IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST)

December 15-17, 2020

Virtual (IIT Kharagpur)

Kolkata, India

Compact and Secure Generic Discrete Gaussian Sampler based on HW/SW Co-design

Sudarshan Sharma, Arnab Bag†, and Debdeep Mukhopadhyay†*

* Dept. of Electronics and Electrical Communication Engineering, IIT Kharagpur, † Dept. of Computer Science and Engineering, IIT Kharagpur.

Email: * sudarshansharma04@gmail.com

Outline

- Background
  - Lattice-based Cryptosystem
  - Gaussian Sampler
    - Methods
- Our work
  - Generic Gaussian Sampler
    - Multi-level logic optimisation
    - Lightweight countermeasure description
- Results

Lattice-based Cryptosystem

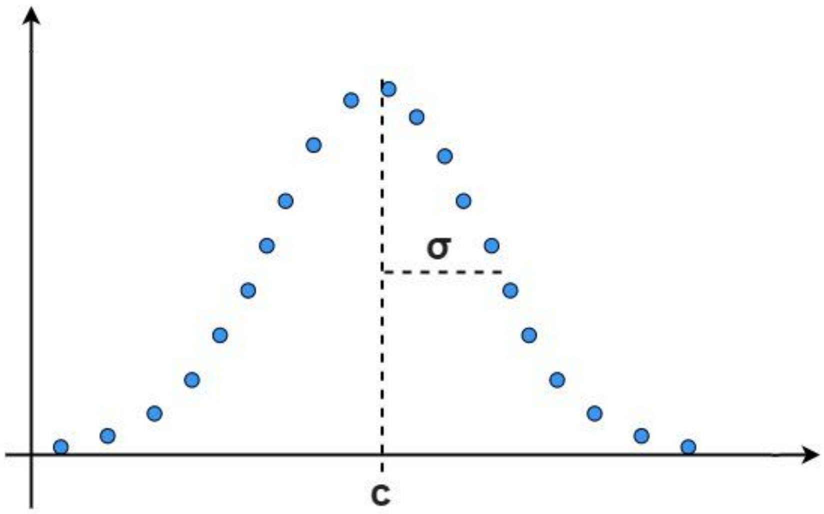
- Existing PKC can be exploited using large scale quantum computers using the Shor's [1] and Proos-Zalka's [2] algorithms.

- Presently, Lattice-based cryptosystems are quantum secure.

Discrete Gaussian Sampler is considered the heart of lattice-based cryptography.

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,"SIAM J. Comput., vol. 26,no. 5, p. 1484–1509, Oct. 1997.
[2] Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves,"Quantum Inf. Comput., vol. 3, pp. 317–344, 2003.

Gaussian Sampler



Challenges Involved

- High-precision architecture design
- Optimisation of precomputed tables access
- Side-channel vulnerability mitigation

Methods

- Problems associated with existing implementations
  - Parameter specific
    - Lack scalability and modularity.
  - Side channel vulnerabilities
    - Resource utilisation is exorbitantly high.

