Side Channel Analysis of AVR XMEGA

Ilya Kizhvatov

UNIVERSITÉ DU LUXEMBOURG

CHES 2009 Rump Session
AVR XMEGA

8-bit RISC µC with the AVR core released by Atmel in 2008 awarded product of the year by Electronic Products Magazine promising set of features

- 4-channel DMA
- Inter-peripheral event system
- ADC/DAC, EBI, SPI, TWI, PDI, WDT, IRCOM, AWeX, . . .
- Advanced clocking options (PLL, DFLL)
- Low power consumption

- Symmetric crypto engines: DES, AES

Available over-the-counter for <10 USD apiece

Applications: sensors, ZigBee, wireless encryption, networking

Reported use by [Rhode et al. CARDIS’08], [Eisenbarth et al. CHES’09]
AVR XMEGA

- 8-bit RISC μC with the AVR core
AVR XMEGA

- 8-bit RISC μC with the AVR core
- released by Atmel in 2008
AVR XMEGA

- 8-bit RISC μC with the AVR core
- released by Atmel in 2008
- awarded product of the year by Electronic Products Magazine
AVR XMEGA

- 8-bit RISC μC with the AVR core
- released by Atmel in 2008
- awarded product of the year by Electronic Products Magazine

- promising set of features
  - 4-channel DMA
  - inter-peripheral event system
  - ADC/DAC, EBI, SPI, TWI, PDI, WDT, IRCOM, AWeX, ...
  - advanced clocking options (PLL, DFLL)
  - low power consumption
AVR XMEGA

- 8-bit RISC µC with the AVR core
- released by Atmel in 2008
- awarded product of the year by Electronic Products Magazine

- promising set of features
  - 4-channel DMA
  - inter-peripheral event system
  - ADC/DAC, EBI, SPI, TWI, PDI, WDT, IRCOM, AWeX, ...
  - advanced clocking options (PLL, DFLL)
  - low power consumption

- symmetric crypto engines: DES, AES
AVR XMEGA

- 8-bit RISC μC with the AVR core
- released by Atmel in 2008
- awarded product of the year by Electronic Products Magazine

- promising set of features
  - 4-channel DMA
  - inter-peripheral event system
  - ADC/DAC, EBI, SPI, TWI, PDI, WDT, IRCOM, AWEx, ...
  - advanced clocking options (PLL, DFLL)
  - low power consumption

- symmetric crypto engines: DES, AES
- available over-the-counter for <10 USD apiece
AVR XMEGA

- 8-bit RISC μC with the AVR core
- released by Atmel in 2008
- awarded product of the year by Electronic Products Magazine

- promising set of features
  - 4-channel DMA
  - inter-peripheral event system
  - ADC/DAC, EBI, SPI, TWI, PDI, WDT, IRCOM, AWEx, . . .
  - advanced clocking options (PLL, DFLL)
  - low power consumption

- symmetric crypto engines: DES, AES
- available over-the-counter for <10 USD apiece
- applications: sensors, ZigBee, wireless encryption, networking
AVR XMEGA

- 8-bit RISC \( \mu \)C with the AVR core
- released by Atmel in 2008
- awarded product of the year by Electronic Products Magazine

- promising set of features
  - 4-channel DMA
  - inter-peripheral event system
  - ADC/DAC, EBI, SPI, TWI, PDI, WDT, IRCOM, AWeX, ... 
  - advanced clocking options (PLL, DFLL)
  - low power consumption

- symmetric crypto engines: DES, AES
- available over-the-counter for \(<10 \) USD apiece
- applications: sensors, ZigBee, wireless encryption, networking
- reported use by [Rhode et al. CARDIS’08], [Eisenbarth et al. CHES’09]
XMEGA Crypto Engines

**DES Instruction**
- performs single DES round
- full DES in 17 clock cycles

**AES Peripheral**
- AES-128 in **375** clock cycles (vs. 3-4K cycles in software)
- around **10 Mbps** bandwidth at maximum clock speed
- DMA transfer triggering, support for CBC mode

What about resistance to implementation attacks?
No single word about countermeasures in the datasheet or anywhere else.
XMEGA Crypto Engines

DES Instruction
- performs single DES round
- full DES in 17 clock cycles

AES Peripheral
- AES-128 in 375 clock cycles (vs. 3-4K cycles in software)
- around 10 Mbps bandwidth at maximum clock speed
- DMA transfer triggering, support for CBC mode

What about resistance to implementation attacks?
- no single word about countermeasures in the datasheet or anywhere else
Side-Channel Attack on XMEGA AES Engine

![Image of oscilloscope and circuit board]

![Graphs showing data over clock cycle and N values]

- Clock cycle vs. ρ
- N vs. ρ
Side-Channel Attack on XMEGA AES Engine

Attack details

- CPA in HD leakage model
- **3000 power traces** for full 128-bit key recovery
- 100 MS/s sampling rate
- setup cost $\approx$ $1000
- reveals that implementation is not parallel
Take care when using XMEGA crypto features

http://cryptolux.org/Implementation_attacks