Johanna Loyer, Inria Paris

Lattice sieving via quantum walks

Joint work with André Chailloux

QUANTUM COMPUTERS

QUANTUM COMPUTERS

efficiently solves

Factorization
Discrete logarithm

QUANTUM COMPUTERS

Factorization
Discrete logarithm

Need to standardize **quantum resistant** cryptosystems

QUANTUM COMPUTERS

Factorization
Discrete logarithm

Need to standardize quantum resistant cryptosystems

NIST PQC

Post-quantum cryptography international contest
to standardize the most secure cryptosystems

QUANTUM COMPUTERS

Factorization
Discrete logarithm

Need to standardize **quantum resistant** cryptosystems

NIST PQC

Lattice-based problems

NTRU

LWE

SIS

SVP

One of the categories of problems that resist to quantum attacks

QUANTUM COMPUTERS

Factorization
Discrete logarithm

Need to standardize **quantum resistant** cryptosystems

NIST PQC

Lattice-based problems

NTRU

LWE

SIS

SVP

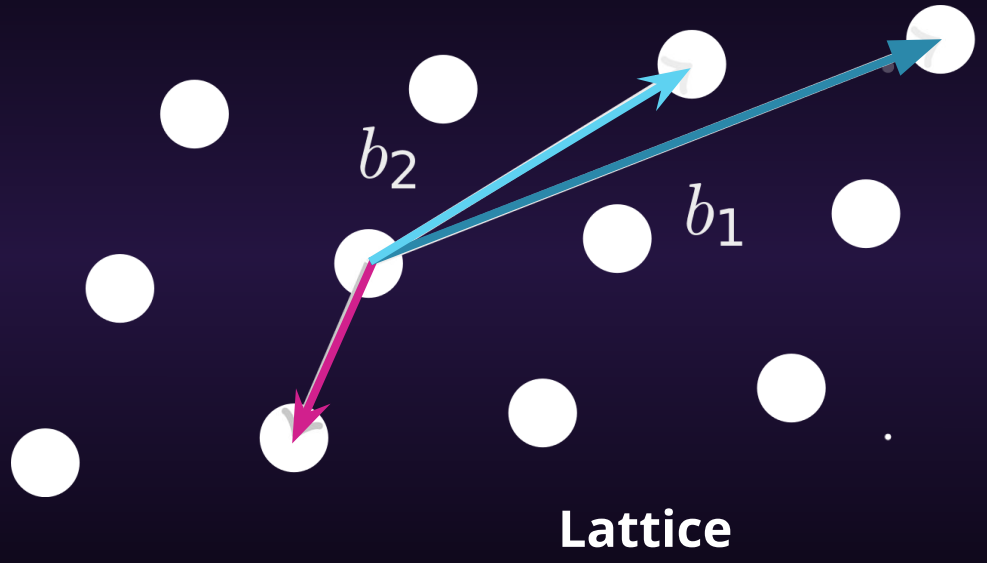
Efficiently solving SVP implies efficiently solving any lattice problem

SVP hardness

Tomorrow world cybersecurity

Shortest Vector Problem

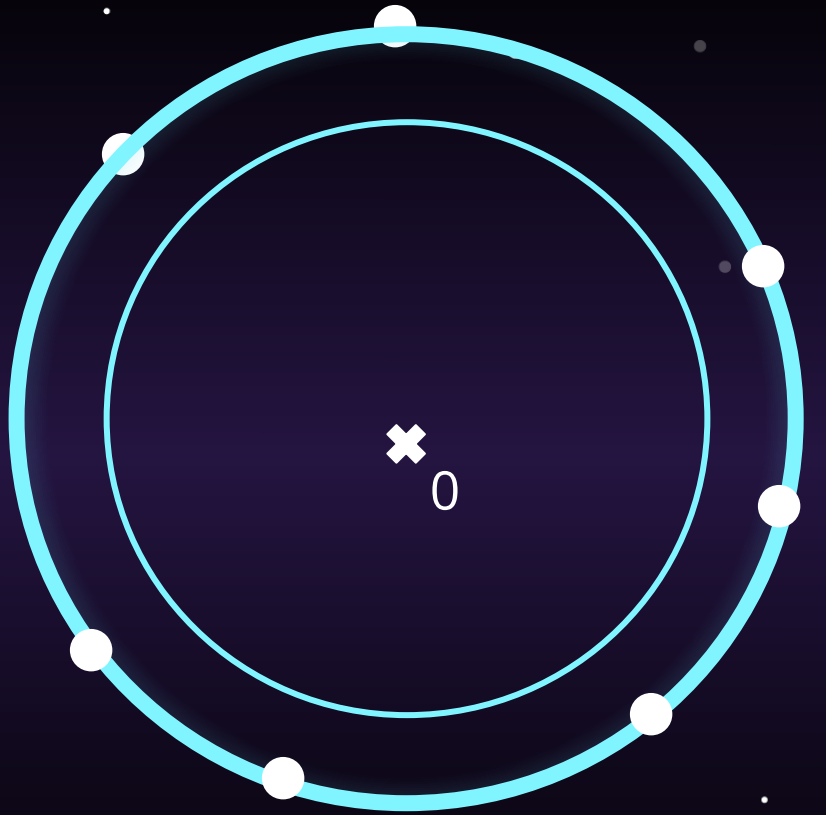
Given a basis of vectors, find its shortest (non-zero) integer linear combination.



