

Post-quantum key exchange from (ideal) lattices

Craig Costello

Microsoft®
Research

Part 1: Recap and motivation

Part 2: Lattice basics

Part 3: PQ key exchange based on (R)LWE

Diffie-Hellman key exchange (circa 2016)

$$q =$$

5809605995369958062859502533304574370686975176362895236661486152287203730997110225737336044533118407251326157754980517443990529594540047121662885672187032401032111639706440498844049850989051627200244765807041812394729680540024104827976584369381522292361208779044769892743225751738076979568811309579125511333093243519553784816306381580161860200247492568448150242515304449577187604136428738580990172551573934146255830366405915000869643732053218566832545291107903722831634138599586406690325959725187447169059540805012310209639011750748760017095360734234945757416272994856013308616958529958304677637019181594088528345061285863898271763457294883546638879554311615446446330199254382340016292057090751175533888161918987295591531536698701292267685465517437915790823154844634780260102891718032495396075041899485513811126977307478969074857043710716150121315922024556759241239013152919710956468406379442914941614357107914462567329693649

$$g = 123456789$$

g^a
 $(\text{mod } q)$
 $=$

19749664818322719328626201861425055597190979976253376065400814799487577544566705421857810513313821749720689059955492842945066789947685466859559403409349363756245107893829696031348869617884814249135168725305460220296624704610577077157724832168211717424612832119567853763152027864940346479735369199673699357709268717838560229887355895412105643052289961976145372708221782347574622380379001423505139679904944650822466185016814995740147463845671662440190670139447244701505256941774637218509330253573938379198007057238142172902965163930423436126876497170776348430066892397286870912166556869830978657804740157916611563508569886847487772676671207386096152947607114559706340209059103703018182635521898738094546294558035569752596676346614699327742088471255741184755866117812209895514952436160199336532605242210147489825669666012419572610049572551002200293281421876806011231076345540456724876139639963344901857872119208518550803791724

4116046620695933066832285256534418724107779992205720799935743972371563687620383783327424719396665449687938178193214952698336131699379861648113207956169499574005182063853102924755292845506262471329301240277031401312209687711427883948465928161110782751969552580451787052540164697735099369253619948958941630655511051619296131392197821987575429848264658934577688889155615145050480918561594129775760490735632255728098809700583965017196658531101013084326474277865655251213287725871678420376241901439097879386658420056919119973967264551107584485525537442884643379065403121253975718031032782719790076818413945341143157261205957499938963479817893107541948645774359056731729700335965844452066712238743995765602919548561681262366573815194145929420370183512324404671912281455859090458612780918001663308764073238447199488070126873048860279221761629281961046255219584327714817248626243962413613075956770018017385724999495117779149416882188

$=$
 g^b
 $(\text{mod } q)$

$$a =$$



7147687166405; 9571879053605547396582692405186145916522354912615715297097100679170037904924330116019497881089087696131592831386326210951294944584400497488929803858493191812844757232102398716043906200617764831887545755623377085391250529236463183321912173214641346558452549172283787727566955898452199622029450892269665074265269127802446416400\97464722529088780604931419862375878988193612187945591802864062679\86483957813927304368495559776413009721221824915810964579376354556\65546298837778595680891578821511273574220422646379170599917677567\30420698422392494816906777896174927072071297603455802621072109220\5466273969774855343758990879608882627763290293452560094576029847\39136138876755438662247926529997805988647241453046219452761811989\97464722529088780604931795419514638292288904557780459294373052654\10485180264002079415193983851143425084273119820368274789460587100\30497747706924427898968991057212096357725203480402449913844583448

$$g^{ab} =$$

330166919524192149323761733598426244691224199958894654036331526394350099088627302979833339501183059198113987880066739419999231378970715307039317876258453876701124543849520979430233302775032650107245135512092795731832349343596366965069683257694895110289436988215186894965977582185407675178858364641602894716513645524907139614566085360133016497539758756106596557555674744381803579583602267087423481750455634370758409692308267670340611194376574669939893893482895996003389503722513369326735717434288230260146992320711161713922195996910968467141336433827457093761125005143009836512019611866134642676859265636245898172596372485581049036573719816844170539930826718273452528414333373254200883800592320891749460865366649848360413340316504386926391062876271575757583831289710534010374070317315095828076395094487046179839301350287596589383292751993079161318839043121329118930009948197899907586986108953591420279426874779423560221038468

$$b =$$



655456209464694; 93360682685816031704969423104727624468251177438749706128879957701\93698826859762790479113062308975863428283798589097017957365590672\835713863895712246676094993008985548024464030395443007480025079620363866193152298860635410053224484639158978641210273772558373965\48653931285483865070903191974204864923589439190352993032676961005\08840431979272991603892747747094094858192679116146502863521484987\08623286193422239171712154568612530067276018808591500424849476686\706784051068715397706852664532638332403983747338379697022624261377163163204493828299206039808703403575100467337085017748387148822224875309641791879395483731754620034884930540399950519191679471224\055585570932193507471557775698163700850920394705281936392411084\43600686183528465724969562186437214972625833222544865996160464558\5462993701658947042526445624157899586972652935647856967092689604\42796501209877036845001246792761563917639959736383038665362727158

ECDH key exchange (1999 – nowish)

$$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$$

$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$

$$E/\mathbb{F}_p: y^2 = x^3 - 3x + b$$

$\#E = 115792089210356248762697446949407573529996955224135760342422259061068512044369$

$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286, \\ 36134250956749795798585127919587881956611106672985015071877198253568414405109)$

$[a]P = (84116208261315898167593067868200525612344221886333785331584793435449501658416, \\ 102885655542185598026739250172885300109680266058548048621945393128043427650740)$

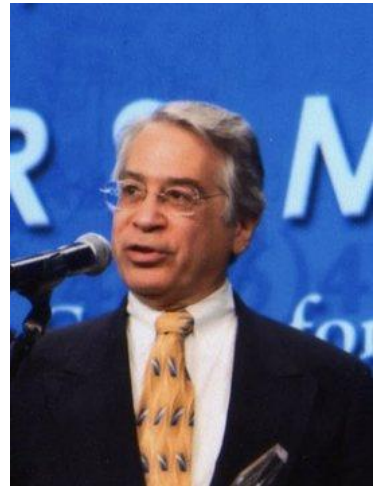
$[b]P = (101228882920057626679704131545407930245895491542090988999577542687271695288383, \\ 77887418190304022994116595034556257760807185615679689372138134363978498341594)$



