SPA and DPA: Possible Testing Solutions and Associated Costs

Stan Kladko, *BKP Security Labs*

Abstract— **We provide a review of SPA and DPA taken from the point of view of a Cryptographic Module Validation Program (CMVP) testing lab. The review concentrates on public knowledge in this field including commonly used testing methods and techniques. We also try to estimate possible time and cost implications for the testing lab, as well as equipment and personnel requirements.**

1. Simple Power Analysis (SPA) and Differential Power Analysis (DPA) were introduced by Kocher et al. in [1]. Initially, DES cipher was studied. The method was then generalized to such algorithms as AES [2], RSA [3] and Elliptic Curve algorithms [4]. SPA involves analyzing time-resolved electric current measurements directly, while DPA is based on statistical correlations between key bits and time-resolved current, and requires multiple runs to separate correlations from the background noise. ElectroMagnetic Analysis (EMA) is a closely related topic, where time-resolved intensity of electromagnetic emission is used as the measured quantity [5]. EMA measurements have to be performed close to the surface of the chip, and require significantly more effort and, as compared to power analysis measurements.

2. A number of methods were proposed to make SPA and DPA ineffective [6]. Many of such methods work by suppressing the signal-to-noise ratio. The proposed methods include among others placing a capacitor between power and ground connections of the device, physical shielding, adding random power consumption, randomizing algorithm execution, randomizing circuit timing, interleaving dummy instructions with the cryptographic code, and introducing new specifically redesigned cryptographic algorithms and circuit layouts. EMA countermeasures could also include using an upper metal layer to shield the radiation, introducing variable random currents to increase electromagnetic noise, as well as tuning hardware design to reduce radiation [5].

3. It is clear, that lack of SPA and DPA testing requirements is a weakness for the current version of the FIPS Pub 140-2 standard [8]. In particular, a smartcard which is susceptible to an SPA or DPA attack can hardly be deemed secure for government use purposes, such as the PIV project [9]. From this perspective adding SPA and DPA requirements to the FIPS Pub 140-3 standard seems to be rather well justified. To consider potential implications of adding SPA and DPA-related requirements to the FIPS Pub 140-3 standard one first needs to review physical security requirements present in the current version of the standard. FIPS Pub 140-2 describes four security levels for cryptographic modules. Security Level 1 does not include significant physical security requirements. Security Level 2 is mainly concerned with tamper-evidence, i.e., with ability of a user to detect a key compromise once it has occurred. Security Levels 3 and 4 aim to provide for destruction of keys in case of a compromise, Level 3 focusing on protection against basic compromise attempts, and Level 4 aiming to protect against more advanced and elaborate attacks. FIPS Pub 140-2 classifies cryptographic modules into three categories: single-chip, multiple-chip standalone, and multiple-chip embedded. Smartcards, which are usually classified as single-chip modules are of the most relevance for SPA and DPA.

4. Here we would like to consider potential mapping of SPA and DPA requirements to Security Levels. It is rather clear that SPA and DPA requirements shall not be applicable to Security Level 1, as it does not make any significant physical security claims. Since Security Level 2 seeks to provide for tamper-evidence, and since compromising a secret or private key using SPA or DPA techniques may be potentially performed without leaving any traces of tampering, one could argue that protection against SPA and DPA shall be provided for Security Levels 2 and higher. One could also argue that potential SPA and DPA requirements shall be limited to single-chip modules, since published practical SPA and DPA attacks concentrate on single-chip devices.

5. One then needs to come up with a set of well defined SPA and DPA-related requirements, which could be included into the FIPS Pub 140-3 standard. Here one has to consider potential implications of such new

Dr. Stan Kladko is with BKP Security Labs, 3080 Olcott Suite 110-A, Santa Clara, CA 95054 USA (e-mail: kladko@bkpsecurity.com).
).

requirements for the existing cryptographic module testing labs. The past success of the cryptographic module testing program can be attributed, in part, to the relatively low cost (<$50K) of a typical FIPS 140-2 validation, as well as to relative simplicity of the security requirements formulated in the standard. One could reasonably argue that to keep cryptographic module validations relatively inexpensive and accessible to vendors, the costs of performing SPA and DPA testing shall not exceed 20% of the total validation costs, and the additional time and resources the vendor has to allocate to satisfy the SPA and DPA requirements shall not exceed 20% of the total time and resources the vendor currently allocates to a typical cryptographic module validation. Applying these criteria one can estimate a tentative lab budget for SPA and DPA-related activities at $5K - $10K, which, could amount to approximately one or two person/weeks.

6. In order to be able to fit SPA and DPA testing within the time frames mentioned above, several issues have to be addressed. First of all SPA and DPA requirements have to be simple and clear enough to enable effective usage of these requirements for a variety of products. Second, an effort shall be made to standardize the experimental setup, testing methods and software tools to provide the testing labs with a way to perform testing in repeatable, traceable and well defined manner. It seems that the actual hardware acquisition costs related to DPA and SPA testing are not going to present significant problems. A typical setup for power analysis testing described, e.g., in [6] could include such equipment items as a variable DC power supply, a function generator to provide clocking signal, a digital oscilloscope to take time-resolved current measurements, and a PC to perform analysis of measurements, with the total cost of the setup described in [6] running at less than $5K. Another cost dimension is represented by a software package, which is required to acquire and analyze power traces. This software package has to be tightly integrated with the control interface provided by the digital oscilloscope, in particular, to ensure correct time alignment of power traces for DPA. In this case, one option would be for the CMVP to design a standard test setup, which would include a particular oscilloscope model and a software package. This setup could be then distributed to the testing labs.

