Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 5- Issue 1, Paper 35 January 2022

A Language Based System Architecture for Multiplanar Cryptosystems

Prathic R G , Jayachandiran U , Shanmuganathan S, Dinesh Gokul S
Sri Sairam Engineering College
Chennai, Tamil Nadu,India.
e8ec103@sairamtap.edu.in

***Abstract* - One of the most promising branches of quantum resilient cryptography is lattice based cryptography which offers versatility and efficiency. Discrete Gaussian samplers are a core building block in lattice-based cryptosystems, where optimized samplers are desirable both for high-speed and low-area applications. The inherent structure of existing sampling methods makes lattice-based cryptosystems vulnerable to side-channel attacks, such as timing analysis. The first comprehensive evaluation of discrete Gaussian samplers in hardware is presented, targeting FPGA devices.**

Keywords— Discrete Gaussian samplers, Cryptosystems, side channel attacks, FPGA.

I. INTRODUCTION

Cryptography is a method of protecting information and communications through the use of codes, encryption, decryption, keys, algorithms so that only those for whom the message is intended can read and process it. There are two types of ciphers symmetric and asymmetric ciphers. Asymmetric cryptographic primitives are used for secure Internet communications, such as Diffie-Hellman key exchange, RSA and ECDSA, will be rendered completely insecure with the practical development of a quantum computer. Even symmetric-key encryption schemes, such as the advanced encryption standard (AES), DES will have a quadratic brute-force speedup, decreasing search space. There are now emerging branches of cryptography resistant to these quantum reductions, namely, quantum-resilient or post-quantum cryptography which deals with non-quantum operations but is theoretically strong against cryptanalysis on classical and quantum computers. Lattice-based cryptography is the generic term for constructions of cryptographic primitives that involve lattices, either in the construction itself or in the security proof. They are currently important candidates for post-quantum cryptography. Unlike the RSA, Diffie-Hellman or ECC, which could, theoretically, be easily attacked by a quantum computer, some lattice-based constructions appear to be resistant to attack by both classical and quantum computers.

II. SIDE CHANNEL ATTACKS

In computer security a side-channel attack is any attack based on gaining information from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself. Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited. A timing attack watches data movement into and out of the CPU or memory on the hardware running the cryptosystem such as caches or algorithm. Simply by observing variations in how long it takes to perform cryptographic operations, it might be possible to determine the entire secret key. A power-analysis attack can provide even more detailed information by observing the power consumption of a hardware device such as CPU or cryptographic circuit.

III. DISCRETE GUASSIAN SAMPLERS

A discrete Gaussian distribution over some fixed lattice is a distribution in which each lattice point is sampled with probability proportional to the probability density function of a continuous Gaussian distribution of width s evaluated at that point. Gaussian distribution, also known as Normal distribution is a probability distribution that is symmetric about the mean, showing that data near the mean are more frequent in occurrence than data far from the mean. In graph form, normal distribution will appear as a bell curve. Sampling from a discrete Gaussian distribution is an essential part of lattice-based cryptography. The probability distribution function of a discrete Gaussian distribution defined over Z with mean $\mu = 0$ and standard deviation σ is defined as,

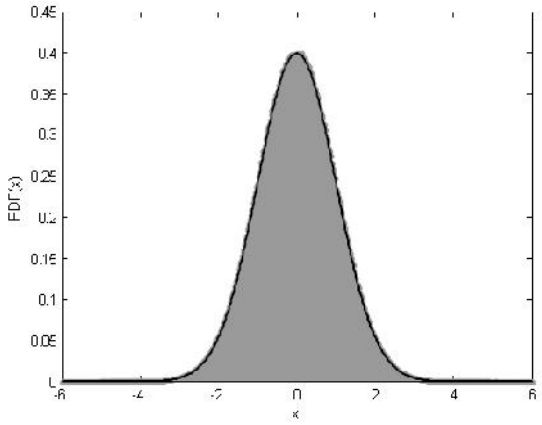
$$D_{z,\sigma}(X = z) = (1/S)e^{((-z^2)/2\sigma^2)}$$

To generate samples over Z, it is sufficient to generate samples over Z+ using a single random bit to determine the sign due to the symmetry of discrete Gaussian distribution across its mean. Sampling thus performed has a wide range of applications in different fields of science, mathematics, and engineering. Since the start of their use in lattice-base cryptography, several methods have been proposed to sample from a discrete Gaussian distribution including rejection sampling, cumulative distribution table (CDT) based sampling, discrete Ziggurat sampling, Knuth-Yao sampling, and Bernoulli sampling. The

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

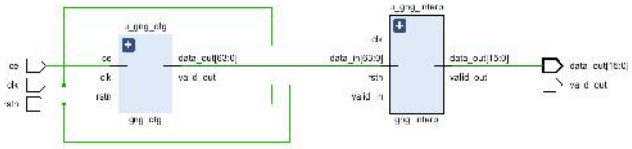
Volume 5- Issue 1, Paper 35 January 2022

CDT based sampling precomputes a cumulative distribution function (CDF) table T according to the given discrete Gaussian distribution with λ bits of precision.

