An SVP attack on Vortex

Zhenfei Zhang

Scroll
zhenfei@scroll.io

December 27, 2022

Abstract. In [BS22], the authors proposed a lattice based hash function that is useful for building zero-knowledge proofs with superior performance. In this short note we analysis the underlying lattice problem with the classic shortest vector problem, and show that 2 out of 15 proposed parameter sets for this hash function do not achieve the claimed security.

1 Introduction

In [BS22], the authors proposed a lattice based hash function that is useful for building zero-knowledge proofs with superior performance. Essentially, the hash function relies on the ring short integer solution (Ring-SIS) problem.

Definition 1 (Ring-SIS$_{q,n,m,\beta}$). *Let $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathcal{R}$, where $\mathcal{R} = \mathbb{Z}_q[x]/(x^n + 1)$ for some prime q and a power-of-2 n. Find a set of short elements $\mathbf{s}_1, \ldots, \mathbf{s}_m$ such that $\|\mathbf{s}_i\|_\infty \leq \beta$ and $\sum_{i=1}^{m} \mathbf{a}_i \mathbf{s}_i = 0$.*

Table 1 lists the parameters that are abstracted from the Appendix A.6 of [BS22]. All the parameter sets claim 128 bits of security.

Breaking the Ring-SIS problem with the above parameters implies that one is able to find collisions of the hash function. This in return breaks the binding property of vector commitment scheme build from this hash function. Those reductions are orthogonal to the analysis in this note. Here we focus on the underlying Ring-SIS problem.

Acknowledgement We would like to thank Antonio Sanso and Ye Zhang for suggesting this topic; Alexadre Belling for explaining some details of the construction; for pointing out some misunderstanding of Vortex construction that lead to an overestimation of around 8 bits in the cryptanalysis in a previous version of this note; and for suggesting to use l_∞ norm instead of l_2 norm in the analysis.

We communicated our attack with the authors of [BS22]. The authors acknowledged attack publicly [Sol22] and revised the parameters in a later version of the paper.

Param Set	$\log(q)$	$\log(\beta)$	n	m
A1	64	4	32	5,000,000
A2	64	6	64	33,554,432
A3	64	10	128	33,554,432
A4	64	15	256	33,554,432
A5	64	21	512	33,554,432
A6	64	31	1024	33,554,432
B1	254	2	2	33,554,432
B2	254	3	4	33,554,432
B3	254	4	8	33,554,432
B4	254	6	16	33,554,432
B5	254	10	32	33,554,432
B6	254	15	64	33,554,432
B7	254	23	128	33,554,432
B8	254	31	256	33,554,432
B9	254	50	512	33,554,432

Table 1. Proposed Ring-SIS parameters for the hash function in Vortex [BS22]. You may notice some slight difference between this table and [BS22]. This is because the ring-SIS solution has coefficients in $[-\beta, \beta]$, while the actual inputs to the hash functions are polynomials with coefficients between $[0, 2\beta)$ [BS22].

2 Our attack

2.1 Assumptions

We make the following assumptions reported in [BDGL16].

Assumption 1 *The runtime for a single call to SVP oracle is* $2^{0.292k+16.4}$*, where* k *is the dimension of the lattice.*

This assumption has been used widely in the literature, including [BS22], for estimating the cost of BKZ.

We also rely on the well-known Gaussian heuristic.

Assumption 2 *For a random lattice* $\mathcal{L}$*, the length of its shortest non-zero vector, a.k.a., first minima, is expect at*

$$\lambda_1^{\infty}(\mathcal{L}) \approx \frac{\det^{\frac{1}{\dim}} - 1}{2}$$

where dim *and* det *are the dimension and determinant of the lattice.*

Assumption 3 *We assume the lattice* $\mathcal{L}$*, defined in Equation 1, behaves as a random lattice.*

2.2 Intuition

As pointed out in [DM08], the attacker is not obliged to take all the input elements; finding a solution for a subset of $\{\mathbf{a}_i\}$ is already sufficient. The optimal subset has a size of $m' := \sqrt{n \log q \log \delta}$ if $m' < m$. Here δ is a constant factor that depends on the lattice reduction algorithm.

In such a typical attack, the size of the subset, m', is still large. Via BKZ reduction, one is able to find an approximate shortest vector in the corresponding lattice, and hope that this approximate shortest vector is short enough to solve the problem. Handwavingly speaking, for BKZ 2.0 [CN11] it is possible to achieve $\delta = 1.005$ or smaller. The approximation is due to the existence of various BKZ models in the literature [APS15].

Out attack follows the same intuition. We take an even smaller subset where finding the exact shortest vector becomes feasible. In other words, we invoke the more costly and more powerful SVP solver. Note that the best known SVP algorithm runs in exponential time. Our strategy is only possible if the dimension of the lattice is small. In our case, the degree of the polynomial ring, i.e., n is super small (2, 4, 8, ...). Then, we just need to take a large enough subset such that the shortest vector happens to be smaller than β. This solve the ring-SIS problem. In the following, we will show how the lattice is build, give concrete estimation of the length of its shortest vector and the cost to find such a vector.

