Asynchronous Dual-Rail Transition Logic for Enhanced DPA Resistance

Rajath Srivathsav N[1], Prathiba A[2] and V S Kanchana Bhaaskaran[3]
[#]School of Electronics Engineering, VIT University, Chennai – 600127
[1]rajath.srivathsav2013@vit.ac.in
[2]prathiba.a@vit.ac.in
[3]vskanchana@gmail.com

Abstract - An Asynchronous Dual–Rail Transition Logic (ADTL) is proposed in this paper. The new logic style can be used in the encryption circuit of cryptography to counter the differential power analysis (DPA) attacks. The resistance to the DPA attacks is achieved by randomizing the power dissipated in the circuit through Manchester input signal coding and unpredictable initial state of the toggle flip-flops (T-FF). The proposed logic uses two wires to transmit the signal, in the form of a single transition on either one of the two wires to indicate the input logic value. T-FFs are employed to randomize the power dissipated by the circuit. The randomizing is made possible by making the initial states of the flip-flops un-deterministic. Furthermore, the clock is completely eliminated in the conceived design, thus realizing increased power randomization and resistance to the DPA attacks. The design is demonstrated through the systematic simulations on a typical encryption circuit. The validation of the ADTL is made through extensive comparisons with the existing Dual-rail Transition Logic (DTL) for power, delay and the DPA resistance. Industry standard EDA tools with 90nm technology libraries provided by the UMC foundry have been employed in the designs.

Keywords—Differential Power Analysis, Dual-Rail Transition Logic, Dual-Edge Triggered Flip-Flops.

I. INTRODUCTION

Cryptology is the study of sending the message in the encrypted form, from one person to another in the presence of a third person such that the third person will not be able to understand the message. Cryptology study focuses on two major branches, namely, (1) cryptography, which is an art of hiding the message in the encrypted form and (2) cryptanalysis, which is an art of breaking the encryption in an unorthodox way to obtain the information back. Cryptanalysis attacks [1][2][3] mainly concentrate on the loop holes of the process mechanisms used while sending the message, either through the algorithm used in the encryption process, or through the leakage currents obtained from the hardware. Recent literatures [1] - [8] identify that the attacks concentrate on the hardware parameters, such as the delay, the electromagnetic radiation or the power dissipation and they are normally non-invasive. By analyzing these parameters, the intermediate data under process can be hacked. This is known as the *side channel attack*. Among these types of attacks, the power analysis attacks are very easy, non-invasive and efficient to conduct. Hence, many researchers focus on countering the power analysis attacks.

The major divisions in the power analysis attack are *Simple Power Analysis* (SPA) attacks and *Differential Power Analysis* (DPA) attacks [2]. The SPA attack is done with a rough idea of the encryption circuit and is carried out with the help of one or two power traces. On the other hand, the DPA attacks are purely statistical in nature. This is due to the fact that irrespective of the knowledge of the encryption circuit, the set of power trace obtained are mapped to the set of power trace from the hypothetical intermediate key power trace. The mostly matching power trace will provide the key of the encryption mechanism. The DPA attacks have several variants such as the correlation power analysis attacks, the zero–input DPA attacks and the frequency based DPA attacks. In order to avoid these power analysis attacks, several circuits have been proposed in the literature [3].

In the algorithmic level, it was revealed that the number of toggles is the leakage factor and can be used to hack the data [4]. Hence, the circuit or the cell level encryption circuits were introduced to counter such attacks. Some typical circuits were the Sense Amplifier Based Logic (SABL) and Wave Dynamic Differential Logic (WDDL) [3]. These circuits employ the pre-charge logic to produce unvarying or constant power dissipation. The architectures, namely, the Masked Dual rail Pre-charge Logic (MDPL) [9] and the Random Switching Logic (RSL) [10] produce random power traces to alleviate the attacks. The power traces normally has a relation to the data under processing. Hence, the Dual-rail Transition Logic (DTL) [1] was proposed to randomize the power traces. The DTL de-correlates the data under process and the power dissipated by the circuit. This was realized with the help of introducing random initial states for the toggle flip-flops (T-FF), which could be configured by adding a key, to either *set* or *reset* the flip flop. As the power dissipation is different for the positive and negative transitions as decided by the initial state of the T-FF, the probability of identifying the power traces grows exponentially for the same input/s, making it increasingly resistant to the DPA attacks [11].

However, the drawback found in the DTL logic circuit is its clock dependency, which results in the leaking of the clock information through the periodic power traces. This paper proposes an Asynchronous Dual-rail Transition Logic (ADTL) circuit to remove such a dependency of the power trace on the clock. The ADTL circuit aims at removing the clock related information from the circuit, such that the power traces are completely randomized and it renders the circuit resistant to the DPA attacks.

The proposed design focuses on the following:

- The logic followed in the design of dual rail transition logic is employed.
- Dual edge triggered flip-flops [11] [12] [13] have been employed to detect the data from the Manchester coding block.
- Manchester coding has been used for the representation of the input data for conversion to DTL logic.
- The reference signal is generated according to the functionality of the logic required and the input data.
- Dual edge triggered flip-flops are employed in the receiver end for converting the data back to the original logical signal.

The paper is arranged is as follows: The foundations of the proposed ADTL and the design methodology are explained in Section II. The design of the individual blocks used in the circuit and the operating features of the blocks are presented in Section III. The results obtained through simulations of the circuits and the inferences are elaborated in Section IV and Section V concludes the paper. Section VI suggests the future work.

II. METHODOLOGY

The logic of the proposed asynchronous dual rail transition model is explained in this section. It also explains how the ADTL proves to be more DPA resistant than the existing DTL logic. Exhaustive simulations have been carried out to compare the performances through the transient input waveform patterns and the resulting output power patterns.

A. Asynchronous Dual Rail Transition Logic:

The proposed ADTL model is derived from the DTL model [1]. In the present work, the clock is eliminated entirely to avoid the clock dependence [14] [15]. In place of the clock signal, the inherent data edges are used for signaling the transition on the complementary wires. In order to realize this, the transmission signal encoding of data is used to identify the data pattern even while taking care of the long runs of *zeroes* or *ones*. Using the data and its transmission signaling, the logical signals can be converted to DTL signals with the help of dual edge triggered flip flops. Fig. 1 shows the signaling of the data used in the proposed logic. The conversion of the data from logical to DTL without the help of an external clock and the data edges, in either the logical or DTL form is used for further processing. Hence, it can be inferred that the proposed design is an asynchronous version of the DTL [16] [17].

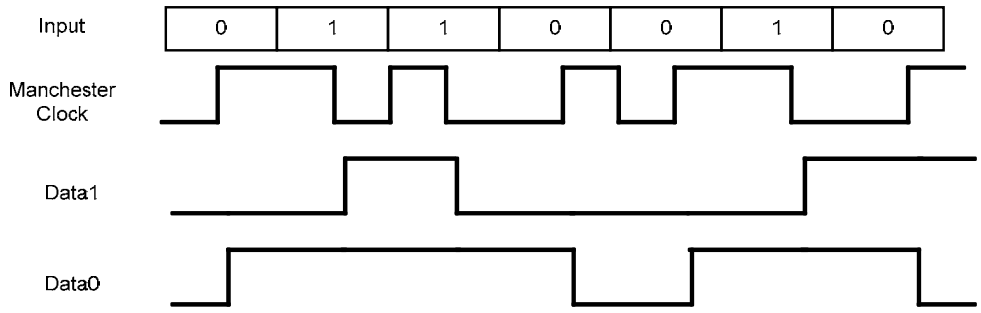

Fig. 1 ADTL Signaling of data

To explain the proposed logic better, a brief overview of the existing logic is presented below, with justifiable comparisons. At the end of this section, the theoretical advantages of the proposed logic are highlighted.