 # Requirement for Generic Sampler for various lattice based constructions.

Intuitive Idea

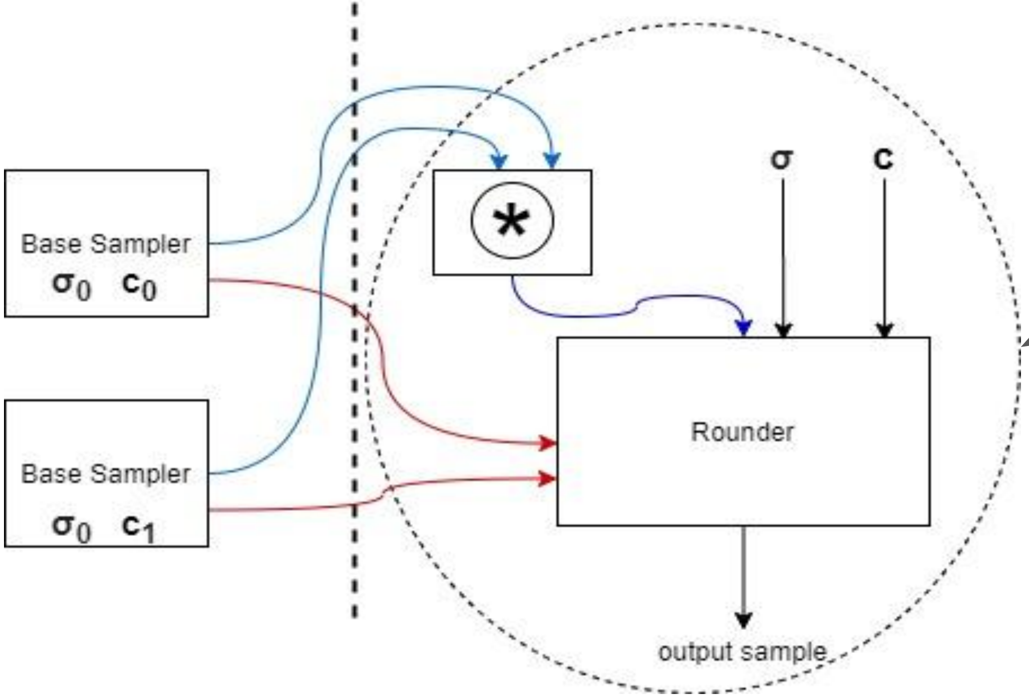
- *Combine samples from a smaller distribution and generate samples with higher standard deviation*.

- Micciancio et al. [3] proposed an algorithm to sample **any** discrete Gaussian distribution with **an arbitrary** center and standard deviation using multiple fixed smaller distributions.

- However, they do not propose any design methodologies, feasibility metrics, and strategies to incorporate the fixed samplers architecture in hardware.

[3] M. D. and W. M., "Gaussian Sampling over the Integers: Efficient,Generic, constant-time,"Advances in Cryptology - CRYPTO. LectureNotes in Computer Science, vol. 10402, 2017.

Generic Gaussian Sampler



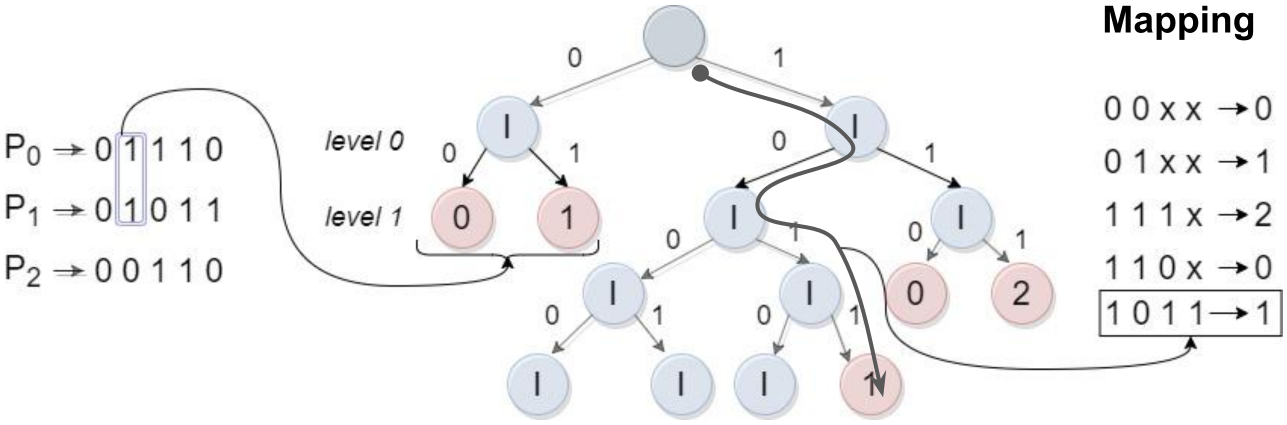
Recursive, so implementation in hardware is difficult.

