Performance Evaluation of AES Finalists on the High-End Smart Card

Fumihiko Sano  Masanobu Koike
Shinichi Kawamura*  Masue Shiba

System Integration Technology Center, Toshiba

*Research and Development Center, Toshiba
Contents

• Background
  – Applications of smart card
  – Platform
• Previous works
• Our contribution
  – Implementation for crypto-coprocessor
  – Performance comparison
• Conclusion
Applications of smart card

Digital cash

Smart card

Digital signature

Common key cryptosystem
  e.g. secure messaging

Encryption

DES/Triple DES

AES

replace
High-end smart card platform (JT6N55)

- Smart card
  - Frequency: 3.5~10MHz
  - 5MHz
  - Power supply: external
  - Aid multiple-precision integer arithmetic
    - Max. of Modulus 2,048-bit

- RAM: 1KB (±608B on coprocessor)
  - 512~2,048 Bytes

- ROM: 48KB
  - 20~64K Bytes

- EEPROM: 8KB
  - 8~16K Bytes

- Z80 (8-bit architecture)
  - COPROCESSOR
    - typical 8-bit or 16-bit (special 32-bit)
Previous works -- only CPU

On various 8-bit CPUs
6805, 8051, Z80, etc.
low-power, and small circuit.
They are good for smart card.

Some of AES finalists can be implemented.

Question (on high-end smart card)
High-end smart cards will be popular.
Is the coprocessor efficient for AES?

It will enhance the performance.
Implementation for coprocessor

Role of coprocessor

- Speed up multiple-precision integer arithmetic.
  - Mainly used for public key cryptosystems.
  - (e.g. modular exponentiation modulo 1,024 bits.)

new role

- Addition, multiplication, division, and logical operations.

Applying to common key cryptosystems.

The use of coprocessor reduces…

- code size,
- time for encryption and key scheduling.
Sketch

CPU

Z80

RAM

source

destination

CRYPTO COPROCESSOR

command+parameter (20～60 clocks)

write result

read src/dest

data

small

less efficient

large

efficient
Implementation

**Rules for coding**

- On-the-fly key generation, if possible.
- We use all registers on the Z80.
- No data depended branches.
  - Tamper-resistance.
- Use operations performed by the coprocessor, if efficient.
  - Previously mentioned.

**Available resources**

- ROM and RAM
  EEPROM area is used for user’s data or JAVA applets.
Comparison

Evaluation measures:

- **ROM** *(important)*
  - Most environment doesn’t have enough ROM.
  - The less ROM requirements, the more excellent.

- **RAM**
  - The high-end smart card has an enough memory.
  - It is an optional measure.

- **Speed** *(key scheduling and encryption)*
  - faster than DES?
  - faster than Triple DES?
  - better throughput than DES?
  - better throughput than Triple DES?
  - an allowable performance on specification?

**Target of speed.**

MARS, RC6, Rijndael, and Serpent: 256-bit key.
Twofish: 128-bit key (includes padding).
Comparison (ROM)

- MARS
- RC6
- Rijndael
- Serpent
- Twofish
- DES
- T-DES
- MISTY1
- E2

(bitslice estimation)
Comparison (RAM)

- MARS
- RC6
- Rijndael
- Serpent
- Twofish
- DES
- T-DES
- MISTY1
- E2

(on-the-fly?
- YES
- NO

0 100 200 300 400 500 600 (Byte)
Comparison (Time)

Minimum instruction takes 4 clocks.

(MARS)  
RC6  
Rijndael  
Serpent  
Twofish  
DES  
T-DES  
MISTY1  
E2

Minimum instruction takes 4 clocks.

depends on fixing subkey

encryption
key schedule

( msec@5MHz )
Conclusion

We report the performance of AES finalists on the high-end smart card. (8-bit CPU and crypto-coprocessor)

As small as Triple DES
- RC6
- Rijndael

Faster than Triple DES
- Rijndael
- Twofish

Remarks
- Rijndael is the most efficient algorithm on the high-end smart card.
- All finalists can be implemented on the high-end smart card.
- The performance of MARS will depend on subkeys.
- Do you need hardware? costly, lead time, ...