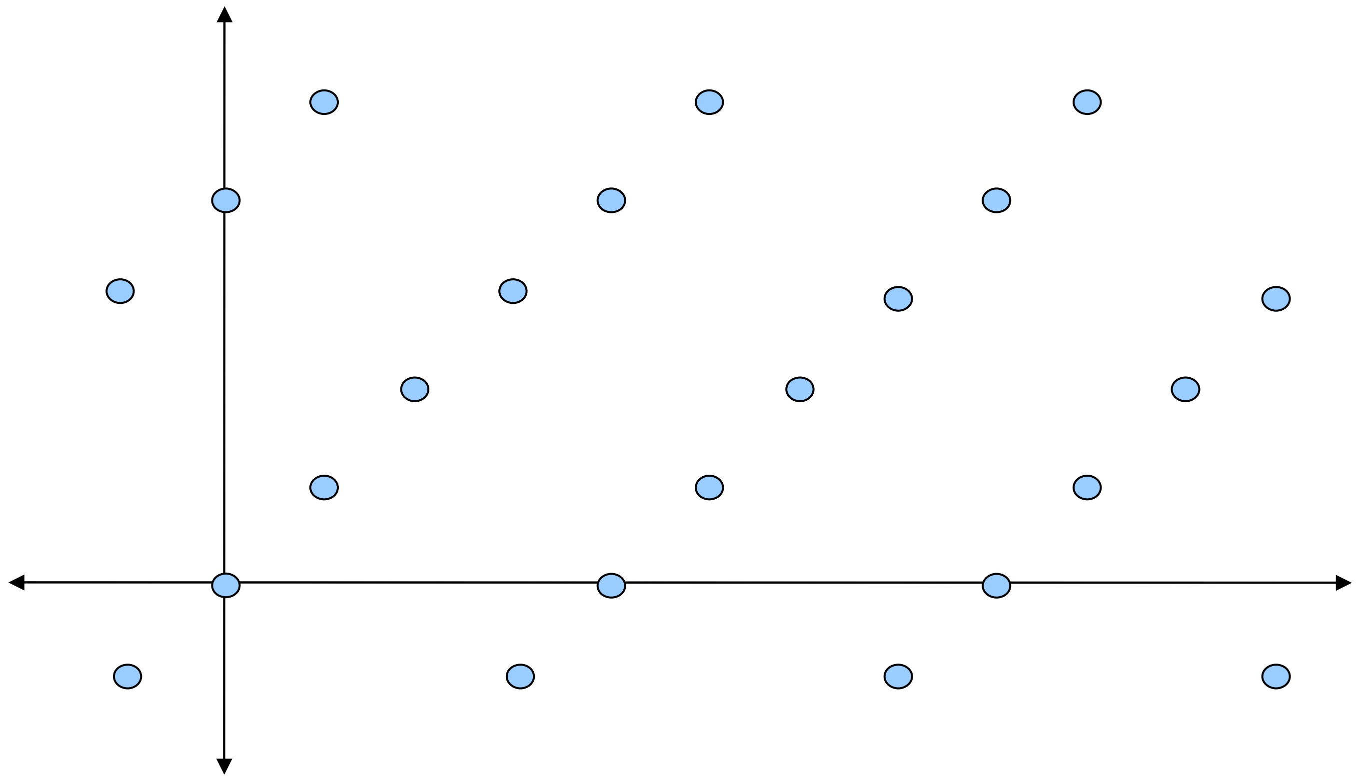
On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem

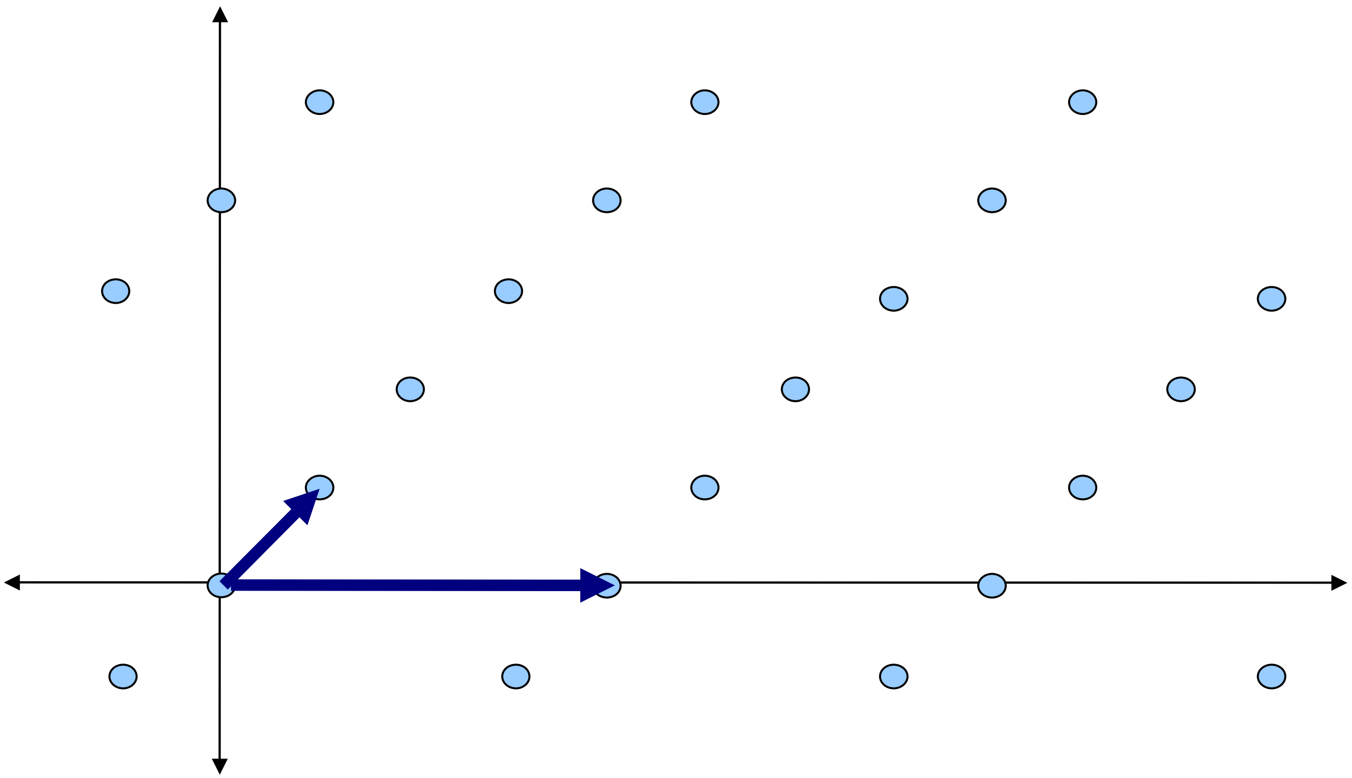
Vadim Lyubashevsky Daniele Micciancio

Lattices



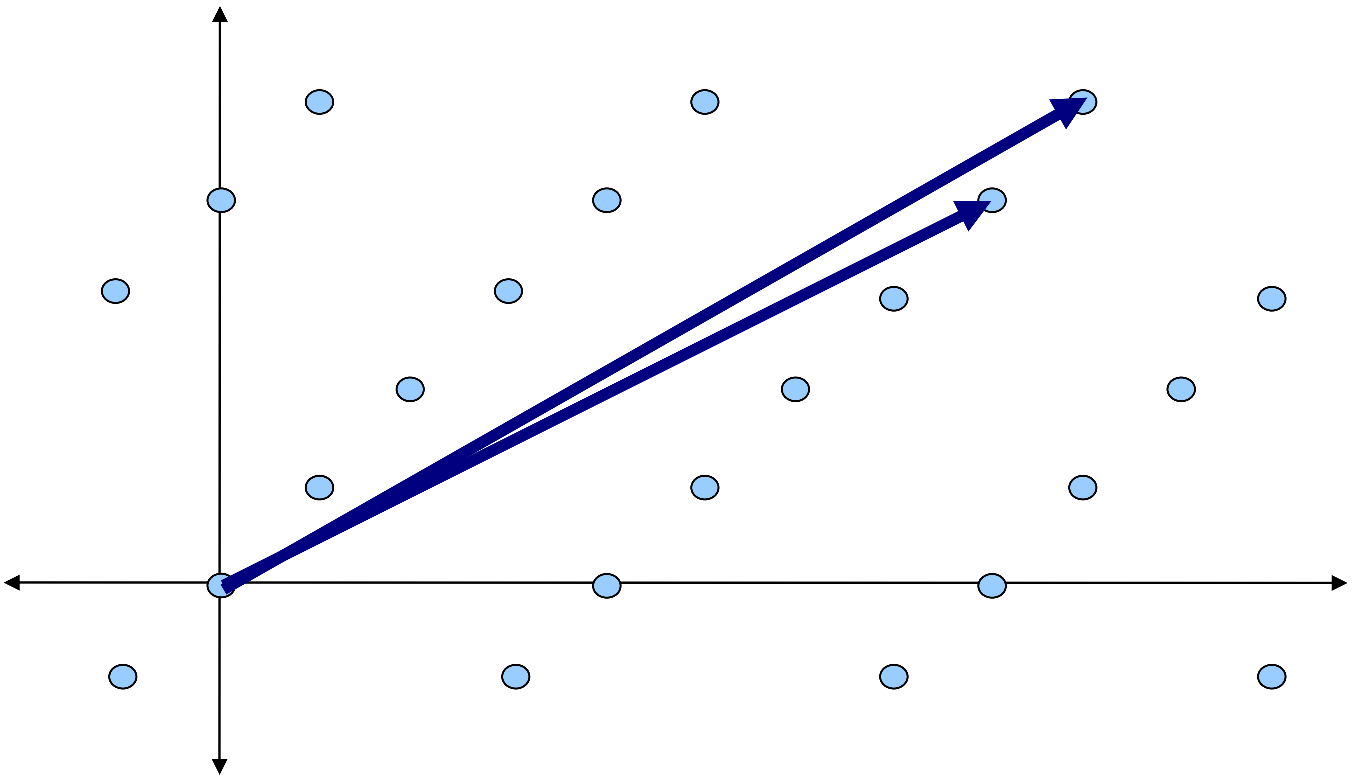
Lattice: A discrete additive subgroup of R^n

Lattices



Basis: A set of linearly independent vectors that generate the lattice.

Lattices

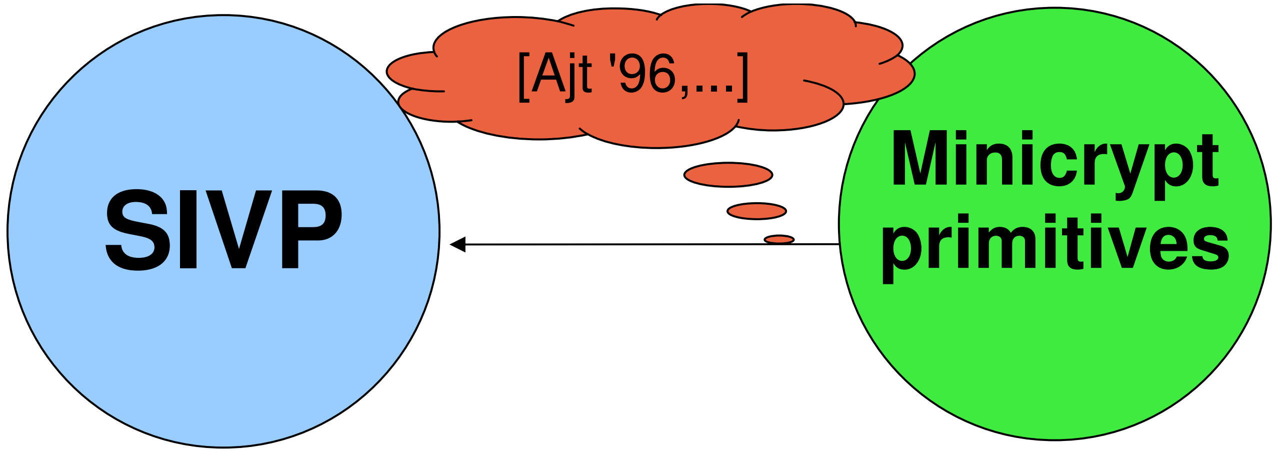


Basis: A set of linearly independent vectors that generate the lattice.

