Efficient quantum algorithms for the principal ideal problem and class group problem in *arbitrary-degree* number fields

Fang Song
Institute for Quantum Computing
University of Waterloo

Joint work with
Jean-François Biasse (U. South Florida)

exponentially

Which problems have faster |quantum⟩ algorithms than classical algorithms?

∃ Poly-time quantum algorithms for:

- Factoring and discrete logarithm [Shor'94]
- Basic problems in computational algebraic number theory
  - Unit group in number fields
    - Constant degree [Hallgren'02'05, SchmidtVollmer'05]
    - **Arbitrary degree** [EHKS'14]
  - Principal Ideal Problem (PIP) & Class group problem
    - Constant degree number fields [H'02'05, SV'05]
    - This work: arbitrary degree!

Best known classical algorithms need (at least) sub-exponential time

Results and Implications

Principal ideal problem

Class group

Computing S-units

Norm equations,

Ray class group

...

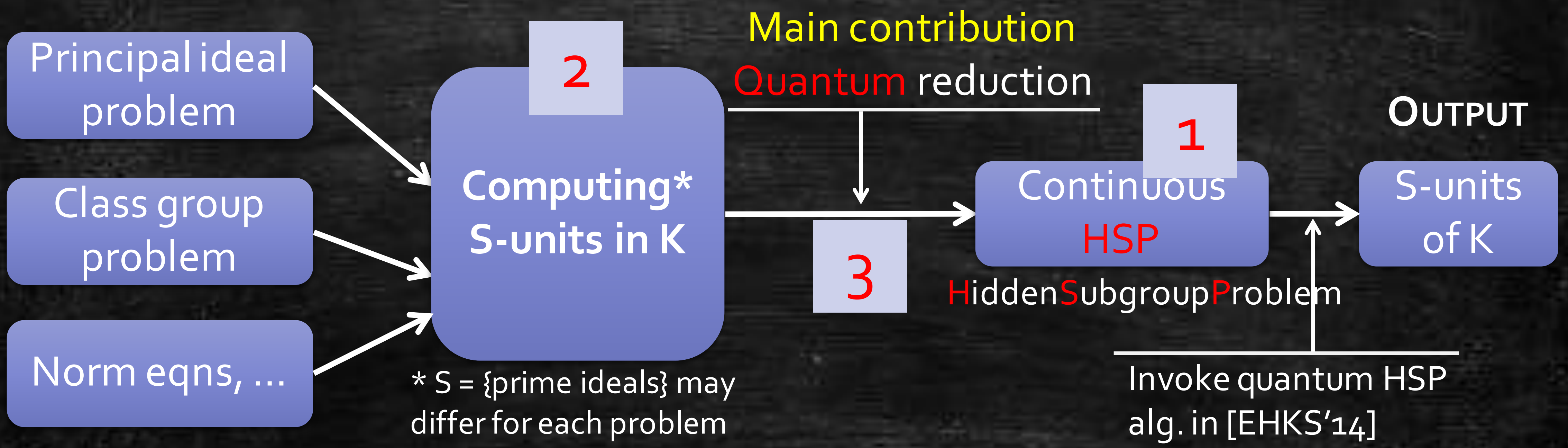
- Efficient quantum algorithms for several basic problems in number fields of arbitrary-degree
- Examples of quantum exponential speedup
- Minor: converting solutions into **compact representation**

Application: PIP algorithm can be used to break classical crypto

- Smart-V Fully Homomorphic Encryption, GargGH multilinear mapping scheme, ... [CGS14,CDPR15,BS15]
- Previously considered quantum-safe (based on ideal lattice problems instead of factoring/DL)

Outline of our quantum algorithms

INPUT: a degree n number field K



Hidden subgroup problem (HSP) framework

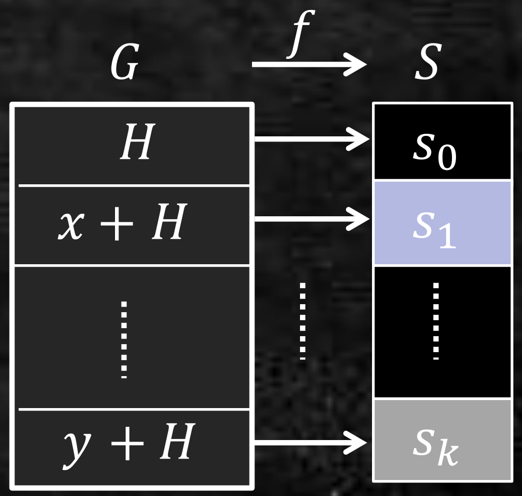
✓ Captures most quantum exponential speedup

- Standard Def.: HSP on finite group G

Given: oracle function $f: G \to S$, s.t. $\exists\, H \leq G$,

1. (Periodic on H) $x - y \in H \Rightarrow f(x) = f(y)$
2. (Injective on G/H) $x - y \notin H \Rightarrow f(x) \neq f(y)$

Goal: Find (hidden subgroup) H.



