Post-Quantum Security of Lattice-based Cryptosystems

Rajendra Kumar

TQC 2025 Bengaluru, India

Lattices

Lattices

- L is a discrete set of vectors in $\mathbb{R}^m$.

Lattices

- L is a discrete set of vectors in $\mathbb{R}^m$.

- Specified by a basis $\vec{b}_1, \vec{b}_2, \cdots, \vec{b}_n \in \mathbb{R}^m$, linearly independent vectors.

Lattices

- L is a discrete set of vectors in $\mathbb{R}^m$.

- Specified by a basis $\vec{b}_1, \vec{b}_2, \cdots, \vec{b}_n \in \mathbb{R}^m$, linearly independent vectors.

- $L = \left\{ z_1\vec{b}_1 + z_2\vec{b}_2 + \cdots + z_n\vec{b}_n \mid \forall i \in [n], z_i \in \mathbb{Z} \right\}$

Lattices

- L is a discrete set of vectors in $\mathbb{R}^m$.

- Specified by a basis $\vec{b}_1, \vec{b}_2, \cdots, \vec{b}_n \in \mathbb{R}^m$, linearly independent vectors.

- $L = \left\{ z_1\vec{b}_1 + z_2\vec{b}_2 + \cdots + z_n\vec{b}_n \mid \forall i \in [n], z_i \in \mathbb{Z} \right\}$

- Lattice: set of vectors formed by integer linear combinations.

Lattices

- L is a discrete set of vectors in $\mathbb{R}^m$.

- Specified by a basis $\vec{b}_1, \vec{b}_2, \cdots, \vec{b}_n \in \mathbb{R}^m$, linearly independent vectors.

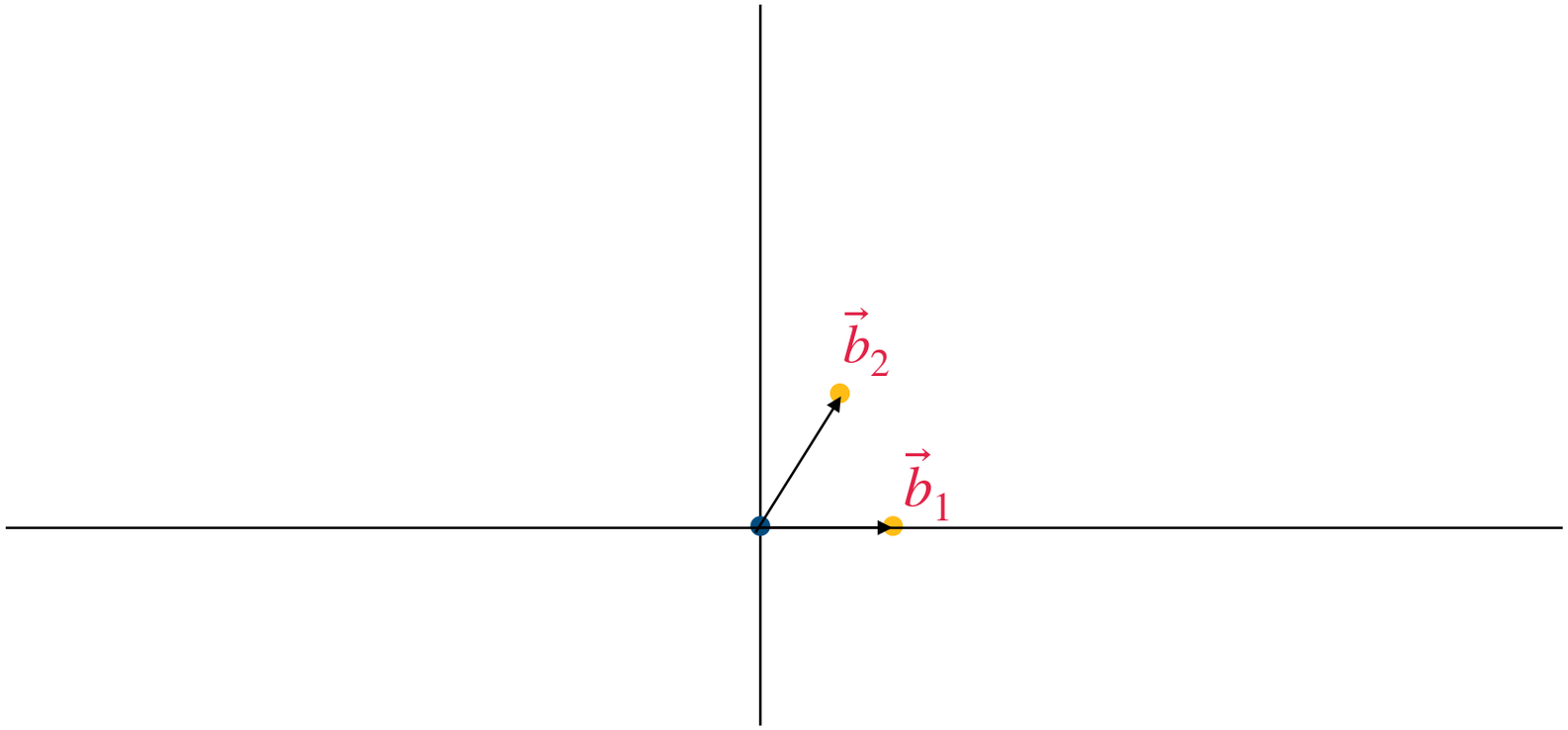
- $L = \left\{ z_1\vec{b}_1 + z_2\vec{b}_2 + \cdots + z_n\vec{b}_n \mid \forall i \in [n], z_i \in \mathbb{Z} \right\}$

- Lattice: set of vectors formed by integer linear combinations.

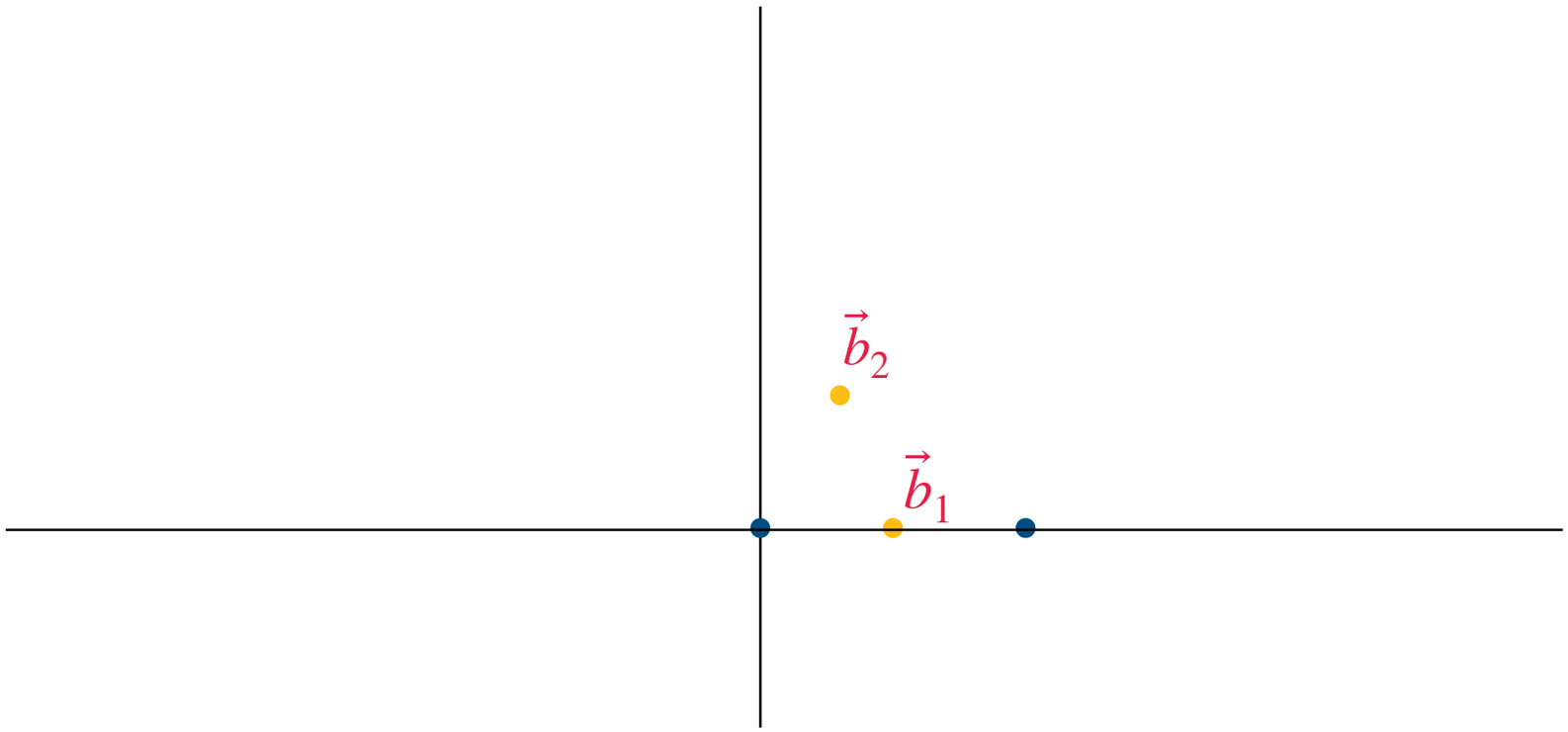
n : rank of the lattice

Lattices

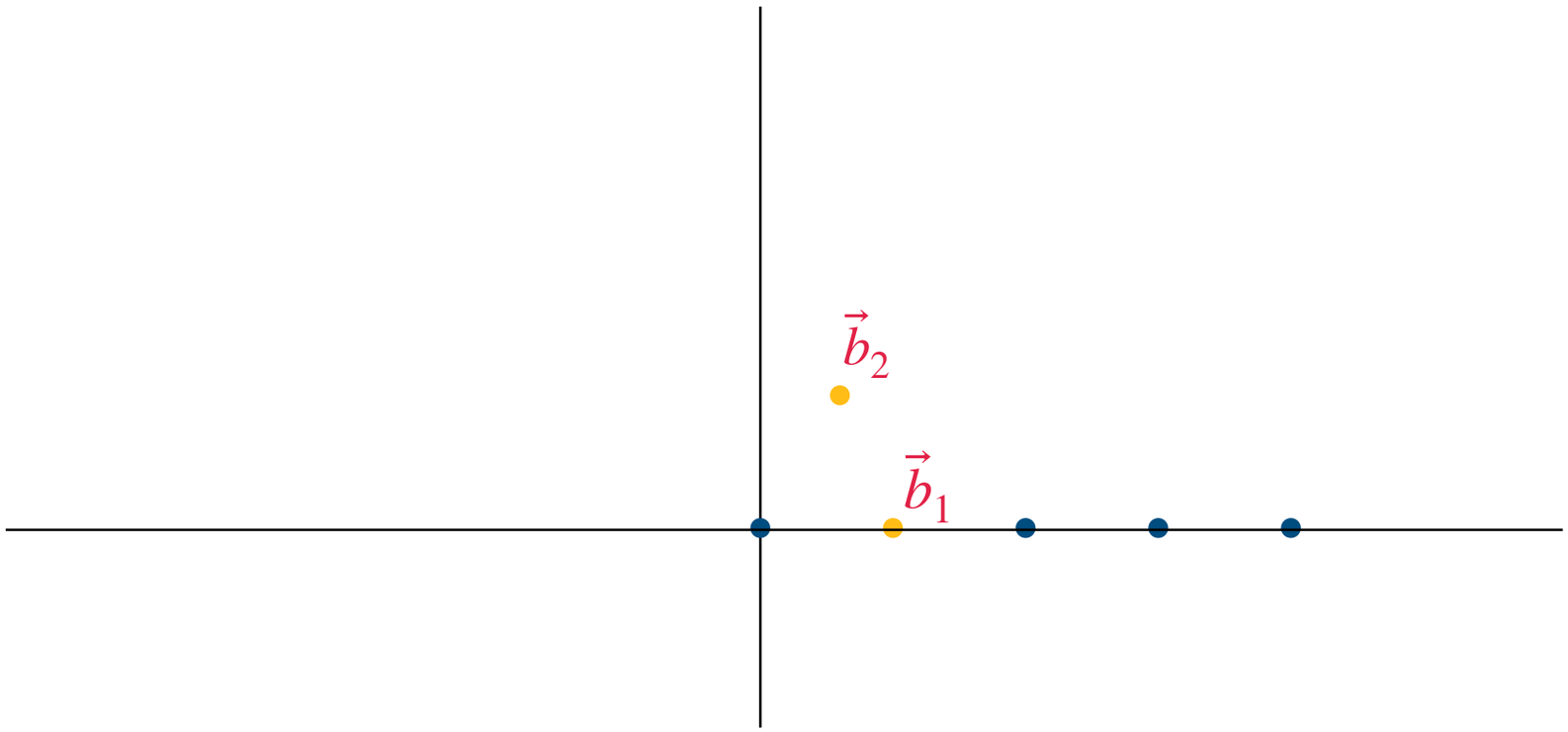
Lattices



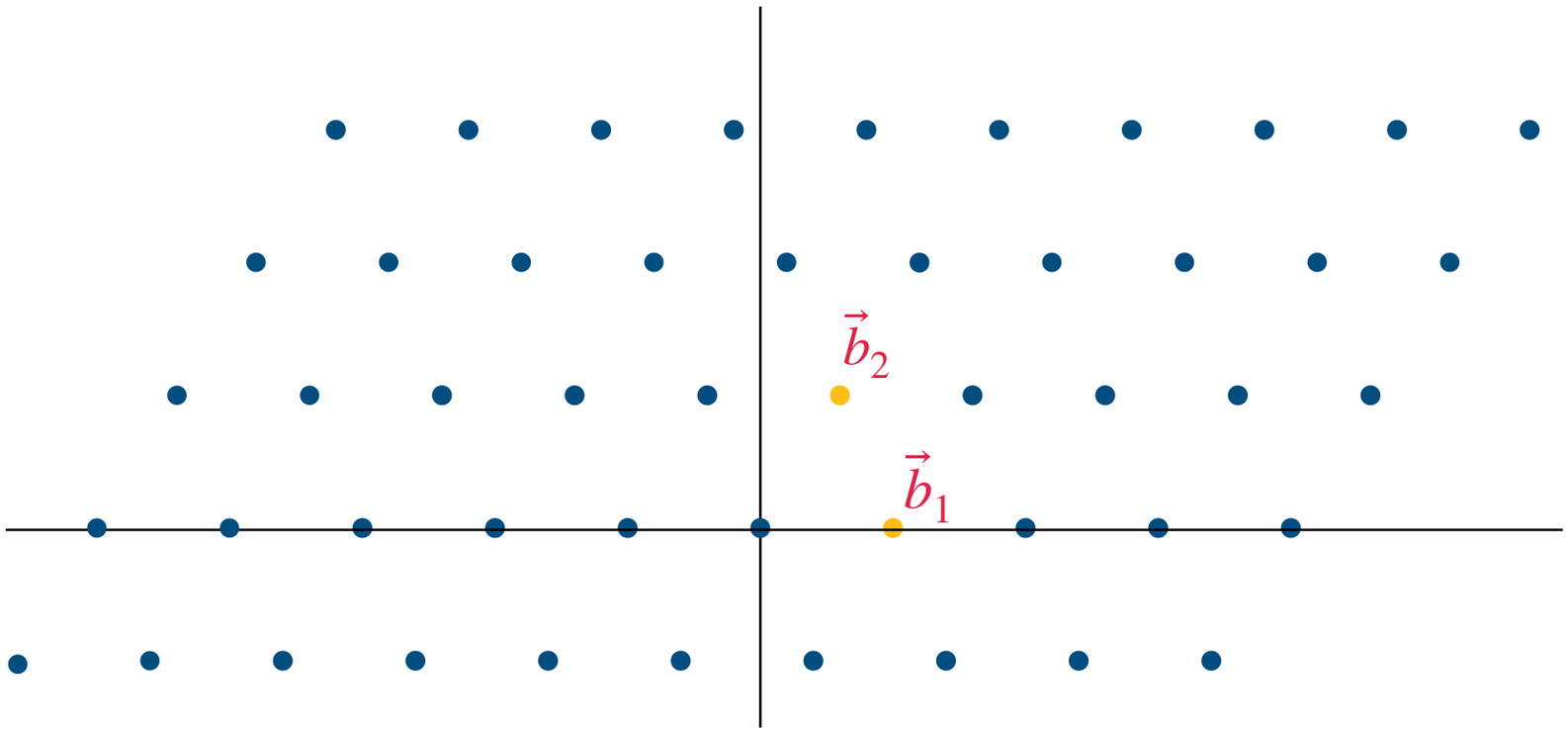
Lattices



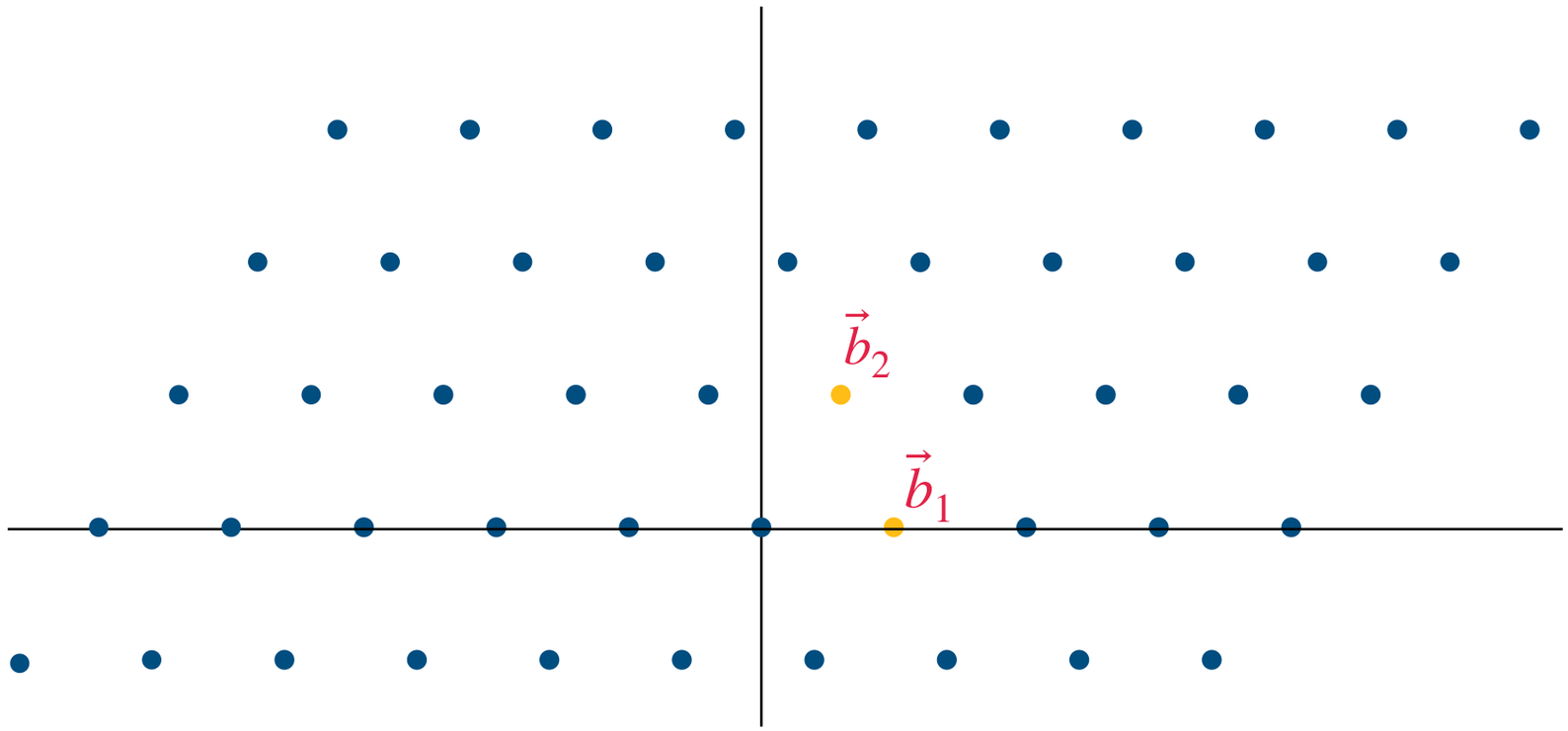
Lattices



Lattices



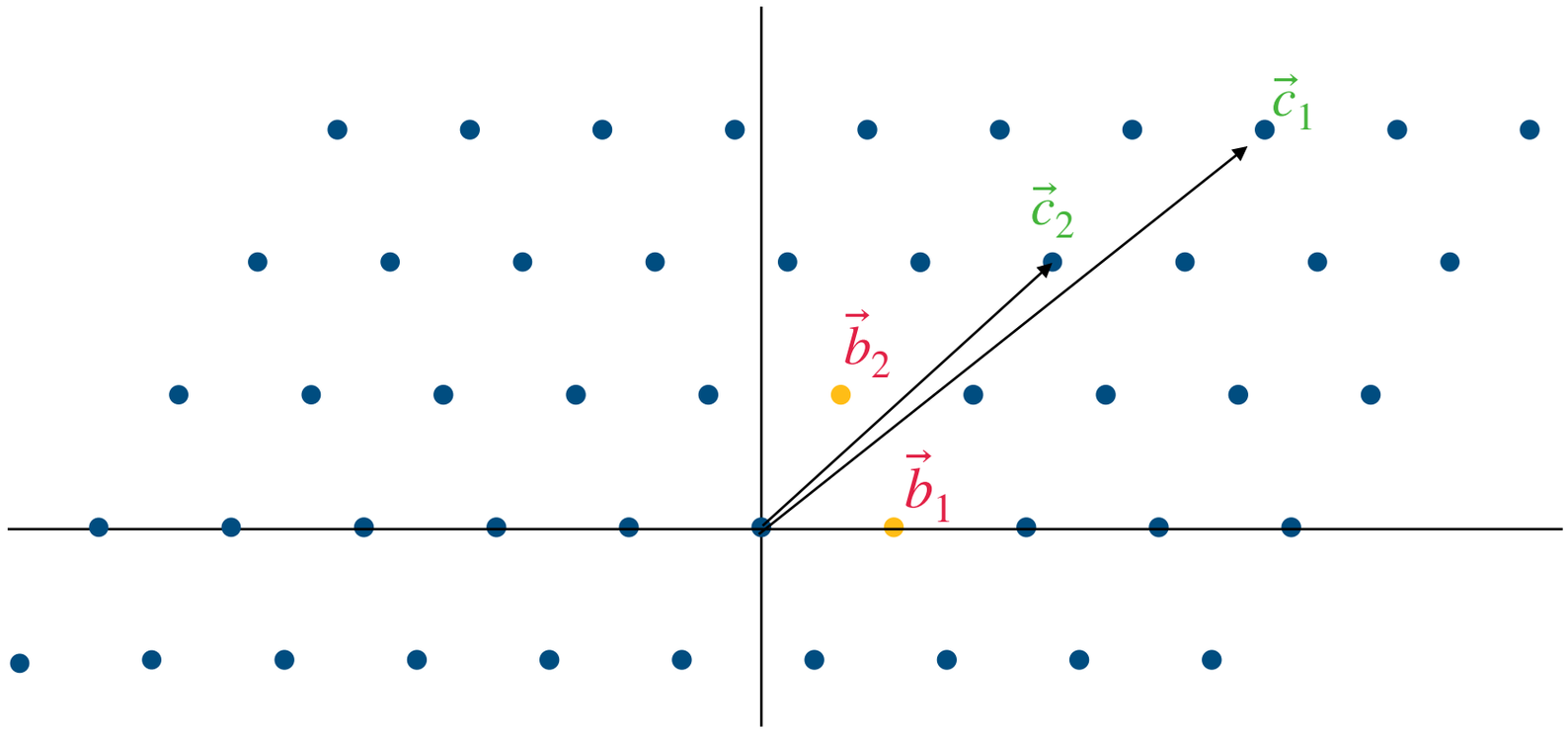
Lattices



$$L = \left\{ z_1 b_1 + z_2 b_2 + \cdots + z_n b_n \mid \forall i \in [n], z_i \in \mathbb{Z} \right\}$$

