Breakthrough silicon scanning discovers backdoor in military chip

Sergei Skorobogatov, Christopher Woods

http://www.cl.cam.ac.uk/~sps32

email: sps32@cam.ac.uk

http://www.quovadislabs.com

email: chris@quovadislabs.com

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Introduction

- Many semiconductor devices are vulnerable to attacks
  - theft of service
  - gaining access to information (IP, data, ID)
  - cloning and overbuilding
  - denial of service
- How secure is the design?
  - What security features are implemented?
  - Who has access to the design?
  - How easy is it to modify the design or add extra capabilities?
  - How is the integrity of the design verified?
- Hardware security challenges
  - keys and passwords storage
  - get design engineers educated on security
  - developing countermeasures
  - patching the holes

Introduction

- Hardware Assurance (HWA) concerns
  - ensuring hardware has not been manipulated
  - industry dependence on limited fabs and design templates
- Trojans and backdoors
  - production outside of chip manufacturers' control
  - most devices are produced in Asia
  - recognised problem but no ultimate solution in place
- Cloned or counterfeit parts
  - verify design integrity
  - identify the source of production
  - test quickly in assembly line before use
- Research with responsible disclosure of findings
  - prevents dishonest exploitation of security vulnerabilities
  - allows chip manufacturers to implement countermeasures

Trojan, Backdoor or Feature?

- Trojans are normally introduced by adversaries
  - post design insertion but before production
  - modifying production masks at chip foundry
- Backdoors are expected to be introduced by contractors
  - third party libraries and designs
  - design engineer
  - deliberate insertion made by the design house
- Undocumented features are inserted by many chip vendors
  - used for factory testing and debugging
- Outsider attacker cannot distinguish between those options
  - analyses the device as a black box
  - usually very limited information is provided about low-level features
  - some form of reverse engineering is usually required
  - *"backdoor – an undocumented way to get access to a computer system or the data it contains"*

Find ideal research target

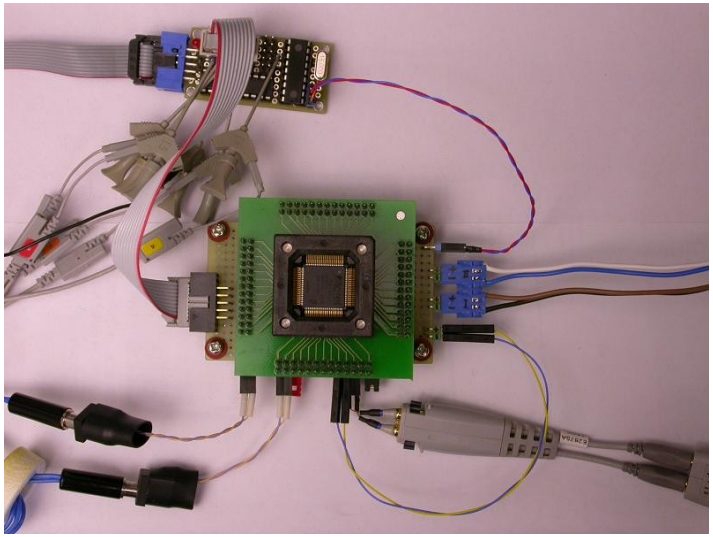
- Requirements
  - available samples and development tools without restrictions
  - high security specifications by manufacturer
  - use in military and critical infrastructure
  - FPGA vs microcontroller
  - SRAM FPGAs offer low security, tougher challenge for Flash FPGA
- *´Highly secure´* Actel/Microsemi ProASIC3 Flash FPGAs
  - *“offer one of the highest levels of design security in the industry”*
  - *“having inherent resistance to both invasive and noninvasive attacks on valuable IP”*
  - used in military applications according to the manufacturer
  - used in sensitive industrial applications
    - automotive, avionics and space industry
    - medical equipment
    - power plants
    - critical infrastructure

