Sophisticated security verification on routing repaired balanced cell-based dual-rail logic against side channel analysis

Wei He , Shivam Bhasin , Andres Otero , Tarik Graba , Eduardo de la Torre , Jean-Luc Danger

Abstract: Conventional dual-rail precharge logic suffers from difficult implementations of dual-rail structure for obtaining strict compensation between the counterpart rails. As a light-weight and high-speed dual-rail style, balanced cell-based dual-rail logic (BCDL) uses synchronised compound gates with global precharge signal to provide high resistance against differential power or electromagnetic analyses. BCDL can be realised from generic field programmable gate array (FPGA) design flows with constraints. However, routings still exist as concerns because of the deficient flexibility on routing control, which unfavourably results in bias between complementary nets in security-sensitive parts. In this article, based on a routing repair technique, novel verifications towards routing effect are presented. An 8 bit simplified advanced encryption processing (AES)-co-processor is executed that is constructed on block random access memory (RAM)-based BCDL in Xilinx Virtex-5 FPGAs. Since imbalanced routing are major defects in BCDL, the authors can rule out other influences and fairly quantify the security variants. A series of asymptotic correlation electromagnetic (EM) analyses are launched towards a group of circuits with consecutive routing schemes to be able to verify routing impact on side channel analyses. After repairing the non-identical routings, Mutual information analyses are executed to further validate the concrete security increase obtained from identical routing pairs in BCDL.

1 Introduction

Modern field programmable gate array (FPGA) devices offer rich configurable resource to implement application-specific digital systems. As one of the major applications, crypto-algorithms in FPGAs may benefit from the lower implementation costs when compared with application specific integrated circuit (ASIC) solutions, and the convenience of including them as sub-modules inside systems for data protection. Users can adjust the algorithm keys or implementation manners with sufficient flexibility to adapt them to different usages. Considering security, crypto-algorithms implemented in FPGAs do not expose structural details of the design, because of the regularity of how its internal logic is arranged. Owing to these features, FPGAs have become attractive platforms for cryptographic applications.

Since side channel attacks (SCAs) were proposed by Kocher *et al.* in [1], data security threats in digital systems lurks beneath the protections features offered by modern cryptographic algorithms. However, these microprocessors, ASIC or FPGA implemented crypto-algorithms have been proven to be vulnerable facing side channel threats because of the 'side channel leakages' typically as the EM and power consumption produced during operations [2–4]. This exploitable information is unintentionally emanated from the atomic logic elements. Once a proper prediction matrix is constructed, the leak amount for specific algorithm points can be estimated. Hence, by making dependency comparison between the hypothetical leakage and the measured side channel leakage, the crypto-key or other confidential information, can be possibly retrieved within a short computation time. Compared with the pure algorithmic cryptanalyses, SCA reveals the secrets by means of the correlation analysis on physical leakage from intermediate logic points during operation. Therefore it requires less computing capabilities and an acceptable analysis time. Additionally, leakage information can be sneakily or remotely gathered from the target devices, without intervening the algorithm function, it poses more serious threats since it cannot be detected and counteracted by traditional defence strategies. Fig. 1 shows a typical setup of EM-based SCA platform, which normally consists of: (i) a target crypto-device; (ii) an EM antenna for measuring the EM radiation from the running device; (iii) an oscilloscope to gather and transfer the EM leakage; and (iv) a computation facility to execute correlation analysis for retrieving the secrets.

Countering strategies against SCA threats have been widely discussed in previous papers. Possible leak points

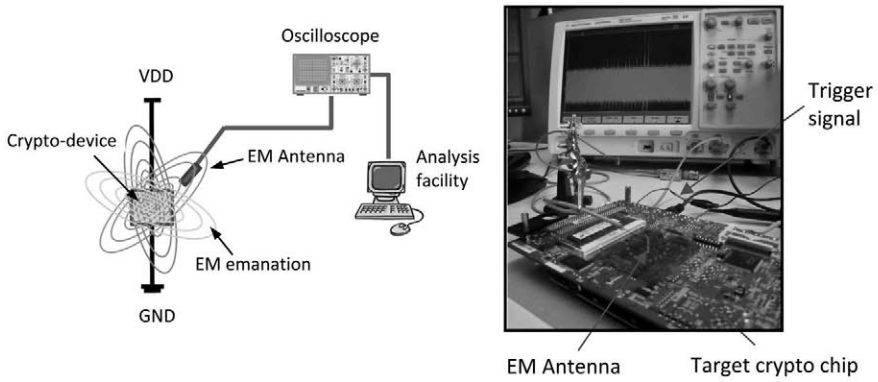

Fig. 1 *Example of setup scheme for EM side channel analysis*

are scattered inside a system from the internal logic elements to the external connectors, such as pin and on-board soldering metal. However, leak source is innately from circuit's fundamental physical cells, that is, transistors and routings. Thus, direct protections on atomic gate-level generally perform better than the algorithmic protections. According to the published works, the studied gate-level countermeasures can be categorised as 'masking' and 'hiding'.

Masking [5, 6] refers to the use of random mask to camouflage critical data that need to be protected. Since the masks used in this protection are random and unknown to the adversaries, the intermediate logic values are not able to be predicted. Therefore the dependence between the hypothetical leakage and measured traces cannot be correlated. However, further researches have revealed that masks can be removed by probability density analyses [7, 8]. Another masking way is to generate noise to submerge the exploitable variants, yet, it can be defeated simply by increasing the number of analysed traces.

Differently, hiding protection approaches flatten the data-dependent variants that can be exploited by differential analysis. It consists on adopting a dual-rail precharge logic (DPL) strategy, in which a generated false (F) rail works simultaneously together with the original true (T) rail for compensating with each other in power or EM behaviours [9, 10]. DPL is controlled using a two-phase protocol ('precharge and evaluation'). During precharge phase, all the values of non-register cells are reset to a fixed state ('0' or '1' in a few cases), whereas evaluation phase switches and propagates valid values from each register to the next register stage. These two phases work alternately with a fixed switching frequency. This protocol theoretically ensures a non-discernible and constant switch manner, and therefore dynamically flattens side channel leakage emitted by the overall system in view of the dual rails. However, the increased security comes at the expense of power, area and complexity, depending on the specific logic styles.

Besides the theoretical assumptions, security of implementation in FPGAs is crippled by the imbalanced parasitic capacitances, induced by routing differences in the T/F signal pair. Let us assume that a pair of net(t) and net (f) have a parasitic capacitance $C(t)$ and $C(f)$, respectively. Owing to the routing variants, $C(t) \neq C(f)$, (e.g. $C(t) > C(f)$). The charged energy $E(t)$–$C(t)$ is different from the charged energy $E(f)$–$C(f)$. Thus, during the transition from precharge phase to evaluation phase, consumed power for this net pair is bigger when net(t) is '1' and net(f) is '0', and smaller if vice versa. This mismatch impairs the perfect compensation for the DPLs in side channel leakage. Routing effects on FPGA implemented DPL have been investigated in [11, 12]. In those works, authors have found that if the corresponding instances are closely placed side-by-side, similar routing paths can be obtained albeit using vendor provided routers. However, only approximately similar shapes can be achieved for the T/F pair, but not identical dual-rail networks. This pitfall still endangers the security assurance facing sophisticated side channel analyses.

In this article, we aim to have verifications of the routing impact for a secure balanced cell-based dual-rail logic (BCDL) [13] implemented AES core with strict dual-rail networks. This work depends on two properties:

- Low fan-out (block RAM [14] implemented) BCDL logic [15] resists side channel analysis on a higher level (e.g. free of glitch/early propagation effect (EPE) and reduced networks) with respect to most of other SCA-resistant logic styles. The major defect of block random access memory (BRAM) BCDL comes from the routing bias between T/F networks that cause imperfect compensation between each net pair.
- The routing repair tool provided in a previous work [16] is able to partially repair the routings from security-sensitive parts to achieve identical net pairs. Since BCDL is immune from most side channel security defects, it is possible to obtain sophisticated security comparisons, exclusively focusing on routing parts.

In the experiments provided in this work, a series of correlation EM analyses (CEMA) attacks are executed to figure out the routing impact against correlation analyses. Mutual information analyses (MIA) is further adopted in order to validate the security increase after the routing repair work. Moreover, timing analyses show greatly reduced time skew compared with previous constrained dual-rail routing methods [11] to stabilise the results obtained in previous real attacks. To the best of our knowledge, it is the first published initiative to date exploring the routing impact based on an EPE-free [17, 18] dual-rail logic with strictly identical networks.

The remainder of this paper is organised as follows. Section 2 discusses the background of SCA-resistant DPLs and secure BCDL styles. Section 3 elaborates the routing barrier in dual-rail system and details the repair work to BCDL implemented crypto-core. A series of security experiments are executed, and results are shown in Section 4. Finally, Section 5 gives the conclusions and perspectives for future work.

2 Background and related work

2.1 Dual-rail precharge style

Based on the principle of 'dynamic compensation', a number of dual-rail logic styles have been devised for counteracting side channel threats and the flaws that exist in many SCA-resistance logic styles.