$a =$

89130644591246033577639
77064146285502314502849
28352556031837219223173
24614395

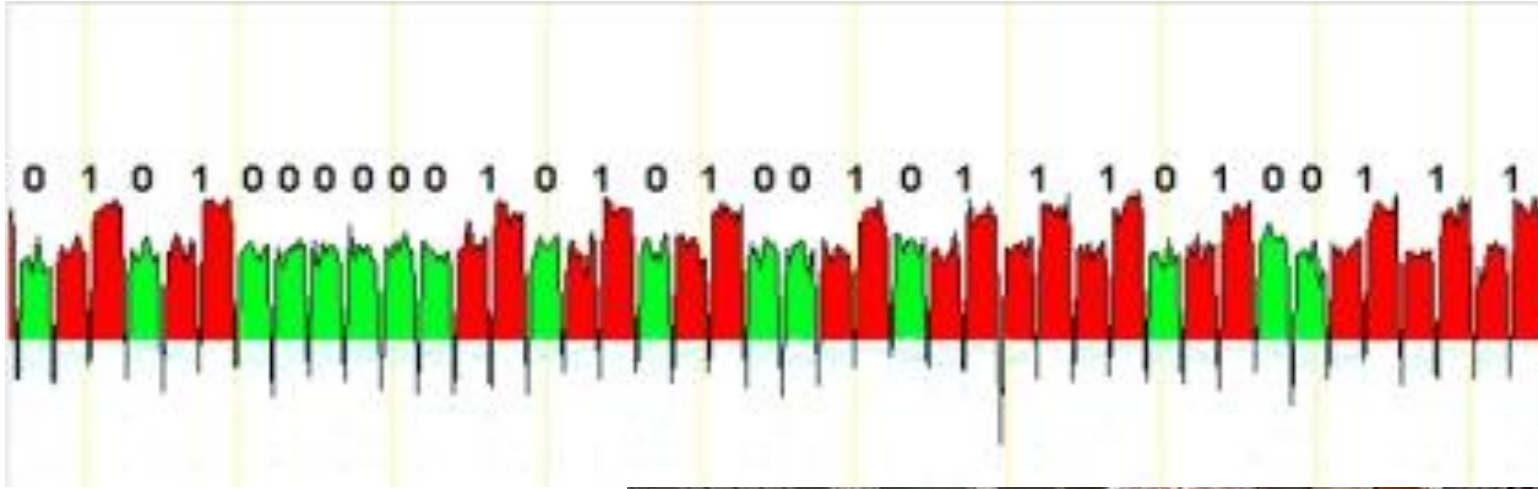
$[ab]P = (101228882920057626679704131545407930245895491542090988999577542687271695288383, \\ 77887418190304022994116595034556257760807185615679689372138134363978498341594)$



$b =$

10095557463932786418806
93831619070803277191091
90584053916797810821934
05190826

What's happened since 1999?



Quantum computers ↔ Cryptopocalypse



- Quantum computers break elliptic curves, finite fields, factoring, everything currently used for PKC



- Aug 2015: NSA announces plans to transition to quantum-resistant algorithms



- Feb 2016: NIST calls for quantum-secure submissions

Elliot Carr

Friday 1 April: Maths Seminar by Craig Co... Tue 9:25 AM

Dear All,

Christian Paquin

QC hardware breakthrough: researchers ... Tue 5:52 AM

One step closer, millions more to go J

Michael Naehrig

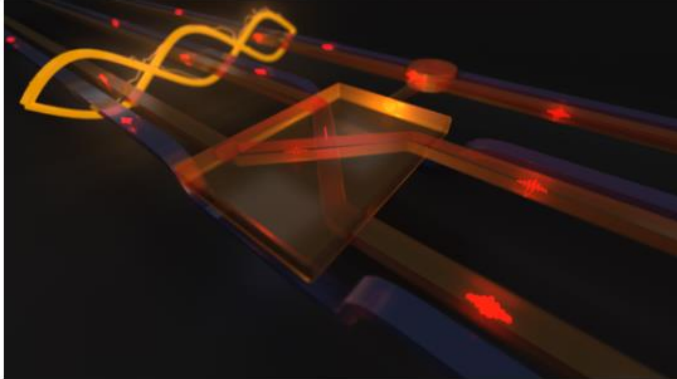
Status for the week ending March 25th, 2... Tue 4:07 AM

PQCrypto

[Home](#) / [Hardware](#)

Quantum computing is now a big step closer thanks to a new breakthrough: the Fredkin gate

For the first time ever, scientists have found a way to build a quantum Fredkin gate.



An artist's rendering of the quantum Fredkin gate, powered by entanglement, operating on photonic qubits.

Credit: Raj Patel and Geoff Pryde, Center for Quantum Dynamics, Griffith University.

[COMMENTS](#)

Katherine Noyes

IDG News Service Mar 28, 2016 11:24 AM

Quantum computing is now within closer reach thanks to a major breakthrough in which scientists have demonstrated that a key building block can be assembled.

Quantum computers are based on atomic-scale quantum bits, or qubits, that can

Cryptopocalypse now?

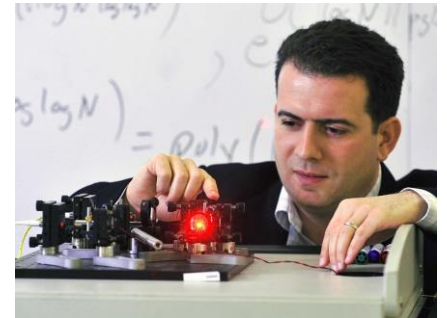
x = how long information needs to be secure

y = how long it takes to deploy

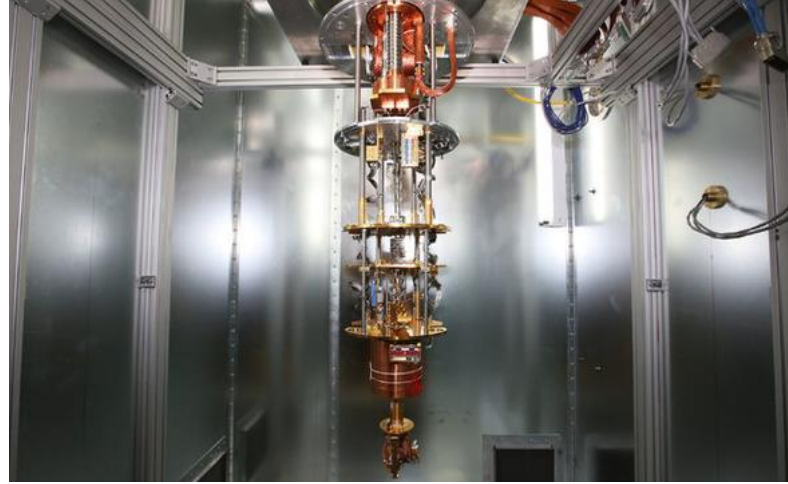
z = how far away is a quantum computer

Mosca's theorem:

if $x + y > z$, we're screwed!



Post-quantum key exchange



What hard problem(s) do we use now???

Codes?
Isogenies?

This talk: lattice problems

Multivariate
eq's?



Just key exchange for this talk...

