
Faculty of Electrical Engineering
and Communication

Brno University of Technology
Technicka 12, CZ-61600 Brno, Czech Rep.

http://www.six.feec.vutbr.cz

# Advances in Cryptography

**Jan Hajný**
**Cryptology Research Group**
Department of Telecommunications, FEEC, BUT
http://crypto.utko.feec.vutbr.cz

# Introduction of CRG

**Cryptology Research Group**:

- small group of around 10 people,
- Professors, Ph.D.s and postdocs,
- part of Department of Telecommunications, BUT,
- forms the SIX Security Laboratory,
- focused on basic and applied research in crypto,
- provides security-related services in ICT.

# Activity Overview

**R&D in Cryptographic Protection:**

- cryptographic design of new protocols and schemes,
- access control systems,
- secure authentication systems,
- privacy-enhancing schemes,
- encryption systems for data transfer and storage.

**Security System Implementation:**

- application development for smart-cards,
- application development for smart-phones (Android, iOS),
- protection of low-performance  systems (sensors, controllers...).

# Services: High-Load Testing and Benchmarking

Extreme-load testing of devices using specialized HW:

- tests with more than 1 mil. HTTP GET requests per second,
- 300 000 HTTPS requests per second, throughput 20 Gb/s,
- up to 30 millions sustained connections,
- real user behavior simulation, web clients simulation,
- more information by Lukáš Malina: “Stress testing and distributed denial of service testing of network infrastructures” at 13:20.


# Current Areas of Research

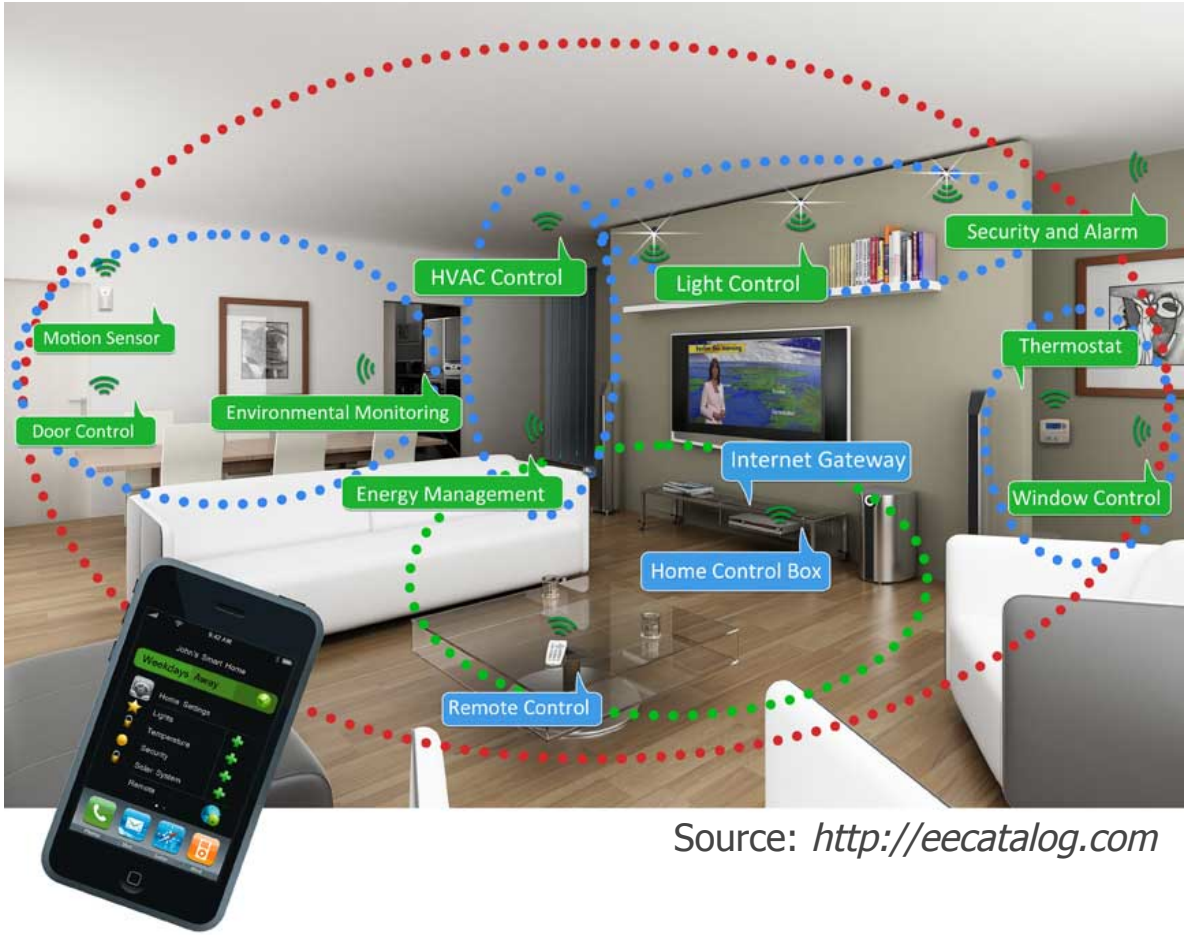
**Research into lightweight cryptography:**