- *Uncountable* group $\mathbb{R}^m$: tricky due to **discretization!**
  - Some earlier defs. only suitable for small dimension m [H02,H05,SV05]
  - A "right" def. in high dimensions: continuous HSP [EHKS14]

Continuous HSP on $\mathbb{R}^m$

(unit vectors $|\cdot\rangle$ in a complex vector space)

Given $f: \mathbb{R}^m \to \{\text{quantum states}\}$, s.t.: $\exists$ discrete $H \leq \mathbb{R}^m$,

1. (Periodic) $x - y \in H \Rightarrow |f(x)\rangle = |f(y)\rangle$.
2. (Pseudo-injective) $x - y$ **far** from $H \Rightarrow |f(x)\rangle \perp |f(y)\rangle$
3. (Lipschitz continuitiy) $x - y$ **close** to $H \Rightarrow |f(x)\rangle \approx |f(y)\rangle$

$\min_{v \in H} ||x - y - v|| \geq r \Rightarrow \langle f(x)|f(y)\rangle \leq \epsilon.$

$|||f(x)\rangle - |f(y)\rangle|| \leq a \cdot ||x - y||.$

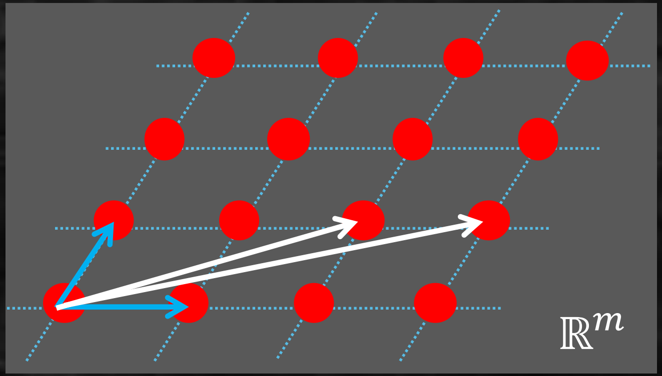
Goal: Find (hidden subgroup) H.

Theorem [EHKS14] $\exists$ efficient quantum algorithm solving continuous HSP on $\mathbb{R}^m$.

N.B.: H is a Lattice

$L(B) = \{a_1 v_1 + \cdots + a_m v_m : a_i \in \mathbb{Z}\} \subseteq \mathbb{R}^m$

- Basis $B: \{v_i \in \mathbb{R}^n : i = 1, \ldots, m\}$
- L has (infinitely) many bases



