```
print(primal_usvp(n, alpha_0, q, secret_distribution=alpha_1, m=n, reduction_cost_model=BKZ.ADPS16)) #+end_src
```

```
: Traceback (most recent call last)
: ...
: NotImplementedError: secret size 0.000701 > error size 0.000484
```

```
#+begin_src jupyter-python :kernel sagemath print(primal_usvp(n, alpha_1, q, secret_distribution=alpha_0, m=n,
reduction_cost_model=BKZ.ADPS16)) #+end_src
```

```
: rop: 2^118.0, red: 2^118.0, delta_0: 1.003955, beta:  404, d: 1022, m: 509
```

That is, the LWE esitmator – in agreement with scripts of Léo Ducas and Dan Bernstein – predicts that the primal uSVP attack requires block size 404 when n samples are available for LightSaber.

There is, however, still a (in this case minor) issue to be resolved:

https://bitbucket.org/malb/lwe-estimator/issues/46/support-small-secrets-that-are-larger-than

Cheers,
Martin

--

_pgp: https://keybase.io/martinralbrecht
_www: https://malb.io/

This email, its contents and any attachments are intended solely for the addressee and may contain confidential information. In certain circumstances, it may also be subject to legal privilege. Any unauthorised use, disclosure, or copying is not permitted. If you have received this email in error, please notify us and immediately and permanently delete it. Any views or opinions expressed in personal emails are solely those of the author and do not necessarily represent those of Royal Holloway, University of London. It is your responsibility to ensure that this email and any attachments are virus free.