The Yin and Yang Sides of Embedded Security

Indocrypt 2011
December 12, Chennai

Christof Paar
Horst Görtz Institute for IT-Security
Ruhr University Bochum
Acknowledgement

- Tim Güneysu
- Markus Kasper
- Timo Kasper
- Gregor Leander
- Amir Moradi
- David Oswald
- Axel Poschmann
Agenda

• Some thoughts about embedded security
• Yin 1: Car crashes and ECC
• Yin 2: Bar codes and SP ciphers
• Yang 1: Routers and AES
• Yang 2: Subways and 3DES
• Auxiliary stuff
Agenda

- Some thoughts about embedded security
- Yin 1: Car crashes and ECC
- Yin 2: Bar codes and SP ciphers
- Yang 1: Routers and AES
- Yang 2: Subways and 3DES
- Auxiliary stuff
Who cares about embedded systems?

CPU market (units sold)

Q: But security?
Embedded Security – Examples

Embedded DRM applications (iTunes, Kindle, ...)

Telemedicine

Privacy & security of car2car communication

Electronic IDs and e-health cards
Research in embedded security

Western view
1. Efficient implementation
2. Secure implementation

Alternative view
1. Yin – constructive
2. Yang – destructive

The concept of yin yang is used to describe how polar opposites or seemingly contrary forces are interconnected and interdependent in the natural world, and how they give rise to each other in turn.
Agenda

• Some thoughts about embedded security
• Yin 1: Car crashes and ECC
• Yin 2: Bar codes and SP ciphers
• Yang 1: Routers and AES
• Yang 2: Subways and 3DES
• Auxiliary stuff
Making Cars Talk

- USA [NHTSA, 2010]
  33,000+ car fatalities in 2009
  2m injuries
- EU [KOM 2010 – 389]
  35,000+ car fatalities
  1.5m injuries
- 90% driver errors

→ Mechanical safety (safety belt, air bag, ABS):
  great success but limits have been reached

→ *Electronic driver assistance* will be key tool
VANET – Vehicular Ad-Hoc Networks

Broadcast position & direction information:
1. greatly improve safety
2. improve traffic management

Network characteristics
- small messages \((\approx 100 \text{ Bytes})\)
- medium frequency \((\approx 10 \text{ messages/sec per car})\)
- very ad-hoc (short lived, high dynamics)
- high number of incoming messages \( (> 1000 \text{msg/sec per car})\)
- IEEE P1609/DSRC standard

But messages must be authenticated!
(safety-critical & legislative requirements)

Key tool for authentication: digital signatures with elliptic curves ...
Elliptic Curve Primitive

- Given an elliptic curve $E$ and a point $P$
  
  $E: y^2 = x^3 + ax + b \mod p$

- Public key $Q$ is multiple of base point $P$
  
  $Q = P + P + \ldots + P = sP$

- EC discrete logarithm problem:
  
  $s = dlog_P(Q)$
Point Addition $R = P + T$

Jacobian Coordinates over $GF(p)$

- **Input** $P = (X_1, Y_1, Z_1)$; $T = (X_2, Y_2, Z_2)$
- **Output** $R = (X_3, Y_3, Z_3)$

- $A = X_1Z_2^2 \mod p$
- $B = X_2Z_1^2 \mod p$
- $C = Y_1Z_2^3 \mod p$
- $D = Y_2Z_1^3 \mod p$
- $E = B - A \mod p$
- $F = D - C \mod p$

\[
\begin{align*}
X_3 &= -E^3 - 2AE^2 + F^2 \\
Y_3 &= -CE^3 + F(AE^2 - X_3) \\
Z_3 &= Z_1Z_2E
\end{align*}
\]

1 Point Add $= 14$ MUL$_{256\text{bit}} = 3584$ MUL$_{16\text{bit}}$

Can we generate 1000+ signatures/sec with commodity hardware? (think Tara Tiny < Rs. 300,000)
Real-Time Signature Engine for VANETs

Requirements

• 256bit ECC Engine (long-term security)
• 1000 sign./sec → 1,000,000,000 Mul_{16}/sec

New VANET Signature Engine

• Idea: use DSP blocks (fast mult-and-add units) on commercial FPGAs
• 1 Mul_{256} requires 63 cycles@500MHz
• Low-cost FPGA: > 1.500 signatures/sec
• (high-end FPGA: 30.000 signature/sec)
• performance and cost-performance record for commercial hardware
Agenda

• Some thoughts about embedded security
• Yin 1: Car crashes and ECC
• Yin 2: Bar codes and SP ciphers
• Yang 1: Routers and AES
• Yang 2: Subways and 3DES
• Auxiliary stuff
Lightweight Cryptography

• “We need security with less than 2000 gates”
  Sanjay Sarma, AUTO-ID Labs, CHES 2002

• $3 trillions annually due to product piracy* (> US budget)

⇒ Authentication & identification: can both be fixed with cryptography

*Source: www.bascap.com
Strong Identification (symmetric crypto)

1. random challenge $r$
2. encrypted response $y$
3. verification
   
   $e_k (r) = y'$
   
   $y == y'$

Challenge: Encryption function $e()$ at extremely low cost
→ almost all existing ciphers not optimized for cost …
→ Q: How cheap can we make cryptography?
PRESENT – An aggressively cost-optimized block cipher for RFID

- pure substitution-permutation network
- 64 bit block, 80/128 bit key
- 4-4 bit Sbox
- 31 round (32 clks)
- secure against DC, LC
- joint work with Lars Knudsen, Matt Robshaw et al.
Resource use within PRESENT

