# On the Dihedral Hidden Subgroup Problem

Oded Regev
Institute for Advanced Study

# Hidden Subgroup Problem

- Given a function which is constant and distinct on cosets of $H \leq G$, find H
- Solved for Abelian groups
- Also for certain non-Abelian groups [RöttelerBeth'98,HallgrenRussellTashma'00,GrigniSchulman VaziraniVazirani'01...]

- Still open for many groups. In particular:
  - Symmetric group
  - Dihedral group ($Z_N \rtimes Z_2$)

# Using Dihedral HSP

- Can be used to solve lattice problems [R'02]

$n^{2.5}$-unique Shortest Vector Problem

Dihedral HSP

# Solving Dihedral HSP

- Two approaches:

- Ettinger and Høyer '00
  - Reduction to "Period finding from samples"
- R '02
  - Reduction to average case subset sum

# Solving Dihedral HSP

- Idea of Ettinger and Høyer:
  - Reduce to “Hidden Translation on $Z_N$”:

    Given an oracle that outputs states of the form $|x\rangle + |x+d\rangle$ where x is arbitrary

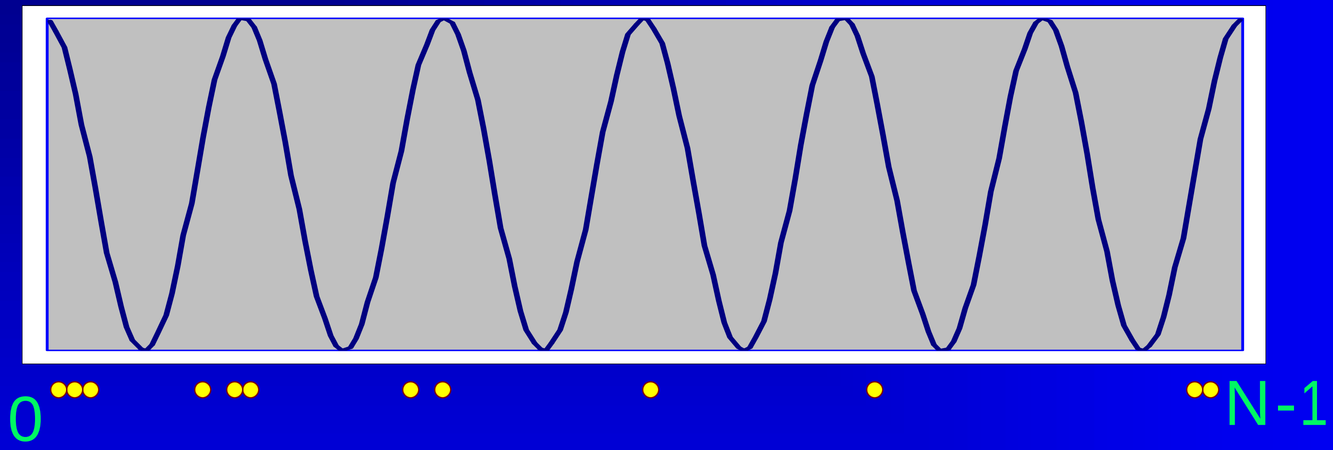
    and d is fixed, find d
  - Take the Fourier transform

$$\sum_{j=0}^{N-1} e^{2\pi i(jx/N)}(1+e^{2\pi i(jd/N)})|j\rangle$$

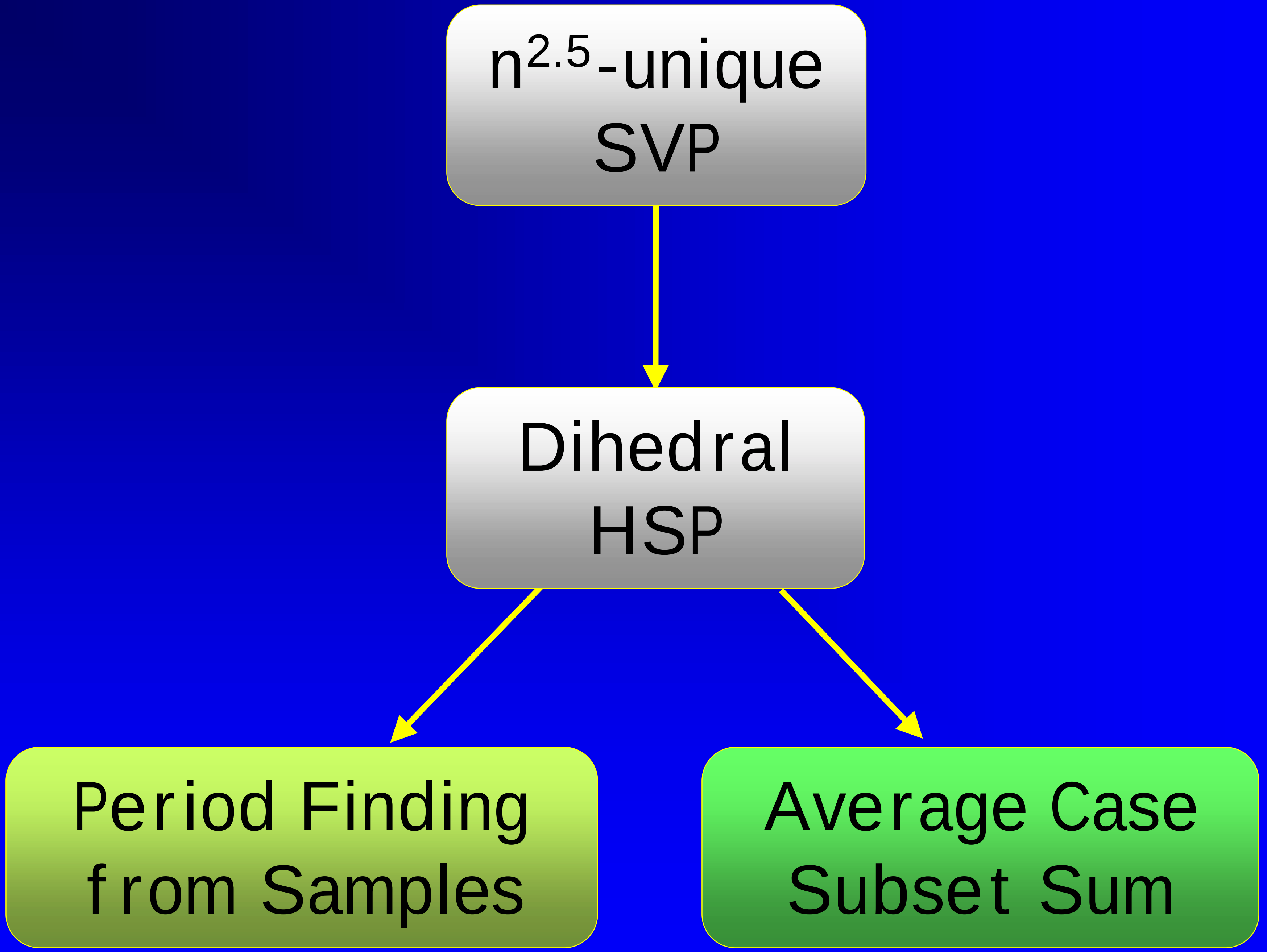
  - Measure

# Period Finding from Samples

- Find the period of the following ($\cos^2$) distribution by sampling:




- [EH] showed that there is enough information in a polynomial number of samples
- Open question in [EH]: is there an efficient solution to this problem?