SCA-targeted dual-rail logic was first proposed in [9] as wave dynamic differential logic (WDDL) based on the principle of 'dynamic compensation'. In this technique, each single gate in the original circuit is replaced by a compound gate which has a pair of complementary T and F gates. A special signal is used to reset the gate outputs to the precharge state during the precharge phase. Yet, the compound gate in WDDL cannot assure identical routing for the true and false rails, which triggers exploitable side channel leakages [6]. Another logic, named masked DPL (MDPL) [19], combines the ideas of WDDL and bit-masking to randomly swap the logic interconnect pairs by majority functions. This helps to obtain a circuit insensitive to routing imbalance, however the power density function is potentially of removing the mask [7] by analysing subsets of the measured traces. Double WDDL presented in [12] uses another WDDL to compensate the routing bias, but the resource cost must be further doubled as well. The suspicious weakness against localised EM measurements also exists.

2.2 Early propagation pitfall

Early evaluation, or called EPE, was first put forward in [17]. A typical gate in ASIC or look-up table (LUT) in FPGA has one or more input nets. It is very likely that a gate has different arrival time between each input if no special constraint is adopted to the routing scheme. A critical problem because of this result is that the switch time for this gate may differ, or a glitch may occur, according to the combination of the input values, while switching between phases. Since the switch time or the glitch is related to the gate input combination, the minor variants induced in power or EM characteristic is data-dependent, and therefore can possibly be exploited by sophisticated side channel measurements.

In previous contributions, some logic styles have been devised straightforward to overcome EPE. Dual-rail random switching logic proposed in [20] guarantees synchronised arrival time before the evaluation phase, yet not before the precharge phase. Seclib [21] resists EPE in nature, but was just for ASICs. secure triple track logic (STTL) [22] uses a third rail as the validation signal to synchronise the inputs. However, the gate type is pretty unique and cannot be implemented easily. iMDPL [23] is a corrected version of MDPL to resynchronise all the inputs by inserting SR-latches. However, the increased complexity is a big concern. Precharge absorbed (PA) PA-DPL introduced in [24] has big decrease of resource cost by absorbing the precharge logic into the LUT itself. Since it is evolved from simple dynamic differential logic (SDDL) style and avoids of swapped T/F rails, PA-DPL can achieve symmetric dual-rail networks both in separate and interleaved placement [24, 25], whereas, further investigation reveals that EPE cannot be fully prevented from the second LUT stage in its combinatorial parts. iWDDL [26] is proposed based on the conclusion in [27] that short combinational path reduces less occurrence of EPE. The extra registers inserted into the combinational path is a big cost however. DPL-noEE [28] resists EPE by the special LUT encoding functions, without using extra synchronisation signals. However, the routing bias has not yet been eliminated as well.

2.3 Low fan-out BCDL

BCDL [15] is a DPL countermeasure specially designed for securing implementations of crypto-systems in FPGAs. The main advantage of BCDL is achieved by a global synchronisation signal named precharge (PRE). A BCDL cell is split into two stages (Fig. 2 – left). The first stage or the 'synchronisation stage' is responsible for synchronising all input signals before being processed. The second stage or the 'data stage' performs the required logical operations. Timing diagram of a BCDL cell is described in Fig. 2 – right. The global synchronisation signal PRE is faster than data signals, since it is routed through high-speed clock buffers of the FPGA. During the precharge phase, the BCDL cell is forced to precharge state instantly without waiting for data signals. During evaluation, the second stage produces an output only when all the inputs are valid and PRE is '1'. A BCDL cell can be imagined as a master slave configuration where the synchronisation stage behaves as a master, which enables the data stage.

Modern FPGAs provide various features which may benefit secure crypto-system implementations. For instance, using the embedded block BRAM, complex functions like an AES substitution box can be easily implemented. In addition, configurable logic block (CLB) in Xilinx series can efficiently implement a two-stage BCDL cell at minimum overhead [13]. Thus, Virtex-5 family possess LUT6 which can be used as one 6-input 1-output LUT or two 5-input 1-output LUT. Similarly, Stratix-II has adaptive look-up table (ALUT) which is capable of implementing two 5-input 1-output LUT, if two or more inputs are

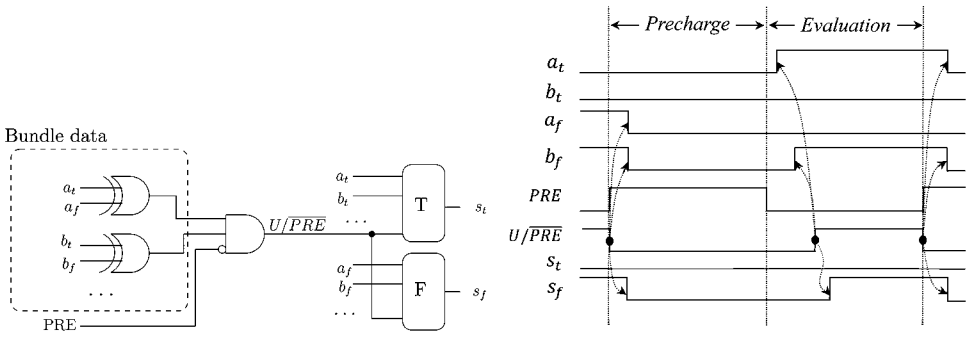

Fig. 2 *n-Input BCDL cell and its timing diagram*

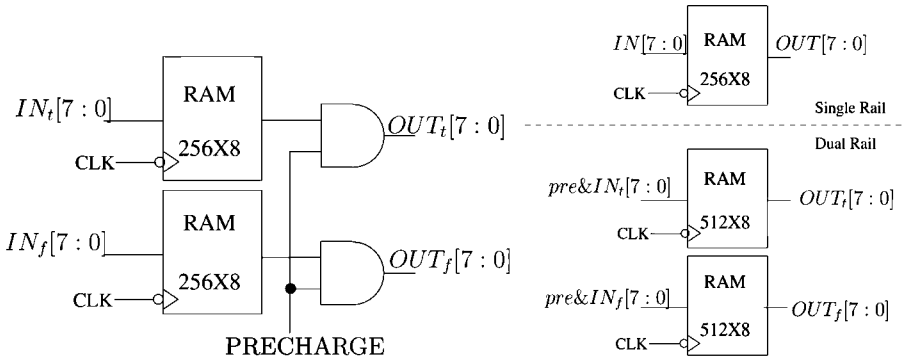

Fig. 3 *Low-cost DPL S-box and a BCDL S-box*

common. A whole 2-input BCDL cell with true and false outputs may be therefore synthesised in a single LUT6-2 or ALUT, that is, a single LUT is calculating the true and the false outputs. Such configuration helps in making a compact design while reducing mismatch between the true and false networks. As in most of other DPL styles, BCDL also has two flip–flop stages. The main characteristics of using a global signal PRE are:

1. PRE with the synchronisation stage counteracts EPE.
2. PRE forces the precharge phase which removes the constraint of using only positive gates (gate without inverter factor in its function [9]), hence low cost.
3. Since PRE is faster than other signals, the precharge phase can be made faster which results in higher throughputs.
4. PRE is used to synchronise (enable) input addresses of memories which allows using BRAM in DPL.

Let us take the example of a substitution box (S-box) in symmetric ciphers, such as the AES. An AES S-box is an $8 \mapsto 8$ bit bijection, defined as $y \mapsto y^{-1}$ in $\mathrm{GF}(2)[x]/x^8 + x^4 + x^3 + x + 1$ if $y \neq 0$ or 0 otherwise. Such a module will have a high fan-out when implemented in glue logic. Therefore BRAM is a popular choice to implement such S-boxes. In DPL, there are several approaches to duplicate the S-boxes. The first way is costly which involves a simple duplication of the RAM. This means that an AES S-box which fits in $2^8 \times 8$ bits (2 kB) needs $2^{16} \times 16$ bits (1 MB) after duplication. In a parallel AES implementation, there are 16 instances of the same S-box, that is, 16 Mb of BRAM is needed. Medium size FPGA might not have these many BRAM resources and therefore would make the implementation infeasible.

The second way to use BRAM in DPL is based on deployment of a special circuitry at the output to enable dual-rail operation. As shown in Fig. 3 – left, an AES S-box is replaced by a true and false S-box of size $2^8 \times 8$. Thereafter, a couple of AND gates are used to precharge the output of the S-boxes. The net overhead of this solution stays a little over two. However, this low-cost implementation (in Fig. 3 – left) is vulnerable to glitches and the input of AND gate can leak information if not implemented properly. Moreover, special routing resources are required to route the the precharge signal to the output of the RAM. Since the precharge signal is only used at the DPL gate inputs, routing precharge signal may require extra efforts. Thus in other DPL styles, using BRAM without glitches will have an exponential area overhead.