Interesting HSP instances

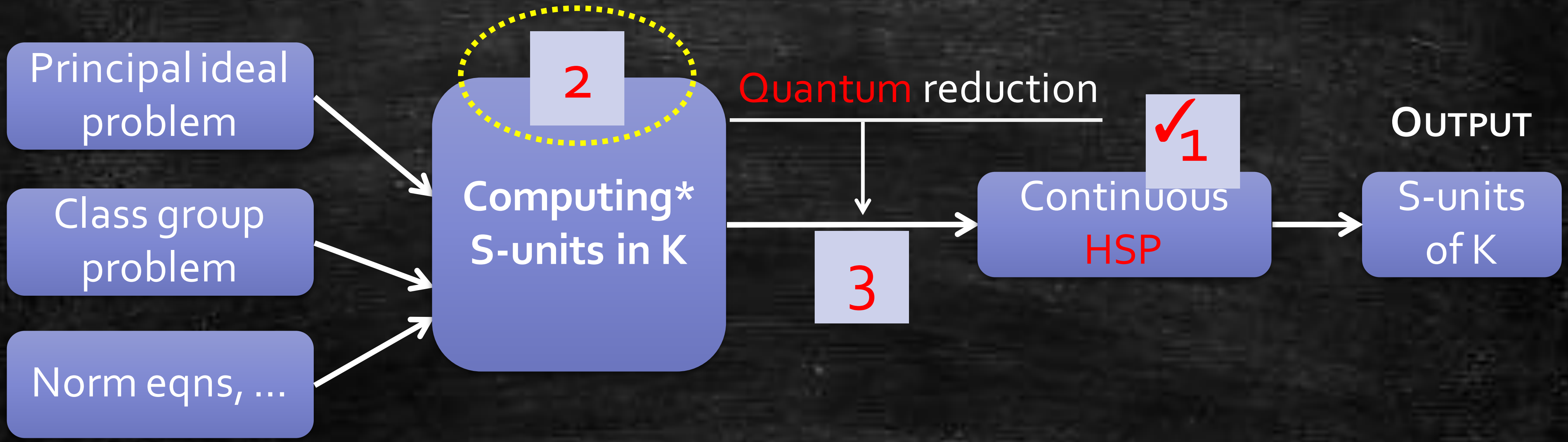
Computational Problems	HSP on G
Factoring	$\mathbb{Z}$
Discrete logarithm	$\mathbb{Z}_N \times \mathbb{Z}_N$
Unit group, PIP, class group, constant-degree fields	$\mathbb{R}^{\mathrm{const}}$
Unit group, arbitrary degree n	Continuous $\mathbb{R}^{O(n)}$
[This work] PIP, class group, arbitrary degree n	Continuous $\mathbb{R}^{O(n)}$
Graph isomorphism	Symmetric group
Unique shortest vector problem	Dihedral group

Abelian groups
∃ efficient quantum alg.

Non-abelian groups
Open question: ? ∃ efficient quantum alg.

Outline of our quantum algorithms

INPUT: a degree n number field K



Number Field Basics

- Number Field $K \subseteq \mathbb{C}$: Finite extension of $\mathbb{Q}$.
  - **Degree n**: dimension of K as vector space over $\mathbb{Q}$
- Ring of Integers $\mathcal{O}$: $K \cap$ Roots of monic irreducible poly $\mathbb{Z}[X]$. (e.g. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$)

Ex (Cyclotomic field). $\mathbb{Q}(\omega) = \{a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}: a_i \in \mathbb{Q}\}$. $\omega = e^{2\pi i/p}$, p prime.

  - $\mathcal{O} = \mathbb{Z}[\omega]$, $n = p - 1$

- Group of S-units U_S: $U_S := \{\alpha \in \mathcal{O}: \alpha\mathcal{O} = p_1^{v_1} \cdot \ldots \cdot p_k^{v_k} \text{ for some } v_i \in \mathbb{Z}\}$
  - $S = \{p_1, \ldots, p_k\}$ a set of prime ideals
  - i.e. $\alpha \in \mathcal{O}$, s.t. $\alpha\mathcal{O} \cdot \Pi p_i^{-v_i} = \mathcal{O}$
- Special case: Unit group U
  - $S = \emptyset \Rightarrow U_\emptyset = U = \{$invertible elements in $\mathcal{O}.\}$
  - i.e. $\alpha \in \mathcal{O}$, s.t. $\alpha\mathcal{O} = \mathcal{O}$

