Fast, Compact, and Constant-time Discrete Gaussian Sampling over Integers

Raymond K. Zhao

Faculty of Information Technology,
Monash University

Background

- Sampling from $\mathcal{D}_{\mathbb{Z},\sigma}$ for large σ: Base sampler with smaller deviation + Expander.
- Binary Sampling Algorithm [DDLL13]:
  - Base samplers: $x \hookleftarrow \mathcal{D}^{+}_{\mathbb{Z},\sigma_0}$, and $y \hookleftarrow \mathcal{U}(\{0,\ldots,k-1\})$, where $\sigma_0 = \sqrt{1/2\ln 2}$ and $k \in \mathbb{Z}^{+}$.
  - Expander: Compute $z = kx + y$. Use a Bernoulli sampler to reject z, with the acceptance bias: $p = \exp\left(-y(y+2kx)/2\sigma^2\right)$.
  - This algorithm will generate $z \hookleftarrow \mathcal{D}^{+}_{\mathbb{Z},k\sigma_0}$.
  - Side-channel attacks: [BHLY16, PBY17, EFGT17, BDE^{+}18].
  - Previous countermeasures:
    - Full-table access [PBY17, EFGT17].
    - Compute p by using a large look-up table (qTesla [BAA^{+}17]).

Renyi Divergence [Pre17]

- The Bernoulli sampler could fit in double precision (53 bits).
- Efficiency is independent of σ (relies on the number of samples instead).
- The $\exp(x)$ in C library is not constant-time (floating-point division).

Adapted from [Pre17], Lemma 3 and Eq. 4

For two distributions $\mathcal{P}$ and $\mathcal{Q}$ such that $\mathrm{Supp}(\mathcal{P}) = \mathrm{Supp}(\mathcal{Q})$, we have:

$$R_\alpha(\mathcal{P}||\mathcal{Q}) \leq 1 + \frac{\alpha \cdot (\Delta(\mathcal{P}||\mathcal{Q}))^2}{2},$$

when $\Delta(\mathcal{P}||\mathcal{Q}) \to 0$. In addition, for M independent samples, sampling from $\mathcal{P}$ will be λ-bit secure if $R_{2\lambda}(\mathcal{P}||\mathcal{Q}) \leq 1 + 1/(4M)$. Typically we have $M = m \cdot q_s$, where m is the dimension of the lattice, and q_s is the number of queries.