The use of BRAM in BCDL is possible because of the presence of a global synchronisation signal PRE. An AES S-box in BCDL needs $2^9 \times 8$ bits (4 kB) of memory for S-box_T and 4 kB for S-box_F (Fig. 3 – right). It is because of the global synchronisation signal that the memory utilisation is increased by 2^{n+2} and not 2^{2n}. The cost can be further reduced to 2^{n+1} by using certain BRAM features [29].

We refer interested reader to [13, 15] for further details on BCDL. In [30], authors have demonstrated that the security of BCDL can be further enhanced by using low fan-out cells in the circuit. Complex cryptographic algorithms like AES rely substitution and diffusion function for security. Therefore it is difficult to provide identical placement and routing to the corresponding gate in the false part which causes routing imbalance. Timing imbalance is also increased with high fan-out. It can be roughly expressed as $\Delta T = K \times F$, where K is the constant capacitance and F is the fan-out.

Scale of fan-out can be reduced by using BRAM. Once used as read-only memories BRAM can make up for complex unstructured or structured high algebraic degree combinational blocks, keeping an unitary fan-out. Such a module will have high fan-out when implemented in glue logic. Therefore BCDL using BRAM is better for FPGA implemented DPL logic in terms of cost, speed and particularly security.

2.4 Attack metrics

We use two SCA tools in our analysis. The first tool is CEMA which is similar to correlation power analysis (CPA) [30] proposed by Brier *et al.* Correlation analysis is a computation of the Pearson correlation coefficient between the side channel leakage L and the leakage model Z, which can be estimated as

$$\text{CPA: } \rho(L, Z) = \frac{\sum_{\{i=0\}}^{n} (l_i - \mu_L)(Z_i - \mu_Z)}{\sigma_L \sigma_Z} \tag{1}$$

where σ and μ denote the standard deviation and the mean, respectively, and n is the traces count. The CEMA is efficient when L and Z are linearly related. Otherwise, the MIA ([31]) is a more appropriate tool as it is agnostic in the joint distribution $(L; Z)$. Mutual information between a sensitive variable Z and a side channel leakage L, measured in bits is

$$\text{MIA: } I(L; Z) = H(L) - H(L|Z) \tag{2}$$

Here, $H(L)$ gives the entropy in bits of L and $H(L|Z)$ gives the conditional entropy of L knowing Z. Many methods have

been proposed to estimate entropy like histograms, kernel density functions, Gaussian parametric estimators etc. [32]. In the experimental work provided in this work, Gaussian parametric estimation is used, where the distribution of L, Z and the joint distribution $(L;\ Z)$ are assumed to be Gaussian. This method might not be ideal for estimating entropy, but works well in practice [32] mainly because of the presence of environmental noise. Nevertheless, other methods of estimating entropy can be applied. For instance, using Gaussian parametric estimation, the entropy of a random variable X can be calculated as

$$H(X) = -\sum_{i} p(x_{\{i\}}) \log_2 p(x_i) = \log_2\left(\sigma_x \sqrt{\pi e}\right) \quad (3)$$

Similar to the counterpart CPA, CEMA evolves from the original differential power analysis (DPA), and introduces a prediction matrix to estimate the states of certain intermediate logic points. This prediction depends on possible key hypotheses and some known information, such as a set of plaintexts or ciphertexts. Since CPA or CEMA is a multi-bit prediction, it efficiently exploits the information hidden inside the collected traces. So the correlation comparison fits better than the matrix used in DPA.

3 Routing issues for symmetric dual-rail

3.1 Routing obstacles in FPGA implementations

Highly balanced dual-rail networks contribute to better dynamic power compensation. Closely deployed T and F nets increase resistance against carefully localised EM measurements. This is mainly due to the fact that the distance-sensitive EM fields from corresponding T and F nets induce matched voltage drops in the EM coil. However, implemented DPL is jeopardised by routing bias from three facts: (i) mainstream FPGAs just provide fixed routing resources. Users cannot freely place logic into a limited fabric area because of the lack of available routing resources; (ii) the routing paths cannot be controlled using vendor provided routers. So the routing lengths and shapes are not able to be predicted; and (iii) previously proposed copy and paste process is hindered by the potential routing conflicts. Thus, special solutions are needed which should be capable of fulfiling the two tasks: (a) provide extensive dual-rail routing control with proper constraints and (b) be capable of reserving the routing resources and prevent conflicts between different routings.

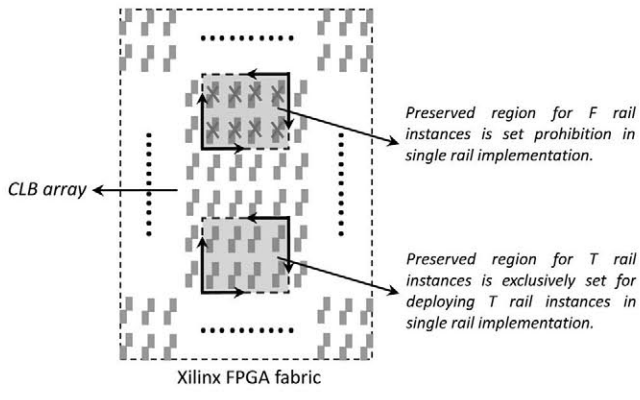

Fig. 4 *Pre-placement for the dual-rail logic*

The duplication method has been used to achieve identical networks, where the designer copies the netlist of the original T rail and relocates it into non-occupied FPGA fabric. As just mentioned, resource conflicts are very likely to occur if the original T part and complementary F part are interleaved or closely located [16]. This fact is produced because the instance or net resource for F part may have already been occupied by previously mapped logic (logic corresponding to the T part or control and I/O block interconnects). One solution to alleviate the resource competition is to discreetly plan the placement in advance, for instance, previously reserving a space for deploying the instances of the F rail. As explained in Fig. 4, the resource for placing the F part may be reserved beforehand as prohibit region. Yet, on the contrary of the placement of logic instances which can be precisely controlled, routing conflicts remain unsolved because routing can still pass through this prohibit region.

3.2 Identical routing techniques

In [33], authors use dummy hard-macros to preoccupy the CLBs that would later be used to place the (F) rails. By this method, all the driver (input) pins and load (output) pins for CLB included in the blocking macro are disabled. Thus, the resource for the CLB block will not be used when routing the T part. This technique exclusively reserves the routing resource for the F logic, but it is not automated because the failed nets after 'sanity check [33]' need to be manually corrected. As well, dummy macros also need to be prepared, and implementation to different devices requires starting work from scratch. Another drawback is blocking the CLB means excluding all the T routing that preferably pass through these CLB blocks. This exacerbates the congestion in surrounding routing arteries.

A routing repair technique is proposed in [16], which is specially used to search the non-identical routing pair or conflicting routing nodes, and repair them in an automatic manner. The precondition of this technique bases on the possible parallel placement between the dual rails of SDDL where swapped nets, which commonly exist in WDDL logic categories, are not used. However, the net pair of each compound gate in BCDL style needs to be synchronised in bundled cells. This, as well, complicates acquiring identical nets. Owing to the characteristics of block RAM, the repair work can be partially applied to the security-sensitive nets.

3.3 Pre-place arrangement for BCDL

The advantage of low fan-out BCDL countermeasure is that it can be applied at the RTL level, which makes it easier to move from one platform to another one. On the other hand, when the platform is fixed, routing techniques can be applied to improve BCDL. As demonstrated in [13], the reduction of fan-out improves the robustness of BCDL implementations. Whereas, low fan-out circuit still has some leakage present which can be exploited by a stronger attacker. In this work, we apply the identical routing technique to improve the security of a simplified AES core in low fan-out BCDL implementation.

Low fan-out in block RAMs offer an opportunity to partially obtain parallel net paths between complementary networks. Implementing the T and F S-box in different BRAM provides parallel formats for the T and F S-box outputs. The synchronous clock controlling the BRAM outputs ensures glitch-free SubByte outputs.

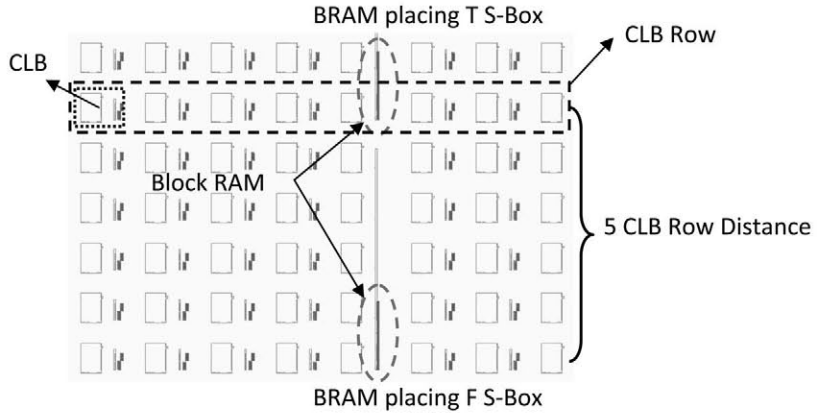

Fig. 5 *Placement of neighbouring BRAM in Xilinx Virtex-5 FPGA*

In this work, we choose the BRAM outputs (i.e. S-box outputs) as the target to repair, and also as the nets on which the attack will be done. In spite that a single BRAM in Xilinx Virtex-5 FPGA is sufficient to implement two independent S-box blocks, a couple of neighbouring BRAMs are chosen to locate the T and F S-box. In Xilinx Virtex-5 series, 20 CLB rows and 4 block BRAM are equally distributed in each clock region. As a view from FPGA-editor in Fig. 5, the neighbouring BRAMs have a distance equivalent with a width of five CLB-row in the applied FPGA. Since we use the BRAM to implement the S-box, the complementary output pair between the T and F BRAM also have the same distance to obtain parallel rails. The pre-place arrangement involves placing the corresponding output registers to the locations where all the complementary elements universally have identical distances. Xilinx placement tool, like PlanAhead, can easily fulfill this task.