$n^{2.5}$-unique SVP
Dihedral HSP
Period Finding from Samples
Average Case Subset Sum

# Our Results

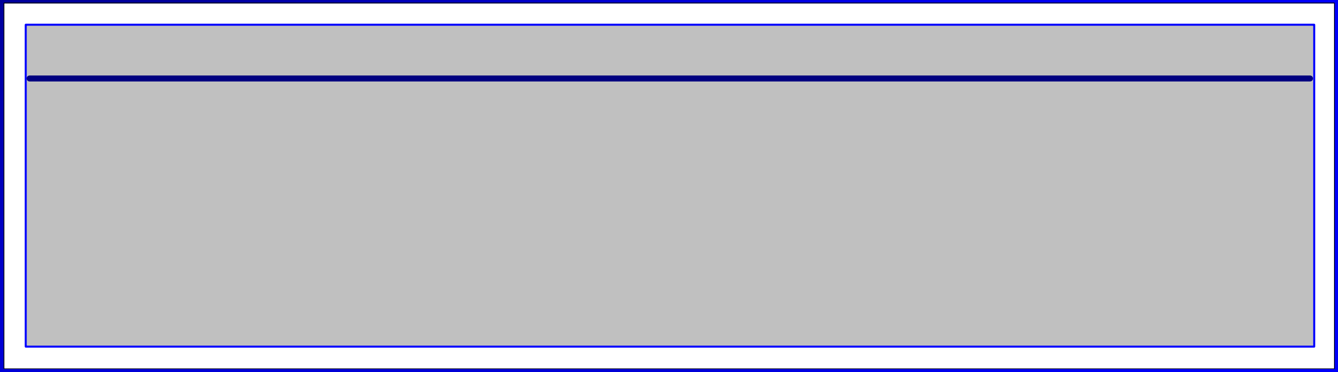
- “Period finding from samples” is hard

- Actually, our techniques also show that average case subset sum is hard
- Our results are based on one main tool

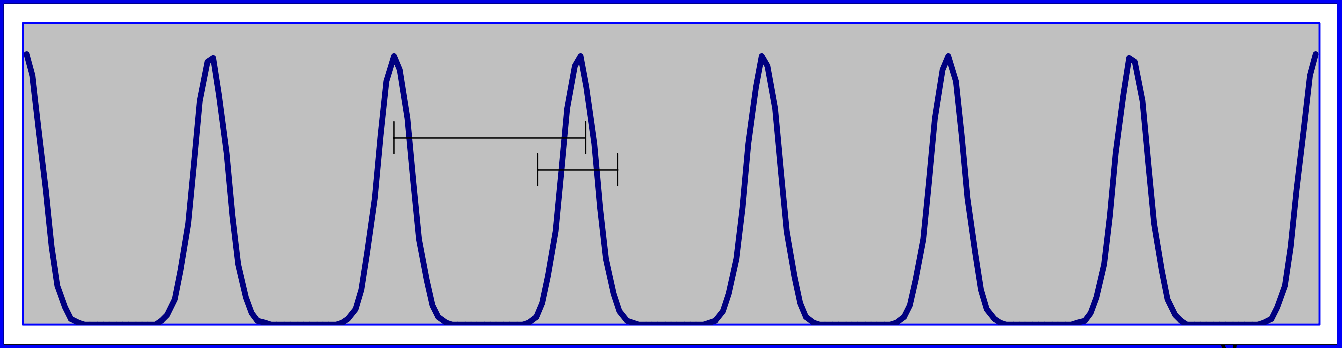
# Main Tool

- It is hard to distinguish between the distributions:

Uniform:




Wavy:



# Main Tool

- Theorem:

  The wavy distribution is indistinguishable from the uniform distribution

  (i.e., it is pseudorandom)

# Classical Uses of Main Tool

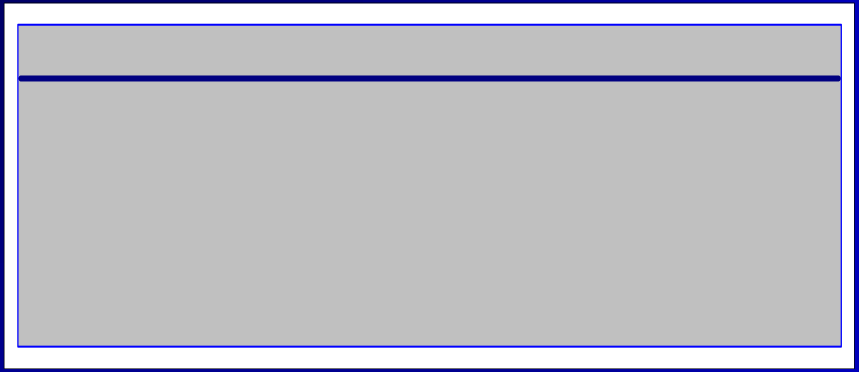
- New public key cryptosystem
  - Based on worst case hardness of $n^{1.5}$-unique-SVP
  - First major improvement of the Ajtai Dwork 1996 cryptosystem (which is $n^7$)
- Collision resistant hash function
  - First construction not based on Ajtai's iterative step
- This tool might have other uses

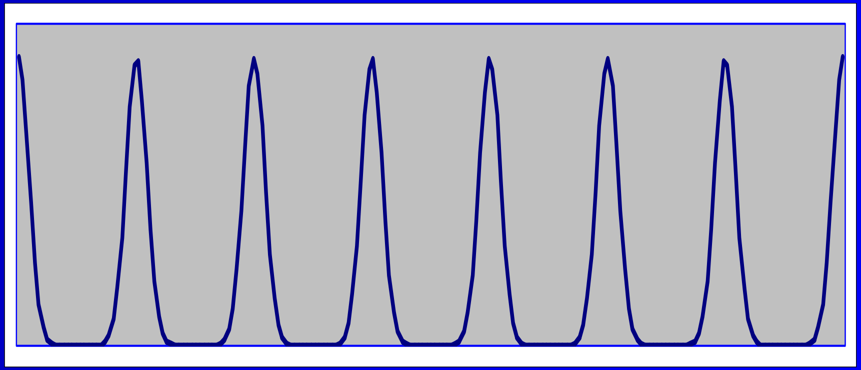
# Reducing the Main Tool to Period Finding from Samples

# Reduction

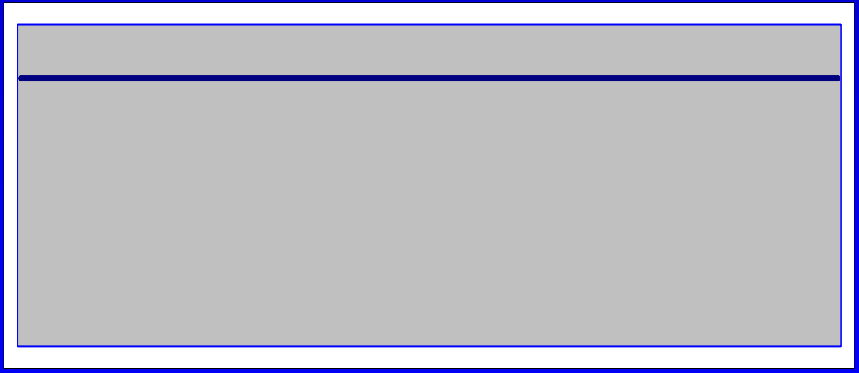
- Lemma: the $\cos^2$ distribution is pseudo-random

