A Survey of the State-of-the-Art Fault Attacks

Jakub Breier and Dirmanto Jap
Physical Analysis and Cryptographic Engineering,
Temasek Laboratories@NTU
School of Physical and Mathematical Sciences, Division of Mathematical Sciences, Nanyang Technological University, Singapore
jbreier@ntu.edu.sg, dirm0002@e.ntu.edu.sg

***Abstract*—Since 1996, when Boneh, DeMillo and Lipton introduced the idea of fault attacks, many theoretical and practical publications were made on this topic. These attacks belong to the class of physical cryptanalysis attacks.**

In this paper we describe several methods of fault injection attacks. We provide an overview of both attacks and countermeasures on AES algorithm and on ECC.

***Keywords*—physical cryptanalysis, fault attacks, AES, ECC**

I. Introduction

Cryptographic algorithms protect the confidentiality and the integrity of information. Each of widely used algorithms is proved to be secure from the view of the classical cryptanalysis, that means it is mathematically infeasible to decrypt a given ciphertext in a reasonable time without a key. Since late 90's, there is increasing popularity of the physical cryptanalysis, which attacks the implementation of an algorithm instead of an algorithm itself. When attacking unprotected implementations, these attacks can be very effective.

The idea of fault attacks was introduced by Boneh, DeMillo and Lipton in 1996 [9]. These attacks exploit the possibility to insert a fault in the process of the algorithm execution in a way that could help to reveal the key. The first practical attack was implemented by Biham and Shamir [5], they implemented a successful attack on the DES algorithm, introducing a technique called the Differential Fault Attack. Since then, many types of fault attacks on different cryptosystems were proposed.

In this paper we describe the most recent techniques and methods of fault attacks. Fault injection techniques include supply voltage glitching and laser attacks as the most popular types, also the electromagnetic fault injection is getting more attention as it can be as accurate as a laser, but with the advantage of keeping the chip in its original package. Fault attack methods for cryptographic algorithms include for example Differential Fault Analysis (DFA), Collision Fault Analysis (CFA), Ineffective Fault Analysis (IFA), Safe-Error Analysis (SEA) [13], [14].

The rest of the paper is organized as follows. Section II provides overview of attacks on symmetric cryptosystems, with emphasis on the Advanced Encryption Standard (AES) algorithm. Section III describes attacks on asymmetric algorithms, providing an overview of attacks on Elliptic Curve Cryptography (ECC) algorithms. Finally, section IV concludes this paper.

978-1-4799-4833-8/14$31.00

II. Secret Key Cryptosystems

This section describes fault attacks that have been proposed for the purpose of breaking symmetric algorithms. The most common attack method is the *Differential Fault Analysis (DFA)*. The usual procedure is to invoke faults in a chosen round of the algorithm to get the desired fault propagation in the end of an encryption. The secret key can then be determined by examining the differences between a correct and a faulty ciphertext. The first attack using this technique was aimed at DES, it was proposed in 1997 by Biham and Shamir [5].

The next popular method is the *Collision Fault Analysis (CFA)*, where an attacker invokes a fault in the beginning of the algorithm and then he tries to find a plaintext, which encrypts into the same ciphertext as the faulty ciphertext in the previous case, by using the same key.

The goal of the *Ineffective Fault Analysis (IFA)* method is to find such fault that does not change the intermediate result, therefore it leads into a correct ciphertext. The main problem of this method is to determine if the fault was actually invoked or not. *Safe-Error Analysis (SEA)* also exploits a situation when ciphertexts are equal, but it changes the intermediate result. It utilizes a state when the data is changed but it is not used.

In 2010, a method entitled *Fault Sensitivity Analysis (FSA)* [32] was proposed. This method is effective even for some DFA resistant implementations and does not restrict the fault model to a few bits or bytes. It exploits the side-channel information, such as sensitivity of a device to faults and uses this information to retrieve the secret key.

In 2012, a *Linear Fault Analysis (LFA)* [28] was proposed, which examines linear characteristics for some consecutive rounds of a block cipher. The authors successfully mounted the attack on the DFA resistant implementation of the SERPENT cipher.

A. Fault Attacks on AES

Since AES is the most popular symmetric block cipher, the majority of attacks aims on this algorithm. Table I summarizes the most important attacks on AES, in a chronological order.

