VLSI Architecture of Turbo Codes-IP Secure With PUF for Dedicated Short Range Communication (DSRC) Systems

N.Sindhuja, Dr.Muthammal
ME., Applied Electronics, E.C.E, sriram engineering college
Ph.D, Associate professor, sriram engineering college

***Abstract*-The Dedicated Short Range Communication (DSRC) is an emerging technique to push the Intelligent Transportation System (ITS) into our daily life. To establish proper communication with information security, turbo encoded algorithm is introduced. Turbo encoded algorithm implemented in DSRC system with secure IP core. In this paper, turbo encoded-IP secure with Physical Unclonable Function (PUF) is proposed for a process DSRC system efficiently and enhances the signal reliability. PUFs can enable low-cost authentication of individual ICs and generate volatile secret keys for transceiver operations. This approach requires the authentication mechanism to be implemented in hardware incurring an area overhead, and the authentication secrets to be securely, which may be susceptible to external attacks.**

***Index Terms*-Dedicated Short-Range Communication (DSRC), Turbo Codes, PUF, VLSI**

I.INTRODUCTION

Today as a result of globalization, the development and fabrication of advanced integrated circuits (ICs) is typically migrating offshore. This migration to third-party providers and to low- cost foundries has made ICs vulnerable to security compromise, functional changes, information leaks or even system failures under specific conditions. Such intrusions may pose a major threat to embedded systems in critical applications and infrastructures. These risks have been considered not only in the academic community but also in the fabless semiconductor industry and governmental agencies. In this context, secure IP-core environments are becoming more important in ensuring a trustworthy hardware environment.

Hardware Trojans is any malicious and deliberate change to an integrated circuit(IC) design that may cause unwanted effects [1]. Malicious hardware implantations are called hardware Trojan horses(HTH). They can trigger and effect normal circuit operation, potentially with catastrophic consequences in critical operations in the various domains like communication, space,military and nuclear facilities. The Trojans try to bypass or disable the security fence of the system. During the manufacturing of IC, the adversary tries to hide the additional components; hence more advanced detection techniques are necessary. Therefore the Detection techniques should be non-destructive. Based on the advanced IC manufacturing technology, it is much easier for the attackers to embed some mallious circuits in the unused space, or other parameters without changing the area of whole chip[2]. The earlier model used for detecting the Trojan was by physical inspection i.e. by physical inspection of the IC, it is a time consuming and expensive method. Moreover this technique is destructive. Other proposed approaches to detect the hardware Trojan includes, a security policy together with a root-to-trust model [3], side channel attacks [4], counter probing attacks [5] with the assumption that there is no compromise in the fabrication process. Hardware Trojan detection mechanism using path delay fingerprint [2] was effective only in detecting the explicit payload trojan but not useful for detecting the implicit payload Trojan.

After presenting a brief introduction of PUFs, we explain DSRC in section II. Implementation of turbo-encoded algorithm III. The secure test wrapper and the security of the protocol in section IV. We conclude the paper and discuss future work in section V.

II.DSRC

DSRC(Dedicated Short Range Communications) is a wireless technology for vehicular traffic. Using a modified 802.11a technology for north America cars and trucks, DSRC is designed for several applications. For example, ambulances can cause traffic lights down the road to change in their favour, and traffic congestion can transmitted to automobile navigation systems. It allows vehicles to sense that they are about to crash, and the safety systems can begin to tighten seat be its and warm up the airbags before impact. In addition, a standard for wireless payment allows parking lots and fast-food drive-ins to offer the same convenience as the automated highway toll systems such as E-ZPass. DSRC systems consists of Road Side Units (RSUs) and the On Board Units (OBUs) with the transceivers and transponders. The DSRC standards specify the operational frequencies and the system bandwidths, but also allow for optional frequencies which are covered by national regulations. key issue-Qos – prioritization of safety messages. If a neighbouring car is in the middle of streaming movie application, and I need to communicate about an accident, how to prioritize the message? DSRC has 1 control channel and other service channels. Safety messages are expected to use the control channel.

III.TURBO CODES

The turbo codes are used to provide double data throughput at a given power or work with half of the power. The two men were not known most were thinking that they are wrong in calculation. They realized that it was true, many companies adopted new companies started turbo concept and icoding. Turbo encoding achieves remarkable performance with the relatively low complexity encoding. The turbo coding is the forward error correction scheme. The forward error correction techniques used for controlling errors in data transmission over unreliable noisy communication channel. Turbo encoding is an iterated soft decoding scheme.

Interestingly, the name tubo was given to this code because of the cyclic feedback mechanism that is high speed network to the decoders in an iterative. Turbo decoder decodes information iteratively. Turbo codes can be concatenated series,parallel or in a hybrid manner. There are many different instances of the turbo codes using different components encoders, input/output ratios, and interleavers and puncturing pattern. Turbo code is defined by several convolutional encoders and an equal number of interleavers. First, a string of K source bits is fed into each encoder. Next, the order of the source bits are changed or altered in some way based on the encoder they were fed into.

