

Isochronous Gaussian Sampling: From Inception to Implementation

With Applications to the Falcon Signature Scheme

James Howe¹, Thomas Prest¹, Thomas Ricosset², and Mélissa Rossi^{2,3,4,5}

¹ PQShield, Oxford, UK

`james.howe@pqshield.com` `thomas.prest@pqshield.com`

² Thales, Gennevilliers, France

`thomas.ricosset@thalesgroup.com`

³ ANSSI, Paris, France

⁴ École normale supérieure, CNRS, PSL University, Paris, France

⁵ Inria, Paris, France

`melissa.rossi@ens.fr`

Abstract Gaussian sampling over the integers is a crucial tool in lattice-based cryptography, but has proven over the recent years to be surprisingly challenging to perform in a generic, efficient and provable secure manner. In this work, we present a modular framework for generating discrete Gaussians with arbitrary center and standard deviation. Our framework is extremely simple, and it is precisely this simplicity that allowed us to make it easy to implement, provably secure, portable, efficient, and provably resistant against timing attacks. Our sampler is a good candidate for any trapdoor sampling and it is actually the one that has been recently implemented in the Falcon signature scheme. Our second contribution aims at systematizing the detection of implementation errors in Gaussian samplers. We provide a statistical testing suite for discrete Gaussians called SAGA (Statistically Acceptable GAussian). In a nutshell, our two contributions take a step towards trustable and robust Gaussian sampling real-world implementations.

Keywords.

Lattice based cryptography, Gaussian Sampling, Isochrony, Statistical verification tools

1 Introduction

Gaussian sampling over the integers is a central building block of lattice-based cryptography, in theory as well as in practice. It is also notoriously difficult to perform efficiently and securely, as illustrated by numerous side-channel attacks exploiting BLISS' Gaussian sampler [9,23,54,61]. For this reason, some schemes limit or proscribe the use of Gaussians [6,40]. However, in some situations, Gaussians are unavoidable. The most prominent example is trapdoor sampling [30,53,45]: performing it with other distributions is an open question, except in limited cases [41] which entail a growth $O(\sqrt{n})$ to $O(n)$ of the output, resulting in dwindling security levels. Given the countless applications of trapdoor sampling (full-domain hash signatures [30,58], identity-based encryption (or IBE) [30,20], hierarchical IBE [11,1], etc.), it is important to come up with Gaussian samplers over the integers which are not only efficient, but also provably secure, resistant to timing attacks, and in general easy to deploy.

Our first contribution is to propose a Gaussian sampler over the integers with all the properties which are expected of a sampler for widespread deployment. It is simple and modular, making analysis and subsequent improvements easy. It is efficient and portable, making it amenable to a variety of scenarios. Finally, we formally prove its security and resistance against timing attacks. We detail below different aspects of our sampler:

- **Simplicity and Modularity.** At a high level, our framework only requires two ingredients (a base sampler and a rejection sampler) and combines them in a simple and black-box way. Not only does it make the description of our sampler modular (as one can replace any of the ingredients), this simplicity and modularity also infuses all aspects of its analysis.
- **Genericity.** Our sampler is fully generic as it works with arbitrary center μ and standard deviation σ . In addition, it does not incur hidden precomputation costs: given a fixed base sampler of parameter σ_{\max} , our framework allows to sample from $D_{\mathbb{Z},\sigma,\mu}$ for any $\eta_\epsilon(\mathbb{Z}^n) \leq \sigma \leq \sigma_{\max}$. In comparison, [47] implicitly requires a different base sampler for each different value of σ ; this limits its applicability for use cases such as Falcon [58], which has up to 2048 different σ 's, all computed at key generation.
- **Efficiency and Portability.** Our sampler is instantiated with competitive parameters which make it very efficient in time and memory usage. For $\sigma_{\max} = 1.8205$ and SHAKE256 used as PRNG, our sampler uses only 512 bytes of memory and achieved 1,848,428 samples per second on an Intel i7-6500U clocked at 2.5 GHz. Moreover, our sampler can be instantiated in a way that uses only integer operations, making it highly portable.
- **Provable Security.** A security analysis based on the statistical distance would either provide very weak security guarantees or require to increase the running time by an order of magnitude. We instead rely on the Rényi divergence, a tool which in the recent years has allowed dramatic efficiency gains for lattice-based schemes [3,57]. We carefully selected our parameters as to make them as amenable to a Rényi divergence-based analysis.
- **Isochrony.** We formally show that our sampler is isochronous: its running time is independent of the inputs σ, μ and of the output z . Isochrony is weaker than being constant-time, but it nevertheless suffices to argue security against timing attacks. Interestingly, our proof of isochrony relies on techniques and notions that are common in lattice-based cryptography: the smoothing parameter, the Rényi divergence, etc. In particular, the isochrony of our sampler is implied by parameters dictated by the current state of the art for *black-box* security of lattice-based schemes.

One second contribution stems from a simple observation: implementations of otherwise perfectly secure schemes have failed in spectacular ways by introducing weaknesses, a common one being randomness failure: this is epitomized by nonce reuses in ECDSA, leading to jailbreaking Sony PS3 consoles¹ and exposing Bitcoin wallets [8]. The post-quantum community is aware of this point of failure but does not seem to have converged on a systematic way to mitigate it [51]. Randomness failures have been manually discovered and fixed in implementations of Dilithium [50], Falcon [56,52] and other schemes; the case of Falcon is particularly relevant to us because the sampler implemented was the one described in this document!

Our second contribution is a first step at systematically detecting such failures: we propose a statistical test suite called **SAGA** for validating discrete Gaussians. This test suite can check univariate samples; we therefore use it to validate our own implementation of our sampler. In addition, our test suite can check multivariate Gaussians as well; this enables validation at a higher level: if the base sampler over the integers is validated, but the output of the high-level scheme does not behave like a multivariate Gaussian even though the theory predicts it should, then this is indicative of an implementation mistake somewhere else in the implementation (or, at the worst case, that the theory is deficient). We illustrate that with a simple example of a (purportedly) deficient implementation of Falcon [58], however it can be used for any other scheme sampling multivariate discrete Gaussians, including but not limited to [45,20,29,5,12]. The test suite is publicly available at: <https://github.com/PQShield/SAGA>.

¹ https://media.ccc.de/v/27c3-4087-en-console_hacking_2010.

2 Related Works

In the recent years, there has been a surge of works related to Gaussian sampling over the integers. Building on convolution techniques from [55], [47] proposed an arbitrary-center Gaussian sampler base, as well as a statistical tool (the max-log distance) to analyse it. [3,57,44] revisited classical techniques with the Rényi divergence. Polynomial-based methods were further studied by [57,65,4]. The use of rounded Gaussians was proposed in [34]. Knuth-Yao's DDG trees have been considered in [22,35].² Lazy floating-point precision was studied in [21,18]. We note that techniques dating back to von Neumann [62] allow to generate (continuous) Gaussians elegantly using finite automata [27,2,36]. While these have been considered in the context of lattice-based cryptography [19,17] they are also notoriously hard to make isochronous. Finally, [63] studied previously cited techniques with the goal of minimizing their relative error.

3 Preliminaries

3.1 Gaussians

For $\sigma, \mu \in \mathbb{R}$ with $\sigma > 0$, we call Gaussian function of parameters σ, μ and denote by $\rho_{\sigma, \mu}$ the function defined over \mathbb{R} as $\rho_{\sigma, \mu}(x) = \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$. Note that when $\mu = 0$ we omit it in index notation, e.g. $\rho_{\sigma}(x) = \rho_{\sigma, 0}(x)$. The parameter σ (resp. μ) is often called the standard deviation (resp. center) of the Gaussian. In addition, for any countable set $S \subseteq \mathbb{R}$ we abusively denote by $\rho_{\sigma, \mu}(S)$ the sum $\sum_{z \in S} \rho_{\sigma, \mu}(z)$. When $\sum_{z \in S} \rho_{\sigma, \mu}(z)$ is finite, we denote by $D_{S, \sigma, \mu}$ and call Gaussian distribution of parameters σ, μ the distribution over S defined by $D_{S, \sigma, \mu}(z) = \rho_{\sigma, \mu}(z) / \rho_{\sigma, \mu}(S)$. Here too, when $\mu = 0$ we omit it in index notation, e.g. $D_{S, \sigma, \mu}(z) = D_{S, \sigma}(z)$. We use the notation \mathcal{B}_p to denote the Bernoulli distribution of parameter p .

3.2 Rényi Divergence

We recall the definition of the Rényi divergence, which we will use massively in our security proofs.

Definition 1 (Rényi Divergence). *Let \mathcal{P}, \mathcal{Q} be two distributions such that $\text{Supp}(\mathcal{P}) \subseteq \text{Supp}(\mathcal{Q})$. For $a \in (1, +\infty)$, we define the Rényi divergence of order a by*

$$R_a(\mathcal{P}, \mathcal{Q}) = \left(\sum_{x \in \text{Supp}(\mathcal{P})} \frac{\mathcal{P}(x)^a}{\mathcal{Q}(x)^{a-1}} \right)^{\frac{1}{a-1}}.$$

In addition, we define the Rényi divergence of order $+\infty$ by

$$R_{\infty}(\mathcal{P}, \mathcal{Q}) = \max_{x \in \text{Supp}(\mathcal{P})} \frac{\mathcal{P}(x)}{\mathcal{Q}(x)}.$$

The Rényi divergence is not a distance; for example, it is neither symmetric nor does it verify the triangle inequality, which makes it less convenient than the statistical distance. On the other hand, it does verify cryptographically useful properties, including a few listed below.

Lemma 2 ([3]). *For two distributions \mathcal{P}, \mathcal{Q} and two families of distributions $(\mathcal{P}_i)_i, (\mathcal{Q}_i)_i$, the Rényi divergence verifies these properties:*

² We note that one could use [35] to speed up our base sampler; however this results in a huge code size (more than 50kB). Since the running time of the base sampler was not a bottleneck for the usecase we considered, we instead relied on a straightforward, slightly less efficient CDT-based method.

- **Data processing inequality.** For any function f , $R_a(f(\mathcal{P}), f(\mathcal{Q})) \leq R_a(\mathcal{P}, \mathcal{Q})$ where the distribution $f(\mathcal{P})$ (resp. $f(\mathcal{Q})$) is obtained by applying f to $x \leftarrow \mathcal{P}$ (resp. $x \leftarrow \mathcal{Q}$).
- **Multiplicativity.** Assume that \mathcal{P} and \mathcal{Q} are the joint distribution of a pair of random variables (x_1, x_2) . Assume also that x_1 and x_2 are independent. We then denote $\mathcal{P}(x_1, x_2) := \mathcal{P}_1(x_1) \cdot \mathcal{P}_2(x_2)$ and $\mathcal{Q}(x_1, x_2) := \mathcal{Q}_1(x_1) \cdot \mathcal{Q}_2(x_2)$. Then, $R_a(\mathcal{P}, \mathcal{Q}) = R_a(\mathcal{P}_1, \mathcal{Q}_1) \cdot R_a(\mathcal{P}_2, \mathcal{Q}_2)$.
- **Probability preservation.** For any event $E \subseteq \text{Supp}(\mathcal{Q})$ and $a \in (1, +\infty)$,

$$\mathcal{Q}(E) \geq \mathcal{P}(E)^{\frac{a}{a-1}} / R_a(\mathcal{P}, \mathcal{Q}), \quad (1)$$

$$\mathcal{Q}(E) \geq \mathcal{P}(E) / R_\infty(\mathcal{P}, \mathcal{Q}). \quad (2)$$

The following lemma shows that a bound of δ on the relative error between two distributions implies a bound $O(a\delta^2)$ on the log of the Rényi divergence (as opposed to a bound $O(\delta)$ on the statistical distance).