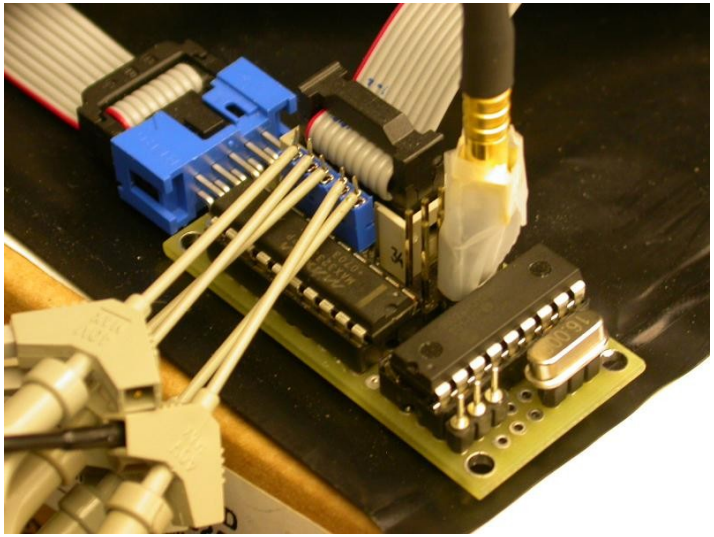
Actel/Microsemi Flash FPGA

- ProASIC3 Flash-based A3P250 FPGA
  - FPGA Array, user FROM, user UROW, AES key, Passkey, configuration fuses
  - JTAG interface to configure the chip
  - 0.13µm process with 7 metal layers
  - "*The contents of a programmed ProASIC3 device cannot be read back, although secure design verification is possible.*"
- Access via JTAG interface
  - no documentation available on JTAG commands
  - development kits and tools are available
  - STAPL programming file is generated by design software
  - bitstream configuration commands: Erase, Write, Verify

Experimental setup

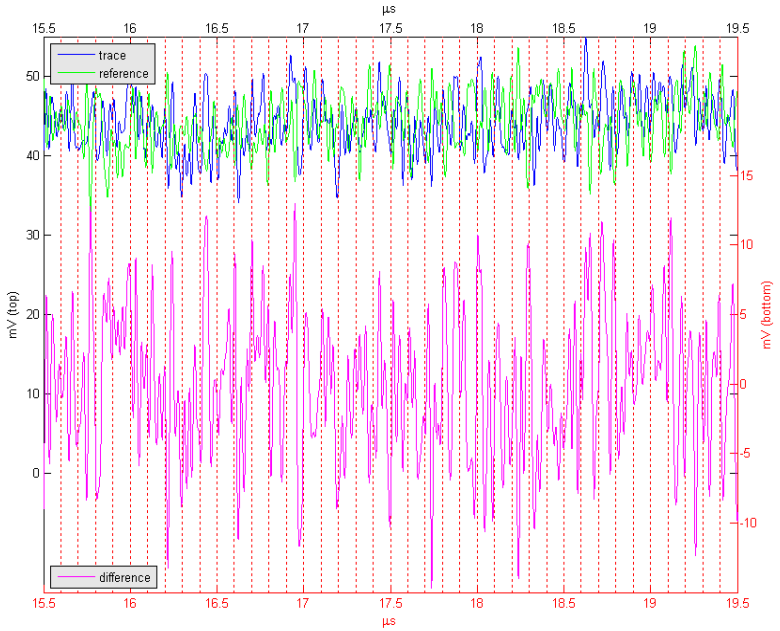
- A3P250 chip in ZIF test socket on a test board
- control board with 40MIPS PIC24 microcontroller
- DPA analysis setup with A3P250 chip in test socket, 20Ω resistor in V_{CC} and 1130A differential probe
- Agilent MSO8104A oscilloscope and Matlab software for analysis of acquired power traces