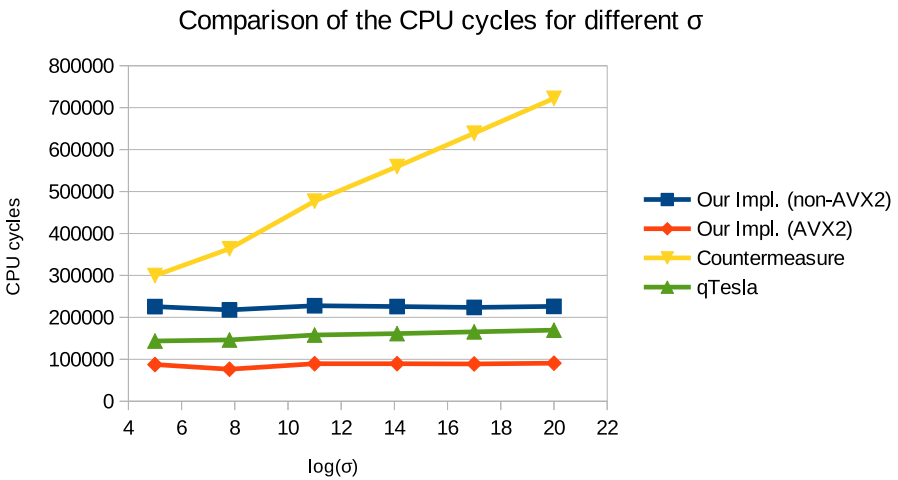
Proposed Techniques

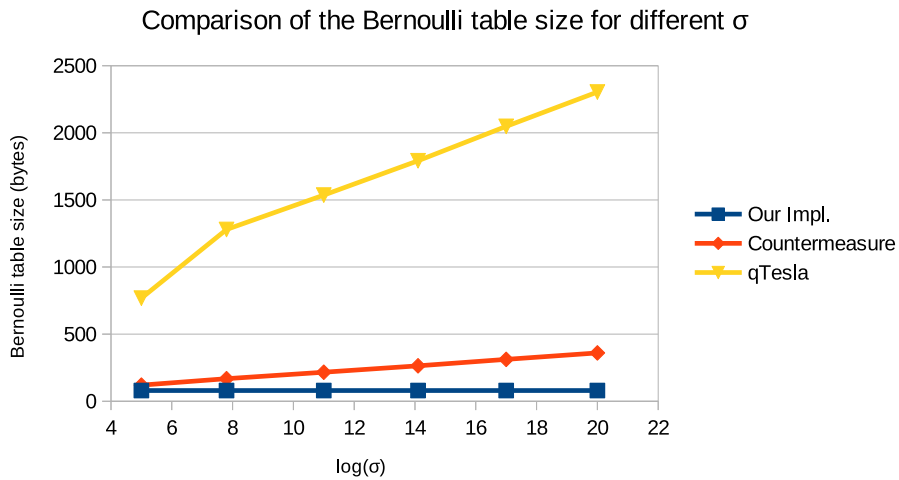
- Use a polynomial to estimate $\exp(x)$ with sufficient precision instead:
  1. Let $t = y(y + 2kx)$. Because $\sigma_0 = \sqrt{1/(2 \ln 2)}$ and $\sigma = k\sigma_0$, we rewrite the Bernoulli bias p as:

$$p = \exp\left(-t/2\sigma^2\right) = \exp\left(-\ln 2 \cdot t/k^2\right) = 2^{-t/k^2}.$$

  2. We adapt the techniques from [MBdD+10] to estimate $2^{-t/k^2}$:
     1. $2^{-t/k^2} = 2^{\lfloor -t/k^2 \rfloor + a} = 2^{\lfloor -t/k^2 \rfloor} \cdot 2^a$, $0 \leq a < 1$.
     2. Change the exponent of a double precision variable to get $2^{\lfloor -t/k^2 \rfloor}$.
     3. Use the Sollya tool [CJL10] to find a polynomial with sufficient precision for evaluating 2^a.

Efficiency Comparison





- $\lambda = 128,\ m = 1024,\ q_s = 2^{64}$.
- Use hardware AES-NI PRNG.

Nina Bindel, Sedat Akleylek, Erdem Alkim, Paulo S. L. M. Barreto, Johannes Buchmann, Edward Eaton, Gus Gutoski, Juliane Kramer, Patrick Longa, Harun Polat, Jefferson E. Ricardini, and Gustavo Zanon.
Submission to NIST's post-quantum project: lattice-based digital signature scheme qTESLA.
https://qtesla.org/, 2017.
Accessed: 2018-11-03.

Jonathan Bootle, Claire Delaplace, Thomas Espitau, Pierre-Alain Fouque, and Mehdi Tibouchi.
LWE without modular reduction and improved side-channel attacks against BLISS.
In *ASIACRYPT (1)*, volume 11272 of *Lecture Notes in Computer Science*, pages 494–524. Springer, 2018.

Leon Groot Bruinderink, Andreas Hülsing, Tanja Lange, and Yuval Yarom.
Flush, gauss, and reload - A cache attack on the BLISS lattice-based signature scheme.
In *CHES*, volume 9813 of *Lecture Notes in Computer Science*, pages 323–345. Springer, 2016.

Sylvain Chevillard, Mioara Joldes, and Christoph Quirin Lauter.
Sollya: An environment for the development of numerical codes.
In *ICMS*, volume 6327 of *Lecture Notes in Computer Science*, pages 28–31. Springer, 2010.

Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky.
Lattice signatures and bimodal gaussians.
In *CRYPTO (1)*, volume 8042 of *Lecture Notes in Computer Science*, pages 40–56. Springer, 2013.

Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi.
Side-channel attacks on BLISS lattice-based signatures: Exploiting branch tracing against strongswan and electromagnetic emanations in microcontrollers.
In *CCS*, pages 1857–1874. ACM, 2017.

Jean-Michel Muller, Nicolas Brisebarre, Florent de Dinechin, Claude-Pierre Jeannerod, Vincent Lefèvre, Guillaume Melquiond, Nathalie Revol, Damien Stehlé, and Serge Torres.
Handbook of Floating-Point Arithmetic.
Birkhäuser, 2010.

Peter Pessl, Leon Groot Bruinderink, and Yuval Yarom.
To BLISS-B or not to be: Attacking strongswan's implementation of post-quantum signatures.
In *CCS*, pages 1843–1855. ACM, 2017.

Thomas Prest.
Sharper bounds in lattice-based cryptography using the rényi divergence.
In *ASIACRYPT (1)*, volume 10624 of *Lecture Notes in Computer Science*, pages 347–374. Springer, 2017.