B. Countermeasures

Along with attacks, works on countermeasures were usually presented as well. There are two main types of countermeasures against fault attacks [10]: sensor-based and error-detection based countermeasures. The first type checks the

TABLE I. FAULT ATTACKS ON AES

Ref.	Year	Fault model	# Faulty ciphertexts	Attack Type	Remarks
[20]	2002	Switch 1 bit / disturb 1 byte	$50/250$	DFA	
[8]	2002	Force 1 bit to 0	128	CFA/IFA	
[38]	2003	Disturb 1 byte	2	DFA	Practical attack on FPGA implementation shown in [26].
[11]	2003	Disturb 1 byte	30	DFA	First attack on the AES key schedule.
[37]	2006	Disturb 1 byte	2^{10}	Square-DFA	Attacks middle rounds of the algorithm, therefore the redundancy countermeasure on the first or last rounds is ineffective.
[6]	2006	Switch 1 byte	285	CFA	Effective against implementations protected by memory encryption mechanisms.
[35]	2006	Disturb 1-4 bytes	6	DFA	Uses a very general fault model, covering 98.45% of all possible faults on each 4 bytes of *MixColumns* input in round 9. This method was improved to be able to attack all key sizes in [30].
[45]	2007	Disturb 1 column	2 and 48b brute-force search	DFA	Attacks the key scheduling process.
[27]	2008	Disturb 3 bytes	2 and 32b brute-force search	DFA	Attacks the key scheduling process.
[36]	2009	Disturb 1 byte	1 and 32b brute-force search	DFA	The attack was further improved to use only 1 pair of faulty and correct ciphertexts and an 8b brute-force search.
[40]	2009	Disturb 1-4 bytes	1 and 32b brute-force search	DFA	Attack requires a random fault anywhere in one of the four diagonals in the round 8.
[32]	2010	Disturb 1-16 bytes	50	FSA	A new method - Fault Sensitivity Analysis was proposed, which does not use values of faulty ciphertexts.
[22]	2010	Disturb 1 diagonal	1 (AES-192) 3 (AES-256)	DFA	Extends the attack proposed in [38] to other keylengths.
[18]	2013	Disturb 1-12 bytes	Hundreds	-	Uses a faulty ciphertext-only model, without the need of faulty/correct ciphertext pairs.
[31]	2013	Disturb 1-16 bytes	1 and 8b brute-force search	CC-FSA	Introduces a Clockwise Collision FSA method.
[42]	2013	Disturb 1 byte		Square-DFA	The key can be revealed even with a large number of noisy fault injections.

environmental conditions of the device - e.g. a presence of unusual voltage peaks, a presence of light. Error-detection countermeasures can be either hardware-based or software-based, they basically check if the algorithm output is correct by various methods. As shown in [39], error-detection circuits increase the information redundancy and therefore, such implementations can be more vulnerable against power analysis attacks.

Besides these two main types, there exist various methods, which can be either device or algorithm specific. We will briefly discuss the countermeasures on the AES presented so far.

Error-detection countermeasures can be found in [25], [24], [19]. Karpovsky et al. [25] proposed two countermeasures: one has a hardware overhead of 35%, but a low protection against small multiplicity faults, while the other one is robust, but with the overhead of 150%. Joye et al. [24] proposed a duplication scheme, with the 60% area overhead on the FPGA. It protects the implementation against the Giraud's attack [20] using 1-4 faults, the resistance decreases rapidly with the higher number of faults. Genelle et al. [19] introduced a scheme that can be combined with the masking in order to provide a protection against the DPA as well. This protection scheme increases timing by 45% and the amount of used RAM by 448%.

The first countermeasure on the AES key schedule-based fault attack was presented by Chen and Yen [11]. They proposed three approaches for the round key protection: storing the key in the flash memory, generating the round key only once after the key update, and a parity check.

Mestiri et al. [34] used a novel scheme of protecting the S-box against faults. Instead of a normal output value from the S-box they xor the output and the input. This value is then xored again with the input in order to get the correct output and the fault can be detected by using a flag, as shown in Figure 1. The other AES stages are protected by a parity check. They tested this scheme on an Virtex-5 FPGA, it can detect 99.998% of the random faults, however the area was increased by more than 1/4 and the frequency decreased by 17.03%.