A simplified AES-co-processor is used as the testing core. Fig. 6 gives the architecture of the encryption core. It starts with an 8 bit XOR blocks, followed by an 8 bit S-box. The outputs of the BRAM are stored in registers. Encryption key is fixed to a specific value and all 256 possible inputs are fed using an LFSR. Since the biggest logic part S-box in the core part is implemented using a BRAM instead of logic elements, BCDL implementation of this core is mainly applied to the Bitxor operations (Fig. 7). The circuit runs on SASEBO-GII evaluation board. Side-chanel attack standard evaluation board (SASEBO)-GII has two FPGAs soldered on it: a Spartan-3 (XC3S50A) and a Xilinx Virtex-5 (XC5VLX30). Only the Virtex-5 FPGA is used to implement the crypto-algorithm.

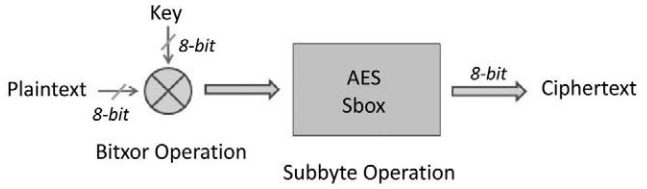

Fig. 6 *Tested simplified 8 bit AES core*

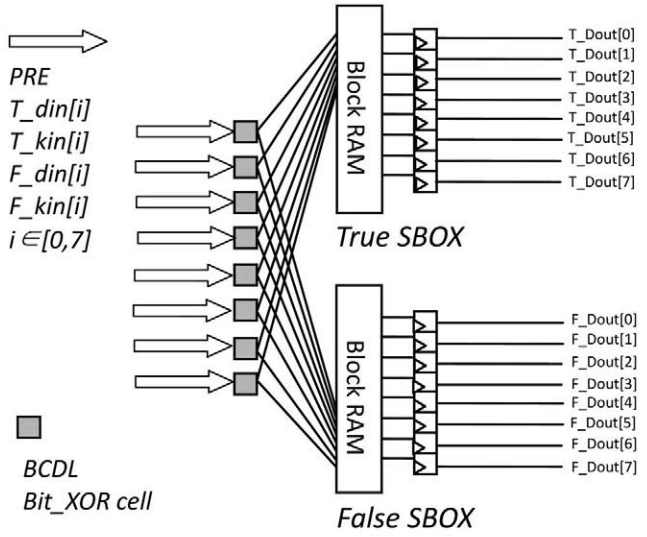

Fig. 7 *Dual block RAMs implemented simplified AES core*

3.4 Routing repair process

The routing repair process is done using the repair tool presented in [16]. It detects the routing shapes of each pair of complementary nets. Once a non-identical net pair is

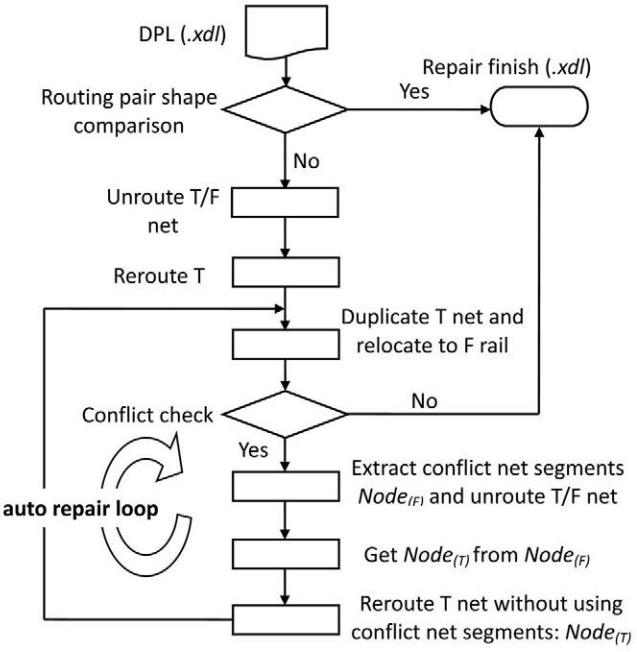

Fig. 8 *Customised automatic repair loop for achieving identical networks*

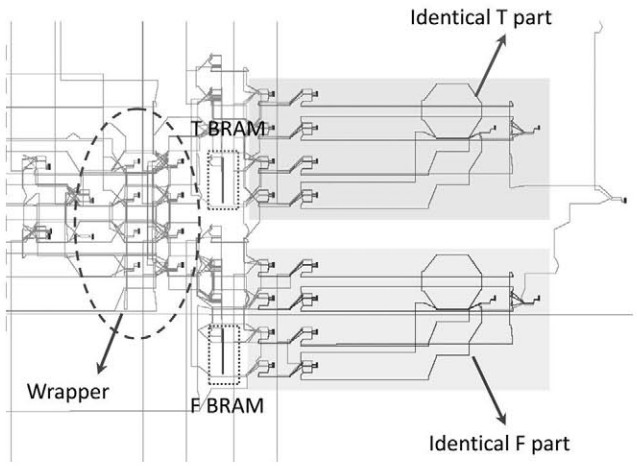

Fig. 9 *Routing repaired BCDL simplified AES in which T/F S-box is implemented by two neighbouring BRAM*

found, a repair mechanism is activated to repair non-identical nets in the process loop described in Fig. 8.

The repair tool is constructed on RapidSmith [34, 35], which is a set of Java-based application programming interface (API) s, offering access to the low-level resources of the FPGA. This way, RapidSmith provides an easy way of building up specific purpose computer-aided design tools for Xilinx FPGAs. All process steps in Fig. 8 ((a) compare net shapes and find non-identical nets; (b) search conflict nodes; and (c) reroute the unrepaired nets etc.) are done automatically just by giving the unrepaired design in XDL format. Features offered by this tool are exploited in this work to reshape the target nets for obtaining identical T/F nets. The names of BCDL dual rails need to be modified so as to be recognised by the repair tool. This task can be done by a regular expression based script embedded into this customised tool. It is just needed to define the area parameters of the fabric where the unrepaired nets reside. After the repair process, the BCDL implemented 8 bit dual-rail AES is obtained, which has identical T/F S-box output nets, as shown in Fig. 9. Wrapper part in this circuit represents the feeding logic, such as LFSR, and the drive logic to cyclically enable the encryptions.

4 Security validations

4.1 Investigation on prolonged nets

As discussed in Section 2.2, block RAM implemented BCDL has the merits of low fan-out and less complexity, compared with most of other DPLs, and also has been proven to be more secure against side channel analysis. This higher security brings trouble to investigate variants for different BCDL schemes, since a very large number of samples is always needed, or being even impossible to be detected using normal equipment. According to author's experience, a pair of dual rails in parallel may yield very similar networks, albeit using vendor provided router if the nets are not densely routed. In this work, the testing circuit is quite small since S-box blocks have been embedded into BRAMs. The low network density brings similar net pairs that are discarded for comparison, since it does not represent the real scenario when a complete AES core or other complex algorithm is under testing, including dense networks resulting in non-identical T/F net pairs. Commercial routers make routing paths obtained to be different, even when equivalent routing resources are totally free.

Owing to these observations, we intentionally strengthen the routing related EM side channel leakage by prolonging the target nets to have a better identification of the routing involved security factors. It facilitates the security check without weakening the fairness. The used routing scheme is presented in Fig. 10 – left. The S-box output nets are extended to the farthest corner in the Virtex-5 fabric. By this measure, we can have more obvious security identification because of the strengthened EM emanation arising from the use of long nets. The auto routed BRAM output nets are illustrated in Fig. 10 – right, in which the true nets and the complementary false nets have very different routing paths as it presents.