- done in cooperation with Honeywell, s.r.o.,
- focused on adding security features to “slow devices”,
- includes final implementations on microcontrollers.

**Research into privacy-enhancing cryptography:**

- both basic and applied research into modern cryptographic protocols,
- done in cooperation with many partners from U.S., EU, Czech Republic,
- includes final implementations on smart-cards, mobile phones.

# Research into Lightweight Cryptography - Introduction




Source: *http://eecatalog.com*

# Research into Lightweight Cryptography I

**What is "lightweight cryptography"?**

- provides secure encryption on computationally (and memory) restricted devices,
- algorithms designed to be efficient in using CPU, RAM and codesize,
- tradeoff between CPU and memory usage,
- many algorithms available, each suits different scenario.

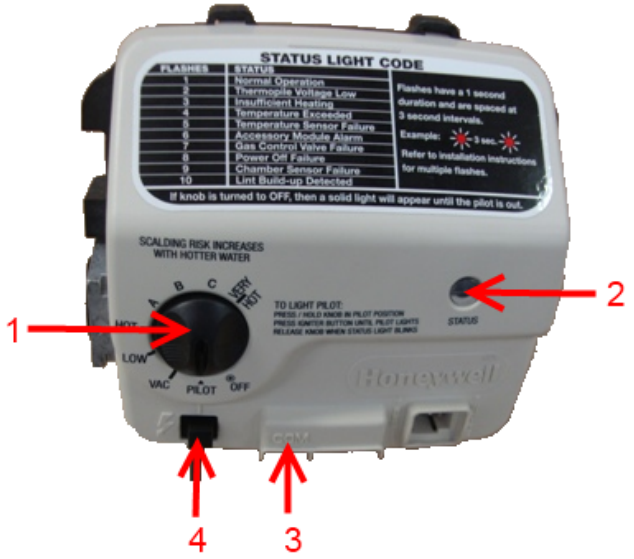
**What are our goals regarding lightweight cryptography?**

- we analyze, implement and benchmark lightweight algorithms on concrete devices to provide data necessary for a suitable algorithm selection,
- we choose algorithms for a real-world implementation for our industry partners,
- we design protocols for cryptographically secured home installations.

