In the blink of an eye: There goes your AES key

(DRAFT of 28 May 2012)

Sergei Skorobogatov
University of Cambridge
Cambridge, UK
e-mail: sps32@cam.ac.uk

Christopher Woods
Quo Vadis Labs
London, UK
e-mail: chris@quovadislabs.com

***Abstract*—This paper is a short summary of a real world AES key extraction performed on a military grade FPGA marketed as 'virtually unbreakable' and 'highly secure'. We demonstrated that it is possible to extract the AES key from the Actel/Microsemi ProASIC3 chip in a time of 0.01 seconds using a new side-channel analysis technique called Pipeline Emission Analysis (PEA). This new technique does not introduce a new form of side-channel attacks (SCA), it introduces a substantially improved method of waveform analysis over conventional attack technology. It could be used to improve upon the speed at which all SCA can be performed, on any device and especially against devices previously thought to be unfeasible to break because of the time and equipment cost. Possessing the AES key for the ProASIC3 would allow an attacker to decrypt the bitstream or authenticate himself as a legitimate user and extract the bitstream from the device where no read back facility exists. This means the device is wide open to intellectual property theft, fraud and reverse engineering of the design to allow the introduction of a backdoor or Trojan. We show that with a very low cost hardware setup made with parts obtained from a local electronics distributor you can improve upon existing SCA up to a factor of x1,000,000 in time and at a fraction of the cost of existing SCA equipment.**

Keywords: AES Key extraction; Side-channel analysis; FPGA bitstream encryption; Power analysis; PEA technique

I. Introduction

Since the introduction of differential power analysis (DPA) in 1999 [1] researchers have been trying to improve the effectiveness of side-channel attacks (SCA) using sophisticated algorithms and techniques [2][3][4][5][6]. A classical DPA setup has several drawbacks. It results in a significant noise level that makes detecting key leaking parts of the signal virtually impossible, even with averaging. Some attempts were made in the past to address a number of issues, for example, an active current measurement technique was introduced in 2008 [7]. In most cases the improvement in signal detection was achieved by acquiring a vast number of samples, often reaching many millions for high-end devices. Our aim was to improve the hardware setup in order to simplify the measurements and allow decision making to be more straightforward.

In a search of the ideal target we decided to test the Actel/Microsemi ProASIC3 (PA3) A3P250 device [8] because of its high security specifications and wide use in military and industrial applications. Most PA3 devices offer the ability to encrypt the configuration bitstream and the internal Flash memory with an AES-128 key. This prevents a potential attacker from obtaining any unencrypted information because the decryption takes place inside the PA3 silicon with secure AES key storage. Actel, who developed this feature in PA3 devices market them as chips which *'offer one of the highest levels of design security in the industry'* [9][10]. Although not having any specialised DPA countermeasures, these devices are at least 100 times harder to attack using DPA than non-protected conventional microcontrollers such as PIC, AVR, MC68HC, MSP430 etc. For example, AES key from AVR XMega can be extracted within minutes [11]. The robust hardware design features are complemented with the total lack of information about JTAG engine operation, hardware implementation and commands. That makes any attacks on AES in PA3 quite a challenging task.

The danger of AES key extraction from PA3 devices should not be underestimated. It could not only lead to decrypting the configuration bitstream from a firmware update, leading to cloning and overbuilding, but a potential attacker could authenticate himself to the FPGA device and either erase it or physically destroy it by uploading a malicious bitstream that will cause a high current to pass through the device and burn it out. Ultimately, an attacker can extract the intellectual property (IP) from the device as well as make a number of changes to the firmware such as inserting new Trojans into its configuration. This would give an attacker several options to carry out more sophisticated attacks at a later stage.

By compromising AES key in PA3 the IP could be extracted even without access to the encrypted bitstream. Attacker can pass authentication, then write arbitrary data masking all but say 16 bits in a 832-bit row. Since each row can be verified independently in 2 ms time he can brute force unknown bits row by row. With 50 samples we extracted full IP from A3P250 in 1 week. There is a message authentication code (MAC) security feature to prevent arbitrary writing in AES mode through validation of data. We broke it figuring out that it uses feedback-shift register (FSR) with just 4 bits of uncertainty per AES CBC (cipher-block chaining) block and easily bruteforceable off-line. Moreover, we managed to disable the MAC verification by modifying few lines in the controlling STAPL file [12] making arbitrary writing seamless.

This paper is organised as follows. Section 2 gives a brief introduction into side-channel analysis of cryptographic devices. Section 3 introduces the experimental setup, while Section 4 sets out our results. Section 5 discusses limitations and possible improvements. The impact of the research is discussed in the concluding section.

II. Background

Most digital circuits built today are based on CMOS technology, using complementary transistors as basic elements. When a CMOS gate changes its state, it charges/discharges a parasitic capacitive load and causes a dynamic short circuit of the gate. The more gates that change their state, the more power is dissipated. The current consumed by a circuit can be measured by placing a 10 Ω to 50 Ω resistor in the power supply line, usually a ground pin, because an ordinary oscilloscope probe has a ground connection.