1) *Transition Signaling Logic:*

Transition signaling is one of the low power communication protocols, which uses the type of transition happening on the line to transmit the data from the source to destination. In other words, the signal *zero* is transmitted with no transition on the line, while the signal *one* is transmitted with a single transition, either from *one* to *zero* or from *zero* to *one* on the transmission line at the clock edge. The transition signaling is shown in Fig. 2. The limitation with the transition signaling is that there can be long runs of *zeroes* in the input, and the transmission line may not have any transitions. This can lead to addition of noise signals which may send a wrong data to the receiver end. It may be pointed out that at the receiver end, the exact frequency of the clock and its pulse width must be known for the decryption process, failing which, the decryption of the transition signal may lead to a wrong or faulty data.

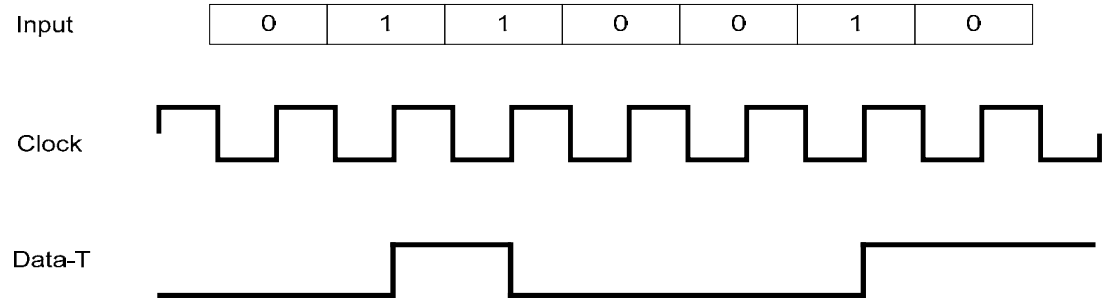

Fig. 2 Transition Signaling of data

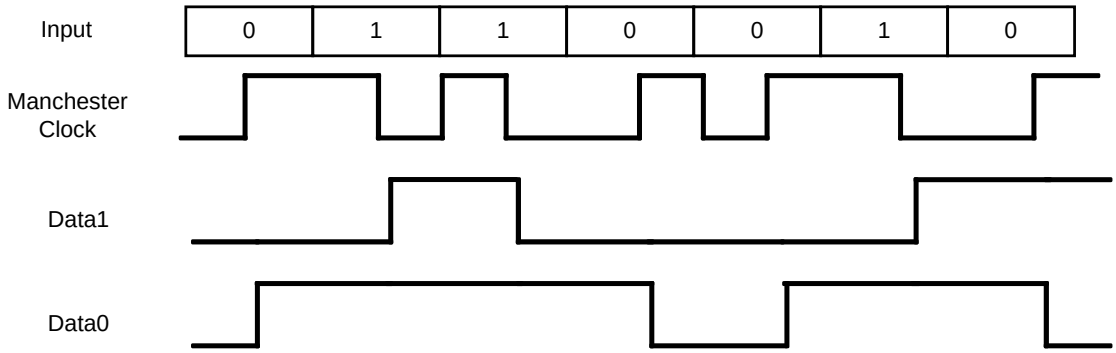

Fig. 3 DTL Signaling of data

2) *Dual rail transition Logic:*

The limitation of the transition signaling model has been taken care of in the DTL signaling model, in which a complimentary wire is added so that every data bit may be transmitted with a transition. That is when the consecutive data transmitted are alternate *zeroes* and *ones* then, the data *zero* will be transmitted with the transition on the *zero* wire, and the data *one* will be transmitted with the transition on the *one* wire at the clock edge. Hence, the problem of the long runs of *zero* is taken care of by the transition on the *zero* wire. The DTL signaling model is as depicted in Fig. 3. The clock frequency can be built by the use of the successive transitions. Hence, the receiver will have no difficulty in finding out the exact frequency of the clock.

However, the disadvantage in this type of transition is the overhead incurred by the clock, since the data is transmitted only at the clock edge even though the data is available beforehand. Furthermore, two clock signals are needed, one for the data conversion and another for the data encryption, which in turn causes an additional overhead for the circuit. Another limitation of this model is that the clock frequency is embedded into the signal transitions and hence, the power trace of the circuit reveals the clock information. This can be used by the hacker to find out the clock edge at which the data is sent, thus making the hacking possible.

3) The advantages of ADTL:

The advantages of the proposed ADTL are listed below.

- The data can be transmitted with varying pulse widths since the data and Manchester waves are interdependent. At the output of encryption, there will be a small positive pulse to indicate the two successive zeroes. In the same way, a small pulse from one to zero and back to one will indicate two successive ones.
- The data transfer depends on the input patterns and on the pulse width of individual data bits, which is allowed to change dynamically and hence the data traces are highly resistive to the side channel attacks.
- Since the design is clock independent, the clock overhead delay problem is completely eliminated, which improves the circuit speed performance.
- Timing of the circuit is asynchronously monitored by the handshaking signals involved in the proposed model and hence, the check for the timing violations is not required.

B. Transmission Signal Encoding:

The format of the data encoding process being practiced for communicating the *zeros* and *ones* are known as transmission signal encoding. The input of the ADTL logic is encoded in the signaling formats, since the logic evaluates on the positive or the negative edge of the data signal. A signal fed in an un-encoded form might well be hacked using the signal transitions so as to reveal the information regarding the data. The properly encoded signaling format hides the actual signal transitions by introducing more transition which will not be

synchronous. Majorly, there are three types of widely used signaling techniques, namely, Manchester, Non – Return to Zero (NRZ) and Return to Zero (RZ).

1) Manchester:

Manchester signaling is used to code the input signal without revealing the transition in the input signal [18]. This is carried out by following the logic of RZ partially. In this method, for the input value of *one* in the data, the signal remains the same, while the signal for indicating a *zero* value is given by *zero* in the first half of data signal width, followed by a signal *one* for the next half period. This coding method hence detects both the *ones* and *zeroes*, even if there happens to be a long run of same value. This feature makes this signaling technique very useful for the ADTL logic. The proposed ADTL exploits this advantage, and it acts as a reference to detect the value of the input given to the circuit. A sample signal transient of this logic is shown in Fig. 4.

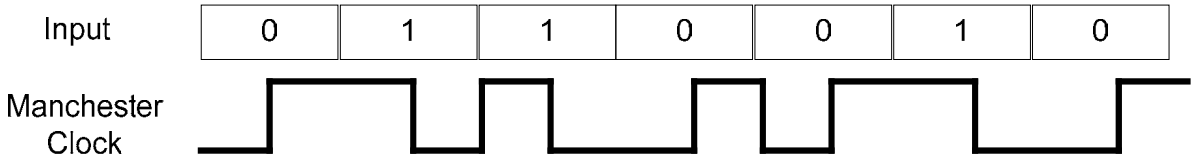

Fig. 4 Manchester Signaling of data

2) Non – Return to Zero:

As the name indicates, the signal transitions come into the focus, whenever the input signal won't return to *zero*. This falls into two types, namely, the NRZ – Level (NRZL) and the NRZ – Invert (NRZI). In the NRZL, the signal will retain its previous value when the input signal is not brought back to the *zero* level as shown in Fig. 5. On the other hand, in the case of the NRZI, the signal value is inverted when the input signal value is not brought back to *zero*. These signals cannot be used in the ADTL, due to the reason that when there happens to be a long run of *zeroes* or *ones*, then the NRZL will be able to identify the *zeroes* of the signals, and not the *ones*. On the other hand, the NRZI can identify the long runs of *ones* but not the *zeroes*. Hence, these signal formats will fail in detecting the number of consecutive values of the same logic state and hence is not applicable for the ADTL.