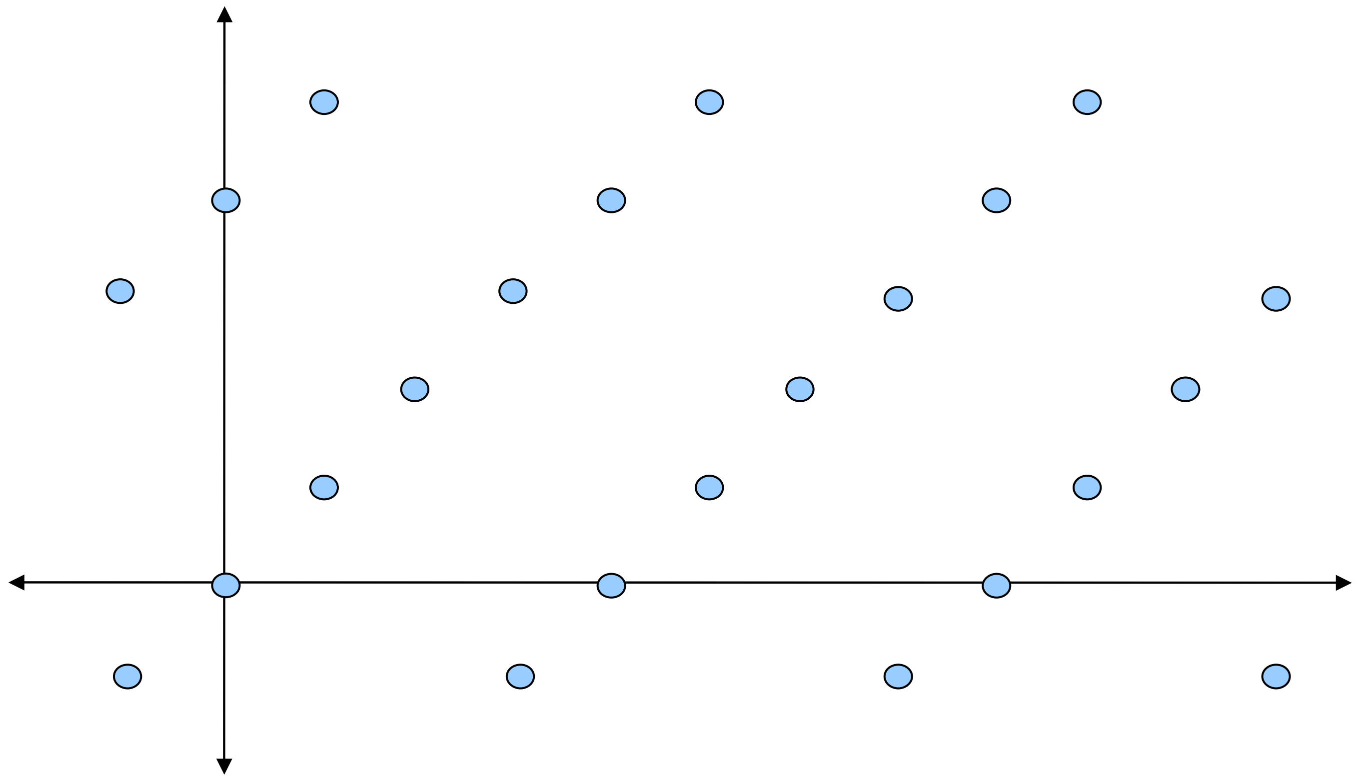
Why are Lattices Interesting?

(In Cryptography)

- Ajtai ('96) showed that solving *“average” instances* of some lattice problem implies solving *all instances* of a lattice problem
- Possible to base cryptography on worst-case instances of lattice problems

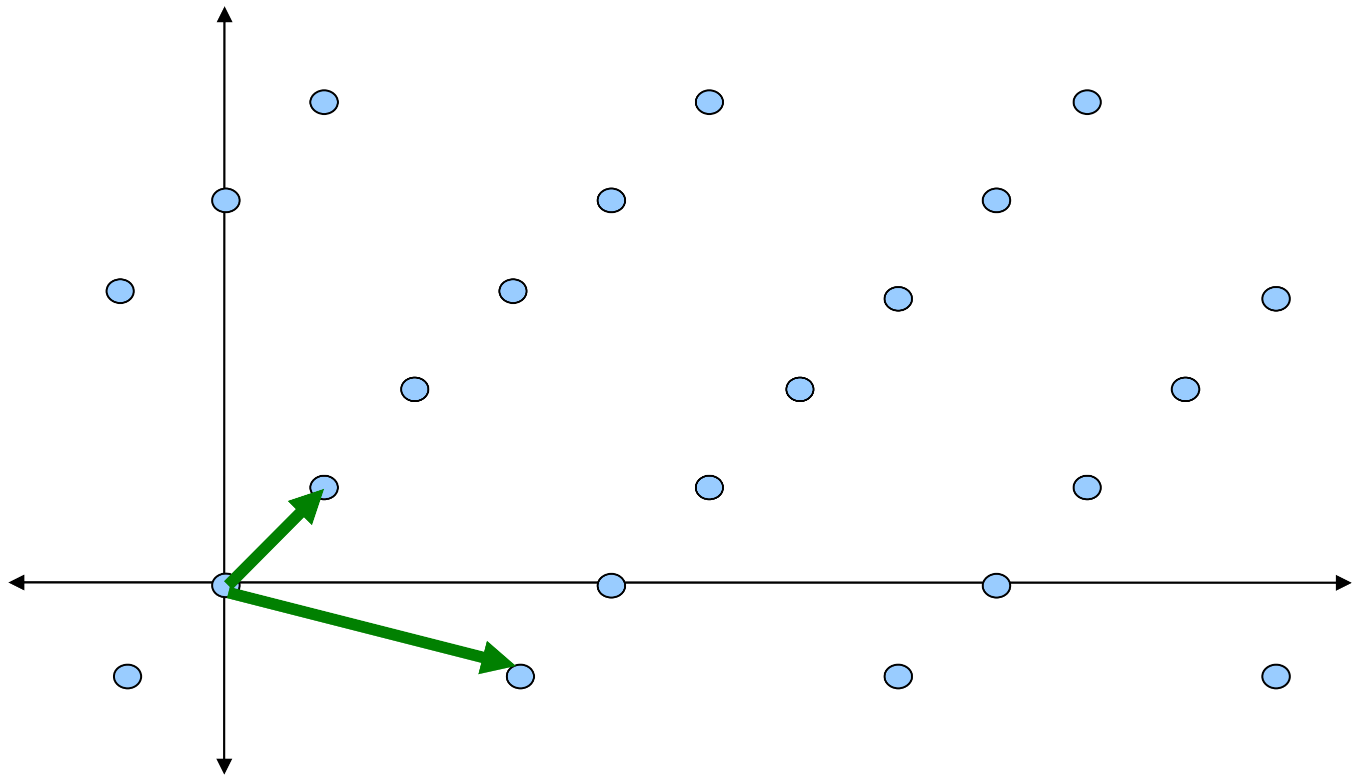

[Ajt '96,...]
SIVP
Minicrypt primitives

Shortest Independent Vector Problem (SIVP)



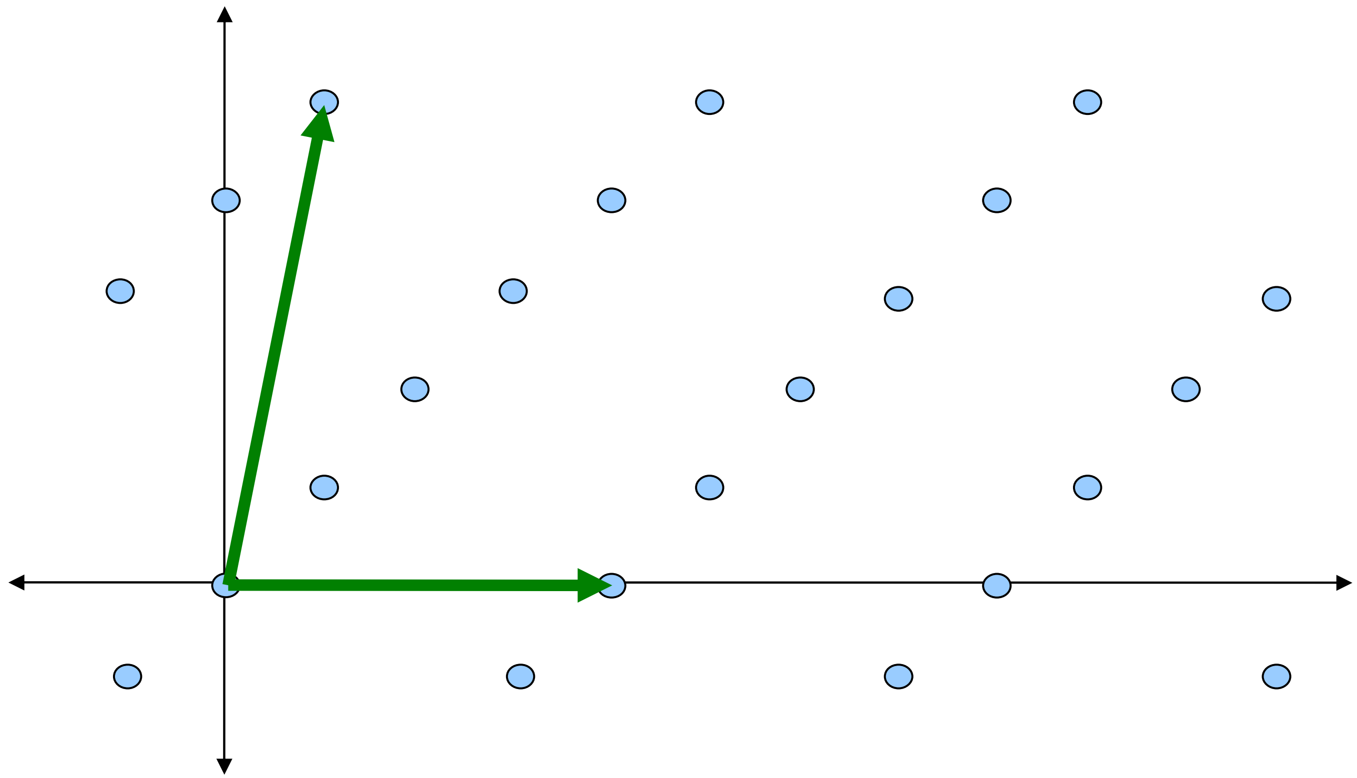
Find n short linearly independent vectors

Shortest Independent Vector Problem (SIVP)