Rank n

Lattices

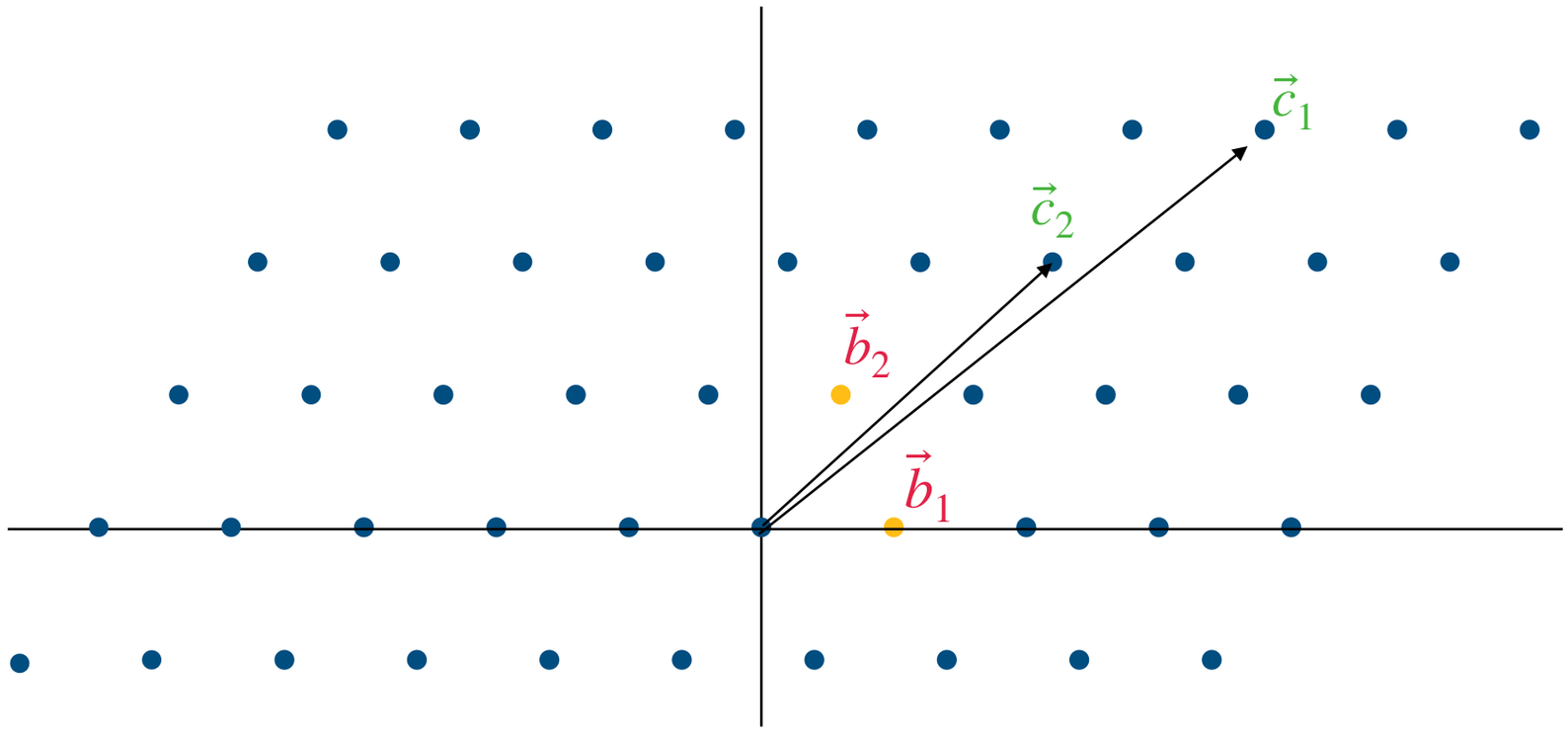


$$L = \left\{ z_1 b_1 + z_2 b_2 + \cdots + z_n b_n \mid \forall i \in [n], z_i \in \mathbb{Z} \right\}$$

Rank n

Lattices

Basis is not unique



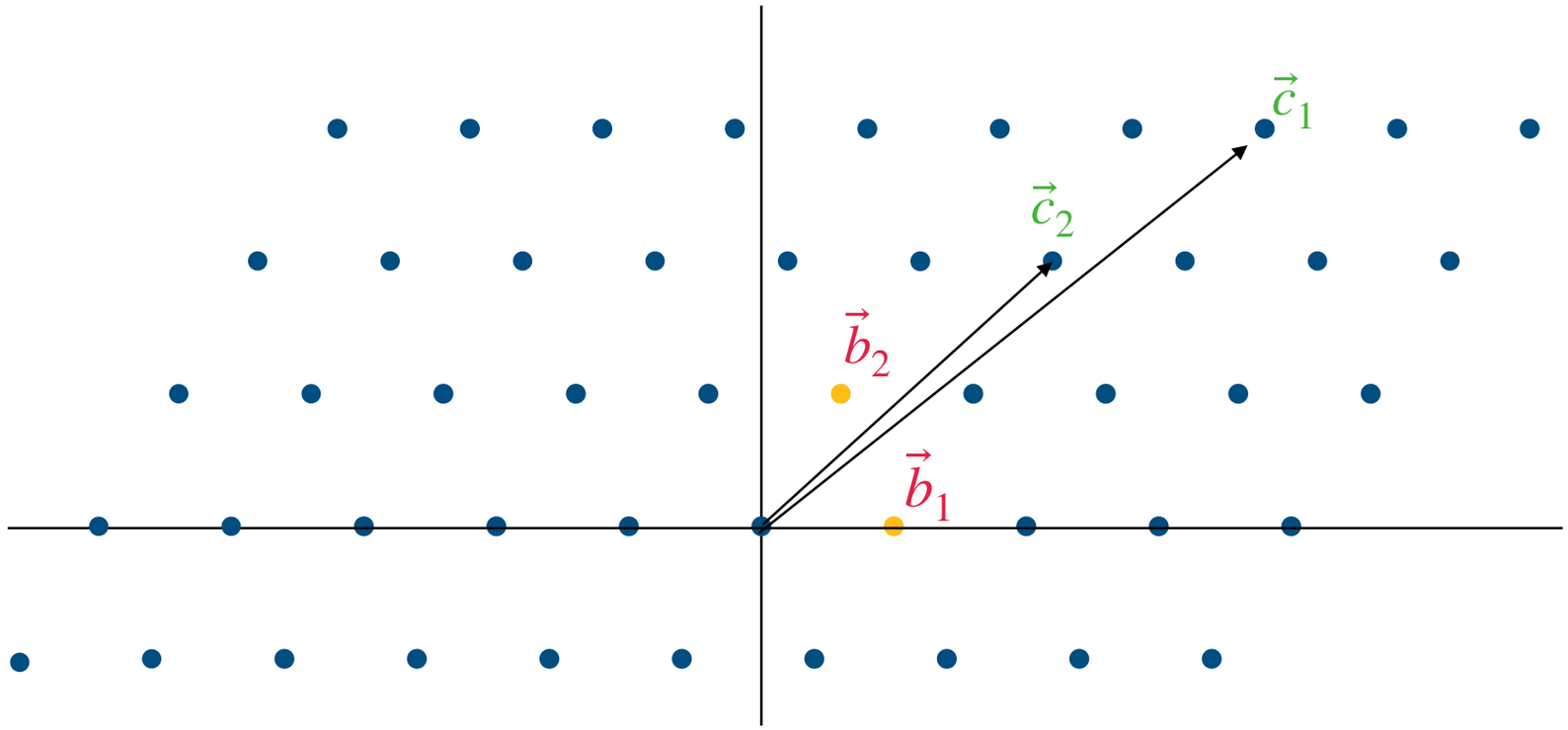
$$L = \left\{ z_1 b_1 + z_2 b_2 + \cdots + z_n b_n \mid \forall i \in [n], z_i \in \mathbb{Z} \right\}$$

Rank n

Lattices

Basis is not unique

Hard to find short basis



$$L = \left\{ z_1 b_1 + z_2 b_2 + \cdots + z_n b_n \mid \forall i \in [n], z_i \in \mathbb{Z} \right\}$$

Rank n

SVP

SVP

γ-Shortest Vector Problem (SVP): $(\gamma \geq 1)$

SVP

γ-Shortest Vector Problem (SVP): $(\gamma \geq 1)$

Input: basis B of lattice L and number $d > 0$

SVP

γ-Shortest Vector Problem (SVP): $(\gamma \geq 1)$

Input: basis B of lattice L and number $d > 0$

Goal: distinguish between

- YES : $\lambda_1(L) \leq d$
- NO : $\lambda_1(L) > \gamma d$

$\lambda_1(L)$: Length of shortest *non-zero* lattice vector.

SVP

γ-Shortest Vector Problem (SVP): $(\gamma \geq 1)$

Input: basis B of lattice L and number $d > 0$

Goal: distinguish between

- YES : $\lambda_1(L) \leq d$
- NO : $\lambda_1(L) > \gamma d$

$\lambda_1(L)$: Length of shortest *non-zero* lattice vector.

Approximate the length of shortest non-zero lattice vector.

SVP

γ-Shortest Vector Problem (SVP): $(\gamma \geq 1)$

Input: basis B of lattice L and number $d > 0$

Goal: distinguish between

- YES : $\lambda_1(L) \leq d$
- NO : $\lambda_1(L) > \gamma d$

$\lambda_1(L)$: Length of shortest *non-zero* lattice vector.

Approximate the length of shortest non-zero lattice vector.

For small γ, decision problem is as hard as search problem.

CVP

CVP

γ-Closest Vector Problem (SVP): $(\gamma \geq 1)$

CVP

γ-Closest Vector Problem (SVP): $(\gamma \geq 1)$

Input: basis B of lattice L, target $\vec{t}$ and number $d > 0$

CVP

γ-Closest Vector Problem (SVP): $(\gamma \geq 1)$

Input: basis B of lattice L, target $\vec{t}$ and number $d > 0$

Goal: distinguish between

- YES : $dist(\vec{t}, L) \leq d$
- NO : $dist(\vec{t}, L) > \gamma d$

$dist(\vec{t}, L)$: minimum distance of $\vec{t}$ from any lattice vector in L.

CVP

γ-Closest Vector Problem (SVP): $(\gamma \geq 1)$

Input: basis B of lattice L, target $\vec{t}$ and number $d > 0$

Goal: distinguish between

- YES : $dist(\vec{t}, L) \leq d$
- NO : $dist(\vec{t}, L) > \gamma d$

$dist(\vec{t}, L)$: minimum distance of $\vec{t}$ from any lattice vector in L.

Approximate the distance of target vector from lattice.

CVP

γ-Closest Vector Problem (SVP): $(\gamma \geq 1)$

Input: basis B of lattice L, target $\vec{t}$ and number $d > 0$

Goal: distinguish between

- YES : $dist(\vec{t}, L) \leq d$
- NO : $dist(\vec{t}, L) > \gamma d$

$dist(\vec{t}, L)$: minimum distance of $\vec{t}$ from any lattice vector in L.

Approximate the distance of target vector from lattice.

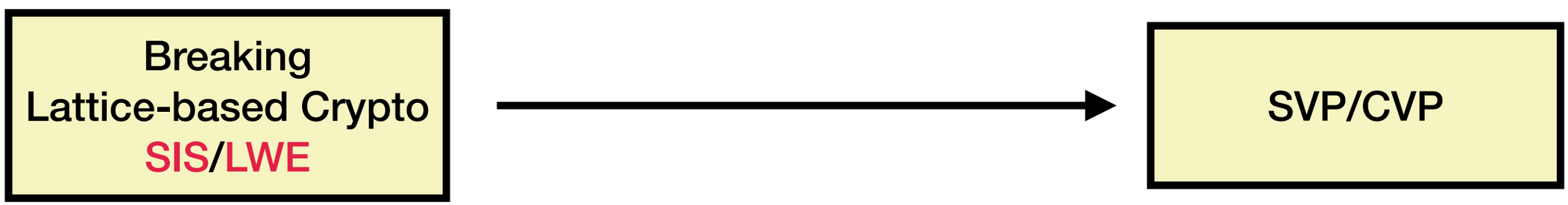
γ-CVP is at least as hard as γ-SVP.

Lattice-based Crypto

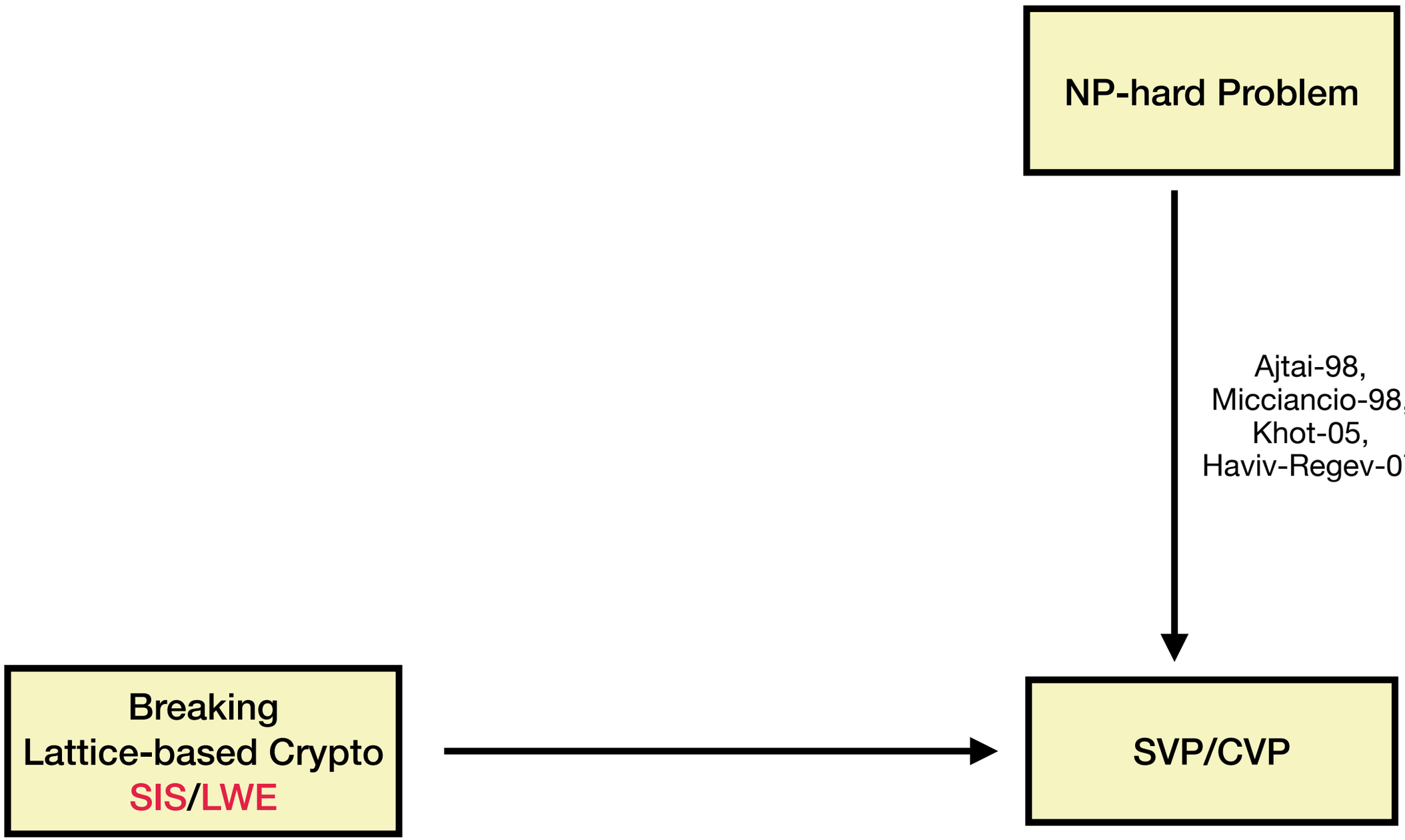
Lattice-based Crypto

Breaking
Lattice-based Crypto
SIS/LWE

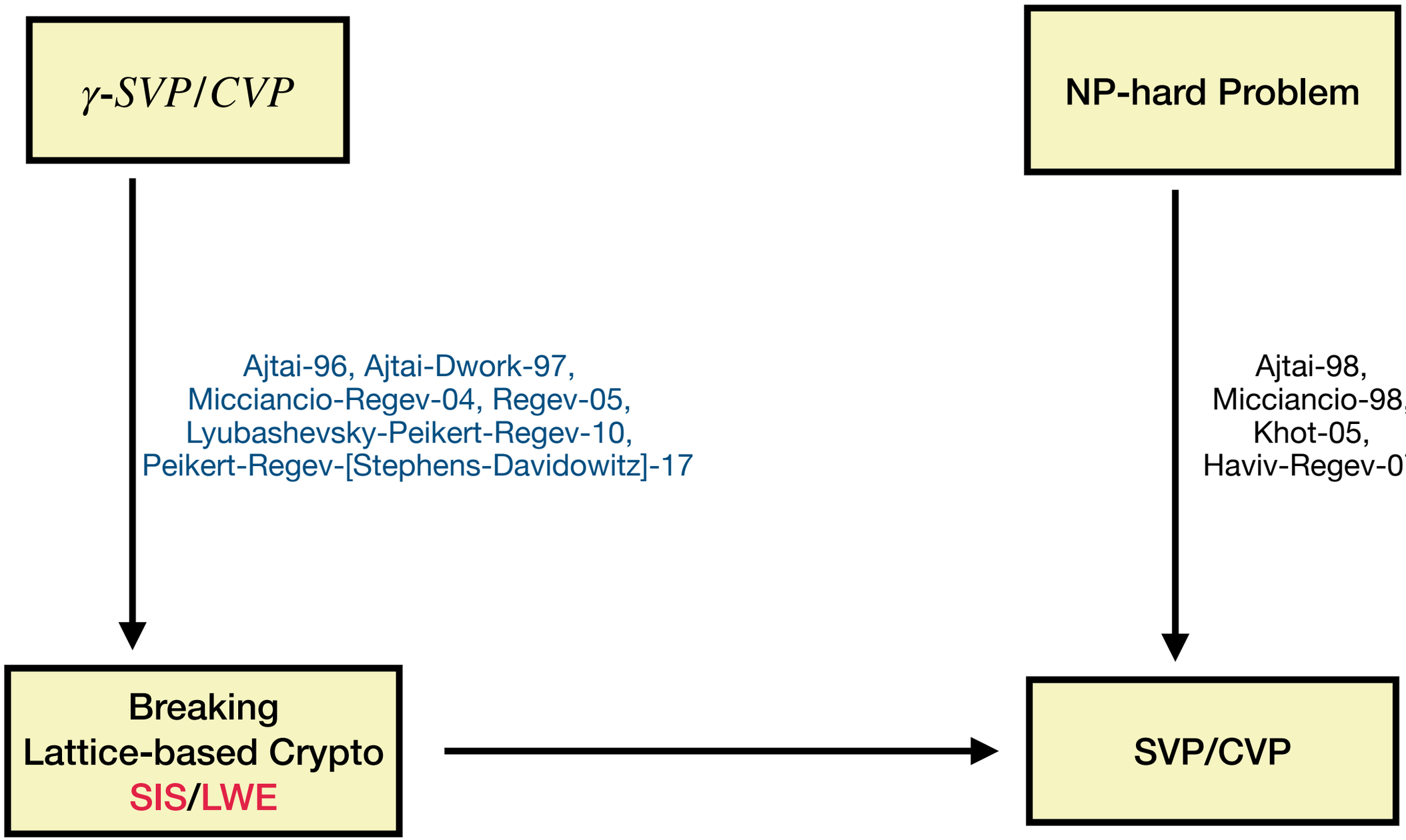
Lattice-based Crypto



Lattice-based Crypto



Lattice-based Crypto



Lattice-based Crypto

γ-SVP/CVP

Is γ-SVP/CVP hard?