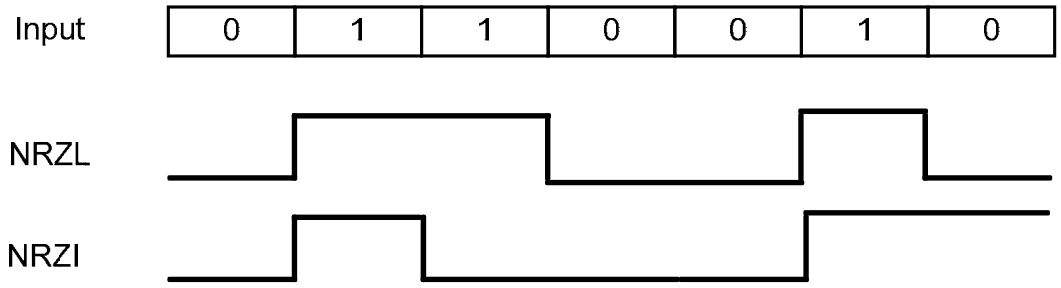

Fig. 5 Non Return to Zero Signaling of data

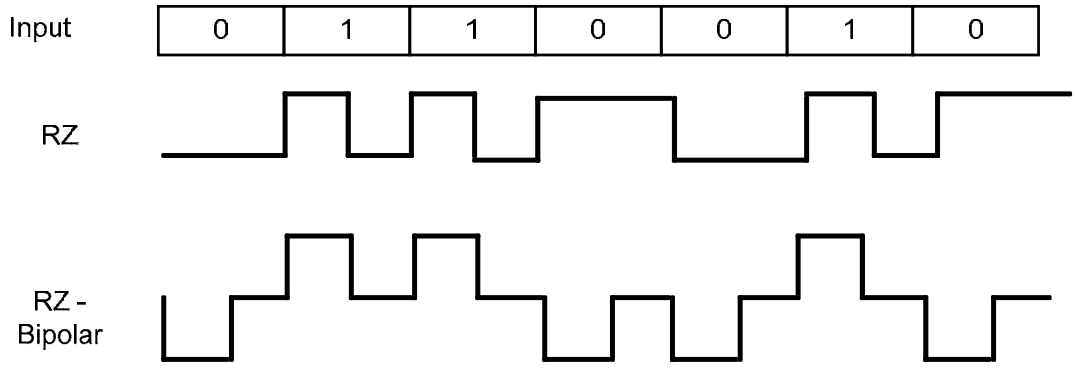

Fig. 6: Return to Zero Signaling of data

3) Return to Zero:

Return to Zero (RZ) signaling is a technique in which the signal value of the input signal is indicated by the relative transitions within the signal. If the signal value is *one*, then the signaling will have half of its period as *one* followed by the next half period as a *zero*. Similarly for a *zero*, there will be no transition in the middle of the signal and the signal will remain at *one*, and for the next *zero* bit occurring in the input, there will be an inversion of the RZ signal with its value staying in *zero*. This can help in detecting the successive *zero* value

after the present *zero* value. A sample signaling representation of RZ is shown in Fig. 6. The transition during the value *one* and no transition during the value *zero* is the disadvantage of RZ, which may result in complicating the detector circuit. This disadvantage can be avoided by using the bipolar transmission signal where the *zero* will have the negative transition for half of the cycle and then for the next half of the cycle it will be *zero*. This method introduces the scheme with a negative voltage level as shown in Fig. 6. It may be noted that it needs a three level mechanism, which is unsuitable for the digital logic systems that follows *true* and *false* states as the only two available states.

III. DESIGN OF THE INDIVIDUAL BLOCKS

This section presents the block schematic of the typical design developed to demonstrate the methodology of operation of the ADTL. The logical data input values signaled in the Manchester encoding is employed as the reference to convert the data into the dual transitions. The encryption of the input signal uses the Manchester reference of the same input values. This encrypted data is silent to side channel power attacks, since as can be observed, it relies completely on the current data values. Even if the current information has been hacked, it will not be useful for further intrusion, since the reference of encryption is designed to be the signal itself. Finally, the encrypted data in the form of dual rail traces are converted back to logical signals for transmission along the channel. The block diagram depicting the operation of the proposed asynchronous scheme is shown in Fig. 7.

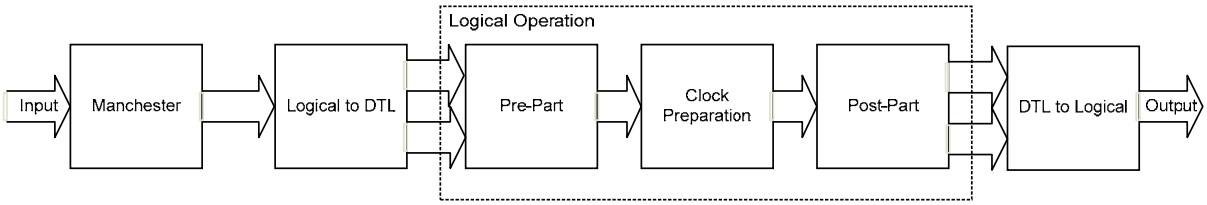

Fig. 7 Basic Block Diagram for the Operation of ADTL

A. Data input representation and Manchester Signaling:

The data representation of the ADTL employs the Manchester encoding. The Manchester encoding is elaborated in this sub-section. The Manchester encoder block is as shown in the Fig. 8. In this block, the period of the data length is represented as a signal with 50% duty cycle was as depicted in Fig. 4 which implements Manchester encoding. The logical data which is XORed with the input signal to provide the Manchester encoding also has the same duty cycle. To identify the data back from the Manchester encoding, the single edge triggered flip-flops are not sufficient, since the data in Manchester coding is represented by both positive and negative transition. Hence, the data indicator uses a dual transition edge triggered flip flops instead of single edge triggered flip flops [19].

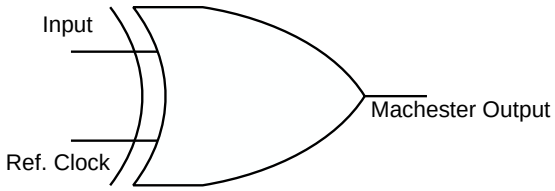

Fig. 8 Logical to Manchester signal encoding

B. Data converter from Logical to DTL:

This block is used to convert the Manchester encoded logical data into the dual transitions using the DTL block. This is carried forward for the encryption purposes. Fig. 9 shows the data converter from logical to DTL which has two dual edge triggered T flip-flops (DETTFF) with one of the inputs as logical data and its compliment fed as the other input. The reference pin to both the flip-flops is provided by the Manchester wave, which produces the outputs at line 1 and line 0.

When the input signal is *one* and if there is a transition in the Manchester wave in either the positive edge or the negative edge, the state of the upper flip-flop will be toggled. Similarly, the state of the lower flip-flop will be toggled when the data is *zero* and when there is a transition in the Manchester clock. These operations will give rise to dual lines with one line carrying the transition when the data is *one*, and the other line carrying the transition when data is *zero* which is the DTL signaling logic.

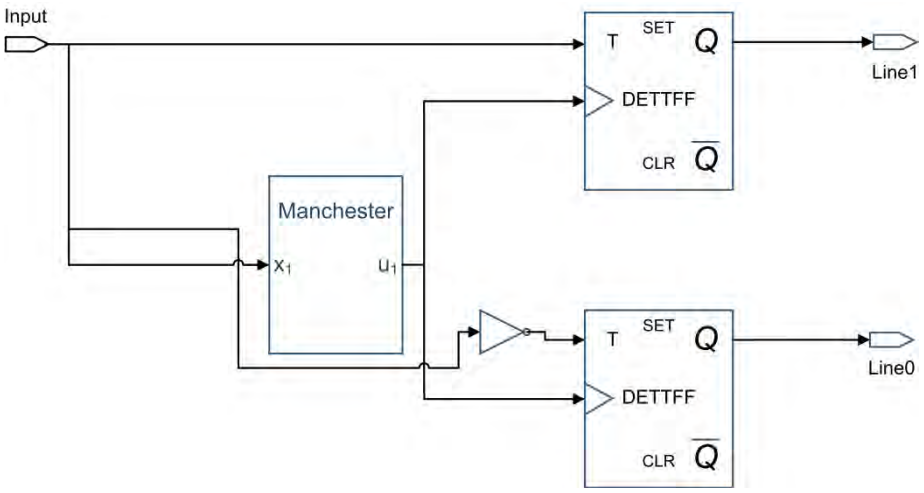

Fig. 9 Logical to DTL Signal Converter

C. Data converter from DTL to Logic:

Fig. 10 shows the custom implemented circuit for the DTL to logic converter. This block will perform the list of actions mentioned below:

- The DTL signals on the *Line 1* and *Line 0* are converted to a logical signal with the help of the dual edge triggered D flip-flop (DETDFF).
- A latch is used to hold the converted logical value.
- A delay element and an XOR gate are introduced for the hand shaking purpose [14].