Drivers on the address and data bus consist of many parallel inverters per bit, each driving a large capacitive load. During transition they cause a significant power surge, up to 1 mA per bit, which is sufficient to enable a modern digital storage oscilloscope to detect the number of bus bits changing at a time. By averaging the measurements of many repeated identical operations, smaller transitions can be identified. Of particular interest for attacking cryptographic algorithms is observing the number of bits changing at a time (Hamming distance model) and the number of bits that are set to one (Hamming weight model). Each type of instruction executed by a CPU causes different levels of activity in the instruction decoder and arithmetic unit, therefore instructions can often be quite clearly distinguished, such that even parts of algorithms can be reconstructed.

When referring to SCA, it is usually assumed they take the form of power analysis attacks. There is another type of SCA called electro-magnetic analysis (EMA) [2]. Instead of measuring the current through a device, these measure electro-magnetic emissions in the form of an electric or magnetic field. Sometimes more information is gained by placing the probe closer to the area of interest and thus reducing the signal from unwanted areas.

There are two major techniques in power analysis – simple power analysis (SPA) and differential power analysis (DPA). Both were introduced by Kocher et al in 1999 [1]. In SPA the power trace acquired with an oscilloscope is directly interpreted in order to understand the internal operation or to extract the key or password. However, some knowledge about the device functionality is usually required to do this. DPA attacks do not require detailed knowledge of the device operation, instead the information is extracted from an analysis of the statistical correlation between the input data and key bits.

The main obstacles for DPA and other attacks is the noise that affects the quality of traces. This noise is present in different forms, from the electronic noise of the power supply and clock generator to noise from surrounding on-board components and other parts of the chip circuit. When it comes to the measurement setup, the measurement resistor and acquisition equipment compound the existing noise. The oscilloscope introduces all sorts of different noises from its active probes, input pre-amplifiers and analog-to-digital converters to quantisation noise of the conversion itself.

To protect cryptographic and data sensitive devices from SCA many countermeasures were introduced over the past decade. They are aimed at making any analysis more difficult by suppressing the useful leakage and/or introducing additional noise to the emission. The first can be achieved at the silicon level by balancing the signal with additional circuits as in dual-rail or pre-charge logic [3]. However, this comes at the cost of silicon size which becomes three or four times larger. The noise can be introduced at a lower cost by inserting dummy cycles into program flow, resulting in an internal clock generator with a very large and unpredictable jitter, or by adding noisy components to the silicon such as charge pumps and clock switches.

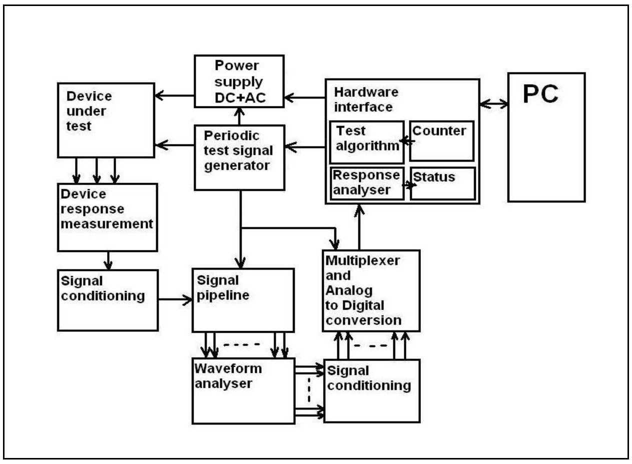


Figure 1. Block diagram of the PEA technique setup.

A logical step to increase the sensitivity of any SCA setup is to increase the speed at which results can be processed and analysed. It is perplexing in our opinion that no one has introduced a hardware platform dedicated to this task since the introduction of DPA. That is why PEA was developed, to deal with the inherent latency and noise of current DPA setups. In this case, PEA can deal with any noise issues in a way that current DPA setups never can.

The system consist of a control interface that can be represented by a personal computer, remote control with embedded processor or other human interface (Figure 1). The test algorithm is either present inside the test generator or it is supplied via the control interface. Each device under test (DUT) requires its own test algorithm which is a part of a standard device operation and consists of a list of commands to run the DUT in the way required by the tester, for example, to establish an authentication or to decrypt the data. The test signal generator produces sets of test patterns according to the programmed algorithm, the signals can be both analog and digital and determined by the DUT specification. One part of the algorithm is fixed while the other is changing. The power supply of the DUT is provided by programmable power supply which can produce both DC and AC power sources. The clock of the AC source can be synchronised to the external clock provided by the signal generator which in turn can be synchronised to the device's internal clock. This is done by injecting the clock signal from the generator into the DUT power supply line. That allows significant improvement over existing measurement equipment setup by significantly reducing the jitter influence on the measurement results.

