From: Marcio Barbado, Jr. <marcio.barbado@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
CC: Márcio Barbado Júnior <mbarbado@usp.br>
Subject: [pqc-forum] central limit theorem convergence acceleration for DGS efficiency
Date: Monday, October 31, 2022 06:51:10 PM ET

Hi. This is to share some results of my MSc work, still in progress, which is about discrete Gaussian sampling for RLWE-based cryptography [1]. The referred work samples in a slightly different fashion. Comparisons are made against the CDT sampling strategy, and the results lead us to believe that the adopted strategy offers consistent efficiency gains for a number of contexts, mostly regarding digital signatures.

Regards,

Márcio Barbado, Jr.
MSc student
Escola Politécnica da Universidade de São Paulo

[1] Efficient Gaussian sampling for RLWE-based cryptography through a fast Fourier transform <https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Feprint.iacr.org%2F2022%2F1490&amp;data=05%7C01%7Cyi-kai.liu%40nist.gov%7C949205c7ea5e414ac24708dabb92657b%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C638028534704093636%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&amp;sdata=DK%2FK9w9XsWlTNzWvToG71WI6cb9rJzSOOwc%2FfkD2Ea8%3D&amp;reserved=0>

--