Ajtai-96, Ajtai-Dwork-97,
Micciancio-Regev-04, Regev-05,
Lyubashevsky-Peikert-Regev-10,
Peikert-Regev-[Stephens-Davidowitz]-17

NP-hard Problem

Ajtai-98,
Micciancio-98,
Khot-05,
Haviv-Regev-07

Breaking
Lattice-based Crypto
SIS/LWE

SVP/CVP

Hardness of γ-SVP/CVP

Hardness of γ-SVP/CVP

- γ-CVP is NP-hard for $\gamma < n^{1/\log\log n}$.

[Arora-Babai-Stern-Sweedyk-93, Dinur-Kindler-Raz-Safra-03, Dinur-03]

Hardness of γ-SVP/CVP

- γ-CVP is NP-hard for $\gamma < n^{1/\log\log n}$.

  [Arora-Babai-Stern-Sweedyk-93, Dinur-Kindler-Raz-Safra-03, Dinur-03]

- γ-SVP is NP-hard for constant γ.

  [Ajtai-98, Micciancio-98, Khot-05, Haviv-Regev-07]

Hardness of γ-SVP/CVP

- γ-CVP is NP-hard for $\gamma < n^{1/\log\log n}$.

  [Arora-Babai-Stern-Sweedyk-93, Dinur-Kindler-Raz-Safra-03, Dinur-03]

- γ-SVP is NP-hard for constant γ.

  [Ajtai-98, Micciancio-98, Khot-05, Haviv-Regev-07]

- γ-SVP is poly-time hard under some reasonable conjecture for $\gamma < n^{1/\log\log n}$.

  [Dinur-03, Khot-05, Haviv-Regev-07, Micciancio-12, Bennett-Peikert-23]

Hardness of γ-SVP/CVP

Hardness of γ-SVP/CVP

$n^{1/\log\log n}$

Hard

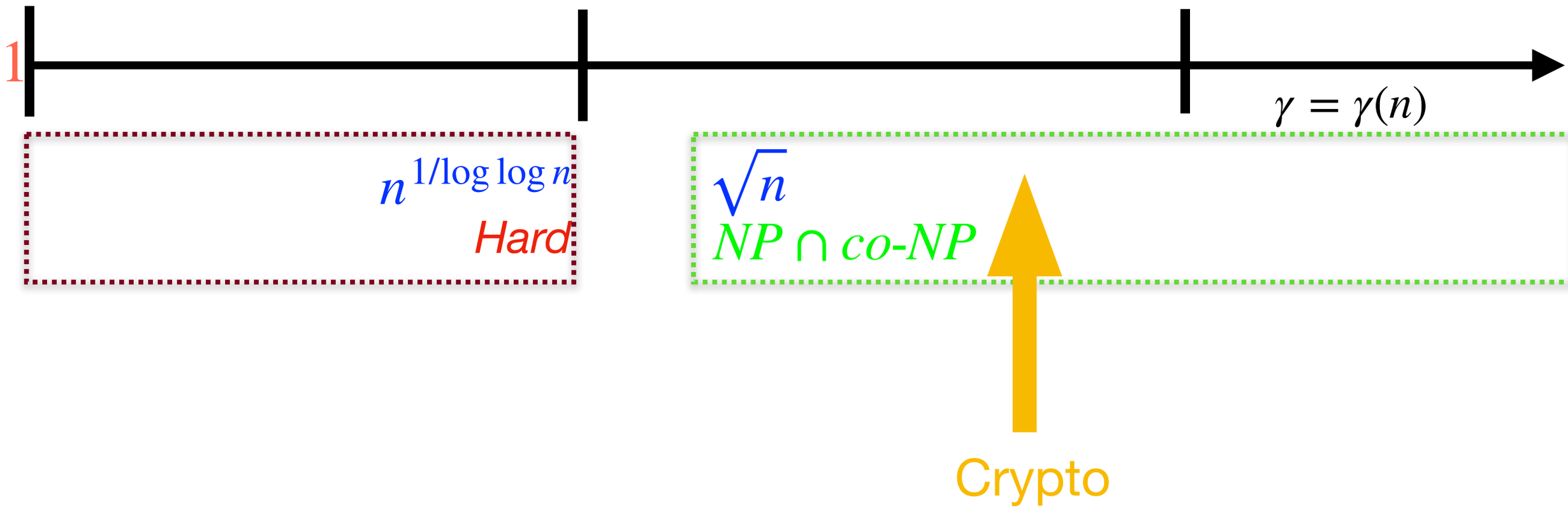
Hardness of γ-SVP/CVP

$n^{1/\log\log n}$

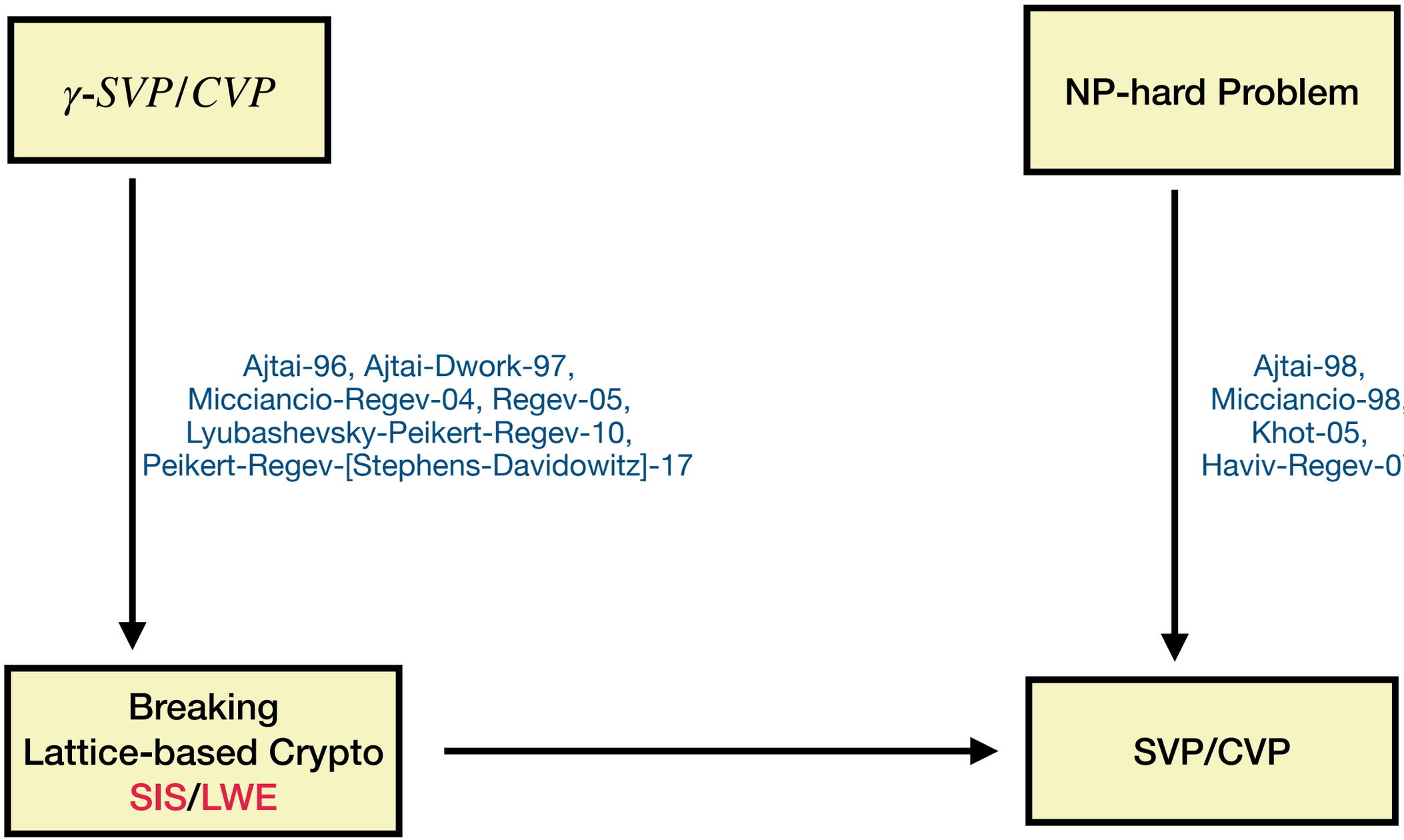
Hard

Crypto

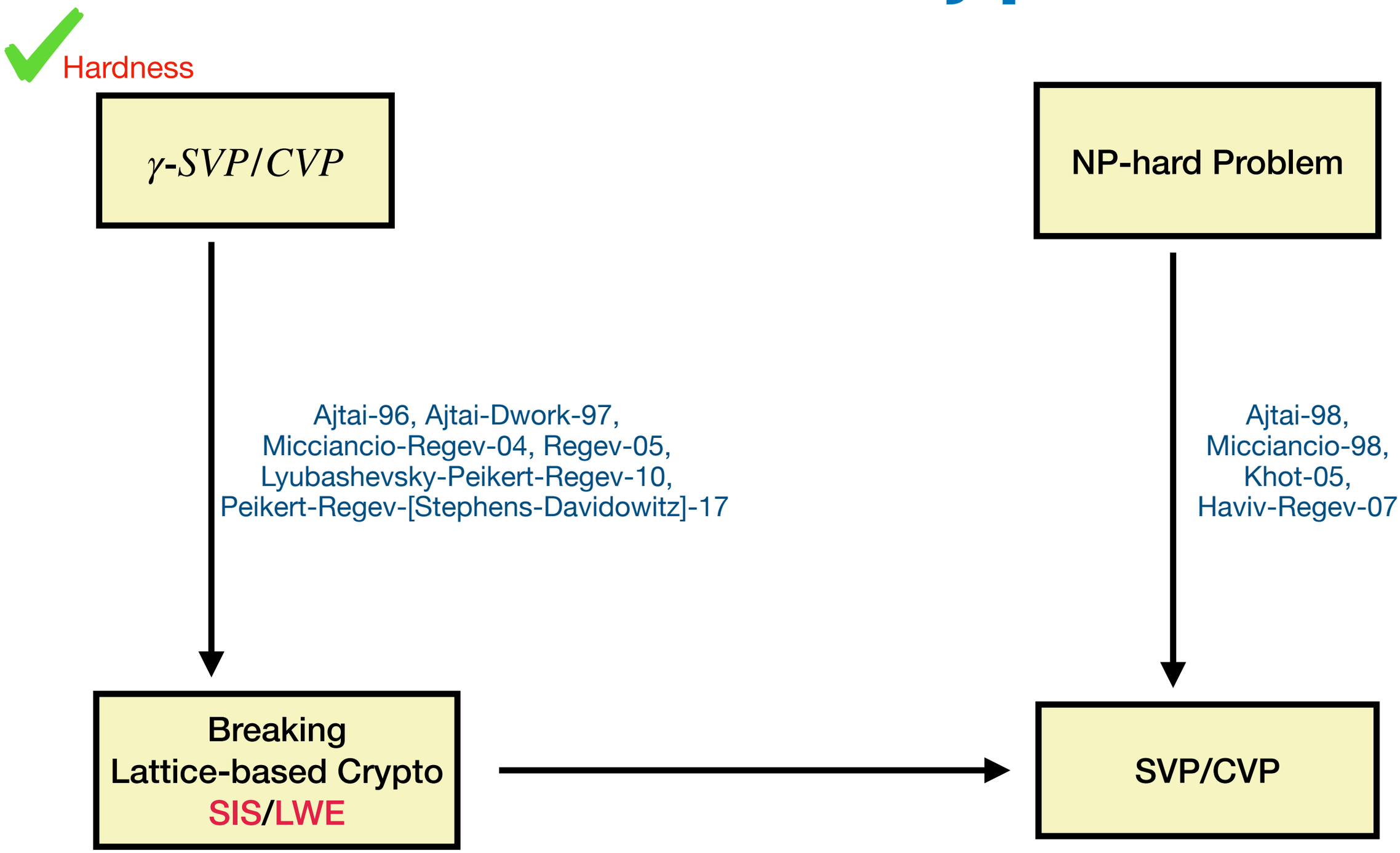
Hardness of γ-*SVP*/*CVP*



Lattice-based Crypto



Lattice-based Crypto



Lattice-based Crypto

✓ Hardness

γ-SVP/CVP

Ajtai-96, Ajtai-Dwork-97,
Micciancio-Regev-04, Regev-05,
Lyubashevsky-Peikert-Regev-10,
Peikert-Regev-[Stephens-Davidowitz]-17

Can we solve poly-approx SVP/CVP efficiently?

NP-hard Problem

Ajtai-98,
Micciancio-98,
Khot-05,
Haviv-Regev-07

Breaking
Lattice-based Crypto
SIS/LWE

SVP/CVP

Algorithm of γ-SVP/CVP

Algorithm of γ-SVP/CVP

➡ Polynomial time algorithm for 2^n-CVP/SVP.

[Lenstra-Lenstra-Lovász-82, Babai-86, Schnorr-87]

Algorithm of γ-SVP/CVP

- Polynomial time algorithm for 2^n-CVP/SVP.

  [Lenstra-Lenstra-Lovász-82, Babai-86, Schnorr-87]

- 2^n-time and space algorithm for exact SVP/CVP.

  [Ajtai-Kumar-Sivakumar-01, Aggarwal-Dadush-Regev-StephensDavidowitz-15, Aggarwal-Dadush-StephensDavidowitz-15,…..]

Algorithm of γ-SVP/CVP

- Polynomial time algorithm for 2^n-CVP/SVP.

  [Lenstra-Lenstra-Lovász-82, Babai-86, Schnorr-87]

- 2^n-time and space algorithm for exact SVP/CVP.

  [Ajtai-Kumar-Sivakumar-01, Aggarwal-Dadush-Regev-StephensDavidowitz-15, Aggarwal-Dadush-StephensDavidowitz-15,…..]

- $2^{0.83n}$-time and $2^{0.5n}$ space ***quantum*** algorithm for exact SVP.

  [Aggarwal-Chen-Kumar-Shen-22]

Algorithm of γ-SVP/CVP

- Polynomial time algorithm for 2^n-CVP/SVP.

  [Lenstra-Lenstra-Lovász-82, Babai-86, Schnorr-87]

- 2^n-time and space algorithm for exact SVP/CVP.

  [Ajtai-Kumar-Sivakumar-01, Aggarwal-Dadush-Regev-StephensDavidowitz-15, Aggarwal-Dadush-StephensDavidowitz-15,…..]

- $2^{0.83n}$-time and $2^{0.5n}$ space ***quantum*** algorithm for exact SVP.

  [Aggarwal-Chen-Kumar-Shen-22]

Open Problem: Quantum advantage for CVP.

Algorithm of γ-SVP/CVP

- Polynomial time algorithm for 2^n-CVP/SVP.

  [Lenstra-Lenstra-Lovász-82, Babai-86, Schnorr-87]

- 2^n-time and space algorithm for exact SVP/CVP.

  [Ajtai-Kumar-Sivakumar-01, Aggarwal-Dadush-Regev-StephensDavidowitz-15, Aggarwal-Dadush-StephensDavidowitz-15,…..]

- $2^{0.83n}$-time and $2^{0.5n}$ space ***quantum*** algorithm for exact SVP.

  [Aggarwal-Chen-Kumar-Shen-22]

Open Problem: Quantum advantage for CVP.

- $k^{n/k}$-approximate SVP reduces to exact SVP on dimension k.

  [Schnorr-87, Gama-Nguyen-08, Hanrot-Pujol-Stehlé-11, Micciancio-Walter-16, ……]

Algorithm of γ-SVP/CVP

- Polynomial time algorithm for 2^n-CVP/SVP.

  [Lenstra-Lenstra-Lovász-82, Babai-86, Schnorr-87]

- 2^n-time and space algorithm for exact SVP/CVP.

  [Ajtai-Kumar-Sivakumar-01, Aggarwal-Dadush-Regev-StephensDavidowitz-15, Aggarwal-Dadush-StephensDavidowitz-15,…..]

- $2^{0.83n}$-time and $2^{0.5n}$ space ***quantum*** algorithm for exact SVP.

  [Aggarwal-Chen-Kumar-Shen-22]

Open Problem: Quantum advantage for CVP.

- $k^{n/k}$-approximate SVP reduces to exact SVP on dimension k.

  [Schnorr-87, Gama-Nguyen-08, Hanrot-Pujol-Stehlé-11, Micciancio-Walter-16, ……]

Conjecture: $poly(n)$-SVP is $exp(\Omega(n))$-hard.

Lattice-based Crypto

✓ Hardness

γ-SVP/CVP

Ajtai-96, Ajtai-Dwork-97
Micciancio-Regev-04, Regev-05,
Lyubashevsky-Peikert-Regev-10
Peikert-Regev-[Stephens-Davidowitz]-17

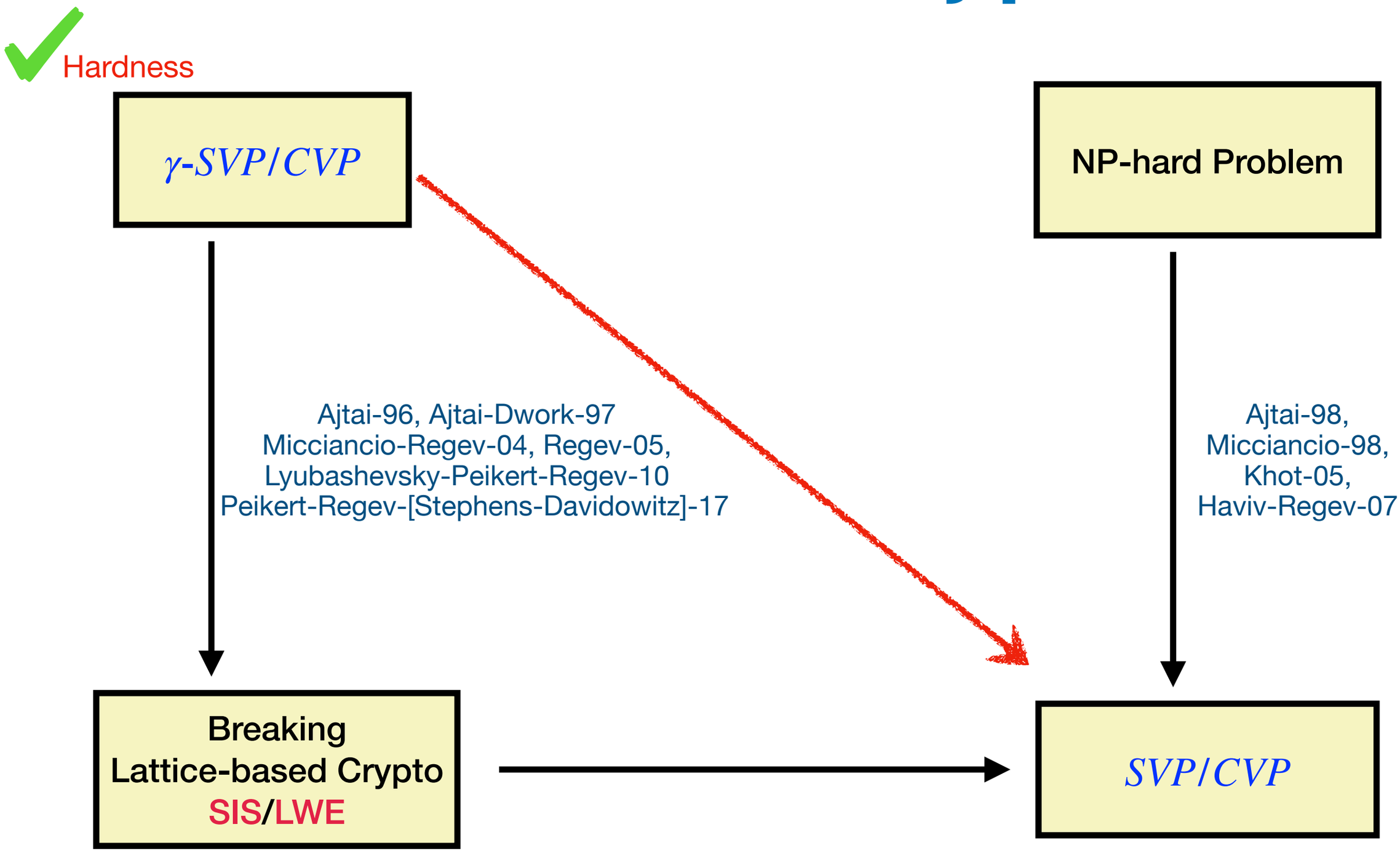
NP-hard Problem

Ajtai-98,
Micciancio-98,
Khot-05,
Haviv-Regev-07

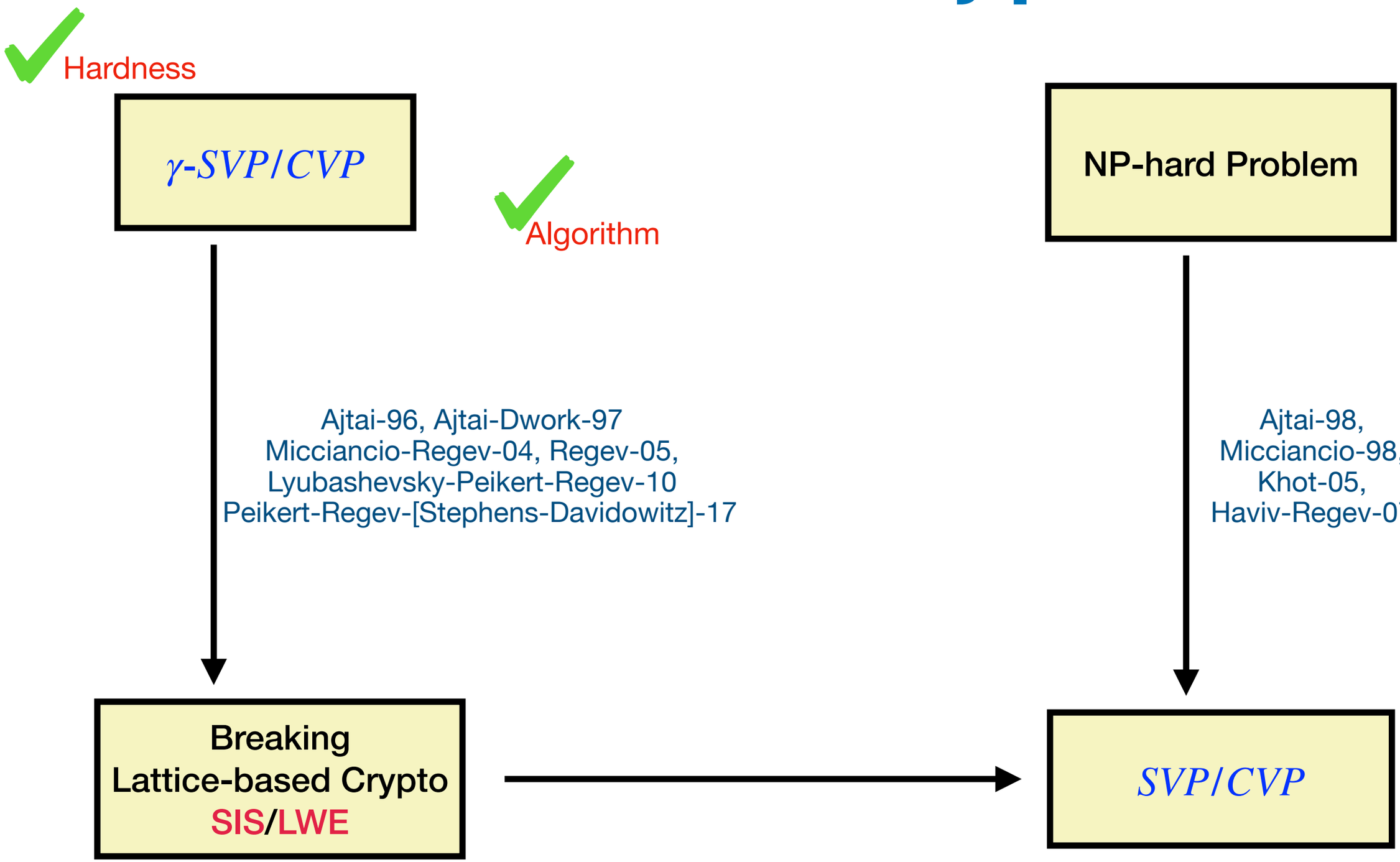
Breaking
Lattice-based Crypto
SIS/LWE

SVP/CVP

Lattice-based Crypto



Lattice-based Crypto



Lattice-based Crypto

✓ Hardness

γ-SVP/CVP

Ajtai-96, Ajtai-Dwork-97
Micciancio-Regev-04, Regev-05,
Lyubashevsky-Peikert-Regev-10
Peikert-Regev-[Stephens-Davidowitz]-17

✓ Algorithm

$exp(n)$-hardness of γ-SVP/CVP?