As the device under test performs some requested operation it leaks some information via channels. A side-channel is an information emitted as a side effect of the device operation. This includes but not limited to time variations, heat dissipation, noise, electromagnetic emission, power consumption and optical emission. Those side-channel responses are measured with dedicated sensors specific for each type of side-channel emission. The sensors output the signals in analog form which then put through signal conditioning circuit to amplify the signal and reduce the noise by applying various filters. The plural results signal conditioning module provides input to an analog signal pipeline whose data are delayed by one clock period, the clock period being determined by the test signal generator. The purpose of the delay is to be able to compare the device side-channel response to different input test data. The pipeline delivers its delayed output to a waveform analyzer which compares the new signal with the delayed signal for the determined number of points and provides an output which is the difference there between.The signal from the analyser is conditioned using amplifiers and filters to meet the requirement of the acquisition system which then convert it in multiplexed way into digital form. The output of the multiplexer is then transferred to the hardware interface. The response analyser makes the decision on the reply based on the predetermined decision making patterns and update the status register which is checked by the control system in a form of PC or other human interface. Our invention of the new analysis technique is covered by patent which is available to public [13].

Our improvement comes from: real-time attack with no latency associated with oscilloscope hardware/software, network and memory; lower noise with better probe design, analog signal processing and efficient filtering.

III. Experimental Method

As a target for our experiments we chose the ProASIC3 A3P250 device [14] for many reasons. Firstly, it has high security specifications and is positioned as the device with highest security protection in the industry. Actel, who developed PA3 chips, market them as devices which *'provide the most impenetrable security for programmable logic designs'* [8][15]. Secondly, PA3 chips are widely used in military and industrial applications especially in critical systems. Therefore, without doubt PA3 devices posed suitable challenges for this research. Any outcome occurring from analysing this device will have a greater impact and will be more useful compared to low-end security chips such as normal microcontrollers or standard FPGAs.

Initially, we analysed the chip with standard design tools from Actel – Libero IDE and FlashPro. The sample A3P250 device was connected to a standard Actel FlashPro3 programmer. PA3 devices are configured using a JTAG interface [16][17]. All of the JTAG operations are undocumented for PA3, however, using Actel development software we were able to generate series of STAPL files which we analysed for the commands used for different operations [12]. These configuration files are self-explanatory and easy to follow with all subroutines being clearly marked. Once we had established the JTAG communication we moved onto using only AES specific commands and optimising the time of their usage. To do this we built a special test board with a master JTAG interface and simple functions controlled by PC software via an RS-232 interface for convenience (Figure 2). The PA3 chip was placed into a ZIF socket for easier handling. During that stage we managed to reliably assess all encryption-related commands and their fields.

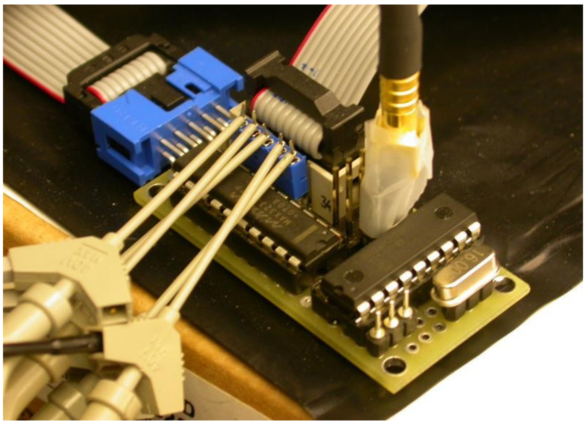


Figure 2. JTAG control board.

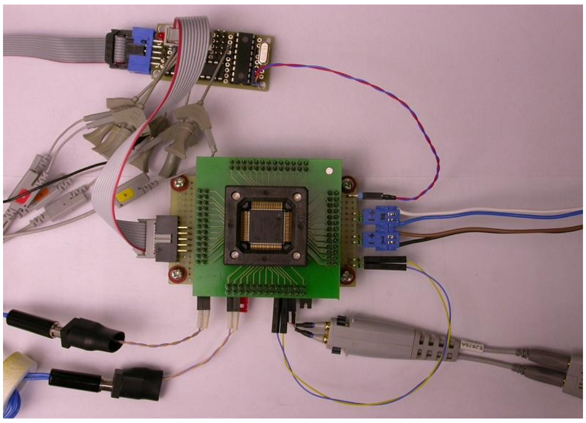


Figure 3. DPA setup.

Then we used a classic DPA setup to analyse the side-channel emission from the PA3 devices during decryption and other crypto related operations. We constructed a simple prototype board with a ZIF socket for the A3P250 device (Figure 3) and connected it to our test board which was providing some additional triggering functions for the oscilloscope. The power consumption was measured via a 20 Ω resistor in VCC core supply line with the Agilent 1130A differential probe and acquired with the Agilent MSO8104A digital storage oscilloscope. Then the waveforms were analysed using MatLab software with our own proprietary program code.