Lemma 3 (Lemma 3 of [57]). Let \mathcal{P}, \mathcal{Q} be two distributions of same support Ω . Suppose that the relative error between \mathcal{P} and \mathcal{Q} is bounded: $\exists \delta > 0$ such that $|\frac{\mathcal{P}}{\mathcal{Q}} - 1| \leq \delta$ over Ω . Then, for $a \in (1, +\infty)$:

$$R_a(\mathcal{P}, \mathcal{Q}) \leq \left(1 + \frac{a(a-1)\delta^2}{2(1-\delta)^{a+1}}\right)^{\frac{1}{a-1}} \underset{\delta \rightarrow 0}{\sim} 1 + \frac{a\delta^2}{2}$$

In some cases, the queries to the distributions are not independent³, thus, one cannot apply the multiplicativity directly in our proofs. To handle these dependencies, we introduce the following proposition.

Proposition 4. Let \mathcal{P} and \mathcal{Q} denote two distributions of a N -uple of random variables $(x_i)_{i < N}$. For $0 \leq i < N$, assume \mathcal{P}_i (resp \mathcal{Q}_i) is the marginal distribution of X_i , and let $\mathcal{P}_{i|<i}(\cdot|x_{<i})$ denote the conditional distribution of x_i given that $(x_0, \dots, x_{i-1}) = x_{<i}$. Let $a > 1$. Suppose that for all $0 \leq i < N$, there exists $r_{a,i} \geq 1$ such that for all i -uple $x_{<i}$ in the support of \mathcal{Q} restricted to its first i variables,

$$R_a(\mathcal{Q}_{i|x_{<i}}, \mathcal{P}_{i|x_{<i}}) \leq r_{a,i}. \quad (3)$$

Then:

$$R_a(\mathcal{Q}, \mathcal{P}) \leq \prod_{i < N} r_{a,i}. \quad (4)$$

Proof. We prove the result in the case $N = 2$, the general case then follows by induction. We have:

$$R_a(\mathcal{Q}, \mathcal{P})^{a-1} = \sum_{x_1, x_2} \frac{(\mathcal{Q}_1(x_1) \cdot \mathcal{Q}_{2|1}(x_2|x_1))^a}{(\mathcal{P}_1(x_1) \cdot \mathcal{P}_{2|1}(x_2|x_1))^{a-1}} \quad (5)$$

$$= \sum_{x_1} \frac{\mathcal{Q}_1(x_1)^a}{\mathcal{P}_1(x_1)^{a-1}} \cdot \left(\underbrace{R_a(\mathcal{Q}_{2|1}(\cdot|x_1), \mathcal{P}_{2|1}(\cdot|x_1))}_{\leq r_{a,2}} \right)^{a-1} \quad (6)$$

$$\leq (r_{a,1} \cdot r_{a,2})^{a-1} \quad (7)$$

This concludes the proof. \square

³ We thank Damien Stehlé for pointing that out.

3.3 Smoothing Parameter

For $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\Lambda)$ of a lattice Λ is the smallest value $\sigma > 0$ such that $\rho_{\frac{1}{\sigma\sqrt{2\pi}}}(\Lambda^* \setminus \{\mathbf{0}\}) \leq \epsilon$, where Λ^* denotes the dual of Λ . In the literature, some definitions of the smoothing parameter scale our definition by a factor $\sqrt{2\pi}$. It is shown in [46] that $\eta_\epsilon(\mathbb{Z}^n) \leq \eta_\epsilon^+(\mathbb{Z}^n)$, where:

$$\eta_\epsilon^+(\mathbb{Z}^n) = \frac{1}{\pi} \sqrt{\frac{1}{2} \log \left(2n \left(1 + \frac{1}{\epsilon} \right) \right)}. \quad (8)$$

3.4 Isochronous algorithms

We now give a semi-formal definition of isochronous algorithms.

Definition 5. Let \mathcal{A} be a (probabilistic or deterministic) algorithm with set of input variables \mathcal{I} , set of output variables \mathcal{O} , and let $\mathcal{S} \subseteq \mathcal{I} \cup \mathcal{O}$ be the set of sensitive variables. We say that \mathcal{A} is perfectly isochronous with respect to \mathcal{S} if its running time is independent of any variable in \mathcal{S} .

In addition, we say that \mathcal{A} statistically isochronous with respect to \mathcal{S} if there exists a distribution \mathcal{D} independent of all the variables in \mathcal{S} , such that the running time of \mathcal{A} is statistically close (for a clearly identified divergence) to \mathcal{D} .

We note that we can define a notion of computationally isochronous algorithm. For such an algorithm, it is computationally hard to recover the sensitive variables even given the distribution of the running time of the algorithm. We can even come up with a contrived example of such an algorithm: let $\mathcal{A}()$ select in an isochronous manner an x uniformly in a space of min-entropy $\geq \lambda$, compute $y = H(x)$ and wait a time y before outputting x . One can show that recovering x given the running time of \mathcal{A} is hard if H is a one-way function.

4 The sampler

In this section, we describe our new sampler with arbitrary standard deviation and center. The main assumption of our setting is to consider that all the standard deviations are bounded and that the center is in $[0, 1]$. In other words, denoting the upper bound and lower bound on the standard deviation as $\sigma_{\max} > \sigma_{\min} > 0$, we present an algorithm that samples the distribution $D_{\mathbb{Z}, \sigma, \mu}$ for any $\mu \in [0, 1]$ and $\sigma_{\min} \leq \sigma \leq \sigma_{\max}$.

Our sampling algorithm is called **SamplerZ** and is described in Algorithm 1. We denote by **BaseSampler** an algorithm that samples an element with the fixed half Gaussian distribution $D_{\mathbb{Z}^+, \sigma_{\max}}$. The first step consists in using **BaseSampler**. The obtained z_0 sample is then transformed into $z := (2b - 1) \cdot z_0 + b$ where b is a bit drawn uniformly in $\{0, 1\}$. Let us denote by $BG_{\sigma_{\max}}$ the distribution of z . The distribution of z is a discrete bimodal half-Gaussian of centers 0 and 1. More formally,

$$BG_{\sigma_{\max}}(z) = \frac{1}{2} \begin{cases} D_{\mathbb{Z}^+, \sigma_{\max}}(-z) & \text{if } z \leq 0 \\ D_{\mathbb{Z}^+, \sigma_{\max}}(z - 1) & \text{if } z \geq 1. \end{cases} \quad (9)$$

Then, to recover the desired distribution $D_{\mathbb{Z}, \sigma, \mu}$ for the inputs (σ, μ) , one might want to apply the classical rejection sampling technique applied to lattice based schemes [39] and accept z with

Algorithm 1 SamplerZ(σ, μ)

Require: $\mu \in [0, 1], \sigma \leq \sigma_{\max}$
Ensure: $z \sim D_{\mathbb{Z}, \sigma, \mu}$

- 1: **while** True **do**
- 2: $z_0 \leftarrow \text{BaseSampler}()$
- 3: $b \leftarrow \{0, 1\}$ uniformly
- 4: $z := (2b - 1) \cdot z_0 + b$
- 5: $x := \frac{z_0^2}{2\sigma_{\max}^2} - \frac{(z - \mu)^2}{2\sigma^2}$
- 6: **if** AcceptSample(σ, x) **then**
- 7: **return** z

Algorithm 2 AcceptSample(σ, x)

Require: $\sigma_{\min} \leq \sigma \leq \sigma_{\max}, x < 0$
Ensure: $b \sim \mathcal{B}_{\frac{\sigma_{\min}}{\sigma} \cdot \exp(x)}$

- 1: $p := \frac{\sigma_{\min}}{\sigma} \cdot \text{ApproxExp}(x)$
Lazy Bernoulli sampling
- 2: $i := 1$
- 3: **do**
- 4: $i := i \cdot 2^8$
- 5: $u \leftarrow \llbracket 0, 2^8 - 1 \rrbracket$ uniformly
- 6: $v := \lfloor p \cdot i \rfloor$ & **0xff**
- 7: **while** $u = v$
- 8: **return** ($u < v$)

probability

$$\begin{aligned} \frac{D_{\mathbb{Z}, \sigma, \mu}(z)}{BG_{\sigma_{\max}}(z)} &= \begin{cases} \exp\left(\frac{z^2}{2\sigma_{\max}^2} - \frac{(z - \mu)^2}{2\sigma^2}\right) & \text{if } z \leq 0 \\ \exp\left(\frac{(z-1)^2}{2\sigma_{\max}^2} - \frac{(z - \mu)^2}{2\sigma^2}\right) & \text{if } z \geq 1 \end{cases} \\ &= \exp\left(\frac{z_0^2}{2\sigma_{\max}^2} - \frac{(z - \mu)^2}{2\sigma^2}\right). \end{aligned}$$

The element inside the exp is computed in step 5. Next, we also introduce an algorithm denoted AcceptSample. The latter performs the rejection sampling (Algorithm 2): using ApproxExp an algorithm that returns $\exp(\cdot)$, it returns a Bernoulli sample with the according probability. Actually, for isochrony matters, detailed in Section 6, the latter acceptance probability is rescaled by a factor $\frac{\sigma_{\min}}{\sigma}$. As z follows the $BG_{\sigma_{\max}}$ distribution, after the rejection sampling, the final distribution of SamplerZ(σ, μ) is then proportional to $\frac{\sigma_{\min}}{\sigma} \cdot D_{\mathbb{Z}, \sigma, \mu}$ which is, after normalization exactly equal to $D_{\mathbb{Z}, \sigma, \mu}$. Thus, with this construction, one can derive the following proposition.

Proposition 6 (Correctness). *Assume that all the uniform distributions are perfect and that BaseSampler = $D_{\mathbb{Z}^+, \sigma_{\max}}$ and ApproxExp = exp, then the construction of SamplerZ (in Algorithms 1 and 2) is such that SamplerZ(σ, μ) = $D_{\mathbb{Z}, \sigma, \mu}$.*

In practical implementations, one cannot achieve perfect distributions. Only achieving BaseSampler $\approx D_{\mathbb{Z}^+, \sigma_{\max}}$ and ApproxExp $\approx \exp$ is possible. Section 6 proves that, under certain conditions on BaseSampler and ApproxExp and on the number of sampling queries, the final distribution remains indistinguishable from $D_{\mathbb{Z}, \sigma, \mu}$.

5 Proof of Security

Table 1 gives the notations for the number of calls to SamplerZ, BaseSampler and ApproxExp and the considered values when the sampler is instantiated for Falcon. Due to the rejection sampling in step 6, there will be a (potentially infinite) number of iterations of the **while** loop. We will show later in Lemma 8, that the number of iterations follows a geometric law of parameter $\approx \frac{\sigma_{\min} \cdot \sqrt{2\pi}}{2 \cdot \rho_{\sigma_{\max}}(\mathbb{Z}^+)}$. We note $\mathcal{N}_{\text{iter}}$ a heuristic considered maximum number of iterations. By a central limit argument, $\mathcal{N}_{\text{iter}}$ will only be marginally higher than the expected number of iterations. To instantiate the values $Q_{\text{exp}} = Q_{\text{bs}} = \mathcal{N}_{\text{iter}} \cdot Q_{\text{samplerZ}}$ for the example of Falcon, we take $\mathcal{N}_{\text{iter}} = 2$. In fact, $\frac{\sigma_{\min} \cdot \sqrt{2\pi}}{2 \cdot \rho_{\sigma_{\max}}(\mathbb{Z}^+)} \leq 2$ for Falcon's parameters.

Table 1: Number of calls to `SamplerZ`, `BaseSampler` and `ApproxExp`

	Notation	Value for Falcon
Calls to sign (as per NIST)	Q_s	$\leq 2^{64}$
Calls to <code>SamplerZ</code>	Q_{samplerZ}	$Q_s \cdot 2 \cdot n \leq 2^{75}$
Calls to <code>BaseSampler</code>	Q_{bs}	$\mathcal{N}_{\text{iter}} \cdot Q_{\text{samplerZ}} \leq 2^{76}$
Calls to <code>ApproxExp</code>	Q_{exp}	$Q_{\text{bs}} \leq 2^{76}$

The following Theorem estimates the security of `SamplerZ`, it is independent of the chosen values for the number of calls.