NP-hard Problem

Ajtai-98,
Micciancio-98,
Khot-05,
Haviv-Regev-07

Breaking
Lattice-based Crypto
SIS/LWE

SVP/CVP

$exp(n)$-hardness

$exp(n)$-hardness

Use ***ETH/SETH/QSETH*** and fine-grained reductions from $k\text{-}SAT$.

$exp(n)$-hardness

Use ***ETH/SETH/QSETH*** and fine-grained reductions from $k\text{-}SAT$.

ETH (**E**xponential **T**ime **H**ypothesis):

$3\text{-}SAT$ on n-variables requires $exp(\Omega(n))$-time.

$exp(n)$-hardness

Use ***ETH/SETH/QSETH*** and fine-grained reductions from $k\text{-}SAT$.

ETH (**E**xponential **T**ime **H**ypothesis):

$3\text{-}SAT$ on n-variables requires $exp(\Omega(n))$-time.

SETH (**S**trong **E**xponential **T**ime **H**ypothesis):

For every $\epsilon > 0$, $\exists k$ such that $k\text{-}SAT$ on n-variables requires $2^{(1-\epsilon)n}$-time.

$exp(n)$-hardness

Use ***ETH/SETH/QSETH*** and fine-grained reductions from $k\text{-}SAT$.

ETH (**E**xponential **T**ime **H**ypothesis):

$3\text{-}SAT$ on n-variables requires $exp(\Omega(n))$-time.

SETH (**S**trong **E**xponential **T**ime **H**ypothesis):

For every $\epsilon > 0$, $\exists k$ such that $k\text{-}SAT$ on n-variables requires $2^{(1-\epsilon)n}$-time.

QSETH (**Q**uantum **S**trong **E**xponential **T**ime **H**ypothesis):

For every $\epsilon > 0$, $\exists k$ such that quantum algorithms for $k\text{-}SAT$ on n-variables requires $2^{(1-\epsilon)n/2}$-time.

$exp(n)$-hardness

➡ ***ETH*** (**E**xponential **T**ime **H**ypothesis):

$3\text{-}SAT$ on n-variables requires $exp(\Omega(n))$-time.

$exp(n)$-hardness

ETH (**E**xponential **T**ime **H**ypothesis):

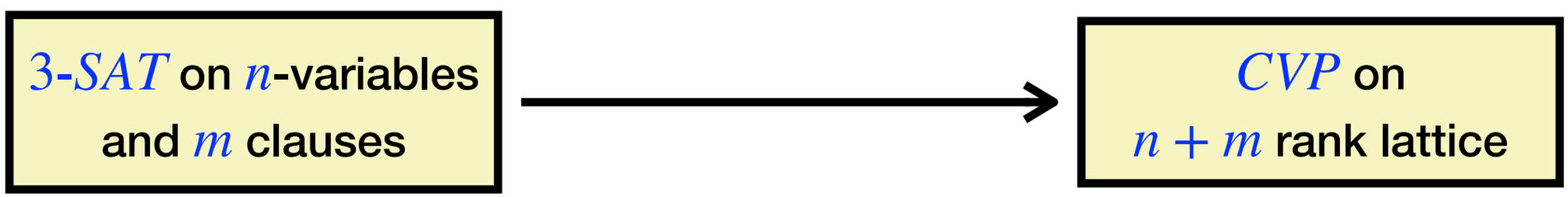
$3\text{-}SAT$ on n-variables requires $exp(\Omega(n))$-time.

$3\text{-}SAT$ on n-variables
and m clauses

$exp(n)$-hardness

ETH (**E**xponential **T**ime **H**ypothesis):

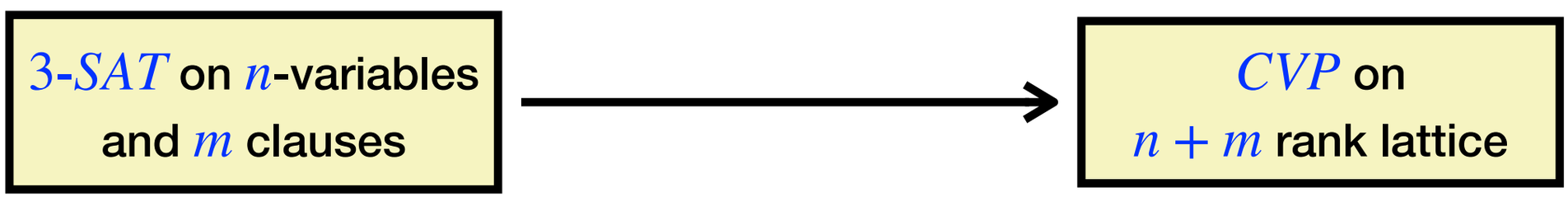
$3\text{-}SAT$ on n-variables requires $exp(\Omega(n))$-time.



$exp(n)$-hardness

ETH (**E**xponential **T**ime **H**ypothesis):

$3\text{-}SAT$ on n-variables requires $exp(\Omega(n))$-time.



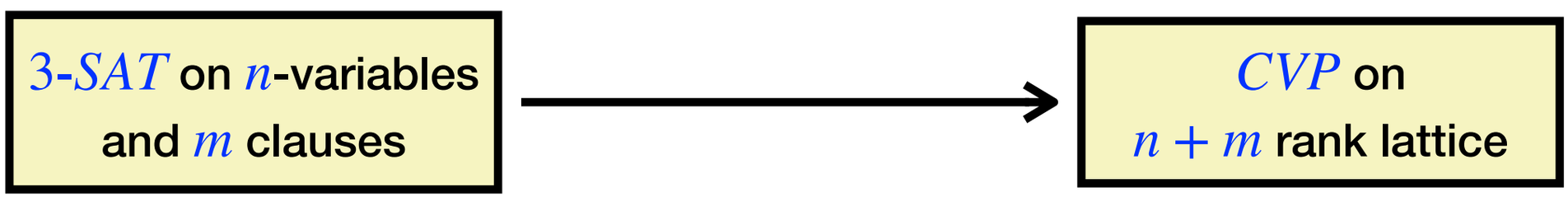
ETH and sparsification lemma $\Longrightarrow$ CVP on n rank lattice is $exp(\Omega(n))$-hard.

[Bennett-Golovnev-StephensDavidowitz 17]

$exp(n)$-hardness

ETH (**E**xponential **T**ime **H**ypothesis):

$3\text{-}SAT$ on n-variables requires $exp(\Omega(n))$-time.



ETH and sparsification lemma $\Longrightarrow$ CVP on n rank lattice is $exp(\Omega(n))$-hard.

[Bennett-Golovnev-StephensDavidowitz 17]

Open Problem: $exp(\Omega(n))$-hardness of SVP.

$exp(n)$-hardness

$exp(n)$-hardness

➡ $exp(\Omega(n))$-time hardness for SVP/CVP is not enough for practical security.

$exp(n)$-hardness

➡ $exp(\Omega(n))$-time hardness for SVP/CVP is not enough for practical security.

⚠ Practical applications choose $n \approx 500$ for efficiency.

$exp(n)$-hardness

➡ $exp(\Omega(n))$-time hardness for SVP/CVP is not enough for practical security.

⚠ Practical applications choose $n \approx 500$ for efficiency.

⚠ $2^{n/20}$-time algorithm for SVP/CVP either breaks these cryptosystems or make them inefficient.

$exp(n)$-hardness

$exp(\Omega(n))$-time hardness for SVP/CVP is not enough for practical security.

Practical applications choose $n \approx 500$ for efficiency.

$2^{n/20}$-time algorithm for SVP/CVP either breaks these cryptosystems or make them inefficient.

Can we get 2^{Cn}-hardness for CVP for some specific constant $C > 0$?

$exp(n)$-hardness

➡ $exp(\Omega(n))$-time hardness for SVP/CVP is not enough for practical security.

⚠ Practical applications choose $n \approx 500$ for efficiency.

⚠ $2^{n/20}$-time algorithm for SVP/CVP either breaks these cryptosystems or make them inefficient.

Can we get 2^{Cn}-hardness for CVP for some specific constant $C > 0$?

➡ It is impossible to get 2^{Cn}-hardness for CVP under **SETH/QSETH** via poly-time Turing reductions from k-SAT unless the polynomial hierarchy collapses to the third level.

[Aggarwal-Kumar 23]

Barrier for $exp(Cn)$-hardness

Barrier for $exp(Cn)$-hardness

➡ ***Instance Compression***: reduce to some problem with smaller instance size while preserving the information whether the input instance is in the language or not.

Barrier for $exp(Cn)$-hardness

➡ ***Instance Compression***: reduce to some problem with smaller instance size while preserving the information whether the input instance is in the language or not.

➡ A compressed instance may not be of the same problem.

Barrier for $exp(Cn)$-hardness

➡ ***Instance Compression***: reduce to some problem with smaller instance size while preserving the information whether the input instance is in the language or not.

➡ A compressed instance may not be of the same problem.

⚠ $k\text{-}SAT$ instance on n-variables can not compressed to $n^{k-\epsilon}$ size instance unless the polynomial hierarchy collapses to the third level. [Dell-vanMelkebeek14]

Barrier for $exp(Cn)$-hardness

➡ ***Instance Compression***: reduce to some problem with smaller instance size while preserving the information whether the input instance is in the language or not.

➡ A compressed instance may not be of the same problem.

⚠ $k\text{-}SAT$ instance on n-variables can not compressed to $n^{k-\epsilon}$ size instance unless the polynomial hierarchy collapses to the third level. [Dell-vanMelkebeek14]

➡ Any CVP instance can be compressed to $\mathcal{O}(n^8)$ bits.

Barrier for $exp(Cn)$-hardness

➡ ***Instance Compression***: reduce to some problem with smaller instance size while preserving the information whether the input instance is in the language or not.

➡ A compressed instance may not be of the same problem.

⚠ $k\text{-}SAT$ instance on n-variables can not compressed to $n^{k-\epsilon}$ size instance unless the polynomial hierarchy collapses to the third level. [Dell-vanMelkebeek14]

➡ Any CVP instance can be compressed to $\mathcal{O}(n^8)$ bits.

for all constant k

$k\text{-}SAT$ on n variables

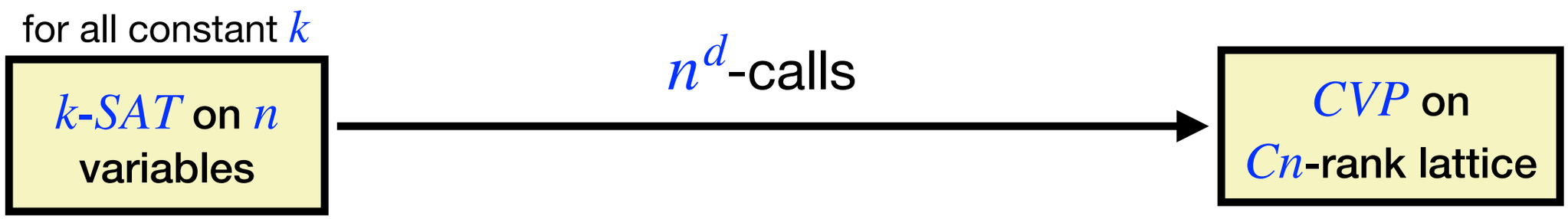
Barrier for $exp(Cn)$-hardness

➡ ***Instance Compression***: reduce to some problem with smaller instance size while preserving the information whether the input instance is in the language or not.

➡ A compressed instance may not be of the same problem.

⚠ $k\text{-}SAT$ instance on n-variables can not compressed to $n^{k-\epsilon}$ size instance unless the polynomial hierarchy collapses to the third level. [Dell-vanMelkebeek14]

➡ Any CVP instance can be compressed to $\mathcal{O}(n^8)$ bits.



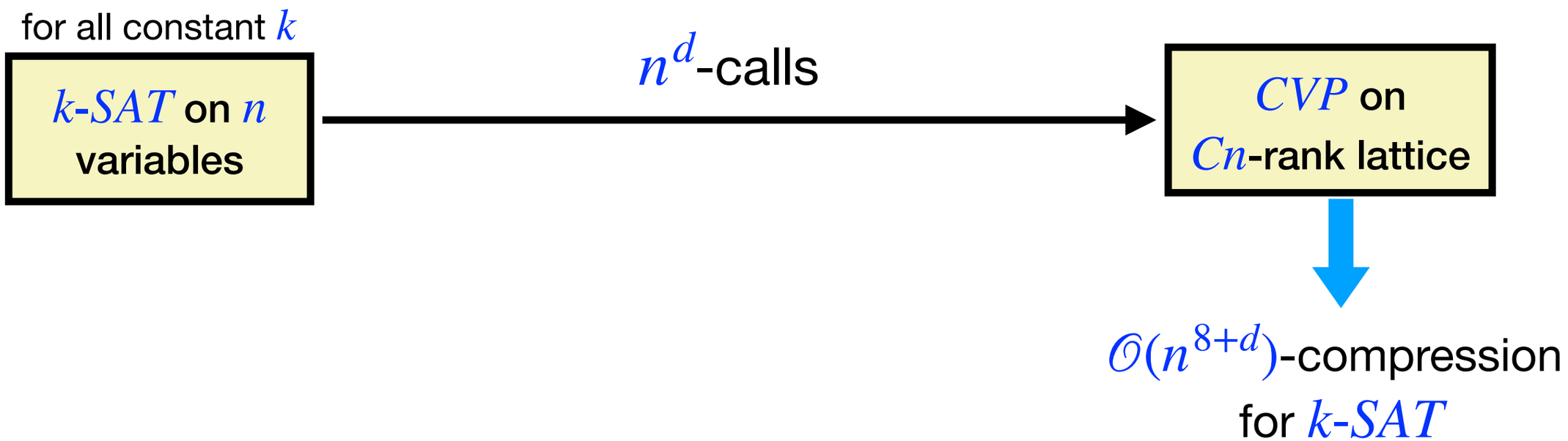
Barrier for $exp(Cn)$-hardness

➡ ***Instance Compression***: reduce to some problem with smaller instance size while preserving the information whether the input instance is in the language or not.

➡ A compressed instance may not be of the same problem.

⚠ $k\text{-}SAT$ instance on n-variables can not compressed to $n^{k-\epsilon}$ size instance unless the polynomial hierarchy collapses to the third level. [Dell-vanMelkebeek14]

➡ Any CVP instance can be compressed to $\mathcal{O}(n^8)$ bits.



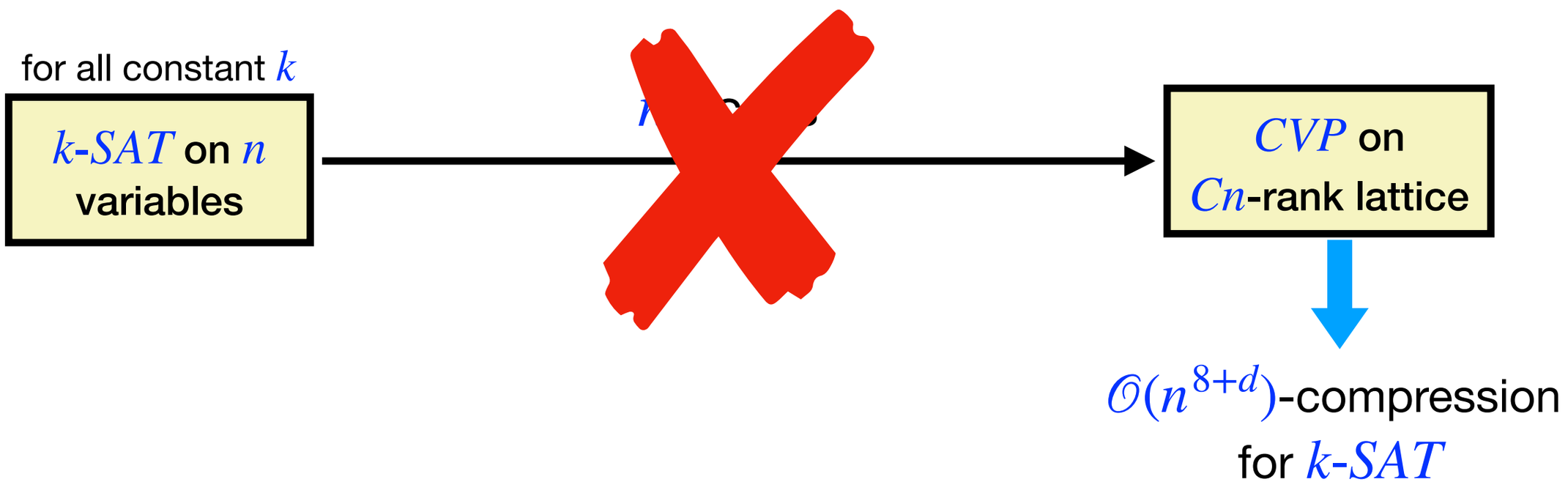
Barrier for $exp(Cn)$-hardness

➡ ***Instance Compression***: reduce to some problem with smaller instance size while preserving the information whether the input instance is in the language or not.

➡ A compressed instance may not be of the same problem.

⚠ $k\text{-}SAT$ instance on n-variables can not compressed to $n^{k-\epsilon}$ size instance unless the polynomial hierarchy collapses to the third level. [Dell-vanMelkebeek14]

➡ Any CVP instance can be compressed to $\mathcal{O}(n^8)$ bits.



Instance Compression

➡ Any CVP instance can be compressed to $\mathcal{O}(n^8)$ bits.

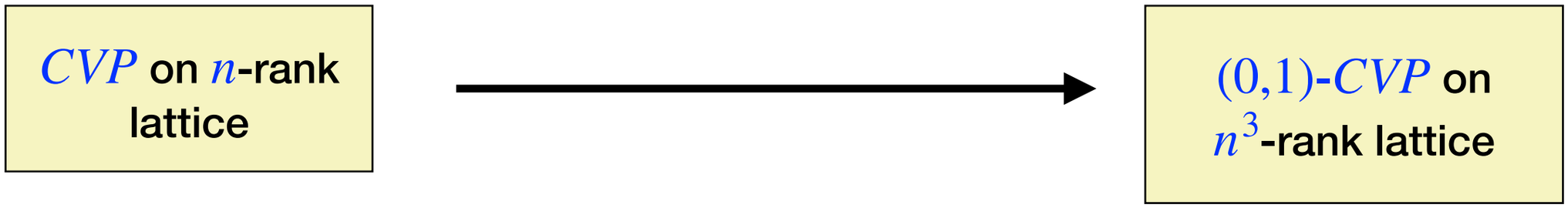
Instance Compression

➡ Any CVP instance can be compressed to $\mathcal{O}(n^8)$ bits.