In order to evaluate the effectiveness of our new technology we developed several evaluation setups. The third generation of the probe is presented in Figure 4 and the whole measurement setup is shown in Figure 5. We completely redesigned the hardware used for analysis. By removing the oscilloscope in the acquisition chain and by making dedicated hardware we managed to substantially reduce the equipment cost of our setup from tens of thousands of dollars to merely two hundred dollars' worth of components. We bought all the parts from a local electronics distributor. A proprietary circuit was developed specifically for PA3 power trace measurements in order to reduce the overall electronic noise and thus improve the effectiveness of the analysis.

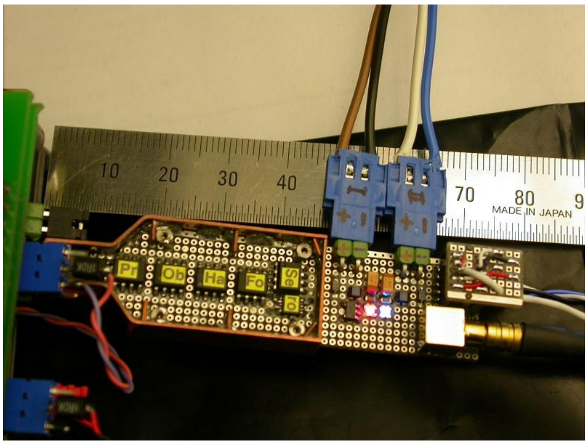


Figure 4. Prototype of the 3rd generation of the QVL sensor.

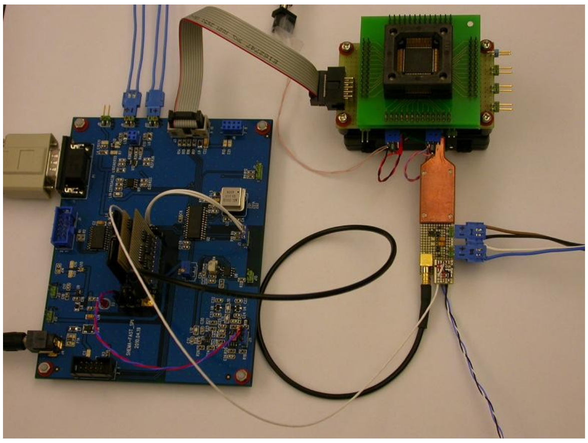
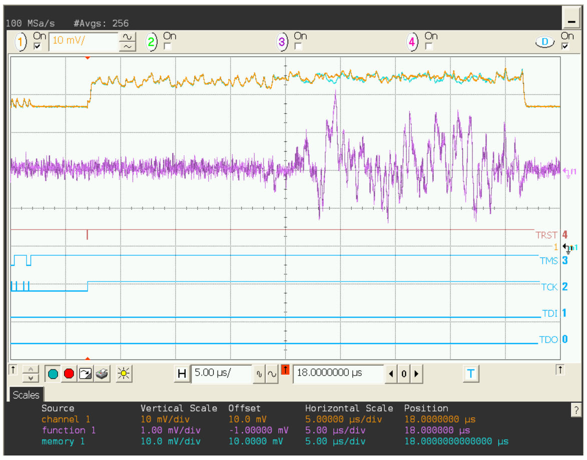


Figure 5. AES key extraction setup.

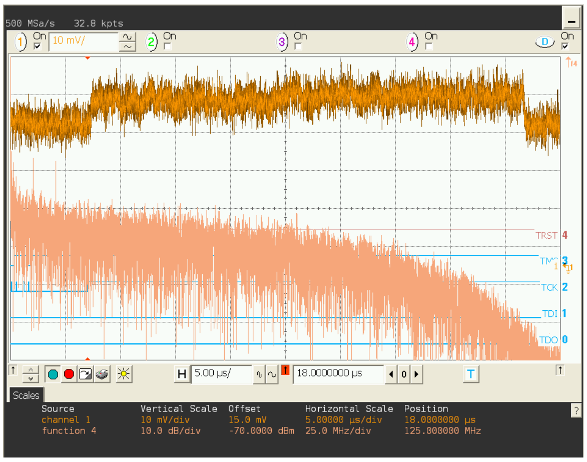
IV. Results

From our analysis of the STAPL programming code and through playing with JTAG commands we learned that there are three basic AES operations in PA3 chips. One is AES initialisation during which the on-chip AES engine is checked and AES round keys are calculated and stored in on-chip secure SRAM memory, which does not have any external access. Second is an AES authentication operation during which the user verifies to the PA3 chip that he knows the AES key by submitting a constant which is encrypted by the shared key. However, this protocol has an obvious flaw in that the constant is always 00...00. Third is the AES decryption itself which can be applied to either the FROM or FPGA array for both writing and verification operations. From a security point of view, even knowing the (00...00)K and being able to authenticate yourself to the PA3 device is a serious threat. This allows the device to be mass erased resulting in denial of service attack, or partially reconfigured with random data and physically damaged as a result. This is because the configuration bits control switches inside the FPGA and some combinations can cause excessive current to be sent through the device.



```
Source          Vertical Scale  Offset        Horizontal Scale  Position
channel 1       10 mV/div       10.0 mV       5.00000 µs/div    18.0000000 µs
function 1      1.00 mV/div     -1.00000 mV   5.00 µs/div       18.000000 µs
memory 1        10.0 mV/div     10.0000 mV    5.00 µs/div       18.0000000000000 µs
```

Figure 6. Power analysis on AES in PA3 with 1024 averages.



```
Source          Vertical Scale  Offset        Horizontal Scale  Position
channel 1       10 mV/div       15.0 mV       5.00000 µs/div    18.0000000 µs
function 4      10.0 dB/div     -70.0000 dBm  25.0 MHz/div      125.000000 MHz
```

Figure 7. FFT spectrum for AES operation in PA3.