Sieving
[NV08]

In: N lattice vectors of norm $\leq R$
$y < 1$

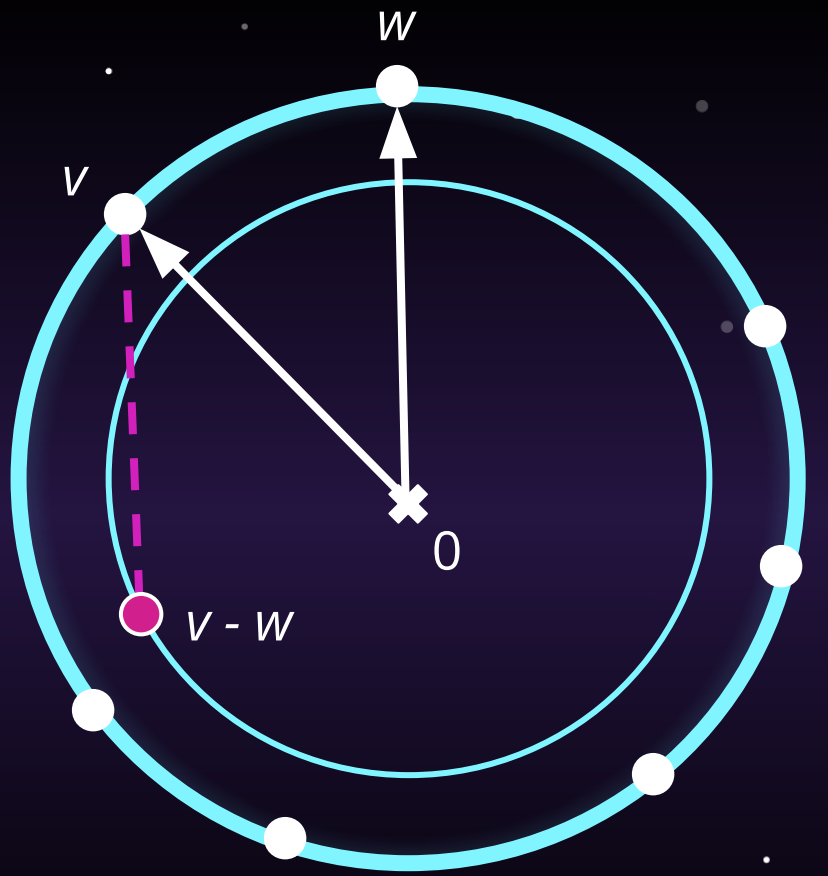
Out: N lattice vectors of norm $\leq y \cdot R < R$



Sieving [NV08]