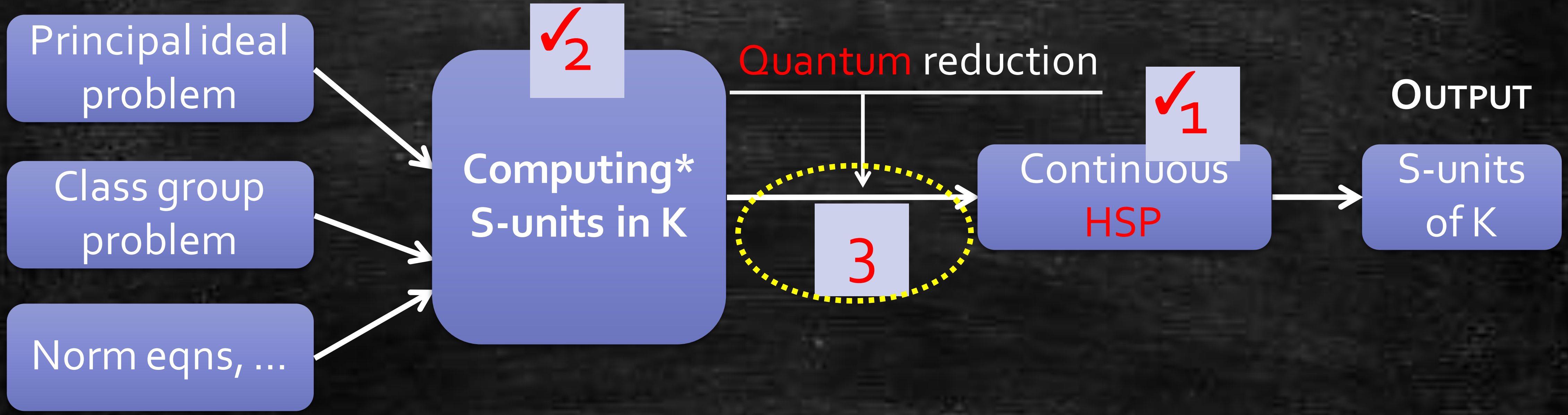
Principal Ideal Problem

Given ideal $I \subseteq \mathcal{O}$ decide if $I = \alpha\mathcal{O}$ and find α if so.

- Classical alg's: $\exp(n)\exp(|\mathcal{O}|)$
- Quantum alg's: $\exp(n)$ poly$(|\mathcal{O}|)$
- This work: poly(n) poly$(|\mathcal{O}|)$

Outline of our quantum algorithms

INPUT: a degree n number field K



Reducing S-units to Continuous HSP

[EHKS14]

$$\begin{tikzcd} \text{Units } U \arrow[d, "\phi"', "m = O(n)"] \\ \Lambda \leq \mathbb{R}^m \arrow[d, "f_c"] \\ \{\text{lattices in } \mathbb{R}^n\} \arrow[d, "f_q"] \\ \{\text{quantum states}\} \end{tikzcd}$$

HSP instance
$f = f_q \circ f_c$

This work $S = \{p_1, \dots, p_k\}$

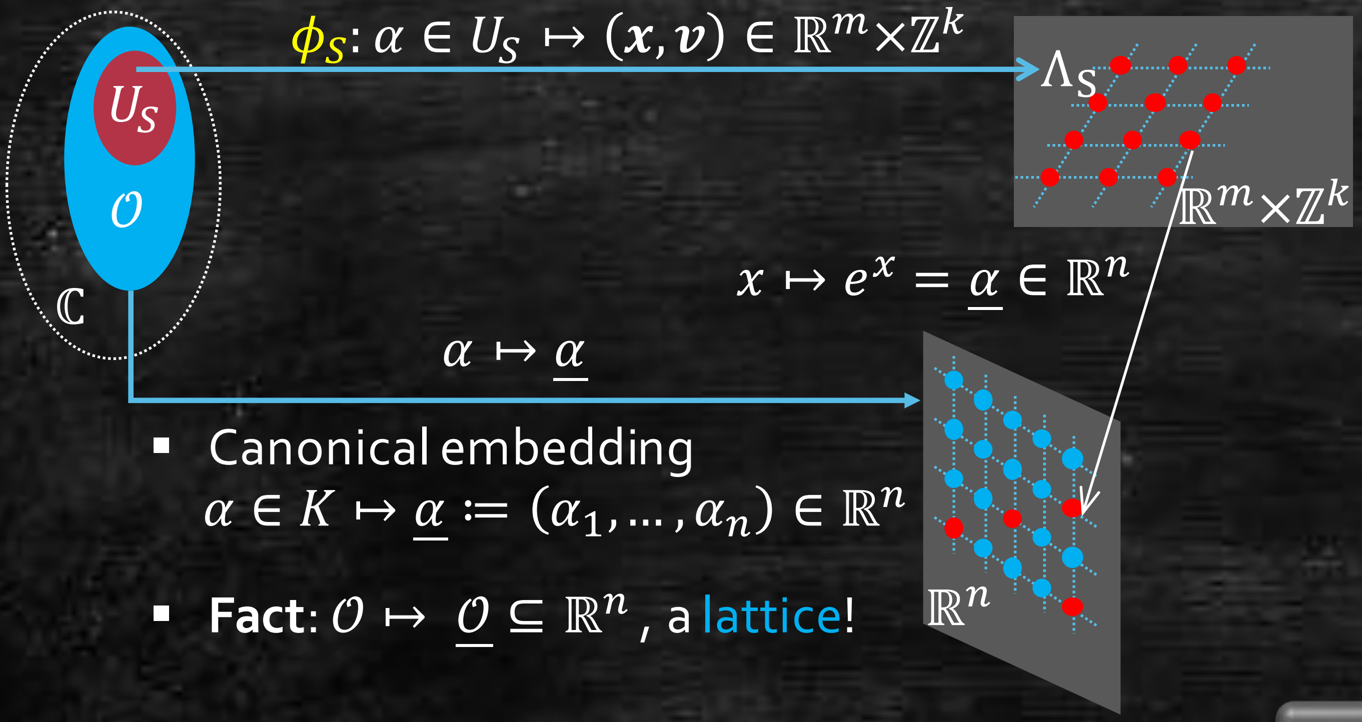
$$\begin{tikzcd} \text{S-Units } U_S \arrow[d, "\phi_S"'] \\ \Lambda_S \leq \mathbb{R}^m \times \mathbb{Z}^k \arrow[d, "g_c"'] \\ \{\text{lattices in } \mathbb{R}^n\} \arrow[d, "f_q"'] \\ \{\text{quantum states}\} \end{tikzcd}$$