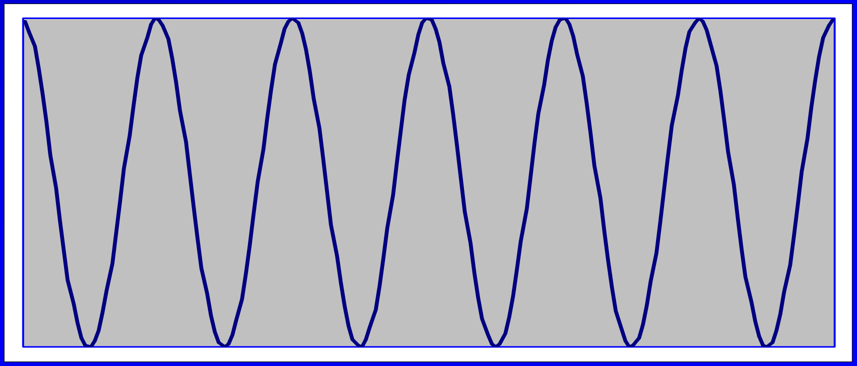
- Proof: Any distinguisher between $\cos^2$ and the uniform distribution implies a distinguisher between the wavy and uniform distribution





## Guess the period and add noise





# Reduction

- Corollary: finding the period of the $\cos^2$ distribution is hard

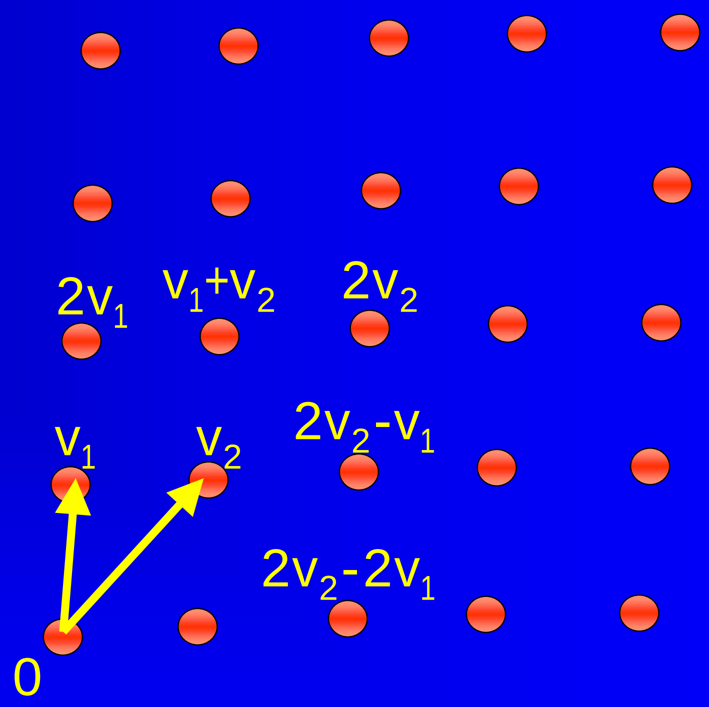
- Proof: Since all $\cos^2$ distributions look like uniform, they all look the same