A.TURBO ENCODER

A turbo code encoder sends out three sub-blocks of bits. The figure 4 shows how the source bits are passed through an interleaver and two separate encoders to generate three outputs. The first sub-block is the source data. The second and third sub-blocks are of parity bits computed based on different convolutional coding schemes. The resulting transmitted code word consists of K source bits, and M2 parity bits.

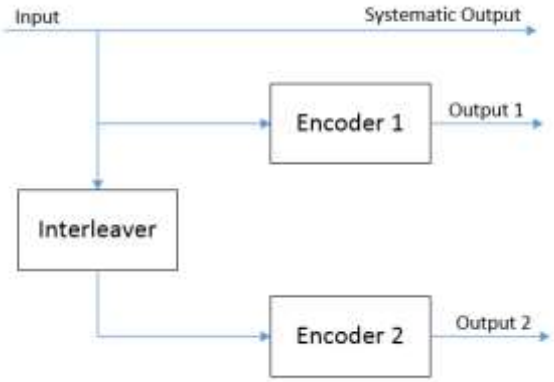


Fig.1.Turbo encoder

B. TURBO DECODER

The figure shows how a turbo code is decoded when it has been received. The encoded bit stream is sent through a series of decoders and interleavers to output the orginal data stream to the receiver. Turbo codes have exceptional performance with decoded error probabilities of around 10-5. The use of recursive convolutional encoder and interleavers is critical for turbo codes. This helps to make the turbo code appear to be more random and as a result reduces the number of low –weight code words are considered beneficial to turbo codes. Because of their attempt to maximize the minimum distance between two code words, a turbo code can correct about half of the patterns of channel errors.

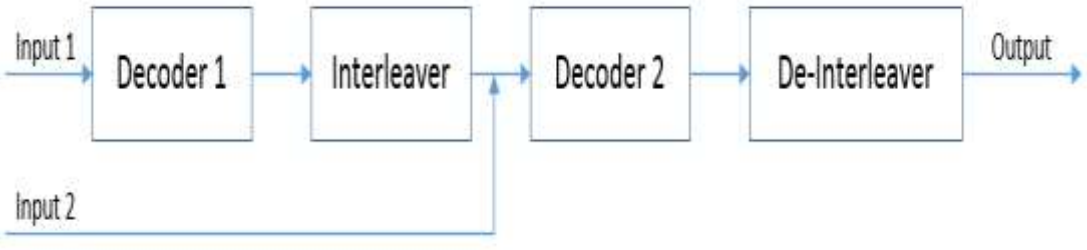


Fig.2.Turbo decoder

IV. PUF Block Diagram For Turbo-Encoded IP Core

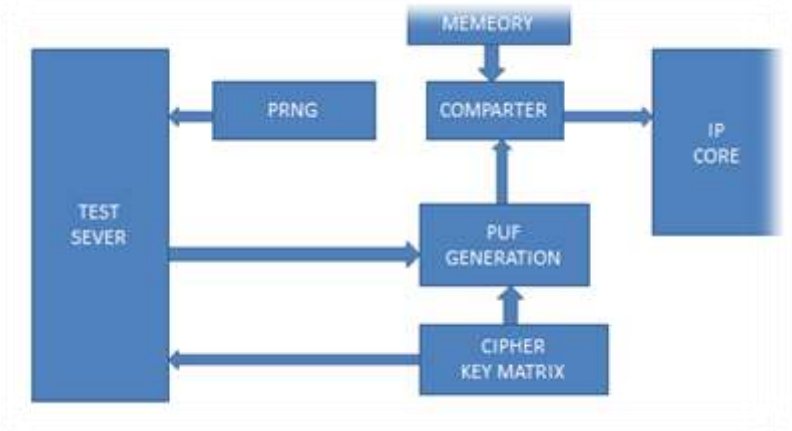
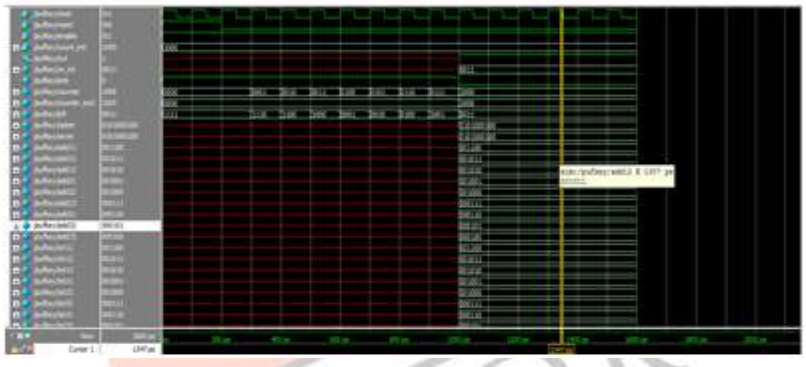