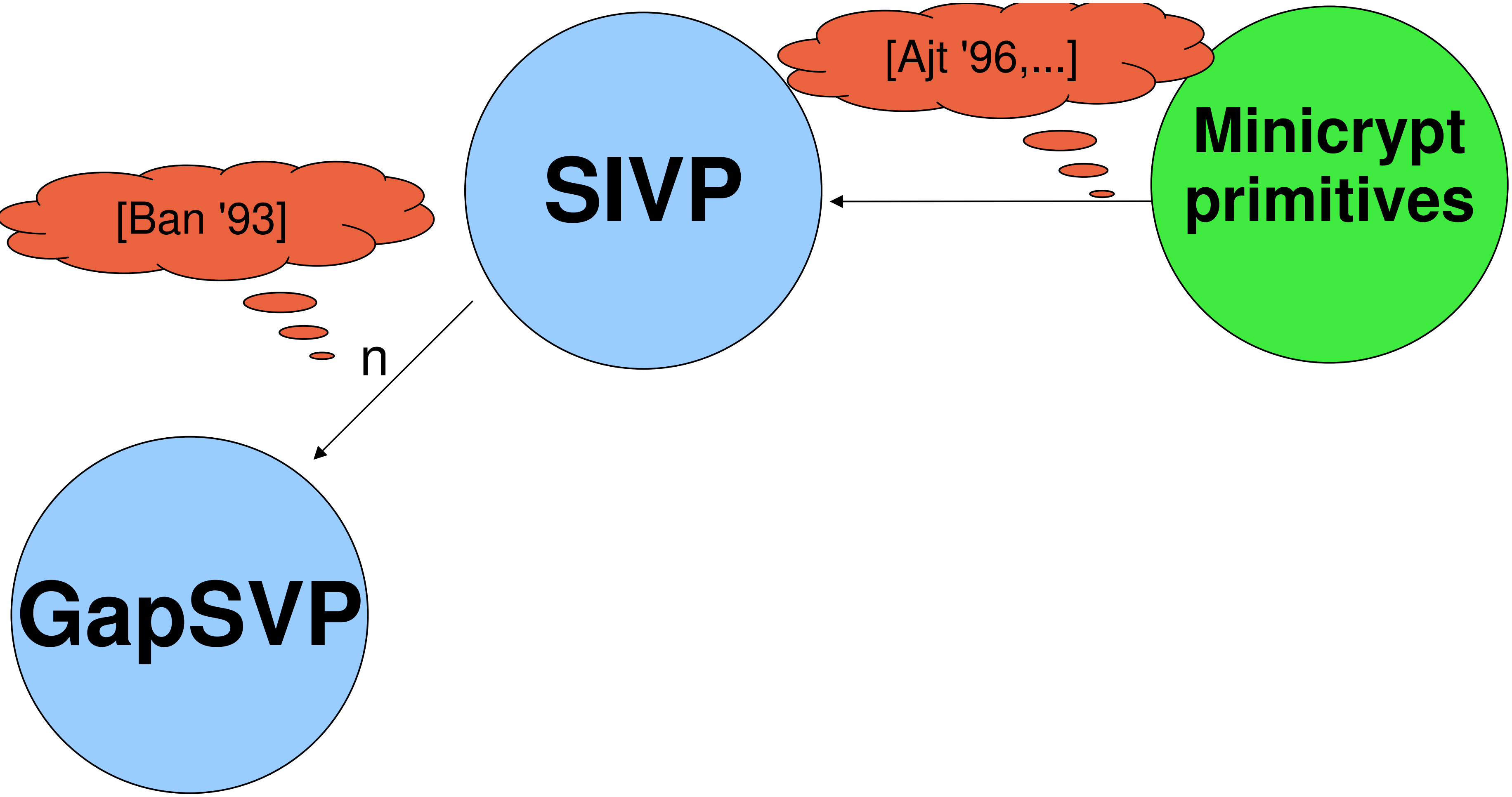


Find n short linearly independent vectors

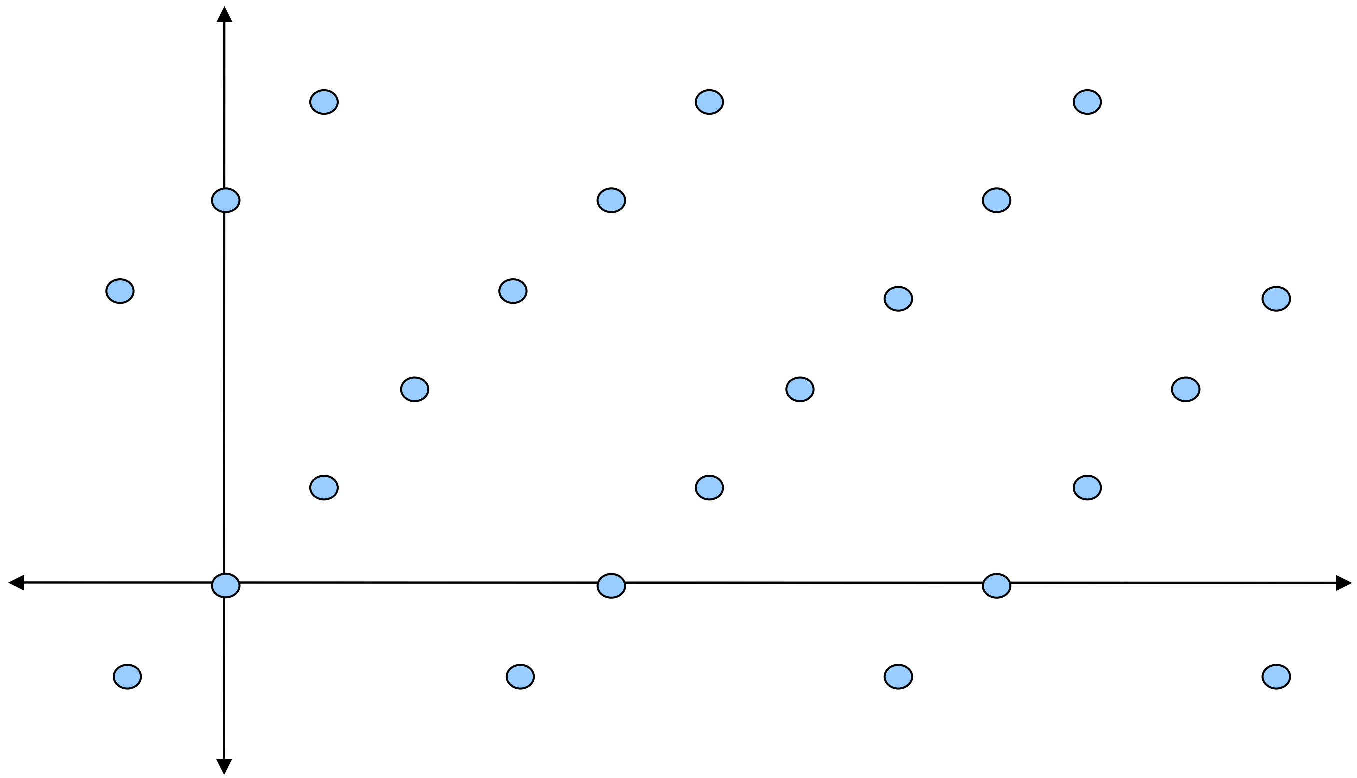
Approximate Shortest Independent Vector Problem



Find n *pretty* short linearly independent vectors

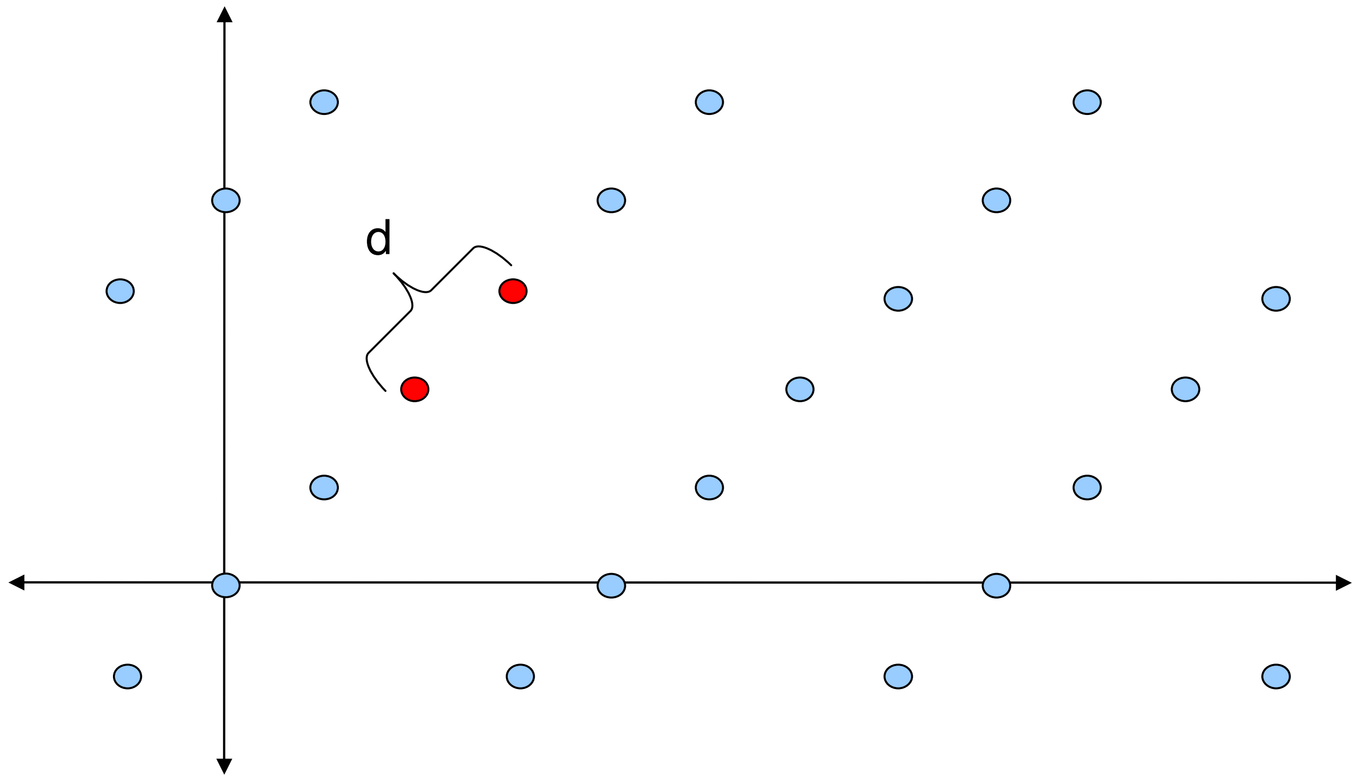

[Ajt '96,...]
Minicrypt primitives
SIVP
[Ban '93]
n
GapSVP

Minimum Distance Problem (GapSVP)

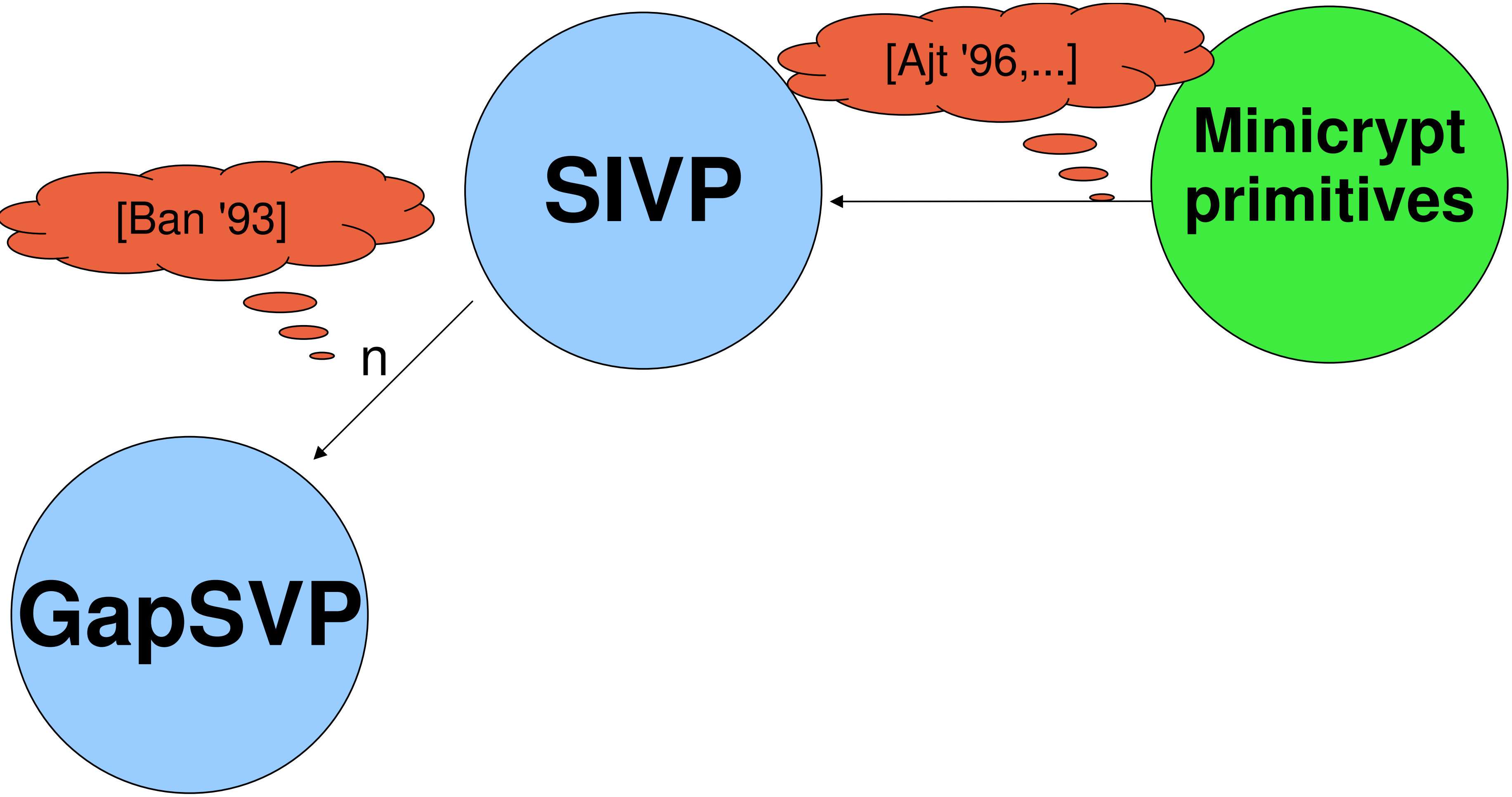


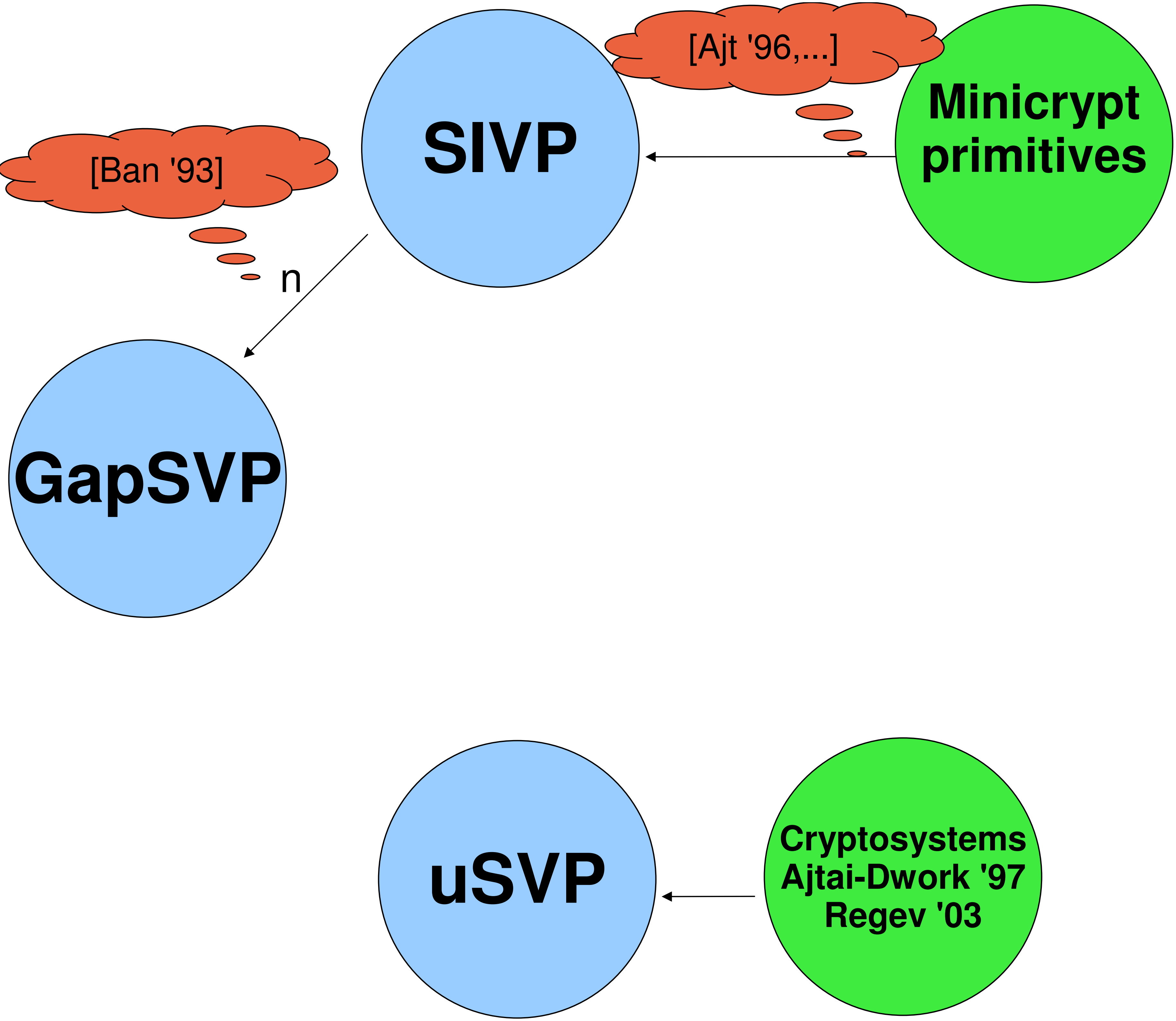
Find the minimum distance between the vectors in the lattice