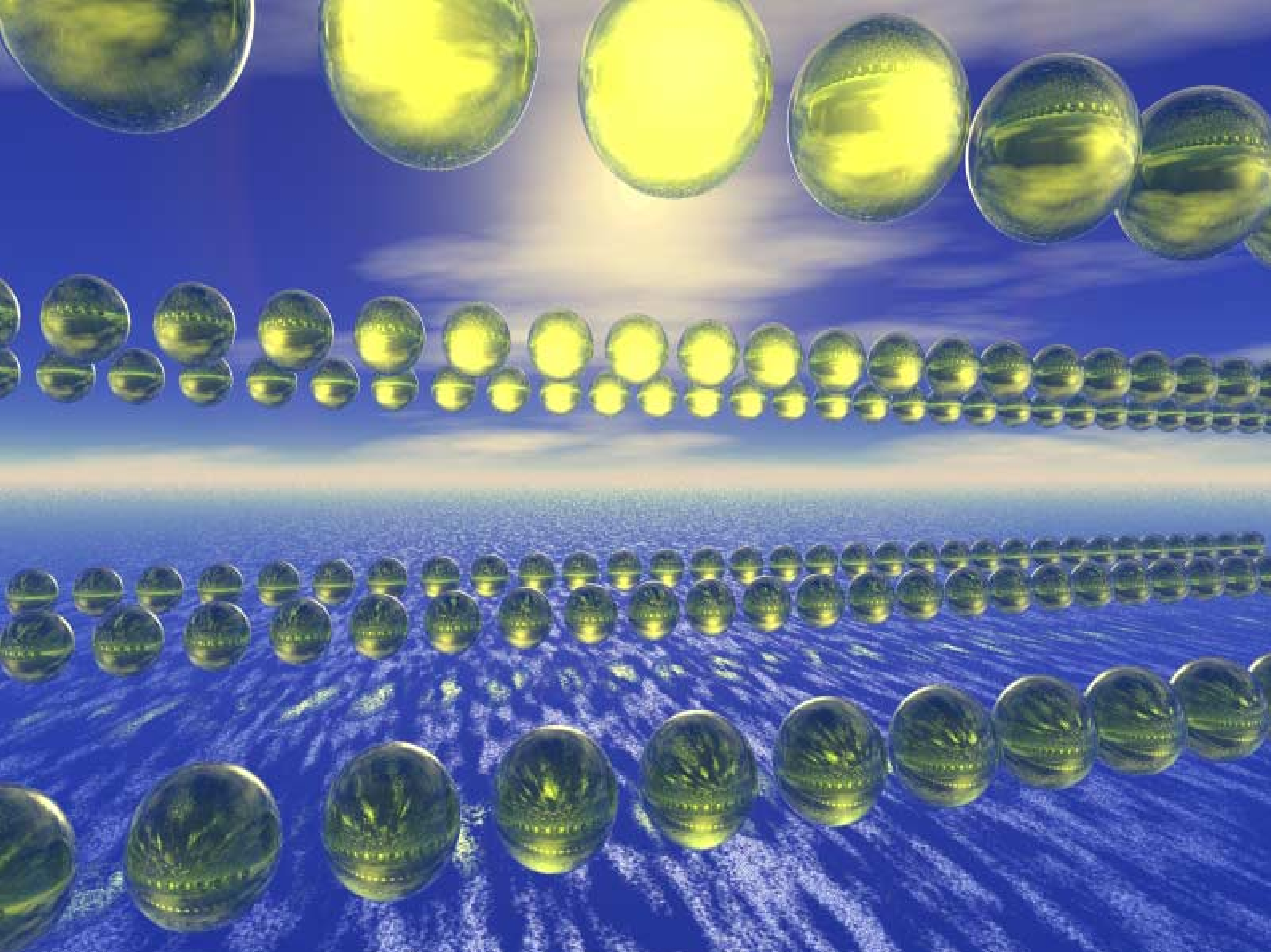
# Proof of the

# Main Tool

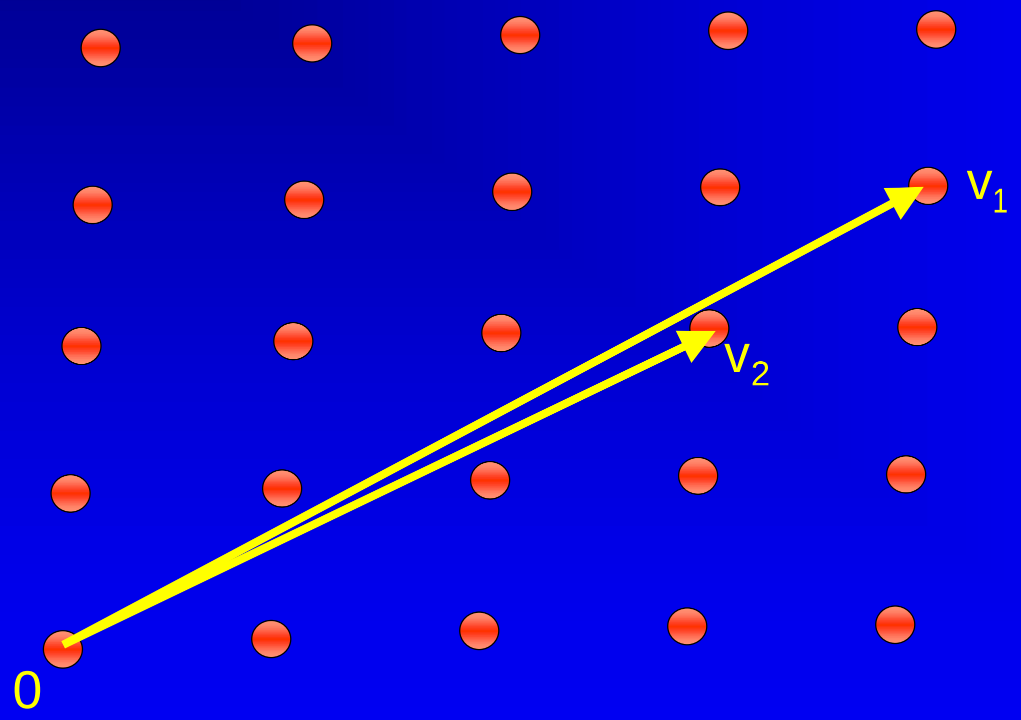
# Lattices

- Basis: $v_1,\ldots,v_n$ vectors in $R^n$
- The lattice is $a_1v_1+\ldots+a_nv_n$ for all *integer* $a_1,\ldots,a_n$.
- What is the shortest vector u ?



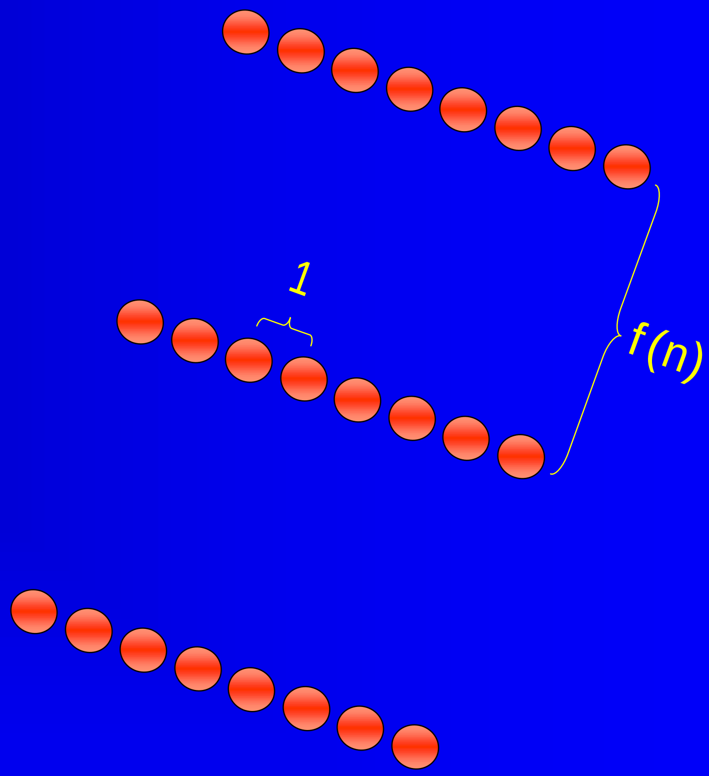


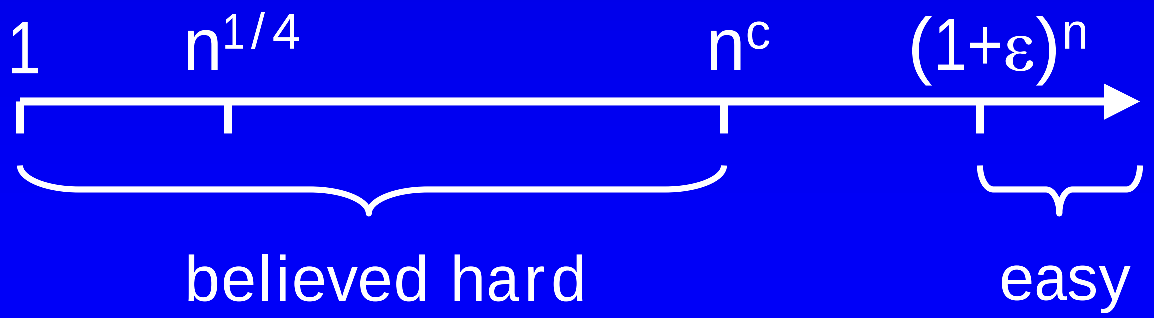
# Lattices – not so easy



# f(n)-unique-SVP (shortest vector problem)

- Promise: the shortest vector u is shorter by a factor of f(n)
- Algorithm for $(1+\varepsilon)^n$-unique SVP [Schnorr87]
- Believed to be hard for any $n^c$
- $n^{1/4}$-unique-SVP not NP-hard [Cai,Goldreich&Goldwasser98]

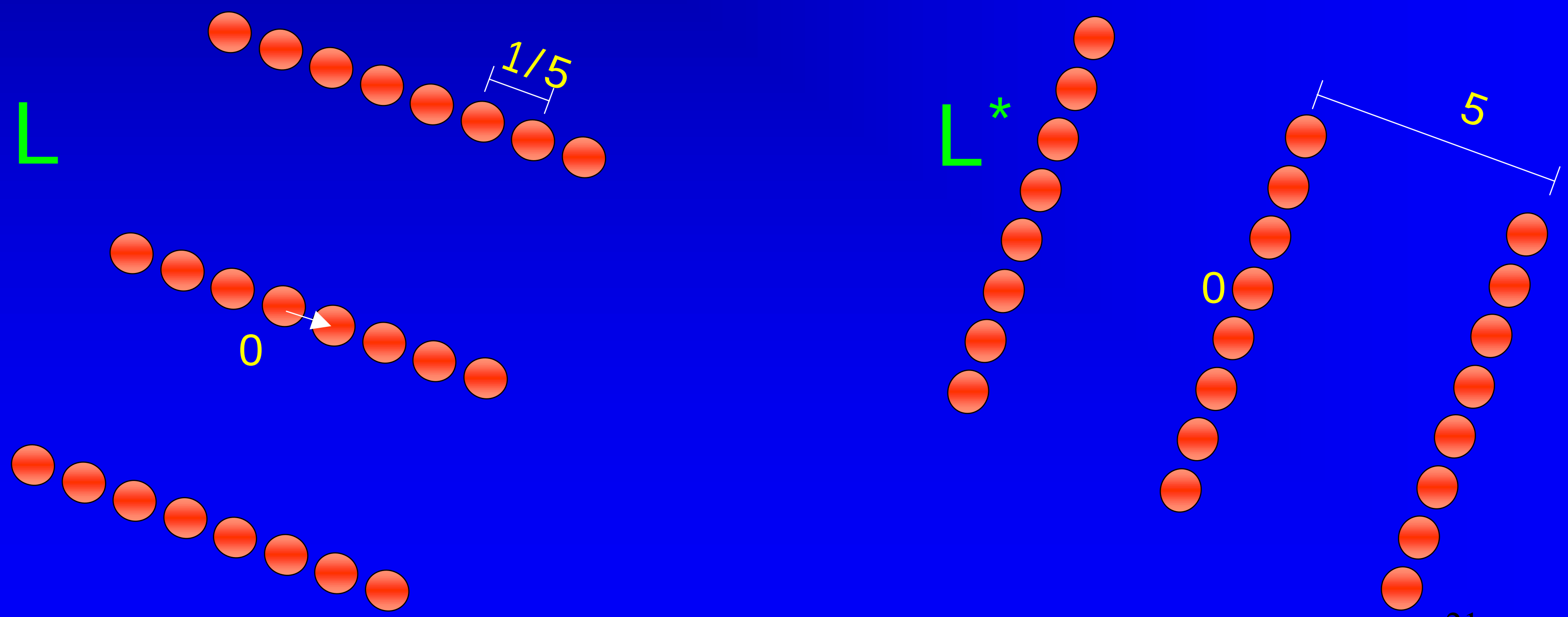


# Dual Lattice

- Given a lattice L, the dual lattice is

$$L^* = \{ x \mid \forall y \in L,\ \langle x,y \rangle \in \mathbb{Z} \}$$



# Techniques in the Proof

- Reduction to the decision problem
- Use of tools from harmonic analysis
- Reduction to one dimension