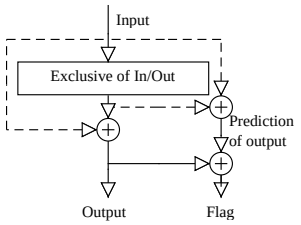

Fig. 1. Countermeasure proposed by Mestiri er al. [34]

Lomne et al. [33] analyzed several countermeasures and came to conclusions that most of them can be defeated by a slightly changed attack model or a multiple-fault model. They proposed enhanced countermeasures based on the randomness, that should minimize the probability of a successful attack.

Barenghi et al. [3] analyzed the efficiency of several software countermeasures based on redundant computations. Based on their findings, the instruction duplication or triplication can provide a protection for AES against all known attacks. The overhead can be lowered by selecting only vulnerable parts of the algorithm to be duplicated or triplicated.

III. PUBLIC KEY CRYPTOSYSTEMS

The first and a well-known attack on public key cryptosystem was proposed by Boneh, DeMillo and Lipton [9], shortly improved by Lenstra [29]. The attack exploits the RSA-CRT implementation, enabling an efficient factorization of the modulus N with just a one pair of a faulty and a correct ciphertext. Since then, many fault attacks aiming at public key cryptosystems have been proposed.

A. Fault Attacks on ECC

Elliptic curve cryptosystems were proved to be vulnerable against several types of implementation attacks. The majority

of fault attacks attempt to move the computation from a secure curve to a weaker curve. There are several ways to perform this step, either by injecting faults into the curve parameters or the base point, or by attacking the scalar multiplication [1]. The first attack was proposed by Biehl et al. [4] in 2000, using the DFA technique. By disturbing 1 bit during the secret scalar multiplication, they were able to obtain the information about this scalar. This attack was further improved by Ciet and Joye [12]. ECC are also vulnerable to SEA attacks, which are based on the assumption that the injected fault will change the output only if some condition of the secret data is fulfilled. Otherwise the output will stay unchanged. There are two types of these attacks: computational safe-error attacks (called *C Safe-Error Attacks*) [47], and *M Safe-Error Attacks* [46], [44]. The first type tries to induce a temporary random computational fault inside the ALU and the second type induces a memory fault, inside a register or a memory location.

Giraud and Knudsen [21] presented byte-fault attacks on multiple signature schemes, including the ECDSA. They extended the bit-fault model presented by Dottax in 2002 [16]. Using their method, they were able to recover the secret key with 2300 faulty signatures.

Blömer et al. [7] proposed a new method of the scalar multiplication based fault attack, called Sign Change Attacks. The main difference is that points do not leave the curve after the attack, therefore it makes the detection harder.

Schmidt and Medwed [43] suggested a new attack on ECDSA. The idea of the attack is to determine parts of the ephemeral key for several signatures. This key is different for each encryption, but it is possible to obtain the secret key by using the lattice attacks. They needed 50 faulty signatures to reveal a 160b key. Their countermeasure against this attack has an overhead of 36% in the worst case.

Sakamoto et al. [41] adjusted the Fault Sensitivity Analysis method, originally proposed by Li et al. [32] for the fault attack on the AES. They implemented an attack on the ECC implementation using the López-Dahab algorithm, which is less vulnerable to fault attacks than classical implementations.

Dominguez-Oviedo et al. [15] presented the invalid-curve attack that can be applied to the Montgomery ladder elliptic curve scalar multiplication algorithm.

Jarvinen et al. [23] extended Giraud's attack on signature schemes [21]. They have shown that if faults are biased and the attacker can accurately estimate these biases, it can lead to a more efficient attack.

B. Countermeasures

There exist several types of countermeasures against fault attacks on ECC [17]. *Point validation* countermeasure verifies whether a given point lies on a curve or not. *Curve integrity check* can detect faults on curve parameters. *Coherence check* can verify the intermediate or final result with respect to a pattern. *Combined curve check* uses a reference curve for checking for fault occurrence and *co-factor multiplication* is used in order to prevent small subgroup attacks.

Baek and Vasyltsov [2] propose countermeasures against side-channel attacks and fault attacks, based on converting the definition field of elliptic curves into its random extension ring, while performing operations in the ring. It is possible to perform a validation check in a small subring, which provides a countermeasure against fault attacks.