Although PA3 devices do not have any specialised DPA countermeasures, they are at least 100 times harder to attack using DPA than non-protected conventional microcontrollers such as PIC, AVR, MC68HC, MSP430 etc. The robust hardware design features are complemented with the total lack of information about JTAG engine operation, hardware implementation and commands. That makes any attacks on the PA3 chips quite a challenging task. The averaged power trace of the AES authentication operation is showed in Figure 6. The FFT spectrum of the single AES power trace does not have any characteristic peaks (Figure 7) and filtering will not provide any substantial improvement for DPA results. Figure 8 shows the result obtained by comparing single traces for different input data. Averaging over 4096 traces gives a pretty nice result but takes a couple of minutes to acquire (Figure 9). As can be seen, for single traces the noise overshadows any useful signal with SNR being at the best –20 dB. In our standard DPA experiments the acquired waveforms were analysed using MatLab software with our own proprietary program code. We successfully extracted a sample AES key from an A3P250 device within two hours.

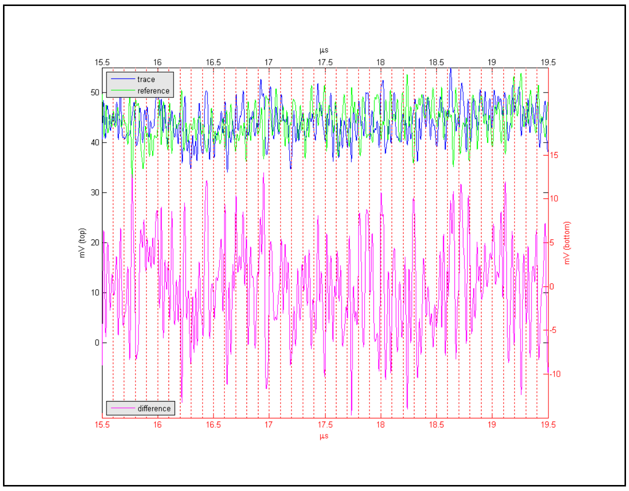


Figure 8. Power analysis on AES in PA3 with single trace difference.

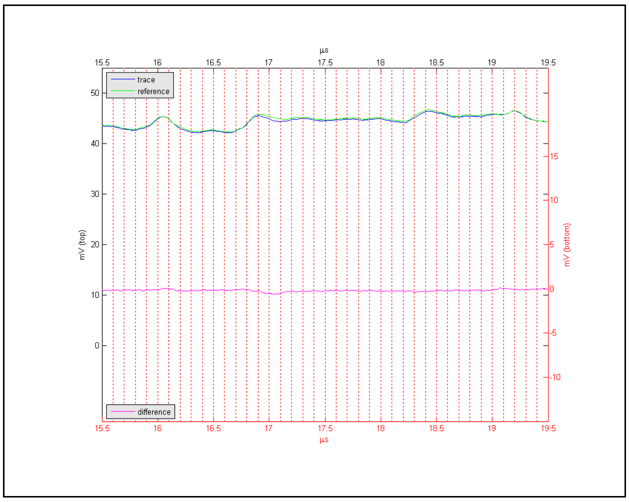
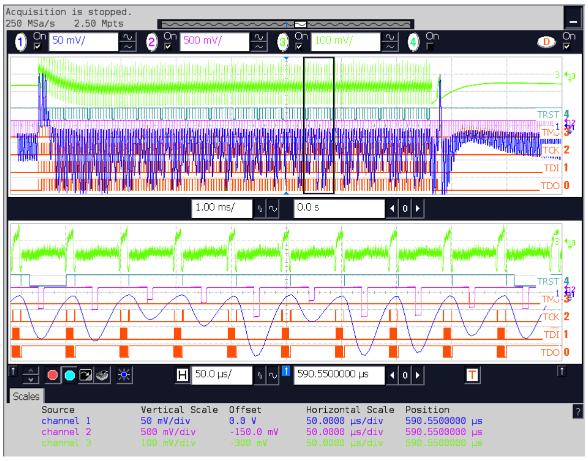


Figure 9. Power analysis on AES in PA3 with 4096 averages.