Theorem 7 (Security of `SamplerZ`). *Consider a cryptosystem, denoted C_{ideal} that makes at most Q_s **independent** queries to $D_{\mathbb{Z},\sigma,\mu}$. Assume that C_{ideal} is λ -bit secure against a search problem. Let us consider a copy of the latter cryptosystem, denoted C_{real} , where the only differences are that `SamplerZ`(σ, μ) instead of $D_{\mathbb{Z},\sigma,\mu}$. If the two following conditions are respected;*

$$\forall x < 0, \max \left(\left| \frac{\text{ApproxExp}(x) - \exp(x)}{\exp(x)} \right|, \left| \frac{\text{ApproxExp}(x) - \exp(x)}{1 - \exp(x)} \right| \right) \leq \frac{1}{\sqrt{2 \cdot (2 \cdot \lambda - 1) \cdot Q_{\text{exp}}}} \quad (\text{Cond. (1)})$$

$$R_{2 \cdot \lambda_{\text{REAL}} + 1}(\text{BaseSampler}, D_{\mathbb{Z}^+, \sigma_{\text{max}}}) \leq 1 + \frac{1}{4 \cdot Q_{\text{bs}}} \quad (\text{Cond. (2)})$$

then, C_{real} is $(\lambda - 2)$ -bit secure against the search problem.

The proof of this Theorem is given in Appendix A.

To get concrete numerical values, we assume that 256 bits are claimed on the original scheme, thus 254 bits of security are claimed for the real implementation. Then for an implementation of `Falcon`, the numerical values are

$$\frac{1}{\sqrt{2 \cdot (2 \cdot \lambda + 1) \cdot Q_{\text{exp}}}} \approx 2^{-43} \quad \text{and} \quad \frac{1}{4 \cdot Q_{\text{bs}}} \approx 2^{-78}.$$

5.1 Instanciating the `ApproxExp`

To achieve condition (1) with `ApproxExp`, we use a polynomial approximation of the exponential on $[-\ln(2), 0]$. In fact, one can reduce the parameter x modulo $\ln(2)$ such that $x = -r - s \ln(2)$. Compute the exponential remains to compute $\exp(x) = 2^{-s} \exp(-r)$. Noting that $s \geq 64$ happen very rarely, thus s can be saturated at 63 to avoid overflow without loss in precision.

We use the polynomial approximation tool provided in GALACTICS [4]. This tool generates polynomial approximations that allow a computation in fixed precision with chosen size of coefficients and degree. As an example, for 32-bit coefficients and a degree 10, we obtain a polynomial

$$P_{\text{gal}}(x) := \sum_{i=0}^{10} a_i \cdot x^i, \text{ with:}$$

$$\begin{aligned} \circ a_0 &= 1; & \circ a_6 &= 3127580083557 \cdot 2^{-51}; \\ \circ a_1 &= 1; & \circ a_7 &= 28579833423385 \cdot 2^{-57}; \\ \circ a_2 &= 2^{-1}; & \circ a_8 &= 14399595757739 \cdot 2^{-59}; \\ \circ a_3 &= 11728124023891 \cdot 2^{-46}; & \circ a_9 &= 23649690795601 \cdot 2^{-63}; \\ \circ a_4 &= 23456248667481 \cdot 2^{-49}; & \circ a_{10} &= 28643805083125 \cdot 2^{-66}; \\ \circ a_5 &= 18764980474255 \cdot 2^{-51}; & & \end{aligned}$$

For any $x \in [-\ln(2), 0]$, P_{gal} verifies $\left| \frac{P_{\text{gal}}(x) - \exp(x)}{\exp(x)} \right| \leq 2^{-47}$, which is sufficient to verify condition (1) for `Falcon` implementation. In addition, we experimentally check that P_{gal} verifies

$$\left| \frac{P_{\text{gal}}(x) - \exp(x)}{1 - \exp(x)} \right| \leq 2^{-45}$$

Algorithm 3 SampleCDT: full-table access CDT

```

 $z \leftarrow 0$ 
 $u \leftarrow [0, 1)$  uniformly with  $\theta$  bits of absolute precision
for  $0 \leq i \leq w$  do
     $b \leftarrow (\text{CDT}[w] \geq u)$   $\triangleright b = 1$  if it is true and 0 otherwise
     $z \leftarrow z + b$ 
return  $z$ 

```

Flexibility on the implementation of the polynomial. Depending on the platform and the requirement for the signature, one can adapt the polynomial to fit their constraints. For example, if one wants to minimize the number of multiplications, implementing the polynomial with Horner’s form is the best option. The polynomial is written in the following form :

$$P_{\text{gal}}(x) = a_0 + x(a_1 + x(a_2 + x(a_3 + x(a_4 + x(a_5 + x(a_6 + x(a_7 + x(a_8 + x(a_9 + xa_{10})))))))))).$$

Evaluating P_{gal} is then done serially as follows:

$$\begin{aligned}
 \mathbf{y} &\leftarrow \mathbf{a}_{10} \\
 \mathbf{y} &\leftarrow \mathbf{a}_9 + \mathbf{y} \times \mathbf{x} \\
 &\vdots \\
 \mathbf{y} &\leftarrow \mathbf{a}_1 + \mathbf{y} \times \mathbf{x} \\
 \mathbf{y} &\leftarrow \mathbf{a}_0 + \mathbf{y} \times \mathbf{x}
 \end{aligned}$$

Some architectures enjoy some level of parallelism, in which case it is desirable to minimise the depth of the circuit computing the polynomial⁴. Writing P_{gal} in Estrin’s form [24] is helpful in this regard.

$$\begin{aligned}
 \mathbf{x}_2 &\leftarrow \mathbf{x} \times \mathbf{x} \\
 \mathbf{x}_4 &\leftarrow \mathbf{x}_2 \times \mathbf{x}_2 \\
 P_{\text{gal}}(\mathbf{x}) &\leftarrow (\mathbf{x}_4 \times \mathbf{x}_4) \times ((\mathbf{a}_8 + \mathbf{a}_9 \times \mathbf{x}) + \mathbf{x}_2 \times \mathbf{a}_{10}) \\
 &\quad + (((\mathbf{a}_0 + \mathbf{a}_1 \times \mathbf{x}) + \mathbf{x}_2 \times (\mathbf{a}_2 + \mathbf{a}_3 \times \mathbf{x})) + \mathbf{x}_4 \times ((\mathbf{a}_4 + \mathbf{a}_5 \times \mathbf{x}) + \mathbf{x}_2 \times (\mathbf{a}_6 + \mathbf{a}_7 \times \mathbf{x})))
 \end{aligned}$$

5.2 Instanciating the BaseSampler

To achieve condition (2) with **BaseSampler**, we rely on a cumulative distribution table (CDT). We precompute a table of the cumulative distribution function of $D_{\mathbb{Z}^+, \sigma_{\text{max}}}$ with a certain precision; then, to produce a sample, we generate a random value in $[0, 1]$ with the same precision, and return the index of the last entry in the table that is greater than that value. In variable time, the sampling can be done rather efficiently with a binary search, but a constant-time implementation has essentially no choice but to read the entire table each time and carry out each comparison. This process is summed up in Algorithm 3. The parameters w and θ are respectively the number of elements of the CDT and the precision of its coefficients. Let $a = 2 \cdot \lambda_{\text{REAL}} + 1$. To derive the parameters w and θ we use a simple script that, given σ_{max} and θ as inputs:

1. Computes the smallest tailcut w such that the Renyi divergence R_a between the ideal distribution $D_{\mathbb{Z}^+, \sigma_{\text{max}}}$ and its restriction to $\{0, \dots, w\}$ (noted $D_{[w], \sigma_{\text{max}}}$) verifies $R_a(D_{[w], \sigma_{\text{max}}}, D_{\mathbb{Z}^+, \sigma_{\text{max}}}) \leq 1 + 1/(4Q_{\text{bs}})$;
2. Rounds the probability density table (PDT) of $D_{[w], \sigma_{\text{max}}}$ with θ bits of absolute precision. This rounding is done “cleverly” by truncating all the PDT values except the largest:
 - for $z \geq 1$, the value $D_{[w], \sigma_{\text{max}}}(z)$ is truncated: $PDT(z) = 2^{-\theta} \lfloor 2^\theta D_{[w], \sigma_{\text{max}}}(z) \rfloor$.

⁴ We are thankful to Thomas Pornin for bringing up this fact.

- in order to have a probability distribution, $PDT(0) = 1 - \sum_{z \geq 1} PDT(z)$.
- 3. Derives the CDT from the PDT and computes the final $R_a(\text{SampleCDT}_{w=19, \theta=72}, D_{\mathbb{Z}^+, \sigma_{\max}})$.

Taking $\sigma_{\max} = 1.8205$ and $\theta = 72$ as inputs, we found $w = 19$.

- | | |
|--|--|
| ◦ $PDT(0) = 2^{-72} \times 1697680241746640300030$ | ◦ $PDT(10) = 2^{-72} \times 476288472308334$ |
| ◦ $PDT(1) = 2^{-72} \times 1459943456642912959616$ | ◦ $PDT(11) = 2^{-72} \times 20042553305308$ |
| ◦ $PDT(2) = 2^{-72} \times 928488355018011056515$ | ◦ $PDT(12) = 2^{-72} \times 623729532807$ |
| ◦ $PDT(3) = 2^{-72} \times 436693944817054414619$ | ◦ $PDT(13) = 2^{-72} \times 14354889437$ |
| ◦ $PDT(4) = 2^{-72} \times 151893140790369201013$ | ◦ $PDT(14) = 2^{-72} \times 244322621$ |
| ◦ $PDT(5) = 2^{-72} \times 39071441848292237840$ | ◦ $PDT(15) = 2^{-72} \times 3075302$ |
| ◦ $PDT(6) = 2^{-72} \times 7432604049020375675$ | ◦ $PDT(16) = 2^{-72} \times 28626$ |
| ◦ $PDT(7) = 2^{-72} \times 1045641569992574730$ | ◦ $PDT(17) = 2^{-72} \times 197$ |
| ◦ $PDT(8) = 2^{-72} \times 108788995549429682$ | ◦ $PDT(18) = 2^{-72} \times 1$ |
| ◦ $PDT(9) = 2^{-72} \times 8370422445201343$ | |

Our experiment showed that for any $a \geq 509$, $R_a(\text{SampleCDT}_{w=19, \theta=72}, D_{\mathbb{Z}^+, \sigma_{\max}}) \leq 1 + 2^{-80} \leq 1 + \frac{1}{4Q_{\text{bs}}}$, which validates condition (2) for Falcon implementation.

6 Analysis of resistance against timing attacks

In this section, we show that Algorithm 1 is impervious against timing attacks. We formally prove that it is isochronous with respect to σ, μ and the output z (in the sense of Definition 5). We first prove a technical lemma which shows that the number of iterations in the **while** loop of Algorithm 1 is (almost) independent of σ, μ, z .

Lemma 8. *Let $\epsilon \in (0, 1)$, $\mu \in [0, 1]$ and let $\sigma_{\min}, \sigma, \sigma_0$ be standard deviations such that $\eta_{\epsilon}^+(\mathbb{Z}^n) = \sigma_{\min} \leq \sigma \leq \sigma_0$. Let $p = \frac{\sigma_{\min} \cdot \sqrt{2\pi}}{2 \cdot \rho_{\sigma_{\max}}(\mathbb{Z}^+)}$. The number of iterations of the **while** loop in $\text{SamplerZ}(\sigma, \mu)$ follows a geometric law of parameter*

$$P_{\text{true}}(\sigma, \mu) \in p \cdot \left[1, 1 + \frac{(1 + 2^{-80})\epsilon}{n} \right].$$

The proof of Lemma 8 can be found in Appendix B.

Next, we show that Algorithm 1 is perfectly isochronous with respect to z and statistically isochronous (for the Rényi divergence) with respect to σ, μ .

Theorem 9. *Let $\epsilon \in (0, 1)$, $\mu \in \mathbb{R}$, let $\sigma_{\min}, \sigma, \sigma_0$ be standard deviations such that $\eta_{\epsilon}^+(\mathbb{Z}^n) = \sigma_{\min} \leq \sigma \leq \sigma_0$, and let $p = \frac{\sigma_{\min} \cdot \sqrt{2\pi}}{2 \cdot \rho_{\sigma_{\max}}(\mathbb{Z}^+)}$ be a constant in $(0, 1)$. Suppose that the elementary operations $\{+, -, \times, /\}$ over integer and floating-point numbers are isochronous. The running time of Algorithm 1 follows a distribution $T_{\sigma, \mu}$ such that:*

$$R_a(T_{\sigma, \mu} \| T) \lesssim 1 + \frac{a\epsilon^2 \max(1, \frac{1-p}{p})^2}{n^2(1-p)} = 1 + O\left(\frac{a\epsilon^2}{n^2}\right)$$

for some distribution T independent of its inputs σ, μ and its output z .

