IETE JOURNAL OF RESEARCH
https://doi.org/10.1080/03772063.2023.2204829

Novel Single-Step 32nm-CMOS Hardware T-Encryptor/Decryptor

Aloke Saha[1], Rakesh Kumar Singh[1], Prerona Sanyal[1] and Dipankar Pal[2]

[1]Department of ECE, Dr. B. C. Roy Engineering College, Durgapur, India; [2]Department of EEE & EI, BITS-Pilani, K. K. Birla Goa-Campus, Goa, India

ABSTRACT

This paper unfolds a new speed-power efficient single-step design to hardware-encrypt-decrypt original-message in a binary format with a block-wise ternary-operator to achieve secured end-to-end-communication, hiding confidential information from third-party intervention. The scheme can be integrated as cryptographic hardware primitive cells with IoT/portable devices. The proposed T-Encryptor operates in a single step on a 4-bit binary input block at a time, to produce corresponding 3-trit encrypted ternary output. Encryption is done by taking 2's complement of the original binary message and converting it to ternary. Reverse steps are followed at the receiving end. A novel design that consists of 2:1-binary and 3:1 ternary multiplexer modules along with a clever pass-transistor input-switching network, implements the proposed T-Encryptor/Decryptor on conventional MOS. The Design and optimization of the proposed T-Encryptor/Decryptor are done on the BSIM4 device parameter using the 32nm-standard-CMOS Technology at 0.9 V supply-rail at 27°C. Bits "0" and "1" are denoted by 0 and 0.9 V, respectively, whereas ternary digits "0", "1" and "2" are denoted by 0, 0.45 and 0.9 V, respectively. The transient response of the proposed design is validated by extensive T-Spice simulations.

KEYWORDS

Hardware-encryption-decryption; MOSFET; multiplexing; PVT analysis; ternary logic; 2's complement method

1. INTRODUCTION

Rapid progress in Internet-of-Things (IoT), smart-communication-system and the associated network complexity make data security a major challenge to the system/network designer [1–5]. Encrypting the original message with a security key at the source end and decrypting it at the destination is the conventional strategy to hide sensitive information from third-party intervention [6]. However, consistent technological advancement makes hardware-driven defence strategy [7,8] against emerging security threats more robust compared to its software counterpart. In addition, the increased demand for portable hand-held electronic devices has shaped the need to embed area and power-efficient hardware-encryptor/decryptor for secured end-to-end communication [9–12] through IoT. The related security key exchange plays an important role to keep the original information confidential from external intruders [13]. The binary is the globally accepted radix system to represent information digitally due to the ease of implementation of communicating devices by exploiting practical ON–OFF characteristics of solid-state switching devices [14–16]. Yet, increasing encryption bit-length can enhance data security at the cost of more processing time and interconnect complexity as far as physical implementation is concerned. More interconnect complexity calls for more power cost, chip area needs to wither liability degradation [17], hence it is impractical to be integrated as a cryptographic primitive cell for IoT/portable devices.

The data encryption based on MVL (Multi-Valued Logic) can offer an effective solution for previously mentioned issues by reducing interconnect complexity. Being closer to natural base-e ($\approx$2.718), the ternary (base-3) system won the race against other MVL systems and it has been exhibited [18] for long that it enhances the performance of the digital system. Ternary uses three levels of signalling (*i.e.* "0", "1" and "2") instead of two (*i.e.* "0" and "1") as in binary and hence carries relatively more information than its binary counterpart [19]. More information-carrying capability reduces the interconnect overhead and eventually fan-in/out driving hazard by using fewer circuit modules in the system [19–23]. As a possible outcome, ternary-based encryption can increase data security along with entropy and hence, the information transmission rate [21]. It can also offer Power-Delay efficiency from a crypto processor perspective in favour of hardware integration in IoT devices. B. Cambou *et al.* in 2018 [21,22] investigated the feasibility of a ternary (base-3) operator to rule in its favour on improving cyber security for the public key exchange aspect. A novel Public Key Infrastructure strategy using Addressable Ternary Cryptographic-Table (CT) was also presented in [21]. In another study presented in 2019, S. Assiri *et al.* [24] explored a ternary-based random public key-exchange