Journal of Nonlinear Analysis and Optimization
Vol. 11(11) (2020), November 2020
https://ph03.tci-thaijjo.org/
ISSN : 1906-9685

J.Nonlinear
Anal. Optim

Distribution System Load Forecasting using Neural Networks for SPDCL

Dr G Ravikumar
Associate Professor, Department of ECE
Sri Sai Institute of Technology and Science, Rayachoti
Email: ravikumargphd@gmail.com

***Abstract*— Power consumption is a primary concern for light weight cryptographic applications. With the development of low-cost, low-power FPGAs for battery powered devices, they are becoming an interesting target for light weight cryptography (LWC). This paper describes compact architectures of TEA, XTEA, and AES are implemented on low-cost Xilinx Vetex6 FPGAs. Different optimization techniques are employed to minimize the area consumption by smart use of the Configurable Logic Block (CLB) structure in FPGAs. Cipher implementations are light weight but with full strength security i.e. not 80-bit but 128-bit key length. Furthermore, differential power analysis (DPA) attacks are performed on these implementations to investigate their "natural".**

Keywords: Tiny encryption algorithm (TEA), Extended Tiny encryption algorithm (XTEA), Advanced encryption standard (AES), efficient design, low power, low area.

I. INTRODUCTION

As computer systems become more pervasive and complex, security is increasingly important. Cryptographic algorithms [1] and protocols constitute the central component of systems that protect network transmissions and store the data. The security of such systems greatly depends on the methods used to manage, establish, and distribute the keys employed by the cryptographic techniques. Even if a cryptographic algorithm is ideal in both theory and implementation, the strength of the algorithm will be rendered useless if the relevant keys are poorly managed.

Cryptography is the art and science behind the principles, means, and methods for keeping messages secure. Cryptanalysis is a study of how to compromise (defeat) cryptographic mechanism. There are two classes of key-based encryption algorithms: symmetric (or secret-key) and asymmetric (or public-key) algorithms. Symmetric algorithms use the same key for encryption and decryption, whereas asymmetric algorithms use different keys for encryption and decryption. Ideally it is infeasible to compute the decryption key from the encryption key.

Symmetric algorithms can be divided into stream ciphers and block ciphers. Stream ciphers encrypt a single bit of plain text at a time, whereas block ciphers take a number of bits (say
64 bits), and encrypt them as a single unit. Symmetric encryption is the backbone of many secure communication systems. Dozens of symmetric algorithms have been inventedand implemented, both in hardware and software. It enables you to store information or transmit it across insecure networks (like the internet) so that it cannot be read by anyone except the intended recipient. Out of these algorithms mainly TEA, XTEA, and AES are best for security and power point of view.

II. CRYPTOGRAPHY ALGORITHMS

A. TEA:

The Tiny Encryption Algorithm (TEA) [4] is said to be one of the fastest and most efficient cryptographic algorithms which is developed by David Wheeler and Roger Needham of Computer Laboratory of Cambridge University. TEA is a fiestal cipher that uses only XOR, ADD and SHIFT operations to provide the property of Shannon, diffusion and confusion are necessary for a secure block cipher without any need for the P-boxes and S-boxes. The TEA algorithm source code is shown in Figure 1. TEA is assumed to be as secure as the IDEA algorithm, but is much simpler and faster than that. It is also in public domain. For software implementation, the code is lightweight and portable and therefore particularly suits real-time applications.

```
void encrypt(long* v, long* k)
{ unsigned long y=v[0], z=v[1], sum=0,delta=0x9e3779b9,n=32;
```

```
while (n-->0)
{ sum += delta;
   y += ((z<<4)+k[0]) (z+sum)^((z >>5)+k[1]);
   z += ((y<<4)+k[2]) (y+sum)^((y>>5)+k[3]);}
  v[0]=y; v[l]=z;}
}
```

Figure 1. TEA Encryption

For the hardware implementation, the structure is simple, with only hardware for the addition, XOR, and registers are required. This is compared with the other block ciphers such as DES and AES where we need bigger blocks such as the s- boxes are necessary for the hardware. Figure. 2. shows a blockdiagram of TEA encryption (for one cycle).

The sub keys K[*i*] are different from K and from each other. The constant delta = $(\sqrt{5}-1)*2^{31}$ [4], is derived from the golden $9E3779B9_h$ number ratio to ensure

TEA was extended to XTEA (Extended TEA) [5] by David Wheeler et al. (1997). It was proposed to fix the two minor weaknesses pointed out by Kelsey et al. (1997). Like TEA, XTEA makes use of arithmetic and logic operations. The first enhancement is to adjust the key schedule, and the second is to introduce the key material slowly.

B. XTEA:

XTEA (eXtended TEA) [9] is a 64-bit block Feistel network which is a 128-bit key that is designed to correct the weaknesses in TEA. It was also created by David Wheeler and Roger Needham. The algorithm was first reported in [9]. Similar to TEA, XTEA is also not patented. XTEA is similar to TEA in such a way that it requires addition, XOR and shift operations only. The only key difference is that with the more Figure 5. Fiestal structure of XTEA Encryption routine

Functions and Constants used: Each step uses a primitive logical function, which takes three register values and outputs a 32-bit value. The functions are:

y += (z<<4) +K [0] ^ z+sum ^ (z>>5) +K [1]z += (y<<4) +K [2] ^ y+sum ^ (y>>5) +K [3]

Each step uses a additive constant delta and their values are either decreasing order or decreasing order from an initial value delta[i] = 0x9e3779b9. The sub parts of keys are distributed as

K = K0 for 0 ⩽ round ⩽ 7 or for 32 ⩽ round ⩽ 39K = K1 for 8 ⩽ round ⩽ 15 or for 40 ⩽ round ⩽ 47 K = K2 for 16 ⩽ round ⩽ 23 or for 48⩽ round ⩽ 55

References

[1] J. Kelsey, B. Schneier, and D. Wagner, "Related-key cryptanalysis of 3WAY, Biham-DES, CAST, DES-X NewDES, RC2, and TEA," Lecture Notes in Computer Science (LNCS),Vol. 1334, pp. 233-246, Springer-Verlag 2007.

[2] NIST, Springfield, VA, "Data Encryption Standard (DES)," Oct. 1999.

[3] P. Israsena, "Design and Implementation of Low Power Hardware Encryption for Low Cost Secure RFID using TEA," Proc. International Conference on Information and Communication Systems (ICICS 2007), pp. 1402-1406, Dec2007.