- Simplicity and ease of exposition
- [BCNS'15]'s excuse: more important to quantum-secure key exchange first
- Possible to do lattice-based [*insert favorite primitive*]

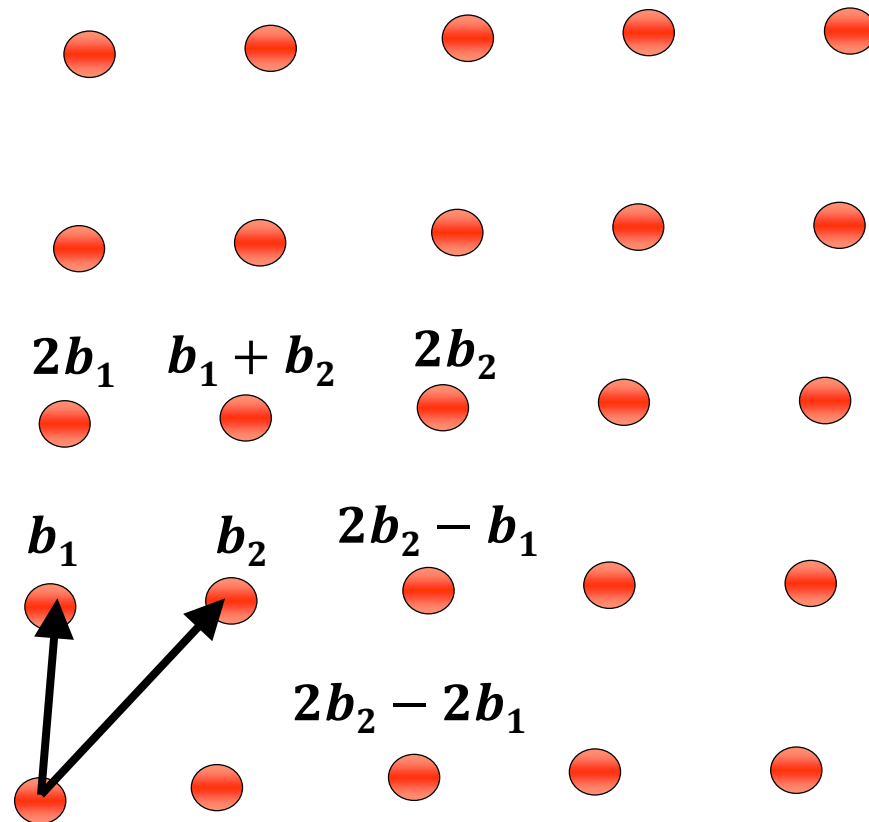
Part 1: Recap and motivation

Part 2: Lattice basics

Part 3: PQ key exchange based on (R)LWE

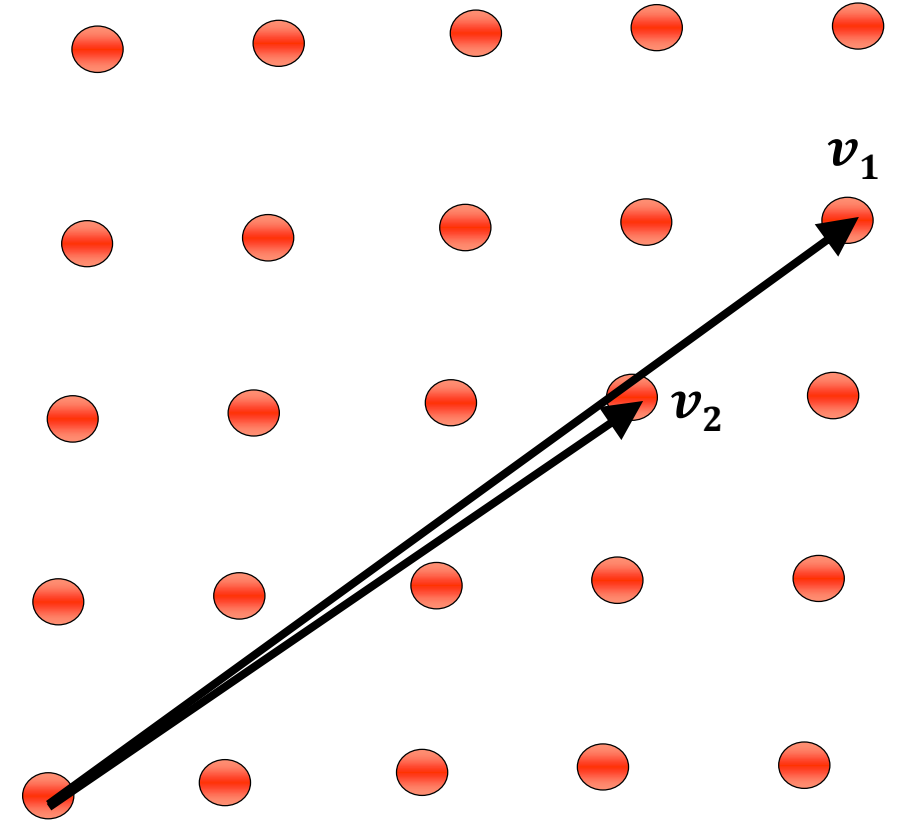
Lattices

- Basis $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^n$
- Lattice $\mathbf{L} = \{a_1 \mathbf{b}_1 + \dots + a_n \mathbf{b}_n : a_i \in \mathbb{Z}\}$



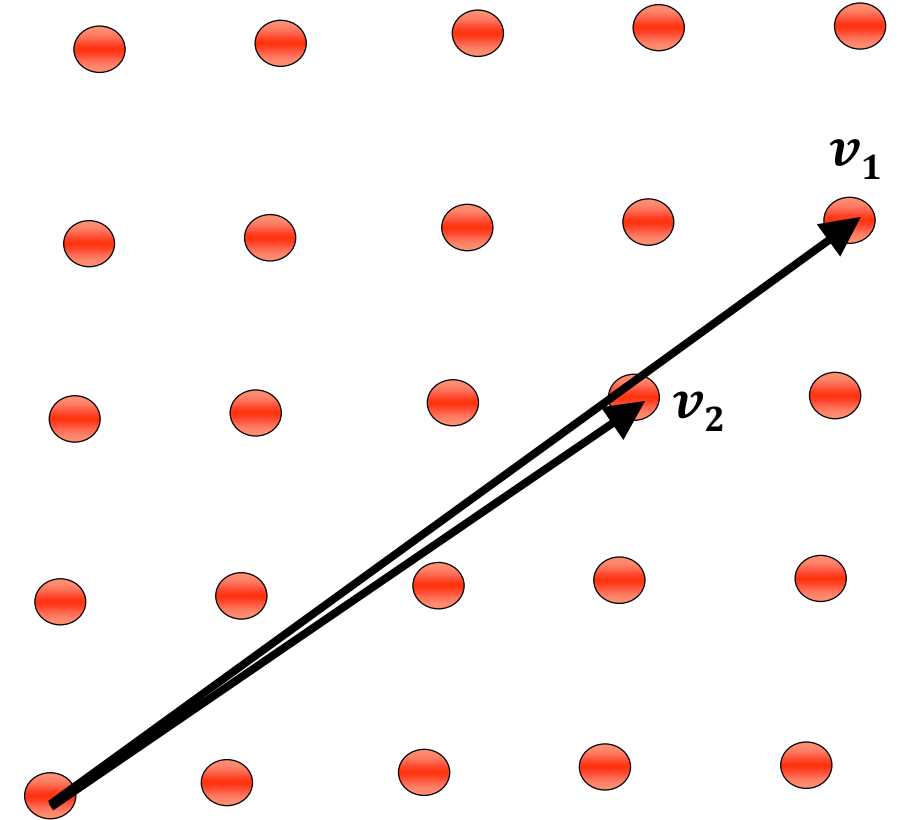
Lattices

- Basis $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^n$
- Lattice $\mathbf{L} = \{a_1\mathbf{b}_1 + \dots + a_n\mathbf{b}_n : a_i \in \mathbb{Z}\}$
- Bases not unique $\mathbf{L} = \sum a_i \mathbf{v}_i$
- e.g., $b_1 = (-2, 1), b_2 = (10, 6)$
 $v_1 = (4, -3), v_2 = (2, 4)$