HW/SW co-design

Base Sampler Improvements

- Knuth Yao Algorithm[4] as Base Sampler

Pmat **DDG Tree** **Boolean Mapping**



Toy Example

Implementation

Existing Work

Two level optimisation using ESPRESSO.

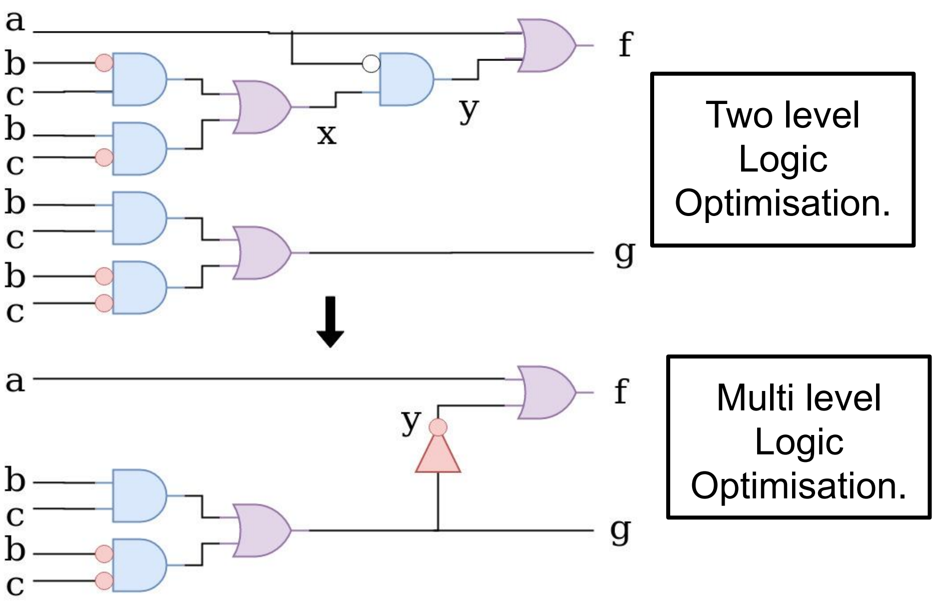
This Work

Multi level Logic Optimisation.

[4] D. Knuth and A. Yao,The complexity of nonuniform random number generation, in Algorithms and Complexity: New Directions and Recent Results. Cambridge, MA, USA: Academic Press 1976, 1976.

Multi level logic Optimisation

$$f = a + y$$
$$g = b.c + \bar{b}.\bar{c}$$
$$y = \bar{a}.x$$
$$x = \bar{b}.c + b.\bar{c}$$



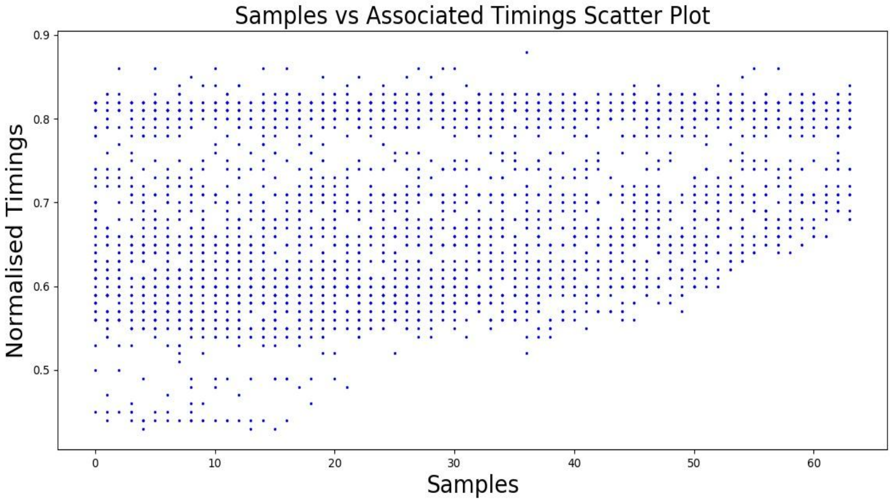
Example from [5]

Multi level logic Optimisation Advantages

- Minimizes the number of literals in the logic expression.
- Re-utilization of logic created previously.