HSP instance∗
$f_S = f_q \circ g_c$

∗ f_S can further be turned into an f_S' on $\mathbb{R}^{m+k}$

Identifying S-units as a subgroup

$\alpha \in U_S \Leftrightarrow \alpha\mathcal{O} \cdot \Pi_{i=1}^{k} p_i^{-v_i} = \mathcal{O}, v_i \in \mathbb{Z}$



- Canonical embedding
  $\alpha \in K \mapsto \underline{\alpha} := (\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n$
- **Fact**: $\mathcal{O} \mapsto \underline{\mathcal{O}} \subseteq \mathbb{R}^n$, a lattice!

Fact: $\Lambda_S := \phi_S(U_S) \subseteq \mathbb{R}^m \times \mathbb{Z}^k$ is a full-rank lattice!

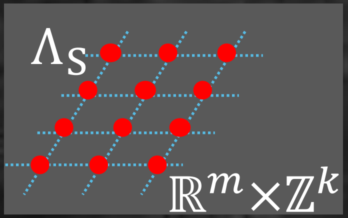
Characterization of S-units

- $L_x := e^x \underline{\mathcal{O}} = \begin{bmatrix} e^{x_1} & & \\ & \ddots & \\ & & e^{x_m} \end{bmatrix} \cdot \underline{\mathcal{O}}$
- $L_v := \underline{\Pi_{i=1}^{k} p_i^{-v_i}} \subseteq \underline{\mathcal{O}}$

$\rightarrow (x, v) \in \Lambda_S \Leftrightarrow L_x \cdot L_v = \underline{\mathcal{O}}$

Defining hiding function: classical part

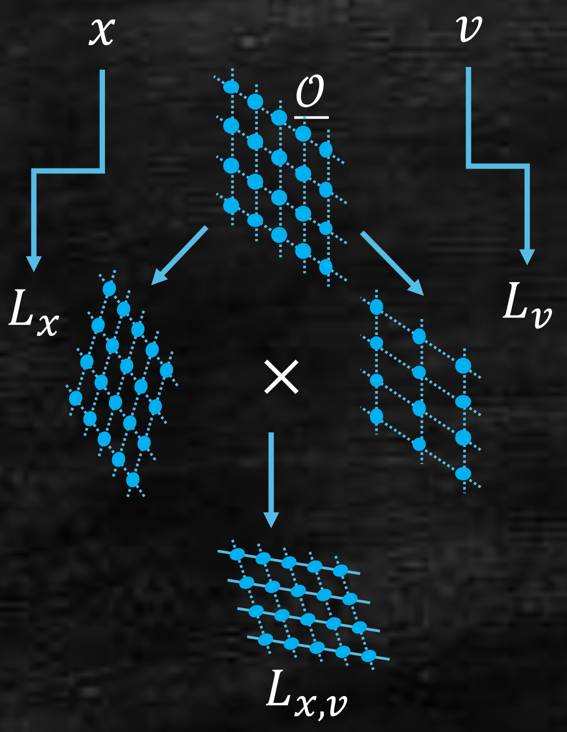
$(x, v) \in \Lambda_S \Leftrightarrow L_x \cdot L_v = \underline{\mathcal{O}}$



- $L_x \coloneqq \begin{bmatrix} e^{x_1} & & \\ & \ddots & \\ & & e^{x_n} \end{bmatrix} \cdot \underline{\mathcal{O}}$
- $L_v \coloneqq \underline{p_1^{-v_1} \cdots p_k^{-v_k} \mathcal{O}}$

$$(x, v) \in \mathbb{R}^m \times \mathbb{Z}^k \xrightarrow{g_c} L_{x,v} \subseteq \mathbb{R}^n$$