Minimum Distance Problem (GapSVP)

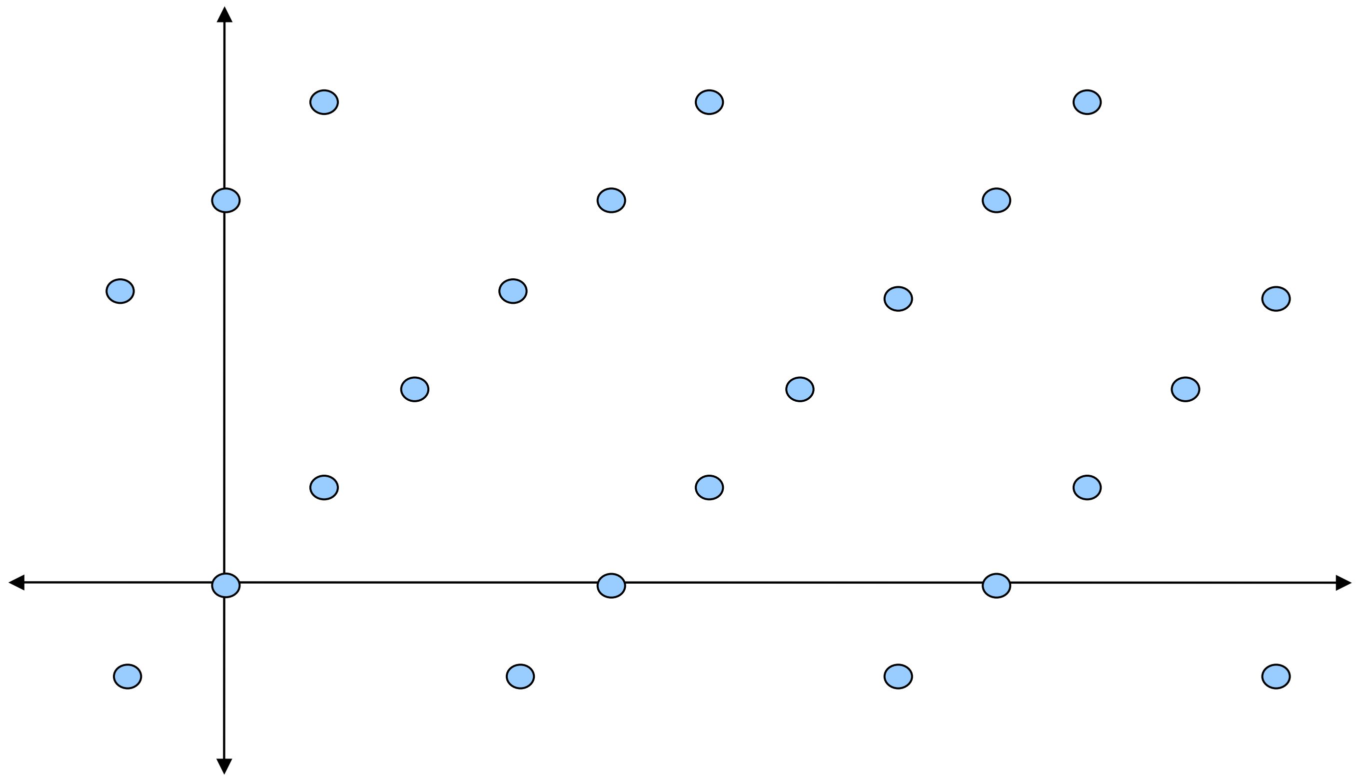


Find the minimum distance between the vectors in the lattice


[Ajt '96,...]
SIVP
Minicrypt primitives
[Ban '93]
n
GapSVP

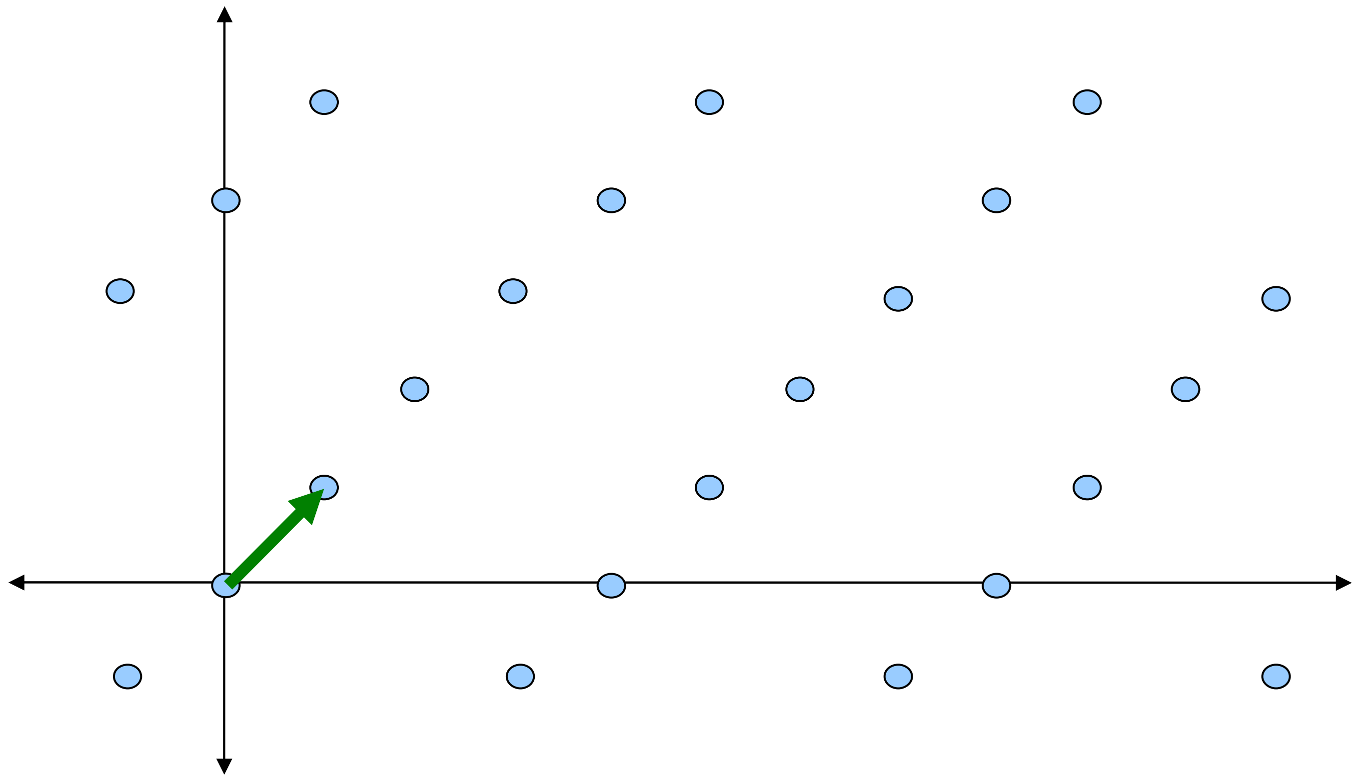

[Ajt '96,...]
SIVP
Minicrypt primitives
[Ban '93]
n
GapSVP
uSVP
Cryptosystems
Ajtai-Dwork '97
Regev '03

Unique Shortest Vector Problem (uSVP)

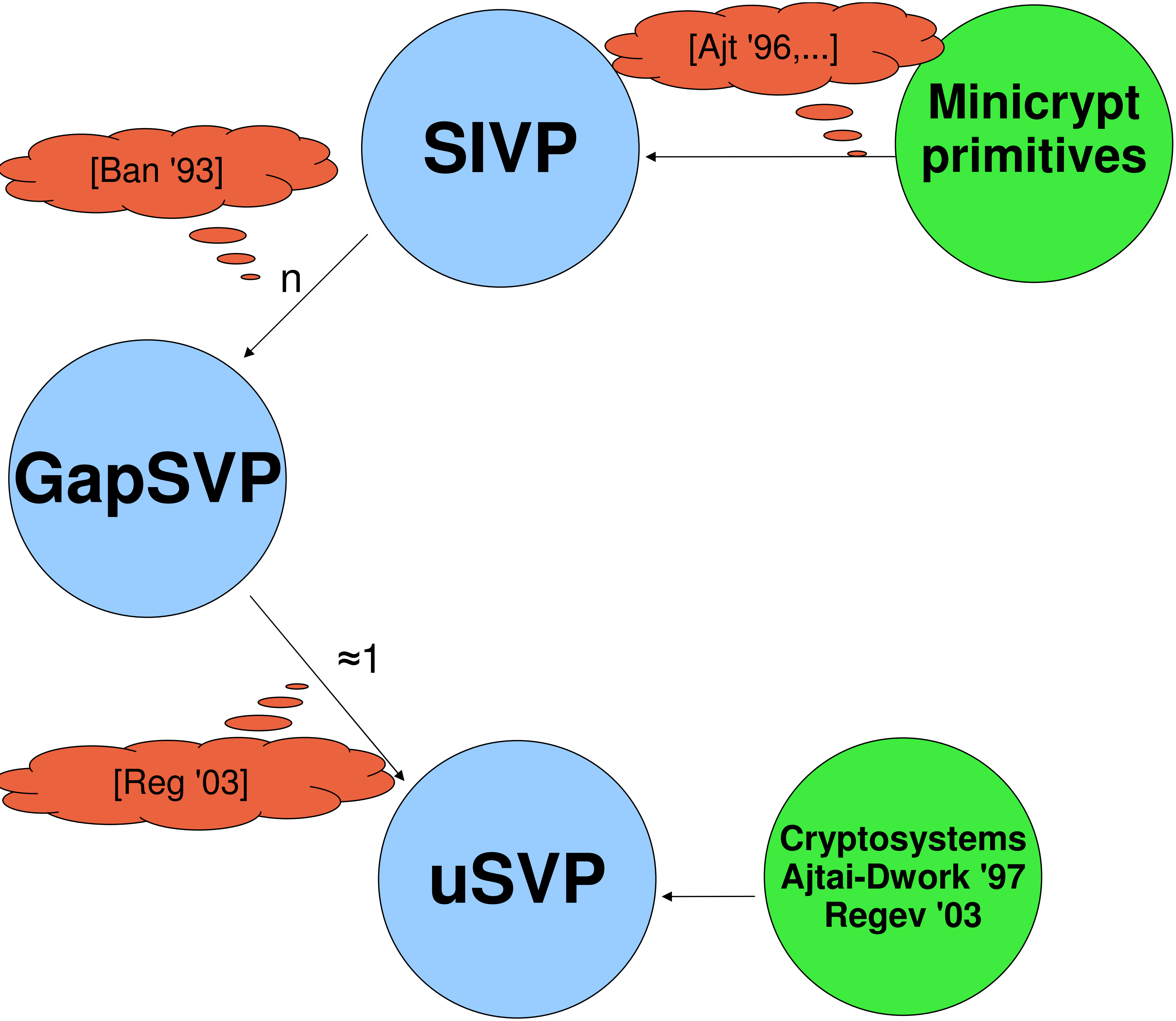


Find the shortest vector in a lattice in which the shortest vector is much smaller than the next non-parallel vector

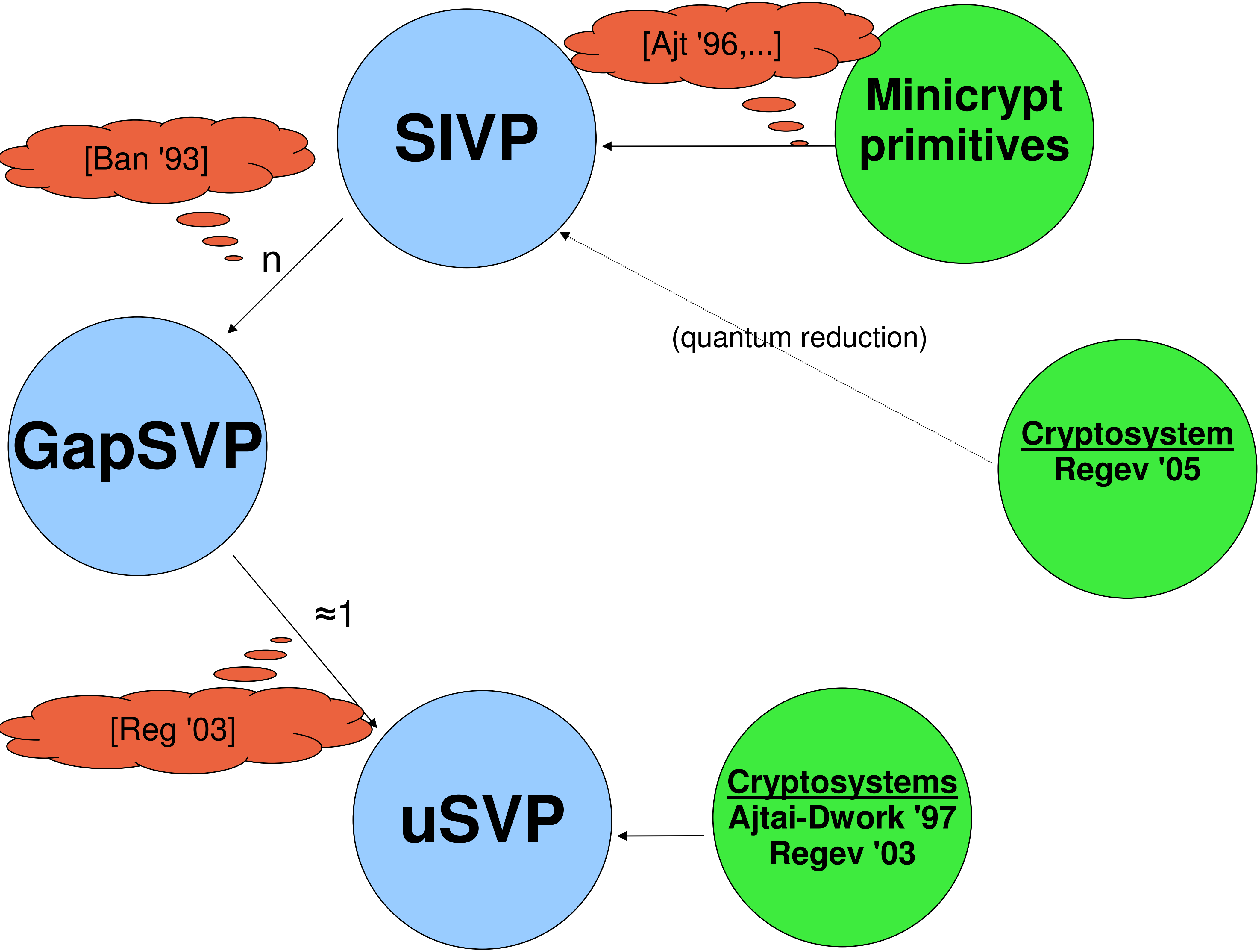
Unique Shortest Vector Problem (uSVP)