4.2 CEMA test analyses

In our work, CEMA is used to check the security improvement for the BRAM-based BCDL implemented simplified AES after the routing repair work. Measurement setup consists of a 54 855 Infiniium Agilent oscilloscope with a bandwidth of 6 GHz and a maximal sampling rate of 20 G sample/s, antennae of the HZ-15 kit from Rohde & Schwarz. These antennae are able to capture very precise EM signals from the decoupling capacitor of the FPGA. Since there are several decoupling capacitors on the testing FPGA board that control different clock regions, the most suited one is chosen by trial-and-error methodology. Once a suitable capacitor is found traces for each input combination are acquired. The traces were acquired at a sampling rate of 2 G sample/s for the simplified AES at 24 MHz clock frequency. The experiments are executed based on the following aspects:

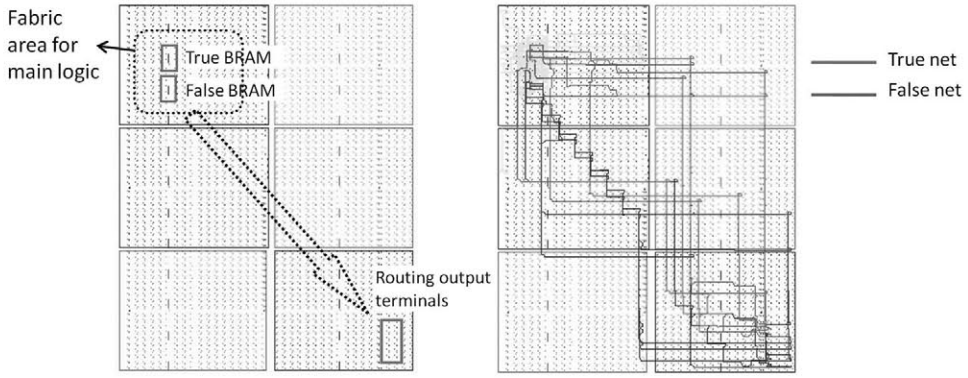

Fig. 10 *Target EM leakage is strengthened by prolonged nets (imbalanced networks)*

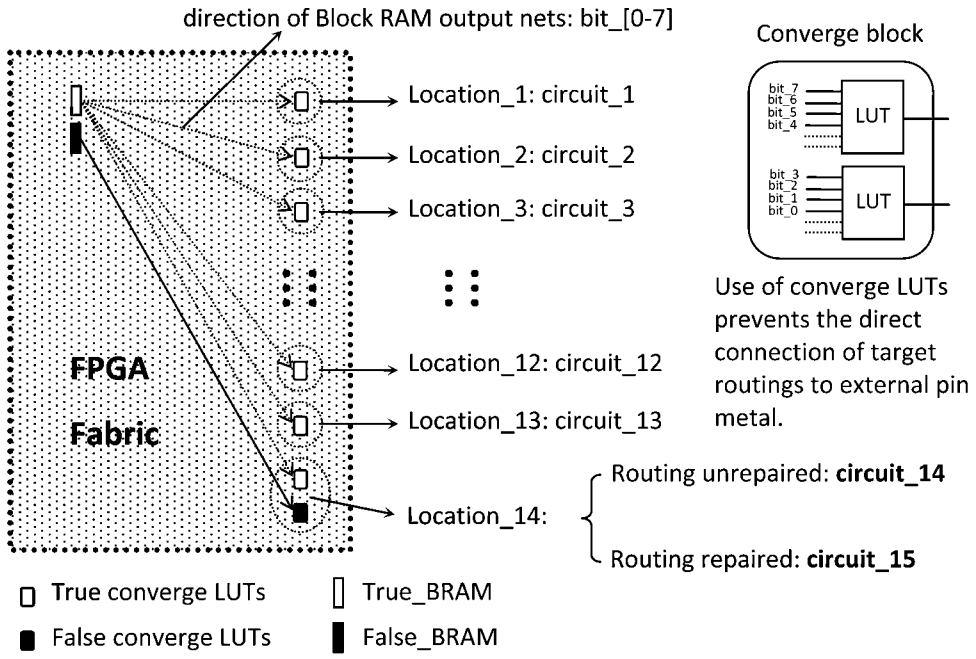

Fig. 11 *Asymptotic routing strategy*

1. Block RAM implemented BCDL poses exploitable leakage from the routing bias of security-sensitive parts.
2. BRAM naturally does not behave as a leakage source, except the I/O pins [24].
3. BCDL 'bundle' cell and synchronised T/F BRAM ensure no glitch and EPE in tested simplified AES block.
4. We disable the connection to external output pins to eradicate the unfair strengthened EM emanation from metal solder balls on seating plane of the testing board.

The testing work is executed in six phases:

1. Setting the S-box output nets in Fig. 6 as target nets. Nets of bit [0–7] are converged to two extra LUTs; we hereby name them 'converge LUTs'. Therefore target nets do not need to be connected to external pins. This solution fairly guarantees that the target EM leakage is solely emitted from internal routings, but not strengthened by external on-board solder balls.
2. We intentionally relocate the F converge LUTs to the farthest corner of the target Xilinx Virtex-5 FPGA, so as to have longer net paths and therefore yield stronger, but fair EM emanation from the target nets.
3. Deploy the T converge LUTs into the clock region far away from the clock region where F converge LUTs resides, and then move to T converge LUTs to the clock region close to F converge LUTs step-by-step, as explained in Fig. 11.
4. We set 14 consecutive steps for this asymptotic comparison. As the normal design, Xilinx tool is used to route all the nets, without considering the needs for net symmetry.
5. Since T/F converge LUTs have the same distance as that between the T/F BRAMs in circuit_14, we can use the customised routing repair tool to obtain the circuit_15 with identical routing pair from circuit_14.
6. CEMA attacks are launched, respectively, to all the 15 circuits with 300 000 EM traces in each analysis.

A snippet of the repair report from phase V is given below. According to the report, 8 bit BRAM output net pairs are non-identical. Since the extended nets pass through a section of the fabric which has plenty of free routing resource, only bit1, bit2 and bit7 need two loops to find proper identical routing paths for both T and F nets without conflicts. All the rest bits successfully find the routing path with just one repair iteration. This analysis can be further compared with the repair result in [16], where all the nets inside a crowded fabric are repaired and some net pairs need even six iterations to find a feasible path because of the routing jam.

```
Asymmetric repair is starting:
** Shape comparison is running
0 T/F net pair are equal in shape
8 T/F net pair are unequal in shape
** List of eight asymmetric T net:
asymmetric T nets are: ooo_dout_⟨7⟩
asymmetric T nets are: ooo_dout_⟨0⟩
asymmetric T nets are: ooo_dout_⟨1⟩
asymmetric T nets are: ooo_dout_⟨3⟩
asymmetric T nets are: ooo_dout_⟨4⟩
asymmetric T nets are: ooo_dout_⟨2⟩
asymmetric T nets are: ooo_dout_⟨5⟩
asymmetric T nets are: ooo_dout_⟨6⟩
** List of nets that are partially outside of the rectangle: total number of nets that are inside of rectangle: 8
...
...
**- Repair iteration report
/0/ ooo_dout_⟨6⟩ **Successful**. Reroute iteration: 1
/1/ ooo_dout_⟨5⟩ **Successful**. Reroute iteration: 1
/2/ ooo_dout_⟨1⟩ **Successful**. Reroute iteration: 2
/3/ ooo_dout_⟨0⟩ **Successful**. Reroute iteration: 1
/4/ ooo_dout_⟨3⟩ **Successful**. Reroute iteration: 1
/5/ ooo_dout_⟨4⟩ **Successful**. Reroute iteration: 1
/6/ ooo_dout_⟨7⟩ **Successful**. Reroute iteration: 2
/7/ ooo_dout_⟨2⟩ **Successful**. Reroute iteration: 2
There are 0 conflicting net(s) failed in repair. (Failed nets are kept unrouted!)
Creating output file: top_repaired.xdl
Time collapsed is: 4 s
** Repair work is finished
```

Table 1 CEMA attacks with asymptotic routing schemes

Attacked circuits	Routing pair identical	F converge LUT location	T converge LUT location	The key (hex) with highest correlation[a]	Correlation value of highest key ($\times 10^{-3}$)	Rank position of the right key ('C6')	Correlation value of right key ($\times 10^{-3}$)
Circuit_1	×	14	1	'B1'	82	2	67
Circuit_2	×	14	2	'77'	72	4	61
Circuit_3	×	14	3	'2D'	71	6	59
Circuit_4	×	14	4	'94'	65	8	53
Circuit_5	×	14	5	'2A'	66	33	46
Circuit_6	×	14	6	'D3'	64	32	41
Circuit_7	×	14	7	'04'	59	10	51
Circuit_8	×	14	8	'5A'	61	40	41
Circuit_9	×	14	9	'70'	70	63	37
Circuit_10	×	14	10	'A2'	72	38	41
Circuit_11	×	14	11	'18'	69	166	24
Circuit_12	×	14	12	'56'	67	167	26
Circuit_13	×	14	13	'78'	66	130	27
Circuit_14	×	14	14	'B0'	78	143	29
Circuit_15	√	14	14	'E2'	68	174	22

Higher the ranking position is, the easier the right key is likely to be differentiated out
[a]CEMA attacks: 300 000 EM traces/circuit (real algorithm key 'C6' (hex)). Descending rank positions show a rising difficulty to differentiate the right key

We launched 15 CEMA attacks, respectively, on the 15 circuits with different routing schemes. From the circuits 1–14, Xilinx router is used to select the routing paths. Since vendor provided router finds the optimised short path from each path source to the path sink, the T/F path lengths are roughly obtaining closer by steps from circuit 1 to circuit 14. We strictly adjust the T output nets without touching other parts of the circuit, and the comparison attacks are all done in the same testing environment, so we kept the effect from unexpected factors under the same level.