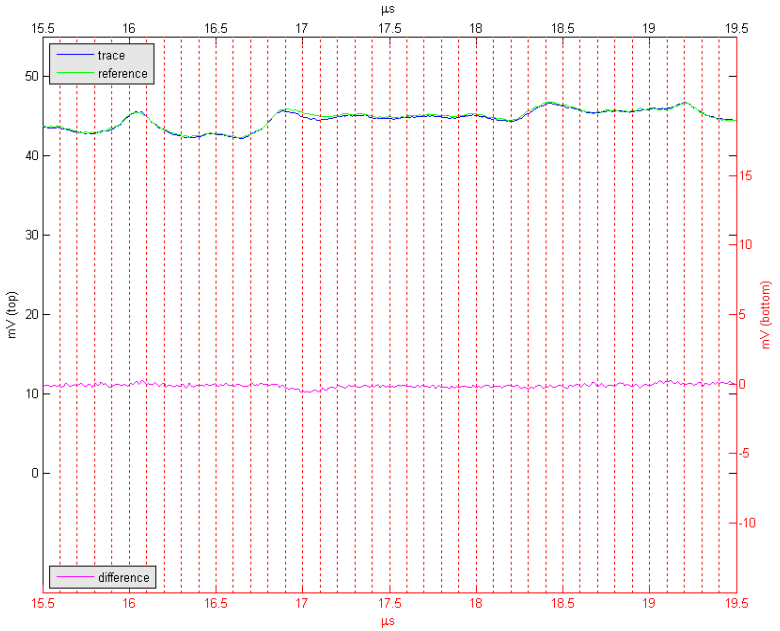




Results

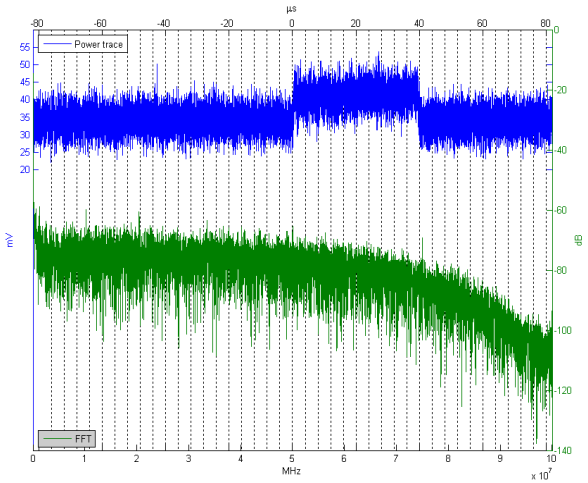
- Power analysis on different JTAG operations
  - high noise in the power traces (SNR of –20dB)
  - long averaging is required to distinguish single bit of data (Av=4096)
  - AES 128-bit key extraction takes over an hour to succeed

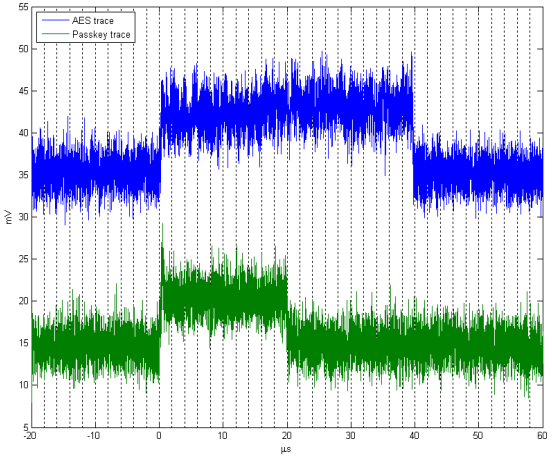


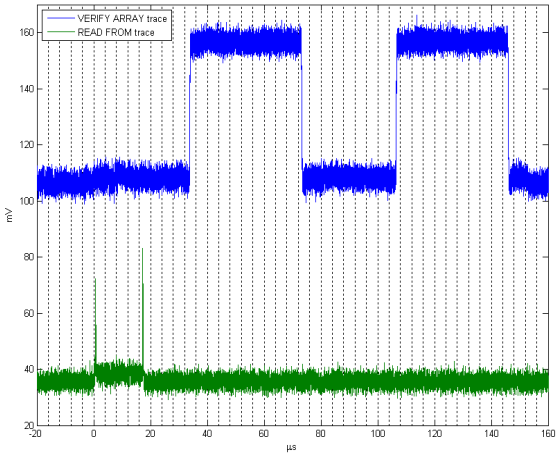


Results

- Simple power analysis to distinguish between commands
  - high noise in the power traces and no specific bandwidth to filter
- AES vs Passkey (bitstream encryption and user access)
- Array verify vs FROM reading
- Additional hidden functions were found, but their unlocking required a key with similar to passkey protection
- DPA attack on passkey with off-the-shelf equipment would require hundreds of years to succeed

