New side-channel attack against scan chains

Jean da Rolt, Marie-Lise Flottes, Giorgio Di Natale, Bruno Rouzeyre

New side-channel attack against scan chains

Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
LIRMM (Université Montpellier II /CNRS UMR 5506)
Montpellier, France
{darolt, dinatale, flottes, rouzeyre}@lirmm.fr

Abstract—**Insertion of scan chains is the most common technique to ensure observability and controllability of sequential elements in an IC. However, when the chip deals with secret information, the scan chain can be used as back door for accessing secret (or hidden) information, and thus jeopardize the overall security. Several scan-based attacks on cryptographic functions have been described and shown the need for secure scan implementations. These attacks assume a single scan chain. However the conception of large designs and restrictions in terms of test costs may require the implementation of many scan chains and additional test infrastructures for test response compression. . In this paper, we present a new generic scan attack that covers a wide range of industrial test infrastructures, including spatial response compressors.**

Keywords – security, testability, scan-based attack

I. Introduction

While scan insertion is one of the most popular Design for Testability (DfT) methods, its use for secure devices, smart cards for instance, opens a backdoor for security threats. “Scan attacks” (e.g. [1]) exploit facilities offered by scan chains to retrieve embedded secret data, e.g. secret encryption keys. These attacks rely on the possibility for hackers to shift out the scan chain content while the circuit contains data correlated with the secret. More precisely, they rely on the possibility to switch the device from mission mode to test mode in order to observe intermediate states of the circuit by means of scan-out operations.

In face of these scan attacks, several counter-measures were proposed, as controlling the access to the chip [1], detecting unauthorized scan shifts [2] or providing confusion in the stream shifted out from the scan chain [3].While these techniques initially address single scan chain circuits, other test architectures must be considered as well, for instance, multiple scan chains with decompression of test vectors and spatial compaction of test responses. Since the compaction reduces the observation of scan-out responses, it could be thought that it sufficiently increases the complexity of the scan attack for preventing such practice (as proposed in [4]).

The attack described in [1] imposes the need of accessing the whole round-register in order to calculate the hamming distance between two values. However, it is possible that the attacker is not able to observe all 128 bits of the round-register. For instance, in presence of response compression, only the parity of the round-register is available out of the chip bounds and the previous attack is not valid anymore. The goal of this method is to propose a new attack against the Advanced Encryption Standard (AES, details are fully described in [5]) that aims at recovering the secret key while observing a subset of FFs related to the secret and controlling the circuit input.

II. Signature Attack

In the first phase of this attack the device implementing the crypto algorithm is modeled and logic simulation is used to predict its behavior. In this phase the attacker must know specifically which information can be observed, for instance it may usually be the whole round-register value, as the attack described in [1], or it may be the parity of the round-register, which is the case of response compression schemes.

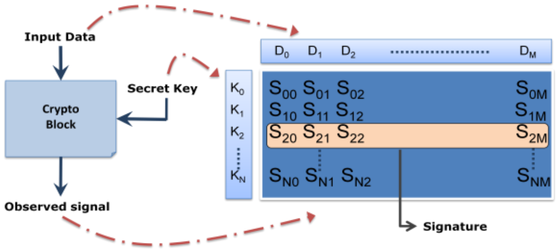
Input Data
Crypto Block
Secret Key
Observed signal
D_0 D_1 D_2 D_M
K_0 K_1 K_2 K_N
S_{00} S_{01} S_{02} S_{0M}
S_{10} S_{11} S_{12} S_{1M}
S_{20} S_{21} S_{22} S_{2M}
S_{N0} S_{N1} S_{N2} S_{NM}
Signature

Figure 1: Pre-attack phase

Figure 1 shows a generic crypto block model and the signature table built in the pre-attack phase. For each secret key value K, all the M possible input data D are simulated and the observed signal S is stored in the table at the right side, creating signatures for all N keys. This procedure is complete when all possible values of both key and input data are covered. It must be noticed that the width of the S elements is exactly the number of observed bits.

Considering the AES as the targeted crypto block, it is known that, when differential attacks are used (when the used output is actually the difference between two measured outputs), the first round can be decomposed in 16 independent datapaths of 8-bit inputs, where each 8 bits of key affects 32 bits of the round-register [1]. In this case, the pre-attack phase consists on generating 16 signature tables, where for all the 256 possibilities of sub-key there is one signature.

After the simulation is over and the signature table is complete, the attacker may start to load the vectors D at the input of the real circuit. This procedure consists of: first, the circuit is reset, secondly a message is loaded at the input of the crypto chip, then the cipher encrypts (just for one round) the message using the secret key (while in normal mode), and finally the attacker force the circuit to enter in test mode and scan out all the data stored in the scan chains. Since we suppose that the circuit is reset after each step and only the AES input message is changed, it implies that only the round-register bits may change. Thus calculating the hamming distance between two scan chains leads to the hamming distance of the desired signal.

Finally, the unauthorized user will proceed by loading at the input of the crypto circuit the messages corresponding to the first row in the signature table. If the collected signal does not correspond to the value stored in one line at the first row, the key respective to that line cannot be the secret key. In doing so, after all pairs are finished there will be only one key left, which is the correct one.