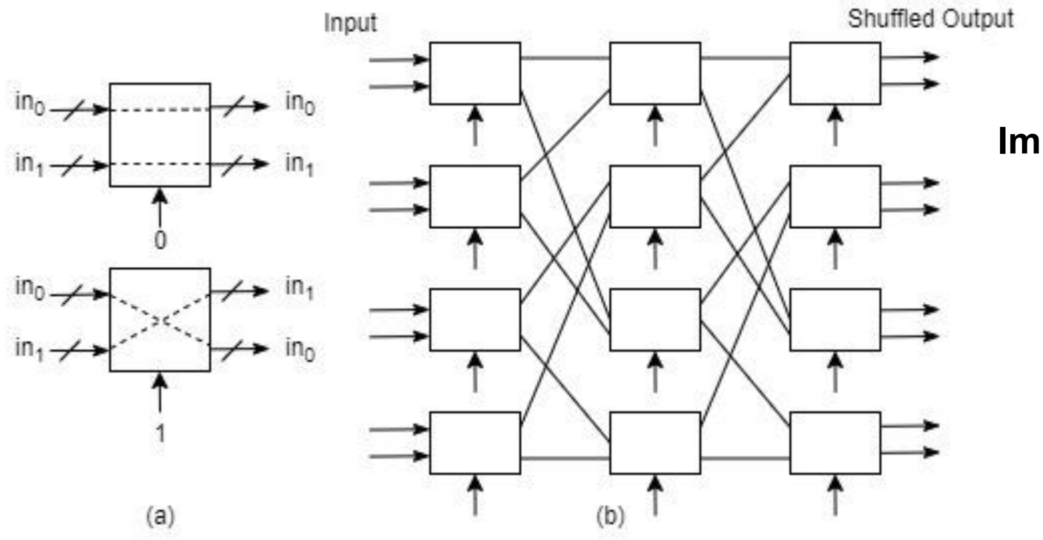
[5] M. Fujita, "Basic and advanced researches in logic synthesis and their industrial contributions," inProceedings of the 2019 International Symposium on Physical Design, ser. ISPD '19. New York, NY, USA:Association for Computing Machinery, 2019, p. 109–116.

Side-Channel Vulnerability



Boolean mapping is many-to-one where each sample has multiple timing leakages related to different inputs as seen above which shows the normalized timing for every path corresponding to a particular sample.