# Research into Lightweight Cryptography II

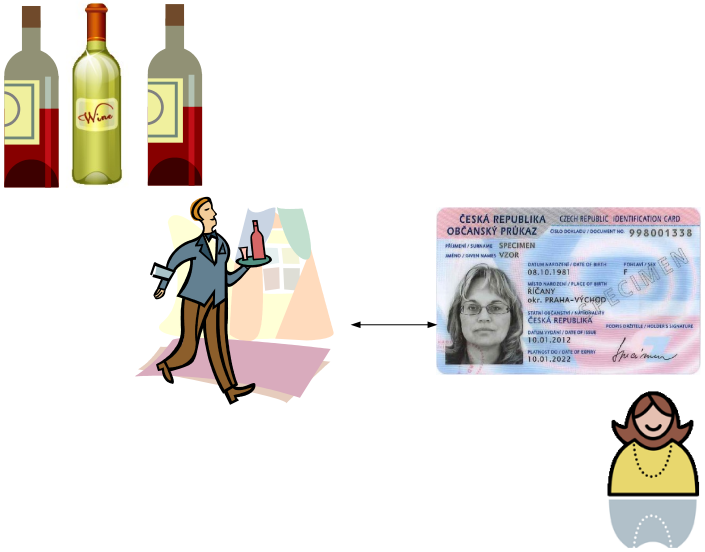
**What are our preliminary results?**

- during 2013, we analyzed existing block ciphers, implemented them on targeted hardware (MSP430F2274) and ran benchmarks,
- XTEA, IDEA, BlowFish, AES, Clefia, Present, Noekeon, RC5, RC6 and BeepBeep ciphers were benchmarked,
- codesize, memory size and speed were evaluated,
- the design of a cryptographically protected communication protocol has been started.

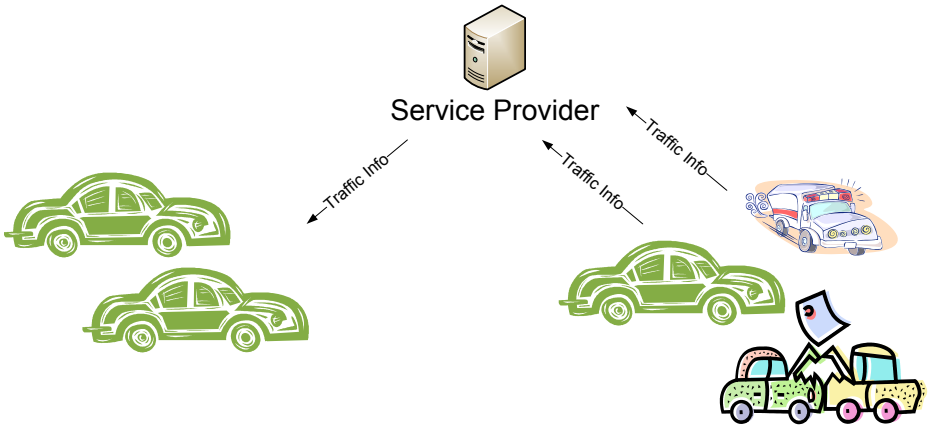


# Research into Privacy-Enhancing Cryptography - Intro

Bar scenario:
anonymous age proofs.




Car2Car scenario:
anonymous membership proofs.




SIX research centre
sensor, information and communication systems

crypto@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

# Research into Privacy-Enhancing Cryptography I

**What is "privacy-enhancing cryptography"?**

- Special algorithms and cryptographic schemes which protect personal data and digital identity.
- Cryptographic tools which protect us against digital tracing, profiling, identity thefts, personal information leaks etc.
- Applications: electronic ID (eID) cards, passports, eVoting, transportation cards, access control systems, Internet authentication, etc.
- Required by U.S. and EU institutions (NSTIC, ENISA).

**What are our goals regarding privacy-enhancing cryptography?**

- Design novel, original cryptographic protocols with better privacy protection.
- Provide new features missing in existing schemes (such as revocation).
- Implement protocols in an efficient, *practical* way.

# Research into Privacy-Enhancing Cryptography II

**Privacy-enhancing cryptography at BUT**

- **Basic research stage:**
  - design of a novel cryptographic scheme,
  - based on advanced cryptography (provable cryptography, zero-knowledge non-interactive proofs)
  - in cooperation and with consultations with University of Minnesota, USA, NIST and IBM Zurich
- **Applied research stage, implementation:**
  - implementation of protocols on smart-cards,
  - significant protocol modifications for optimization,
  - done with industry partner OKsystem.