IV. Conclusions

In this paper we provided an overview of the current state of fault attacks and their countermeasures on AES as a representative of symmetric algorithms and on ECC as a representative of public key cryptosystems.

It is worth to mention that some mathematical fault models presented in several publications can be difficult to implement in practice. For instance, bit-fault models require high-precision measuring and fault injection tools, which are costly and require an experienced operator.

References

[1] A. Alkhoraidly, A. Domnguez-Oviedo, and M. Hasan. Fault Attacks on Elliptic Curve Cryptosystems. In M. Joye and M. Tunstall, editors, *Fault Analysis in Cryptography*, Information Security and Cryptography, pages 137–155. Springer Berlin Heidelberg, 2012.

[2] Y.-J. Baek and I. Vasyltsov. How to Prevent DPA and Fault Attack in a Unified Way for ECC Scalar Multiplication Ring Extension Method. In E. Dawson and D. Wong, editors, *Information Security Practice and Experience*, volume 4464 of *Lecture Notes in Computer Science*, pages 225–237. Springer Berlin Heidelberg, 2007.

[3] A. Barenghi, L. Breveglieri, I. Koren, G. Pelosi, and F. Regazzoni. Countermeasures Against Fault Attacks on Software Implemented AES: Effectiveness and Cost. In *Proceedings of the 5th Workshop on Embedded Systems Security*, WESS '10, pages 7:1–7:10, New York, NY, USA, 2010. ACM.

[4] I. Biehl, B. Meyer, and V. Mller. Differential Fault Attacks on Elliptic Curve Cryptosystems. In M. Bellare, editor, *Advances in Cryptology CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 131–146. Springer Berlin Heidelberg, 2000.

[5] E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems. In J. Kaliski, BurtonS., editor, *Advances in Cryptology CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 513–525. Springer Berlin Heidelberg, 1997.

[6] J. Blömer and V. Krummel. Fault Based Collision Attacks on AES. In L. Breveglieri, I. Koren, D. Naccache, and J.-P. Seifert, editors, *Fault Diagnosis and Tolerance in Cryptography*, volume 4236 of *Lecture Notes in Computer Science*, pages 106–120. Springer Berlin Heidelberg, 2006.

[7] J. Blömer, M. Otto, and J.-P. Seifert. Sign Change Fault Attacks on Elliptic Curve Cryptosystems. In L. Breveglieri, I. Koren, D. Naccache, and J.-P. Seifert, editors, *Fault Diagnosis and Tolerance in Cryptography*, volume 4236 of *Lecture Notes in Computer Science*, pages 36–52. Springer Berlin Heidelberg, 2006.

[8] J. Blömer and J.-P. Seifert. Fault based cryptanalysis of the Advanced Encryption Standard. Cryptology ePrint Archive, Report 2002/075, 2002. http://eprint.iacr.org/.

[9] D. Boneh, R. A. DeMillo, and R. J. Lipton. On the Importance of Checking Cryptographic Protocols for Faults. In *Proceedings of the 16th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'97, pages 37–51, Berlin, Heidelberg, 1997. Springer-Verlag.

[10] K. Bousselam, G. Di Natale, M.-L. Flottes, and B. Rouzeyre. On Countermeasures Against Fault Attacks on the Advanced Encryption Standard. In M. Joye and M. Tunstall, editors, *Fault Analysis in Cryptography*, Information Security and Cryptography, pages 89–108. Springer Berlin Heidelberg, 2012.

[11] C.-N. Chen and S.-M. Yen. Differential Fault Analysis on AES Key Schedule and Some Countermeasures. In R. Safavi-Naini and J. Seberry, editors, *Information Security and Privacy*, volume 2727 of *Lecture Notes in Computer Science*, pages 118–129. Springer Berlin Heidelberg, 2003.

[12] M. Ciet and M. Joye. Elliptic Curve Cryptosystems in the Presence of Permanent and Transient Faults. *Designs, Codes and Cryptography*, 36(1):33–43, 2005.

[13] C. Clavier. Attacking Block Ciphers. In M. Joye and M. Tunstall, editors, *Fault Analysis in Cryptography*, Information Security and Cryptography, pages 19–35. Springer Berlin Heidelberg, 2012.