In: N lattice vectors of norm $\leq R$
$y < 1$

Out: N lattice vectors of norm $\leq y \cdot R < R$

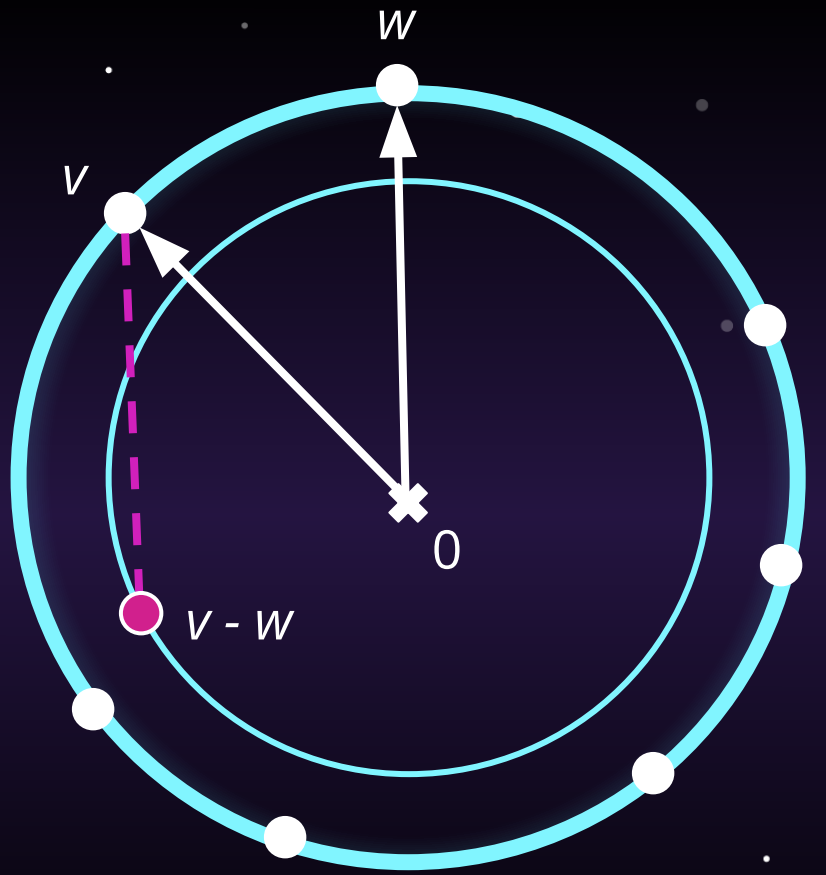


Sieving [NV08]

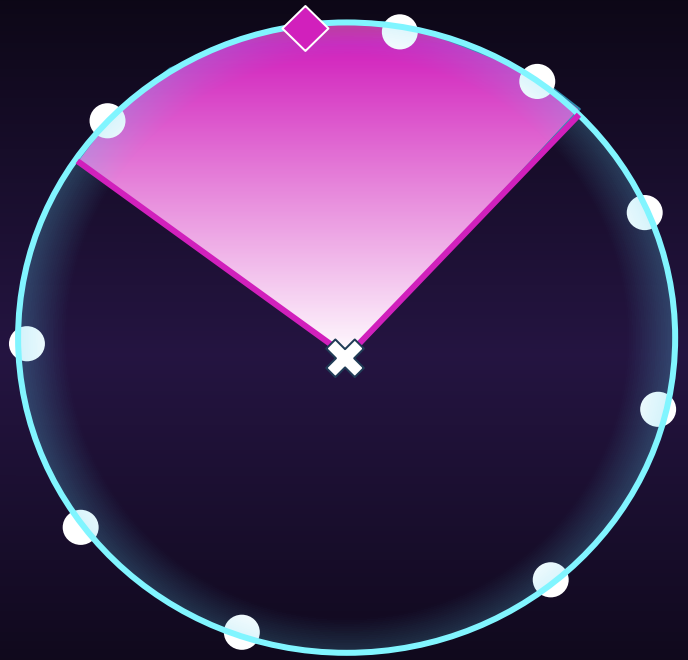
In: N lattice vectors of norm $\leq R$
$y < 1$

Out: N lattice vectors of norm $\leq y \cdot R < R$

Apply sieve steps until we find a short vector



Locality sensitive filters [BDGL16]

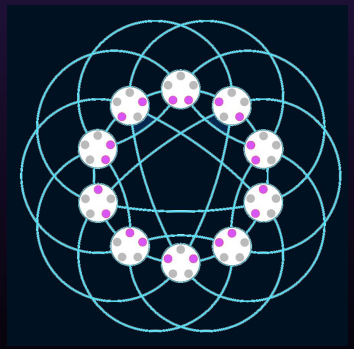


OUR ALGORITHM

1. Separate the sphere in large areas using **locality sensitive filters**

OUR ALGORITHM

1. Separate the sphere in large areas using **locality sensitive filters**



2. In each area, run **quantum random walks** to find all the pairs of close vectors.

COMPLEXITY

$2^{c\,d + o(d)}$, d dimension of the lattice

	CLASSIC	QUANTUM (previous)	QUANTUM (new)
Time exponent	0.293	0.265	0.257
Q. space & QRAM exp.	0	0.05	0.07

128 bits of security → 124

THANK YOU FOR YOUR ATTENTION!