Finally, we leverage Theorem 9 to prove that the running time of $\text{SamplerZ}(\sigma, \mu)$ does not help an adversary to break a cryptographic scheme. We consider that the adversary has access to some function $g(\text{SamplerZ}(\sigma, \mu))$ as well as the running time of $\text{SamplerZ}(\sigma, \mu)$: this is intended to capture the fact that in practice the output of $\text{SamplerZ}(\sigma, \mu)$ is not given directly to the adversary, but processed by some function before. For example, in the signature scheme Falcon,

samples are processed by algorithms depending on the signer’s private key. On the other hand, we consider that the adversary has powerful timing attack capabilities by allowing him to learn the exact runtime of each call to `SamplerZ`(σ, μ).

Corollary 10. *Consider an adversary \mathcal{A} making Q_s signature queries against a signature algorithm that uses `SamplerZ`. Assume that \mathcal{A} breaks the security by solving a search problem with success probability $2^{-\lambda}$ for some $\lambda \geq 1$. Learning the running time of each call to `SamplerZ` does not increase the success probability of \mathcal{A} by more than a constant factor.*

The proof of Corollary 10 can be found in Appendix D. A nice thing about Corollary 10 is that the conditions required to make it effective are *already met in practice* since they are also required for black-box security of cryptographic schemes. For example, it is systematic to set $\sigma \geq \eta_\epsilon^+(\mathbb{Z}^n)$.

Impact of the scaling factor. The scaling factor $\frac{\sigma_{\min}}{\sigma} \leq \frac{\sigma_{\min}}{\sigma_{\max}}$ is crucial in making our sampler isochronous, as it decorrelates the running time $T_{\sigma,\mu}$ from σ . However, it also impacts the $T_{\sigma,\mu}$, as one can easily show that $T_{\sigma,\mu}$ is proportional to the scaling factor. It is therefore desirable to make it as small as possible. The maximal value of the scaling factor is actually dependent on the cryptographic scheme in which our sampler is used. In Appendix E, we show that for the case of the signature scheme `Falcon`, $\frac{\sigma_{\min}}{\sigma_{\max}} \leq 1.17^{-2} \approx 0.73$ and the impact of the scaling factor is limited. Moreover, one can easily show that for Peikert’s sampler [53], the scaling factor is equal to 1 and has no impact.

7 “Err on the side of Gaussian”

This section focuses on ensuring correct and verified implementations of our proposed isochronous Gaussian sampler. The motivation for this section is to minimize implementation bugs, such as implementation issues with `Falcon` [56,52] or the famous Heartbleed (CVE-2014-0160) or ROCA vulnerabilities [49] (CVE-2017-15361). We propose a test suite named `SAGA` (Statistically Acceptable GAussians) in order to verify correct univariate or multivariate Gaussian variables. At the very least, `SAGA` can act as a “sanity check” for implementers and practitioners. Furthermore, `SAGA` is designed to run in a generic fashion, agnostic to the technique used, by only requiring as input a list of univariate (i.e., outputs of `SamplerZ`) or multivariate (i.e. a set of signatures) Gaussian samples. Although we evaluate `SAGA` by applying it to `Falcon`, `SAGA` is applicable to any lattice-based cryptographic scheme requiring Gaussian sampling, such as other GPV-based signatures [5,13], `FrodoKEM` [48], identity-based encryption [20,10], and in fully homomorphic encryption [59].

7.1 Univariate tests

The statistical tests we implement here are inspired by a previous test suite proposal called `GLITCH` [33]. We use standard statistical tools to validate a Gaussian sampler is operating with the correct mean, standard deviation, skewness, and kurtosis, and finally we check whether it passes a chi-square normality test. Skewness and kurtosis are descriptors of a normal distribution that respectively measure the symmetry and peakedness of a distribution. To view the full statistical analysis of these tests we created a Python class, `UnivariateSamples`, which take as initialization arguments the expected mean (`mu`), expected standard deviation (`sigma`), and the list of observed univariate Gaussian samples (`data`). An example of how this works, as well as its output, is shown in Appendix F.1.

7.2 Multivariate tests

This section details multivariate normality tests. The motivation for these tests is to detect situations where the base Gaussian sampler over the integers is correctly implemented, yet the high-level scheme (e.g. a signature scheme) uses it incorrectly way and ends up with a defective multivariate Gaussian.

Multivariate normality. There are a number of statistical tests which evaluate the normality of multivariate distributions. We found that multivariate normality tests predominantly used in other fields [43,32,14] suffer with size and scaling issues. That is, the large sample sizes we expect to use and the poor power properties of these tests will make a type II error highly likely⁵. In fact, we implemented the Mardia [43] and Henze-Zirkler [32] tests and found, although they worked for small sample sizes, they diverged to produce false negatives for sample sizes ≥ 50 even in small dimensions $n = 64$.

However, the Doornik-Hansen test [16] minimises these issues by using transformed versions of the skewness and kurtosis of the multivariate data, increasing the test’s power. We also note that it is much faster (essentially linear in the sample size) than [43,32] (essentially quadratic in the sample size). As with the univariate tests, we created a Python class, denoted `MultivariateSamples`, which outputs four results; two based on the covariance matrix, and two based on the data’s normality. An example of how this works, as well as its output, is shown in Appendix F.2.

A glitch in the (covariance) matrix. Our second multivariate test asks the following question: *how could someone implement correctly the base sampler, yet subsequently fail to use it properly?* There is no universal answer to that, and one usually has to rely on context, experience and common sense to establish the most likely way this could happen.

For example, in `Falcon`, univariate samples are linearly combined according to node values of a balanced binary tree computed at key generation (the `Falcon` tree). If there is an implementation mistake in the procedure computing the tree (during key generation) or when combining the samples (during signing), this effectively results in nodes of the `Falcon` tree being incorrect or omitted. Such mistakes have a very recognizable effect on the empiric covariance matrix of `Falcon` signatures: they make them look like block Toeplitz matrices (Figure 1b) instead of (scaled) identity matrices in the nominal case (Figure 1a).

We devised a test which discriminates block Toeplitz covariance matrices against the ones expected from spherical Gaussians. The key idea is rather simple: when adding $O(n)$ coefficients over a (block-)subdiagonal of the empiric covariance matrix, the absolute value of the sum will grow in $O(\sqrt{n})$ if the empiric covariance matrix converges to a scaled identity matrix, and in $O(n)$ if it is block Toeplitz. We use this difference in growth to detect defective Gaussians. While we do not provide a formal proof of our test, in practice it detects reasonably well Gaussians induced by defective `Falcon` trees. We see proving our test and providing analogues for other GPV-based schemes as interesting questions.

Supplementary tests. In the case where normality has been rejected, `SAGA` also provides a number of extra tests to aid in finding the issues. More details for this can be found in Appendix F.3.

⁵ Type I and type II errors are, respectively, rejection of a true null hypothesis and the non-rejection of a false null hypothesis.

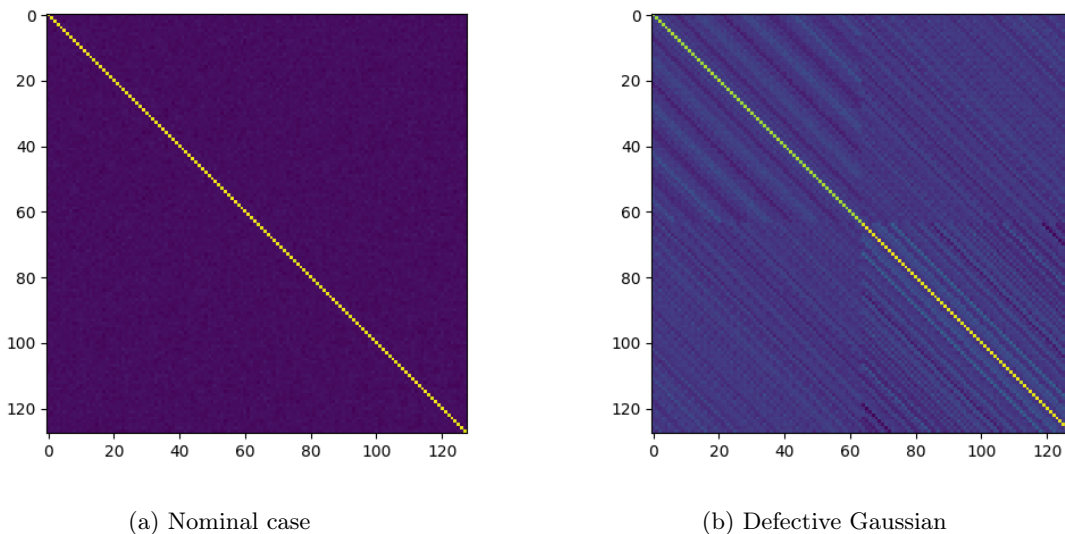


Figure 1: Empiric covariance matrices of Falcon signatures. Figure 1a corresponds to a correct implementation of Falcon. Figure 1b corresponds to an implementation where there is a mistake when constructing the Falcon tree.

Table 2: Number of samples per second at 2.5 GHz for our sampler and [64].

Algorithm	Number of samples
This work ⁶	$1.84 \times 10^6/\text{sec}$
This work (AVX2) ⁷	$7.74 \times 10^6/\text{sec}$
[64] (AVX2) ⁸	$5.43 \times 10^6/\text{sec}$

8 Application and Limitations

Our sampler has been implemented by Pornin as part of the new isochronous implementation of Falcon [56]. This implementation can use floating-point hardware or AVX2 instructions when available, but also includes floating-point emulation code that uses only usual integer operations. On ARM Cortex M4 CPUs, which can only support single-precision floating-point instructions, this implementation provides assembly implementations for the core double-precision floating-point operations more than twice faster than the generic emulation. As a result, our sampler can be efficiently implemented on embedded platforms as limited as Cortex M4 CPUs, while some other samplers (e.g. [35] due to a huge code size) are not compact enough to fit embedded platforms.

We perform benchmarks of this sampler implementation on a single Intel Core i7-6500U CPU core clocked at 2.5 GHz. In Table 2 we present the running times of our isochronous sampler. To compare with [64], we scale the numbers to be based on 2.5GHz. Note that for our sampler the number of samples per second is on average for $1.2915 < \sigma \leq 1.8502$ while for [64] $\sigma = 2$ is fixed.

In Table 3 we present the running times of the Falcon isochronous implementation [56] that contains our sampler and compare it with a second non-isochronous implementation nearly identical excepting the base sampler which is a faster lazy CDT sampler, and the rejection sam-

⁶ [56] standard double-precision floating-point (IEEE 754) with SHAKE256.

⁷ [56] AVX2 implementation with eight ChaCha20 instances in parallel (AVX2).

⁸ [64] constant-time implementation with hardware AES256 (AES-NI).

pling which is not scaled by a constant. Compared to the non-isochronous implementation, the isochronous one is about 22% slower, but remains very competitive speed-wise.

Table 3: Falcon signature generation time at 2.5 GHz.

Degree	Non-isochronous (using AVX2)	isochronous (using AVX2)
512	210.88 μ s (153.64 μ s)	257.33 μ s (180.04 μ s)
1024	418.76 μ s (311.33 μ s)	515.28 μ s (361.39 μ s)

Cache-timing protection. Following this implementation of the proposed sampler also ensures cache-timing protection [25], as the design *should*⁹ bypass conditional branches by using a consistent access pattern (using linear searching of the table) and have isochronous runtime. This has been shown to be sufficient in implementations of Gaussian samplers in Frodo [7,48].