2.3 The actual attack

For a ring element $\mathbf{a}(x) := \sum_{i=0}^{n-1} a_i x^i$, denote $Rot(\mathbf{a})$ the nega-cyclic rotation matrix of $\mathbf{a}$, i.e.,

$$Rot(\mathbf{a}) := \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ -a_{n-1} & a_0 & \dots & a_{n-2} \\ -a_{n-2} & -a_{n-1} & \dots & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \dots & a_0 \end{pmatrix}$$

For ring elements, $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{c} := \mathbf{a} \cdot \mathbf{b}$ where $\cdot$ is the ring multiplication, let $\boldsymbol{b}$ and $\boldsymbol{c}$ be the vector form of $\mathbf{b}$ and $\mathbf{c}$. Then we have $\boldsymbol{b} \times Rot(\mathbf{a}) = \boldsymbol{c} \bmod q$ where $\times$ is the vector-matrix multiplication. Also, denote $\mathbf{I}_n$ the identity matrix of dimension n, and $q\mathbf{I}_n$ the matrix obtained by scaling $\mathbf{I}_n$ with q.

Concretely our lattice that is spanned by the row vector of the following matrix

$$\mathcal{L} := \begin{pmatrix} q\mathbf{I}_n & 0 & 0 & \dots & 0 \\ Rot(\mathbf{a}_1) & \mathbf{I}_n & 0 & \dots & 0 \\ Rot(\mathbf{a}_2) & 0 & \mathbf{I}_n & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ Rot(\mathbf{a}_{m'}) & 0 & 0 & \dots & \mathbf{I}_n \end{pmatrix} \tag{1}$$

The dimension of this lattice is $(m'+1)n$, and the determinant of the lattice is q^n. The vector $\langle 0, \mathbf{s}_1, \dots, \mathbf{s}_{m'} \rangle$ is a vector is this lattice, where the l_∞ norm is

bounded by β. If β is greater than the Gaussian expected length, there exists a vector of such length with overwhelming probability, and an SVP solver will be able to find this vector.

So concretely, our attack takes the following steps:

- For a given tuple of q, β and n, find the largest m' s.t.,

$$\beta > \frac{\det^{\frac{1}{\dim}} - 1}{2} = \frac{q^{\frac{1}{(m'+1)}} - 1}{2}; \tag{2}$$

- Plugin the run time formula of the SVP solver with $2^{0.292(m'+1)n+16.4}$

We summarize our evaluations in Table 2. Parameter sets B1 and B2 do not meet 128 bits of security from our analysis.

Param Set	$\log(q)$	$\log(\beta)$	n	m'	dim	log SVP cost
A1	64	4	32	12	46	138
A2	64	6	64	9	640	203
B1	254	2	2	80	162	**64**
B2	254	3	4	62	252	**90**
B3	254	4	8	50	408	136
B4	254	6	16	36	592	190
B5	254	10	32	23	768	241

Table 2. Concrete cost for the proposed attack

References

[APS15] Martin R. Albrecht, Rachel Player, and Sam Scott. On the concrete hardness of learning with errors. Cryptology ePrint Archive, Report 2015/046, 2015. https://ethresear.ch/t/vortex-building-a-prover-for-the-zk-evm/14427/2.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. pages 10–24, 2016.

[BS22] Alexandre Belling and Azam Soleimanian. Vortex : Building a lattice-based snark scheme with transparent setup. Cryptology ePrint Archive, Paper 2022/1633, 2022. https://eprint.iacr.org/2022/1633.

[CN11] Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better lattice security estimates. pages 1–20, 2011.

[DM08] Oded Regev Daniele Micciancio. Lattice-based cryptography. *Post-quantum Cryptography*, 2008.

[Sol22] Azam Soleimanian. Vortex : building a prover for the zk-evm. Ethereum Reserach, 2022. https://eprint.iacr.org/2015/046.

Sage script

```
params = [\
    ["A1", 64, 5, 32],\
    ["A2", 64, 7, 64],\
    ["A3", 64, 11, 128],\
    ["A4", 64, 16, 256],\
    ["A5", 64, 22, 512],\
    ["A6", 64, 32, 1024],\
    ["B1", 254, 3, 2],\
    ["B2", 254, 4, 4],\
    ["B3", 254, 5, 8],\
    ["B4", 254, 7, 16],\
    ["B5", 254, 11, 32],\
    ["B6", 254, 16, 64],\
    ["B7", 254, 24, 128],\
    ["B8", 254, 32, 256],\
    ["B9", 254, 51, 512],\
]


def log_svp_cost(dim):
    return 0.292 * dim + 16.4


def find_m_prime(n, beta, q):
    for m in range(1,10000):
        if 2*beta >= q^(1/(m+1)) - 1:
            return m

for param in params:
    m = find_m_prime(param[3], 2^(param[2]-1), 2^param[1])
    dim = round((m + 1) * param[3])
    print (param[0], m, dim, log_svp_cost(dim))
```