They tried to make use of the hybrid sampler, but they couldn't find a way to generate (f, g) of sufficient quality in an efficient way.

Mitaka makes progress in this direction.

Hybrid sampler works correctly for $\sigma \geq \eta_\varepsilon(\mathbb{Z}^d) \, \|B\|_K$

↗ R-module analogue of $\|B\|_{GS}$

Quality measure for hybrid

For it to make the signature secure,

we need $(f,g) \in R^\times$ to satisfy

$$\frac{q}{\alpha^2} \leq \|B\|_K = \max_i \left(\|\sigma_{2i-1} f\|^2 + \|\sigma_{2i-1} g\|^2 \right) \leq \alpha^2 q$$

for α close to 1.

Mitaka achieves this by improving Falcon's keygen in a couple of ways:

① key reuse: if (f,g) fails the test, don't throw it away; if we have

$$(f_1, g_1), (f_2, g_2), \cdots, (f_k, g_k)$$

maybe something like (f_i, g_j) will work

② key combination: sample

$$f_1, f_2, \cdots, f_k \quad \text{from } D_{R, \tau/2, 0}$$

then any $f_i + f_j \sim D_{R, \tau, 0}$

This way we can make $\approx k^2/2$

candidate keys from k samples.

They claim this works with

$\alpha = 2.04$ $n = 512$ 102/92

for $\Rightarrow$ security

$\alpha = 2.33$ $n = 1024$ 233/211

Gain: signing is twice as fast as Falcon, because hybrid is twice as fast as Klein.

But one performance metric is not mentioned anywhere in the Miteka paper...

keygen time.

They actually couldn't present a

C implementation. Their python implementation is 400x as slow (!!) as Falcon's keygen.

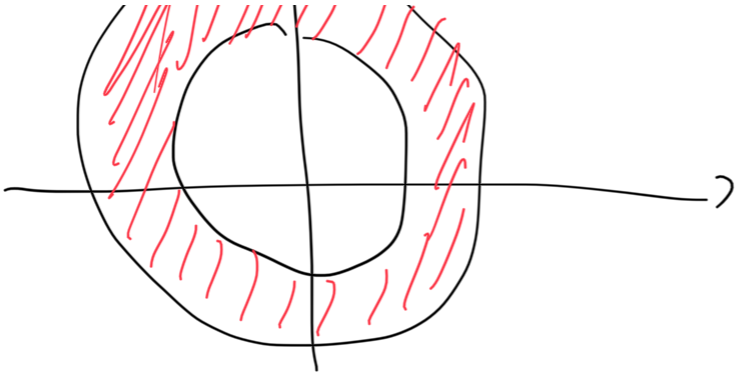
Solmae / Antrag

The idea of Solmae is:
there's actually no need to sample $(f, g) \in R^2$ by Gaussian sampling.

Recall the criterion

$$\frac{q}{d^2} \leq \max_i \left(\|\sigma_{2i-1} f\|^2 + \|\sigma_{2i-1} g\|^2 \right) \leq d^2 q$$

For each $i = 1, 2, \cdots, n$, this defines an annulus in $\mathbb{R}^2$ of inner rad $d/\sqrt{q}$ outer rad $d\sqrt{q}$



So just sample $(\sigma_{2i-1} f, \sigma_{2i-1} g)$ from the annulus, and take inverse FFT and roundoff to get $(f, g) \in \mathbb{R}^2$.

This leads to an efficient keygen for hybrid samplers: for $n = 512$

Falcon's keygen takes 4.7 ms

Solmae's keygen takes 5.7 ms.

Furthermore, this is achieved with $\alpha = 1.17$ so it's a few bits more secure than Falcon.

And it uses the hybrid sampler,

so signing is twice as fast!

Security analysis, concrete or otherwise, goes exactly the same as that of Falcon.

Some drawbacks

Common to all Falcon families

- The NTRU assumption:
  there are some proofs of security based on the assumption that $h = g/f$ is distributed uniformly on R/qR. (e.g. Stehlé-Steinfeld)
  But these signatures don't really care.
- Use of DGS makes it susceptible to side-channel attacks: constant-time signing, power analysis...

I have an idea to free Falcon, Solmae, Hawk... all these birds from DGS, it's a work in progress, but performance is an issue.

But GPV was very inefficient in the beginning too, and took almost 20 years of research to reach its current state. Perhaps the same thing will happen.