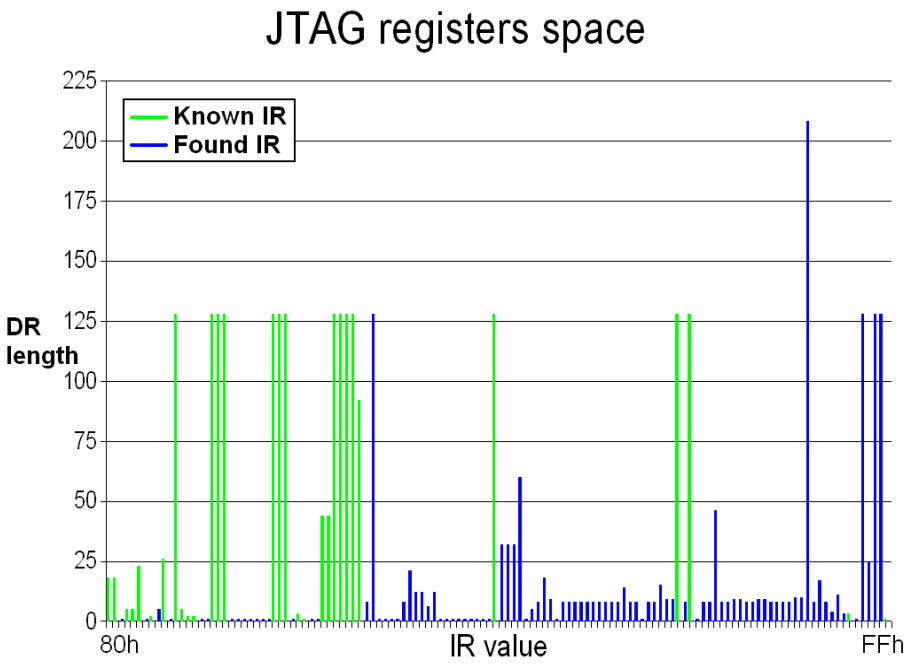


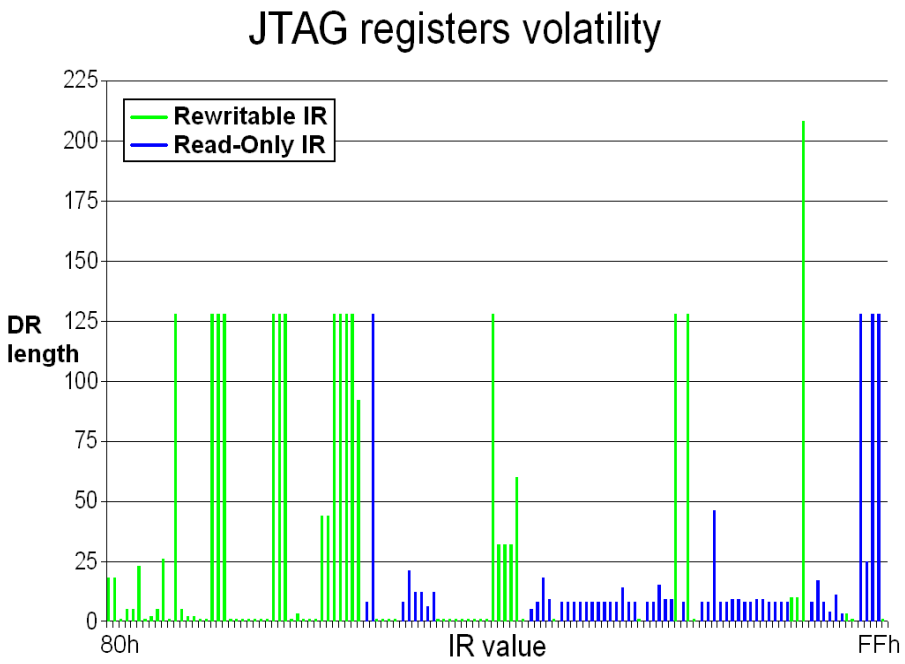




Results

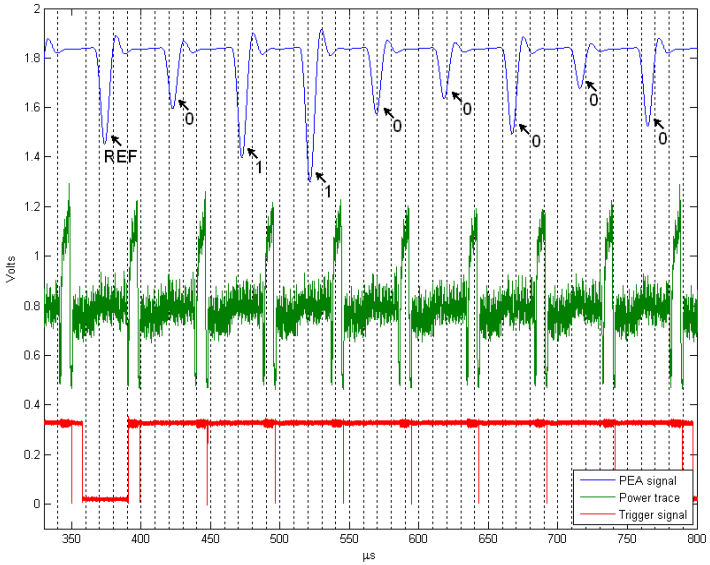
- Scanning JTAG for command space
  - find depth of DR registers associated with each command
  - test if those DR registers can be amended
- Analysing STAPL programming file from design software
  - hints on unused spaces





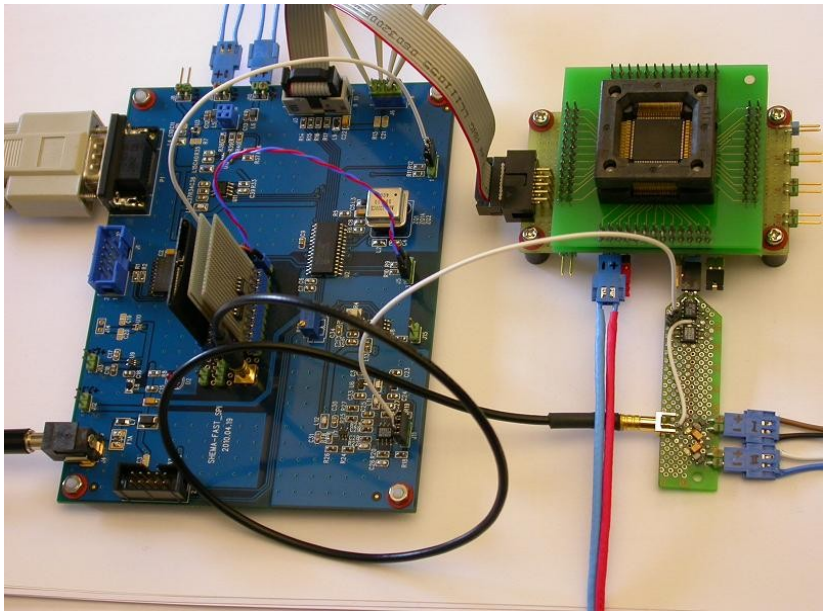
Improvements

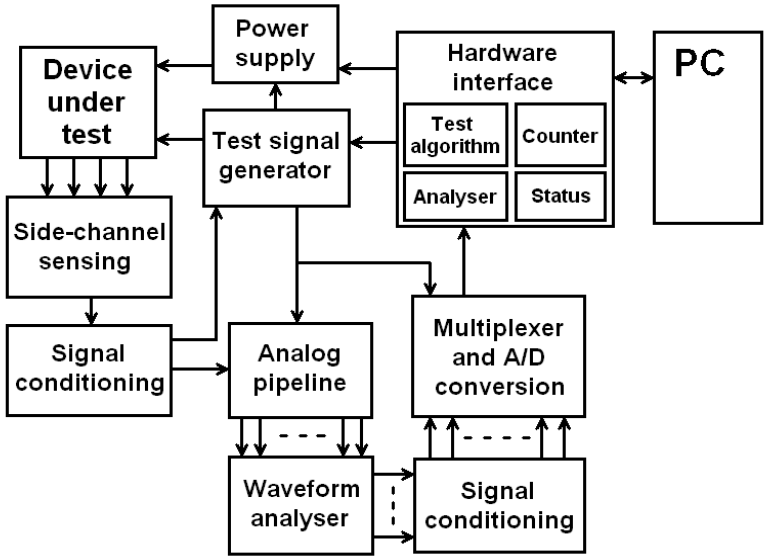
- New side-channel analysis technique which proved to be effective for AES key extraction from ProASIC3 devices
  - down to 0.01 second time vs over 1 hour with off-the-shelf DPA
  - S. Skorobogatov, C. Woods: In the blink of an eye: There goes your AES key. IACR Cryptology ePrint Archive, Report 2012/296, 2012. http://eprint.iacr.org/2012/296
- Pipeline emission analysis (PEA) technique improves SCA
  - dedicated hardware rather than off-the-shelf equipment
  - lower noise, higher precision, low latency, fast processing