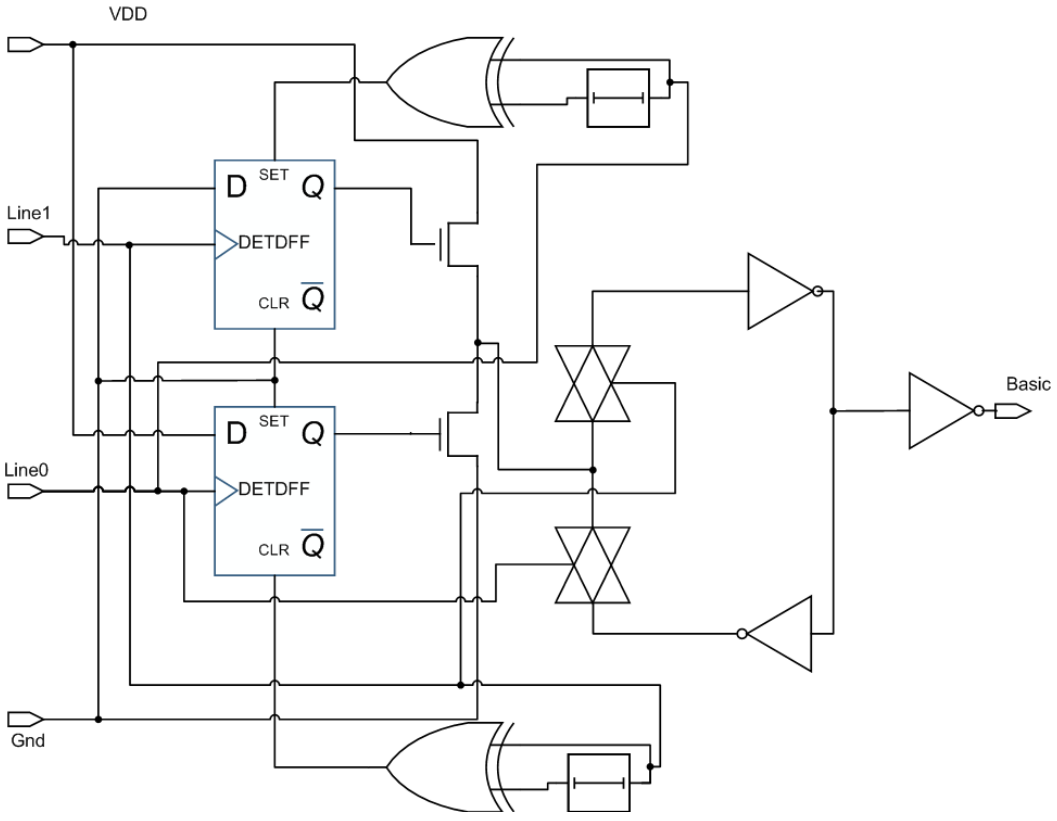

Fig. 10 DTL to Logical Signal Converter (Pre-Part Logic)

The *Line 1* and *Line 0* of the DTL logic are used as the reference signal for the upper and the lower DETDFF respectively. The input *D* for these flip flops are *zero* for upper and *one* for lower flip-flops this is to activate the next part of the circuit which detects the data. The flip-flops are connected to the hand shaking signal as preset for upper and clear for lower flip flop which sets or resets the flip-flop depending on the transition on the other reference line. When there is a transition in *Line 1*, it indicates that it is a logical *one*. This recognition of the *one* from the dual representation logic (as logical one) will trigger the upper flip-flop. Hence, the PMOS device

which is triggered with this logical *one* will turn *on* and passes the VDD to the latch, which produces the desired logical *one* value. This is retained till the transition is *Line 0,* at which point of time, it causes the handshake signal of upper flip-flop to go *high* and presets the value to *one,* and in the process turning the PMOS device *off.* At this instance, the transition on *line 0* triggers the lower flip flop, which passes the *one* to the NMOS device turning it *on* such that the GND will be latched to the output, producing a logical *zero.* This state is retained till there is a transition in the *Line 1*. This process is carried out till the last transition is converted to the corresponding logical values. This completes the conversion of data from ADTL to basic binary coding [20] [21].

D. Logical operation block:

In the logical operation block shown in Fig. 7, the standard logical operations such as the AND, OR, XOR, etc. are performed. This block is mainly divided into three parts, namely, 1) the Pre-part, 2) the reference signal preparation part and 3) the Post-Part.

1) *The Pre-part:*

The pre-part of the reference signal preparation is the same as that of the DTL to logical data converter. This is due to the fact that performing the operation on the DTL signals is costlier, in terms of the time and the area involved. Hence, the DTL signal is converted into the logical signal and then it is passed on to the clock preparation block. The pre-part circuit is depicted in Fig. 10.

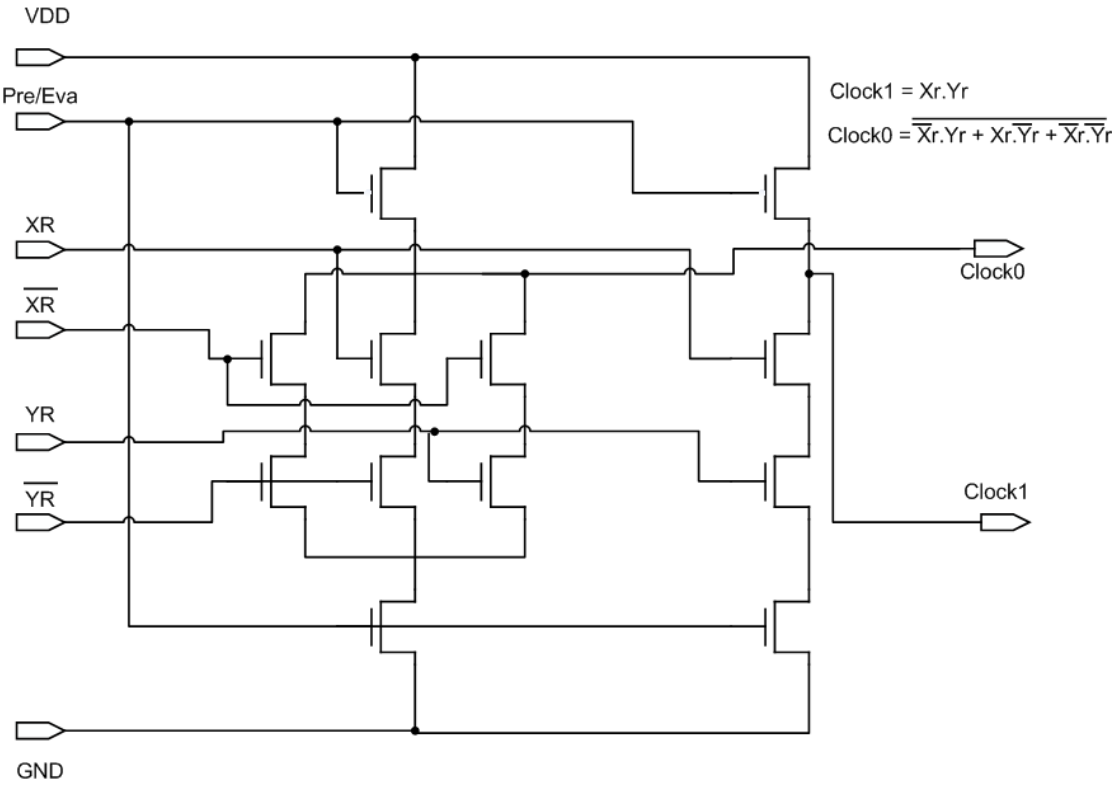

Fig. 11a AND Reference preparation for functional block

2) Functional Reference Preparation Block:

The purpose of the reference preparation block is to produce the two references *ref1* and *ref0,* which will subsequently be passed on to the post-part of the logical operation block, which uses the negative edge of the reference signal. Hence, the main function of the reference preparation part is to produce the negative edges which will trigger the next part. For this purpose, a simple NMOS logic with the pre-charge and the evaluation transistor are used to prepare the reference signal. The *enable* signal will be initially *low*, which will make the pre-charging of the circuit possible. When there is a transition in either of the inputs, the enable signal goes *high*, thus stopping the *charging* process and letting the circuit to start *evaluating* the logic.

