Design and Implementation of Lattice and Chaos based Post-Quantum Cryptography Algorithms

A

Thesis submitted

for the award of the degree of

DOCTOR OF PHILOSOPHY

By

BIKRAM PAUL

DEPARTMENT OF ELECTRONICS AND ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI

GUWAHATI - 781 039, ASSAM, INDIA

MARCH 2022

Abstract

The achievements we have made in the field of varied technology have largely fueled modern human growth. Data and digital information based innovations are playing a major role in the accelerated growth. Personal and other important secret data are considered vital asset since historical time and have become prime focus for the current information and digital generation. Various rudimentary data encryption methodologies, such as, Caesar cipher, Scytale cipher, Vigenère cipher, Steganography, Enigma machine were introduced in the past. With the invention of digital computers, to introduce greater resilience in security newer symmetric (e.g. DES, AES etc.) and asymmetric (e.g. RSA, ECC etc.) cryptography schemes are formulated in late ′90s, which are acting as the primary protector of data against adversary and unwanted intruders.

The rapid advancements of powerful and efficient hardware, data processing and computation are getting stronger, and breaking encryption has become simpler. To deal with new and stronger attacks, larger keys are being deploying to existing algorithms and more advance encryption schemes are getting developed. Moreover, it is theoretically proven that a sufficiently large quantum computer can easily break encryption based on asymmetric key cryptosystems employing Shor's algorithm and is able to exponentially shorten the time to determine key in symmetric cryptosystems using Grover's algorithm. According to Moscas inequality, there is a technical race persists between developing stronger encryption and actual scalable quantum computer. A security system that is completely secure against all types of attacks, is practically nearly impossible to implement. Therefore, in order to maintain a leading position in the race against advanced and efficient sophisticated quantum computing, better and stronger data security methodologies are of prime focus of the researchers.

A fully quantum cryptosystem can resists attacks generated from a quantum computer, which employs quantum channels and qubit as the medium of communication and computational units, respectively. To implement fully quantum security algorithms, massive changes need to be incorporated

within current communication infrastructure, which is not feasible in the recent times. Therefore, we need to adopt an alternative path to design cryptography algorithms called as post quantum cryptography (PQC) algorithms, which can overcome the vulnerability of classical as well as quantum computing based crypto attacks. Although, several PQC algorithms are developed recently, but due to hardware resource constraints, these algorithms were never deployed in any major cryptography applications. Thus, in the proposed work, we aim to resolve these issues.

In order to develop PQC algorithms, building blocks, such as, custom Pseudo-Random Number Generators (PRNGs) and polynomial modulo multiplier of finite field arithmetic are realized on FPGA platform. We propose two PRNGs in this thesis; BluXor for general purpose applications and MPCG for low-power IoT applications, which are inspired from Blum-Blum-Shub (BBS), Xorshift and Permuted Congruential PRNGs. The dynamic power consumption of the proposed PRNGs is $17mW$ at $48.31Mhz$ and $16mW$ at $42.90Mhz$ while generating 4.83×10^7 and 4.29×10^7 random 32-bit numbers per-second, respectively. The proposed PRNGs pass all the benchmark tests of standard NIST-SP $800-22$ and Diehard battery suite benchmark test for the analysis of randomness quality. These proposed PRNGs are further used during implementation cryptosystems.

Thereafter, a tensor based novel modulo multiplication method for multivariate polynomials over $GF(2^m)$ is realized, which is an essential building block while designing lattice LWE cryptosystem. The proposed method utilizes 6% lower resources, 6.5× less power consumption and achieves more than 6× speedup with respect to other contemporary single variable polynomial multiplication implementations. Its total power consumption is estimated to be approximately $0.2W$ and $0.492W$ at 100 MHz and 197 MHz while implement on Zynq-7000-Z020 and Artix-7-200T FPGA board, respectively. For multivariate polynomial of 9 variables having maximum degree of 128 for each variable, chip area, power and delay estimated for the proposed multiplier are $50113.9\mu m^2$, $1.485\ W$ and $8.812\ ns$ during its ASIC realizing. The computational complexity of single variable and multivariate polynomial multiplications are $O(n)$ and $O(np)$, respectively, where n is the maximum degree of a polynomial having p variables.

Finally, employing the above building blocks two PQC schemes, chaotic triple pendulum based cryptosystem and polynomial lattice based cryptosystem, are developed. A novel nonlinear chaos generator scheme is derived from a mechanical model depicting nonlinear dynamics of a triple pendulum physical system and a its effectiveness is validated against various standard tests, such as Lyapunov ex-

ponents test, bifurcation diagrams, sensitivity to parametric and to initial values, ergodicity, collision test, NIST randomness test etc. The proposed chaotic generator is utilized to develop a symmetric key encryption scheme, which is secure against various crypto attacks. The cryptosystem is verified through an FPGA implementation to assess its usage in low power high throughput applications, where its power consumption, resource utilization and throughput are 1.785×, 1.825× and 2.396× better as compared to other known contemporary methods. Further, it is observed that the proposed design can work efficiently with various wide range of applications. The average power and area of its ASIC implementation at 180-nm technology are 61.8836 mW and 0.20374 mm^2 at 250 MHz, respectively while realizing with SCL's 180-nm CMOS technology node. Moreover, the stable power consumption profile is generated by varying the operating frequency ranging from 1 KHz to 500 MHz.

Further, two lattice based fully homomorphic encryption (FHE) schemes are designed and implemented using software hardware co-design (on ARM-SoC and FPGA) approach, which provide strong resistance against quantum as well as classical computer based adversary security attacks. It is to mention that all the proposed algorithms and building blocks are compared with the best known contemporary methodologies. The proposed first scheme takes $\{6.88\mu s, 16.18\mu s, 2.84\mu s\}$ and $\{1.65\mu s, 4.38\mu s, 0.72\mu s\}$ for encryption, decryption and recryption using Zedboard and Virtex-7 FPGA platforms, respectively. Similarly, the second scheme consumes $\{1.44\mu s, 0.96\mu s, 0.22\mu s\}$ and $\{0.35\mu s, 0.225\mu s, 0.055\mu s\}$, respectively for encryption, decryption and recryption on the above mentioned FPGA platforms, respectively. The best implementation of the proposed FHE scheme is found to be 52.71× more resource efficient than another contemporary method based on BGV RLWE. The cumulative throughput of the proposed scheme is 6523.752 Mbps exhibiting 43% and 29% improvement over non-pipelined and pipelined BGV RLWE schemes, respectively, on Virtex-7 FPGA board. Similarly, the cumulative delay of our proposed FHE scheme developed for IoT enabled hardware applications is $0.63\mu s$, which is 23× lower than the BGV RLWE based FHE schemes. Since the proposed methods are having lowest area and delay footprints among the other contemporary schemes, they are the most suitable candidates for providing edge security to enabled IoT devices and other applications.