Adapting to other schemes. A natural question is how our algorithms could be adapted for other schemes than Falcon, for example [45,20,29,5,12]. An obvious bottleneck seems to be the size of the CDT used in SampleCDT, which is linear in the standard deviation. For larger standard deviations, where linear searching becomes impractical, convolutions can be used to reduce σ , and thus the runtime of the search algorithm [55,37]. It would also be interesting to see if the DDG tree-based method of [35] has better scalability than our CDT-based method, in which case we would recommend it for larger standard deviations. On the other hand, once the base sampler is implemented, we do not see any obvious obstacle for implementing our whole framework. For example, [12] or using Peikert’s sampler [53] (in Falcon) entail a small constant number of standard deviations, therefore the rejection step would be very efficient once a base sampler for each standard deviation is implemented.

Advantages and limitations. Our sampler has an acceptance rate $\approx \frac{\sigma_{\min}}{\sigma_{\max}+0.4}$ making it especially suitable when σ_{\min} and σ_{\max} are close. In particular, our sampler is, so far, the fastest isochronous sampler for the parameters in Falcon. However, the larger the gap between σ_{\min} and σ_{\max} , the lower the acceptance rate. In addition, our sampler uses a cumulative distribution table (CDT) which is accessed in an isochronous way. This table grows when σ_{\max} grows, while making both running time and memory usage larger. When σ_{\max} is large or far from σ_{\min} , there exist faster isochronous samplers based on convolution [47] and rejection sampling [64]¹⁰ techniques.

Acknowledgements

We thank Léo Ducas and Damien Stehlé for helpful suggestions. We also thank Thomas Pornin and Mehdi Tibouchi for useful discussions. The first and second authors were supported by the project PQ Cybersecurity (Innovate UK research grant 104423). The third and fourth authors were supported by BPI-France in the context of the national project RISQ (P141580), and by the European Union PROMETHEUS project (Horizon 2020 Research and Innovation Program, grant 780701). The fourth author was also supported by ANRT under the program CIFRE N2016/1583.

⁹ Compilers may alter the design, thus one should always verify the design post-compilation.

¹⁰ The constant-time sampler in [64] may still reveal σ .

References

1. S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In Gilbert [31], pages 553–572.
2. J. Ahrens and U. Dieter. Extension of forsythe’s method for random sampling from the normal distribution. *Mathematics of computation*, 27:927–937, 1973.
3. S. Bai, A. Langlois, T. Lepoint, D. Stehlé, and R. Steinfeld. Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 3–24. Springer, Heidelberg, Nov. / Dec. 2015.
4. G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, M. Rossi, and M. Tibouchi. GALACTICS: Gaussian Sampling for Lattice-Based Constant-Time Implementation of Cryptographic Signatures, Revisited. Cryptology ePrint Archive, Report 2019/511, 2019.
5. P. Bert, P.-A. Fouque, A. Roux-Langlois, and M. Sabt. Practical implementation of ring-SIS/LWE based signature and IBE. In T. Lange and R. Steinwandt, editors, *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018*, pages 271–291. Springer, Heidelberg, 2018.
6. N. Bindel, S. Akleyek, E. Alkim, P. S. L. M. Barreto, J. Buchmann, E. Eaton, G. Gutoski, J. Kramer, P. Longa, H. Polat, J. E. Ricardini, and G. Zanon. qTESLA. Technical report, National Institute of Standards and Technology, 2019. available at <https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions>.
7. J. W. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila. Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE. In E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, editors, *ACM CCS 2016*, pages 1006–1018. ACM Press, Oct. 2016.
8. J. Breitner and N. Heninger. Biased nonce sense: Lattice attacks against weak ecdsa signatures in cryptocurrencies. In I. Goldberg and T. Moore, editors, *Financial Cryptography and Data Security*, pages 3–20, Cham, 2019. Springer International Publishing.
9. L. G. Bruinderink, A. Hülsing, T. Lange, and Y. Yarom. Flush, gauss, and reload - A cache attack on the BLISS lattice-based signature scheme. In B. Gierlichs and A. Y. Poschmann, editors, *CHES 2016*, volume 9813 of *LNCS*, pages 323–345. Springer, Heidelberg, Aug. 2016.
10. P. Campbell and M. Groves. Practical post-quantum hierarchical identity-based encryption. 16th IMA International Conference on Cryptography and Coding, 2017.
11. D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In Gilbert [31], pages 523–552.
12. Y. Chen, N. Genise, and P. Mukherjee. Approximate trapdoors for lattices and smaller hash-and-sign signatures. In S. D. Galbraith and S. Moriai, editors, *ASIACRYPT 2019*, volume 11923 of *LNCS*, pages 3–32. Springer, 2019.
13. Y. Chen, N. Genise, and P. Mukherjee. Approximate trapdoors for lattices and smaller hash-and-sign signatures. In S. D. Galbraith and S. Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 3–32. Springer, Heidelberg, Dec. 2019.
14. D. R. Cox and N. Small. Testing multivariate normality. *Biometrika*, 65(2):263–272, 1978.
15. R. B. D’Agostino, A. Belanger, and R. B. D’Agostino Jr. A suggestion for using powerful and informative tests of normality. *The American Statistician*, 44(4):316–321, 1990.
16. J. A. Doornik and H. Hansen. An omnibus test for univariate and multivariate normality. *Oxford Bulletin of Economics and Statistics*, 70:927–939, 2008.
17. Y. Du, B. Wei, and H. Zhang. A rejection sampling algorithm for off-centered discrete gaussian distributions over the integers. *Science China Information Sciences*, 62(3):39103, Sep 2018.
18. L. Ducas. *Signatures fondées sur les réseaux euclidiens : attaques, analyses et optimisations*. Theses, École Normale Supérieure, 2013.
19. L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. Lattice signatures and bimodal Gaussians. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 40–56. Springer, Heidelberg, Aug. 2013.
20. L. Ducas, V. Lyubashevsky, and T. Prest. Efficient identity-based encryption over NTRU lattices. In P. Sarkar and T. Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of *LNCS*, pages 22–41. Springer, Heidelberg, Dec. 2014.
21. L. Ducas and P. Q. Nguyen. Faster Gaussian lattice sampling using lazy floating-point arithmetic. In X. Wang and K. Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 415–432. Springer, Heidelberg, Dec. 2012.
22. N. C. Dwarakanath and S. D. Galbraith. Sampling from discrete gaussians for lattice-based cryptography on a constrained device. *Applicable Algebra in Engineering, Communication and Computing*, 25(3):159–180, 2014.
23. T. Espitau, P.-A. Fouque, B. Gérard, and M. Tibouchi. Side-channel attacks on BLISS lattice-based signatures: Exploiting branch tracing against strongSwan and electromagnetic emanations in microcontrollers. In Thuraisingham et al. [60], pages 1857–1874.

24. G. Estrin. Organization of computer systems: The fixed plus variable structure computer. In *Papers Presented at the May 3-5, 1960, Western Joint IRE-AIEE-ACM Computer Conference*, IRE-AIEE-ACM '60 (Western), pages 33–40, New York, NY, USA, 1960. ACM.
25. A. Facon, S. Guilley, M. Lec'Hvien, A. Schaub, and Y. Souissi. Detecting cache-timing vulnerabilities in post-quantum cryptography algorithms. In *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*, pages 7–12. IEEE, 2018.
26. J. J. Filliben and A. Heckert. *1.3.3.24. Quantile-Quantile Plot*. 2013.
27. G. E. Forsythe. Von neumann's comparison method for random sampling from the normal and other distributions. *Mathematics of Computation*, 26(120):817–826, 1972.
28. N. Gama, N. Howgrave-Graham, and P. Q. Nguyen. Symplectic lattice reduction and NTRU. In S. Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 233–253. Springer, Heidelberg, May / June 2006.
29. N. Genise and D. Micciancio. Faster Gaussian sampling for trapdoor lattices with arbitrary modulus. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 174–203. Springer, Heidelberg, Apr. / May 2018.
30. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In R. E. Ladner and C. Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.
31. H. Gilbert, editor. *EUROCRYPT 2010*, volume 6110 of *LNCS*. Springer, Heidelberg, May / June 2010.
32. N. Henze and B. Zirkler. A class of invariant consistent tests for multivariate normality. *Communications in Statistics-Theory and Methods*, 19(10):3595–3617, 1990.
33. J. Howe and M. O'Neill. GLITCH: A discrete gaussian testing suite for lattice-based cryptography. In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT, Madrid, Spain, July 24-26, 2017.*, pages 413–419, 2017.
34. A. Hülsing, T. Lange, and K. Smeets. Rounded Gaussians - fast and secure constant-time sampling for lattice-based crypto. In M. Abdalla and R. Dahab, editors, *PKC 2018, Part II*, volume 10770 of *LNCS*, pages 728–757. Springer, Heidelberg, Mar. 2018.
35. A. Karmakar, S. S. Roy, F. Vercauteren, and I. Verbauwhede. Pushing the speed limit of constant-time discrete Gaussian sampling. A case study on the Falcon signature scheme. In *Proceedings of the 56th Annual Design Automation Conference 2019*, pages 1–6, 2019.
36. C. F. F. Karney. Sampling exactly from the normal distribution. *ACM Trans. Math. Softw.*, 42(1):3:1–3:14, Jan. 2016.
37. A. Khalid, J. Howe, C. Rafferty, F. Regazzoni, and M. O'Neill. Compact, scalable, and efficient discrete gaussian samplers for lattice-based cryptography. In *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–5. IEEE, 2018.
38. S. Korkmaz, D. Goksuluk, and G. Zararsiz. Mvn: An r package for assessing multivariate normality. *The R Journal*, 6(2):151–162, 2014.
39. V. Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In M. Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 598–616. Springer, Heidelberg, Dec. 2009.
40. V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, and D. Stehlé. CRYSTALS-DILITHIUM. Technical report, National Institute of Standards and Technology, 2019. available at <https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions>.
41. V. Lyubashevsky and D. Wichs. Simple lattice trapdoor sampling from a broad class of distributions. In J. Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 716–730. Springer, Heidelberg, Mar. / Apr. 2015.
42. P. C. Mahalanobis. On the generalized distance in statistics. National Institute of Science of India, 1936.
43. K. V. Mardia. Measures of multivariate skewness and kurtosis with applications. *Biometrika*, 57(3):519–530, 1970.
44. C. A. Melchor and T. Ricosset. CDT-Based Gaussian Sampling: From Multi to Double Precision. *IEEE Trans. Computers*, 67(11):1610–1621, 2018.
45. D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 700–718. Springer, Heidelberg, Apr. 2012.
46. D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.*, 37(1):267–302, 2007.
47. D. Micciancio and M. Walter. Gaussian sampling over the integers: Efficient, generic, constant-time. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 455–485. Springer, Heidelberg, Aug. 2017.
48. M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. FrodoKEM. Technical report, National Institute of Standards and Technology, 2019. available at <https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions>.
49. M. Nemeč, M. Šýs, P. Svenda, D. Klinec, and V. Matyas. The return of coppersmith's attack: Practical factorization of widely used RSA moduli. In Thuraisingham et al. [60], pages 1631–1648.