Lattices

- Basis $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^n$
- Lattice $\mathbf{L} = \{a_1 \mathbf{b}_1 + \dots + a_n \mathbf{b}_n : a_i \in \mathbb{Z}\}$
- Bases not unique $\mathbf{L} = \sum a_i \mathbf{v}_i$

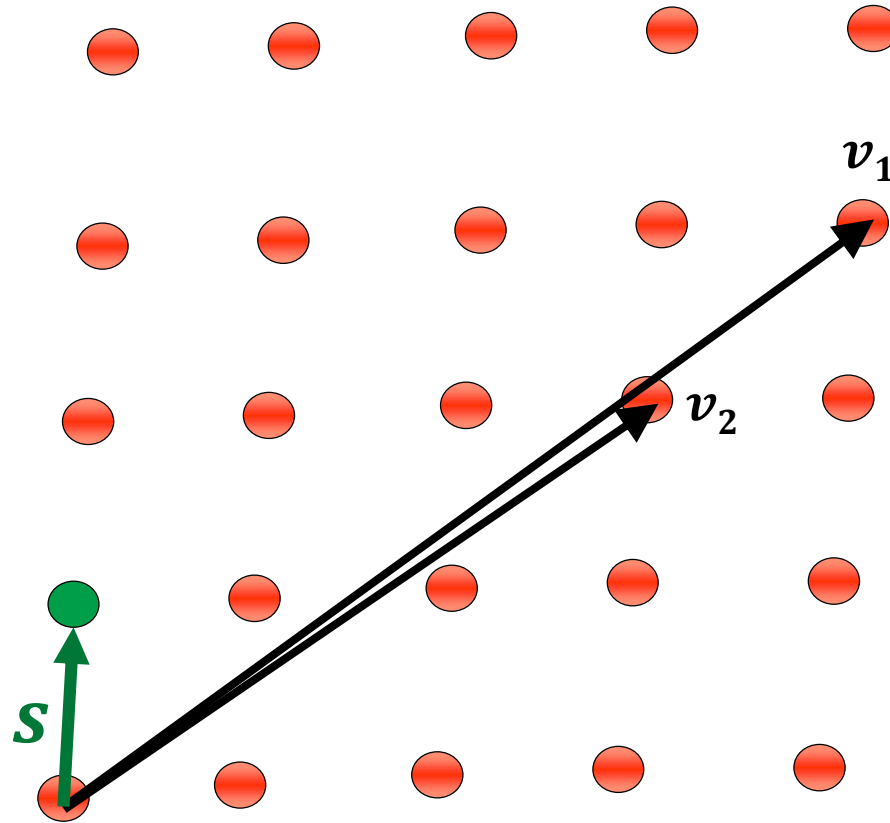


- e.g., $\mathbf{b}_1 = (-2, 1), \mathbf{b}_2 = (10, 6)$
 $\mathbf{v}_1 = (4, -3), \mathbf{v}_2 = (2, 4)$

$$\begin{bmatrix} -2 & 1 \\ 10 & 6 \end{bmatrix}_{\mathbf{b}_i} = \begin{bmatrix} 4 & -3 \\ 2 & 4 \end{bmatrix}_{\mathbf{v}_i} \cdot \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \quad \det = \pm 1$$

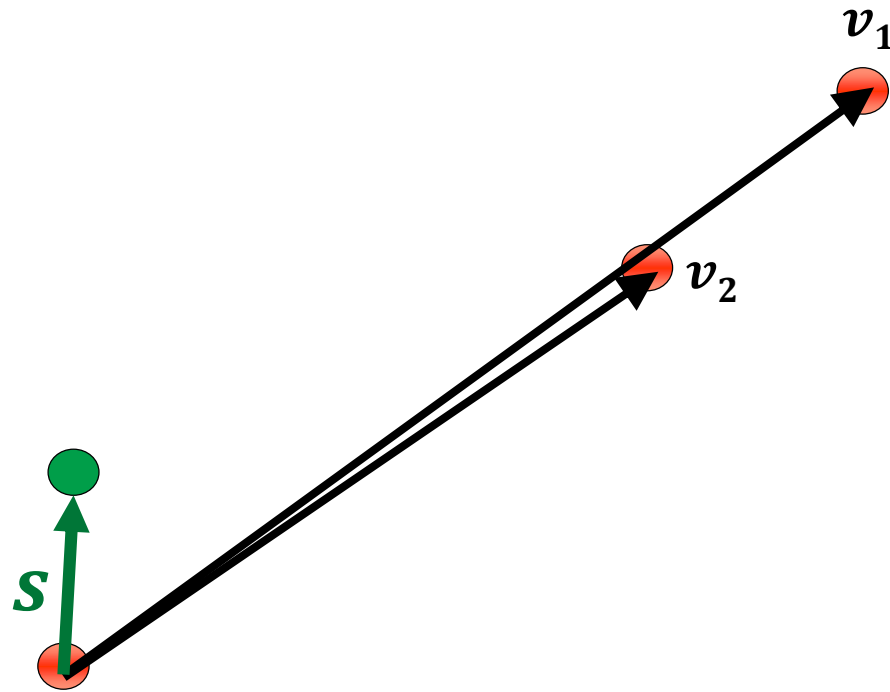
- Invariant $\det(\mathbf{L}) = |\det(\mathbf{b}_i)| = |\det(\mathbf{v}_i)|$

Hard Lattice Problem #1: Shortest Vector Problem (SVP_γ)



SVP: Given lattice $L = \{v_1, v_2\}$, find short vector $|s| \leq \gamma \cdot \lambda(L)$
($\gamma = 1$ means shortest vector)

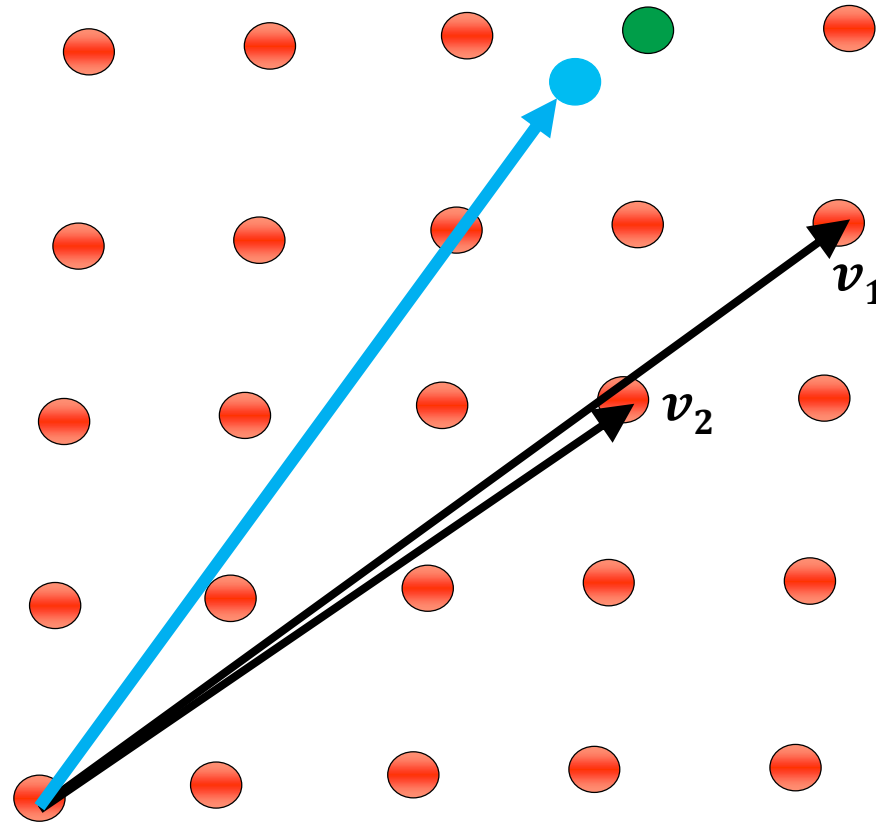
Hard Lattice Problem #1: Shortest Vector Problem (SVP_γ)



