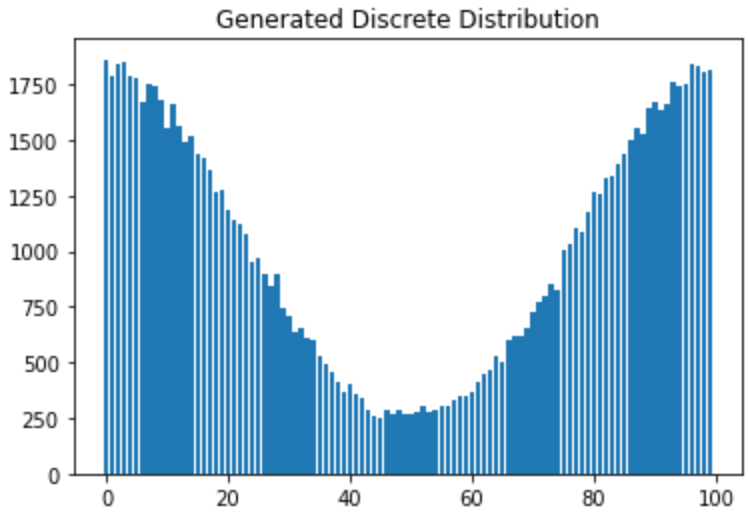
Post Quantum Cryptography

Issues in Discrete Gaussian Distribution Implementation



Introduction

For the implementation of a public key cryptosystem, the noise '**e**' is chosen from a discrete gaussian distribution. However, we have found that the generated distribution has a distorted bell curve shape.

Methodology

x : value from a normal distribution X ~ N(0,σ)

q : parameter in the LWE crypto system.

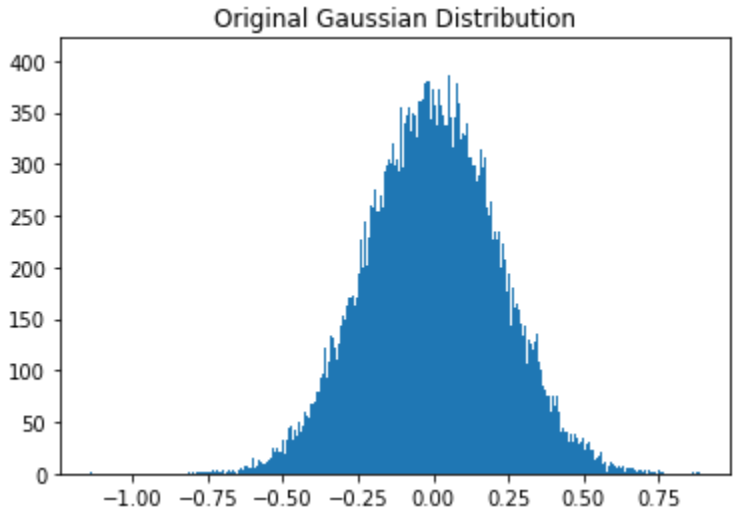
We transform x into a discrete distribution using the following steps.

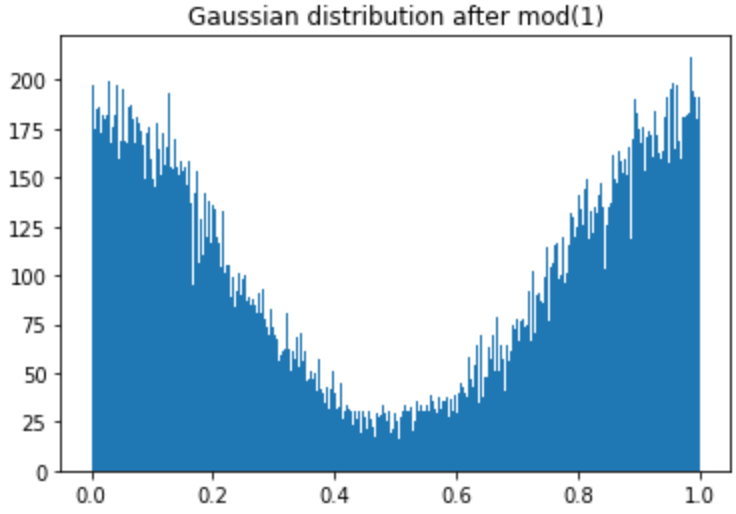
1. x mod(1)
2. y = round(X mod(1)*q) mod q