50. NIST et al. OFFICIAL COMMENT: CRYSTALS-DILITHIUM, 2018. <https://groups.google.com/a/list.nist.gov/d/msg/pqc-forum/aWxC2ynJDLE/Y0sMJ2ewAAAJ>.
51. NIST et al. Footguns as an axis for security analysis, 2019. <https://groups.google.com/a/list.nist.gov/forum/#!topic/pqc-forum/l2iYk-8sGnI> last accessed 23-09-2019.
52. NIST et al. OFFICIAL COMMENT: Falcon (bug & fixes), 2019. <https://groups.google.com/a/list.nist.gov/forum/#!topic/pqc-forum/7Z8x5AMXy8s> last accessed on 23-09-2019.
53. C. Peikert. An efficient and parallel Gaussian sampler for lattices. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 80–97. Springer, Heidelberg, Aug. 2010.
54. P. Pessl, L. G. Bruinderink, and Y. Yarom. To BLISS-B or not to be: Attacking strongSwan’s implementation of post-quantum signatures. In Thuringham et al. [60], pages 1843–1855.
55. T. Pöppelmann, L. Ducas, and T. Güneysu. Enhanced lattice-based signatures on reconfigurable hardware. In L. Batina and M. Robshaw, editors, *CHES 2014*, volume 8731 of *LNCS*, pages 353–370. Springer, Heidelberg, Sept. 2014.
56. T. Pornin. New Efficient, Constant-Time Implementations of Falcon. Cryptology ePrint Archive, Report 2019/893, 2019.
57. T. Prest. Sharper bounds in lattice-based cryptography using the Rényi divergence. In T. Takagi and T. Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 347–374. Springer, Heidelberg, Dec. 2017.
58. T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. FALCON. Technical report, National Institute of Standards and Technology, 2019. available at <https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions>.
59. Microsoft SEAL (release 3.4). <https://github.com/Microsoft/SEAL>, Oct. 2019. Microsoft Research, Redmond, WA.
60. B. M. Thuringham, D. Evans, T. Malkin, and D. Xu, editors. *ACM CCS 2017*. ACM Press, Oct. / Nov. 2017.
61. M. Tibouchi and A. Wallet. One Bit is All It Takes: A Devastating Timing Attack on BLISS’s Non-Constant Time Sign Flips. *MathCrypt 2019*, 2019.
62. J. von Neumann. Various techniques used in connection with random digits. *National Bureau of Standards, Applied Math Series*, 12:36–38, 11 1950.
63. M. Walter. Sampling the integers with low relative error. In J. Buchmann, A. Nitaj, and T. Rachidi, editors, *AFRICACRYPT 2019*, volume 11627 of *LNCS*, pages 157–180. Springer, 2019.
64. R. K. Zhao, R. Steinfeld, and A. Sakzad. Compact and scalable arbitrary-centered discrete gaussian sampling over integers. Cryptology ePrint Archive, Report 2019/1011, 2019.
65. R. K. Zhao, R. Steinfeld, and A. Sakzad. Facct: Fast, compact, and constant-time discrete gaussian sampler over integers. *IEEE Transactions on Computers*, 2019.

A Proof of Theorem 7

Proof. Let us introduce an intermediate case where only the base sampler is modified (the exponential stays a perfect distribution). The 3 cases are defined as follows.

1. (IDEAL) a perfect $D_{\mathbb{Z},\sigma,\mu}$ distribution is called
2. (INTER) Only the exponential is considered as perfect.
3. (REAL) The final SamplerZ is called.

We first apply Lemma 11 (detailed and proved below) for assessing the bit security of the INTER case. Thanks to Condition (2), we get that $\lambda_{\text{INTER}} \geq \lambda - 1$. We then apply Lemma 12 (detailed and proved below) (for each input of the Bernoulli distribution) for assessing the bit security of the REAL case. Thanks to Condition (1), we get $\lambda_{\text{REAL}} \geq \lambda_{\text{INTER}} - 1 \geq \lambda - 2$. \square

Lemma 11. *Consider a cryptosystem denoted $C_{\mathcal{P}}$ in which a \mathbb{Q} -uple $(x_0, \dots, x_{\mathbb{Q}-1})$ is drawn according to a distribution \mathcal{P} . Assume that $C_{\mathcal{P}}$ is λ -bit secure against a search problem. Let us consider a copy of the latter cryptosystem, denoted $C_{\mathcal{Q}}$, where the only difference is that $(x_0, \dots, x_{\mathbb{Q}-1})$ is drawn according to a distribution \mathcal{Q} such that $\text{Supp}(\mathcal{Q}) \subseteq \text{Supp}(\mathcal{P})$.*

We denote $(x_0, \dots, x_{\mathbb{Q}-1})$ the random variables corresponding to $(x_0, \dots, x_{\mathbb{Q}-1})$ that follow \mathcal{P} or \mathcal{Q} depending on the case. For $0 \leq i < \mathbb{Q}$, we denote by $\mathcal{P}_{i|<i}(\cdot|x_{<i})$ (resp. $\mathcal{Q}_{i|<i}(\cdot|x_{<i})$) the

conditional distribution of x_i given the knowledge of $(x_1, \dots, x_{i-1}) = x_{<i}$ under \mathcal{P} (resp. \mathcal{Q}). If, for all $0 \leq i < \mathbf{Q}$, and for all i -uple $x_{<i}$ in the support of \mathcal{Q} restricted to its first i variables,

$$R_{2\lambda-1}(\mathcal{Q}_{i|x_{<i}}, \mathcal{P}_{i|x_{<i}}) \leq 1 + \frac{1}{4\mathbf{Q}}, \quad (10)$$

then $C_{\mathcal{Q}}$ is $(\lambda - 1)$ -bit secure against the search problem.

Note that when the drawing of x_i is independent from the preceding drawings, Equation 10 is equivalent to assume for all $0 \leq i < \mathbf{Q}$,

$$R_{2\lambda-1}(\mathcal{Q}_i, \mathcal{P}_i) \leq 1 + \frac{1}{4\mathbf{Q}}. \quad (11)$$

When they are not independent, we informally assume that the Rényi divergence is small no matter the preceding knowledge.

Proof. Let us assume that $C_{\mathcal{Q}}$ is *not* $(\lambda - 1)$ -bit secure against the search problem. Then, we assume that an attacker that breaks the scheme $C_{\mathcal{Q}}$ by solving the search problem with a probability, denoted $\varepsilon_{\mathcal{Q}}$, that is higher than $2^{-(\lambda-1)}$ exists. Thus,

$$\varepsilon_{\mathcal{Q}} > 2^{-(\lambda-1)}.$$

To succeed, the attacker draws a \mathbf{Q} -uple $(x_0, \dots, x_{\mathbf{Q}-1})$ (in $\text{Supp}(\mathcal{Q})$) according to the distribution \mathcal{Q} . Let us denote $\varepsilon_{\mathcal{P}}$ the probability that the same attacker breaks the scheme $C_{\mathcal{P}}$ with querying the distribution \mathcal{P} instead of \mathcal{Q} . By probability preservation, for all $a \in (1, +\infty)$,

$$\varepsilon_{\mathcal{P}} \geq \varepsilon_{\mathcal{Q}}^{a/(a-1)} / R_a(\mathcal{Q}, \mathcal{P}) \quad (12)$$

Let us set $a := 2\lambda - 1$ in Equation 12. For the numerator, we have

$$\varepsilon_{\mathcal{Q}}^{a/(a-1)} > \left(2^{-(\lambda-1)}\right)^{\frac{2\lambda-1}{2(\lambda-1)}} = \sqrt{2} \cdot 2^{-\lambda}. \quad (13)$$

Thus, $\varepsilon_{\mathcal{P}}$ satisfies

$$\varepsilon_{\mathcal{P}} > \frac{\sqrt{2} \cdot 2^{-\lambda}}{R_{2\lambda-1}(\mathcal{Q}, \mathcal{P})} \quad (14)$$

We apply Proposition 4 using the hypothesis in Equation 10,

$$R_{2\lambda-1}(\mathcal{Q}, \mathcal{P}) \leq \left(1 + \frac{1}{4\mathbf{Q}}\right)^{\mathbf{Q}} \leq e^{1/4} \leq \sqrt{2}. \quad (15)$$

Thus,

$$\varepsilon_{\mathcal{P}} > 2^{-\lambda}. \quad (16)$$

We can conclude that our attacker is also able to break $C_{\mathcal{P}}$ by solving the search problem with a success probability strictly higher than $2^{-\lambda}$.

Thus, assuming that $C_{\mathcal{Q}}$ is *not* $(\lambda - 1)$ -bit secure against the search problem leads to proving that $C_{\mathcal{P}}$ is *not* λ -bit secure against the search problem either. The lemma is, therefore, proved by contraposition. □

Lemma 12. Consider a cryptosystem denoted $C_{\mathcal{P}}$ in which a \mathbb{Q} -uple $(x_0, \dots, x_{\mathbb{Q}-1})$ is drawn according to a distribution \mathcal{P} . Assume that $C_{\mathcal{P}}$ is λ -bit secure against a search problem. Let us consider a copy of the latter cryptosystem, denoted $C_{\mathcal{Q}}$, where the only difference is that $(x_0, \dots, x_{\mathbb{Q}-1})$ is drawn according to a distribution \mathcal{Q} such that $\text{Supp}(\mathcal{Q}) = \text{Supp}(\mathcal{P})$.

We denote $(x_0, \dots, x_{\mathbb{Q}-1})$ the random variables corresponding to $(x_0, \dots, x_{\mathbb{Q}-1})$ that follow \mathcal{P} or \mathcal{Q} depending on the case. For $0 \leq i < \mathbb{Q}$, we denote by $\mathcal{P}_{i|x_{<i}}(\cdot|x_{<i})$ (resp. $\mathcal{Q}_{i|x_{<i}}(\cdot|x_{<i})$) the conditional distribution of x_i given the knowledge of $(x_1, \dots, x_{i-1}) = x_{<i}$ under \mathcal{P} (resp. \mathcal{Q}). If, for all $0 \leq i < \mathbb{Q}$ and for all i -uple $x_{<i}$ in the support of \mathcal{Q} restricted to its first i variables, $\mathcal{P}_{i|x_{<i}}$ and $\mathcal{Q}_{i|x_{<i}}$ satisfy

$$\forall x \in \text{Supp}(\mathcal{P}) \quad \left| \frac{\mathcal{P}_{i|x_{<i}}(x) - \mathcal{Q}_{i|x_{<i}}(x)}{\mathcal{P}_{i|x_{<i}}(x)} \right| \leq \frac{1}{\sqrt{2(2\lambda - 1) \cdot \mathbb{Q}}}, \quad (17)$$

then $C_{\mathcal{Q}}$ is $(\lambda - 1)$ -bit secure against the search problem.

Proof. Let us fix $0 \leq i < \mathbb{Q}$ and a i -uple $x_{<i}$ in the support of \mathcal{Q} restricted to its first i variables. Equation 17 can be rewritten as follows.

$$1 - \delta \leq \frac{\mathcal{Q}_{i|x_{<i}}}{\mathcal{P}_{i|x_{<i}}} \leq 1 + \delta \quad \text{with } \delta := \frac{1}{\sqrt{2(2\lambda - 1) \cdot \mathbb{Q}}}.$$

Since $\text{Supp}(\mathcal{Q}_{i|x_{<i}}) = \text{Supp}(\mathcal{P}_{i|x_{<i}})$ (because $\text{Supp}(\mathcal{P}) = \text{Supp}(\mathcal{Q})$), we apply \mathbb{Q} times Lemma 3 with $a = 2\lambda - 1$ and get

$$\begin{aligned} R_{2\lambda-1}(\mathcal{Q}_{i|x_{<i}}, \mathcal{P}_{i|x_{<i}}) &\leq 1 + \frac{(2\lambda-1) \cdot \frac{1}{2(2\lambda-1)\mathbb{Q}}}{2} \\ &= 1 + \frac{1}{4\mathbb{Q}}. \end{aligned}$$

The application of Lemma 11 allows to conclude. \square

B Proof of Lemma 8

Proof. We note $p_1(z)$ the probability that $z \in \mathbb{Z}$ (with a uniquely associated z_0) is output by `SamplerZ` in a given iteration. It holds that:

$$p_1(z) = \underbrace{\frac{\rho_{\sigma_{\max}}(z_0)}{\rho_{\sigma_{\max}}(\mathbb{Z}^+)}}_{\mathbb{P}[\text{BaseSampler} \rightarrow z_0]} \cdot \underbrace{\frac{1}{2}}_{\mathbb{P}[b]} \cdot \underbrace{\frac{\sigma_{\min}}{\sigma} \cdot \frac{\rho_{\sigma, \mu}(z)}{\rho_{\sigma_{\max}}(z_0)}}_{\mathbb{P}[\text{AcceptSample} \rightarrow \text{true}|z]} = \frac{\sigma_{\min} \cdot \rho_{\sigma, \mu}(z)}{2 \cdot \sigma \cdot \rho_{\sigma_{\max}}(\mathbb{Z}^+)}.$$

The probability P_{true} that $(\text{AcceptSample} \rightarrow \text{true})$ in a given iteration is:

$$P_{\text{true}} = \mathbb{P}[\text{AcceptSample} \rightarrow \text{true}] = \sum_z p_1(z) = \frac{\sigma_{\min} \cdot \rho_{\sigma, \mu}(\mathbb{Z})}{2 \cdot \sigma \cdot \rho_{\sigma_{\max}}(\mathbb{Z}^+)}. \quad (18)$$

One can see in (18) that P_{true} is independent of the output z . This is unsurprising since a different z is picked at each new iteration of the **while** loop, and each iteration's running time is constant.