# Research into Privacy-Enhancing Cryptography III

## Privacy-enhancing cryptography at BUT – results:

**User** | **Verifier**

$A_{seed} = g_1^{w1} g_2^{w2} g_3^{wRR} \bmod n$

$K_S \in_R \{0,1\}^l$
$A = A_{seed}^{K_S} \bmod n$
$C_1 = g_3^{K_S w_{RR}} \bmod n$
$C_2 = g_3^{K_S} \bmod n$
$r_1, r_2 \in_R \{0,1\}^{m+k+3l}$
$r_3 \in_R \{0,1\}^{m+k+4.5l}$
$r_S \in_R \{0,1\}^{m+k+l}$
$\bar{A}_{seed} = g_1^{r1} g_2^{r2} g_3^{r3} \bmod n$
$\bar{A} = A_{seed}^{r_S} \bmod n$
$\bar{C}_1 = g_3^{r3} \bmod n$
$\bar{C}_2 = g_3^{r_S} \bmod n$

$\xrightarrow{A, \bar{A}, \bar{A}_{seed}, C_1, C_2, \bar{C}_1, \bar{C}_2}$

$\xleftarrow{e \in_R \{0,1\}^k}$

$z_1 = r_1 - eK_S w_1$
$z_2 = r_2 - eK_S w_2$
$z_3 = r_3 - eK_S w_{RR}$
$z_S = r_S - eK_S$

$\xrightarrow{z_1, z_2, z_3, z_S}$

$C_1 \stackrel{?}{\neq} C_2^{rev} \bmod n$
$\bar{A}_{seed} \stackrel{?}{\equiv} A^e g_1^{z1} g_2^{z2} g_3^{z3} \bmod n$
$\bar{A} \stackrel{?}{\equiv} A^e A_{seed}^{z_S} \bmod n$
$\bar{C}_1 \stackrel{?}{\equiv} C_1^e g_3^{z3} \bmod n$
$\bar{C}_2 \stackrel{?}{\equiv} C_2^e g_3^{z_S} \bmod n$


| Hardware Specification | |
|---|---|
| Chip | SLE78CLXxxxPM |
| CPU | 16 bit |
| Int./Ext. clock | 33 MHz/7.5 MHz |
| RAM Memory | 1088+960 B |
| ROM/EEPROM | 280 kB/60 kB |
| Modular API | Yes |

# Research into Privacy-Enhancing Cryptography III

**Privacy-enhancing cryptography at BUT – results:**

- original cryptographic scheme has been designed and published,
- complex cryptographic protocols are running on off-the-shelf smart-cards,
- system is fully functional, providing users with the ability to anonymously, untraceably prove their attributes (such as age, citizenship, driving license ownership) to electronic verifiers,
- system is ready to be deployed in privacy-preserving access control systems,
- currently, only two comparable systems exist: U-Prove from Microsoft and Idemix from IBM.

# Research Results and Partners

Research Projects in 2014:

- „Cryptographic primitives for secure authentication and digital identity protection“,
- „Integration Server with Cryptographic Protection“,
- „System for Cryptographic Protection of Electronic Identity “,
- „Application of Modern Cryptographical Methods to Telematics Systems “.

Selected Recent Papers:

- Optimization of Power Analysis Using Neural Network, CARDIS 2013, Berlin, Germany, Springer LNCS.
- Unlinkable Attribute-Based Credentials with Practical Revocation on Smart-Cards, CARDIS 2012, Graz, Austria, Springer LNCS.
- Short-Term Linkable Group Signatures with Categorized Batch Verification, FPS 2012, Montreal, Canada, Springer LNCS.

Honeywell GAČR GRANTOVÁ AGENTURA ČESKÉ REPUBLIKY MINISTRY OF INDUSTRY AND TRADE Technology Agency of the Czech Republic

SIX research centre
sensor, information and communication systems

crypto@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

# Contacts

## Thank you for attention!

WWW: http://crypto.utko.feec.vutbr.cz

Email: crypto@feec.vutbr.cz

Contact Person:
Ing. Jan Hajný, Ph.D.
hajny@feec.vutbr.cz
+420 54114 6961

SIX research centre
sensor, information and communication systems