SVP_γ is NP-hard for $\gamma = O(1)$

SVP_γ is P for $\gamma = 2^{\Omega(n)}$

Hard Lattice Problem #2: Closest Vector Problem (CVP_d)



CVP_d : Given lattice $L = \{v_1, v_2\}$ and target vector $v \notin L$ within distance d ,
find the closest lattice point

Why are they hard?

- Gaussian elimination for CVP? What about least-squares?

- Gram-Schmidt to reduce basis?

$$b_i^* \leftarrow b_i - \sum_{1 \leq j \leq i-1} \mu_{ij} \cdot b_j^*$$

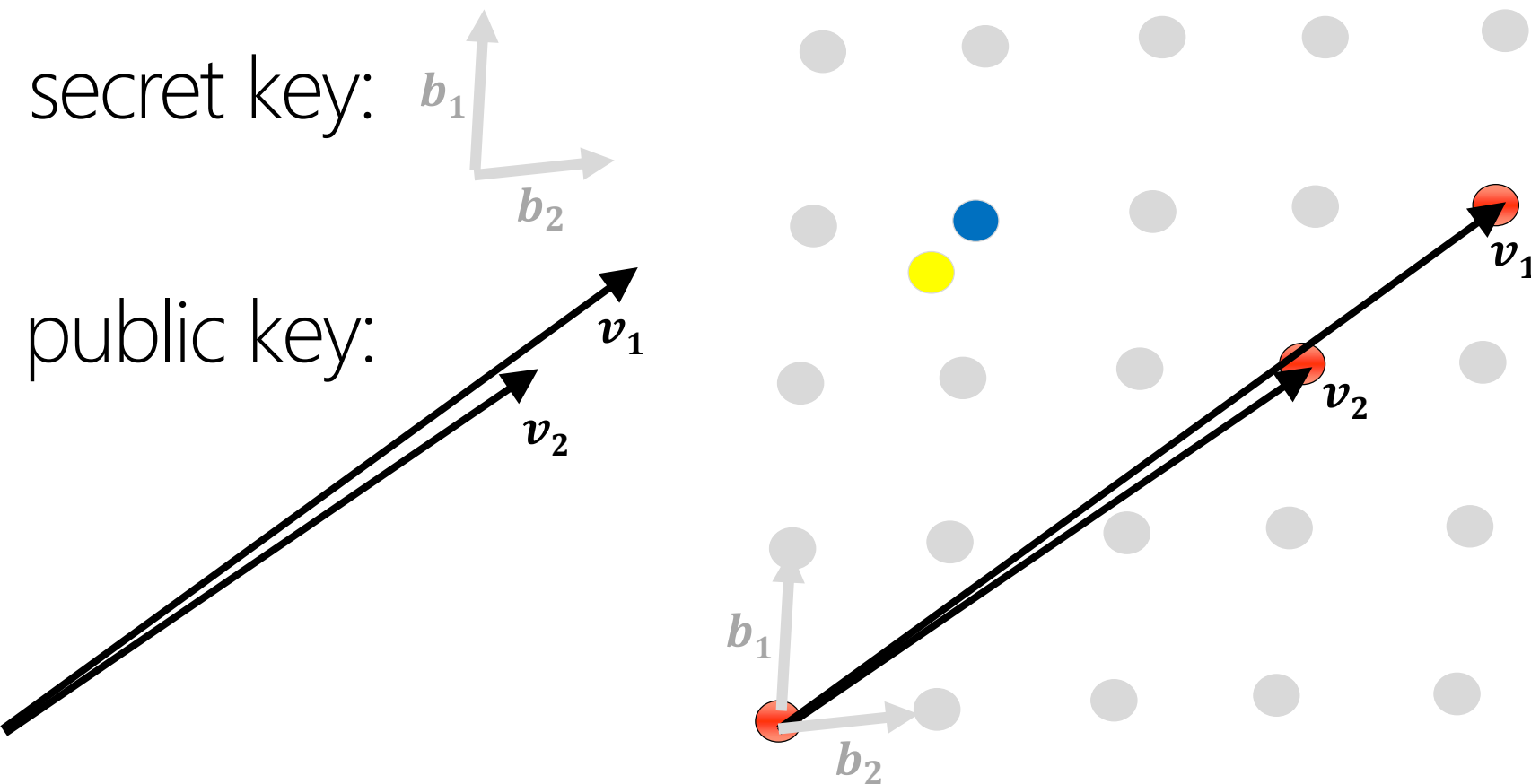
~~$$\mu_{ij} = \frac{\langle b_i^*, b_j^* \rangle}{|b_j^*|^2}$$~~

- SVP_γ NP-hard for $\gamma = O(1)$: "at least as hard as the hardest problems in NP" (if $P \neq NP$, then no polynomial time alg.)

Play time...

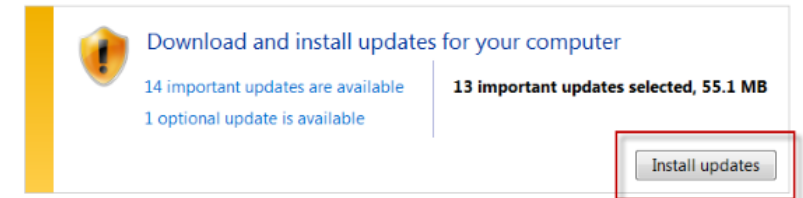
e.g., GGH'97 signatures (\approx NTRUSign)

Idea: CVP is hard, but easy with good basis



message: ●

signature: ●



Security reductions

- GGH'97 (\approx right idea, but) did not come with a “security proof”
- If you can solve CVP, you can obviously forge messages, but this scheme was completely broken without solving CVP
- We want Thm: “if you can forge signatures, you can solve CVP”
- **Ajtai'96:** worst-to-average-case reduction unlocks lattice-based crypto
“if you can break an average case, you can break the worst case”

Part 1: Recap and motivation

Part 2: Lattice basics

Part 3: PQ key exchange based on (R)LWE

Computing

Securing Today's
Data Against
Tomorrow's
Quantum Computers

RING LEARNING WITH ERRORS

Algorithmen für die Post-Quanten-Ära

RWC2015

Forscher haben das vor Quantencomputern sichere Key-Exchange-Verfahren Ring Learning With Errors präsentiert. Das lässt sich bereits experimentell in OpenSSL für TLS-Verbindungen einsetzen.

