Time-Independent Discrete Gaussian Sampling For Post-Quantum Cryptography

Ayesha Khalid, James Howe, Ciara Rafferty, and Máire O'Neill,

Centre for Secure Information Technologies (CSIT), Queen's University Belfast, UK.

@CSIT_QUB @SAFEcrypto

jhowe02@qub.ac.uk

Aims and Objectives

This research aims to provide:

- **Area/speed efficient discrete Gaussian sampling hardware designs**
- **The hardware designs are scalable with results given for both Encryption and Signature parameters.**
- **Sampler designs run in constant-time and this are resilient to side-channel (SCA) timing analysis attacks.**
- **Practical hardware cumulative distribution table (CDT) designs for both lattice-based Encryption and Signatures.**

Cumulative Distribution Table (CDT) Sampling

The use of discrete Gaussian sampling based on large pre-computed tables was first proposed by Peikert [2010]. The procedure works as:

1. **The Cumulative Distribution Table (CDT) sampler requires a precomputed table of discrete Gaussian cumulative distribution function (CDF) values, with λ-bits of precision.**
2. **A lookup table stores the N samples (0 = S[0] < S[1] < ⋯ < S[N-3] = 1).**
3. **CDF values S[·] are then accessed via a random sample r ← [0,1).**
4. **The desired sample x is found satisfying interval S[x] ≤ r < S[x+1], which occurs with probability ρ[x] = S[x+1] - S[x].**
5. **Initial table values (close to x = 0) are more probable than values near the end.**

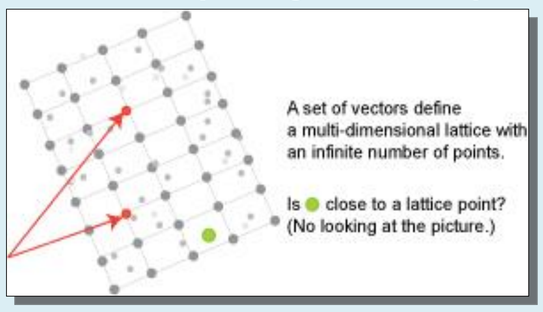
C. Peikert, "An efficient and parallel Gaussian sampler for lattices," in CRYPTO, 2010, pp. 80–97.

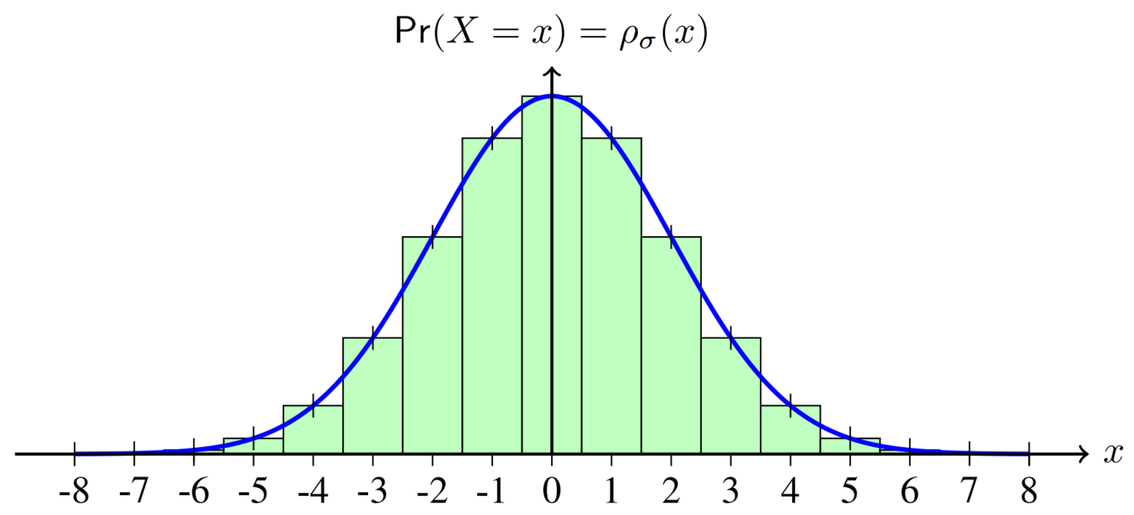
Post-Quantum Cryptography

Conventional non-quantum cryptographic algorithms that will remain secure even after practical quantum computing is a reality.

Advantages of lattice-based crypto:

- Underlying operations can be implemented efficiently.
- Most promising as allows for other constructions/applications beyond encryption/signatures, e.g. IBE, ABE, homomorphic encryption etc.