CVP on n-rank lattice

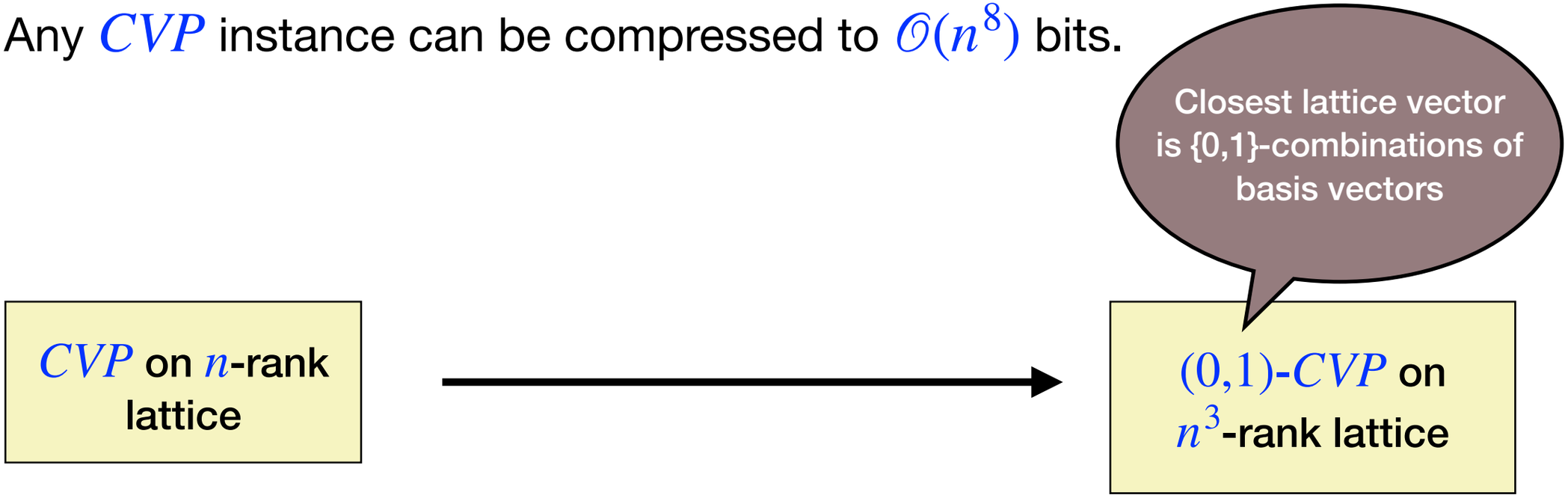
Instance Compression

➡ Any CVP instance can be compressed to $\mathcal{O}(n^8)$ bits.



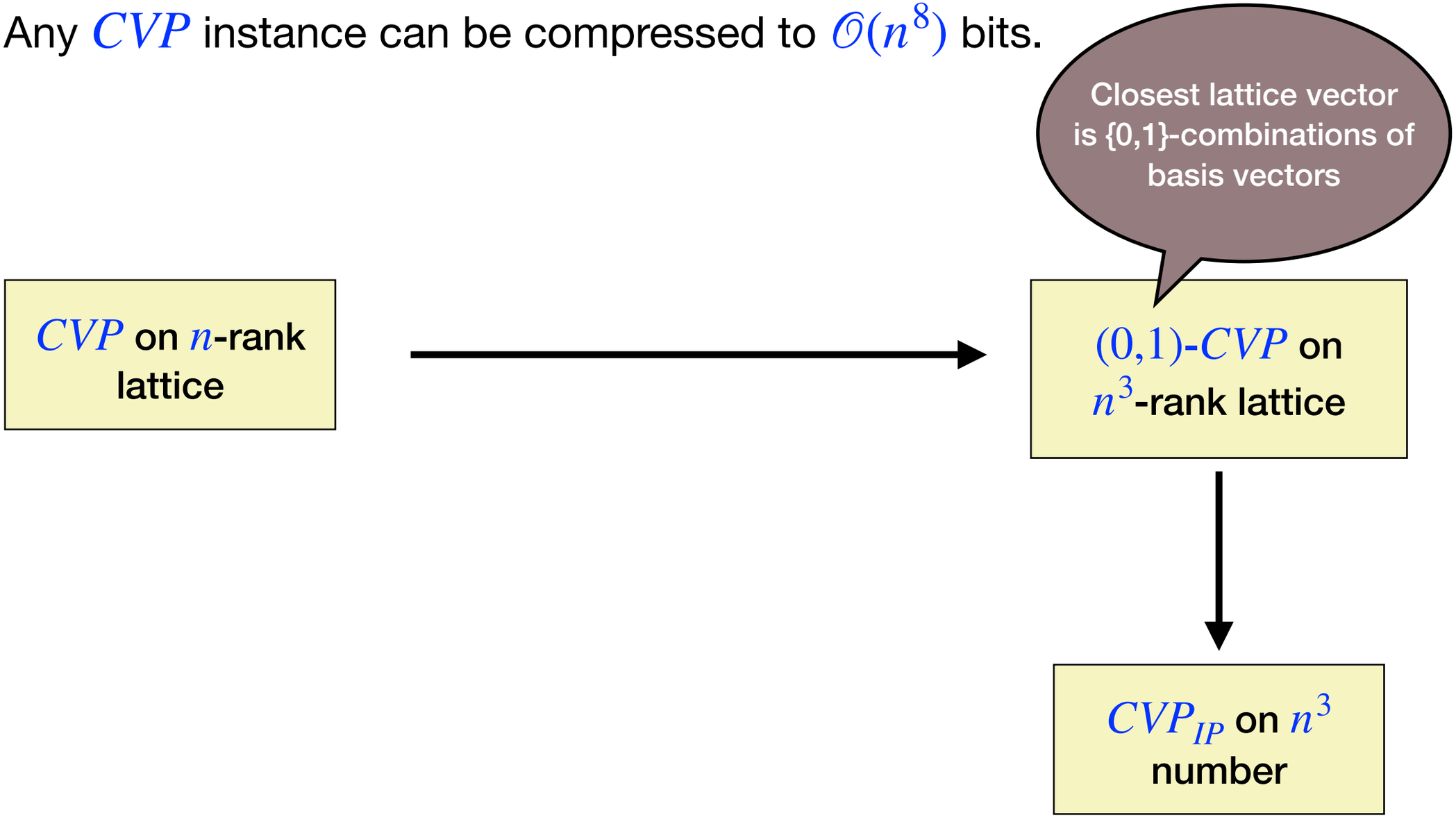
Instance Compression

➡ Any CVP instance can be compressed to $\mathcal{O}(n^8)$ bits.



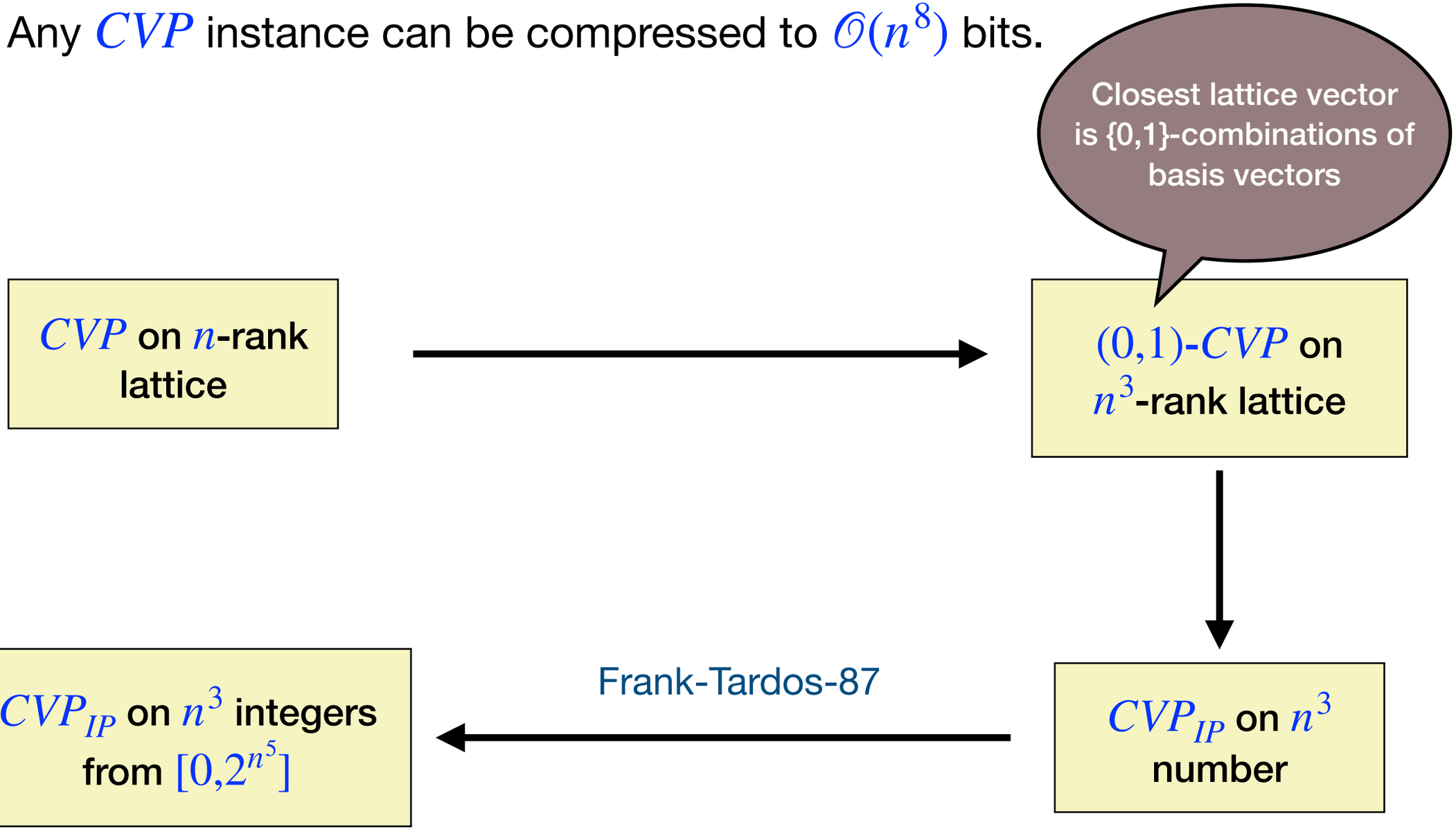
Instance Compression

➡ Any CVP instance can be compressed to $\mathcal{O}(n^8)$ bits.



Instance Compression

➡ Any CVP instance can be compressed to $\mathcal{O}(n^8)$ bits.




for all constant k
k-SAT on n variables
CVP on Cn-rank lattice

for all constant k

k-SAT on n variables

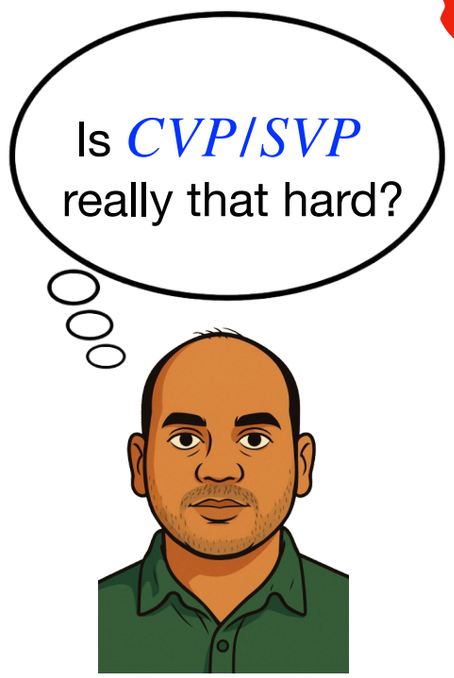
CVP on Cn-rank lattice

Is CVP/SVP really that hard?

for all constant k

k-SAT on n variables

CVP on Cn-rank lattice

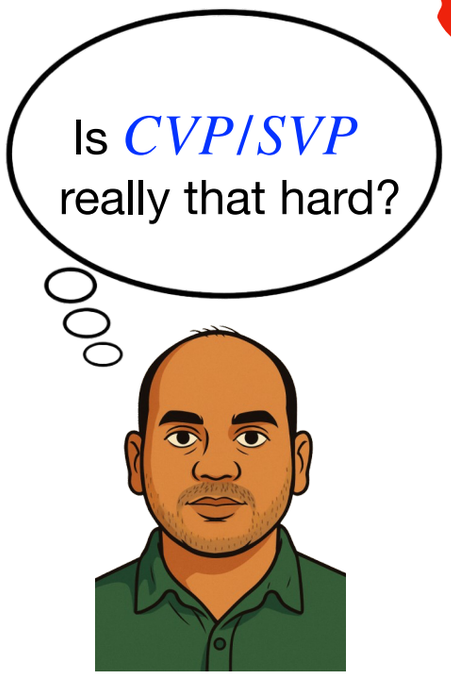


$Weighted$-Max-2-SAT on n-variables

for all constant k

k-SAT on n variables

CVP on Cn-rank lattice



$Weighted$-Max-2-SAT on n-variables

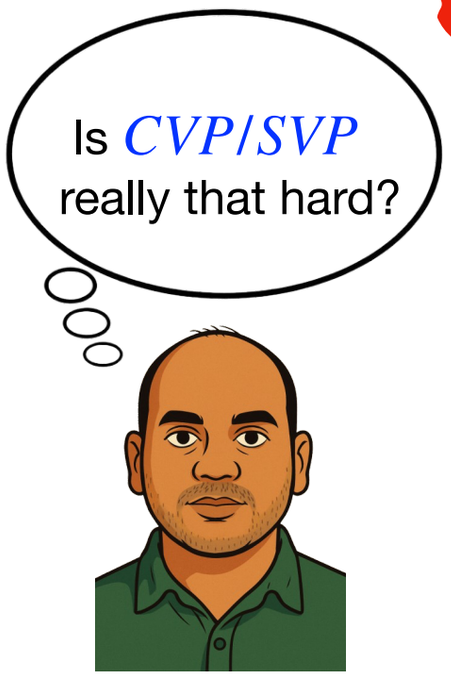
[Bennett-Golovnev-StephensDavidowitz 17]

$(0,1)$-CVP on n-rank lattice

for all constant k

k-SAT on n variables

CVP on Cn-rank lattice



$Weighted$-Max-2-SAT on n-variables

[Bennett-Golovnev-StephensDavidowitz 17]

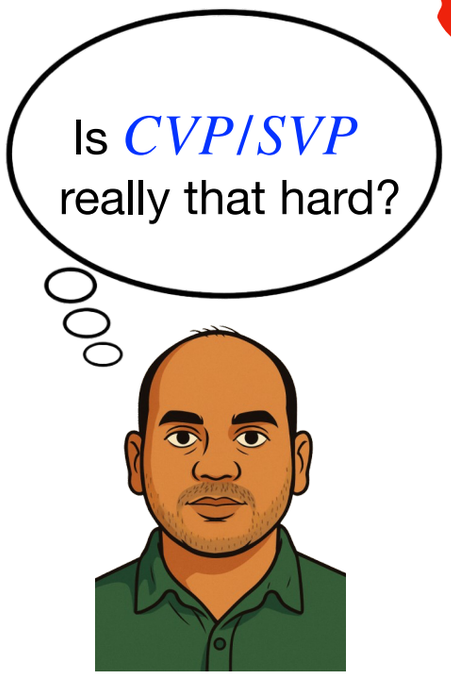
$(0,1)$-CVP on n-rank lattice

[Abboud-Kumar-25]

for all constant k

k-SAT on n variables

CVP on Cn-rank lattice



$Weighted$-Max-2-SAT on n-variables

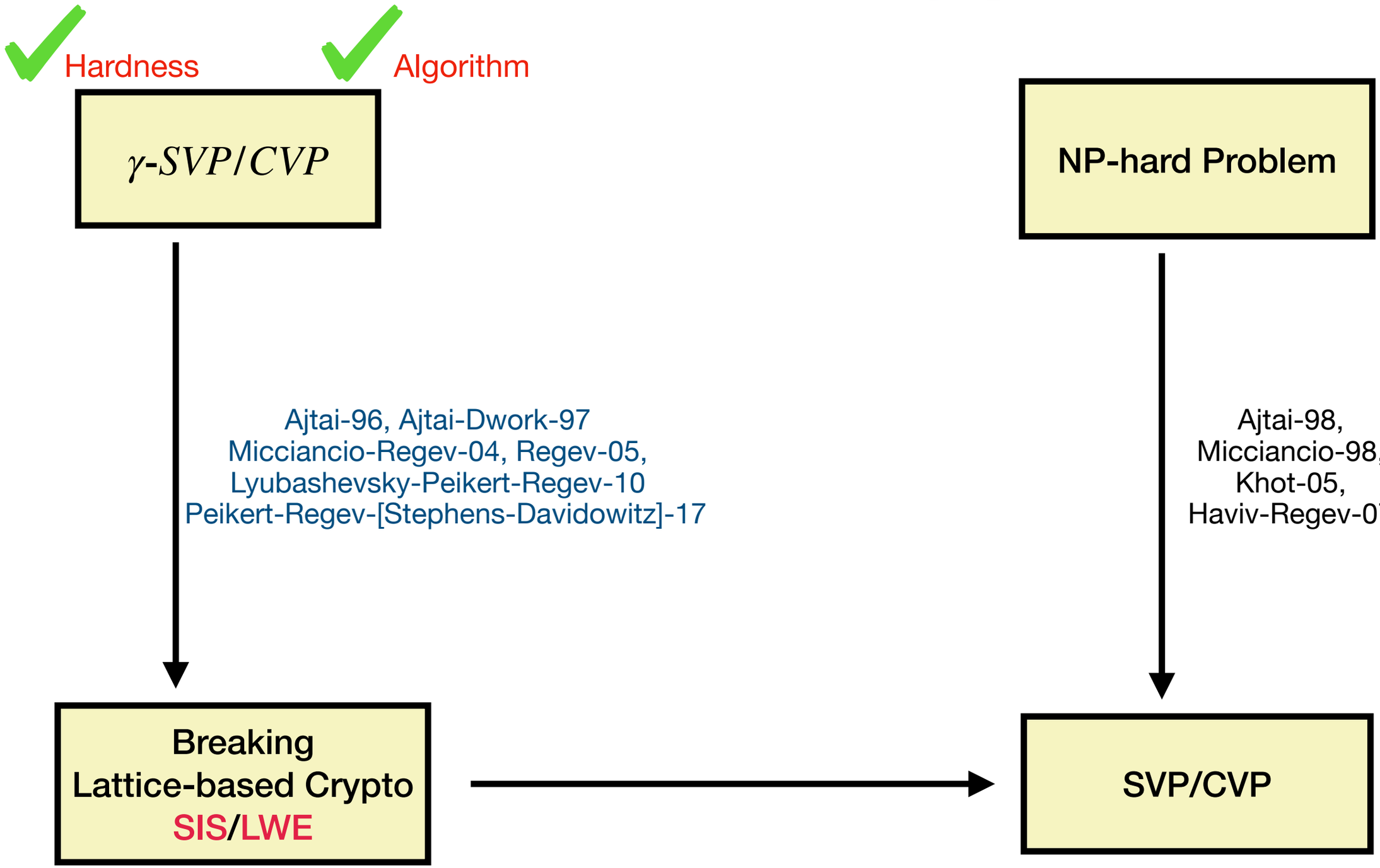
[Bennett-Golovnev-StephensDavidowitz 17]

$(0,1)$-CVP on n-rank lattice

[Abboud-Kumar-25]

Open problem: Rank-preserving reduction from CVP to $(0,1)$-CVP

Lattice-based Crypto



Lattice-based Crypto

✓ Hardness ✓ Algorithm

γ-SVP/CVP

Can we build crypto on relatively hard problems?

Ajtai-96, Ajtai-Dwork-97
Micciancio-Regev-04, Regev-05,
Lyubashevsky-Peikert-Regev-10
Peikert-Regev-[Stephens-Davidowitz]-17

Breaking Lattice-based Crypto SIS/LWE

NP-hard Problem

Ajtai-98,
Micciancio-98,
Khot-05,
Haviv-Regev-07

SVP/CVP

LWE and SIS

➡️ Security of lattice-based crypto is equivalent to hardness of average-case lattice problems: Learning with Errors (LWE) and Short Integer Solutions (SIS).

LWE and SIS

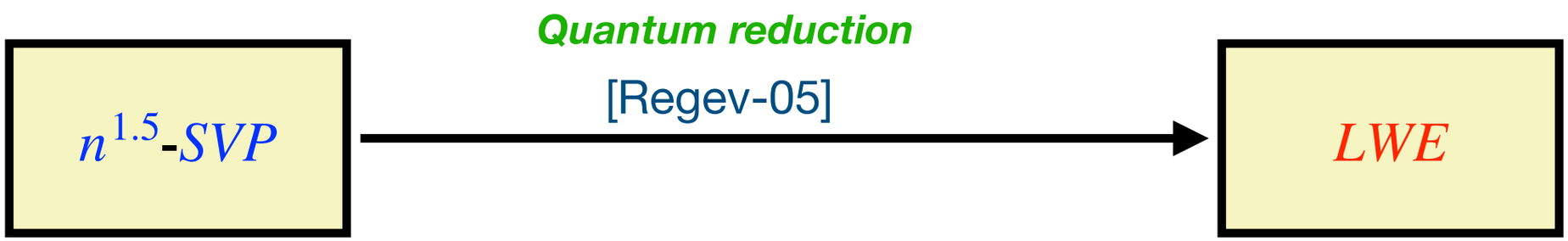
➡️ Security of lattice-based crypto is equivalent to hardness of average-case lattice problems: Learning with Errors (LWE) and Short Integer Solutions (SIS).

LWE and SIS

➡️ Security of lattice-based crypto is equivalent to hardness of average-case lattice problems: Learning with Errors (LWE) and Short Integer Solutions (SIS).