The first step maps the distribution X into [0,q) and the second step maps that distribution to the discrete range [0,q-1].

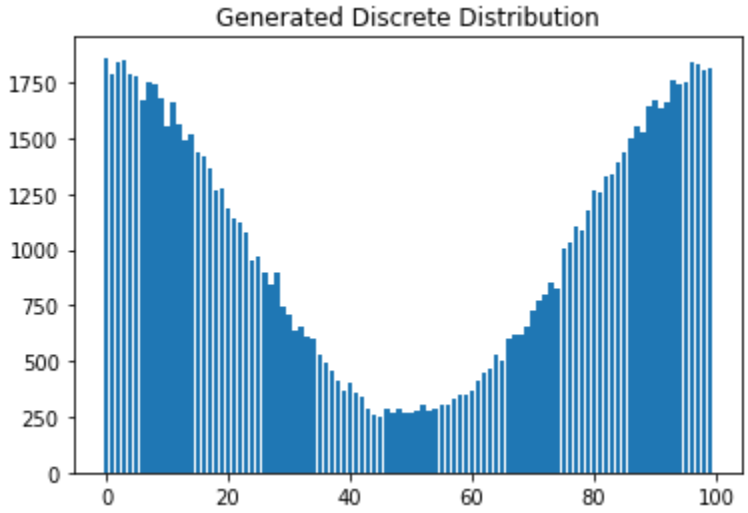
Issue

From step 1, the negative half of the gaussian distribution is mapped to the positive half. (σ is increased to easily observe the issue.)



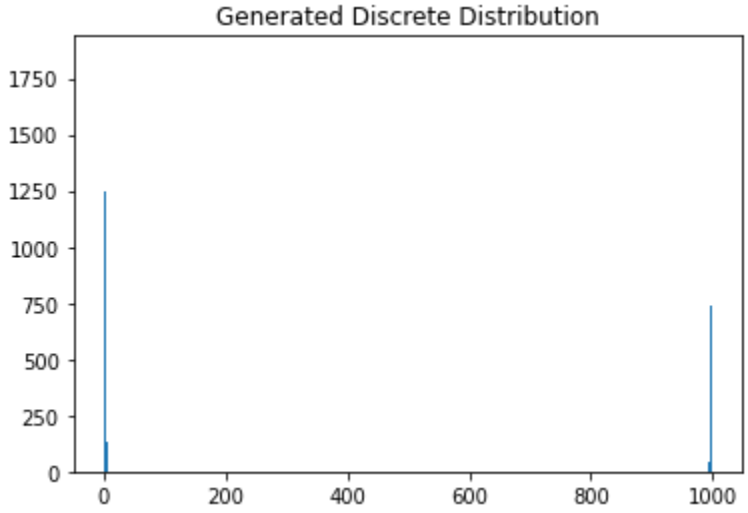


Since the resulting distribution does not have any positive values, the resulting discrete distribution also does not have negative values and does not have a proper gaussian bell curve.



Since the noise is added according to the discrete gaussian distribution, with mean =0, standard deviation σ = α / sqrt(2*pi) where α = sqrt(n)/q.

According to the above steps, and with alpha calculated, the following distribution was generated.



n = 30, q = 1000,α =0.005477, σ = 0.002185. SInce smaller positive and negative values are used for the noise, the values at the higher end of the distribution should be mapped back to the minus region by subtracting q.