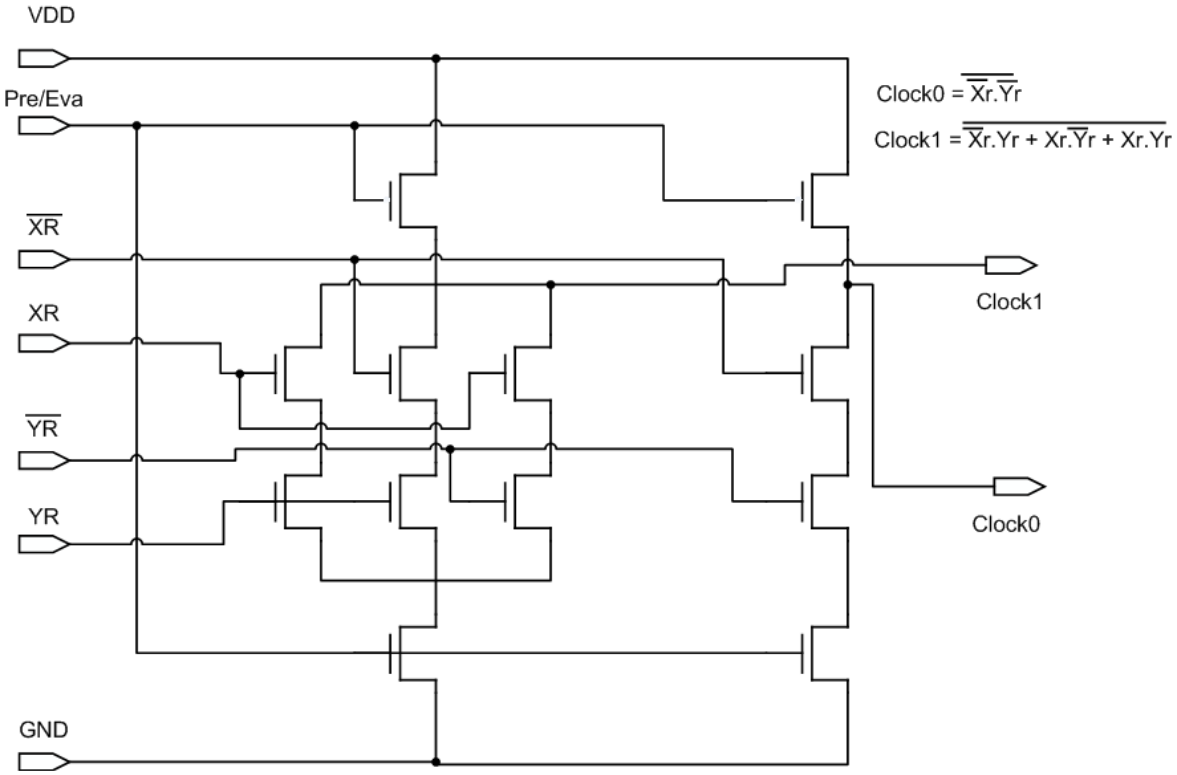

Fig. 11b OR Reference preparation for functional block

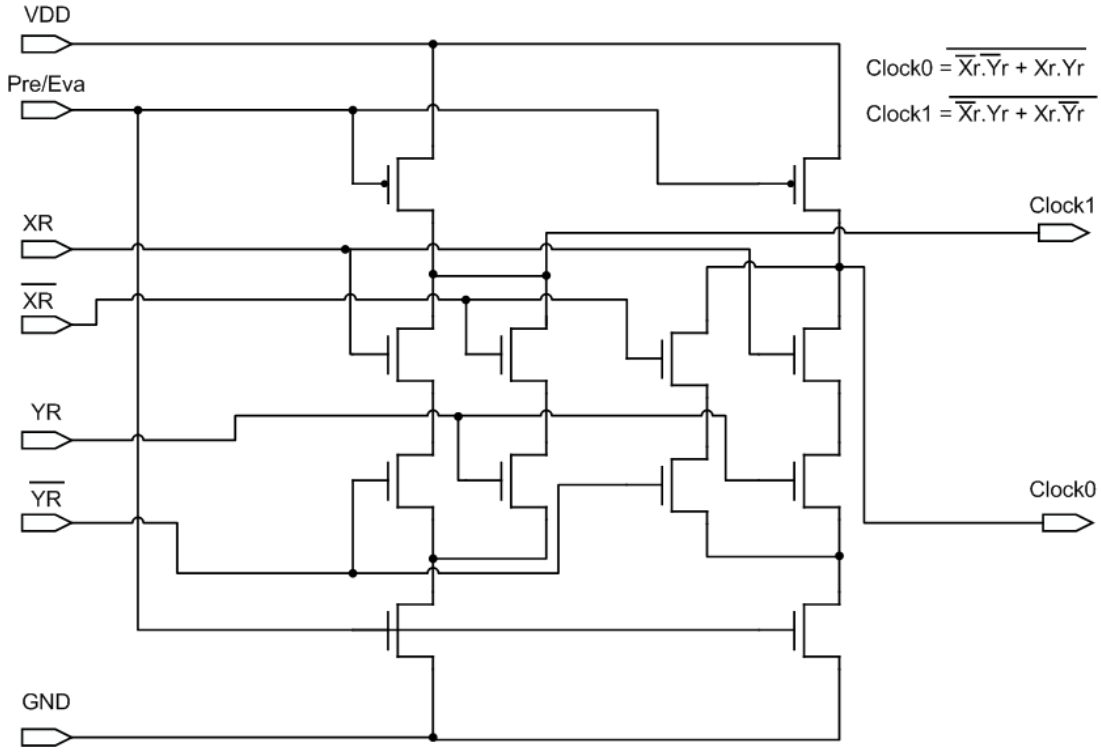

Fig. 11c XOR Reference preparation for functional block

1. The *ref1* logic is designed in such a way that the circuit evaluates to *zero* when the logical output is *one*
2. The *ref0* logic evaluates to *zero* when the logical evaluation of the signal is *zero*.

Hence, this block produces the *ref1* and *ref0* possessing the negative edges when the logical output for the inputs are *one* and *zero* respectively. Figs. 11a, 11b and 11c shows the reference preparation circuits for AND, OR and XOR functions respectively.

3) Post-Part Block:

The functionality of the post-part in the logical operation block is to convert the reference produced by the reference preparation circuit to the DTL logic. This is done using a simple negative edge triggered T flip-flop. As the reference signal has the negative edges in accordance with logic value evaluated by the reference signal generation circuit, the states of the T-FF in the post-part will be toggled producing *Line1* and *Line0* of the DTL logic. Fig. 12 shows the custom implementation of the post-part of the logical operational block.