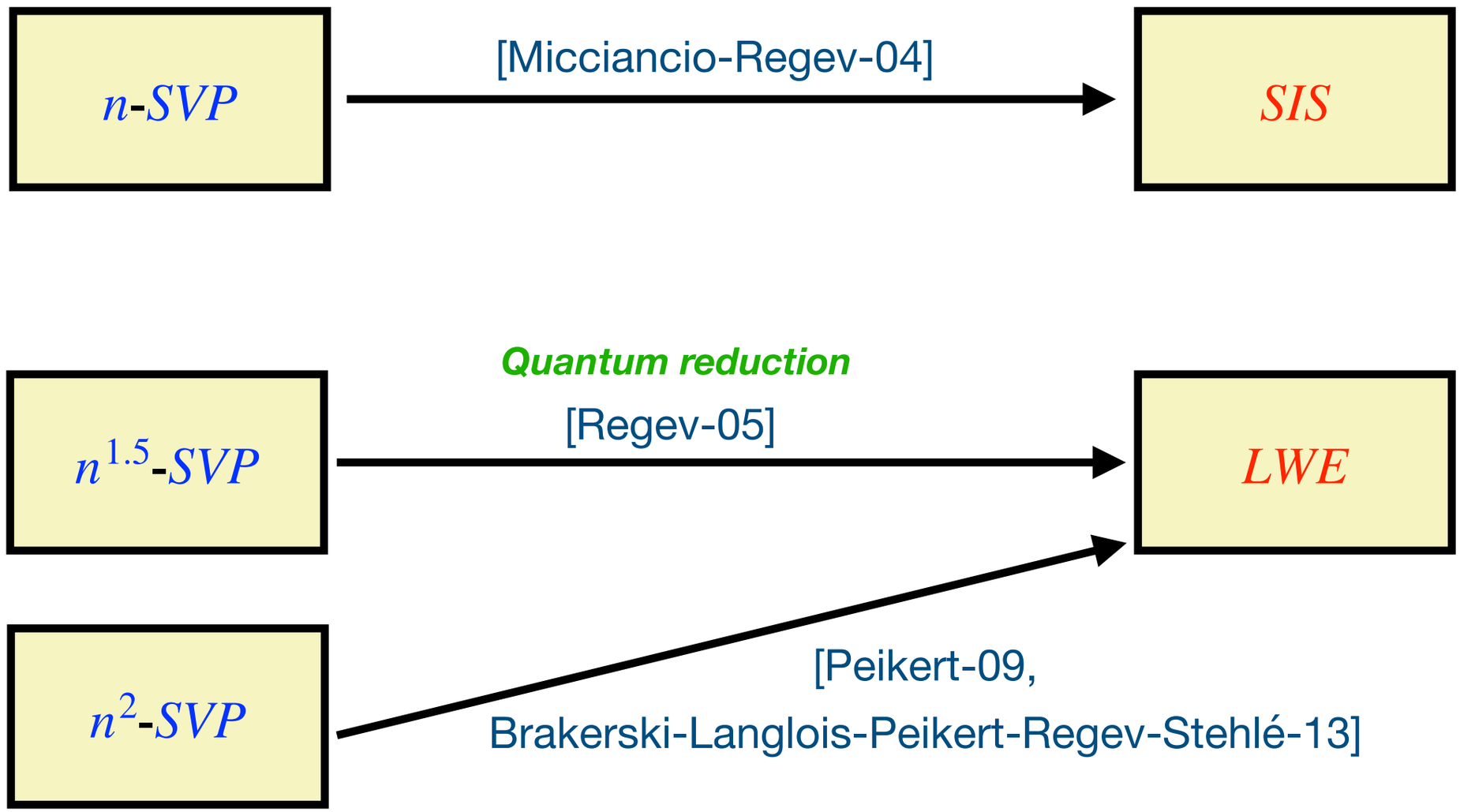
LWE and SIS

➡️ Security of lattice-based crypto is equivalent to hardness of average-case lattice problems: Learning with Errors (LWE) and Short Integer Solutions (SIS).



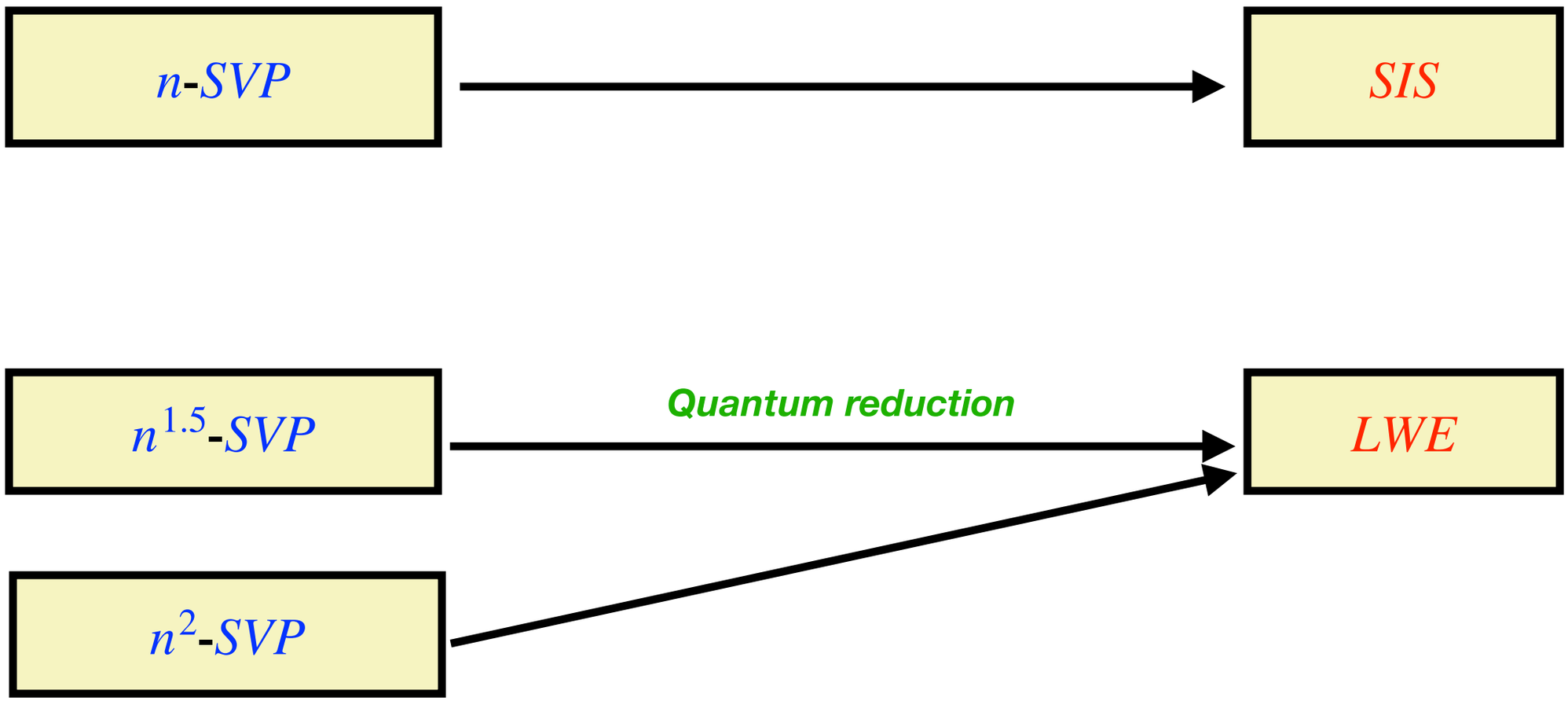
LWE and SIS

➡️ Security of lattice-based crypto is equivalent to hardness of average-case lattice problems: Learning with Errors (LWE) and Short Integer Solutions (SIS).



LWE and SIS

➡ We need exponential hardness of LWE and SIS for real-world security.

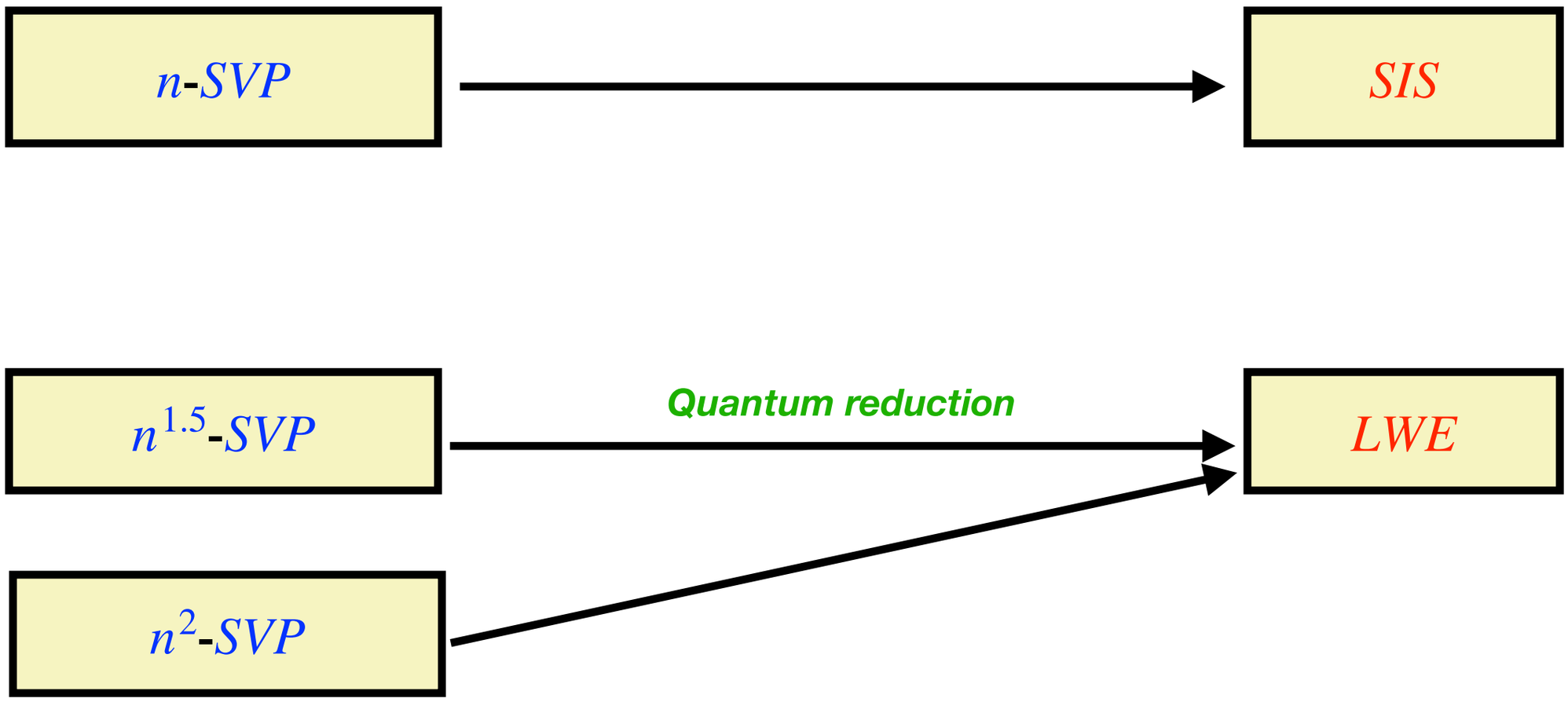


LWE and SIS

➡ We need exponential hardness of LWE and SIS for real-world security.

Can we improve the hardness by allowing $2^{\epsilon n}$ time reduction ?

[Aggarwal-Bennett-Brakerski-Golovnev-Kumar-Li-Peters-StephensDavidowitz-Vaikuntanathan-23]

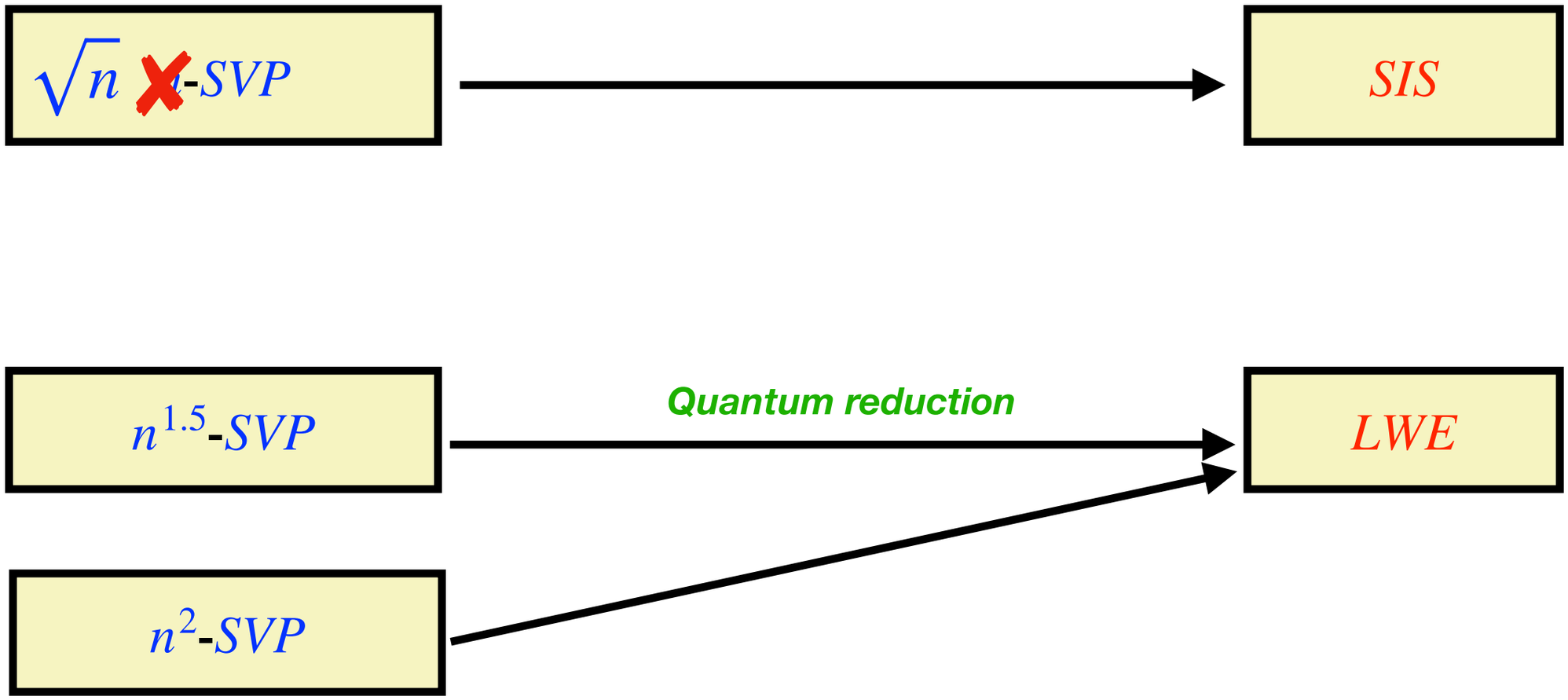


LWE and SIS

We need exponential hardness of LWE and SIS for real-world security.

Can we improve the hardness by allowing $2^{\epsilon n}$ time reduction ?

[Aggarwal-Bennett-Brakerski-Golovnev-Kumar-Li-Peters-StephensDavidowitz-Vaikuntanathan-23]

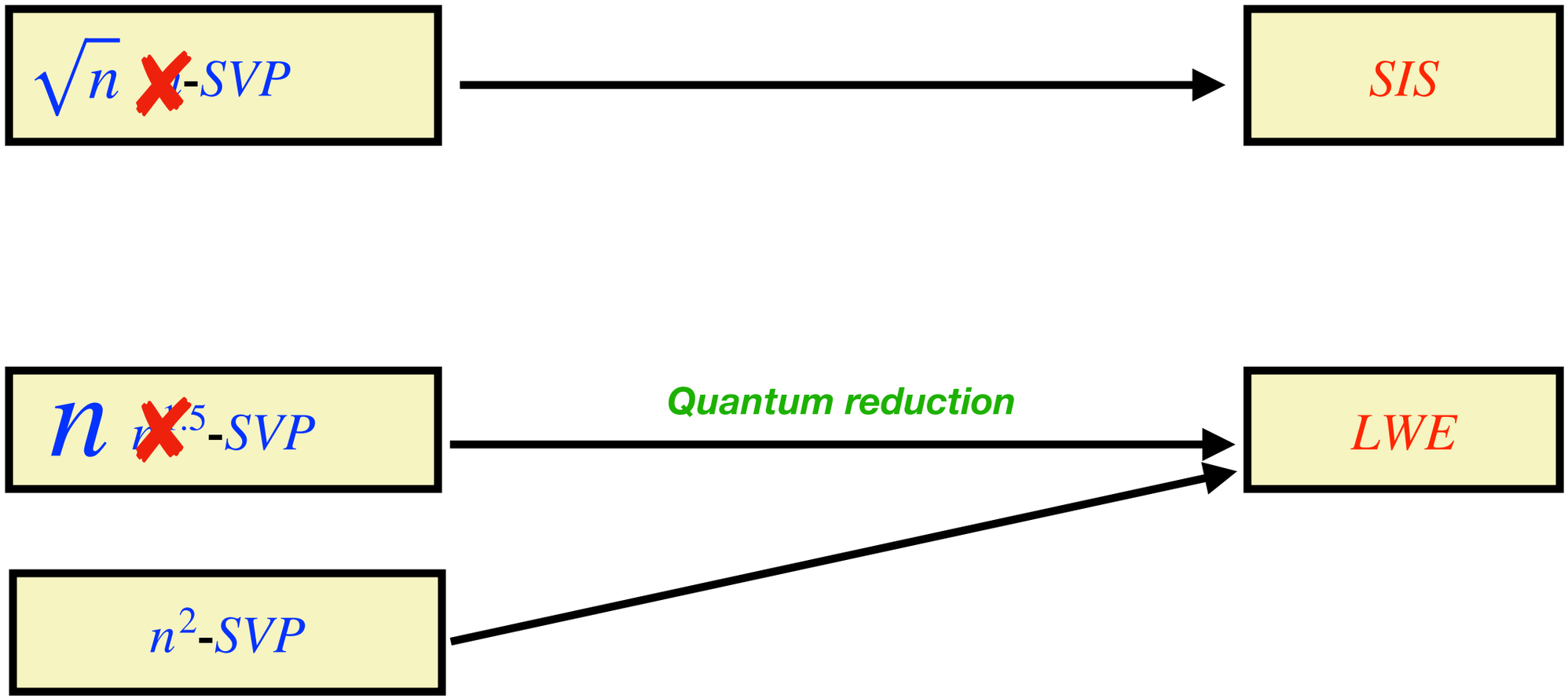


LWE and SIS

We need exponential hardness of LWE and SIS for real-world security.

Can we improve the hardness by allowing $2^{\epsilon n}$ time reduction ?

[Aggarwal-Bennett-Brakerski-Golovnev-Kumar-Li-Peters-StephensDavidowitz-Vaikuntanathan-23]

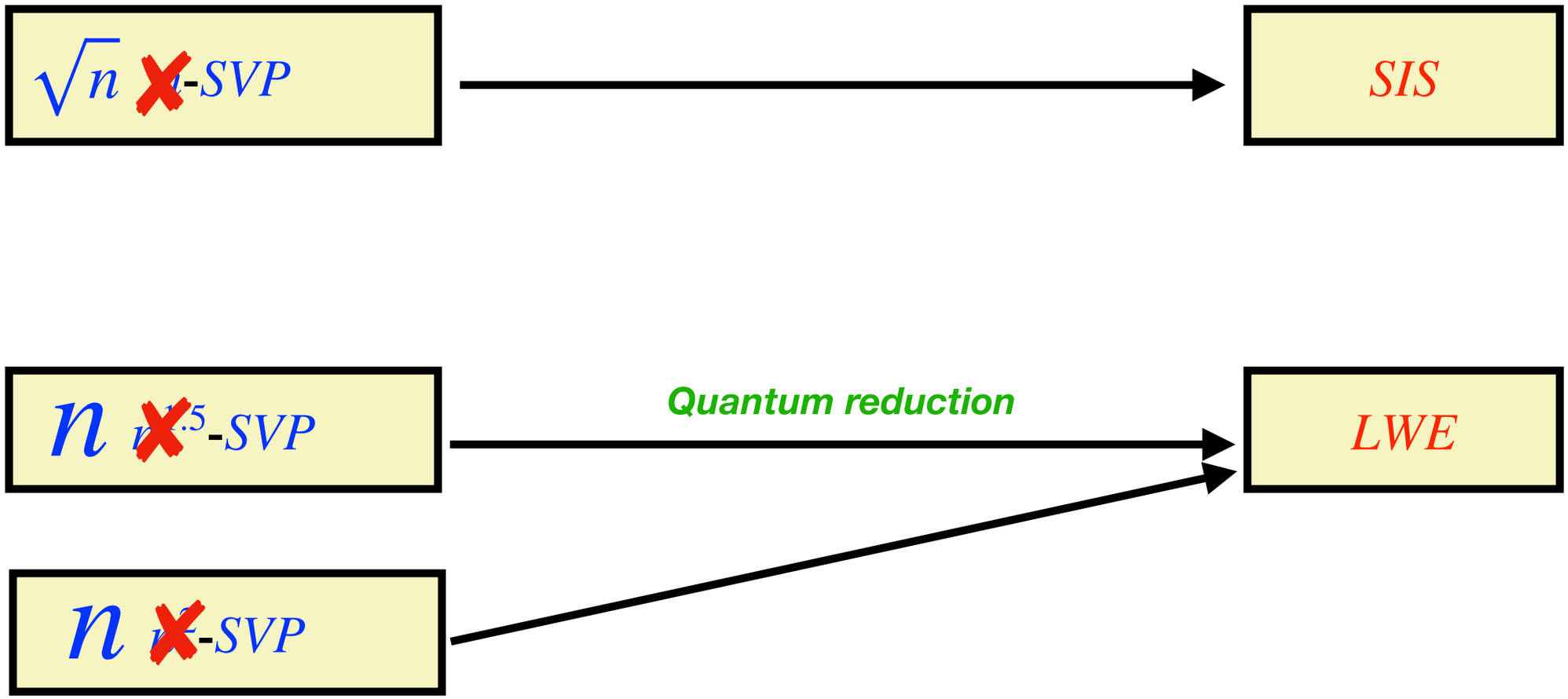


LWE and SIS

We need exponential hardness of LWE and SIS for real-world security.