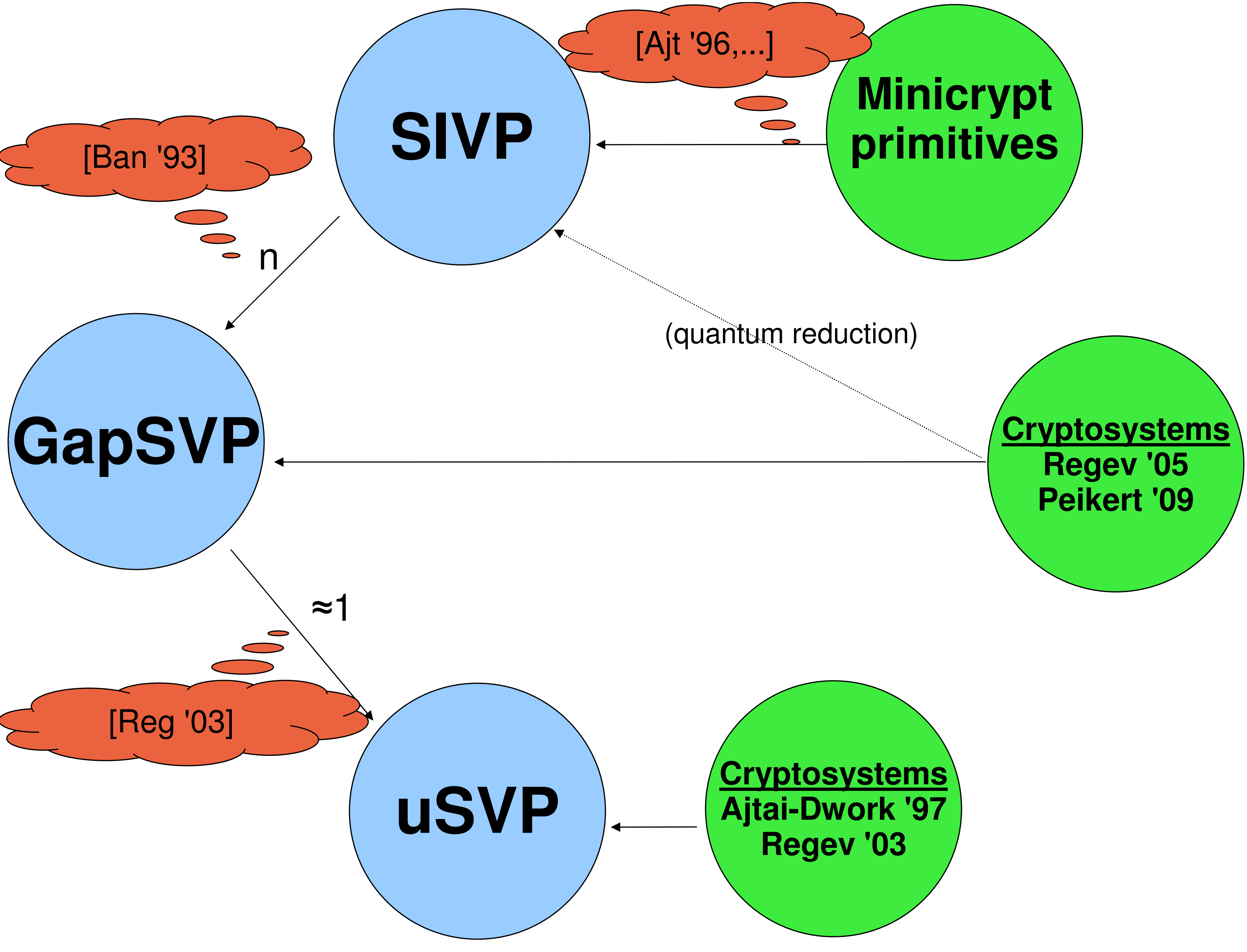


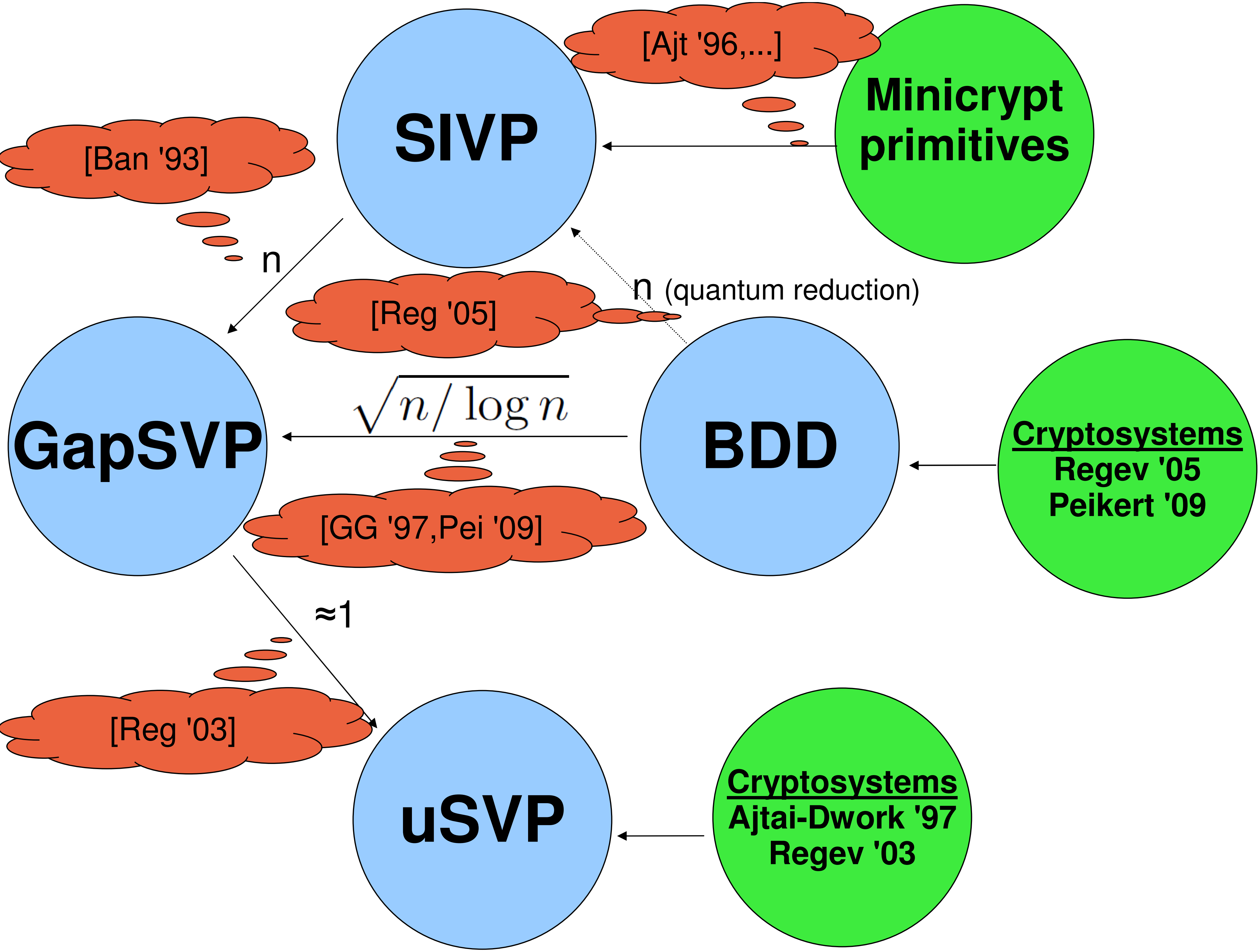
Find the shortest vector in a lattice in which the shortest vector is much smaller than the next non-parallel vector



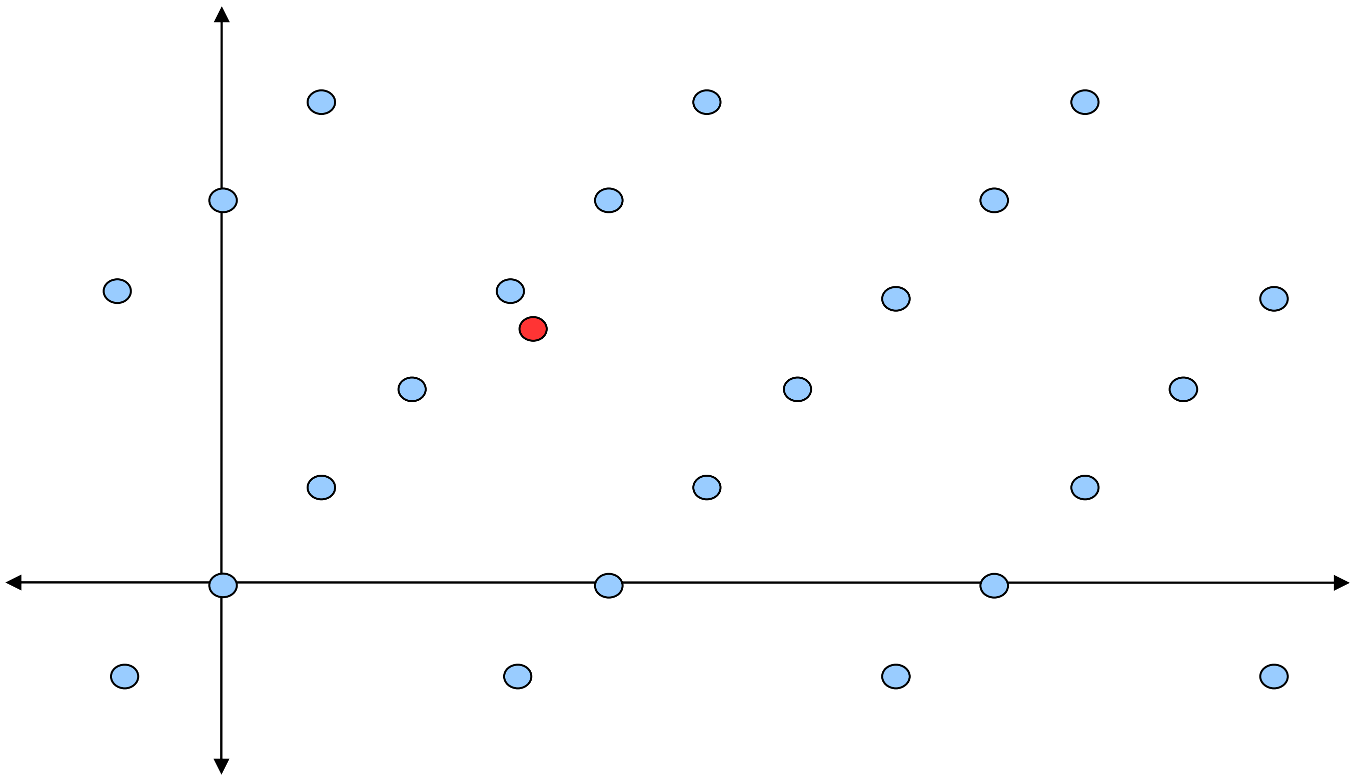
[Ajt '96,...]
SIVP
Minicrypt primitives
[Ban '93]
n
GapSVP
≈1
[Reg '03]
uSVP
Cryptosystems
Ajtai-Dwork '97
Regev '03


[Ajt '96,...]
SIVP
Minicrypt primitives
[Ban '93]
n
GapSVP
(quantum reduction)
Cryptosystem
Regev '05
≈1
[Reg '03]
uSVP
Cryptosystems
Ajtai-Dwork '97
Regev '03