Call it an abundance of caution. A Microsoft research project has upgraded the encryption protocol that secures the Web to resist attacks from quantum computers—machines that are expected to have stupendous power but have never been built.

Governments and computing giants like IBM, Microsoft, and Google are vying to understand the effects of quantum computing problems that could arise in years (see “1

Microsoft Tests Quantum Computer-Proof Web Encryption

Matthew Broersma, August 4, 2015, 12:10 pm



0 Comments

Items to fend off attacks by advanced quantum

Hacked NEWS VIDEOS SECURITY TUTORIALS TOP LISTS SHOWCASES PRESS RELEASES WHITEPAPERS WIKI Q

HOME / CYBERSECURITY NEWS

Cryptographers Develop Encryption Method Resistant to Future Quantum Attacks

August 18, 2015 Clulio Prisco 5

Cybersecurity News, Science News

Advertising

TechWeek europe

RELATED THEMES

Microsoft

Cryptographers aim to future-proof protocol

THE AUSTRALIAN | AUGUST 18, 2015 12:00AM

SAVE



Jennifer Foreshew
Technology reporter
Sydney



Queensland University of Technology's Douglas Stebila and his team are upgrading encryption protocols.

The need to secure today's communications from the powerful quantum computers of the future has propelled new research aimed at upgrading the internet's core encryption protocol.

This work is being led by a team of cryptographers, including Queensland University of Technology's Douglas Stebila, that has tested some new techniques and found promising steps towards future-proofing internet encryption.

Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. IEEE Security & Privacy, 2015. DOI: [10.1109/SP.2015.40](https://doi.org/10.1109/SP.2015.40)

joint work with

Joppe Bos (NXP), Michael Naehrig (MSR), Douglas Stebila (QUT)



Microsoft Research



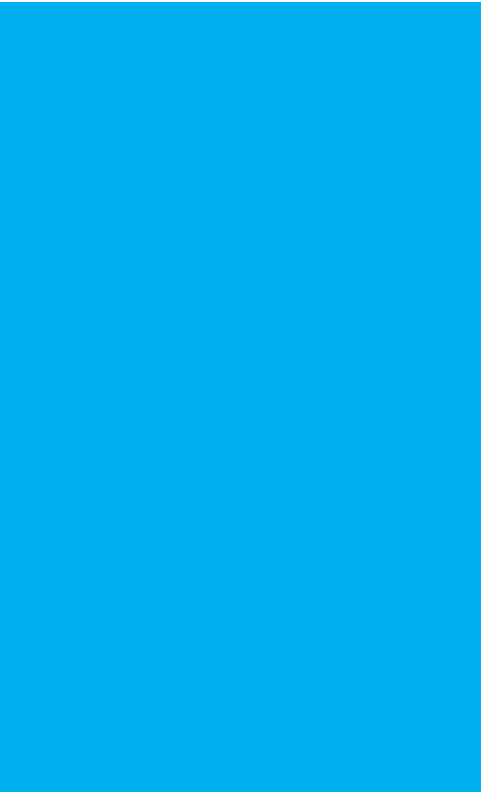
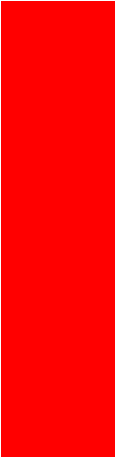
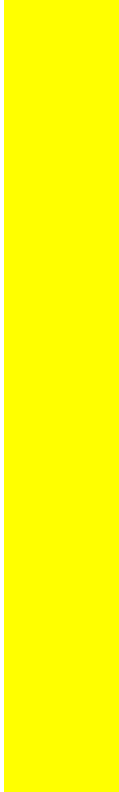

Regev'05

- Introduces the “Learning with Errors” (LWE) problem
- Uses it to construct LWE encryption
- Shows that breaking LWE implies (quantum) solving hard lattice problems (GapSVP and SIVP)

see his 2012 talk

<http://research.microsoft.com/apps/video/default.aspx?id=166559>

The learning with errors (LWE) problem

random		secret		small		ind. from random
$\mathbb{Z}_q^{m \times n}$		$\mathbb{Z}_q^{n \times 1}$		$\mathbb{Z}_q^{m \times 1}$		$\mathbb{Z}_q^{m \times 1}$
	\times		$+$		$=$	

LWE problem: given **blue**, find (or just decide if \exists) **red**

The learning with errors (LWE) problem

random $\mathbb{Z}_{13}^{7 \times 4}$ secret $\mathbb{Z}_{13}^{4 \times 1}$ small $\mathbb{Z}_{13}^{7 \times 1}$ ind. from random $\mathbb{Z}_{13}^{7 \times 1}$

4	1	11	10
5	5	9	5
3	9	0	10
1	3	3	2
12	7	3	4
6	5	11	4
3	3	5	0

\times

$+$

$=$

4
7
2
11
5
12
8

LWE problem: given **blue**, find **red**

The learning with errors (LWE) problem

random $\mathbb{Z}_{13}^{7 \times 4}$		secret $\mathbb{Z}_{13}^{4 \times 1}$		small $\mathbb{Z}_{13}^{7 \times 1}$		ind. from random $\mathbb{Z}_{13}^{7 \times 1}$																																														
<table><tr><td>4</td><td>1</td><td>11</td><td>10</td></tr><tr><td>5</td><td>5</td><td>9</td><td>5</td></tr><tr><td>3</td><td>9</td><td>0</td><td>10</td></tr><tr><td>1</td><td>3</td><td>3</td><td>2</td></tr><tr><td>12</td><td>7</td><td>3</td><td>4</td></tr><tr><td>6</td><td>5</td><td>11</td><td>4</td></tr><tr><td>3</td><td>3</td><td>5</td><td>0</td></tr></table>	4	1	11	10	5	5	9	5	3	9	0	10	1	3	3	2	12	7	3	4	6	5	11	4	3	3	5	0	\times	<table><tr><td>6</td></tr><tr><td>9</td></tr><tr><td>11</td></tr><tr><td>11</td></tr></table>	6	9	11	11	$+$	<table><tr><td>0</td></tr><tr><td>-1</td></tr><tr><td>1</td></tr><tr><td>1</td></tr><tr><td>1</td></tr><tr><td>0</td></tr><tr><td>-1</td></tr></table>	0	-1	1	1	1	0	-1	$=$	<table><tr><td>4</td></tr><tr><td>7</td></tr><tr><td>2</td></tr><tr><td>11</td></tr><tr><td>5</td></tr><tr><td>12</td></tr><tr><td>8</td></tr></table>	4	7	2	11	5	12	8
4	1	11	10																																																	
5	5	9	5																																																	
3	9	0	10																																																	
1	3	3	2																																																	
12	7	3	4																																																	
6	5	11	4																																																	
3	3	5	0																																																	
6																																																				
9																																																				
11																																																				
11																																																				
0																																																				
-1																																																				
1																																																				
1																																																				
1																																																				
0																																																				
-1																																																				
4																																																				
7																																																				
2																																																				
11																																																				
5																																																				
12																																																				
8																																																				

