IEEE VLSI Based projects based on verilog and Xilinx.

Network Security & Cryptographic Sciences

1. **Theoretical Modeling of Elliptic Curve Scalar Multiplier on LUT-Based FPGAs for Area and Speed**

This paper uses a theoretical model to approximate the delay of different characteristic two primitives used in an elliptic curve scalar multiplier architecture (ECSMA) implemented on k input lookup table (LUT)-based field-programmable gate arrays. Approximations are used to determine the delay of the critical paths in the ECSMA. This is then used to theoretically estimate the optimal number of pipeline stages and the ideal placement of each stage in the ECSMA. This paper illustrates suitable scheduling for performing point addition and doubling in a pipelined data path of the ECSMA. Finally, detailed analyses, supported with experimental results, are provided to design the fastest scalar multiplier over generic curves. Experimental results for GF(2163) show that, when the ECSMA is suitably pipelined, the scalar multiplication can be performed in only 9.5 μs on a Xilinx Virtex V. Notably the design has an area which is significantly smaller than other reported high-speed designs, which is due to the better LUT utilization of the underlying field primitives.

2. **Efficient Implementation of Reconfigurable Warped Digital Filters With Variable Low-Pass, High-Pass, Bandpass, and Bandstop Responses**

In this brief, an efficient implementation of reconfigurable warped digital filter with variable low-pass, high-pass, bandpass, and bandstop responses is presented. The warped filters, obtained by replacing each unit delay of a digital filter with an all-pass filter, are widely used for various audio processing applications. However, warped filters require first-order all-pass transformation to obtain variable low-pass or high-pass responses, and second-order all-pass transformation to obtain variable bandpass or bandstop responses. To overcome this drawback, the proposed method combines the warped filters with the coefficient decimation technique. The proposed architecture provides variable low-pass or high-pass responses with fine control over cut-off frequency and variable bandwidth bandpass or bandstop responses at an arbitrary center frequency without updating the filter coefficients or filter structure. The design example shows that the proposed variable digital filter is simple to design and offers substantial savings in gate counts and power consumption over other approaches.

3. **FPGA-Based 40.9-Gbits/s Masked AES With Area Optimization for Storage Area Network**

In order to protect “data-at-rest” in storage area networks from the risk of differential power analysis attacks without degrading performance, a high-throughput masked advanced encryption standard (AES) engine is proposed. However, this engine usually adopts the unrolling technique which requires extremely large field programmable gate array (FPGA) resources. In this brief, we aim to optimize the area for a masked AES with an unrolled structure. We achieve this by mapping its operations from to as much as possible. We reduce the number of mapping [to] and inverse mapping [to] operations of the masked SubBytes step from ten to one. In order to be compatible, the masked MixColumns, masked AddRoundKey, and masked ShiftRows including the redundant masking values are carried over . We also use FPGA block RAM (BRAM) to further reduce hardware resources. Compared with a state-of-the-art design, our implementation reduces the overall area by 36.2% (20.5% is contributed by the main method, and 15.7% is contributed by the BRAM optimization). It achieves 40.9-Gbits/s at 4.5-Mbits/s/slice on the Xilinx XC6VLX240T platform. We have attacked the iterative version of this masked AES in hardware. Results show that none of the bytes can be guessed from the masked AES with the collected 10 000 power traces, but 14 out of 16 bytes can be guessed from the unprotected AES with the same number of traces.

4. An efficient FPGA implementation of the Advanced Encryption Standard algorithm.

A proposed FPGA-based implementation of the Advanced Encryption Standard (AES) algorithm is presented in this paper. This implementation is compared with other works to show the efficiency. The design uses an iterative looping approach with block and key size of 128 bits, lookup table implementation of S-box. This gives low complexity architecture and easily achieves low latency as well as high throughput. Simulation results, performance results are presented and compared with previous reported designs.

5. A compact 32-Bit AES design for embedded system.

Recently, much research has been conducted for security of data transactions on embedded platforms. Advanced Encryption Standard (AES) is considered as one of a candidate algorithm for data encryption/decryption. One important application of this standard is cryptography on smart cards. In this paper we describe a 32-bits architecture developed for Rijndael algorithm to accelerate execution on 32-bits platforms with reduced memory. Using the FPGA device xc5vfx70t- 2ff1136-6, a very low-cost implementation of 375 occupied Slices is obtained under 303.364 MHz frequency.

6. **An Implementation of AES Algorithm Based on FPGA.**

An implementation of high speed AES algorithm based on FPGA is presented in this paper in order to improve the safety of data in transmission. The mathematic principle, encryption process and logic structure of AES algorithm are introduced. So as to reach the porpose of improving the system computing speed, the pipelining and papallel processing methods were used. The simulation results show that the high-speed AES encryption algorithm implemented correctly. Using the method of AES encryption the data could be protected effectively.

7. A FPGA Design of AES Core Architecture for Portable Hard Disk

This paper describes a high effective AES core hardware architecture for implementing it to encrypt/decrypt the data in portable hard disk drive system that apply to effectively in the terms of speed, scale size and power consumption to comply with minimum speed of 5 Gbps (USB3.0). We proposed the 128 bits data path of two different AES architectures design, Basic Iterative AES, which reuses the same hardware for all the ten iterations and , One Stage Sub Pipelined AES, with one stage of outer pipelining in the data blocks that both of them are purely 128 bits data path architecture that different from the previous public paper. The implementation result on the targeted FPGA, the basic iterative AES encryption can offer the throughput of 3.85 Gbps at 300 MHz and one stage sub pipelined AES can offer the throughput to increase the efficiency of 6.2 Gbps at 481 MHz clock speed. Index Terms- AES, Encrypt/decrypt, USB3.0, FDE, ATM