In each attack, 300 000 EM traces are gathered under the same testing environments for each circuit. Table 1 demonstrates the testing results. The ranking position of the correlation value for the right key 'C6' in all the 256 possible keys are generally obtaining lower by step. The results indicate the routing impact for correlation attacks to

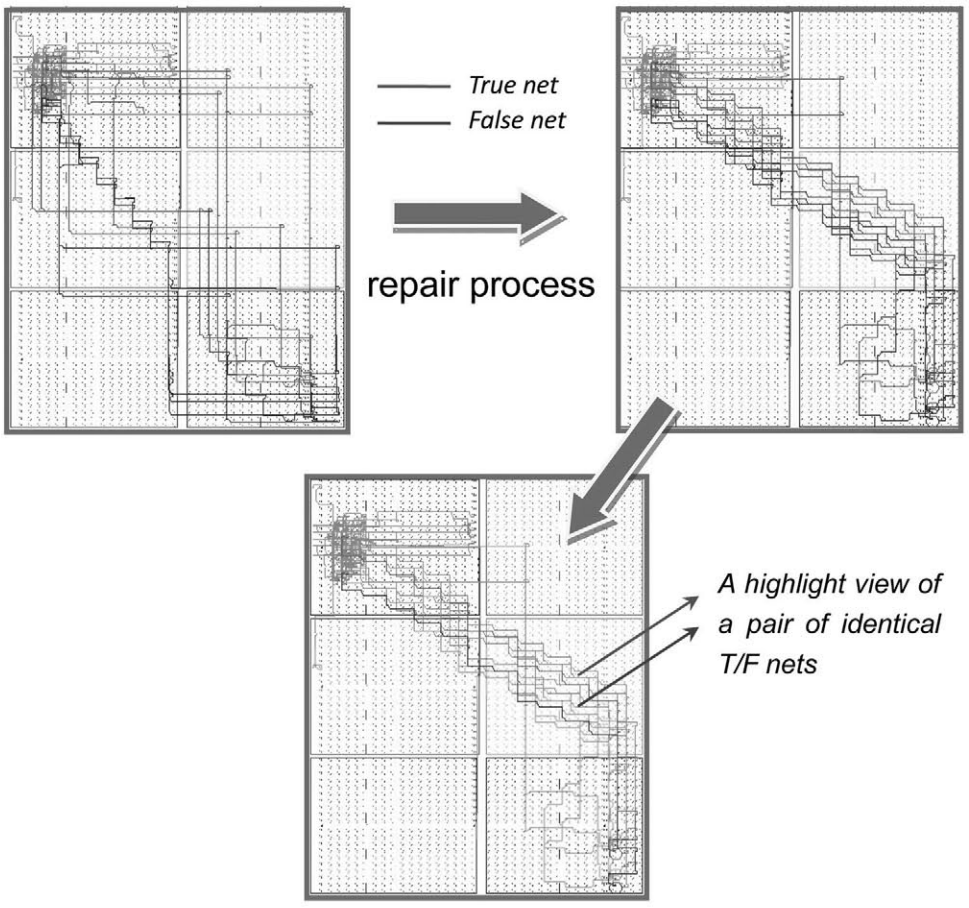

Fig. 12 *Identical (balanced) T/F target nets are obtained after the repair process*

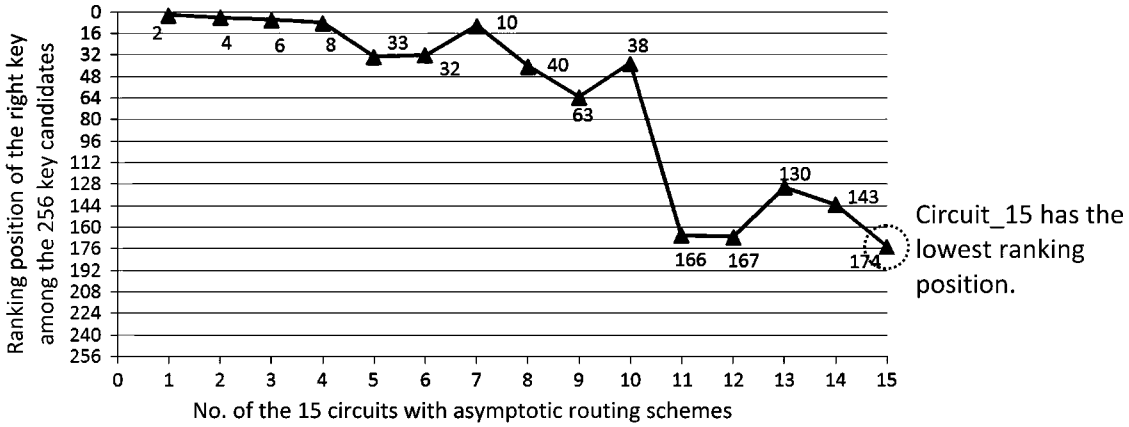

Fig. 13 *Plot of the right key position in the correlation rank of all 256 possible keys*

the crypto-core, that is, more routing variants lead to easier right key differentiation from the rest key candidates. More precisely, two routings with similar lengths have similar parasitic capacitance. So, they compensate with each other better than net pair with bigger length variants in dual-rail compensation manner. It should be pointed out that the ranking positions for the right key do not show monotonic decrease. This is mainly because of the statistic feature of the measurements that cannot fully eliminate the random environmental factors which slightly impacts the analysis results. This effect can be minimised by significantly increasing the analysed traces. Although the results shown here are sufficient to present changing trend.

Using the routing repair tool introduced in Section 3.5, circuit 15 is obtained by repairing the non-identical net pair of circuit 14 with precisely and fully identical T/F outputs, as plotted in Fig. 12. The same EM attack is done to circuit 15, and the right hexadecimal key 'C6' ranks the lower position compared with the rankings from previous tests. The result reveals weaker correlation between the hypothetical leakage and actual measured leakages because of the improved compensation, as specified in Table 1. The right key ranking position among the 256 key candidates for the 15 circuits is plotted in Fig. 13, which demonstrates the observed general change trend.

Even with positive experiment results, we note that these tests just show rough results because of the characteristic of statistics. Noise affecting the results from other factors cannot be fully eradicated. For instance, in some tests, ranking position of right key for circuit 15 varies might be

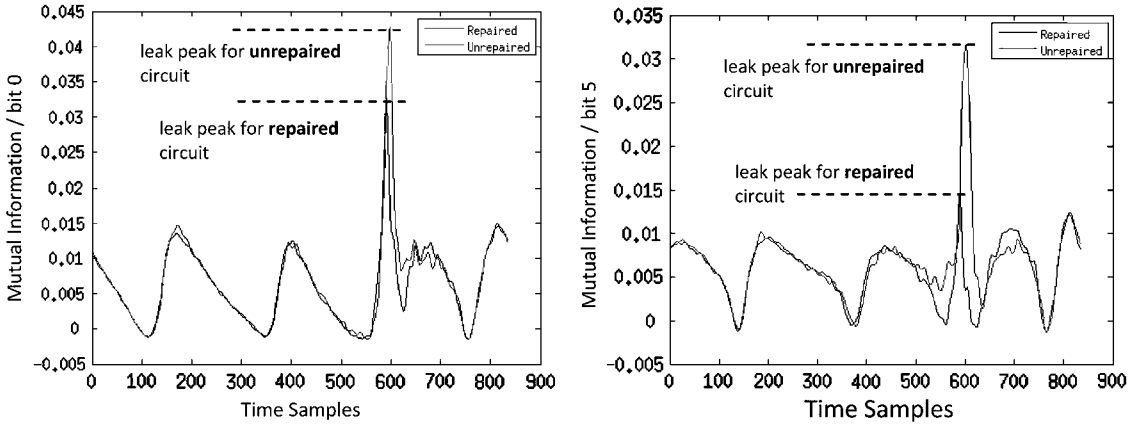

Fig. 14 *MIA analyses for two S-box output bits*

Table 2 Peak mutual information value for different output bits

Architectures	Bit 0	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
unrepaired	0.043	0.048	0.053	0.013	0.041	0.032	0.035	0.022
repaired	0.033	0.039	0.040	0.015	0.028	0.013	0.029	0.017
difference	0.010	0.011	0.013	−0.002	0.013	0.029	0.006	0.005

Table 3 Net delays for T and F rails (upper two values) and time skew (lower value) comparison for the 15 described test circuits