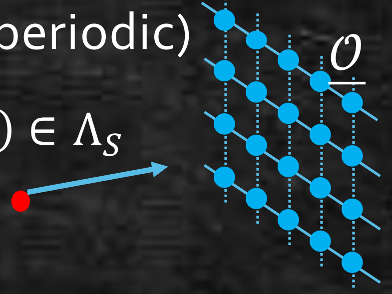
$$x \in \mathbb{R}^m \xrightarrow{f_c} L_x \subseteq \mathbb{R}^n$$



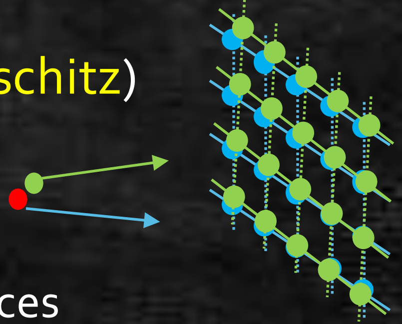
- $g_c(x, v) = L_x \cdot L_v$

1. (Λ_S-periodic)

$(x, v) \in \Lambda_S$

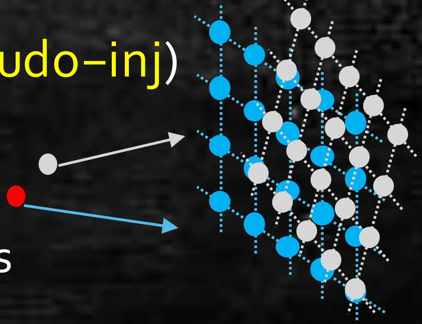


2. (Lipschitz)



"**Small**" shift in inputs
→ "**Similar**" output lattices

3. (Pseudo–inj)



"**Big**" shift in inputs
→ Small–overlap lattices

Completing the HSP reduction

S-Units U_S

$\downarrow \phi_S$

$\Lambda_S \leq \mathbb{R}^m \times \mathbb{Z}^k$

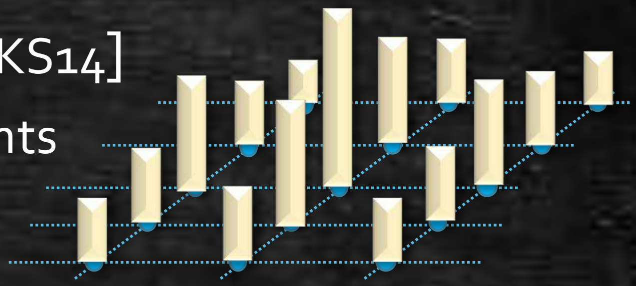
$\downarrow g_c$

$\{\text{lattices in } \mathbb{R}^n\}$

$\downarrow f_q$

$\{\text{quantum states}\}$

- **Issue**: no unique representation for lattices in $\mathbb{R}^n$
  - $L_{x,v} = L_{x',v'}$ same lattice, but $g_c(x,v)$ and $g_c(x',v')$ output different bases.
- **Fix**: encode lattices in quantum states [EHKS14]
  - $f_q: L \mapsto |L\rangle$ = superposition over "all" lattice points



$\boxed{\Rightarrow \langle L'|L\rangle \propto L \cap L'}$

Theorem. $f_S = f_q \circ g_c$ is a continuous HSP instance w. period Λ_S.

- (Lipschitz) $(x,v)-(x',v')$ close to $\Lambda_S \xrightarrow{g_c} L \approx L' \xrightarrow{f_q} \langle L'|L\rangle \approx 1$
- (P-Inj.) $(x,v)-(x',v')$ far from $\Lambda_S \xrightarrow{g_c} L$ & L' small overlap $\xrightarrow{f_q} \langle L'|L\rangle$ small

- What's missing: efficiently implement f_S
  - ! Computing g_c delicate: e^x doubly-exp. large & precision loss

➔ Invoke quantum HSP algorithm [EHKS14], we find Λ_S efficiently!

Summary

Number field K of arbitrary degree n

PIP, class group, … → Computing S-units in K → Continuous HSP → Solutions

- Future Directions
  - Solving more problems in the continuous HSP framework
  - Quantum attacks on other (ideal) lattice cryptosystems
  - Better quantum algorithms for Non-abelian HSP?

Thank you!