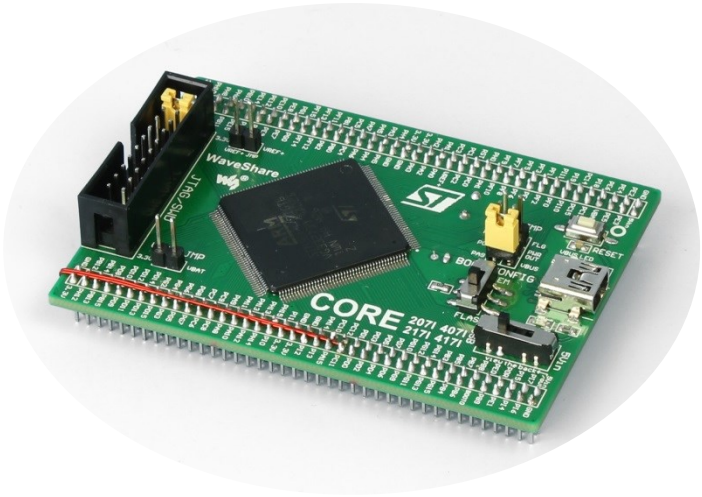
Piñata board



What is the Piñata board?

The Piñata board is a development board based on an ARM Cortex-M4F core working at a 168MHz clock speed. The board has been physically modified and programmed in order to be a training target for passive Side Channel Analysis (SCA) attacks such as Differential Power Analysis (DPA) or active Fault Injection attacks such as Differential Fault Analysis (DFA). Additionally, the source code and IDE is provided in order to allow users to extend the functionality of the board and use it as a development/prototyping board.

Main board features

- 1Mbyte internal FLASH memory, 196 Kbytes internal SRAM. Firmware updateable by user.
- Floating point unit for single-precision arithmetic
- I/O interfaces: 6x UART, 3x SPI, 3x I2C, 2x CAN, serial over USB, Ethernet, 140x GPIO pins
- External memory controller for NAND/NOR FLASH, SRAM, PSRAM, CF
- True Random Number Generator (TRNG)
- Hardware crypto engine for DES, TDES, AES, hashing (MD5, SHA1) and HMAC. This option is only available in the hardware-crypto enabled model of the board.
- Customized for performing easily SCA and FI attacks.
- Integrated with Inspector SCA and Inspector FI software.

Cryptographic implementations present in the board

- DES: software, hardware
- AES-128: software, hardware, 32 bit T-tables software
- TDES: hardware
- RSA: decryption, 1024 bit CRT software implementation

Package contents

- Piñata board
- Piñata board manual
- MiniUSB cable + Serial to USB cable
- Software package with open source IDE + board source code

Attacks possible on the target (training available on request)

Side Channel Analysis (SCA)

- Simple Power Analysis (SPA)
- Differential Power Analysis (DPA)
- Differential EM Analysis (DEMA)

Fault Injection (FI)

- VCC Fault Injection
- EM Fault Injection
- Optical Fault Injection
- Boot glitching

Sample from the manual: Software DES

Software DES – Encrypt (0x44)

Command description: the board will perform a DES encryption of the message contained in the command payload (8 bytes). The cipher is executed in Electronic Code Book (ECB) mode. DES implementation is performed with byte operations. DES S-boxes are implemented in order (S-box 1 to S-box 8).

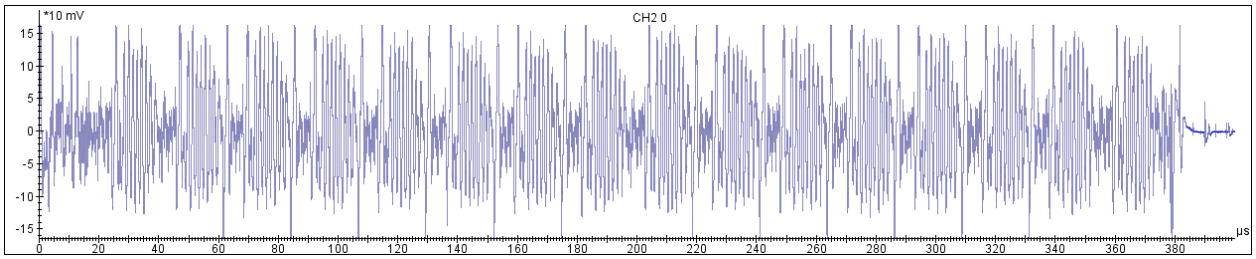
Default DES key: 0xCAFEBABEDEADBEEF

Command byte: 0x44

Payload length: 8 bytes

Response length: 8 bytes

Power trace capture for time reference (3.3V input, measured with Riscure Current Probe):



Interesting time ranges for SCA and FI attacks:

(f=168MHz, trigger signal **PC2** 1V threshold level, typical values)

DPA: 1st and 2nd round → contained in the range [20, 66] us after rising edge in **PC2** trigger signal

DFA: 14th and 15th round → [308, 360] us after rising edge in **PC2** trigger signal

Suitable model for SCA: this implementation leaks the hamming weight of the S-Box output values

Contact information

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90
www.riscure.com

Riscure North America
550 Kearny St.
Suite 330
San Francisco, CA 94108
+1 (650) 646 9979
inforequest@riscure.com