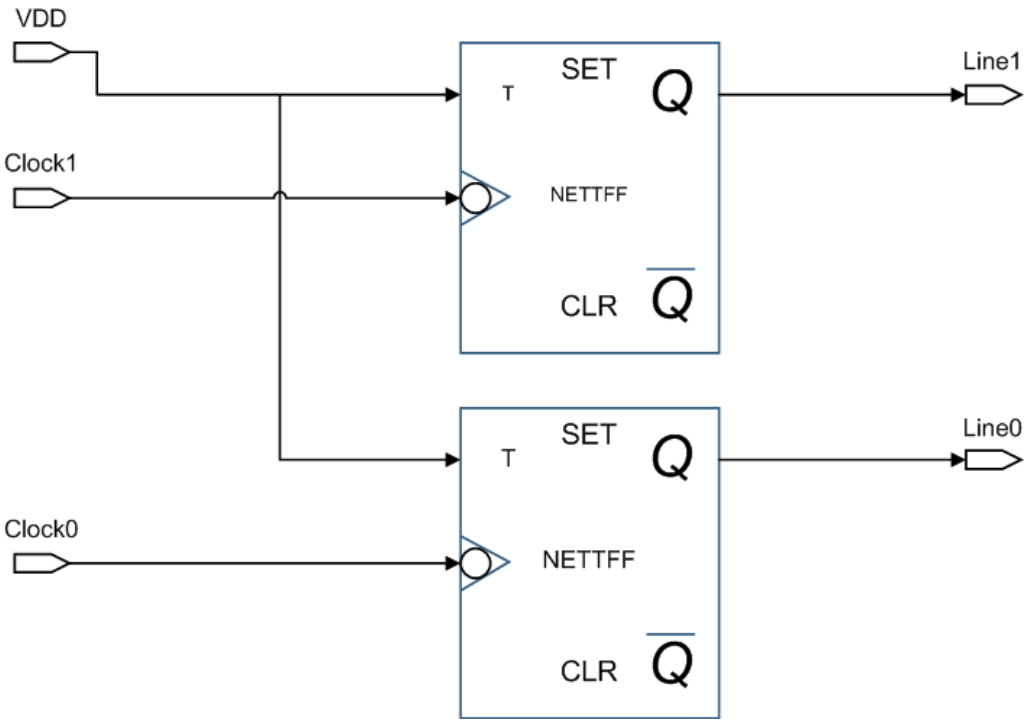

Fig. 12 Post Part Logic for functional block

The encryption circuit employs a tri-gate logic for verification as shown in Fig. 13 with the corresponding data converter blocks and the logical operational blocks.