III. Scenarios

The attack model presented in the previous section may be applied to several different scenarios, depending on which information the attacker is able to observe.

A. Observing the 32 bits

In the usual single chain scenario the whole round register is inserted in the scan chain, meaning that the attacker may access all the 128 bits. So in the pre-attack phase, the signature table is built using the hamming distance over all the FFs in the scan chain. Since the attacker normally changes a reduced set of bits of the AES input message, only the 32 round-register bits affected by the correspondent MixColumns could change between two different input messages, so the hamming distance over all flip-flops is exactly the distance over the targeted 32 bits.

As remarked, the AES attack may be split in 16 parts where the data length is 8 bits and the sub-key length is also 8 bits. In this case, the signature table is composed by 256 keys, and the signature is represented by a series of hamming distances (from 0 to 32). Using the algorithm for finding the least number of input vectors results that with only 4 input vectors we can determine the value of a sub-key (8 bits of the secret key), by means of generating 256 different signatures for all the keys. For instance, the input pairs of vectors used for the first byte of the secret key are (105, 223), (223, 143) and (143, 112). At least, repeating the procedure 16 times for each byte of the key lead the attacker to the 128 bits of the secret key.

B. Observing a particular FF

There are many scenarios where the user may have access to partial information on the round-register, e.g. it is possible that some of the FFs from the round-register are not inserted in the scan chain (partial scan design).

In all these cases, the attack described in [1] may not appropriate because it requires the access to the whole round-register. Considering the attack model where at least 4 bits of the round-register are observable, one per block of 32 bits (MixColumns), the signature attack may be used. Each one of these FFs depends on 32 input bits (due to the MixColumn layer) and 32 key bits of key.

Unlike the case shown in Subsection A, the signature in these scenarios will contain one bit per pair (the observed bit) instead of 32 bits. However the principle remains the same, for each subkey the attacker must create a signature table in the pre-attack simulation. Each table has 256 lines (corresponding to the sub key possible value). For each simulated pair, the Hamming distance of the observed bit is stored in the table.

As the differential output of the MixColumns has a different output for each bit, comparing the signature for a particular bit will not collide with other signature belonging to another round-register bit. This allows the identification of the round-register bits in the scan-chain.

If the attacker already knows the position of the 4 bits he/she is observing, than this attack has a complexity of 16 times 13 (number of subkeys times complexity of retrieving one sub key). Regarding this low complexity, we conclude that all bits in the round-register must be protected, otherwise the signature attack may be used by an attacker to retrieve the key.

C. Attacking response compression schemes

In the current state-of-art, there is no attack that considers a very common test practice: the response compression. In presence of a XOR-tree compactor, the hamming distance of the output bitstream is not anymore the same as the round-register hamming distance. Besides that, the work proposed in [4] shows that a compressor such as EDT naturally protect the circuit against scan-attacks.

The signature attack requires the observation of a signal that is related to a reduced number of secret key bits. The parity of the round-register may be used for this purpose. It is straightforward to measure if the parity of the round-register has changed or not (equivalent to the hamming bit over only one bit), once the output bitstream is completely unloaded, its parity is calculated and then if the resulting parity has changed from the previous bitstream, then the parity of the round-register has changed.

The pre-attack phase consists of the simulation of the AES round, where at each step one byte at the input message is changed and the parity over all round-register is stored in the signature table. This procedure generates 16 tables with 256 lines each. In the practical phase, the attacker reads two output bitstreams and calculates the difference of the parity, then he/she searches for the measured signature in the simulation table till the good signature is found and thus the sub key.

In the same way that this instance of the signature attack works for a generic compressor, it is susceptible to be used against other proposed test structures whose parity is observable. Simulations show that 13 vectors are enough for assuring the uniqueness of the signatures.

IV. Conclusion

This paper proposes a generic scan attack that is applicable to several industrial DfT scenarios: single and multiple chains, with or without response compression structures. In the case of single or multiple chains without compression, this attack on AES is optimized so that only 4 vectors have to be applied on the circuit to retrieve one byte of the secret key. The whole key is thus obtained with 2^6 inputs. Aside from the fact that observing only 4 bits of the round-register results in revealing the secret key, it is shown that all bits of the round-register have to be protected. Conversely, only one bit unprotected leads to divide the brute force attack complexity by a factor 2^{32}.

References

[1] Bo Y.; Kaijie W.; Karri R., "Secure Scan: A Design-for-Test Architecture for Crypto Chips", *IEEE Transactions on* CAD, vol.25, no.10, pp.2287-2293, Oct. 2006

[2] Paul S., Chakraborty R.S., Bhunia, S., "VIm-Scan: A Low Overhead Scan Design Approach for Protection of Secret Key in Scan-Based Secure Chips," *Proc VTS 2007.* pp.455-460.

[3] Hely D., Bancel F.; Flottes M.L., Rouzeyre, B., "Test control for secure scan designs," *Proc. ETS 2005*, pp. 190- 195.

[4] Liu C., Huang Y.; "Effects of Embedded Decompression and Compaction Architectures on Side-Channel Attack Resistance," *Proc. VTS, 2007.* pp. 461-468.

[5] http://csrc.nist.gov/publications/PubsFIPS.html