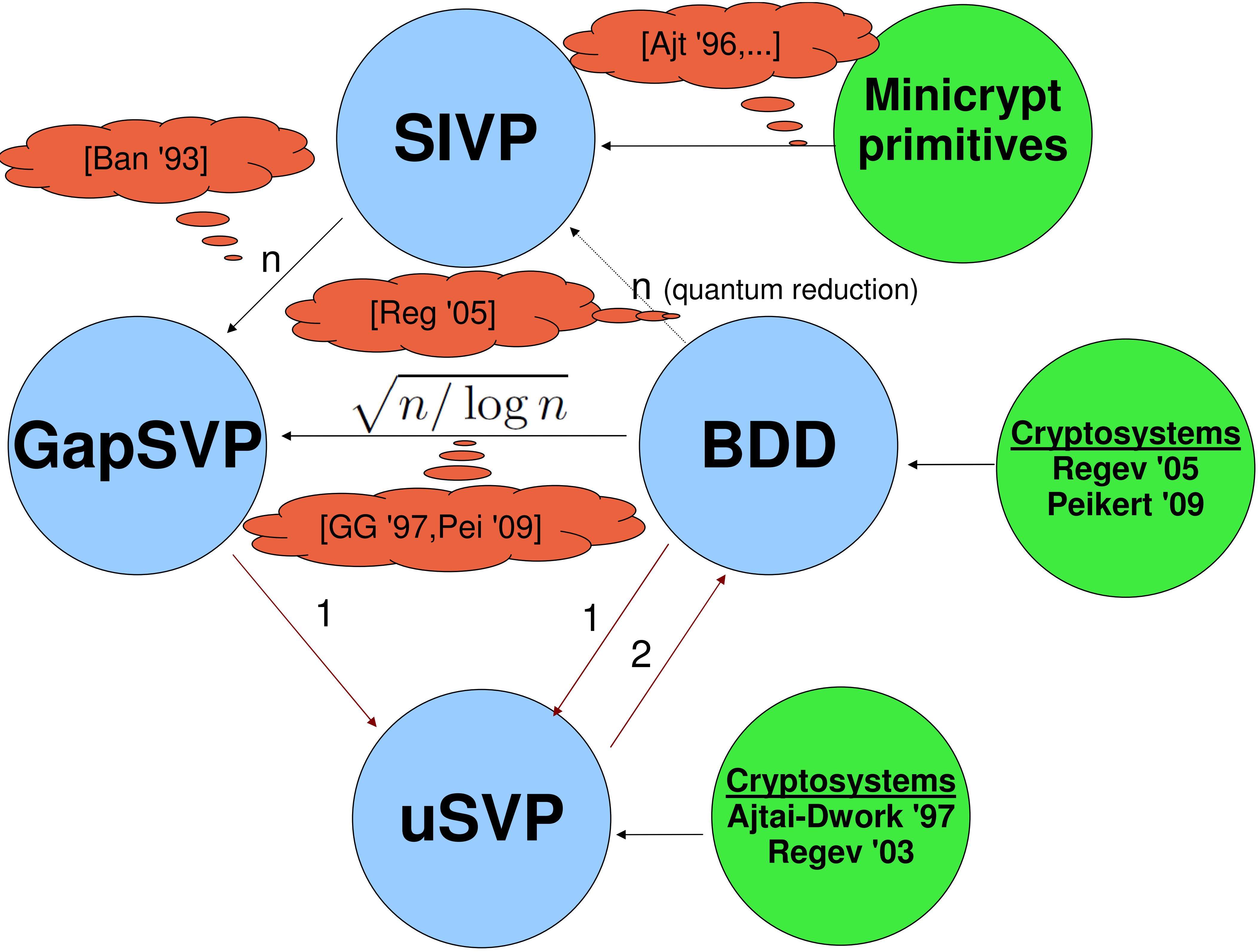

SIVP
[Ajt '96,...]
Minicrypt primitives
[Ban '93]
n
GapSVP
(quantum reduction)
Cryptosystems
Regev '05
Peikert '09
≈1
[Reg '03]
uSVP
Cryptosystems
Ajtai-Dwork '97
Regev '03


SIVP
Minicrypt primitives
[Ajt '96,...]
[Ban '93]
n
[Reg '05]
n (quantum reduction)
GapSVP
BDD
$\sqrt{n/\log n}$
Cryptosystems
Regev '05
Peikert '09
[GG '97,Pei '09]
≈1
[Reg '03]
uSVP
Cryptosystems
Ajtai-Dwork '97
Regev '03

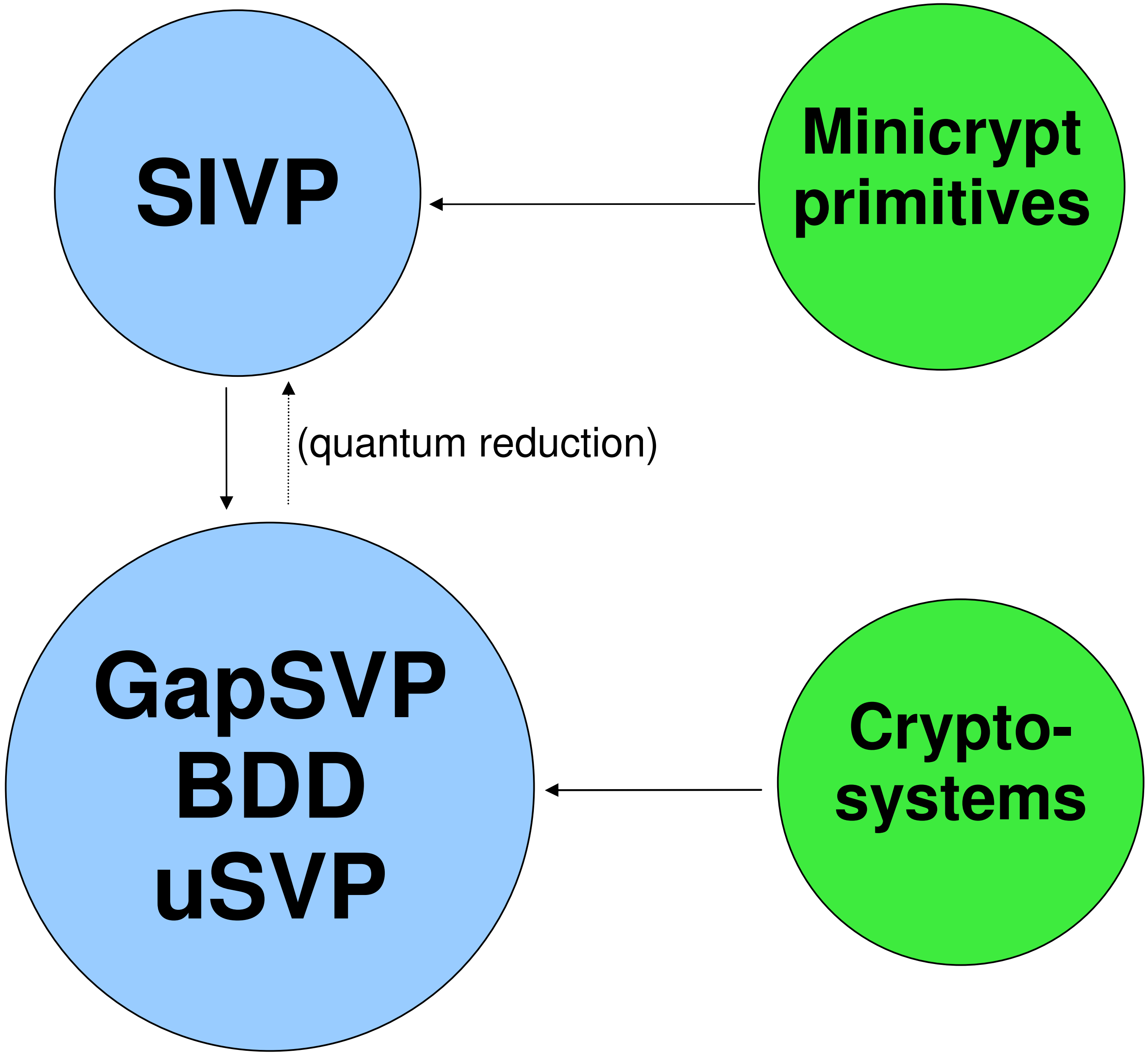
Bounded Distance Decoding (BDD)



Given a target vector *that's close to the lattice,* find the nearest lattice vector



[Ajt '96,...]
SIVP
Minicrypt primitives
[Ban '93]
n
[Reg '05]
n (quantum reduction)
GapSVP
$\sqrt{n/\log n}$
BDD
Cryptosystems
Regev '05
Peikert '09
[GG '97,Pei '09]
1
1
2
uSVP
Cryptosystems
Ajtai-Dwork '97
Regev '03


SIVP
Minicrypt primitives
(quantum reduction)
GapSVP
BDD
uSVP
Crypto-systems

Cryptosystem Hardness Assumptions

	uSVP	BDD	GapSVP	SIVP (quantum)
Ajtai-Dwork '97	$O(n^2)$	$O(n^2)$	$O(n^{2.5})$	$O(n^3)$
Regev '03	$O(n^{1.5})$	$O(n^{1.5})$	$O(n^2)$	$O(n^{2.5})$
Regev '05	-	-	-	$O(n^{1.5})$
Peikert '09	$O(n^{1.5})$	$O(n^{1.5})$	$O(n^2)$	$O(n^{2.5})$

Implications of our results

Lattice-Based Primitives

Minicrypt

- One-way functions [Ajt '96]
- Collision-resistant hash functions [Ajt '96,MR '07]
- Identification schemes [MV '03,Lyu '08, KTX '08]
- Signature schemes [LM '08, GPV '08]

All Based on GapSVP and SIVP

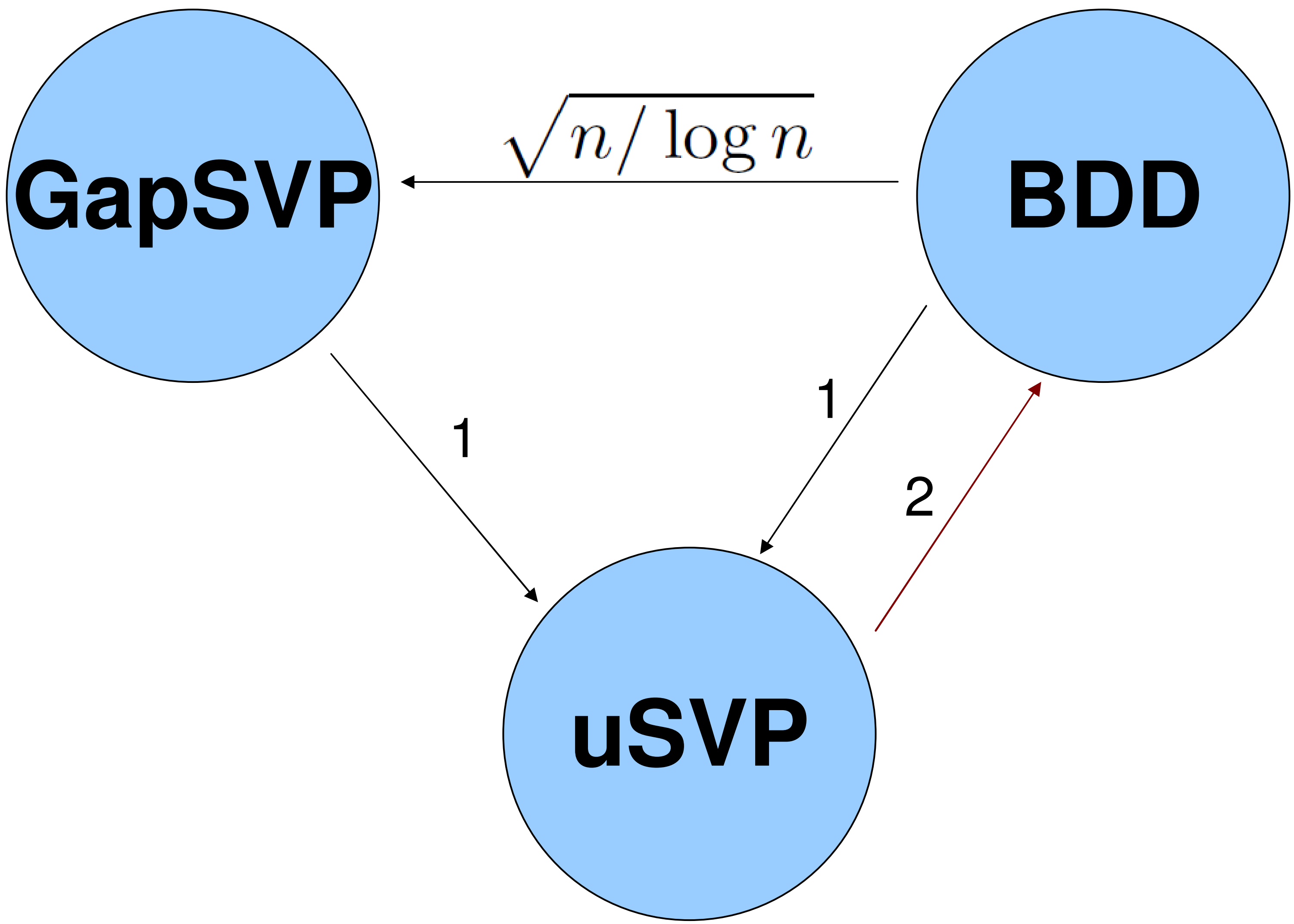
Public-Key Cryptosystems

- [AD '97] (uSVP)
- [Reg '03] (uSVP)
- [Reg '05] (SIVP and GapSVP under quantum reductions)
- [Pei '09] (GapSVP)