Round-parallel implementation (1570ge)

- Registers (state + key) 55%
- Key XOR 11%
- SP Layer ("crypto") 29%
Results – PRESENT

- Smallest secure cipher
- Serial implementation approaches theoretical complexity limit: almost all area is used for the 144 bit state (key + data path)
- ISO standard pending (2012)
- “German Security Award 2010”
Agenda

• Some thoughts about embedded security
• Yin 1: Car crashes and ECC
• Yin 2: Bar codes and SP ciphers
• Yang 1: Routers and AES
• Yang 2: Subways and 3DES
• Auxiliary stuff
FPGAs = Reconfigurable Hardware

Widely used in
• routers
• consumer products
• automotive, machinery
• military

But: Copying the configuration files makes hardware counterfeiting easy!
Solution: Bitstream encryption

PCB board

SRAM FPGA

3DES⁻¹

E2PROM

Factory
Internet
Firmware Update

FPGA Design
Secret Keys
Proprietary Algorithms
IP Cores

Bitstream

3DES

Encrypted

Power-up

Attacker

? =
Let’s try side-channel analysis

- PCB board
- VCC-IO
- VCC-AUX
- Power traces
- VCC-INT
- Power-up
- E2PROM
- 3DES⁻¹
- VCC
- IO
- AUX
- INT
- design file (!)
Side-Channel Attacks (1-slide version)

- Analyze cipher
  - Find a suited predictable intermediate value in the cipher

- Measurements
  - Measure the power consumption

- Post Processing
  - Post-process acquired data

- Key Recovery
  - Perform the attack to recover the key
Our measurement set-up
Our measurement set-up
Signal acquisition
... 6 months later

key of $1^{\text{st}}$ DES

key of $2^{\text{nd}}$ DES

key of $3^{\text{rd}}$ DES
Long story made short: Decryption of “secret” designs is easy!

- Requires *single* power-up ($\approx 50,000$ traces)
- Complete 3DES key recovered with 2-3 min of computation
- Attack possible even though 3DES is only very small part of chip ($< 1\%$)
- Attack requires some experience, but
  - cheap equipment
  - easy to repeat
Implications

- Reverse engineering of design internals
- Cloning of product
- Alterations of design (chip tuning)
- Trojan hardware (i.e., malicious hardware functions)
- ...
Agenda

• Some thoughts about embedded security
• Yin 1: Car crashes and ECC
• Yin 2: Bar codes and SP ciphers
• Yang 1: Routers and AES
• Yang 2: **Subways and 3DES**
• Auxiliary stuff
Contactless Payment Cards

• Contactless card ≈ RFID + symmetric crypto

• Many security-sensitive applications
  – payment
  – passport
  – public transport
  – access control

• Security hinges on secrecy of key ...

Sources: Wikipedia, cutviews.com
**Brief history of contactless cards**

- **First generation** (since 2000 and earlier)
  Mifare Classic, Legic Prime, TI DST, Hitag, ...
  - Proprietary cipher
  - Short key
  - *Classical attacks (mathematical, brute-force)* feasible

- **Today**
  Mifare DESFire (EV1), Mifare Plus, Legic Advant, Infineon SLE, SmartMX, ...
  - 3DES & AES → secure against classical cryptanalysis
  - ?Implementation attacks?
Mifare DESFire Attack

• Strong cipher: 3DES

• Widely used: Prague, San Francisco, ...

• RFID – Power traces from EM field

⇒ High threat for real world (payment) systems
Measurement Setup

Controlling PC

Picoscope

Trigger

Reader

Near-field Probe

Contactless Smartcard

Analogue Preprocessing
**Measurement Setup**

- ISO14443-compatible
- Freely Programmable
- Low Cost (< 40 €)
Measurement Setup

- 1 GS/s, 128 MB Memory
- ± 100 mV
- USB 2.0 Interface
Trace Overview

![Graph showing voltage over time with labels for plaintext, 3DES, ciphertext, and other processing steps.](image-url)
Example: DPA-extraction of 6 key bits

S-Box 1, 150000 traces

Correlation Coefficient

Time (nsec)

x 10^5
DES Full Key Recovery
Conclusions: DESFire Attack

- **Full key-recovery** with appr. 250k traces (≈ hours)
- **Low-cost equipment**, $2500
- Opportunities for optimization

$\Rightarrow$ High threat for real world (payment) systems
Agenda

• Some thoughts about embedded security
• Yin 1: Car crashes and ECC
• Yin 2: Bar codes and SP ciphers
• Yang 1: Routers and AES
• Yang 2: Subways and 3DES
• Auxiliary stuff
Let’s look again at: Yin Yang and Crypto

The concept of yin yang is used to describe how polar opposites or seemingly contrary forces are interconnected and interdependent in the natural world, and how they give rise to each other in turn.

This seems very close to the established notion of

cryptography ↔ cryptanalysis

• Why have we (= crypto community) never talked about yin yang?
• Yin yang might make it easier to explain ethical hacking to the outside world.
Related Workshops

RFIDsec 2012
June 2012, Nijmegen, Holland

CHES – Cryptographic Hardware and Embedded Systems
September 2012, Leuven, Belgium

escar – Embedded Security in Cars
November 2012, Germany
... and yet another crypto book

- accessible (hopefully)
- quite comprehensive
- videos, slides, ...
  www.crypto-textbook.com
- flyers are outside