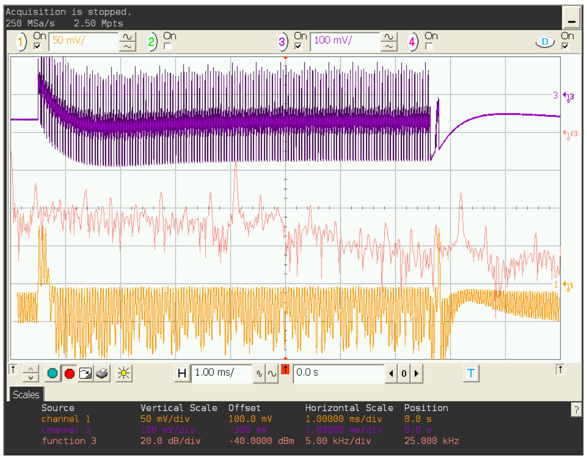
We achieved average extraction time of 0.01 seconds for various sample AES keys. There are no specifically designed countermeasures used that we can see preventing the AES key extraction via DPA. However there are other countermeasures that exist. There is a well thought out silicon design with extra features such as an internal clock with a large amount of jitter which is not synchronised to the JTAG clock and high noise coming from flash memory charge pumps. The key extraction is not in the least trivial. The PA3 relies on an unstable internal clock that is impossible to synchronise to and a signal-to-noise ratio that is 30 dB to 40 dB lower than in common microcontrollers. As an example, –15 dB to –20 dB in PA3 vs +15 dB to +20 dB in ATxmega. We were able to synchronise with the internal clock by means of special filtering and smart triggering using our new approach, so the unstable clock becomes irrelevant as we gain the synchronisation information from smart triggering. The acquisition bandwidth of 100 MHz to 500 MHz in a classic DPA setup has a very low correlation between data and the AES key (128 bits of key from 10 GB of acquired data); versus 20kHz bandwidth in PEA. There is a much stronger correlation between data and AES key (128 bits of key from 256 bits of data in PEA), hence a much reduced bandwidth and number of traces are required. Overall, we can gain 40 dB to 80 dB over a standard DPA setup (oscilloscope + MatLab).



```
Acquisition is stopped.
250 MSa/s    2.50 Mpts
```

```
Source       Vertical Scale  Offset     Horizontal Scale  Position
channel 1    50 mV/div       0.0 V      50.0000 µs/div    590.5500000 µs
channel 2    500 mV/div      -150.0 mV  50.0000 µs/div    590.5500000 µs
channel 3    100 mV/div      -300 mV    50.0000 µs/div    590.5500000 µs
```

Figure 10. PEA results on PA3 for AES key scanning.



```
Acquisition is stopped.
250 MSa/s    2.50 Mpts
```

```
Source       Vertical Scale  Offset        Horizontal Scale  Position
channel 1    50 mV/div       100.0 mV      1.00000 ms/div    0.0 s
channel 3    100 mV/div      -300 mV       1.00000 ms/div    0.0 s
function 3   20.0 dB/div     -40.0000 dBm  5.00 kHz/div      25.000 kHz
```

Figure 11. FFT spectrum of PEA signal for AES in PA3.

AES encryption would require many traces to be averaged in order to achieve a reliable correlation with key bits, even for poorly-protected against DPA attacks PA3 devices (Figure 4). The PEA approach allowed the AES key bits to be guessed at in real time and with a very good correlation with the key bits. The outstanding sensitivity of the PEA is owed to many factors. One of which is the bandwidth of the analysed signal, which for DPA, stands at 200 MHz while in PEA at only 20 kHz. This not only results in much lower noise, which is proportional to the square root of the bandwidth, but the cost of the acquisition hardware becomes several orders of magnitude lower. This also impacts on the latency thus allowing real-time analysis, because the signal produced for the analysis has almost 100% correlation with the key bits (Figure 10, Ch3 – power trace, Ch1 – PEA signal, Ch2 – demodulated signal). This makes extraction time extremely fast. All that needs to be done in the end for the key extraction is to demodulate the signal and compare it with the reference peak. This can be easily performed by a simple one-dollar microcontroller with on-chip ADC. An expensive oscilloscope and PC with proprietary software is not required. The FFT spectrum shows that there is a main frequency of 21 kHz and other frequencies resulted from AM modulation of the extracted key-correlated signal (Figure 11).

V. Implications and Future work

There are several security protection levels in the PA3 devices according to the manufacturer's datasheet [14]. The Passkey offers the highest level of reversible protection mechanism. Various DPA techniques were attempted to extract the Passkey, however, we were unable to get even a single bit in two weeks time using our off-the-shelf DPA equipment (oscilloscope with differential probe and PC with MatLab). The Passkey hardware security had robust countermeasures that proved to be DPA resistant. In addition to the unstable internal clock and high noise from other parts of the circuit, the Passkey access verification had its side-channel leakage reduced by a factor of 100. Only noise can be observed in the power traces without any characteristic peaks in the frequency domain. This was likely to be achieved through using a well compensated silicon design together with ultra-low-power transistors instead of standard CMOS library components. In addition, the useful leakage signal has a spread spectrum with no characteristic peaks in frequency domain, thus making narrow band filtering useless.