LWE problem: given blue, find red

Toy example versus real-world example

$$\mathbb{Z}_{13}^{7 \times 4}$$

4	1	11	10
5	5	9	5
3	9	0	10
1	3	3	2
12	7	3	4
6	5	11	4
3	3	5	0

$$\mathbb{Z}_{4093}^{640 \times 256}$$

256

640	2738 3842 3345 2979 ...			
	2896	595	3607	
	377	1575		
	2760			
	⋮			

$$640 \times 256 \times 12 = 1966080 \text{ bits} \\ = 245 \text{ kB !!}$$

The learning with errors (LWE) problem

random $\mathbb{Z}_{13}^{7 \times 4}$ secret $\mathbb{Z}_{13}^{4 \times 1}$ small $\mathbb{Z}_{13}^{7 \times 1}$ ind. from random $\mathbb{Z}_{13}^{7 \times 1}$

4	1	11	10
5	5	9	5
3	9	0	10
1	3	3	2
12	7	3	4
6	5	11	4
3	3	5	0

\times

6
9
11
11

$+$

0
-1
1
1
1
0
-1

$=$

4
7
2
11
5
12
8

LWE problem: given blue, find red

The **ring** learning with errors (**R-LWE**) problem

random $\mathbb{Z}_{13}^{7 \times 4}$ secret $\mathbb{Z}_{13}^{4 \times 1}$ small $\mathbb{Z}_{13}^{7 \times 1}$ ind. from random $\mathbb{Z}_{13}^{7 \times 1}$

4	1	11	10
10	4	1	11
11	10	4	1
1	11	10	4
12	7	3	4
4	12	7	3
3	4	12	7

\times

6
9
11
11

$+$

0
-1
1
1
1
0
-1

$=$

4
6
4
0
5
8
2

Lyubashevsky-Peikert-Regev '10: add ring structure

The **ring** learning with errors (**R-LWE**) problem

random $\mathbb{Z}_{13}^{7 \times 4}$ secret $\mathbb{Z}_{13}^{4 \times 1}$ small $\mathbb{Z}_{13}^{7 \times 1}$ ind. from random $\mathbb{Z}_{13}^{7 \times 1}$

4	1	11	10
3	4	1	11
2	3	4	1
12	2	3	4
12	7	3	4
9	12	7	3
10	9	12	7

\times

6
9
11
11

$+$

0
-1
1
1
0
-1

$=$

4
3
4
12
5
12
11

The **ring** learning with errors (**R-LWE**) problem

random small secret small ind. from random

$\mathbb{Z}_{13}^{7 \times 4}$ $\mathbb{Z}_{13}^{4 \times 1}$ $\mathbb{Z}_{13}^{7 \times 1}$ $\mathbb{Z}_{13}^{7 \times 1}$

4	1	11	10
3	4	1	11
2	3	4	1
12	2	3	4
12	7	3	4
9	12	7	3
10	9	12	7

\times

-1
0
-1
1

$+$

0
-1
1
1
1
0
-1

$=$

8
6
9
3
3
0
10

The **ring** learning with errors (**R-LWE**) problem

random secret small ind. from random

$\mathbb{Z}_{13}^{7 \times 4}$ $\mathbb{Z}_{13}^{4 \times 1}$ $\mathbb{Z}_{13}^{7 \times 1}$ $\mathbb{Z}_{13}^{7 \times 1}$

4	1	11	10
3	4	1	11
2	3	4	1
12	2	3	4

\times

-1
0
-1
1

$+$

0
-1
1
1

$=$

8
6
9
3

LWE problem: given **blue**, find **red**

The **ring** learning with errors (**R-LWE**) problem

$$\mathbb{Z}_{13}^{4 \times 4} \longrightarrow \mathbb{Z}_{13}[x] / \langle x^4 + 1 \rangle$$

4	1	11	10
3	4	1	11
2	3	4	1
12	2	3	4

$$\longrightarrow 4 + 1x + 11x^2 + 10x^3$$

$$\longrightarrow = x \cdot (4 + 1x + 11x^2 + 10x^3)$$

$$\longrightarrow = x^2 \cdot (4 + 1x + 11x^2 + 10x^3)$$

$$\longrightarrow = x^3 \cdot (4 + 1x + 11x^2 + 10x^3)$$

Ideal lattice: lattice modulo ideal

The **ring** learning with errors (**R-LWE**) problem

$$\begin{array}{r} 4 + 1x + 11x^2 + 10x^3 \\ \times \quad -1 + 0x - 1x^2 + 1x^3 \\ + \quad 0 - 1x + 1x^2 + 1x^3 \\ \hline 10 + 5x + 10x^2 + 7x^3 \\ \hline \end{array} \quad \frac{\mathbb{Z}_{13}[x]}{\langle x^4 + 1 \rangle}$$

R-LWE problem: given **blue**, find **red**

The **ring** learning with errors (**R-LWE**) problem
(the 128-bit secure version)

$$\begin{array}{rcl}
 & 2792930407 + \cdots + 2938465015x^{1023} & \\
 \times & 5 - 3x \dots + 9x^{1022} - 1x^{1023} & \\
 + & 2 + 4x \dots - 0x^{1022} + 6x^{1023} & \\
 \hline
 & 3159804584 + \cdots + 1153769078x^{1023} & \\
 \hline
 \end{array}
 \frac{\mathbb{Z}_{2^{32}-1}[x]}{\langle x^{1024} + 1 \rangle}$$

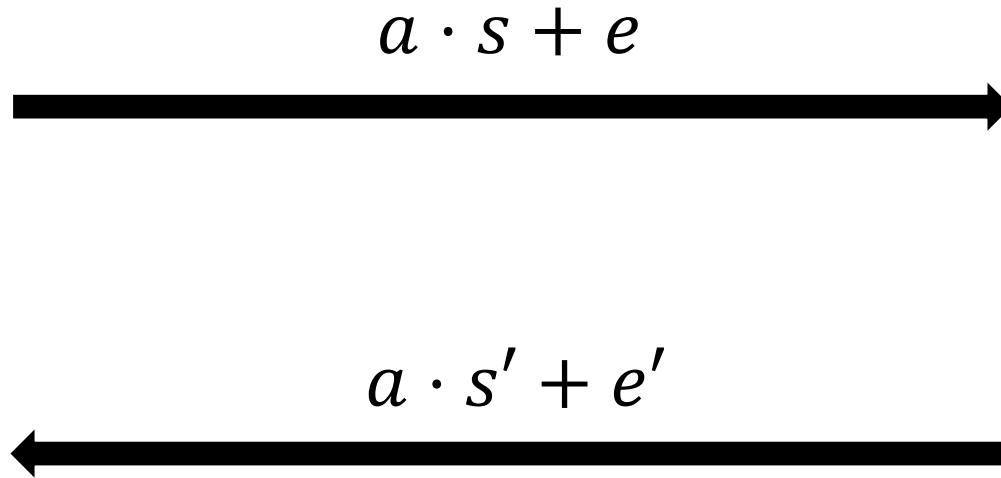
R-LWE problem: given **blue**, find (small!) **red**