Number of circuits	bit0_t bit0_f abs_dif, ns	bit1_t bit1_f abs_dif, ns	bit2_t bit2_f abs_dif, ns	bit3_t bit3_f abs_dif, ns	bit4_t bit4_f abs_dif, ns	bit5_t bit5_f abs_dif, ns	bit6_t bit6_f abs_dif, ns	bit7_t bit7_f abs_dif, ns	*Average abs_dif, ns
Circuit 1	2.873 7.733	2.609 7.451	3.412 7.370	3.572 6.929	3.434 9.118	3.694 7.308	3.44 8.706	3.694 9.013	4.613
	4.86	4.842	3.958	3.357	5.684	3.614	5.266	5.319	
Circuit 2	3.079 7.733	3.317 7.451	3.708 7.370	3.585 6.929	3.147 9.118	3.963 7.308	3.785 8.706	3.678 9.013	4.421
	4.654	4.134	3.662	3.344	5.971	3.345	4.921	5.335	
Circuit 3	3.097 7.733	3.57 7.451	4.683 7.370	4.88 6.929	3.938 9.118	3.888 7.308	4.505 8.706	4.036 9.013	3.879
	4.636	3.881	2.687	2.049	5.18	3.42	4.201	4.977	
Circuit 4	3.782 7.733	4.051 7.451	4.918 7.370	4.971 6.929	3.547 9.118	3.907 7.308	5.065 8.706	5.302 9.013	3.511
	3.951	3.4	2.452	1.958	5.571	3.401	3.641	3.711	
Circuit 5	3.824 7.733	4.501 7.451	5.793 7.370	4.937 6.929	3.841 9.118	4.221 7.308	5.299 8.706	4.862 9.013	3.294
	3.909	2.95	1.577	1.992	5.277	3.087	3.407	4.151	
Circuit 6	4.000 7.733	4.498 7.451	5.794 7.370	5.316 6.929	5.345 9.118	4.062 7.308	5.443 8.706	5.715 9.013	2.932
	3.733	2.953	1.576	1.613	3.773	3.246	3.263	3.298	
Circuit 7	6.059 7.733	4.186 7.451	6.292 7.370	6.158 6.929	5.808 9.118	4.562 7.308	6.016 8.706	5.714 9.013	2.354
	1.674	3.265	1.078	0.771	3.31	2.746	2.69	3.299	
Circuit 8	6.58 7.733	5.448 7.451	6.408 7.370	5.868 6.929	6.058 9.118	6.087 7.308	6.583 8.706	6.375 9.013	1.778
	1.153	2.003	0.962	1.061	3.06	1.221	2.123	2.638	
Circuit 9	6.393 7.733	5.227 7.451	6.641 7.370	6.953 6.929	6.739 9.118	4.968 7.308	6.909 8.706	7.1 9.013	1.593
	1.340	2.224	0.729	0.024	2.379	2.34	1.797	1.913	
Circuit 10	6.78 7.733	5.373 7.451	7.155 7.370	6.808 6.929	7.352 9.118	6.551 7.308	6.175 8.706	7.548 9.013	1.236
	0.953	2.078	0.215	0.121	1.766	0.757	2.531	1.465	
Circuit 11	6.669 7.733	6.155 7.451	7.952 7.370	7.747 6.929	7.505 9.118	5.776 7.308	7.594 8.706	7.71 9.013	1.165
	1.064	1.296	0.582	0.818	1.613	1.532	1.112	1.303	
Circuit 12	6.963 7.733	6.511 7.451	7.707 7.370	7.142 6.929	7.971 9.118	6.271 7.308	8.5 8.706	8.26 9.013	0.675
	0.77	0.94	0.337	0.213	1.147	1.037	0.206	0.753	
Circuit 13	7.543 7.733	7.105 7.451	8.772 7.370	7.127 6.929	7.101 9.118	7.504 7.308	8.826 8.706	8.868 9.013	0.577
	0.19	0.346	1.402	0.198	2.017	0.196	0.12	0.145	
Circuit 14	7.317 7.733	7.106 7.451	8.975 7.370	9.907 6.929	8.25 9.118	7.149 7.308	9.024 8.706	9.84 9.013	0.940
	0.416	0.345	1.605	2.978	0.868	0.159	0.318	0.827	
Circuit 15	6.059 6.056	6.814 6.814	7.549 7.539	7.415 7.409	10.553 10.553	10.655 10.656	5.889 5.889	6.292 6.291	0.003
	0.003	0.000	0.010	0.006	0.000	0.001	0.000	0.001	

*Average abs-dif: absolute differences of the observed routing pairs are averaged in order to demonstrate the general decreasing net bias from asymptomatic routing scheme.

a little higher than circuit 14. Thus, it is not sufficient to have stabilised conclusion. Accordingly, we resort to MIA to have further security verification.

4.3 MIA test analysis

Although correlation analyses (CPA or CEMA) are known to be very efficient for a given leakage model, MIA can sometimes outperform CPA if the hypothetical model is not precisely constructed because of the deficient knowledge about the target device or the unpredictable environmental/ device noise. In an ideal DPL circuit, the information leaked in the side channel is zero. Owing to the imbalance between the true and false parts in real implementation, some leakage is inevitably present. We assume this leakage to be slightly related to Hamming weight model given the construction of circuit and two-phase operation [13]. In this case study, MIA is preferably to be used since it can reveal weak information leakage and find both linear and non-linear dependencies between the model and leakage. Thus, MIA reveals minor dependence variants that CPA may fail to discover.

To analyse the circuits 14 and 15 against MIA, the EM activity of the circuit is observed. Fig. 14 details the leakages plots from bit 2 and bit 5, respectively. X dimension in the plots shows the time of activity. Y dimension is the quantified mutual information. Red and blue curves show leakages from the unrepaired (circuit 14) and repaired (circuit 15) circuits, respectively. The information leak point resides around the sample point 600. A higher peak indicates more leaked information. It can be clearly observed that the repaired circuit leaks less information than the unrepaired one from the nets of the S-box output bits. The MIA plots of most other signals show similar results: less time skew leaks less information. The MIA comparisons for all the 8 bits are given in Table 2, which shows reduced information leakage for seven of these bits, with only an exception for bit 3. Compared with the CEMA analyses, MIA tests show stable results when comparing the security between the circuit 14 and circuit 15. Since circuit 15 is directly obtained from circuit 14 by repairing the non-identical target nets without touching rest part, and both circuits run in the same testing environment, it is hence safe to conclude that it is the identical routing that contributes to the concrete security improvement.

4.4 Further discussion

Repair work exclusively operates on the target nets that are user defined without touching any other logic part. The result above can be further attested with the timing result in Table 3, where complete timing results for all the S-box output nets are extracted using Xilinx timing tool. The timing results show a reducing average net delay difference (indicated as 'Ave abs_dif') from circuit 1 to circuit 15 and generally matches the falling right key ranking position presented in Table 1 and Fig. 13.

Comparison between the unrepaired (circuit 14) and repaired (circuit 15) circuits clearly represents the significantly decreased time skew between each T/F net pair. As given in Table 2, the S-box output nets from the unrepaired circuit 14 have an averaged time skew of 940 ps. Comparatively, the time skew from the repaired circuit 15 is merely 3 ps. It should be noted that even delay differences still exist in some net pairs after the repair process, it does not jeopardise the safety since such tiny time variants (maximal 6 ps in this test case) cannot practically be captured and differentiated by side channel measurements. It therefore guarantees the fairness of our verification.

5 Conclusions and perspective for future work

A major security obstacle for FPGA implemented SCA-resistant DPL is the routing bias between the complementary T/F nets. In this article, the security evaluation based on a simplified AES core in Xilinx Virtex-5 FPGA is systematically elaborated. Block BRAM implemented BCDL benefits from the low fan-out and EPE-free merits, and thus has good resistance against side channel threats. Thereby, since highly secure BCDL resists SCA from an upper level, it implies increasing the evaluation costs to figure out the security variations when improving the methodology. In this article, we specially strengthened the EM leakages from the routings under evaluations by intentionally extending the routing lengths. Owing to this measure, it is possible to easily and fairly evaluate the routing impact on the security resistance against CEMA and MIA attacks. Accomplished security validations are executed by two routing strategies:

1. CEMA attacks are launched towards a series of circuits that reduces the routing bias using asymptotic routing scheme by Xilinx router. Testing results show that the circuits with less routing skew are fortified with better resistance against correlation analyses.
2. A routing repair technique is adopted to reshape the non-identical routing pairs to obtain strictly symmetric dual-rail routing networks. Sophisticated MIA analyses display much less information leakage from the circuit with highly identical routing pairs.

Timing analysis reveals significantly minimised time skew (from average 940 to 3 ps) between the corresponding T/F nets of target routings in this test case, which stabilises the results obtained in previous CEMA and MIA attacks.

In the future work, we plan to have more sophisticated routing security evaluation by optimising the measurements, and improving the testing precision for nets without prolonging the length.