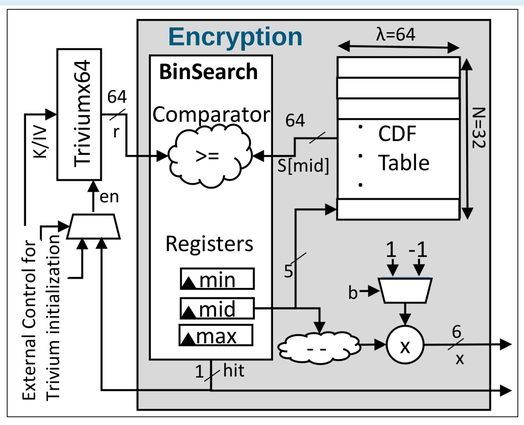


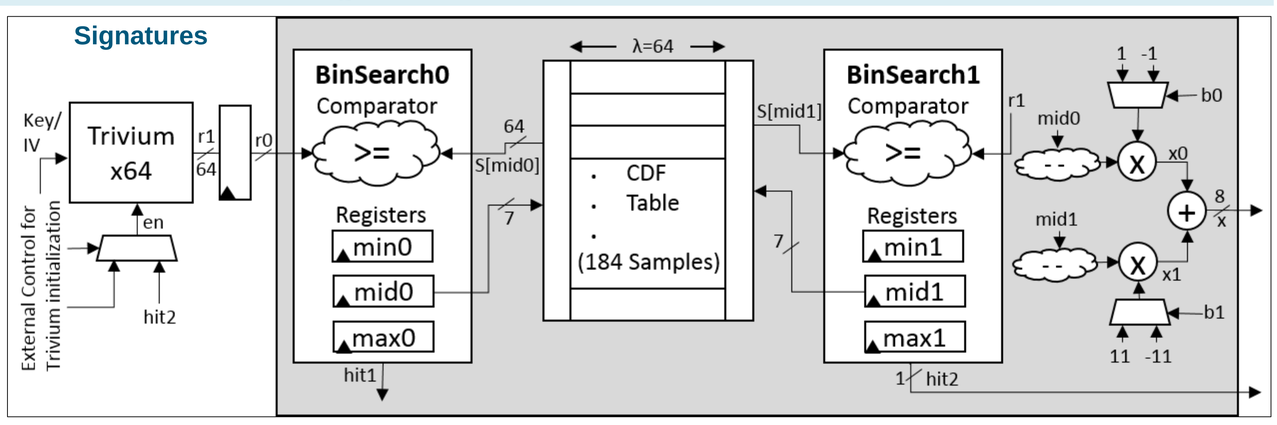
The Discrete Gaussian Distribution

Time-Independent CDT Sampling For Post-Quantum Cryptography

Algorithm 1 CDT Sampling from $D_{\mathbb{Z},\sigma}$ via Binary Search

Require:
1: Three integers min, mid, and max.
2: CDT values $0 = S[0] < S[1] < \cdots < S[N-3] = 1$.
3: Uniformly sampled $r \in \{0, \ldots, (2^\lambda - 1)\}$ and bit $b \in \{0, 1\}$.
Ensure: $(min = 0,\ max = N,\ mid = \lceil (min + max)/2 \rceil)$
▷ Start Binary Search:
4: **while** $(max > min)$ **do**
5: **if** $(r \geq S[mid])$ **then**
6: $min \leftarrow (mid + 1)$;
7: **else**
8: $max \leftarrow mid$;
9: **end if**
10: **end while**
11: **return** $x = (-1)^b(mid - 1)$





Op.	Implementation	Device	λ	LUT/FF /Slice	BRAM	Freq. (MHz)	Clock Cycles	Rand. Bits	Ops/s (MHz)	Ops/s/S (MHz/S)	Time Ind.
$\sigma_{LP} = 3.33$	Pöppelmann & Güneysu [21]	6VLX75T-2	80	863/6/231	0	61	1	85	6.1	0.26	✓
				911/6/255	0	61	1	85	6.1	0.24	✓
	This work	6VLX75T-2	64	112/19/43	0	297	5	64	59.4	1.38	✓
				53/17/15	1	193	5	64	38.6	2.57	✓
	Du & Bai [20]	5VLX30	112	43/33/17	1	259	≈2.28	≈9.44	113.6	6.68	✗
				85/65/39	1	256	≈1.14	≈9.44	224.6	5.76	✗
$\sigma_{BLISS} = 215$	Pöppelmann *et al.* [19]	6SLX25-3	128	928/1121/299	1	129	≈7.5	≈21	17.2	0.06	✗
	This work	6SLX25-3	64	577/64/179	0	130	8	64	16.3	0.09	✓
				130/48/44	2	126	8	64	15.8	0.36	✓

Post-place and route results of the proposed constant-time CDT sampler for Encryption and Signature parameters, in comparison to existing CDT results.

Results significantly outperform previous results for use in Signatures ($\sigma_{BLISS} = 215$), and competes for use in Encryption ($\sigma_{LP} = 3.33$), with added quality of time-independence.

www.**safe**crypto.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644729