[14] J.-L. Danger, S. Guilley, P. Hoogvorst, C. Murdica, and D. Naccache. A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards. *Journal of Cryptographic Engineering*, 3(4):241–265, 2013.

[15] A. Dominguez-Oviedo, M. Hasan, and B. Ansari. Fault-Based Attack on Montgomerys Ladder Algorithm. *Journal of Cryptology*, 24(2):346–374, 2011.

[16] E. Dottax. Fault Attacks on NESSIE Signature and Identification Schemes, 2002.

[17] J. Fan and I. Verbauwhede. An updated survey on secure ecc implementations: Attacks, countermeasures and cost. In D. Naccache, editor, *Cryptography and Security: From Theory to Applications*, volume 6805 of *Lecture Notes in Computer Science*, pages 265–282. Springer Berlin Heidelberg, 2012.

[18] T. Fuhr, E. Jaulmes, V. Lomne, and A. Thillard. Fault Attacks on AES with Faulty Ciphertexts Only. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on*, pages 108–118, Aug 2013.

[19] L. Genelle, C. Giraud, and E. Prouff. Securing AES Implementation against Fault Attacks. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009 Workshop on*, pages 51–62, Sept 2009.

[20] C. Giraud. DFA on AES. Cryptology ePrint Archive, Report 2003/008, 2003. http://eprint.iacr.org/.

[21] C. Giraud and E. Knudsen. Fault Attacks on Signature Schemes. In H. Wang, J. Pieprzyk, and V. Varadharajan, editors, *Information Security and Privacy*, volume 3108 of *Lecture Notes in Computer Science*, pages 478–491. Springer Berlin Heidelberg, 2004.

[22] C. Giraud and A. Thillard. Piret and Quisquater's DFA on AES Revisited. Cryptology ePrint Archive, Report 2010/440, 2010. http://eprint.iacr.org/.

[23] K. Jarvinen, C. Blondeau, D. Page, and M. Tunstall. Harnessing Biased Faults in Attacks on ECC-Based Signature Schemes. In *Proceedings of the 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*, FDTC '12, pages 72–82, Washington, DC, USA, 2012. IEEE Computer Society.

[24] M. Joye, P. Manet, and J.-B. Rigaud. Strengthening hardware AES implementations against fault attacks. *Information Security, IET*, 1(3):106–110, Sept 2007.

[25] M. Karpovsky, K. Kulikowski, and A. Taubin. Differential fault analysis attack resistant architectures for the advanced encryption standard. In J.-J. Quisquater, P. Paradinas, Y. Deswarte, and A. El Kalam, editors, *Smart Card Research and Advanced Applications VI*, volume 153 of *IFIP International Federation for Information Processing*, pages 177–192. Springer US, 2004.

[26] F. Khelil, M. Hamdi, S. Guilley, J.-L. Danger, and N. Selmane. Fault Analysis Attack on an FPGA AES Implementation. In *New Technologies, Mobility and Security, 2008. NTMS '08.*, pages 1–5, Nov 2008.

[27] C. Kim and J.-J. Quisquater. New Differential Fault Analysis on AES Key Schedule: Two Faults Are Enough. In G. Grimaud and F.-X. Standaert, editors, *Smart Card Research and Advanced Applications*, volume 5189 of *Lecture Notes in Computer Science*, pages 48–60. Springer Berlin Heidelberg, 2008.

[28] C. H. Kim. Improved Differential Fault Analysis on AES Key Schedule. *Information Forensics and Security, IEEE Transactions on*, 7(1):41–50, Feb 2012.

[29] A. K. Lenstra. Memo on RSA Signature Generation in the Presence of Faults, 1996.

[30] W. Li, D. Gu, Y. Wang, J. Li, and Z. Liu. An Extension of Differential Fault Analysis on AES. In *Network and System Security, 2009. NSS '09. Third International Conference on*, pages 443–446, Oct 2009.

[31] Y. Li, K. Ohta, and K. Sakiyama. An Extension of Fault Sensitivity Analysis Based on Clockwise Collision. In M. Kutylowski and M. Yung, editors, *Information Security and Cryptology*, volume 7763 of *Lecture Notes in Computer Science*, pages 46–59. Springer Berlin Heidelberg, 2013.

[32] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta. Fault Sensitivity Analysis. In S. Mangard and F.-X. Standaert, editors, *Cryptographic Hardware and Embedded Systems, CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 320–334. Springer Berlin Heidelberg, 2010.