However, it is not obvious from (18) that P_{true} is independent of σ and μ ; we now show that it is essentially the case. Since $\sigma \geq \eta_{\epsilon}^+(\mathbb{Z}^n) \geq \eta_{\epsilon/n}^+(\mathbb{Z}) \geq \eta_{\epsilon/n}(\mathbb{Z})$, it holds from [30, Lemma 2.7] that:

$$\rho_{\sigma, \mu}(\mathbb{Z}) \in \left[\frac{1 - \epsilon/n}{1 + \epsilon/n}, 1 \right] \cdot \rho_{\sigma}(\mathbb{Z}). \quad (19)$$

It is now helpful to bound $\rho_\sigma(\mathbb{Z})$. By the Poisson summation formula:

$$\rho_\sigma(\mathbb{Z}) = \sigma\sqrt{2\pi} \cdot \left(1 + 2 \sum_{i \geq 1} \exp(-2i^2\pi^2\sigma^2) \right). \quad (20)$$

For any $\sigma > 1$, it holds that $\sum_{i \geq 1} \exp(-2i^2\pi^2\sigma^2) \in \exp(-2\pi^2\sigma^2) \cdot [1, 1 + 2^{-80}]$. Moreover, it follows from (8) that $\exp(-2\pi^2\sigma^2) \leq \frac{\epsilon}{2n}$. Combined this fact with (20) yields:

$$\sigma\sqrt{2\pi} \leq \rho_\sigma(\mathbb{Z}) \leq \sigma\sqrt{2\pi} \cdot \left(1 + (1 + 2^{-80}) \cdot \frac{\epsilon}{n} \right) \quad (21)$$

Finally, combining (18), (19) and (21) yields:

$$P_{\text{true}}(\sigma, \mu) \in \frac{\sigma_{\min} \cdot \sqrt{2\pi}}{2 \cdot \rho_{\sigma_{\max}}(\mathbb{Z}^+)} \cdot \left(1, 1 + \frac{(1 + 2^{-80})\epsilon}{n} \right). \quad (22)$$

This concludes the proof. \square

C Proof of Theorem 9

Before proving Theorem 9, we will need a preliminary lemma. Note that this lemma cannot be proven in a black-box way using Lemma 3 since the relative error between any two distinct geometric distributions is infinite.

Lemma 13. *Let \mathcal{P} and \mathcal{Q} be geometric distributions of parameters $p, q \geq C$ for a constant $C \geq 0$. Suppose there exists $\delta = o(1/(a+1))$ such that:*

$$\begin{aligned} e^{-\delta} &\leq p/q \leq e^\delta, \\ e^{-\delta} &\leq (1-p)/(1-q) \leq e^\delta. \end{aligned}$$

Then the Rényi divergence between \mathcal{P} and \mathcal{Q} is bounded as follows:

$$R_a(\mathcal{P} \parallel \mathcal{Q}) \lesssim 1 + \frac{a(1-p)\delta^2}{p^2} \left(\sim 1 + \frac{a(1-q)\delta^2}{q^2} \right).$$

Proof. The beginning of the proof follows the one of [57, Lemma 3], but makes a more precise estimation. Let $f_a : (x, y) \mapsto \frac{y^a}{(x+y)^{a-1}}$. We compute values of f_a and its derivatives around $(0, y)$:

$$\begin{aligned} f_a(x, y) &= y && \text{for } x = 0 \\ \frac{\partial f_a}{\partial x}(x, y) &= 1 - a && \text{for } x = 0 \\ \frac{\partial^2 f_a}{\partial x^2}(x, y) &= a(a-1)y^a(x+y)^{-a-1} \\ &\leq \frac{a(a-1)}{e^{-(a+1)\delta}y} && \text{for } |x+y| \leq e^\delta \cdot y \end{aligned}$$

We now use partial Taylor bounds. If $|x_k| \leq (e^{\delta k} - 1) \cdot y_k$, then:

$$f_a(x_k, y_k) \leq f_a(0, y_k) + \frac{\partial f_a}{\partial x}(0, y_k) \cdot x_k + \frac{a(a-1)(e^{\delta k} - 1)^2}{2e^{-(a+1)\delta k}} \cdot y_k$$

We take $y_k = \mathcal{P}(k)$ and $x_k = \mathcal{Q}(k) - \mathcal{P}(k)$, and note that $e^{-k\delta} \leq \mathcal{P}(k)/\mathcal{Q}(k) \leq e^{k\delta}$, hence $\delta_k \leq k\delta$. Summing all over the support of \mathcal{P} gives:

$$R_a^a(\mathcal{P} \parallel \mathcal{Q}) \leq 1 + \frac{a(a-1)}{2} \sum_{k \in \mathbb{Z}^+} \frac{(e^{k\delta} - 1)^2}{e^{-(a+1)k\delta}} \cdot (1-p)^{k-1} p \quad (23)$$

$$\leq 1 + \frac{pa(a-1)}{2(1-p)} \cdot \left(\frac{2(1-p)^2\delta^2}{p^3} + O\left(\frac{a\delta^3(p-1)^3}{p^4}\right) \right) \quad (24)$$

$$\lesssim 1 + \frac{a(a-1)(1-p)\delta^2}{p^2}$$

To compute the sum in (23), we expanded $(e^{k\delta} - 1)^2$, which then gives us three distinct geometric sums which all converge since $\delta = o(1/(a+1))$, and for which closed formulae are known. A tedious but easy Taylor expansion then gives us 24, at which point we can conclude. \square

We now prove Theorem 9.

Proof. Let T_0 denote the running time of one iteration of the **while** loop in Algorithm 1. It is clear that steps 2 to 5 are isochronous. On the other hand, it is also clear that **AcceptSample** (Algorithm 2) is isochronous; indeed, all its atomic operations are isochronous and each iteration of its **while** loop has a constant probability $1 - 2^{-8}$ of being the last one. We can conclude that T_0 follows a distribution which is independent of σ, μ, z .

Let us denote by $I_{\sigma, \mu}$ (resp. I) the number of iterations of the **while** loop when each iteration accepts with probability P_{true} (resp. p). By Lemma 8, $I_{\sigma, \mu}$ (resp. I) follows a geometric law of parameter P_{true} (resp. p). The relative error between P_{true} and p is upper bounded by $\delta = \frac{(1+2^{-80})\epsilon}{n} \cdot \max(1, \frac{p}{1-p})$. It then follows from Lemma 13 that:

$$\begin{aligned} R_a(I_{\sigma, \mu} \| I) &\lesssim 1 + \frac{a(1-p)\delta^2}{p^2} \\ &\lesssim 1 + \frac{a\epsilon^2 \max(1, \frac{1-p}{p})^2}{n^2(1-p)} \end{aligned}$$

Finally, the total running time T of Algorithm 1 is a function of the running time of each iteration and the number of iterations: $T = f(T_0, I)$ for some function f . This allows to apply once again the data-processing inequality:

$$R_a(T_{\sigma, \mu} \| T) = R_a(f(T_0, I_{\sigma, \mu}) \| f(T_0, I)) \leq R_a(I_{\sigma, \mu} \| I),$$

which concludes the proof. \square

D Proof of Corollary 10

Proof. We denote by D the publicly available signature distribution. We consider two cases:

- **STRONG**: we give powerful timing attack capabilities to the adversary by allowing her to learn the exact runtime of each call to **SamplerZ** (σ, μ) without knowing (σ, μ) . She then learns the joint distribution $(D, (T_{\sigma_0, \mu_0}, \dots, T_{\sigma_{Q-1}, \mu_{Q-1}}))$ where Q is the total number of calls to **SamplerZ** (for Falcon $Q = 2nQ_s$), $T_{\sigma, \mu}$ denotes the runtime of **SamplerZ** (σ, μ) (as in Theorem 9) and (σ_i, μ_i) are the unknown possibly dependent input parameters of **SamplerZ**.
- **STANDARD**: we assume that the attacker has no access to the runtime of each sampling and thus we can write without loss of generality that she has access to (D, T^Q) where T is a distribution defined in Theorem 9.

Let $P_{\text{STRONG}}, P_{\text{STANDARD}}$ denote the success probability of \mathcal{A} in the **STRONG** and **STANDARD** cases, respectively. We set $a := \lambda$ and apply probability preservation.

$$P_{\text{STRONG}} \leq (P_{\text{STANDARD}} \cdot R_\lambda((D, (T_{\sigma_0, \mu_0}, \dots, T_{\sigma_{Q-1}, \mu_{Q-1}})), (D, T^Q))^{(\lambda-1)/\lambda}. \quad (25)$$

Note that D and $(T_{\sigma_0, \mu_0}, \dots, T_{\sigma_{Q-1}, \mu_{Q-1}})$ are independent, thus

$$P_{\text{STRONG}} \leq (P_{\text{STANDARD}} \cdot R_\lambda((T_{\sigma_0, \mu_0}, \dots, T_{\sigma_{Q-1}, \mu_{Q-1}}), T^Q))^{(\lambda-1)/\lambda}. \quad (26)$$

Let us replace ϵ by $\frac{1}{\sqrt{\lambda q}}$ in Theorem 9 and get

$$\forall \sigma \in [\sigma_{\min}, \sigma_{\max}], \forall \mu \in [0, 1] \quad R_\lambda(T_{\sigma, \mu}, T) \lesssim 1 + \frac{1}{n^2 q}.$$

Therefore, we can apply Proposition 4 and get

$$P_{\text{STRONG}} \lesssim \left(P_{\text{STANDARD}} \cdot \left(1 + \frac{1}{n^2 q} \right)^q \right)^{(\lambda-1)/\lambda} \quad (27)$$

$$\lesssim 2^{-\lambda} \cdot 2 \cdot e^{1/n^2}. \quad (28)$$

□

E Impact of the scaling factor in Falcon

We now study the impact of the scaling factor $\frac{\sigma_{\min}}{\sigma} \leq \frac{\sigma_{\min}}{\sigma_{\max}}$ on the running time for the particular case of Falcon. There, each σ verifies $\sigma_{\min} \leq \sigma \leq \sigma_{\max}$, where $\sigma_{\min} = \eta_e^+(\mathbb{Z}^n)$ and $\sigma_{\max} = \sigma_{\min} \cdot \frac{\max_i \|\tilde{\mathbf{b}}_i\|}{\min_i \|\tilde{\mathbf{b}}_i\|}$. The $\tilde{\mathbf{b}}_i$ are the Gram-Schmidt vectors of the secret, short basis \mathbf{B} . In Falcon, it holds that:

$$\max_i \|\tilde{\mathbf{b}}_i\| \leq 1.17\sqrt{q} \quad (29)$$

$$\min_i \|\tilde{\mathbf{b}}_i\| \geq \sqrt{q}/1.17 \quad (30)$$

By construction, (29) is true (Falcon enforces it at key generation). To prove (30), we rely on a peculiar property of Falcon's private bases: *symplecticity*. Let f, g, F, G be such that $fG - gF = q$. Let:

$$\mathbf{J} = \left[\begin{array}{c|c} 0 & 1 \\ \hline -1 & 0 \end{array} \right] \quad \text{and} \quad \mathbf{B} = \left[\begin{array}{c|c} g & -f \\ \hline G & -F \end{array} \right].$$

This form of \mathbf{B} is indeed the one used in Falcon. It has been observed in [28] that \mathbf{B} is q -symplectic, that is, it verifies:

$$\mathbf{B}^t \times \mathbf{J} \times \mathbf{B} = q \cdot \mathbf{J}. \quad (31)$$

As per [28, Corollary 1], this implies that for any i , $\|\tilde{\mathbf{b}}_{2n+1-i}\| = q/\|\tilde{\mathbf{b}}_i\|$. Combining this with (29) yields (30). Thus $\frac{\sigma_{\min}}{\sigma_{\max}} \leq (1.17)^{-2} \approx 0.73$, which means a non-negligible but reasonable impact on the running time of the sampler.