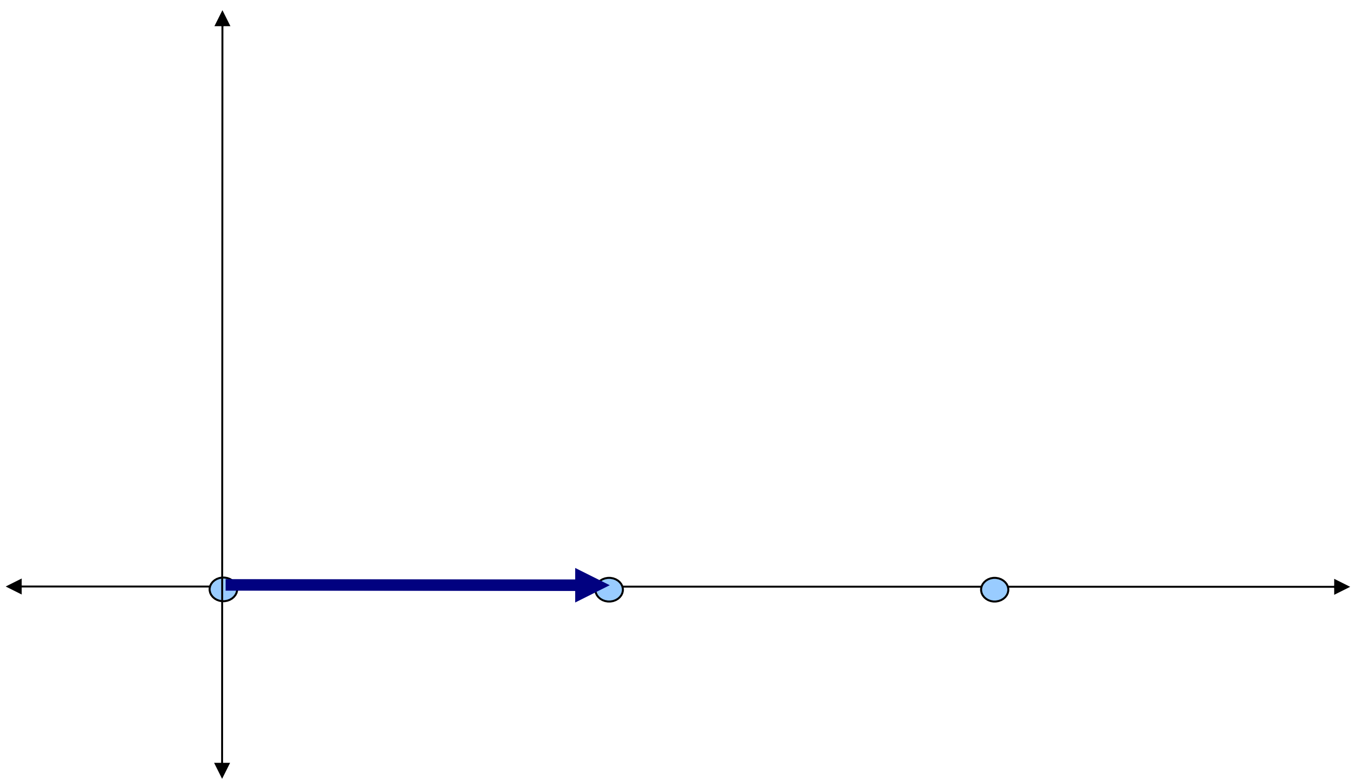
All Based on GapSVP and quantum SIVP

Major Open Problem:
Construct cryptosystems based on SIVP

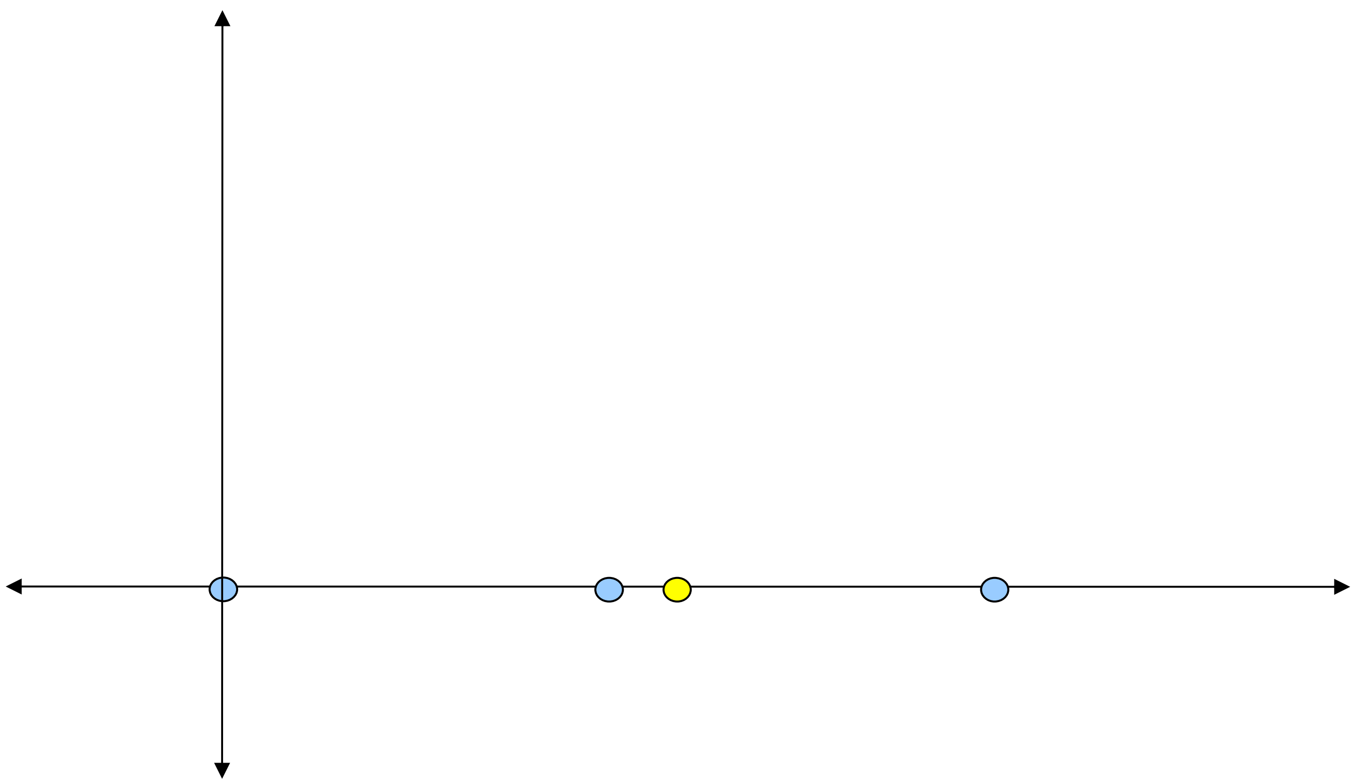
Reductions



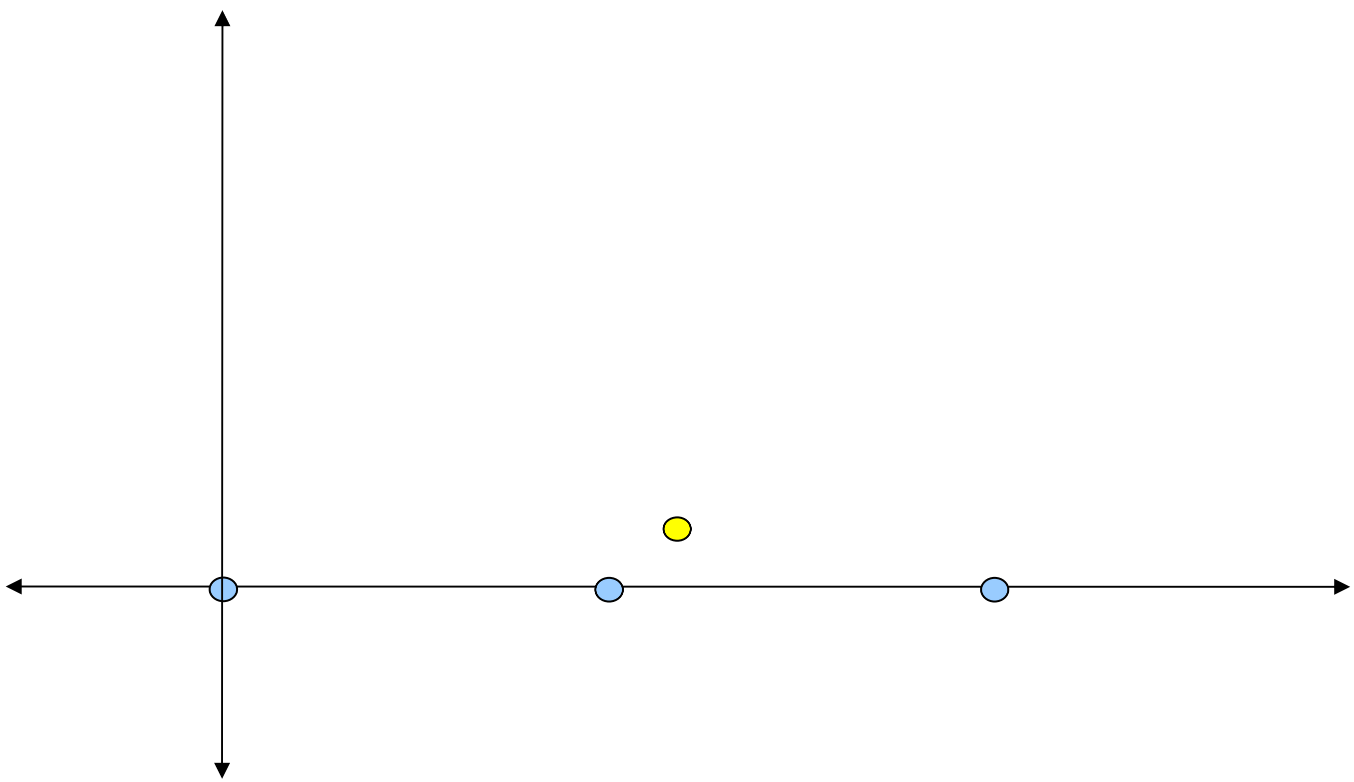
Proof Sketch (BDD < uSVP)



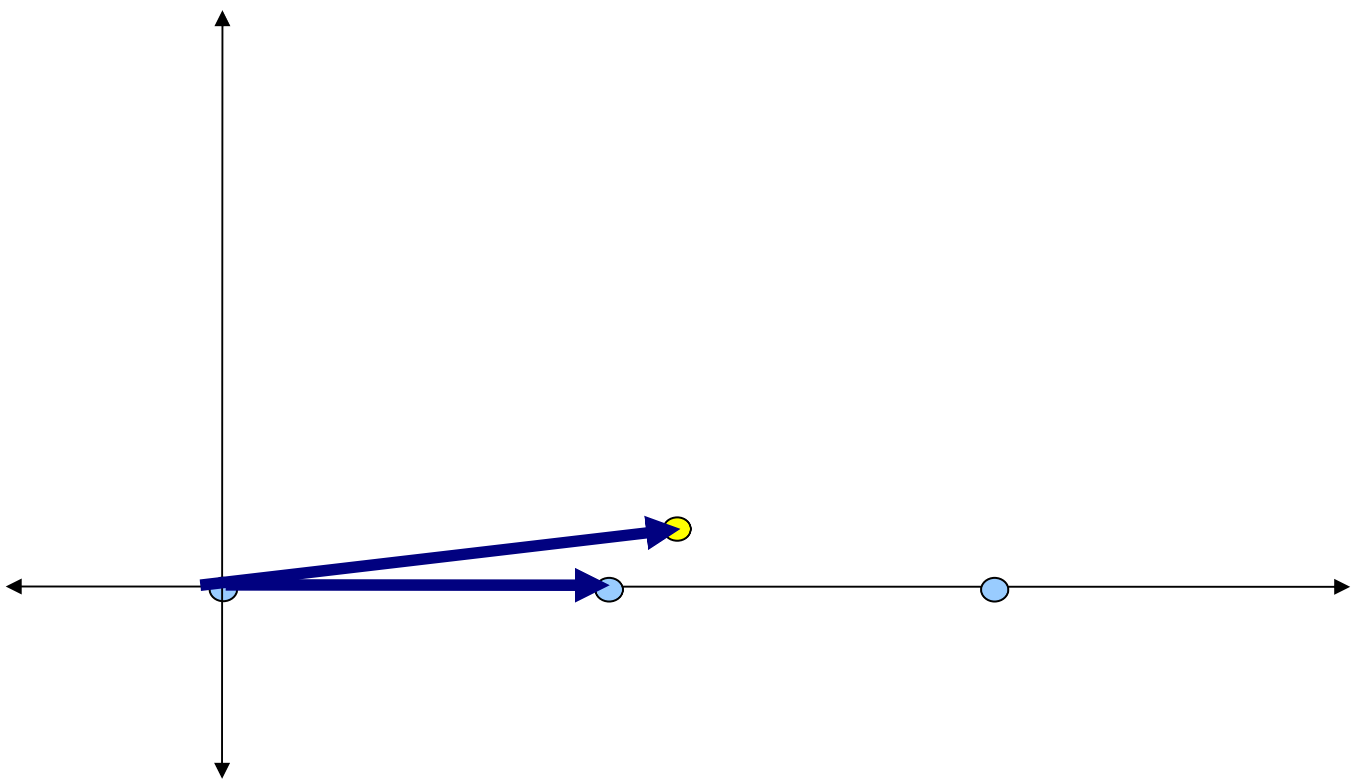
Proof Sketch (BDD < uSVP)