[33] V. Lomne, T. Roche, and A. Thillard. On the Need of Randomness in Fault Attack Countermeasures - Application to AES. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on*, pages 85–94, Sept 2012.

[34] H. Mestiri, N. Benhadjyoussef, M. Machhout, and R. Tourki. An FPGA implementation of the AES with fault detection countermeasure. In *Control, Decision and Information Technologies (CoDIT), 2013 International Conference on*, pages 264–270, May 2013.

[35] A. Moradi, M. T. Shalmani, and M. Salmasizadeh. A Generalized Method of Differential Fault Attack Against AES Cryptosystem. In L. Goubin and M. Matsui, editors, *Cryptographic Hardware and Embedded Systems - CHES 2006*, volume 4249 of *Lecture Notes in Computer Science*, pages 91–100. Springer Berlin Heidelberg, 2006.

[36] D. Mukhopadhyay. An Improved Fault Based Attack of the Advanced Encryption Standard. In B. Preneel, editor, *Progress in Cryptology AFRICACRYPT 2009*, volume 5580 of *Lecture Notes in Computer Science*, pages 421–434. Springer Berlin Heidelberg, 2009.

[37] R.-W. Phan and S.-M. Yen. Amplifying Side-Channel Attacks with Techniques from Block Cipher Cryptanalysis. In J. Domingo-Ferrer, J. Posegga, and D. Schreckling, editors, *Smart Card Research and Advanced Applications*, volume 3928 of *Lecture Notes in Computer Science*, pages 135–150. Springer Berlin Heidelberg, 2006.

[38] G. Piret and J.-J. Quisquater. A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad. In C. Walter, K. tinK., and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2003*, volume 2779 of *Lecture Notes in Computer Science*, pages 77–88. Springer Berlin Heidelberg, 2003.

[39] F. Regazzoni, L. Breveglieri, P. Ienne, and I. Koren. Interaction Between Fault Attack Countermeasures and the Resistance Against Power Analysis Attacks. In M. Joye and M. Tunstall, editors, *Fault Analysis in Cryptography*, Information Security and Cryptography, pages 257–272. Springer Berlin Heidelberg, 2012.

[40] D. Saha, D. Mukhopadhyay, and D. Roychowdhury. A Diagonal Fault Attack on the Advanced Encryption Standard. Cryptology ePrint Archive, Report 2009/581, 2009. https://eprint.iacr.org/.

[41] H. Sakamoto, Y. Li, K. Ohta, and K. Sakiyama. Fault sensitivity analysis against elliptic curve cryptosystems. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on*, pages 11–20, Sept 2011.

[42] Y. Sasaki, Y. Li, H. Sakamoto, and K. Sakiyama. Coupon Collector's Problem for Fault Analysis against AES - High Tolerance for Noisy Fault Injections. In A.-R. Sadeghi, editor, *Financial Cryptography and Data Security*, volume 7859 of *Lecture Notes in Computer Science*, pages 213–220. Springer Berlin Heidelberg, 2013.

[43] J. Schmidt and M. Medwed. A fault attack on ecdsa. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009 Workshop on*, pages 93–99, Sept 2009.

[44] Y. Sung-Ming, S. Kim, S. Lim, and S. Moon. A Countermeasure against One Physical Cryptanalysis May Benefit Another Attack. In K. Kim, editor, *Information Security and Cryptology ICISC 2001*, volume 2288 of *Lecture Notes in Computer Science*, pages 414–427. Springer Berlin Heidelberg, 2002.

[45] J. Takahashi, T. Fukunaga, and K. Yamakoshi. DFA Mechanism on the AES Key Schedule. In *Fault Diagnosis and Tolerance in Cryptography, 2007. FDTC 2007. Workshop on*, pages 62–74, Sept 2007.

[46] S.-M. Yen and M. Joye. Checking before output may not be enough against fault-based cryptanalysis. *Computers, IEEE Transactions on*, 49(9):967–970, Sep 2000.

[47] S.-M. Yen, S. Kim, S. Lim, and S.-J. Moon. RSA speedup with Chinese remainder theorem immune against hardware fault cryptanalysis. *Computers, IEEE Transactions on*, 52(4):461–472, April 2003.