F Additional information on SAGA

F.1 Univariate tests

An example of the standard outputs of the univariate tests in SAGA is shown in Listing 1.1.

```

>>> python3                # initialize python
>>> import saga            # import the test suite
>>> mu = -0.920619        # define the centre
>>> sigma = 1.711864      # define the standard deviation
>>> data = [-1, 2, -4, 0, -2, 1, -2, -3, -1, 1, -1, 0, 0, 1, -4, -1, -2, -2, -1,
0, 1, -1, 2, -3, 2, 0, -1, -2, 0, -3, -1, -2, -1, 1, -5, -1, -2, -2, -1, 0, 2,
1, 0, 0, 1, -1, -2, -2, -1, 0, 2, -2, -1, -3, 0, 0, 0, -2, 0, 0, 0, -3, -4,
0, 1, -1, 0, -1, 1, -3, 0, 0, -3, 0, -4, -1, -2, 0, 0, -2, -2, -1, 1, -1, 0,
-2, -2, -2, 0, -1, -4, -2, 0, -2, -2, 1, -1, 0, -3, -1]
>>>
>>> res = saga.UnivariateSamples(mu, sigma, data)
>>> res

Testing a Gaussian sampler with center = -0.920619 and sigma = 1.711864
Number of samples: 100

Moments | Expected      Empiric
-----+-----
Mean:   | -0.92062      -0.92000
St. dev. | 1.71186       1.51446
Skewness | 0.00000       -0.25650
Kurtosis | 0.00000       -0.26704

Chi-2 statistic: 4.033416341364921
Chi-2 p-value: 0.4015023295495953 (should be > 0.001)

How many outliers? 0

Is the sample valid? True

```

Listing 1.1: Output statistics on univariate Gaussian samples.

F.2 Multivariate tests

An example of the standard outputs of the multivariate tests in SAGA is shown in Listing 1.2.

```

>>> python3                # initialize python
>>> import saga            # import the test suite
>>> sigma, data = saga.parse_multivariate_file("testdata/falcon64_avx2")
                             # parse raw file
>>> res = saga.MultivariateSamples(sigma, data)
                             # compute tests
>>> res                    # print results

Testing a centered multivariate Gaussian of dimension = 128 and sigma = 171.831
Number of samples: 63960

The test checks that the data corresponds to a multivariate Gaussian, by doing the
following:
1 - Print the covariance matrix (visual check). One can also plot
   the covariance matrix by using self.show_covariance().
2 - Perform the Doornik-Hansen test of multivariate normality.
   The p-value obtained should be > 0.001
3 - Perform a custom test called covariance diagonals test.
4 - Run a test of univariate normality on each coordinate

1 - Covariance matrix (128 x 128):
[[ 0.997 -0.0021 0.0065 ... 0.0014 0.0012 -0.0039]
 [-0.0021 1.0001 -0.0014 ... 0.0032 0.0005 -0.0048]
 [ 0.0065 -0.0014 1.0028 ... -0.0006 0.0074 0.0065]
 ...
 [ 0.0014 0.0032 -0.0006 ... 1.0063 -0.0022 -0.0005]
 [ 0.0012 0.0005 0.0074 ... -0.0022 0.993 -0.0008]
 [-0.0039 -0.0048 0.0065 ... -0.0005 -0.0008 1.0081]]

2 - P-value of Doornik-Hansen test:          0.2453

3 - P-value of covariance diagonals test:    0.3244

4 - Gaussian coordinates (w/ st. dev. = sigma)? 128 out of 128

>> u.univariates            # returns univariate tests on each 'row'

Testing a Gaussian sampler with center = 0 and sigma = 164.46976732471182
Number of samples: 1000

Moments | Expected      Empiric
-----+-----
Mean:   | 0.00000       -2.01000
St. dev. | 164.46977    160.92979
Skewness | 0.00000       0.01555
Kurtosis | 0.00000      -0.00831

Chi-2 statistic: 97.98787878787878
Chi-2 p-value: 0.2650065102842649 (should be > 0.001)

How many outliers? 0

Is the sample valid? True

```

Listing 1.2: Output statistics on multivariate Gaussian samples.

F.3 Supplementary, visual, ‘sanity check’ tests

We also provide further sanity check functionality in the code, which will be particularly useful if any of the statistical tests above fail to conform to the expected values. D’Agostino et al. [15] suggested the best way to do this is via graphical methods, thus we provide visuals for both univariate and multivariate Gaussians.

For univariate Gaussians, we provide plots of the observed and expected probability density functions (Figure 2a) and quantile-quantile (QQ) plots (Figure 2b), shown in Figure 2. The QQ plot also provides the coefficient of determination, $R^2 \in [0, 1)$, which measures how well the observed data follows the distribution we expect. There are many different errors which can be observed in QQ plots, from sampling biases to data skewness, but there are some useful guides [26], helpful websites¹¹¹², and online tools¹³ to help analysing these plots.

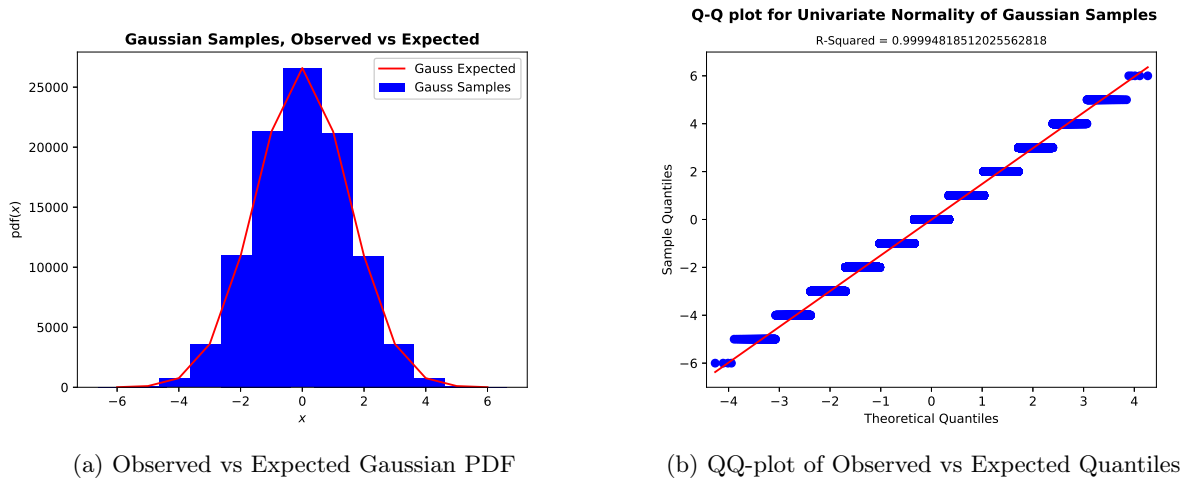


Figure 2: Visual representation of the expected form of univariate Gaussian samples.

For multivariate distributions, it is typically difficult to visualise any statistical properties of a distribution beyond three dimensions. However, there is a method for checking multivariate normality using a distribution’s Mahalanobis distance [42], which is a measure of the distance between certain points to a certain distribution. More specifically, it is a multi-dimensional generalisation of measuring how many standard deviations a point is away from a distribution. These sorted distances should follow a chi-square distribution [38], thus we can visualise this as a QQ-plot comparing the Mahalanobis distance versus the expected chi-square distribution. Figure 3 shows an example of our proposed multivariate normality graphical representation.

A final test we provide is for checking the rejection rate of the Gaussian samplers. Theoretically, the rejection rates of the Gaussian samples should decrease geometrically. An example of what the rejection rates should look like for a fixed σ are provided in Figure 4.

In order to check the rejection rates, the test suite requires the additional output of the rejection rate associated to each sample. An example of this is shown in Listings 1.3 and 1.4, which shows the typical Gaussian sampler (Listing 1.3) and the Gaussian sampler which also outputs the repetitions for each sample (Listing 1.4).

¹¹ <https://stats.stackexchange.com/questions/101274/how-to-interpret-a-qq-plot>.

¹² <https://data.library.virginia.edu/understanding-q-q-plots/>.

¹³ <https://xiongge.shinyapps.io/qqplots/>

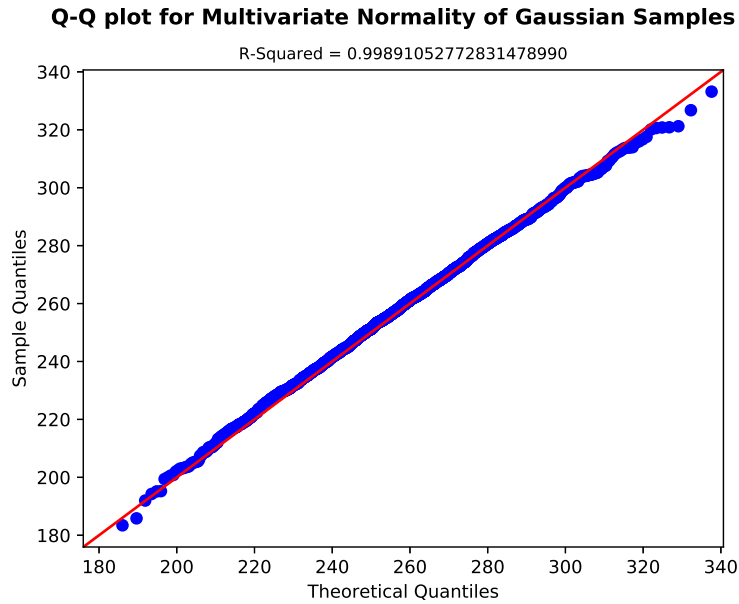


Figure 3: Visual representation of the expected form of univariate Gaussian samples.

```
def samplerz(center, sigma):
    assert(sigma < sigma0)
    assert(sigma >= sigma_min)
    c0 = center - floor(center)
    sf = sigma / sigma0

    while(1):
        z0 = sampler0()
        b = randint(0, 1)
        z = ((b << 1) - 1) * z0 + b
        x = ((z - c0) ** 2) / (2 * (sigma **
            2)) - (z0 ** 2) / (2 * (sigma0 **
            2))

        if berexp(x, sf) is True:
            return floor(center) + z
```

Listing 1.3: Standard Gaussian sampler.

```
def samplerz_rep(center, sigma):
    assert(sigma < sigma0)
    assert(sigma >= sigma_min)
    c0 = center - floor(center)
    sf = sigma / sigma0
    cnt = 0 # repetition counter
    while(1):
        z0 = sampler0()
        b = randint(0, 1)
        z = ((b << 1) - 1) * z0 + b
        x = ((z - c0) ** 2) / (2 * (sigma **
            2)) - (z0 ** 2) / (2 * (sigma0 **
            2))

        cnt += 1 # increment counter
        if berexp(x, sf) is True:
            # output count with value
            return floor(center) + z, cnt
```

Listing 1.4: Gaussian sampler with repetitions.

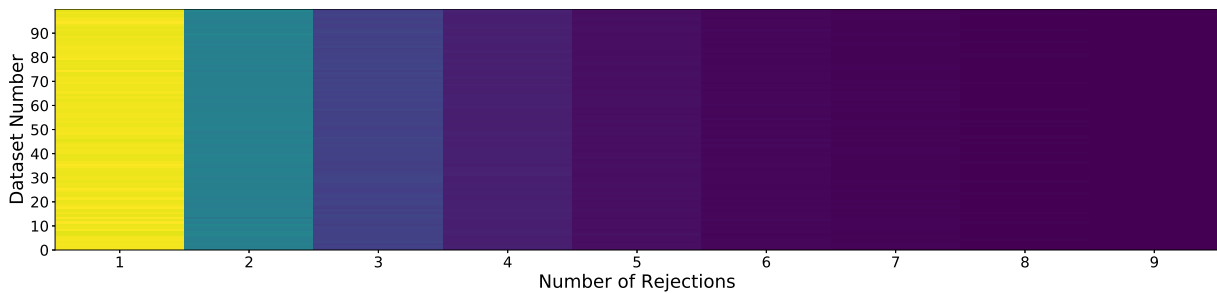


Figure 4: Expected geometric decrease in rejection numbers during Gaussian sampling.