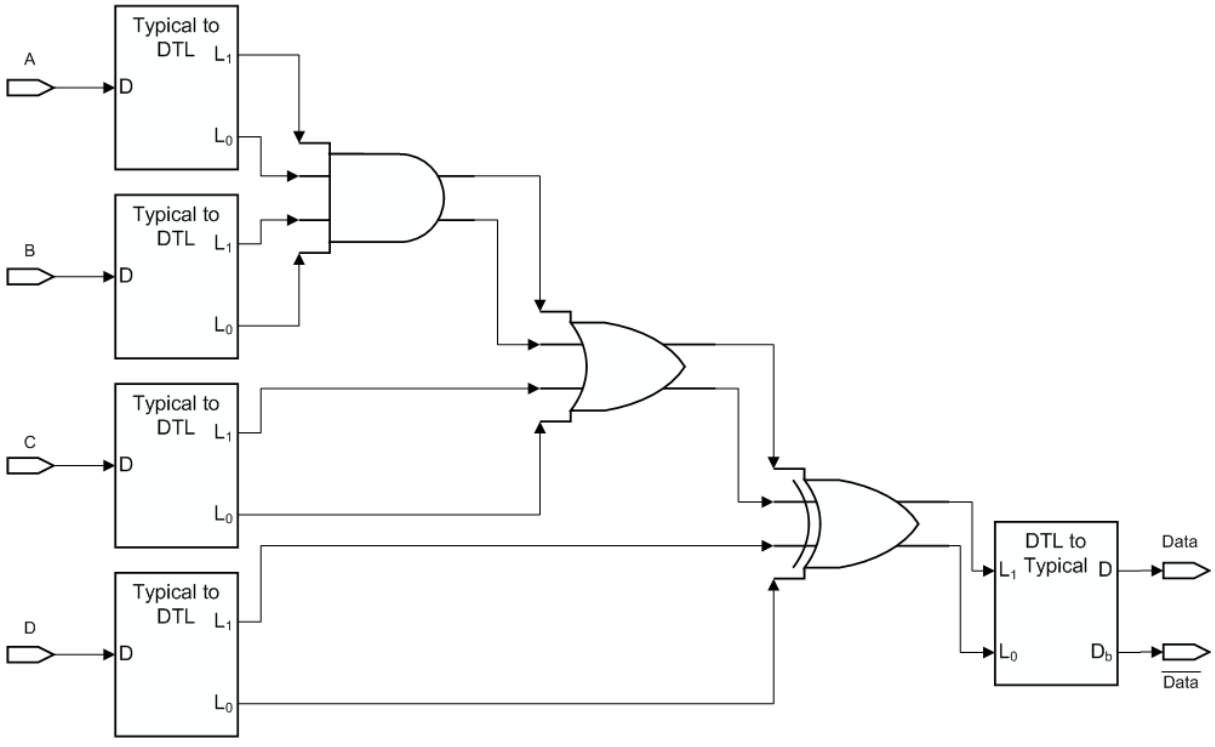

Fig. 13 Tri-gate logic for verification of encryption circuit

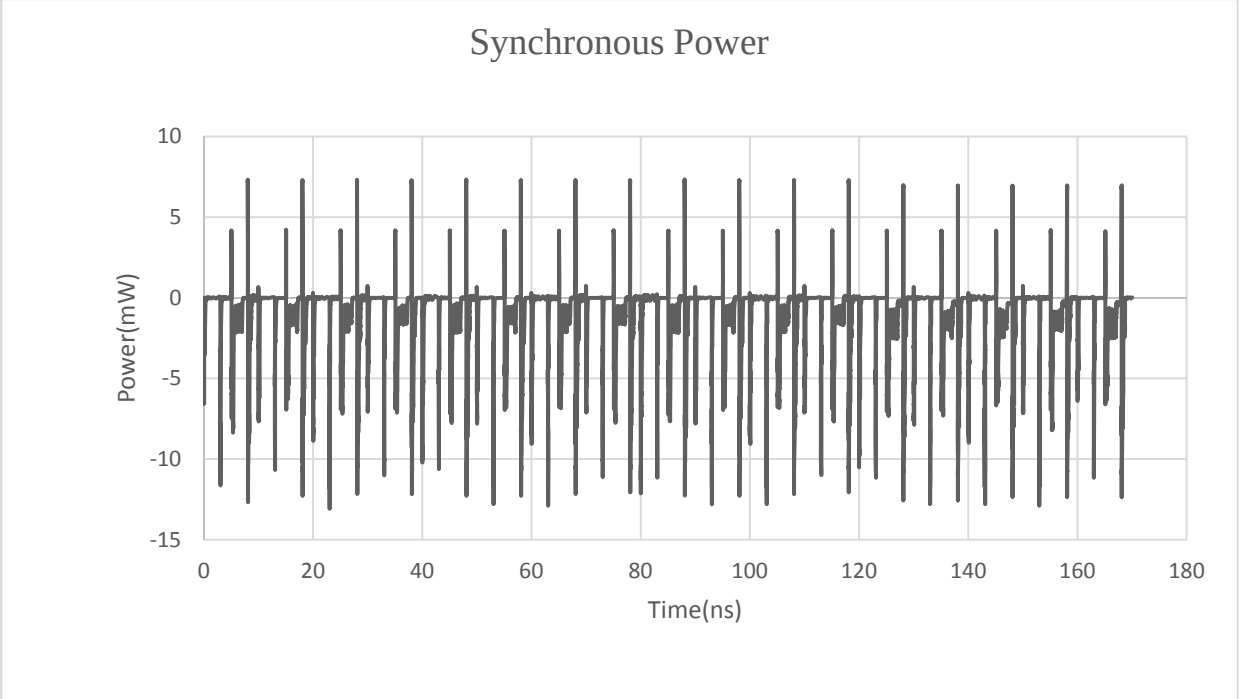

Fig. 14 Synchronous Power Plot of DTL

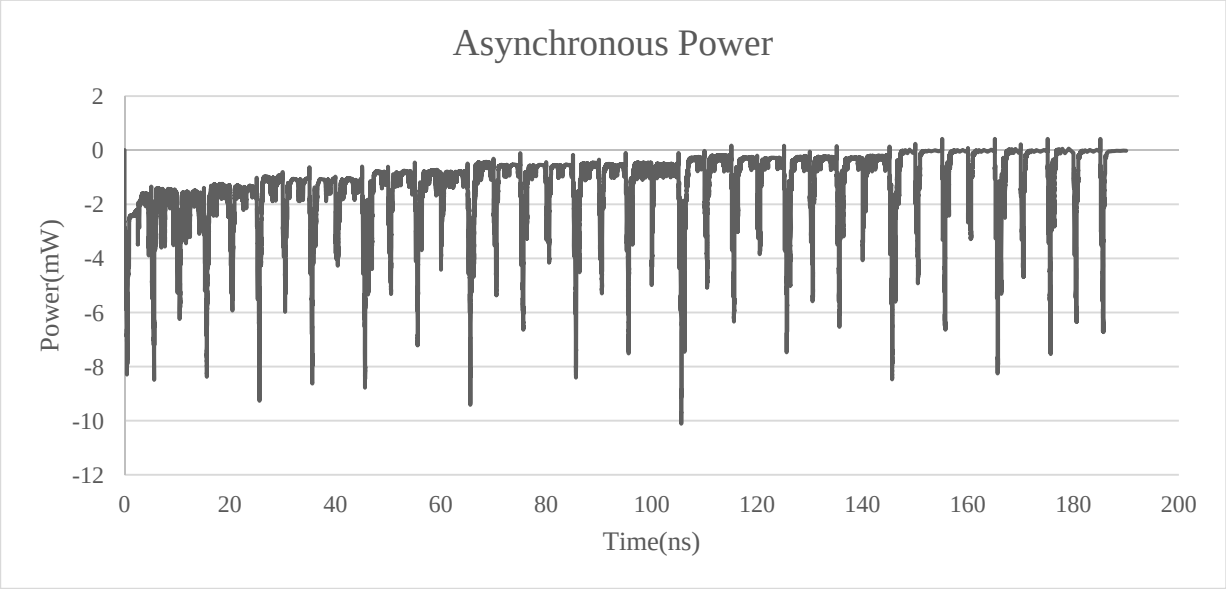

Fig. 15 Asynchronous Power Plots of ADTL

IV. Simulation Results and Performance Comparison

In this section, the results obtained through the simulations of the encryption circuits implemented in the ADTL and DTL are presented and analyzed. The performance comparisons between these two logics are made with respect to the parameters, namely, the average power and the delay. The power dissipation of the DTL is shown in Fig. 14. It amply exhibits the periodicity in the power dissipation waveform with a period equal to clock period which can be the parameter of vulnerability. The ADTL power dissipation is shown in the Fig. 15, which idyllically demonstrates no periodicity. This property thus hides the data period of the signal.

In case of DTL, the power is the same for all the stages, which in effect provides the necessary protection against the DPA. On the other hand, in the case of ADTL, the power dissipated is different for various inputs. The power dissipation is different even for the same inputs at various timings. Hence, this provides a more significant resistance to the side channel power attacks as validated in the paper.

Table 1 presents the comparisons made between the DTL and the ADTL for the parameters, namely, the average power, the clock-to-output delay and the input-to-output delay, as measured and compared through

exhaustive simulations. It may be noted that the results indicate the ADTL operates faster. It may be observed that the ADTL consumes more energy than the DTL. This is due to the fact that the operation is done on both the edges of the signal, which correspondingly results in increasing the switching power. However, this is compensated by removing the clock power of the proposed logic. To add to this advantage, it may be noted that the clock generation, propagation and the power dissipated in the clock interconnects are also eliminated.

Furthermore, the pulse width of the DTL is decided by the delay between the two clocks. On the other hand, the pulse width of the ADTL is independent of any other signals in the circuit.

TABLE I
Comparison of Power and Delay parameters

Parameter	DTL	ADTL
Average Power (mW)	0.786	1.16
Clock to Output Delay	1.91E-09, -1.98E-09	1.73E-09
Input to Output Delay	7.11E-09	7.06E-09

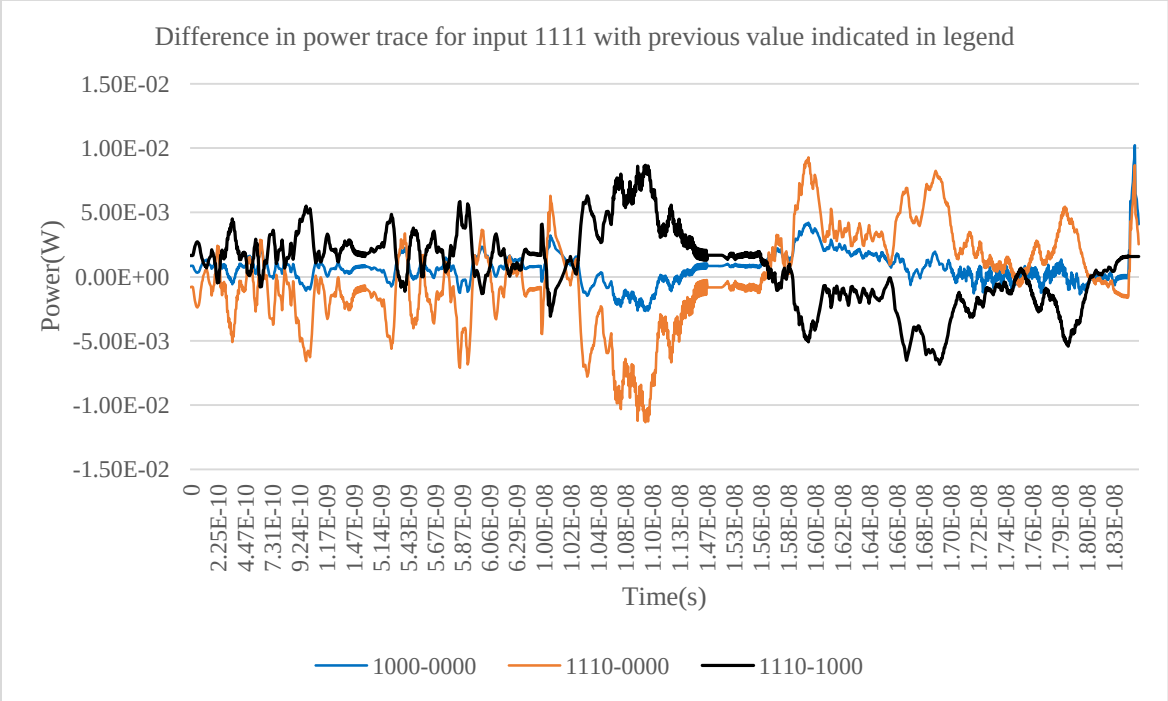

Fig. 16 Difference in power trace for input 1111 with previous value indicated in legend

An additional block is required in the case of DTL to latch out the data in the form of logical values, since the pulse width is small. To increase the pulse width sufficiently, the delay between the clocks must be increased which will inadvertently add to the delay of the circuit. However as discussed before, the pulse width of the data is independent in the proposed ADTL and signal sequence of same value is separated by a small pulse of the opposite magnitude. Hence, the data can be identified without the help of any additional circuit.

Fig. 16 shows the typical differential power traces obtained for a sample input of 1111 when applied with 3 different initial inputs, viz. 0000, 1000 and 1110. These values are chosen so as to include all the possible corner cases and the differences between the power traces of the various combinations of the inputs taken are shown. The power traces are shown for the duration of 20ns with one of the initial inputs mentioned before, and followed by the same input of 1111, which in effect will provide 3 different power traces. To compare the power traces, the difference between the combinations of the two traces is found out and depicted in Fig. 16. It can be clearly observed from the traces that the power is randomized for various initial input combinations i.e., from 0 to 10ns. It may be noted that the power is randomized entirely differently for the same input 1111, as is observed during the 10ns to 20ns duration. It can thus be validated that the differences in the power traces are random and clearly unpredictable. Hence, the DPA resistance property of the circuit is validated.