7. Staff training is an important subject when one considers adding SPA and DPA testing requirements to the FIPS 140-3 standard. Currently NVLAP does not require labs to have staff members familiar with applied physics and electrical engineering concepts employed in SPA and DPA testing. In addition, DPA testing will require familiarity with a number of concepts in statistics. NVLAP handbook 150-17 [10] would probably need to be revised to include a minimum set of staff training requirements required for SPA and DPA testing.

8. SPA and DPA measurements and analysis can be time consuming. In particular the paper [6] cites 22 hours as time required to take 400 power traces required for DPA attack on DES. In [7] Kocher et al. recommend capturing 1000-10000 traces. It is then important to come up with a set of simple and robust testing criteria which could be included in the standard, and which would lead to a reasonably short testing cycle. The existing literature lists a number of SPA and DPA measures and countermeasures, which could go to a very high degree of sophistication. Having to analyze all possible scenarios would probably put undue burden on the testing lab. It would be beneficial to replace such analysis with a well defined mathematical criterion. It seems reasonable to relate such a criterion to the signal-to-noise ratio for time-resolved power measurements. Then the power analysis requirements of the FIPS 140-3 standard could be specified in terms of the maximum allowed signal-to-noise ratio. The exact mathematical definition of the signal-to-noise ratio is subject to discussion and can be left to the experts in the field. Any mathematical definition will not be perfect in a sense that having the ratio below a certain threshold will not guarantee resistance of the product to power analysis attacks, since various methods could potentially be applied to cancel the noise for a particular chip or electronic component. On the other hand, having the signal-to-noise ratio below a certain threshold prescribed by the standard could potentially guarantee a certain degree of effort required from the attacker, and would, therefore, provide assurance against attackers with low attack potential. The entire procedure of signal-to-noise ratio measurement could then be standardized to a large degree, and implemented in the software. SPA and DPA testing would probably require separate definitions for the signal-to-noise ratio, since DPA includes additional averaging over large number of power traces. One possibility would then be to limit Security Level 2 to SPA, and then require DPA testing at Security Level 3 and higher. In such a case, power analysis testing performed at Security Level 2 could be performed significantly faster and with less effort, since calculating signal-to-noise ratio in the SPA sense would not require taking large number of time-aligned measurements. Another possible alternative would be to structure SPA

and DPA testing in a way similar to the currently implemented cryptographic algorithm testing program, where the power traces could be generated by the vendor, and then provided to the lab for processing and evaluation against the power analysis requirements of the standard.

9. To summarize, adding SPA and DPA testing to FIPS Pub 140-3 requirements for single chip modules seems to be well justified. In order to keep the associated time and cost implications within reasonable limits, one would probably need look for a set of simple and well defined SPA and DPA testing criteria, where robustness and ease of implementation should be given priority to the attempts to define testing criteria encompassing all possible attack scenarios, however sophisticated. The existing literature on this subject seems to point out that introduction of limits on the signal-to-noise ratio may be considered as a candidate power analysis requirement to be included in the standard. The exact definition of the single-to-noise ratio and the exact value for the upper limit are subjects to a further discussion.

References

[1] P. Kocher, J. Jaffe, and B. Jun, *Introduction to Differential Power Analysis and Related Attacks*, http://www.cryptography.com/dpa/ technical, 1998

[2] S. Mangard, *A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion*, Proceedings of the 5th International Conference on Information Security and Cryptology - ICISC 2002, November 28-29, 2002, Seoul, Korea

[3] R. Novak, *SPA-based adaptive chosen-ciphertext attack on RSA implementation,* Lecture Notes in Computer Science, vol. 2274, 2001

[4] J. Coron, Resistance against *Differential Power Analysis for Elliptic Curve Cryptosystems*, Lecture Notes in Computer Science, Volume 1717, 1999, p. 292

[5] K. Gandolfi, C. Mourtel, and F. Olivier, "*Electromagnetic analysis: Concrete result*s" Lecture Notes in Computer Science, vol. 2162, 2001.

[6] R. Junee, *Power Analysis Attacks:: A Weakness in Cryptographic Smart Cards and Microprocessors,* Ph.D Thesis, University of Sydney

[7] P. Kocher, J. Jaffe, and B. Jun, *Differential power analysis,* in Advances in Cryptology – CRYPTO ' 99 , vol. 1666 of Lecture Notes in Computer Science, pp. 399–397, 1999

[8] *FIPS Pub 140-2, Security Requirements for Cryptographic Modules*, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[9] *NIST Personal Identity Verification (PIV) Project*, http://csrc.nist.gov/piv-program/fips201-support-docs.html

[10] *NVLAP Handbook 150-17, Cryptographic Module Testing*, http://ts.nist.gov/ts/htdocs/210/214/docs/hnbk-17.pdf