Experimental setup

- Same ProASIC3 A3P250 chip on the test board
- Dedicated hardware for waveform analysis using patented PEA technique
  - same measurement resistor in V_{CC} core supply line
  - analog waveform conditioning and pre-processing before the ADC
  - cost of components below $100 USD



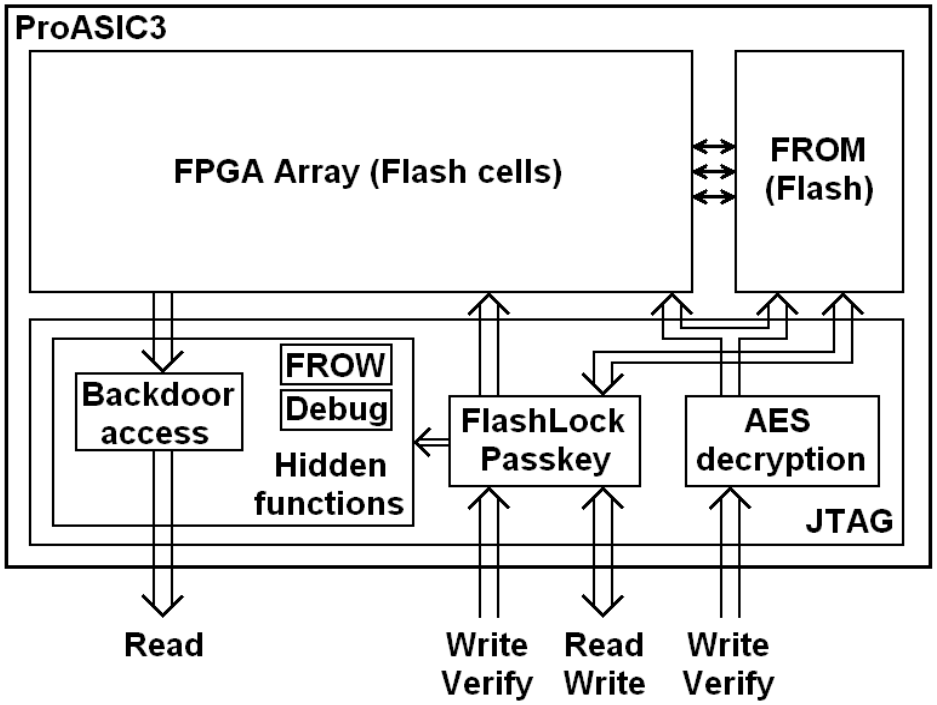


Results

- For both backdoor key and passkey the extraction time of 32 hours was achieved compared to estimated 2000 years required with an off-the-shelf DPA setup
- Backdoor key unlocks additional undocumented functionality (factory test and debug mode), but does not automatically allow readback of the design IP
- Additional reverse engineering of the control registers bit fields was required and this was made using PEA technique
- Is this Backdoor or Trojan?
  - STAPL file contains some characteristic variable names associated with security fuses
  - searching for those names in the installed Actel Libero design software under Windows XP using Search option. This returns some templates and algorithm description files
  - inside some of those files there are traces of the designed backdoor

Simplified ProASIC3 security

- AES encryption engine can only send data in one direction
- Passkey only unlocks FROM readback
- Hidden JTAG functions include different areas
  - factory settings, debug features and control registers
  - no references were found in their tools or documentation that readback of the design was a possibility



Testing security levels

- Security with no readback is not the only one in ProASIC3
  - passkey access protection
  - AES encryption
  - security fuses
  - permanent lock
- Evaluated against Non-invasive and Semi-invasive attacks
  - brute forcing, glitching, bumping, side-channel emission
  - optical fault injection, optical emission analysis

