Open Source Implementations of Hash Functions in an Atmel AtTiny45


- Crypto 2012 rump session -
Presented by Olivier Pereira
Project goal

• Implement several algorithms
  – On the same platform (Atmel AVR AtTiny45) 😊
  – With similar guidelines, the same interface 😊
  – But different programmers 😞
Project goal

• Implement several algorithms
  – On the same platform (Atmel AVR AtTiny45) 😊
  – With similar guidelines, the same interface 😊
  – But different programmers 😞

• Why such a constrained device? (8-bit ALU, 4kB ROM, 256 RAM bytes, 32 8-bit registers)
  – Usually more challenging (e.g. need to share resources, minimize memory, ...) => interesting counterpart to existing implementations in higher-end devices
Project goal

• Implement several algorithms
  – On the same platform (Atmel AVR AtTiny45) 😊
  – With similar guidelines, the same interface 😊
  – But different programmers 😞

• Why such a constrained device? (8-bit ALU, 4kB ROM, 256 RAM bytes, 32 8-bit registers)
  – Usually more challenging (e.g. need to share resources, minimize memory, ...) => interesting counterpart to existing implementations in higher-end devices

• Main message: open source codes, available online!
Previously

• Implementations of 12 block ciphers
  – AES, DESXL, HIGHT, IDEA, KASUMI, KATAN, KLEIN, mCRYPTON, NOEKEON, PRESENT, SEA, TEA
Previously

• Implementations of 12 block ciphers
  – AES, DESXL, HIGHT, IDEA, KASUMI, KATAN, KLEIN, mCRYPTON, NOEKEON, PRESENT, SEA, TEA
• Paper presented at AFRICACRYPT 2012
Previously

• Implementations of 12 block ciphers
  – AES, DESXL, HIGHT, IDEA, KASUMI, KATAN, KLEIN, mCRYPTON, NOEKEON, PRESENT, SEA, TEA

• Paper presented at AFRICACRYPT 2012

• Source codes at the following address:

http://tinyurl.com/openciphers
Previously

- Implementations of 12 block ciphers
  - AES, DESXL, HIGHT, IDEA, KASUMI, KATAN, KLEIN, mCRYPTON, NOEKEON, PRESENT, SEA, TEA
- Paper presented at AFRICACRYPT 2012
- Source codes at the following address: http://tinyurl.com/openciphers
- New contributions still welcome!
New results

• Implementations of 17 hash functions
New results

• Implementations of 17 hash functions
• In three “categories”
  – SHA256 and the SHA3 candidates
  – Lightweight hash functions
  – Block cipher based constructions
New results

• Implementations of 17 hash functions
• In three “categories”
  – SHA256 and the SHA3 candidates
  – Lightweight hash functions
  – Block cipher based constructions
• Work in progress, many source codes already available:

http://tinyurl.com/openhash
For example: code size x cycle count (be aware of different scales!!!)
THANKS!

More benchmarking on the website
http://tinyurl.com/openhash

Full paper to appear...