Lightweight Countermeasure

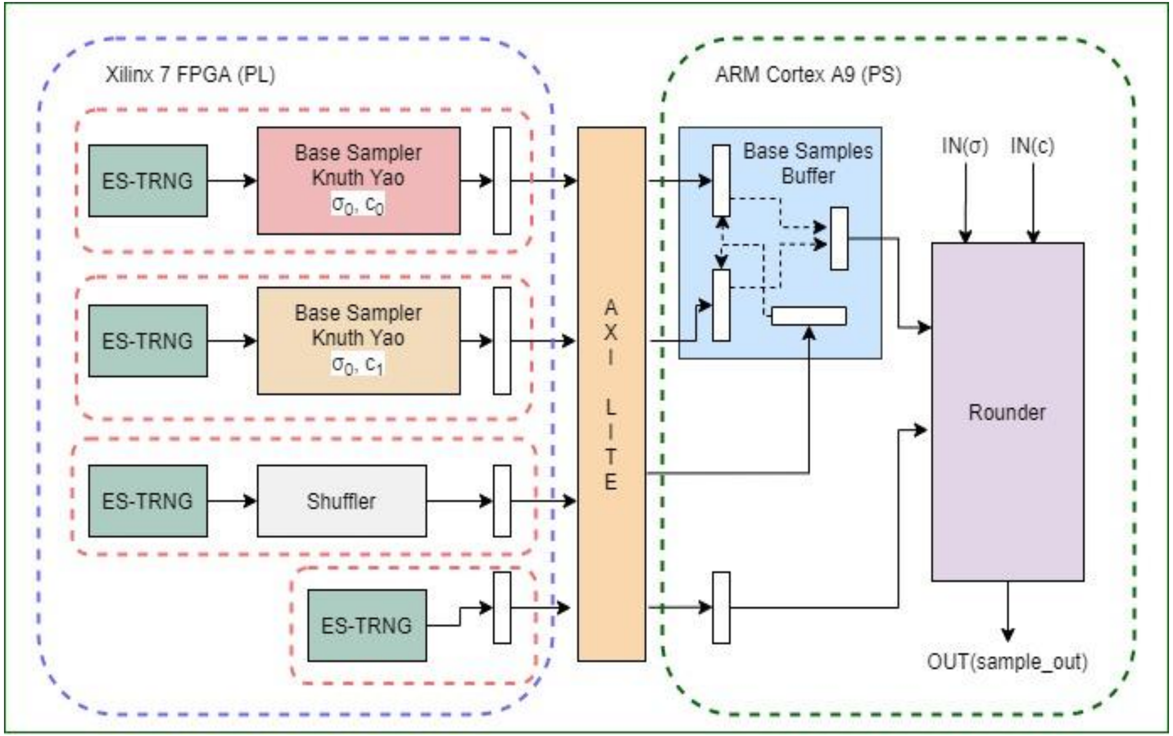


(a) Permutation network building block (swapper) (b) Permutation network for 8 inputs.

Improvement with Shuffling countermeasure

- Parallel shuffling network using the permutation network generator
- Removing the shuffler from the critical path of the sample generation utilizing the HW/SW co-design model
- Increase in shuffling stages by performing shuffling every time the sample is utilized by the Rounder

Combined Architecture



Resource Utilization

Design Block	LUT/FF/Slice	Delay (ns)
Base Sampler (c=0)	1241/0/579	24.26
Base Sampler (c=0.5)	1263/0/589	23.19
Shuffler (n=32)	773/0/170	3.06
ES-TRNG [6]	9/5/9	[a]

[a] the critical path varies depending on the sample

Digilent Zedboard used for the experiment, which has a Zynq-7000 series FPGA as Programmable Logic (PL) coupled with Dual-core ARM Cortex-A9 as Processing Subsystem(PS).

[6] B. Yang, V. Roˇzic, M. Grujic, N. Mentens, and I. Verbauwhede, "Es-trng: A high-throughput, low-area true random number generator based on edge sampling,"IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. Volume 2018, pp. Issue 3–, 2018.

Results

σ	Design	Device	λ	LUT/FF/Slice	BRAM	Clock cycle	Delay per sample (ns)
3.33	Howe et al. [7]	5VLX30-3	64	133/52/48	2	1.23	5.80
3.33	This work w/o shuffling	5VLX30-3	64	339/0/142	0	1	15.90
6.15543	Karmakar et al. (Batchinig) [8]	6VCX75T-2	112	1024/1237/113	15	27344	3204
6.15543	Karmakar et al. (Unrolled) [8]	6VCX75T-2	112	2682/977/*	*	1	4.9
6.15543	This work w/o shuffling	6VCX75T-2	112	1070/0/427	0	1	24.13

- First implementation in HW/SW co-design setting, to generate a Gaussian distribution with any arbitrary center and standard deviation.
- 60% lesser LUT utilisation, suitable for resource constrained systems.
- No delay elements and BRAM used.

[7] J. Howe, A. Khalid, C. Rafferty, F. Regazzoni, and M. O'Neill, "On practical discrete gaussian samplers for lattice-based cryptography,"IEEE Transactions on Computers, vol. 67, no. 3, pp. 322–334, 2018.
[8] Karmakar, S. S. Roy, O. Reparaz, F. Vercauteren, and I. Verbauwhede,"Constant-time discrete gaussian sampling,"IEEE Transactions on Computers, vol. 67, no. 11, pp. 1561–1571, 2018.

Questions

?