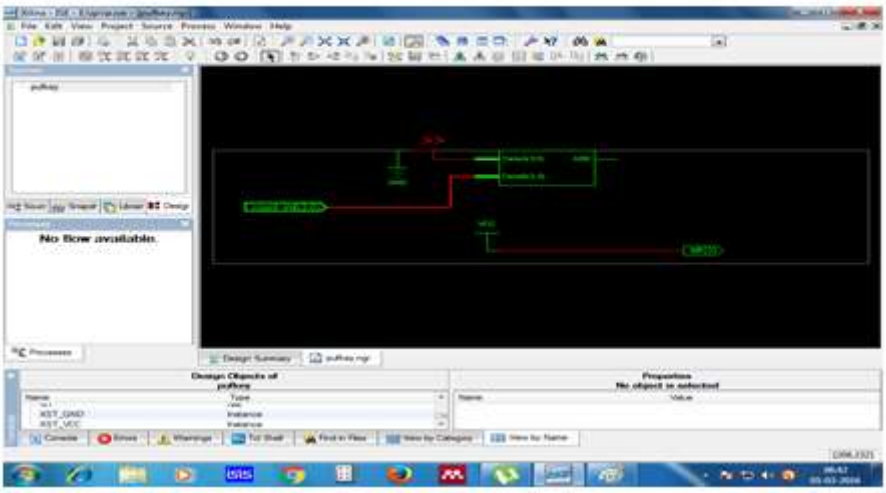
Fig.3.PUF block diagram

The secure test wrapper architecture is constructed with a challenge- response based test protocol using a light-weight block-cipher. The authentication protocol seeks matching response values and executes with the following steps: First, True Random Number Generator (TRNG)generates a nonce value and sends this value to the on chip block cipher and also the test server. Both parties share the same block cipher and generate the same chipper texts according to their secret keys. Only if these cipher texts match, the protocol enables the scan-based testing environment of the crypto IP through the wrapper. Otherwise the protocol rejects any attempts for testing the IP block.

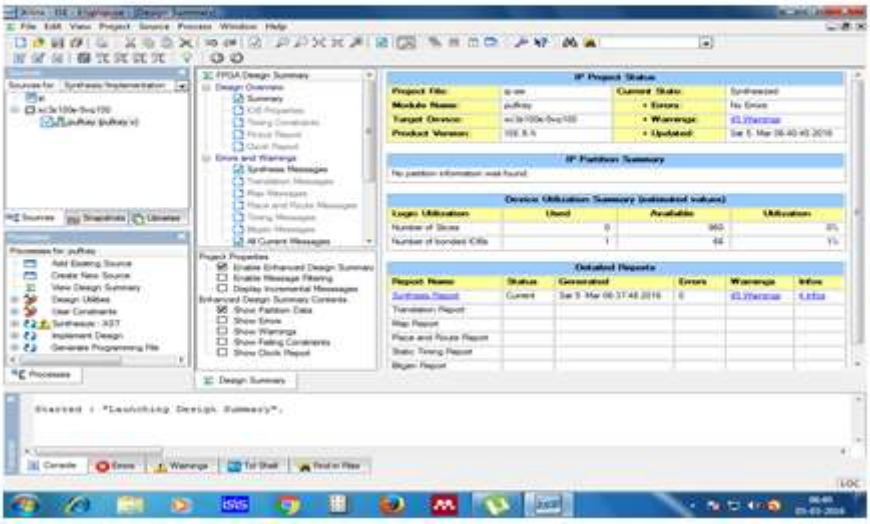
PUF Output



PUF – Synthesis Block



PUF – Design Summary



V. REFERENCE

[1] J.Rajendran, A.K,Kanuparthi,R.Somasekaharan,A.Dhandapani and X.Xu, "Securing FPGA Design using PUF chain and exploitation of other trojan detection circuits.

[2] Yier Jin,Yiorgos Makris,"Hardware Trojan Detection Using Path Delay Fingerprint", 2008,IEEE Xplore.

[3] I. Verbauwhede and P.Schaumount, "Design methods for security and trust," in Design,Automation and Test in Europe Conference and Exhibition, 2007, pp. 1-6.

[4] Paul Kocher, Joshua Jaffe and Benjamin Jun, " Differential Power Analysis," in Advances in Cryptography CRYPTO 99, pp.789-789.

[5] T.S.Messerges,E.A.Dabbis and R.H.Sloan,"Examining Smart –card security under the threat of power analysis attacks," Computers, IEEE Transactions Vol.51,no.5,pp.541-552,2002.

[6]Yu-HsuanLee, *Member, IEEE*, andCheng-WeiPan, A Fully reused VLSI architecture of fmo and Manchester encoding for DSRC applications Very Large Scale Integration (VLSI) Systems, IEEE Transactions on Year: 2015, Volume: 23, Issue: 1Pages: 18 - 29, DOI: 10.1109/TVLSI.2014.2299532

[7]F.Ahmed-Zaid, F.Bai, S.Bai, C.Basnayake,B. Bellur, S. Brovold, et al., "Veicular safety communications -applications sep.2011.

[8]B.Kenney," Dedicated short range communications (DSRC) standards in the U.S. Proc. IEE, Vol. 99. No 7. pp 1162-1182. Jul 2011.