# Proof Outline

$n^{1.5}$-Unique-SVP

$\downarrow$

$n^{1.5}$-Decision-SVP

$\downarrow$

n-dim distributions

$\downarrow$

Main tool

# Decision-SVP

- Given a $n^{1.5}$ unique lattice, and a prime $p > n^{1.5}$
- Assume the shortest vector is:

$$u = a_1 v_1 + a_2 v_2 + \ldots + a_n v_n$$

- Decide whether $a_1$ is divisible by p

# The Reduction

- Idea: reduce the coefficients of the shortest vector

- If we find out that $p|a_1$ then we can replace the basis with $pv_1, v_2, \ldots, v_n$ .
- u is still in the new lattice:

$$u = (a_1/p) \bullet pv_1 + a_2v_2 + \ldots + a_nv_n$$

- The same can be done whenever $p|a_i$ for some i

# The Reduction

- But what if $p \nmid a_i$ for all $i$ ?
- Consider the basis $v_1, v_2 - v_1, v_3, \ldots, v_n$
- The shortest vector is

$$u = (a_1+a_2)v_1 + a_2(v_2-v_1) + a_3 v_3 + \ldots + a_n v_n$$

- So the first coefficient is $a_1+a_2$
- Similarly, we can get the coefficient to be $a_1 - \lfloor p/2 \rfloor a_2, \ldots, a_1 - a_2, a_1, a_1+a_2, \ldots, a_1 + \lfloor p/2 \rfloor a_2$
- One of them is divisible by p, so we choose it and continue

# Still a lot left

$n^{1.5}$-Unique-SVP

↓ ✓

$n^{1.5}$-Decision-SVP

↓

n-dim distributions

↓

Main tool

# Decision-SVP

- Given a $n^{1.5}$ unique lattice, and a prime $p>n^{1.5}$
- Assume the shortest vector is:

  $$u = a_1v_1+a_2v_2+\ldots+a_nv_n$$

- Decide whether $a_1$ is divisible by $p$

# n-dimensional distributions

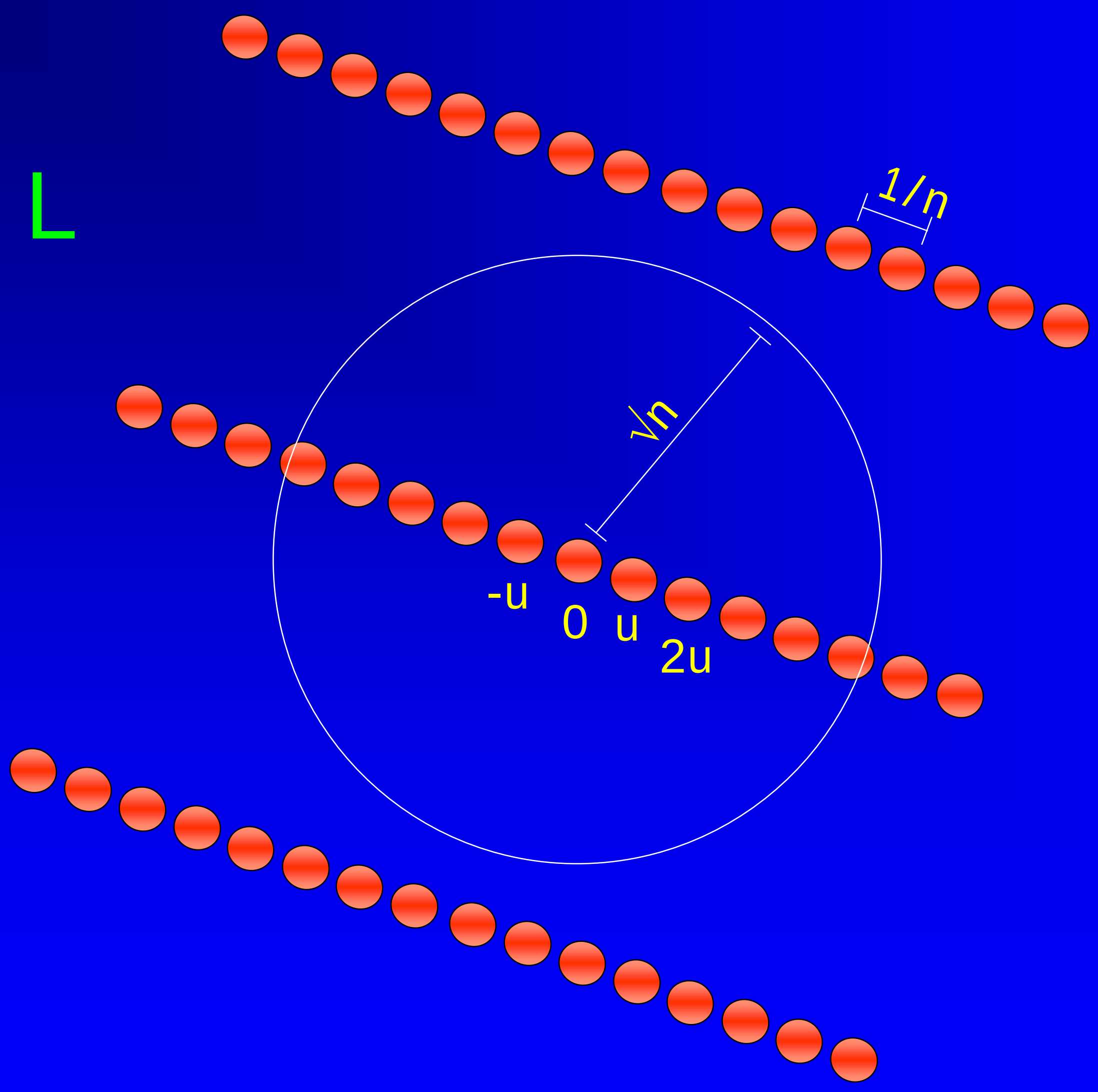
- Distinguish between the distributions:

?

