Hardware Implementation of Discrete Gaussian Sampling for FALCON Digital Signature

Nhat Dang, Padmanabha Nikhil Bhimavarapu

Department of Electrical and Computer Engineering
North Carolina State University

December 9, 2024

Introduction

Problem Statement:

- Quantum computing threatens classical cryptographic systems.
- Post-quantum cryptography (PQC) aims to secure systems against quantum threats.

Objective:

- Design a hardware implementation of Discrete Gaussian Sampling (DGS) for the FALCON signature scheme.
- Optimize DGS on the Xilinx Zynq-7000 SoC FPGA platform.

Significance:

- Enhance performance and efficiency in quantum-safe cryptography.

Background

Lattice-Based Cryptography (LBC):

- A leading approach in PQC, valued for efficiency and adaptability.
- Relies on hard problems like Short Integer Solution (SIS) and Learning with Errors (LWE).

FALCON:

- A lattice-based signature scheme selected by NIST for standardization.
- Combines NTRU lattices with a fast trapdoor sampling technique.

Discrete Gaussian Sampling (DGS):

- Accounts for 72% of FALCON's computational overhead.
- Includes base sampling and rejection sampling stages.

Proposed Design

Hardware-software co-design targeting Xilinx Zynq-7000 SoC ZC702 evaluation board, featuring the XC7Z020-CLG484-1 FPGA.

Key Features:

- Two-layer sampling mechanism: base sampling and rejection sampling.
- ChaCha20-based pseudorandom number generator (PRNG).
- Efficient arithmetic pipeline for rejection sampling
- Full hardware implementation

Discrete Gaussian Sampler Algorithm

Algorithm 1 Discrete Gaussian Sampler

```
Require: $\mu$: mean, $\sigma^{-1}$: inverse std dev
$s \leftarrow \lfloor \mu \rfloor$                                   ▷ Integer part
$r \leftarrow \mu - s$                                               ▷ Fractional part
$d_{ss} \leftarrow \frac{1}{2}(\sigma^{-1})^2$
$c_{cs} \leftarrow \sigma_{\min} \cdot \sigma^{-1}$                  ▷ Scaling factor
loop
    $z_0 \leftarrow$ Gaussian0Sampler                                ▷ Base Gaussian sample
    $b \leftarrow$ RandomBit                                         ▷ ChaCha20-based PRNG
    $z \leftarrow b + (2b - 1) \cdot z_0$                            ▷ Bimodal transformation
    $x \leftarrow (z - r)^2 \cdot d_{ss} - \frac{z^2}{2\sigma_0^2}$
    if BerExp($x, c_{cs}$) then                                      ▷ Rejection criterion
        return $s + z$
    end if
end loop
```

Ref1: Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon: Fast-fourier lattice based compact signatures over ntru. 2019.

Evaluation and Results

Resource Utilization:

- LUTs: 18.62% of available (9,904 out of 53,200).
- Flip-Flops: 8.14% utilized.
- DSP Slices: 29.09% of available slices used.

Performance:

- Latency (SW): 143 clock cycles.
- Latency (HW): 325 clock cycles.
- Throughput: 203,077 samples/sec at 66 MHz.

Design	**Latency (cycles)**	**Frequency (MHz)**	**Throughput (sample/sec)**
Reference Software	96,747	666	6,890
Previous Design	124	45	362,903
Proposed Design*	325	66	203,077

References:

- P.-A. Fouque et al., "Falcon: Fast-fourier lattice-based compact signatures over NTRU," https://falcon-sign.info, 2019. [?]
- E. Karabulut and A. Aysu, "A hardware-software co-design for the discrete gaussian sampling of FALCON digital signature," Cryptology ePrint Archive, Paper 2023/908, 2023. [Online]. Available: https://eprint.iacr.org/2023/908.

*Results do not include generation of s,ccs,dss,r

Performance Comparison

Highlights:

- The reference software, operating at 666 MHz, exhibits:
  - **Latency:** 96,747 cycles.
  - **Throughput:** 6,890 samples/sec.
- The proposed implementation, operating at 66 MHz, achieves:
  - **Latency:** 325 cycles.
  - **Throughput:** 203,077 samples/sec.
- Compared to the software, the proposed design achieves a **29.5× speedup in throughput**.

Insights:

- Hardware acceleration offers significant advantages over software-based approaches.
- The proposed design provides an effective baseline for further optimizations.
- Techniques such as parallelism and pipelining could further enhance performance.
- This design under-performs when compared to the previous work.

Conclusion

Summary:

- Designed a hardware implementation of DGS for FALCON.
- Achieved efficient resource utilization and high throughput.

Thank You!

Questions?