Secure area	Read access	Verify access	Write access	Secure lock	AES crypto	Expected security	Attack time
FROM (Flash)	Yes	Yes	Yes	Yes	Yes	Medium	Hours
FPGA Array	No	Yes	Yes	Yes	Yes	High	Days
AES key	No	Yes	Yes	Yes	No	Medium	Seconds
Passkey	No	Yes	Yes	Yes	No	Very high	Hours
Backdoor key	No	Yes	Yes	Yes	No	Very high	Hours
Permanent lock	No	No	Yes	No	No	Ultra high	Minutes

Implications and countermeasures

- All findings are applicable to other 3rd gen Flash FPGAs
  - Igloo
  - Fusion
  - SmartFusion
- Same devices usually share the same keys and passkeys
- Cryptography does not always help to deter the attackers
- Sensitivity of the hardware setup can be improved
- More complex circuits will require more time for analysis
- Further testing is needed to estimate the attack time if DPA countermeasures are present
- Restricting physical access to the device will always help provided there is no remote update capabilities used

Improvements

- Backdoor readback is not the only way of IP extraction
  - optical fault injection allows IP extraction by masking Verify operation
    - Sergei Skorobogatov: Flash Memory 'Bumping' Attacks. CHES 2010, Santa Barbara, USA, August 2010. Springer-Verlag, LNCS 6225, ISBN 3-642-15030-6, pp 158–172
  - non-invasive bumping with glitch attacks can be used as well
- Knowledge of the AES key paves the way to extract the IP
  - if encrypted communication is allowed an attacker can authenticate himself to the device and perform Erase, Write and Verify commands
  - overwriting is permitted only in one direction: 1 –> 0
  - all but a small number of bits in the memory row can be masked and the remaining bits brute forced with Verify command (2ms)
  - arbitrary writing in encrypted mode is protected with MAC, but it has relatively low security; it can even be defeated by modifying the STAPL programming file

Improvements

- Test previously erased chip for configuration data extraction
  - exploits data remanence effect of Flash memory
    - Sergei Skorobogatov: Data Remanence in Flash Memory Devices. CHES 2005, Edinburgh, UK, September 2005. Springer-Verlag, LNCS 3659, ISBN 3-540-28474-5, pp 339–353
  - use the backdoor findings to unlock JTAG registers responsible for adjustment of the V_{REF} of Flash Array read sense amplifiers
- Quick data recovery method (99% accuracy)
  - set V_{REF}<min(V_{TH}) to flip all bits to '1'
  - increase V_{REF} and note the point of the 1st '0' bit and the last '0' bit
  - set V_{REF} to the middle point and read out the correct configuration
- Reliable recovery method (100% accuracy)
  - set V_{REF}<min(V_{TH}) to flip all bits to '1'
  - increase V_{REF} until any bits change and assign V_{REF} for all bits
  - perform an extra erase operation and repeat V_{REF} assignments
  - larger change in V_{REF} will correspond to '0' bits

Future work

- Using PEA for finding cloned and counterfeit parts
  - obtaining characteristic parameters for legitimate and counterfeit parts for later quick detection before placing into real system
  - developing reliable, fast and automated algorithms for scanning
  - improving hardware setup for better sensitivity, lower noise and higher performance
- Improving PEA performance with more pipelines, better hardware design and more efficient analysis algorithms
- Testing other chips with DPA countermeasures using PEA
- Using semi-invasive attacks for backdoor evaluation
  - S. Skorobogatov: Optically Enhanced Position-Locked Power Analysis. CHES 2006, Yokohama, Japan, October 2006. Springer-Verlag, LNCS 4249, ISBN 3-540-46559-6, pp 61–75
  - S. Skorobogatov: Using Optical Emission Analysis for Estimating Contribution to Power Analysis. FDTC 2009, Lausanne, Switzerland, September 2009. IEEE-CS Press, ISBN 978-0-7695-3824-2, pp 111–119

Conclusion

- Hardware assurance is vital as Trojans/backdoors could be present in many semiconductor devices
- Chip manufacturers face a big challenge in finding the right balance between failure analysis requirements and security
- PEA technique significantly improves the speed of silicon scanning
- Tendency of having more devices plugged into networks and being accessible via the Internet could permit possibility of a large scale remote attack
- Patching hardware and especially silicon chips is expensive and time consuming process
- A security related backdoor present on a silicon chip jeopardises any efforts of adding software level protection
- How many other chips have a backdoor or additional and undocumented factory test/debug functionality?