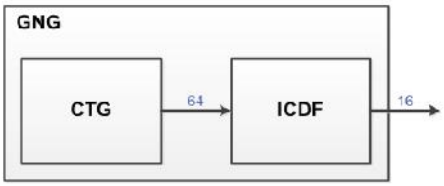


IV. GUASSIAN NOISE AND PSEUDO RANDOM NUMBER GENERATORS

The Gaussian Noise Generator (GNG) core generates white Gaussian noise of standard normal distribution, which can be used to measure extremely low BER levels using a 64-bit combined generator and an approximation of the inverse normal CDF, which obtains a PDF that is Gaussian to up to 9.1σ. An algorithm used to produce an open-ended sequence of bits is referred to as PRNG. PRNGs require uniformity, scalability and consistency. These algorithms fall on the category of purpose built and existing cryptographic algorithms such as a block cipher or hash functions. Random numbers play an important role in the use of encryption for various security applications. A number of network security algorithms and protocols based on cryptography make use of random binary numbers. The concern in the generation of a sequence of random numbers has been that the sequence of numbers be random in a well-defined statistical sense. The two criteria used to validate randomness are uniform distribution and independence. In applications such as reciprocal authentication, session key generation and stream ciphers, the requirements is not just that the sequence of numbers be statistically random but that the successive members of the sequence are unpredictable. With 'true' random sequences, each number is statistically independent of other numbers in the sequence and therefore unpredictable. Thus, it is more common to implement algorithms that generate sequences of numbers that appear to be random.



Cryptographic applications typically make use of algorithm techniques for random number generation. These algorithms are deterministic and therefore produce sequences of numbers that are not statistically random. However, if the algorithm is good, the resulting sequences will pass many tests of randomness. such numbers are referred to as pseudorandom numbers. The core was designed using synthesizable Verilog code and can be delivered as a soft-IP targeted for any FPGA device and ASIC technology. Period of generated noise sequence is about 2^176. Random distribution in the range of ±9.1σ. Noise is quantized to 16 bits with 5 bits of integer and 11 bits of fraction. Internal 64-bit uniform random number generator with configurable initial seeds.



Top module architecture

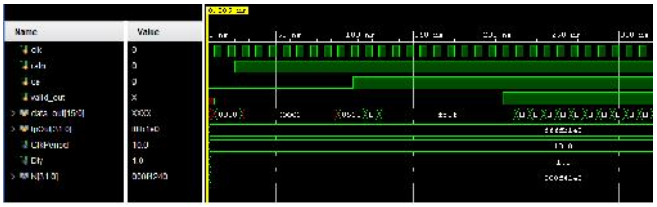
Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 5- Issue 1, Paper 35 January 2022

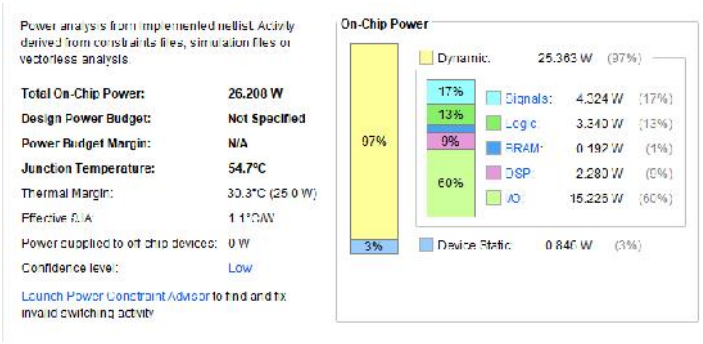
In an advanced FPGA a high throughput of over 300 MHz clock rate and output sample rate is achieved. Fully synchronous design using single clock and optimized design for Xilinx & Altera FPGA technology can be used in Communication system requiring accurate emulation of an AWGN channel.

CONCLUSION

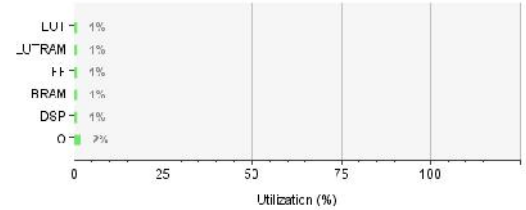
With the proposed hardware CDT design a throughput of 59.4 million samples per second for encryption, which utilizes just 43 slices on a Virtex-6 FPGA and 16.3 million samples per second for signatures with 179 slices on a Spartan 6 device is achievable.



The designs can be implemented on either the Spartan-6 LX25-3, Virtex-5 LX30, or Virtex-6 LX75 FPGA devices, using Xilinx ISE 14.7 or Xilinx VIVADO 2018 tools or higher versions.



Resource	Utilization	Available	Utilization %
LUT	252	433200	0.06
LUTRAM	20	174200	0.01
FF	337	866400	0.04
BRAM	1	1470	0.07
DSP	2	3600	0.06
IO	20	850	2.35



Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 5- Issue 1, Paper 35 January 2022

REFERENCES

[1] Howe, J., Khalid, A., Rafferty, C., Regazzoni, F., & O'Neill, M. (2016). On practical discrete Gaussian samplers for lattice-based cryptography. *IEEE Transactions on Computers*, *67*(3), 322-334.

[2] Karmakar, A., Roy, S. S., Reparaz, O., Vercauteren, F., & Verbauwhede, I. (2018). Constant-time discrete gaussian sampling. *IEEE Transactions on Computers*, *67*(11), 1561-1571.

[3] Roy, S. S., Vercauteren, F., & Verbauwhede, I. (2013, August). High precision discrete Gaussian sampling on FPGAs. In *International Conference on Selected Areas in Cryptography* (pp. 383-401). Springer, Berlin, Heidelberg.

[4] Micciancio, D., & Regev, O. (2009). Lattice-based cryptography. In *Post-quantum cryptography* (pp. 147-191). Springer, Berlin, Heidelberg.

[5] Tiri, K. (2007, June). Side-channel attack pitfalls. In *2007 44th ACM/IEEE Design Automation Conference* (pp. 15-20). IEEE.