6 Acknowledgments

This work was supported by the Spanish Ministry of Economy and Competitiveness under the project Dynamically Reconfigurable Embedded Platforms for Networked Context-Aware Multimedia Systems (DREAMS) with number TEC2011-28666-C04-02. It is also partly supported by the Strategic International Cooperative Program (Joint Research Type), Japan Science and Technology Agency (JST) and the French Agence Nationale pour la Recherche (ANR), via grant for project Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems (SPACES). Besides, we are grateful to the Sylvain Guilley (Institut Mines-Telecom) for interesting comments about the MIA evaluations.

7 References

1 Kocher, P., Jaffe, J., Jun, B.: 'Differential power analysis'. Proc. Int. Conf. Cryptology, Santa Barbara, California, USA, August 1999, pp. 388–397

2 Messerges, T., Dabbish, E.: 'Investigations of power analysis attacks on smartcards'. Proc. Int. WorkShop on SmartCard Technology, May 1999

3 Ors, S.B., Gurkaynak, F., Oswald, E., Preneel, B.: 'Power-analysis attack on an ASIC AES implementation'. Proc. Int. Conf. Information Technology: Coding and Computing, Las Vegas, USA, April 2004, vol. 2, pp. 546–552

4 Ors, S.B., Oswald, E., Preneel, B.: 'Power-analysis attacks on an FPGA-first experimental results'. Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems, Cologne, Germany, September 2003, pp. 35–50

5 Akkar, M.-L., Giraud, C.: 'An implementation of DES and AES secure against some attacks'. Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems, Paris, France, May 2001, pp. 309–318

6 Chari, S., Jutla, C., Rao, J.R., Rohatgi, P.: 'Towards sound approaches to counteract power-analysis attacks'. Proc. Int. Conf. Cryptology, Santa Barbara, California, USA, August 1999, pp. 398–412

7 Schaumont, P., Tiri, K.: 'Masking and dual-rail logic don't add up'. Proc. Int. Workshop of Cryptographic Hardware and Embedded Systems, Vienna, Austria, September 2007, pp. 95–106

8 Tiri, K., Schaumont, P.: 'Changing the odds against masked logic'. Int. Workshop Selected Areas in Cryptography, SAC 2006 LNCS, vol. 4356, pp. 134–146

9 Tiri, K., Verbauwhede, I.: 'A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation'. Proc. Int. Conf. Design, Automation and Design in Europe, Paris, France, February, 2004, pp. 246–251

10 Agrawal, D., Archambeault, B., Rao, J.-R., Rohatgi, P.: 'The EM sideChannel(s)'. Proc. Int. Workshop of Cryptographic Hardware and Embedded Systems, Cologne, Germany, September 2003, pp. 29–45

11 Guilley, S., Chaudhuri, S., Sauvage, L., *et al.*: 'Place-and-route impact on the security of DPL designs in FPGAs'. Proc. Int. Symp. Hardware-Oriented Security and Trust, CA, USA, June 2008, pp. 29–35

12 Yu, P., Schaumont, P.: 'Secure FPGA circuits using controlled placement and routing'. Proc. Int. Conf. Hardware/Software Codesign and System Synthesis, Salzburg, Austria, September 2007, pp. 45–50

13 Bhasin, S., Guilley, S., Souissi, Y., Graba, T., Danger, J.-L.: 'Efficient dual-rail implementations in FPGA using block RAMs'. Proc. Int. Conf. Reconfigurable computing and FPGAs, Cancun, Mexico, November 2011, pp. 261–267

14 Xilinx User Guide UG190(v5.4). Available at http://www.xilinx.com/support/documentation/user_guides/ug190.pdf, accessed March 2012

15 Nassar, M., Bhasin, S., Danger, J.-L., Duc, G., Guilley, S.: 'BCDL: a high performance balanced DPL with global precharge and without early-evaluation'. Proc. Design, Automation and Test in Europe, IEEE Computer Society, Dresden, Germany, March 2010, pp. 849–854

16 He, W., Otero, A., De La Torre, E., Riesgo, T.: 'Automatic generation of identical routing pairs for FPGA implemented DPL logic'. Proc. Int. Conf. Reconfigurable Computing and FPGAs, Cancun, Mexico, December 2012, pp. 1–6

17 Suzuki, D., Saeki, M.: 'Security evaluation of DPA countermeasures using dual-rail pre-charge logic style'. Proc. Int. Workshop of Cryptographic Hardware and Embedded Systems, Yokohama, Japan, October 2006, pp. 255–269

18 Kulikowski, K., Karpovsky, M., Taubin, A.: 'Power attacks on secure hardware based on early propagation of data'. Proc. Int. Symp., On-line Testing, Lake Como, Italy, July 2006, pp. 131–138

19 Popp, T., Mangard, S.: 'Masked dual-rail pre-charge logic: DPA-resistance without routing constraints'. Proc. Int. Workshop of Cryptographic Hardware and Embedded Systems, Edinburgh, UK, August 2005, pp. 172–186

20 Chen, Z., Zhou, Y.: 'Dual-rail random switching logic: a countermeasure to reduce side channel leakage'. Proc. Int. Workshop of Cryptographic Hardware and Embedded Systems, Yokohama, Japan, October 2006, pp. 242–254

21 Guilley, S., Flament, F., Pacalet, R., Hoogvorst, P., Mathieu, Y.: 'Security evaluation of a balanced quasi-delay insensitive library'. Proc. Int. Conf. Design of Circuits and Integrated Systems, Grenoble, France, November 2008, p. 6

22 Soares, R., Calazans, N., Lomne, V., Maurine, P., Torres, L., Robert, M.: 'Evaluating the robustness of secure triple track logic through prototyping'. Proc. Int. Symp. Integrated circuits and Systems Design, NY, USA, September 2008, pp. 193–198

23 Popp, T., Kirschbaum, M., Zefferer, T., Mangard, S.: 'Evaluation of the masked logic style MDPL on a prototype chip'. Proc. Int. Workshop of Cryptographic Hardware and Embedded Systems, Vienna, Austria, September 2007, pp. 81–94

24 He, W., De La Torre, E., Riesgo, T.: 'A precharge-absorbed DPL logic for reducing early propagation effects on FPGA implementations'. Proc. Int. Conf. Reconfigurable Computing and FPGAs, Cancun, Mexico, November 2011, pp. 217–222

25 He, W., De La Torre, E., Riesgo, T.: 'An interleaved EPE-immune PA-DPL structure for resisting concentrated EM side channel attacks on FPGA implementations'. Proc. Int. Workshop on Constructive Side-Channel Analysis and Secure Design, Darmstadt, Germany, May 2012, pp. 39–53

26 McEvoy, R.P., Murphy, C.C., Marnane, W.P., Tunstall, M.: 'Isolated WDDL: a hiding countermeasure for differential power analysis on FPGAs', ACM Trans. Reconfigurable Technol. Syst. (TRETS), 2009, vol. 2, (1), pp. 1–23

27 Kirschbaum, M.: 'Investigation of DPA-resistant logic styles'. MS thesis, Graz University of Technology, 2007

28 Bhasin, S., Guilley, S., Flament, F., Selmane, N., Danger, J.-L.: 'Countering early evaluation: an approach towards robust dual-rail precharge logic'. Proc. Int. Workshop on Embedded Systems Security, Scottsdale, USA, October 2010, p. 6

29 Bhasin, S., He, W., Guilley, G., Danger, J.-L.: 'Exploiting FPGA block memories for protected cryptographic implementations'. Proc. Int. Workshop on Reconfigurable Communication-centric Systems-on-Chip, Darmstadth, Germany, July 2013

30 Brier, E., Clavier, C., Olivier, F.: 'Correlation power analysis with a leakage model'. Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, MA, USA, 2004, Springer, (*LNCS,* **3156**), pp. 16–29

31 Batina, L., Gierlichs, B., Prou, E., Rivain, M., Standaert, F.-X., Veyrat-Charvillon, N.: 'Mutual information analysis: a comprehensive study', *J. Cryptol.* 2011, **24**, pp. 269–291

32 Prouff, E., Rivain, M.: 'Theoretical and practical aspects of mutual information based side channel analysis'. Proc. Int. Conf. Applied Cryptography and Network Security, Paris-Rocquencourt, France, June 2009, pp. 499–518

33 Velegalati, R., Kaps, J.-P.: 'Improving security of SDDL designs through interleaved placement on Xilinx FPGAs'. Proc. Int. Conf. Field Programmable Logic and Applications, Crete, Greece, September 2011, pp. 506–511

34 Lavin, C., Padilla, M., Lamprecht, J., Lundrigan, P., Nelson, B., Hutchings, B.: 'RapidSmith: do-it-yourself CAD tools for Xilinx FPGAs'. Proc. Int. Conf. Field Programmable Logic and Applications, Chania, Greece, September 2011, pp. 349–355

35 Lavin, C., Padilla, M., Lamprecht, J., Lundrigan, P., Nelson, B., Hutchings, B.: 'HM-flow: accelerating FPGA compilation with hard macros for rapid prototyping'. Proc. Int. Symp. Field-Programmable Custom Computing Machines, Salt Lake, USA, May 2011, pp. 117–124