R-LWE-DH: key agreement in $R_q = \mathbb{Z}_q[x]/\langle x^n + 1 \rangle$

public: "big" $a \in R_q$

secret: "small" $e, s \in R_q$

secret: "small" $e', s' \in R_q$

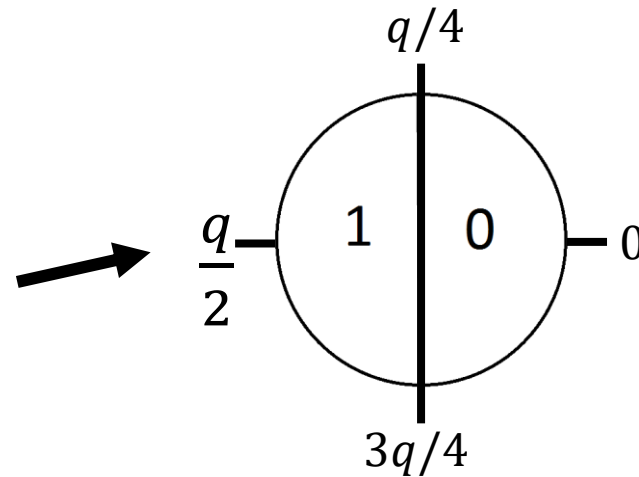


$$(s \cdot (a \cdot s' + e')) \approx s \cdot a \cdot s'$$

$$(s' \cdot (a \cdot s + e)) \approx s \cdot a \cdot s'$$

Approximate agreement mod q

the usual
ROUND
function



$$4079331841 + 1894732145 \cdot x + \dots + 472608255 \cdot x^{1022} + 516748383 \cdot x^{1023}$$

\gg

\gg

\gg

\gg



$$4079332556 + 1894733033 \cdot x + \dots + 472607765 \cdot x^{1022} + 516748363 \cdot x^{1023}$$

\parallel

\parallel

\parallel

\parallel

ROUND

0

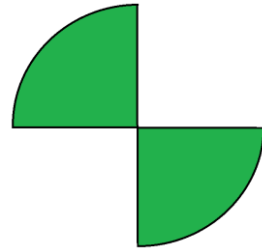
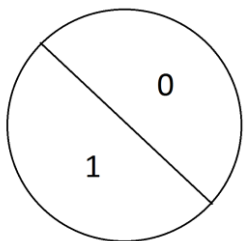
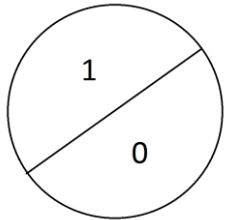
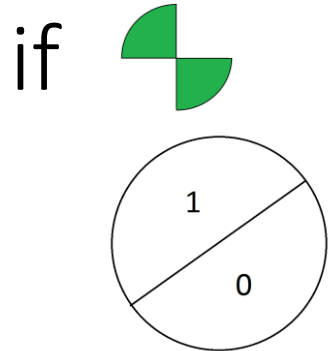
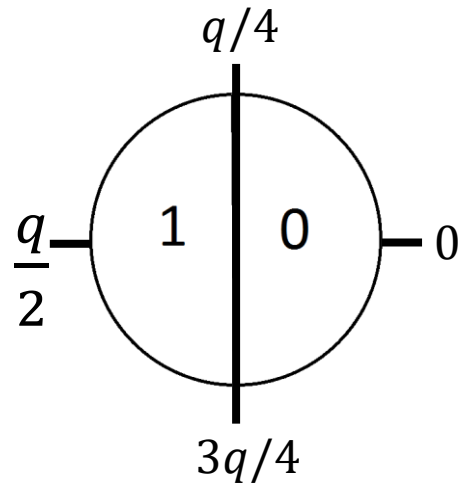
1

0

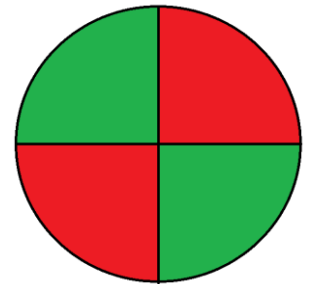
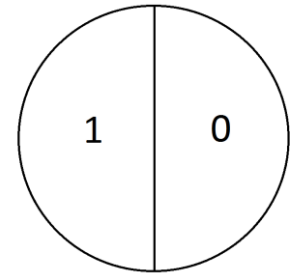
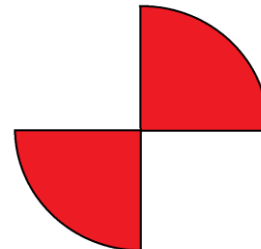
0

This will work most of the time (fails $\approx 1/2^{10}$), but we need **exact agreement**
i.e., what happens if one of the coefficients is in the “**danger zone(s)**”

Making approximate agreement exact in \mathbb{Z}_q



or



R-LWE-DH: exact key agreement

public: “big” $a \in R_q$

secret: “small” $e, s \in R_q$

secret: “small” $e', s' \in R_q$



$a \cdot s + e$



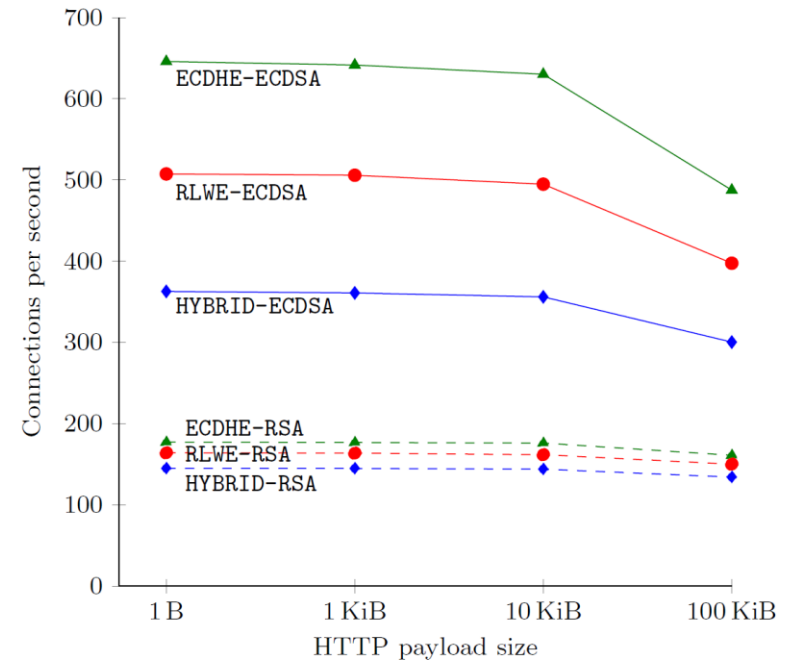
$a \cdot s' + e'$ and $\{\text{green square}, \text{red square}\}^n \in \{0,1\}^n$

$$\text{RECONCILE}(s \cdot (a \cdot s' + e'), \{\text{green square}, \text{red square}\}^n) = \text{ROUND}(s' \cdot (a \cdot s + e))$$

both parties now share $k \in \{0,1\}^n$

Summary

- [BCNS'15] developed and implemented key exchange protocol based on ring-LWE
- Proof of security based on decision-RLWE
- Plugged into TLS protocol and open sourced the software. Showed performance comparable to existing (non-PQ) stuff
- Subsequent work (by others and us) blows our performance out of the water, shows that RLWE-DH much faster than ECC/RSA/finite fields
- Price of PQ paranoia: big keys



Questions?