Can we improve the hardness by allowing $2^{\epsilon n}$ time reduction ?

[Aggarwal-Bennett-Brakerski-Golovnev-Kumar-Li-Peters-StephensDavidowitz-Vaikuntanathan-23]



One more barrier!

➡ Can we show the exponential hardness of n^{ϵ}-SVP/CVP ?

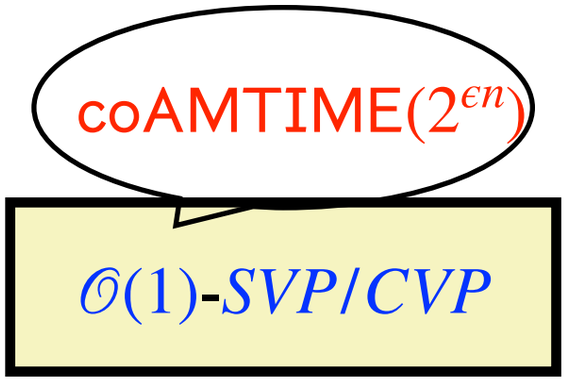
One more barrier!

➡ Can we show the exponential hardness of n^{ϵ}-SVP/CVP ?

$\mathcal{O}(1)$-SVP/CVP

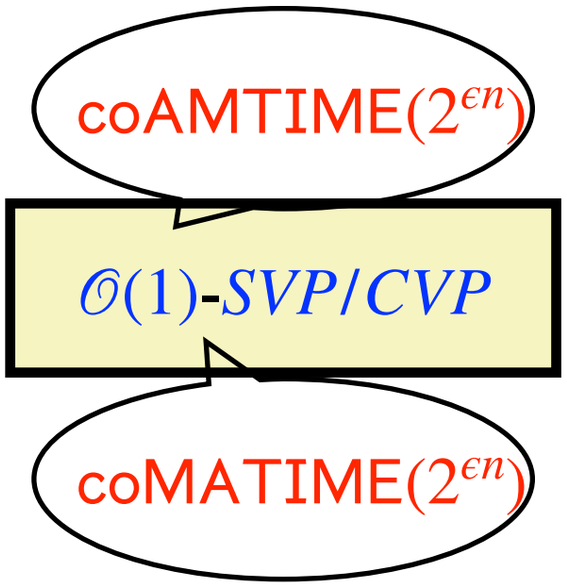
One more barrier!

➡ Can we show the exponential hardness of n^{ϵ}-SVP/CVP ?



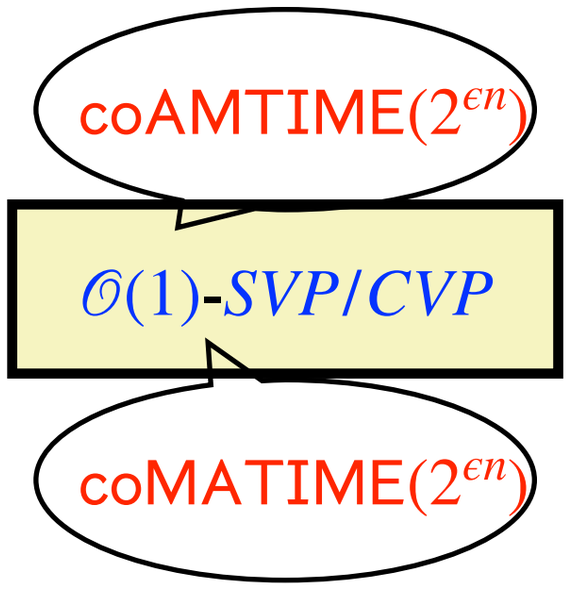
One more barrier!

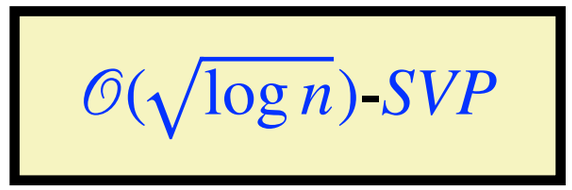
➡ Can we show the exponential hardness of n^{ϵ}-SVP/CVP ?



One more barrier!

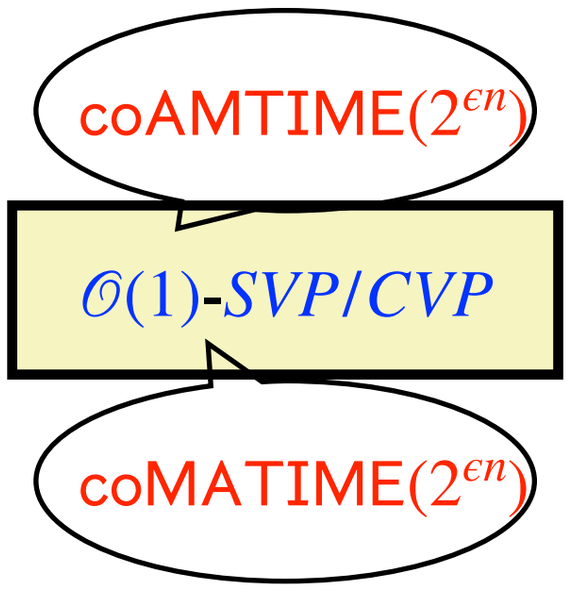
⇨ Can we show the exponential hardness of n^{ϵ}-SVP/CVP ?

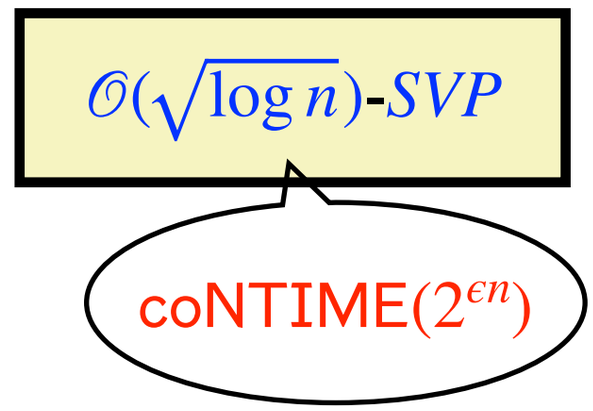




One more barrier!

➡ Can we show the exponential hardness of n^{ϵ}-SVP/CVP ?





One more barrier!

Can we show the exponential hardness of n^{ϵ}-SVP/CVP ?

It is conjectured that such protocols are not possible for k-SAT.

One more barrier!

Goldreich-Goldwasser-00

One more barrier!

Goldreich-Goldwasser-00

 coAMTIME(T) protocol for approx-CVP.

1. YES instance: If dist($\vec{t}, L$) $\leq d$

2. NO instance: If dist($\vec{t}, L$) > 2

One more barrier!

Goldreich-Goldwasser-00

⇨ coAMTIME(T) protocol for approx-CVP.

1. YES instance: If dist($\vec{t}, L$) $\leq d$

2. NO instance: If dist($\vec{t}, L$) > 2

Arthur

(Computationally bounded)

One more barrier!

Goldreich-Goldwasser-00

⇨ coAMTIME(T) protocol for approx-CVP.

1. YES instance: If dist($\vec{t}, L$) $\leq d$

2. NO instance: If dist($\vec{t}, L$) > 2

Arthur

(Computationally bounded)

Merlin

(All powerful)

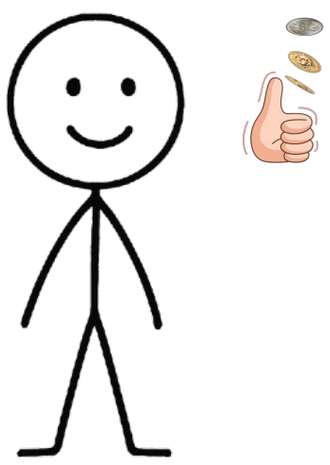
One more barrier!

Goldreich-Goldwasser-00

⇨ coAMTIME(T) protocol for approx-CVP.

1. YES instance: If dist($\vec{t}, L$) $\leq d$

2. NO instance: If dist($\vec{t}, L$) > 2



Arthur

(Computationally bounded)

Merlin

(All powerful)

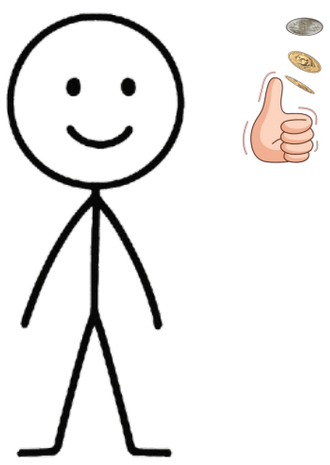
One more barrier!

Goldreich-Goldwasser-00

➡ coAMTIME(T) protocol for approx-CVP.

1. YES instance: If dist($\vec{t}, L$) $\leq d$

2. NO instance: If dist($\vec{t}, L$) > 2



Arthur

(Computationally bounded)

Query

Merlin

(All powerful)

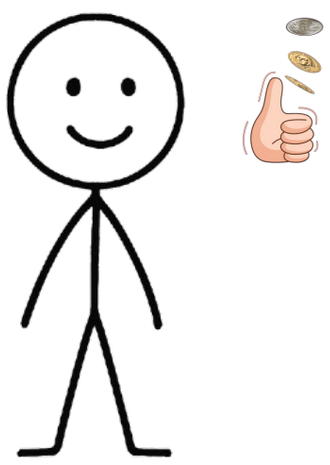
One more barrier!

Goldreich-Goldwasser-00

⇨ coAMTIME(T) protocol for approx-CVP.

1. YES instance: If dist($\vec{t}, L$) $\leq d$

2. NO instance: If dist($\vec{t}, L$) > 2



Query

Response

Arthur
(Computationally bounded)

Merlin
(All powerful)

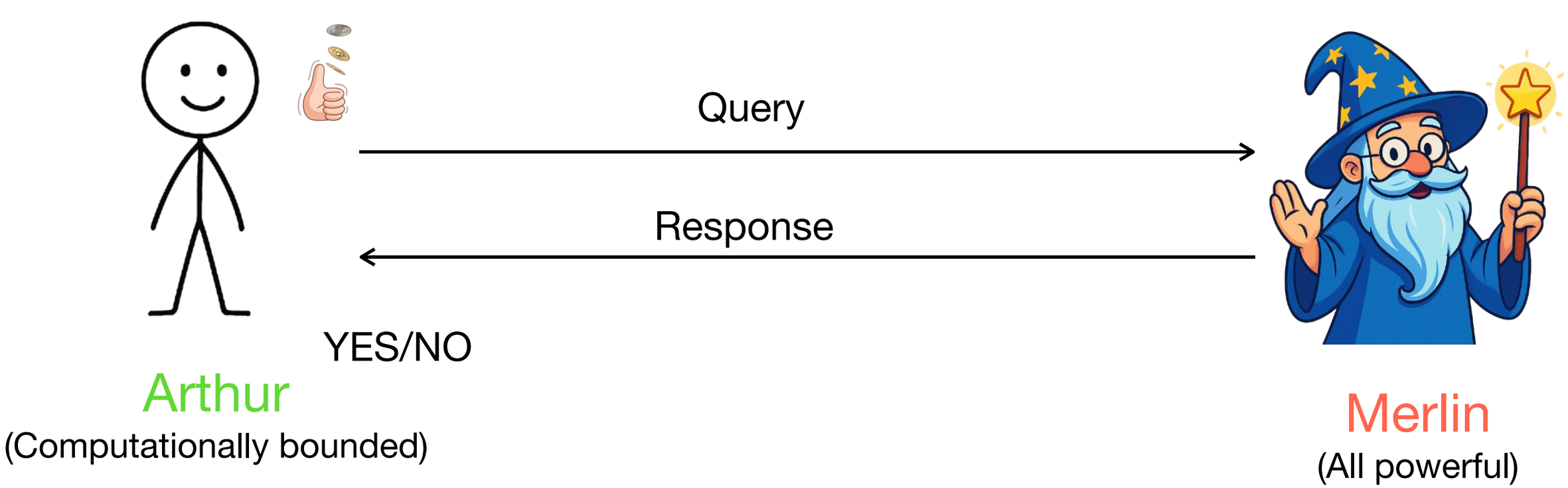
One more barrier!

Goldreich-Goldwasser-00

➡ coAMTIME(T) protocol for approx-CVP.

1. YES instance: If dist($\vec{t}, L$) $\leq d$

2. NO instance: If dist($\vec{t}, L$) > 2



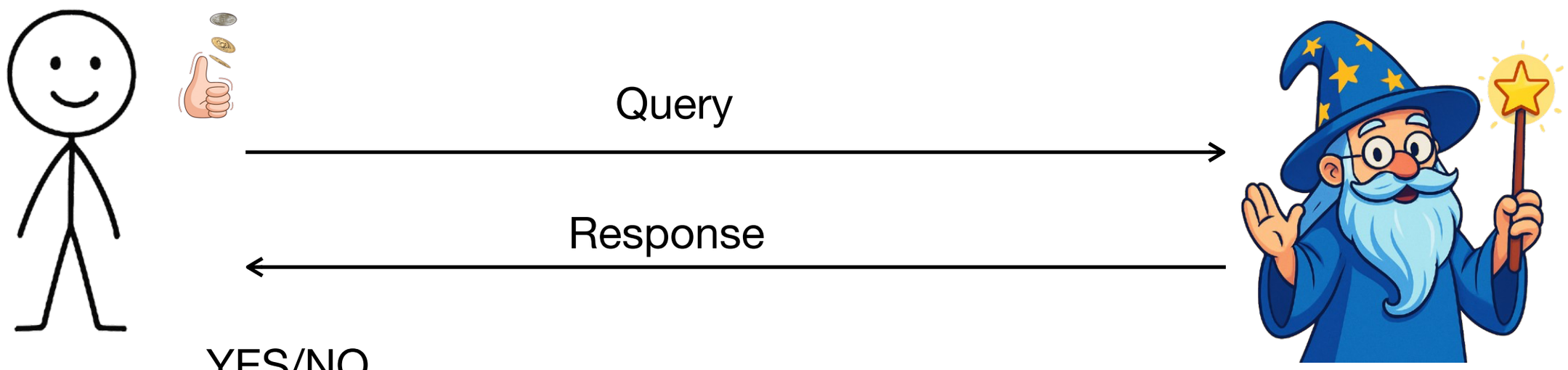
One more barrier!

Goldreich-Goldwasser-00

⇒ coAMTIME(T) protocol for approx-CVP.

1. YES instance: If dist($\vec{t}, L$) $\leq d$

2. NO instance: If dist($\vec{t}, L$) > 2 Merlin convinces Arthur that $\vec{t}$ is far from lattice.

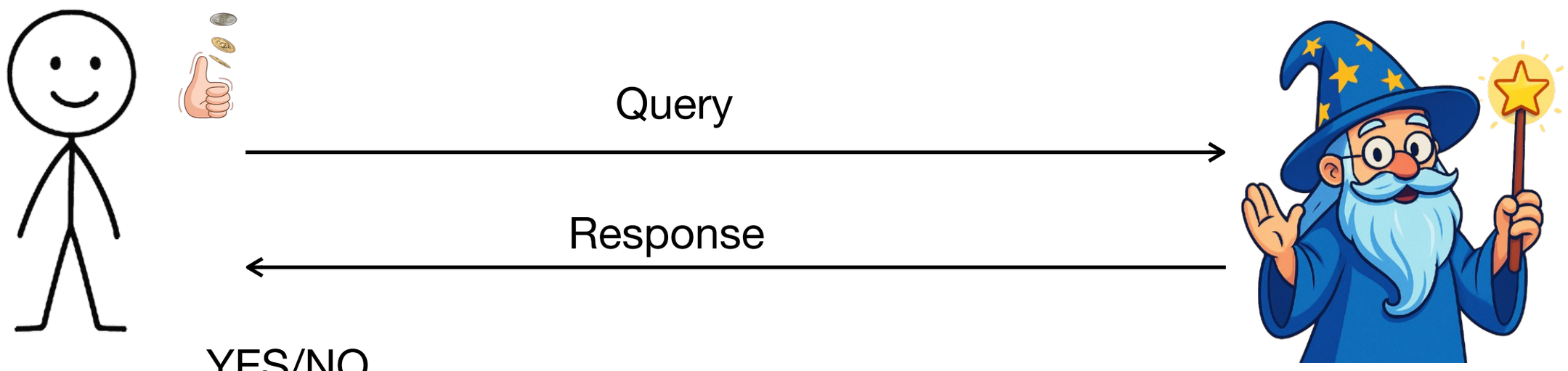


One more barrier!

Goldreich-Goldwasser-00

coAMTIME(T) protocol for approx-CVP.

1. YES instance: If $\text{dist}(\vec{t}, L) \leq d$ Merlin will not be able to convince Arthur that $\vec{t}$ is far from lattice.
2. NO instance: If $\text{dist}(\vec{t}, L) > 2$ Merlin convinces Arthur that $\vec{t}$ is far from lattice.



One more barrier!

One more barrier!

$\mathscr{B} = \{\vec{x} \in \mathbb{R}^m \,|\, \|\vec{x}\| \leq 1\}$ (unit radius ball)

One more barrier!

$\mathscr{B} = \{\vec{x} \in \mathbb{R}^m \,|\, ||\vec{x}|| \leq 1\}$ (unit radius ball)

$S_0 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{y}$

One more barrier!

$\mathscr{B} = \{\vec{x} \in \mathbb{R}^m \,|\, \|\vec{x}\| \leq 1\}$ (unit radius ball)

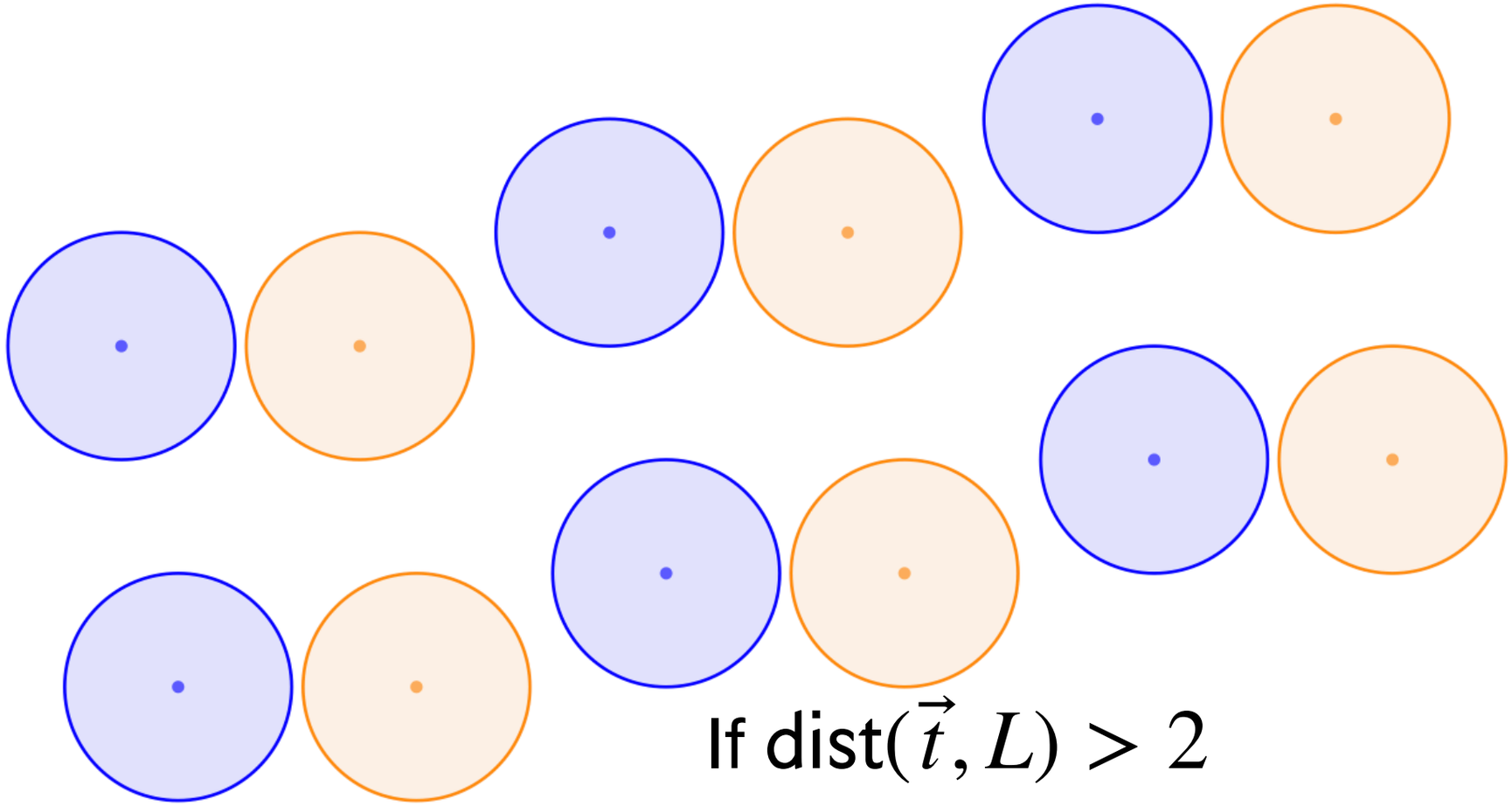
$S_0 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{y}$

$S_1 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{t} + \vec{y}$

One more barrier!