According to our findings and measurements we assessed the effectiveness for various SCA setups. For state-of-the art DPA systems we estimate the capability of extracting the AES key from the PA3 devices within 10 minutes, however, we do not have access to the Cryptography Research DPA Workstation [18] or the Riscure Inspector [19], therefore figures for state-of-the-art DPA equipment are only an estimate.

Many countermeasures are designed to defeat high end oscilloscopes and their known noise, latency and signal issues. These countermeasures prevent themselves from being broken in an affordable time through suppressing the signal or by bringing it to a higher noise level. Our approach, through the use of bespoke hardware and the removal of the oscilloscope from the testing process, is designed to have the sensitivity to detect even the smallest variation in signal, which then allows more detailed analysis. The setup with which we achieved these eye-opening results is in its most basic form, employing a single pipeline (one channel).

Having taken this technology to proof of concept, we would like to develop it by building a multi-pipeline system consisting of 100 channels as well as new, more efficient hardware for our probes, with the aim of further improving sensitivity and speed by a factor of 10. We firmly believe that with this increase in capability planned for the next generation of our technology, defeating these more secure DPA countermeasures is a very real and achievable expectation. Using a low-noise side-channel measurement setup with a carefully designed probe a 10× further improvement can be achieved. Further improvements can be done to the scanning algorithm itself thus improving the effectiveness by a further 10×. All these improvements can bring the analysis time down to hours or even minutes.

A reasonable question can be asked of our results: If the technology is so advanced why haven't you tested other really secure chips which have proprietary DPA countermeasures yet? There are two main reasons for this. With the budget available to us and the time constraints we were working to, we were only limited to researching, designing, testing and building the new sensor technology for use with an off the shelf device with some countermeasures to the proof of concept test stage. We are only interested in testing real world devices, not against countermeasures simulated in hardware or software on a reference system like Sasebo boards [20]. Secondly, it was also important for our project for us to be able to publish our testing results. All the very secure devices we looked at require you to work under NDA so in these cases we would not be in a position to discuss our findings with anyone.

We have, however, tested our technology against countermeasures which are DPA resistant that present another layer of security alongside AES in the PA3 and other Actel FPGAs. Actel's Passkey security protection employs robust countermeasures such as leakage compensation and spread spectrum. Despite our extensive research, we were unable to extract this key using an off-the-shelf DPA system – not even one bit of the key in two weeks time. It took as long as one day to extract the passkey and backdoor key using our PEA technology and this is without any kind of optimisation. We challenge anyone using DPA, or any system, to extract those particular keys in any time comparable with our technology.

There are of course some very complex countermeasures with spread spectrum, random numbers, masking and dummy cycles. These are harder to defeat and will require us to use various techniques such as creating matching filter designs or synchronisation techniques.

Further research will be focused on those more complex countermeasures found in smartcards and silicon chips certified to FIPS140-2 level 3 and chips with in-built self-destruct mechanism.

We are now putting our minds to using our technology for hardware assurance of silicon chips. Further research is being undertaken to use the new PEA technique to achieve something that so far has been muted only as a theory: to find evidence of a backdoor in a production device, and to develop a system of hardware assurance where it is possible to actively scan silicon chip (or a system) for any backdoors or Trojans or to determine if a device is authentic or a clone. This would be the first time such a capability is demonstrated to be feasible. Some new results will be presented at the Cryptographic Hardware and Embedded Systems (CHES) workshop in September 2012.

VI. Conclusion

Our research has demonstrated that the AES key from the PA3 device which is marketed as extremely secure can be extracted in 0.01 seconds thus setting a new milestone in AES key extraction using side-channel attacks (SCA). We achieved this with a low-cost approach without any need for expensive oscilloscopes or expensive SCA equipment. Key extraction time of 0.01 seconds was achieved with minimum resources. A determined attacker can potentially break PA3 in less than 1 ms (0.001 seconds) by using multiple pipelines. Our test result of 0.01 seconds represents a milestone for demonstration purposes, there was no need to challenge it further and go beyond 0.01 seconds, as no existing SCA technique can get the AES key from a PA3 in less than 1 second; even in theory. Using a classical DPA setup as our baseline test system (test board, oscilloscope, PC and Matlab) it was possible for us to extract the AES key from the PA3 in two hours. We do not have access to the DPA Workstation from Cryptography Research or Inspector from Riscure, but we would expect these professional systems to be able to extract the key at least ten times faster than we can achieve with our test system. A fair estimate for these professional systems based upon our test results is somewhere in the ten minute range to extract the AES key from the PA3. Based upon this estimate, using the new PEA technique we can achieve a 60,000 times speed performance against professional SCA systems on the PA3. Devices withstanding Common Criteria can be broken with PEA in a much shorter time, one month at most, we estimate. We analysed other Microsemi/Actel products and found them all having the same AES implementation problems. Those products include but are not limited to: Igloo, Fusion and SmartFusion. The PA3 is heavily marketed to the military and industry and resides in some very sensitive and critical products.