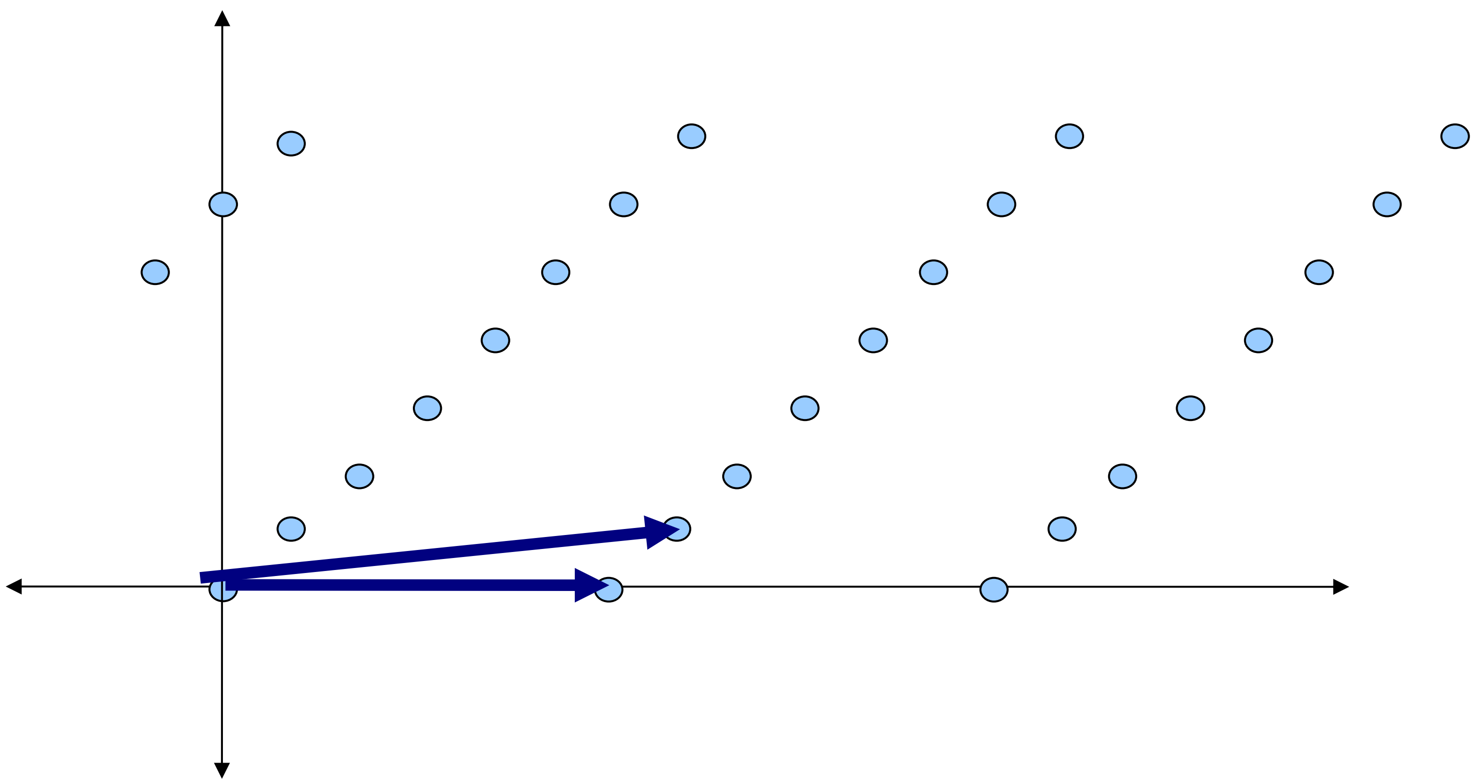
Proof Sketch (BDD < uSVP)



Proof Sketch (BDD < uSVP)

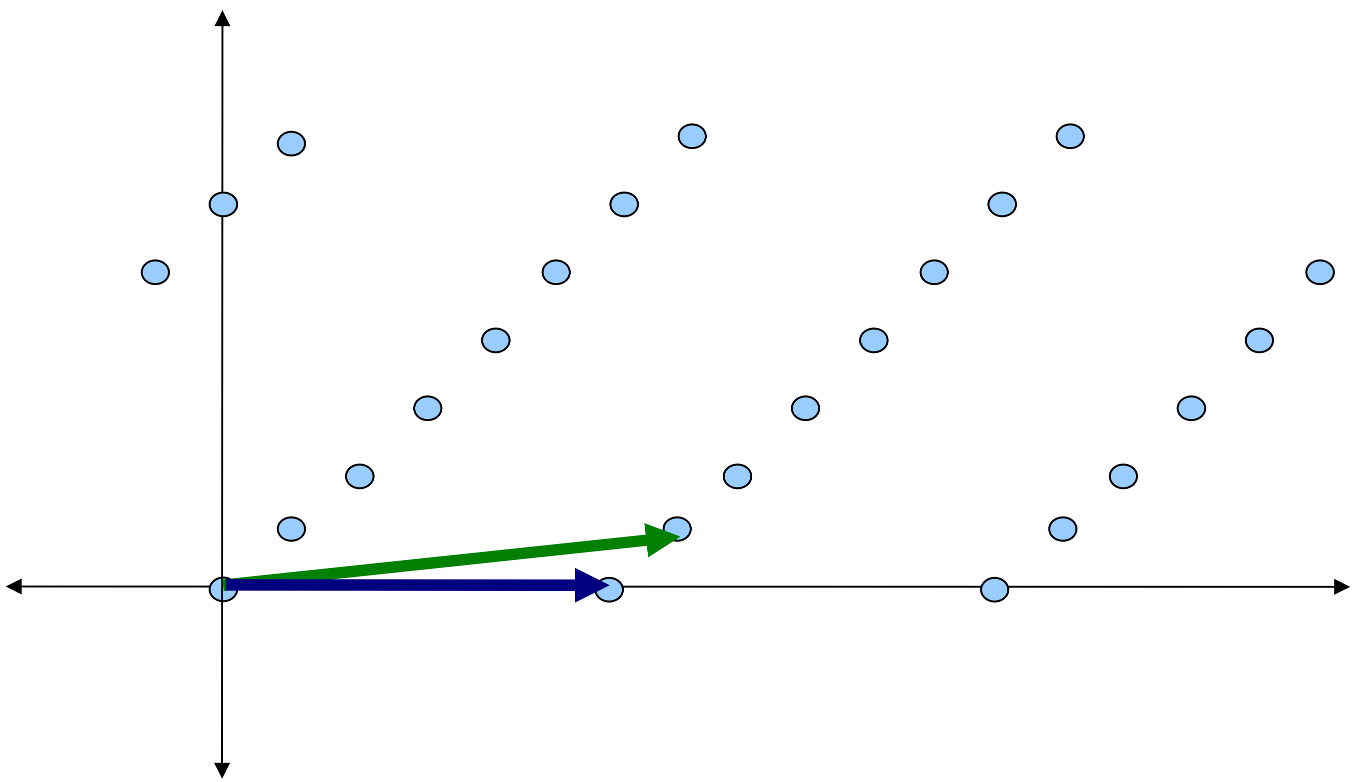


Proof Sketch (BDD < uSVP)



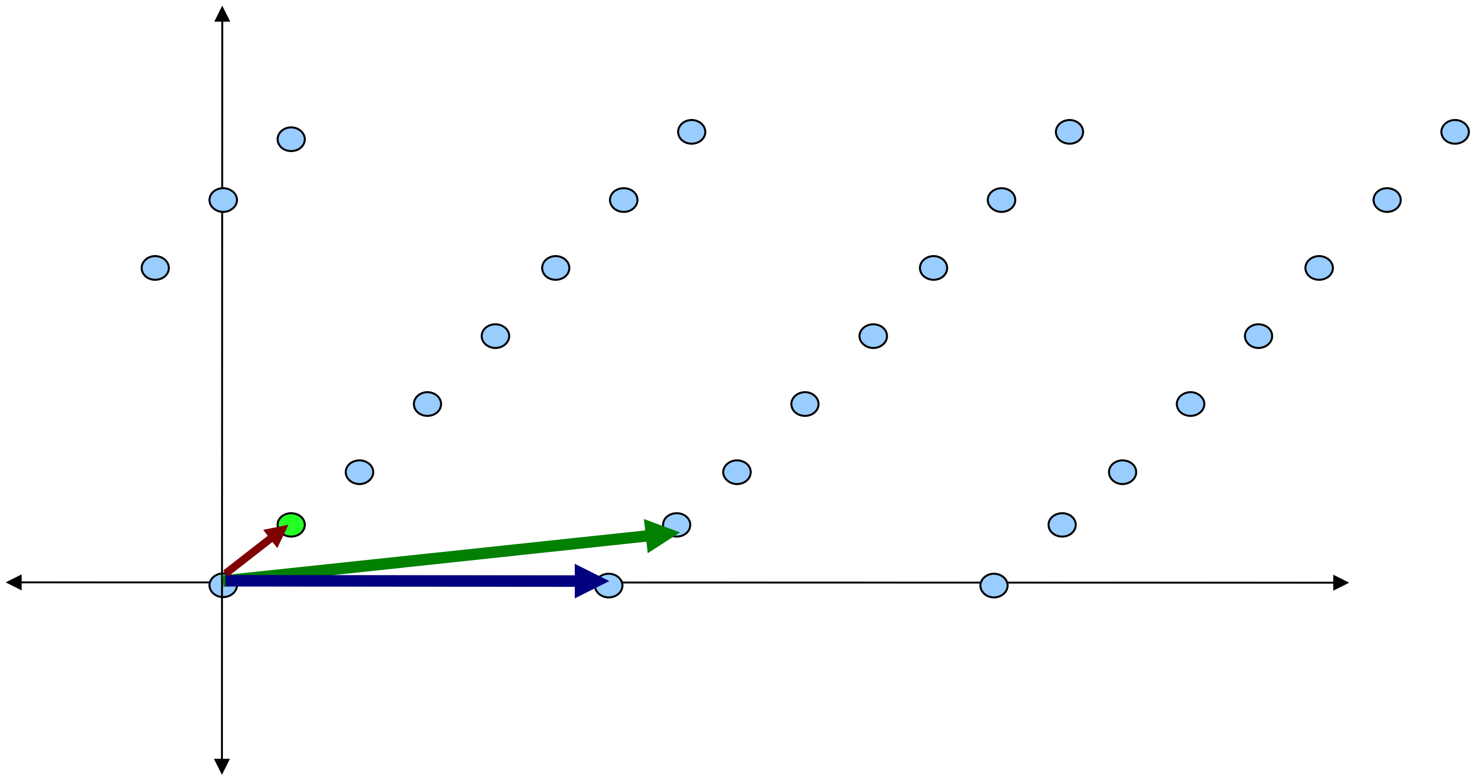
Proof Sketch (BDD < uSVP)

New basis vector used exactly once in constructing the unique shortest vector



Proof Sketch (BDD < uSVP)

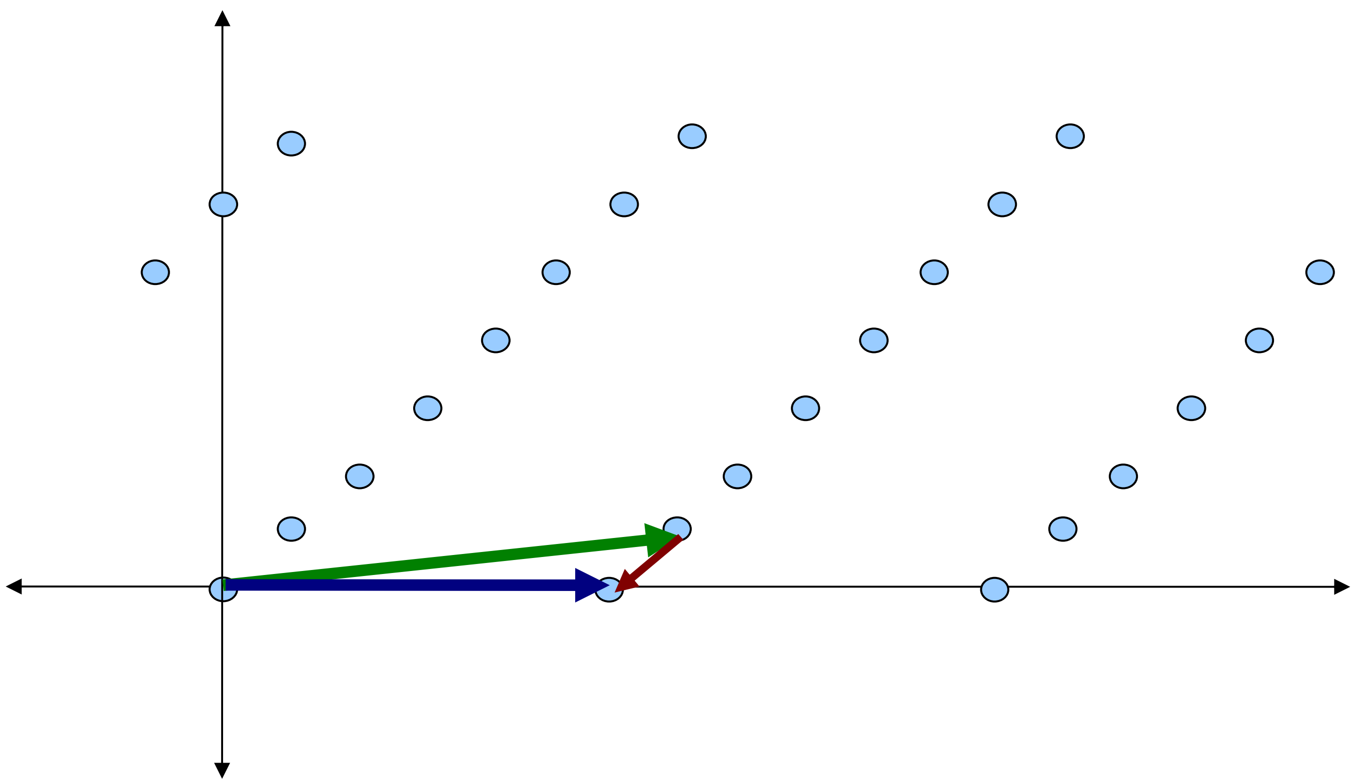
New basis vector used exactly once in constructing the unique shortest vector



Proof Sketch (BDD < uSVP)

New basis vector used exactly once in constructing the unique shortest vector

Subtracting unique shortest vector from new basis vector gives the closest point to the target.



Open Problems

- Can we construct cryptosystems based on SIVP
  - (SVP would be even better!)
- Can the reduction GapSVP $<$ BDD be tightened?
- Can the reduction BDD $<$ uSVP be tightened?

Thanks!