Wavy

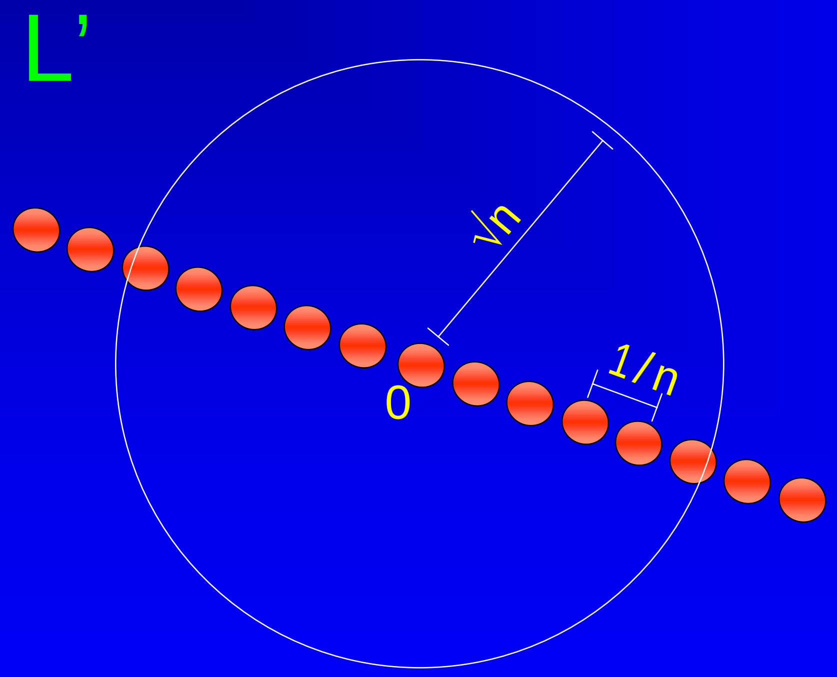
Uniform

# Decision-SVP



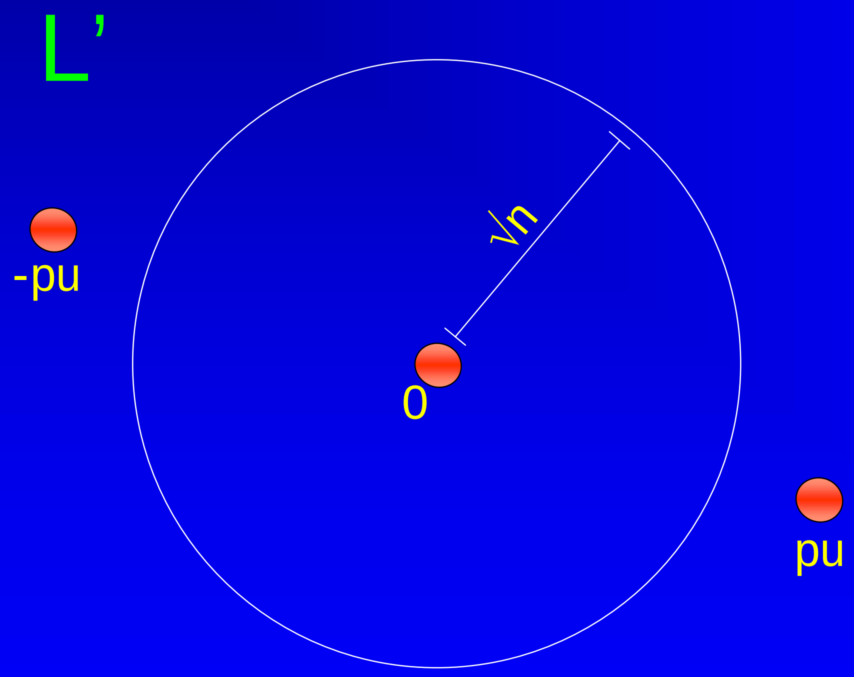
# The lattice L’

- Consider the lattice L’ spanned by $pv_1, v_2, \ldots, v_n$ :
- If $p | a_1$, then $u \in$ L’ :

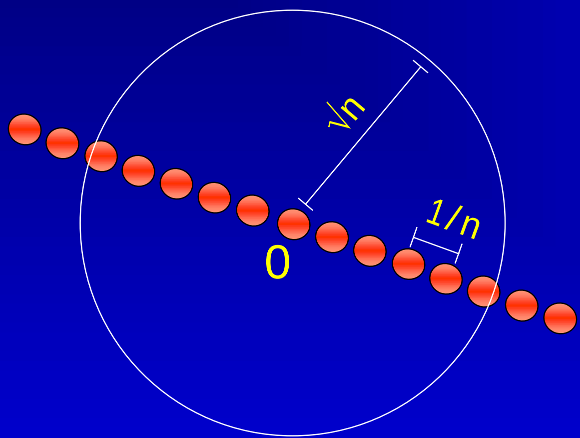
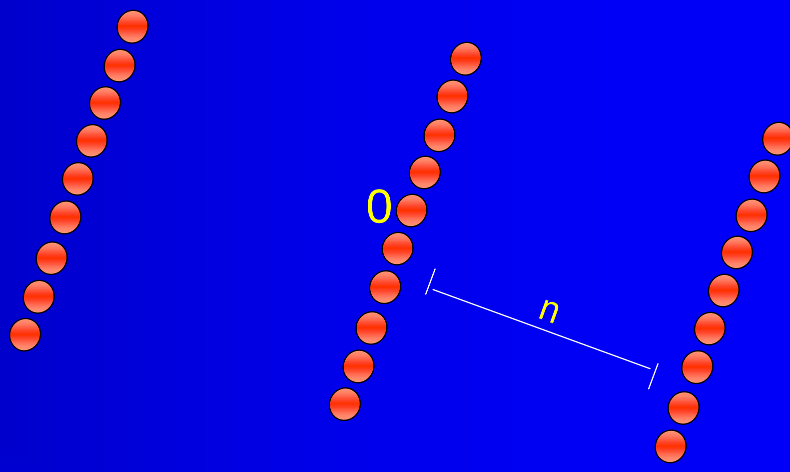
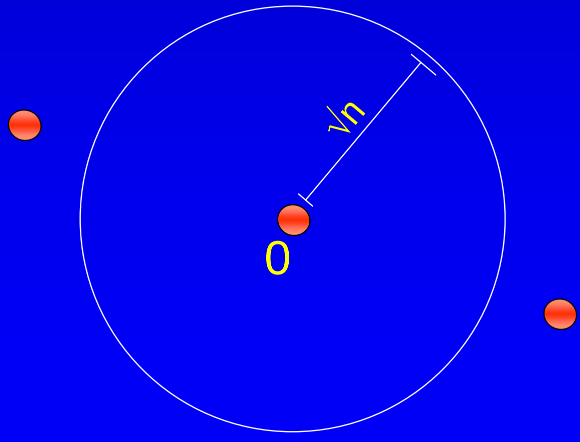
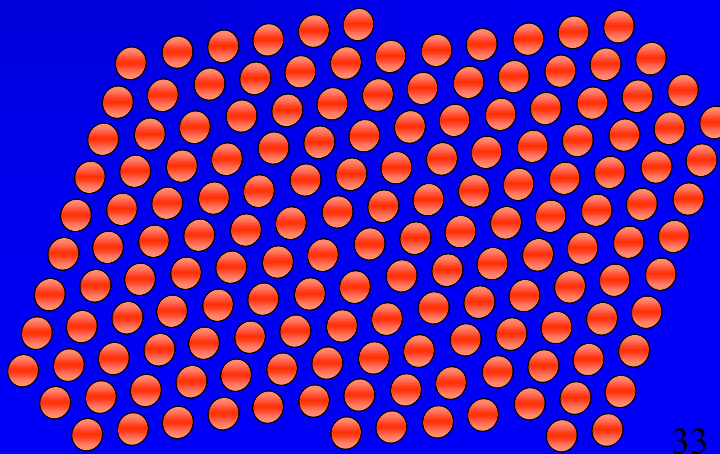


# The lattice L'

- Consider the lattice L' spanned by $pv_1, v_2, \ldots, v_n$ :
- If $p \nmid a_1$, then $u \notin$ L':