V. CONCLUSION

The paper has presented the Asynchronous Dual-Rail Transition Logic (ADTL) that focuses on increasing the differential power side channel attack resistance and the analyses demonstrate significant advantages in terms of the clock independency, reduced overall power consumption and an improved speed performance. The results show the randomization in the power trace of the circuit. The clock signal generation and distribution is completely eliminated in the proposed approach, which may result in a significant value of overall power reduction. This can effectively surmount the impact of the marginal increase in dynamic power. Furthermore, the realistic advantage of the clock independency realized by ADTL is made possible by the dual rail signal encoding.

The most important attribute of the clock independency for the cryptographic applications is accomplished. The power trace results generated by the proposed logic authenticate the design. Moreover, the data pulse width employed for the dual transition signaling is a variable one and this property exhibits an additional benefit in increasing the DPA resistance property. The delay of the circuit is also found to be less than the synchronous DTL circuit, because of the fact that the clock overhead is completely eliminated in the proposed asynchronous DTL approach. Hence, the proposed asynchronous solution demonstrates improved speed performance with enhanced side channel power resistance capability with a slight increase in area overhead.

VI. FUTURE WORK

Since the instantaneous power dissipation in the ADTL is higher than the DTL, in realizing the increased DPA resistance characteristics, the future work would focus on reducing the power consumption by introducing the power gating and the sleep transistor logic. Secondly, for the system to randomize the power, the signals of more random frequency can be generated and employed.

REFERENCES

[1] A. Moradi, M.T.M. Shalmani and M. Salmasizadeh, “Dual-rail transition logic: A logic style for counteracting power analysis attacks”, Journal on Computer and Electrical Engineering, vol. 35 issue 2, page 359-369, March 2009.

[2] A. Moradi and A. Poschmann, “Lightweight Cryptography and DPA Countermeasures: A Survey”, Horst Gortz Institute for IT Security, Ruhr University Bochum, Germany.

[3] T. Popp, E. Oswald and S.Mangard, “Power Analysis Attacks and Countermeasures”, IEEE Design and Test of Computers, vol. 24 Issue 6, December 2007, Page 535-543

[4] Lawson. N and Roots labs, “Side-Channel Attacks on Cryptographic System”, IEEE Security & Privacy, Volume 7 Issue 6, Page 65-68, 2009.

[5] Kocher PC, Jaffe J and Jun B. “Differential power analysis. In: Advances in cryptology”, – CRYPTO 99. Lecture Notes in Computer Science, vol. 1666. Springer; 1999. p. 388–97

[6] Oswald E, Mangard S, Pramstaller N and Rijmen V, “A side-channel analysis resistant description of the AES S-box. In: Fast software encryption”, – FSE 2005. Lecture Notes in Computer Science, vol. 3557. Springer; 2005. p. 413–23

[7] J. Wu, Y. Shi and M. Choi, “Measurement and Evaluation of Power Analysis Attacks on Asynchronous S-Box”, IEEE Transactions on Instrumentation and Measurement, vol. 61, Issue 10, pp. 2765-2775, 2012

[8] Messerges T.S. “Using second-order power analysis to attack DPA resistant software. In: Cryptographic hardware and embedded systems”, – CHES 2000, Lecture notes in computer science, vol. 1965. Springer; 2000. p. 238–51.

[9] Popp T and Mangard S, “Masked dual-rail pre-charge logic: DPA-resistant without routing constraints”, Cryptographic Hardware and Embedded Systems – CHES 2005, vol. 3659. p. 172-86.

[10] Suzuki D, Saeki M and Ichikawa T, “Random switching logic: A countermeasure against DPA based on transition probability”, Cryptology ePrint archive. Report 2004/346; 2004

[11] W. M. Chung and M. Sachdev “A Comparitive Analysis of Dual-edge triggered flip flops”, Canadian Conference on Electrical and Computer Engineering, 2000, Volume 1, pp. 564 - 568

[12] D. Bhargavaram and M.G.K. Pillai “Low power dual edge triggered flip-flop”, IEEE Conference on Advance in Engineering Science and Management, Pp. 63-67, 30-31. Mar. 2012

[13] H. Karimiyan, S.M. Sayedi and H.Saidi “Low-power dual-edge triggered state-retention scan flip-flop”, IET journal on Computers and Digital Techniques, vol. 4, Issue 5, pp 410-419, 2010

[14] K. Sun, X. Pan, J. Wang and J.Wang “Design of A Novel Asynchronous Reconfigurable Architecture for Cryptographic Applications”, First International Symposium on Computer and Computational Sciences, pp 751-757, 2006

[15] Teifel.J, “Asynchronous cryptographic hardware design”, 40th Annual IEEE Carnahan Conference on Security Technologies, pp 221-227, Oct. 2006

[16] I. Lamberski and P. Fiser “Dual-rail asynchronous logic multi-level implementation,” Integration, The VLSI Journal, vol. 47, PP 148-159, 2014

[17] Z. Xia, S. Ishihara, M. Hariyama, M. Kameyama, “Dual-rail/Single-rail hybrid logic design for high-performance asynchronous circuit”, IEEE International Symposium on Circuits and Systems (ISCAS), 2012, pp. 3017-20

[18] Z. Liu and C. K. Chan “Generation of Dispersion Tolerant Manchester-Duobinary Signal Using Directly Modulated Chirp Managed Laser”, IEEE Photonics Technology Letters Journal, vol. 23, Issue-15, pp.1043-45, 2011

[19] Nanda K, Desai SK and Roy S.K., “A new methodology for the design of asynchronous digital circuits,” Proceedings of the International Conference on VLSI Design, 1997, pp. 342–47

[20] Jan M. Rabaey, Anantha Chandrakasan and Borivoje Nikolic, “Digital Integrated Circuits”, Second Edition, Eastern Economy Edition, PHI productions, 2010.

[21] W.G. Ho, K.S. Chong, B.H Gwee, J.S.Chang, Y.Sun and K.L.Chang, “Improved Asynchronous-logic dual-rail sense amplifier-based pass transistor logic with high speed and low power operation”, Nanyang Technological university, Copyright of IEEE, 2011

N Rajath Srivathsav received his B.E degree in Electronics and Communication from Siddaganga Institute of Technology under Visvesvaraya Technological University, India. Currently, he is an M.Tech Candidate in VLSI Design at Vellore Institute of Technology, India. His research interest is in area of side channel attacks on cryptographic system and digital design to counter the attacks.

A Prathiba received her bachelor degree in Electronics and Communication in the year 2002. She obtained her Masters in Communication Systems in the year 2006. She is working as an Assistant Professor in VIT University Chennai. Currently she is pursuing her Ph.D degree and her research areas are hardware design of cryptographic architectures, vulnerability modeling of side channel attacks and light weight cryptography.

Dr V S Kanchana Bhaaskaran is a Professor and Dean of the School of Electronics Engineering at VIT University Chennai. She obtained her undergraduation degree in Electronics and Communication Engineering from Institution of Engineers (India), Calcutta and her M.S. degree in Systems and Information from Birla Institute of Technology and Sciences, Pilani and Ph D from V I T University. She has more than 35 years of industry, research and teaching experience by serving the Department of Employment and Training, Government of Tamil Nadu, IIT Madras, Salem Cooperative Sugar Mills' Polytechnic College, SSN College of Engineering and VIT University Chennai. Her specializations include Low Power VLSI Circuit Design, Microprocessor architectures and Linear Integrated Circuits. She has published around 70 papers in International Journals and conferences, and has one patent published and one filed. She is a reviewer for peer reviewed international journals and conferences. She is the Fellow of the Institution of Engineers (India), Fellow of the Institution of Electronics and Telecommunication Engineers, Life Member of the Indian Society for Technical Education and Member of the Institute of Electrical and Electronics Engineers Inc., USA.