$\mathscr{B} = \{\vec{x} \in \mathbb{R}^m \,|\, ||\vec{x}|| \leq 1\}$ (unit radius ball)

$S_0 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{y}$ $S_1 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{t} + \vec{y}$

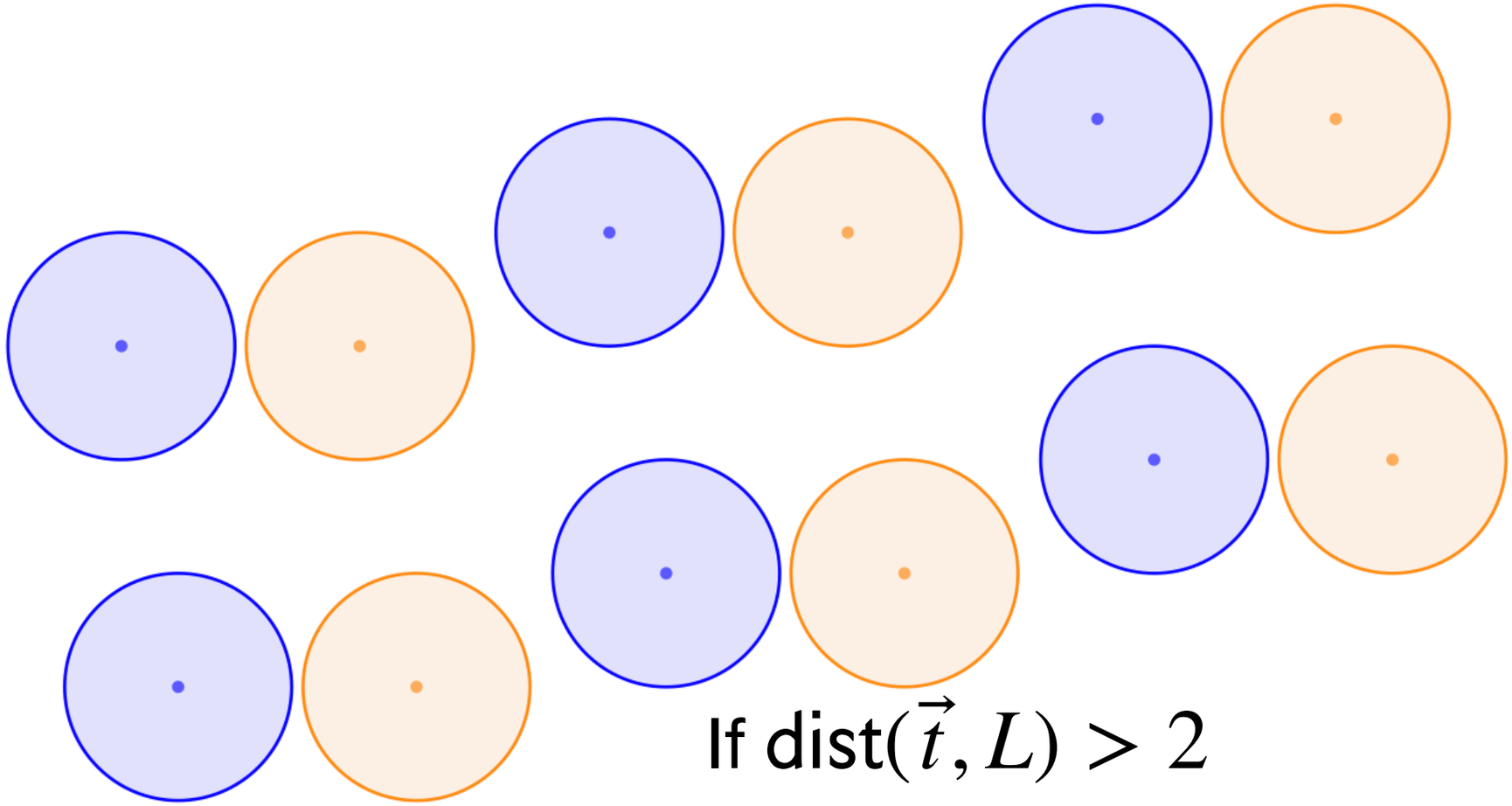


If dist$(\vec{t}, L) > 2$

One more barrier!

$\mathscr{B} = \{\vec{x} \in \mathbb{R}^m \,|\, \|\vec{x}\| \leq 1\}$ (unit radius ball)

$S_0 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{y}$  $S_1 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{t} + \vec{y}$



If dist$(\vec{t}, L) > 2$

One more barrier!

$\mathscr{B} = \{\vec{x} \in \mathbb{R}^m \,|\, \|\vec{x}\| \leq 1\}$ (unit radius ball)

$S_0 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{y}$  $S_1 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{t} + \vec{y}$

One more barrier!

$\mathscr{B} = \{\vec{x} \in \mathbb{R}^m \,|\, \|\vec{x}\| \leq 1\}$ (unit radius ball)

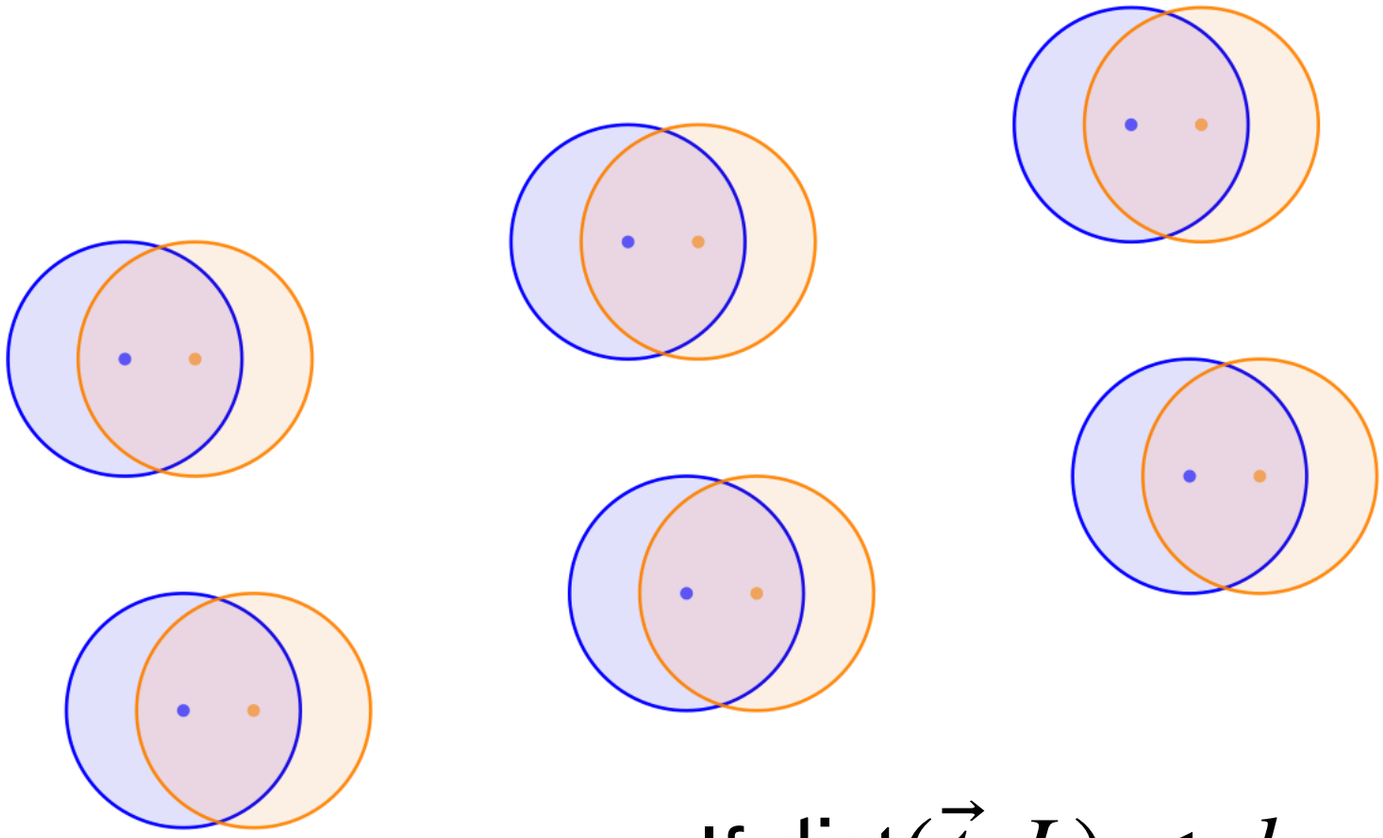
$S_0 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{y}$  $S_1 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{t} + \vec{y}$

If dist$(\vec{t}, L) < d$

One more barrier!

$\mathscr{B} = \{\vec{x} \in \mathbb{R}^m \,|\, ||\vec{x}|| \leq 1\}$ (unit radius ball)

$S_0 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{y}$  $S_1 = \cup_{\vec{y} \in L} \mathscr{B} + \vec{t} + \vec{y}$



If dist$(\vec{t}, L) < d$

$$\sum_{\vec{v}\in L}\sum_{\vec{x}\in\mathcal{B}} |0\rangle\,|\vec{v}\rangle\,|\vec{x}+\vec{v}\rangle + |1\rangle\,|\vec{v}+\vec{t}\rangle\,|\vec{x}+\vec{v}+\vec{t}\rangle$$

$$\sum_{\vec{v}\in L}\sum_{\vec{x}\in\mathcal{B}} |0\rangle\,|\vec{v}\rangle\,|\vec{x}+\vec{v}\rangle + |1\rangle\,|\vec{v}+\vec{t}\rangle\,|\vec{x}+\vec{v}+\vec{t}\rangle$$

Measure last register

$$\sum_{\vec{v}\in L}\sum_{\vec{x}\in\mathcal{B}} |0\rangle\,|\vec{v}\rangle\,|\vec{x}+\vec{v}\rangle + |1\rangle\,|\vec{v}+\vec{t}\rangle\,|\vec{x}+\vec{v}+\vec{t}\rangle$$

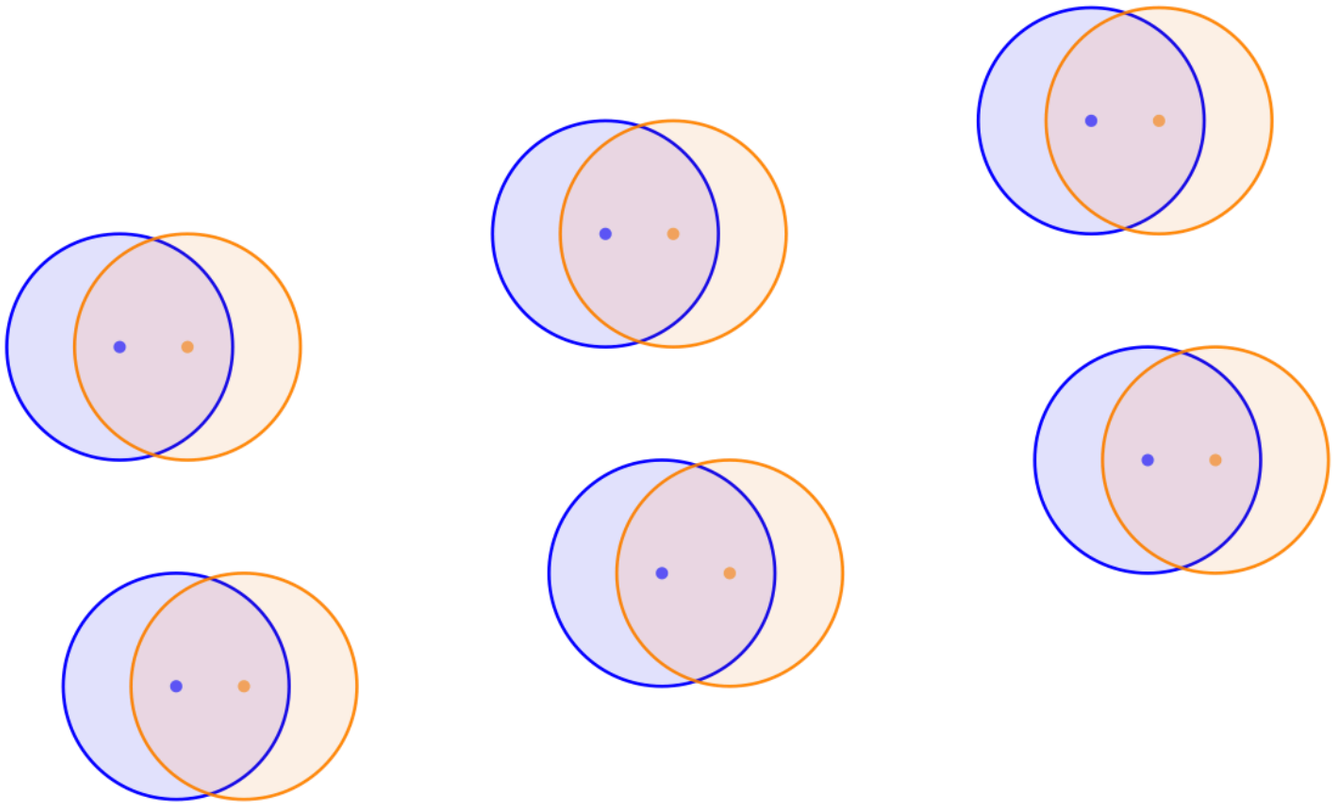
Measure last register

$$|0\rangle\,|\vec{v}\rangle + |1\rangle\,|\vec{v'}+\vec{t}\rangle$$

$$\sum_{\vec{v}\in L}\sum_{\vec{x}\in\mathcal{B}} |0\rangle\,|\vec{v}\rangle\,|\vec{x}+\vec{v}\rangle + |1\rangle\,|\vec{v}+\vec{t}\rangle\,|\vec{x}+\vec{v}+\vec{t}\rangle$$

Measure last register

$$|0\rangle\,|\vec{v}\rangle + |1\rangle\,|\vec{v'}+\vec{t}\rangle$$



$$\sum_{\vec{v}\in L}\sum_{\vec{x}\in\mathcal{B}} |0\rangle\,|\vec{v}\rangle\,|\vec{x}+\vec{v}\rangle + |1\rangle\,|\vec{v}+\vec{t}\rangle\,|\vec{x}+\vec{v}+\vec{t}\rangle$$

Measure last register

$$|0\rangle\,|\vec{v}\rangle + |1\rangle\,|\vec{v'}+\vec{t}\rangle$$

$$\sum_{\vec{v}\in L}\sum_{\vec{x}\in\mathcal{B}} |0\rangle|\vec{v}\rangle|\vec{x}+\vec{v}\rangle + |1\rangle|\vec{v}+\vec{t}\rangle|\vec{x}+\vec{v}+\vec{t}\rangle$$

Measure last register

With
$1 - poly(1/n)$ prob.

$$|0\rangle|\vec{v}\rangle + |1\rangle|\vec{v'}+\vec{t}\rangle$$

$$\sum_{\vec{v}\in L}\sum_{\vec{x}\in\mathcal{B}} |0\rangle|\vec{v}\rangle|\vec{x}+\vec{v}\rangle + |1\rangle|\vec{v}+\vec{t}\rangle|\vec{x}+\vec{v}+\vec{t}\rangle$$

Measure last register

With $1-poly(1/n)$ prob.

$$|0\rangle|\vec{v}\rangle + |1\rangle|\vec{v'}+\vec{t}\rangle$$

$$|0\rangle|\vec{v}\rangle + |1\rangle|\vec{v}+(\vec{v'}+\vec{t}-\vec{v})\rangle$$

$$\sum_{\vec{v}\in L}\sum_{\vec{x}\in\mathcal{B}} |0\rangle|\vec{v}\rangle|\vec{x}+\vec{v}\rangle + |1\rangle|\vec{v}+\vec{t}\rangle|\vec{x}+\vec{v}+\vec{t}\rangle$$

Measure last register

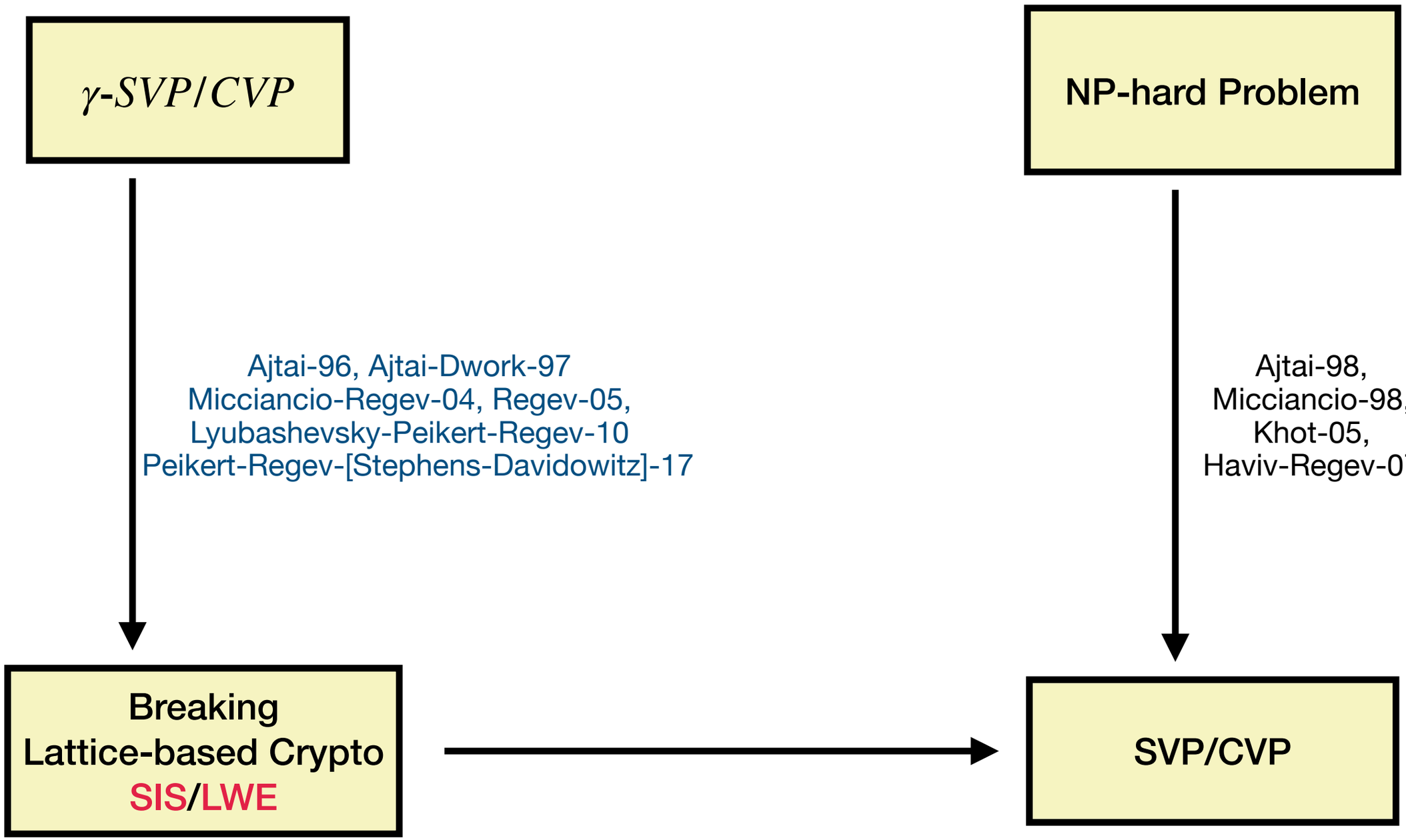
With $1-poly(1/n)$ prob.

$$|0\rangle|\vec{v}\rangle + |1\rangle|\vec{v'}+\vec{t}\rangle$$

$$|0\rangle|\vec{v}\rangle + |1\rangle|\vec{v}+(\vec{v'}+\vec{t}-\vec{v})\rangle$$

Dihedral Hidden Subgroup Problem

Conclusion


γ-SVP/CVP
Ajtai-96, Ajtai-Dwork-97
Micciancio-Regev-04, Regev-05,
Lyubashevsky-Peikert-Regev-10
Peikert-Regev-[Stephens-Davidowitz]-17
NP-hard Problem
Ajtai-98,
Micciancio-98,
Khot-05,
Haviv-Regev-07
Breaking
Lattice-based Crypto
SIS/LWE
SVP/CVP

Conclusion

γ-SVP/CVP

Why Lattice?

NP-hard Problem

Ajtai-96, Ajtai-Dwork-97
Micciancio-Regev-04, Regev-05,
Lyubashevsky-Peikert-Regev-10
Peikert-Regev-[Stephens-Davidowitz]-17

Ajtai-98,
Micciancio-98,
Khot-05,
Haviv-Regev-07

Breaking
Lattice-based Crypto
SIS/LWE

SVP/CVP

Open Problems

Open Problems

➡️ Can we improve the success prob. for reduction from lattice problems to Dihedral hidden subgroup problem?

Open Problems

➡ Can we improve the success prob. for reduction from lattice problems to Dihedral hidden subgroup problem?

➡ Faster quantum algorithms for SVP/CVP.

Open Problems

➡ Can we improve the success prob. for reduction from lattice problems to Dihedral hidden subgroup problem?

➡ Faster quantum algorithms for SVP/CVP.

➡ Quantum advantage for reduction from approx-SVP/CVP to exact-SVP/CVP on smaller dimension.

Open Problems

➡ Can we improve the success prob. for reduction from lattice problems to Dihedral hidden subgroup problem?

➡ Faster quantum algorithms for SVP/CVP.

➡ Quantum advantage for reduction from approx-SVP/CVP to exact-SVP/CVP on smaller dimension.

➡ Quantum fine-grained hardness of approx-SVP/CVP.

Open Problems

➡ Can we improve the success prob. for reduction from lattice problems to Dihedral hidden subgroup problem?

➡ Faster quantum algorithms for SVP/CVP.

➡ Quantum advantage for reduction from approx-SVP/CVP to exact-SVP/CVP on smaller dimension.

➡ Quantum fine-grained hardness of approx-SVP/CVP.

Thank you!