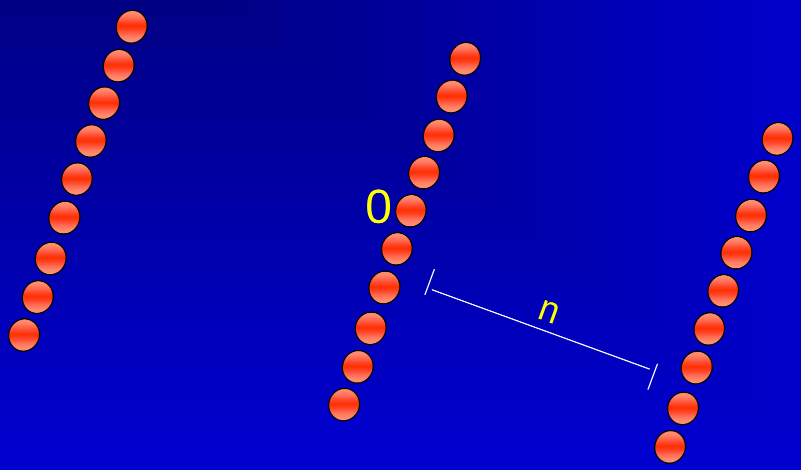
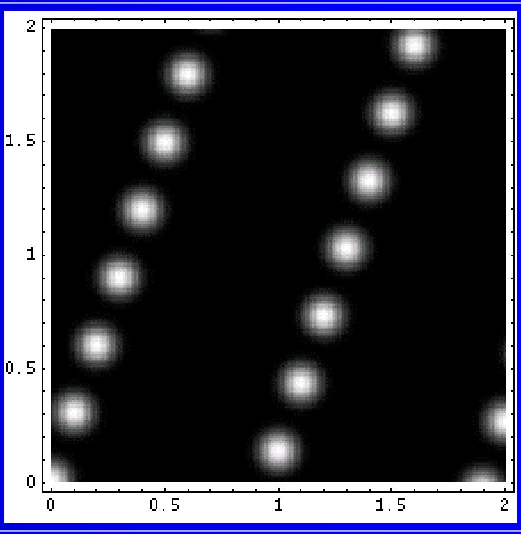
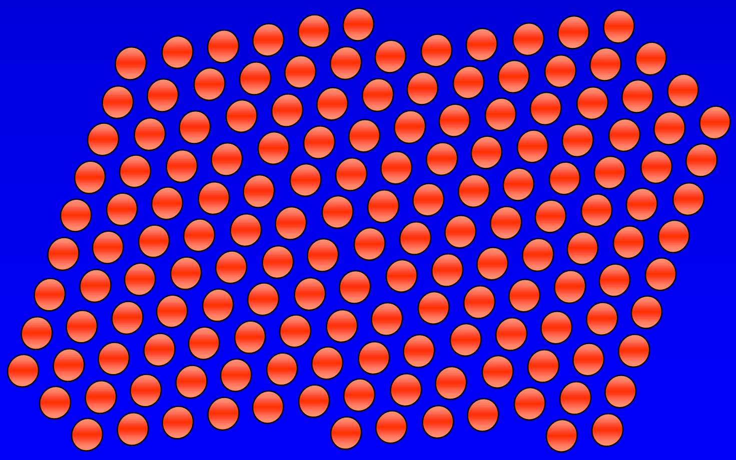
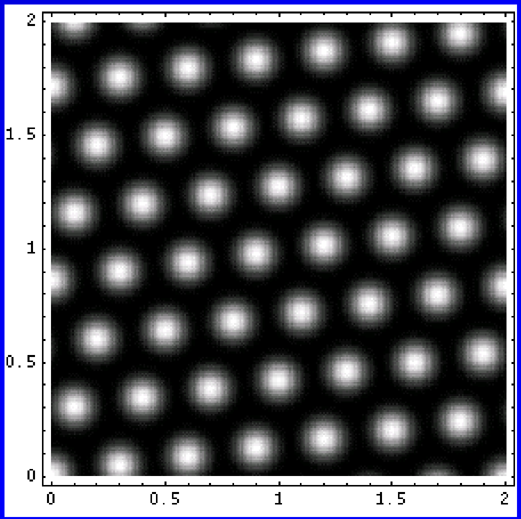
# L'* - the dual of L'

| | L' | L'* |
|---|---|---|
| $p \mid a_1$ |  |  |
| $p \nmid a_1$ |  |  |

# Creating the Distribution

- Choose a point randomly from $L'^*$
- Perturb it by a Gaussian of radius $\sqrt{n}$

# Creating the Distribution

| | L'* | L'*+ perturb |
|---|---|---|
| $p\mid a_1$ |  |  |
| $p\nmid a_1$ |  |  |

# Analyzing the Distribution

- Theorem: (using [Banaszczyk'93])

  The distribution obtained above depends only on the points in L' of distance $\sqrt{n}$ from the origin

  (up to an exponentially small error)

- Therefore, if $p|a_1$, then the distribution is determined by multiples of u and is therefore wavy on hyperplanes orthogonal to u
- If $p\nmid a_1$, then the distribution is determined by the origin and is therefore uniform

# Almost there

$n^{1.5}$-Unique-SVP

↓

$n^{1.5}$-Decision-SVP

↓

n-dim distributions

↓

Main tool

# n-dimensional distributions

- Distinguish between the distributions:

?

Wavy

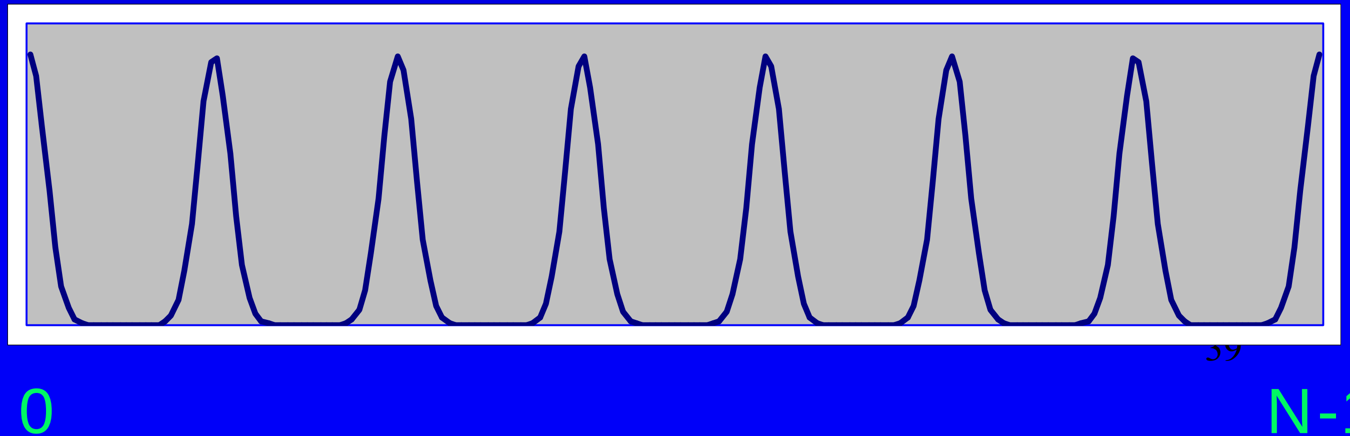
Uniform

# Main tool

- Distinguish between the distributions:

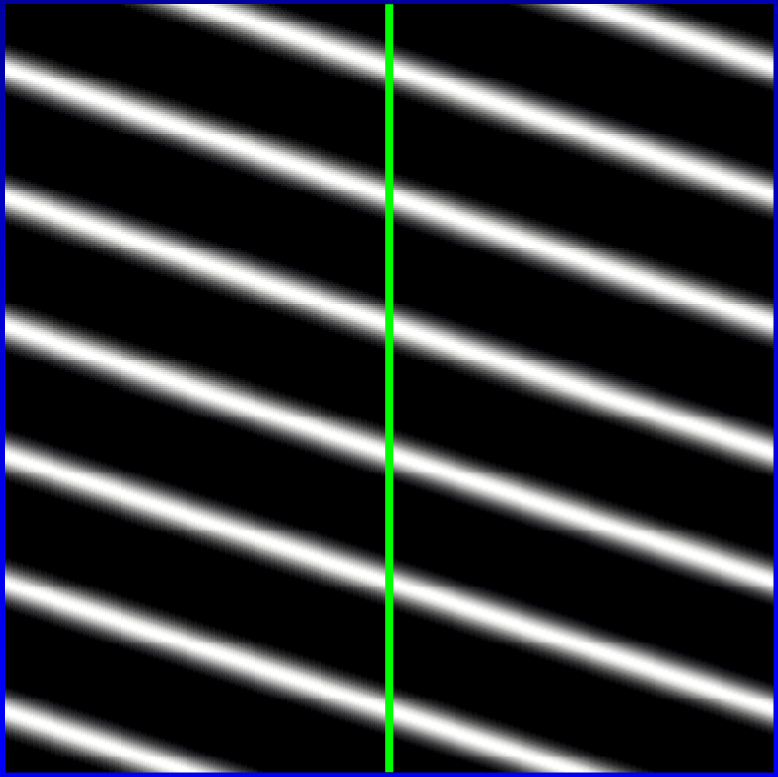
Uniform:

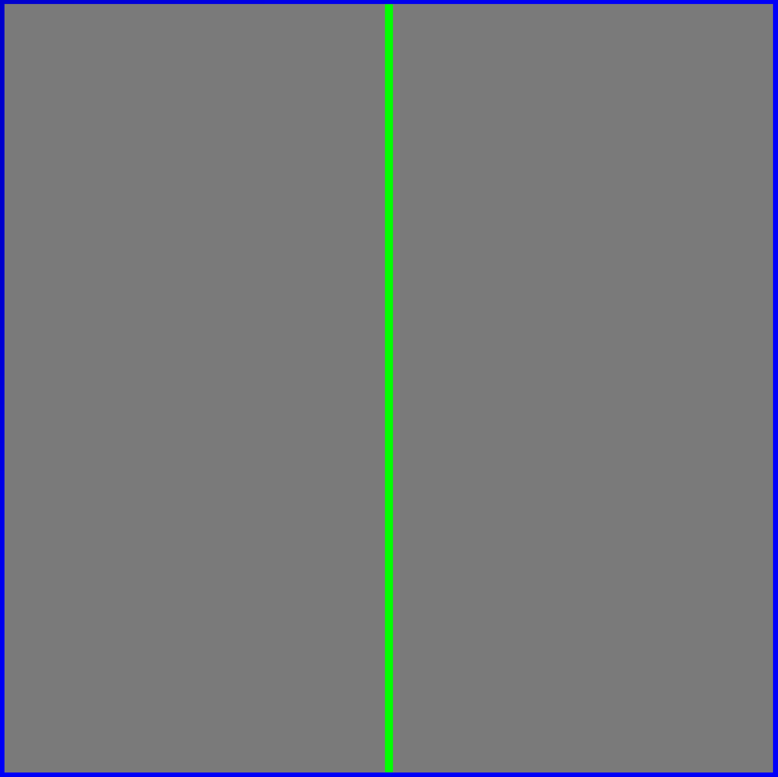

Wavy:



# Reducing to 1-dimension

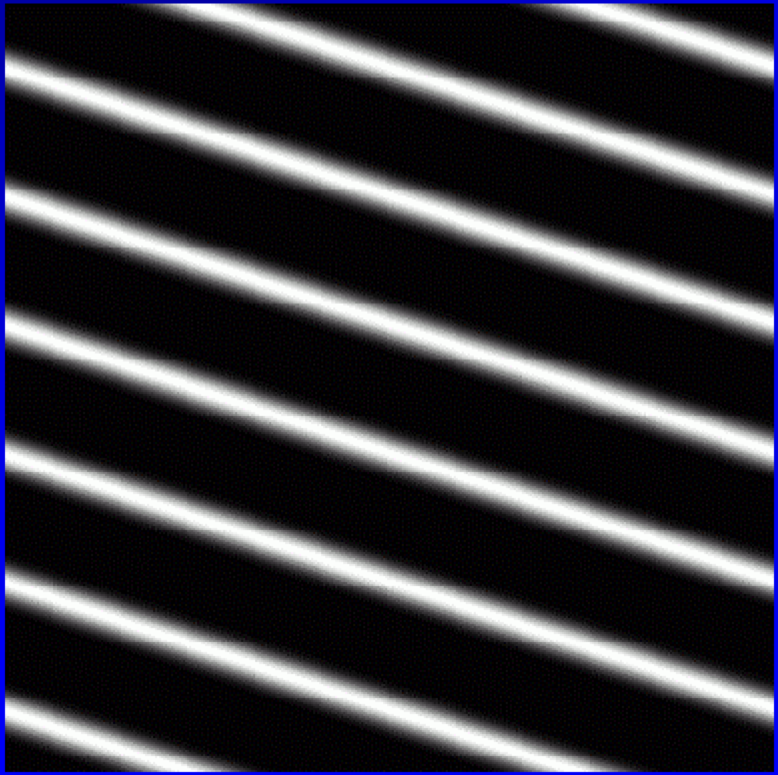
- First attempt: sample and project to a line





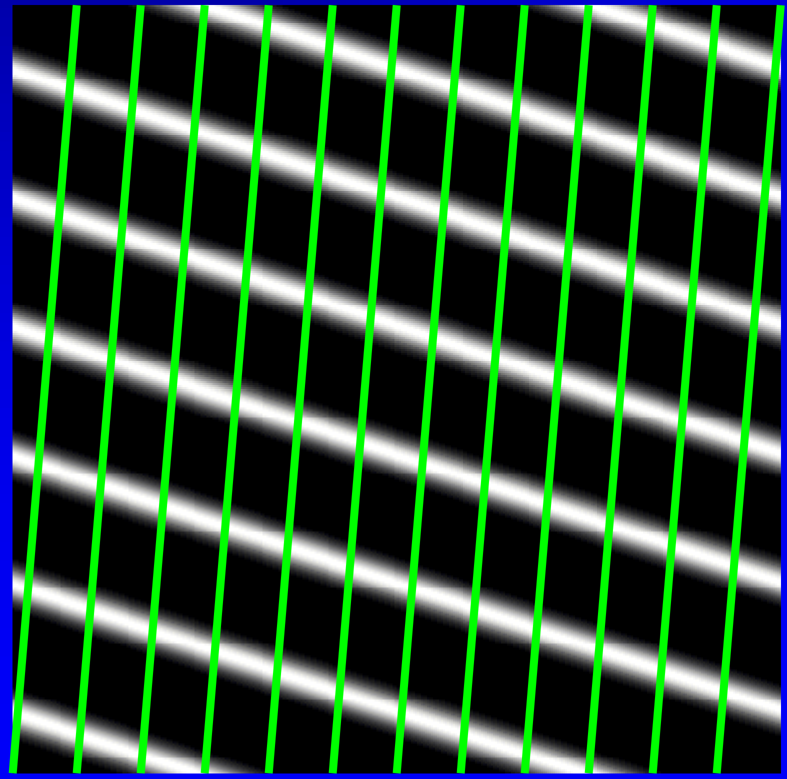
# Reducing to 1-dimension

- But then we lose the wavy structure!
- We can only project from points very close to the line



# Reducing to 1-dimension

- Solution: The distribution is periodic modulo the basic parallelepiped of L'*
- We construct a line that is 'dense' :



# Done

$n^{1.5}$-Unique-SVP

$n^{1.5}$-Decision-SVP

n-dim distributions

Main tool

# Conclusion

- We presented the proof of our main tool
- The main tool implies that the two attempts to solve dHSP fail
- Classically, it implies strong cryptographic constructions

# Open Questions

- Find other uses of the main tool
- Characterize algorithms that fail for the dHSP
- Find other groups with the same behavior