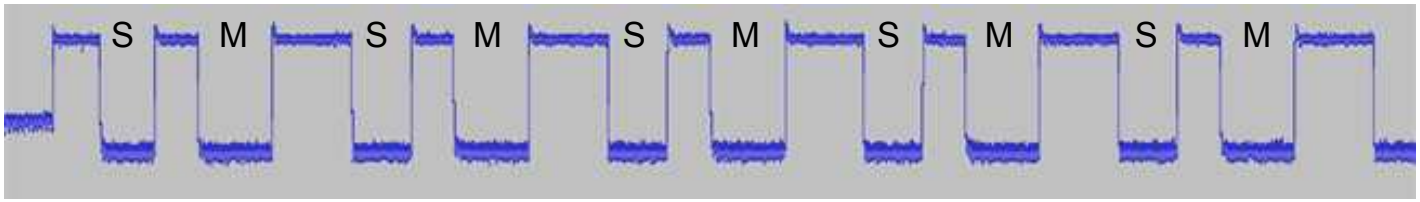


RSA Square and Multiply

Input: Integers x, d, N; $0 \leq x \leq N$, $2^{k-1} \leq d \leq 2^k$
Output: $x^d \bmod N$

$z \leftarrow x$
for $i = k - 2$ **to** 0 **do**
  $z \leftarrow z^2 \bmod N$ (Square)
  if $d_i = 1$ **then** $z \leftarrow z * x \bmod N$ (Multiply)
  else $dummy \leftarrow z * x \bmod N$? (Dummy Multiply)

Squaring and multiplication distinguishable by duration



Conclusion

Realy attack

- Conclusion: Passports pretty well secured, but ...
- Is relay attack possible?

RF signal analysis

- We are able to acquire and extract some information from the RF field
- Processor architecture – if known can provide valuable information
- What signal quality is attainable from greater distance?

References

- Rosa, T.: Bezpečnost RFID v praxi (in czech). Quality and Security '08, Prague, 2008
- Kinneging, T.: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, IACO Technical Report, ver. 1.1, 2004
- ISO/IEC 14443-1..4
- ISO/IEC 7816-3, 4