Even though our technology is patented, the great danger is the proliferation of the attack technology to those who will try to copy it and use it illegally. We are therefore undertaking research as a matter of urgency in collaboration with industrial sponsors to develop new countermeasures to protect silicon chips. This is especially important for the smartcard industry that relies on robust security countermeasures against SCA. The new generation of our technology with an increased number of pipelines can potentially extract a cryptographic key with as little as one measurement thus challenging the existing protection which relies on a dynamic key derivation mechanism.

Common Criteria regards a device as secure if it can withstand an attack within one month using a DPA setup consisting of an oscilloscope, PC and, at times, special triggering hardware [21]. Current Common Criteria does not take into consideration the development of new, more advanced techniques for SCA. We believe the ability to break robust countermeasures within one day or less with PEA represents a serious threat; given that a certification laboratory cannot do so within one month. If SCA technology is significantly more advanced than any available countermeasures, existing devices are rendered completely vulnerable. We believe that further research should be undertaken to understand the risks involved in not updating the certification process of DPA techniques to take into consideration the developments in SCA technology.

This new approach to making SCA attacks has several consequences. It conceivably allows low budget would-be attackers to possess technology far more advanced than state-of-the-art technology; meaning that the number of devices and frequency of attacks on robust hardware could increase. In addition, any attacker with sufficient technical and financial backing could make a multi-pipeline or silicon version of the technology in order to attack even the most secure of devices. We are of course unsure if current countermeasures would be able to survive attacks of this nature. Our current assessment of countermeasures in very secure devices is such that we believe they would be unable to withstand an attack from our upgraded technology.

A solution as simple as off-the-shelf components bought from an electronics distributor and a small budget have makings of a problem for the cryptographic community and a serious threat to the semiconductor industry. Any intellectual property pirate with the relevant electronics knowledge has the potential to attack even the most secure devices with great effect.

References

[1] P. Kocher, J. Jaffe, B. Jun: Differential Power Analysis. CRYPTO99, LNCS, Vol. 1666, Springer-Verlag, 1999, pp. 388-397

[2] J.-J. Quisquater, D. Samyde: ElectroMagnetic analysis (EMA): measures and counter-measures for smard cards. In: Smart Card Programming and Security (E-smart 2001), Cannes, France. Springer-Verlag, 2001, LNCS, vol. 2140, pp. 200-210.

[3] S. Mangard, E. Oswald, T. Popp: Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer, New York, 2007

[4] D. Real, C. Canovas, J. Clediere, M. Drissi: Defeating classical hardware countermesures: a new processing for side channel analysis. DATE2008, pp. 1274-1279

[5] S. Chari, J. R. Rao, P. Riohatgi: Template Attacks. In B. S. Kaliski Jr, C . K. Koc, and C. Paar, editors, Cryptographic Hardware and Embedded Systems CHES 2002, volume 2523 of LNCS, pp. 13-28. Springer-Verlag, 2002

[6] P. Kocher, J. Jaffe, B. Jun, P. Rohatgi: Introduction to differential power analysis. Journal of Cryptographic Engineering (JCEN), Vol. 1, No. 1, Springer, 2011, pp. 5-27

[7] M. Bucci, L. Giancane, R. Luzzi, M. Marino, G. Scotti, A. Trifiletti: Enhancing power analysis attacks against cryptographic devices. IET Circuits, Devices & Systems, Vol. 2, No. 3, 2008, pp. 298-305

[8] Actel ProASIC3 Handbook, ProASIC3 Flash Family FPGAs http://www.actel.com/documents/PA3_HB.pdf

[9] Design Security in Nonvolatile Flash and Antifuse FPGAs, Security Backgrounder http://www.actel.com/documents/DesignSecurity_WP.pdf

[10] Actel ProASIC3/E Production FPGAs, Features and Advantages http://www.actel.com/documents/PA3_E_Tech_WP.pdf

[11] I. Kizhvatov: Side Channel Analysis of AVR XMEGA Crypto Engine. ACM proceedings of Workshop on Embedded Systems Security (WESS), 2009

[12] Actel, ISP and STAPL, Application Note AC171 http://www.actel.com/documents/ISP_STAPL_AN.pdf

[13] Integrated Circuit Investigation Method and Apparatus. Patent number WO2012/046029 A1

[14] Actel ProASIC3 Flash Family FPGAs, Datasheet http://www.actel.com/documents/PA3_DS.pdf

[15] ProASIC3 Frequently Asked Questions, Actel Corporation, Mountain View, CA 94043-4655 USA. Accessed on 04 October 2011. http://www.actel.com/documents/pa3_faq.html

[16] JTAG Boundary scan. IEEE Std 1149.1-2001

[17] JTAG Programming specification. IEEE 1532-2002

[18] Cryptography Research DPA Workstation http://www.cryptography.com/technology/dpa-workstation.html

[19] Riscure Inspector http://www.riscure.com/tools/inspector

[20] Sasebo: Side-channel Attack Evaluation Boards http://staff.aist.go.jp/akashi.satoh/SASEBO/en/index.html

[21] Common Criteria http://www.commoncriteriaportal.org/