Practical post-quantum key agreement from both ideal and generic lattices

Speaker: Valeria Nikolaenko

Stanford University

"New Hope" eprint.iacr.org/2015/1092

[Erdem Alkim, Léo Ducas, Thomas Pöppelmann and Peter Schwabe]

"Frodo" eprint.iacr.org/2016/659

[Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, myself, Ananth Raghunathan and Douglas Stebila]

Real World Cryptography Conference 2017 ◦ January 4, 2017

Quantum computer breaks public key crypto

Public key crypto (key agreement & signatures)

RSA, DH, DSA

ECDH, ECDSA

Symmetric key crypto

AES-128

Hash functions

SHA-256, SHA3-256

Quantum computer breaks public key crypto

In the presence of a quantum computer:

Public key crypto (key agreement & signatures)

~~**RSA, DH, DSA**~~
~~**ECDH, ECDSA**~~

No longer secure

Feb 2016: NIST calls for proposals

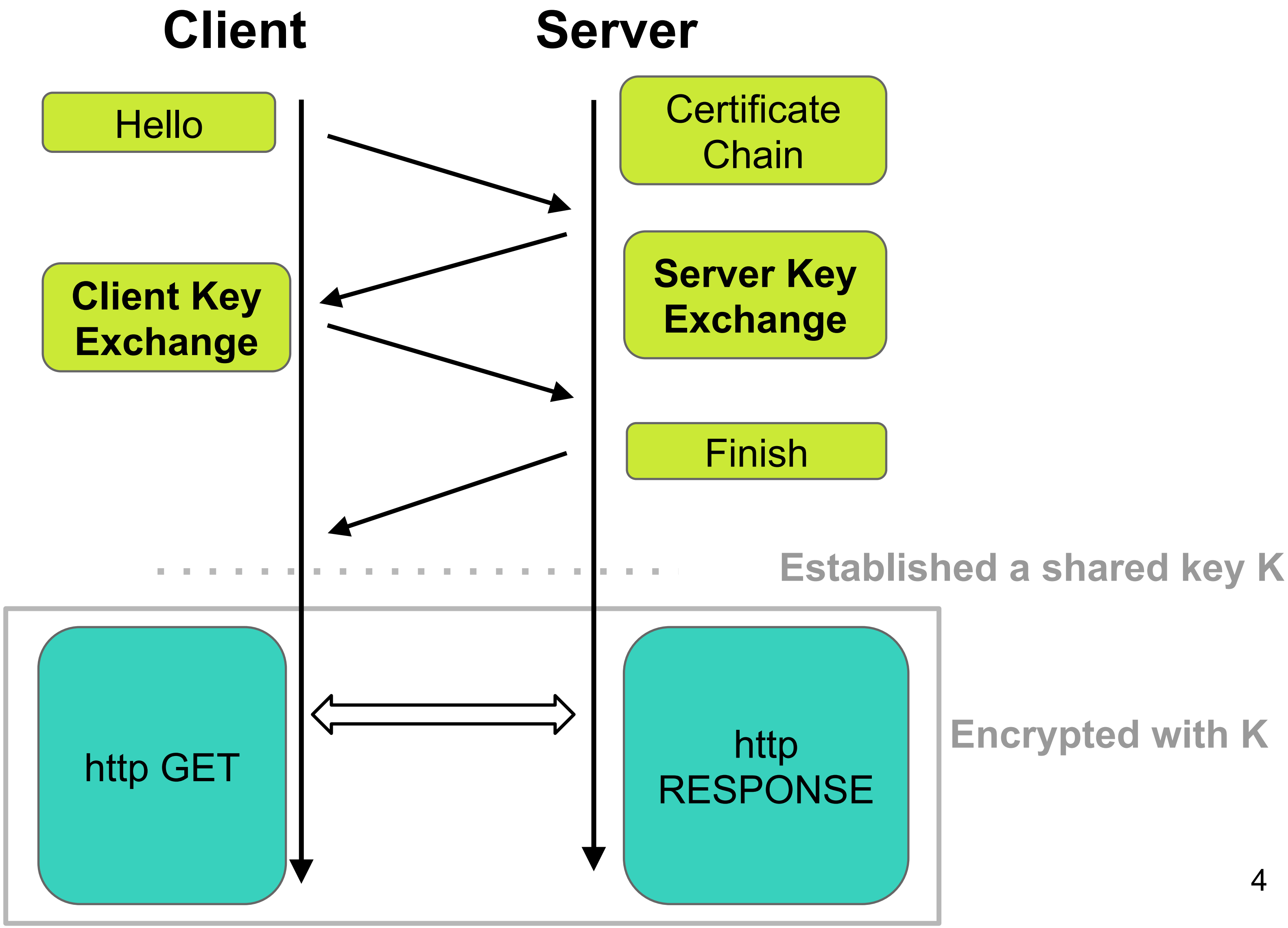
Symmetric key crypto

AES-128 — **Needs longer keys**

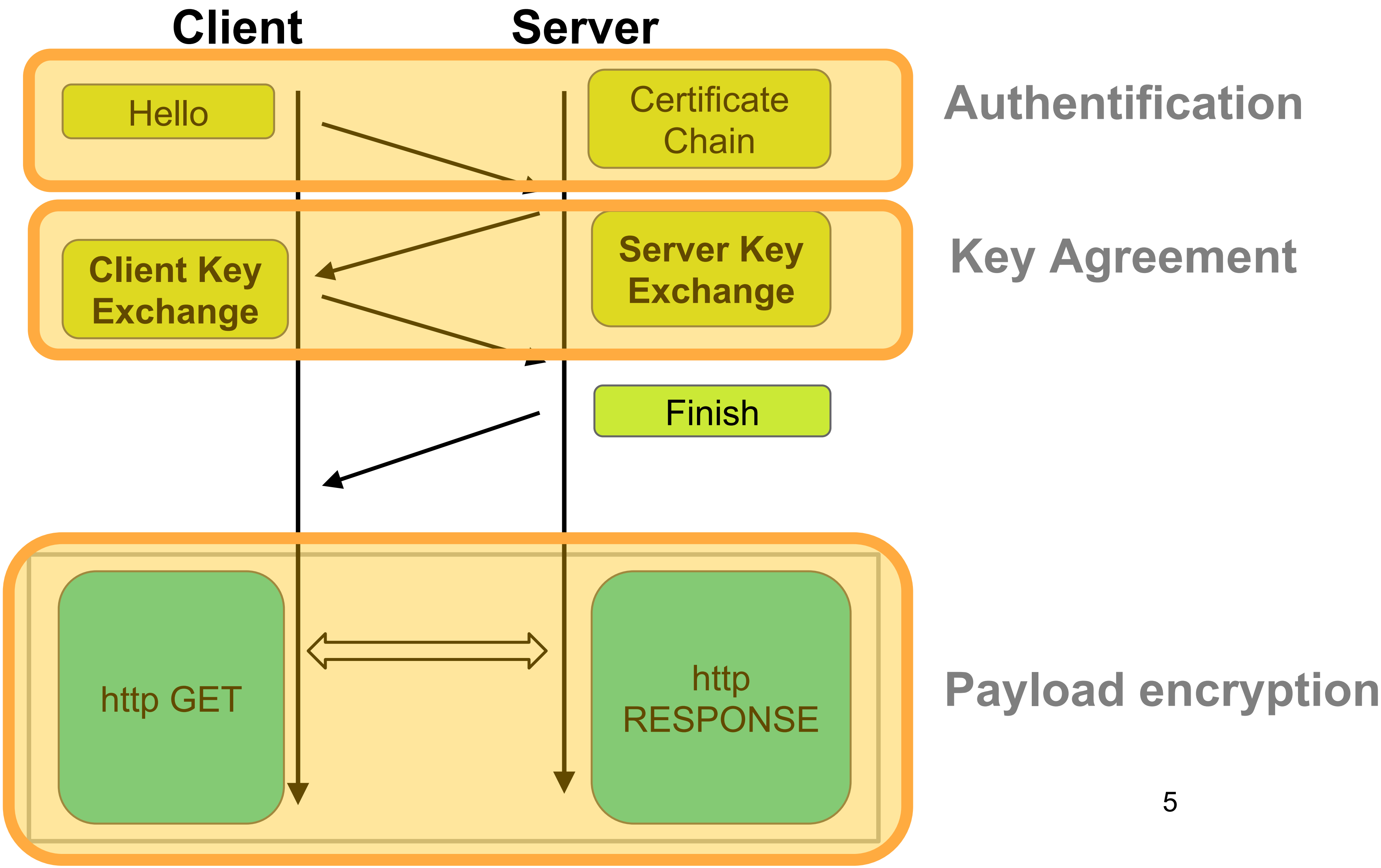
Hash functions

SHA-256, SHA3-256 — **Needs longer output**

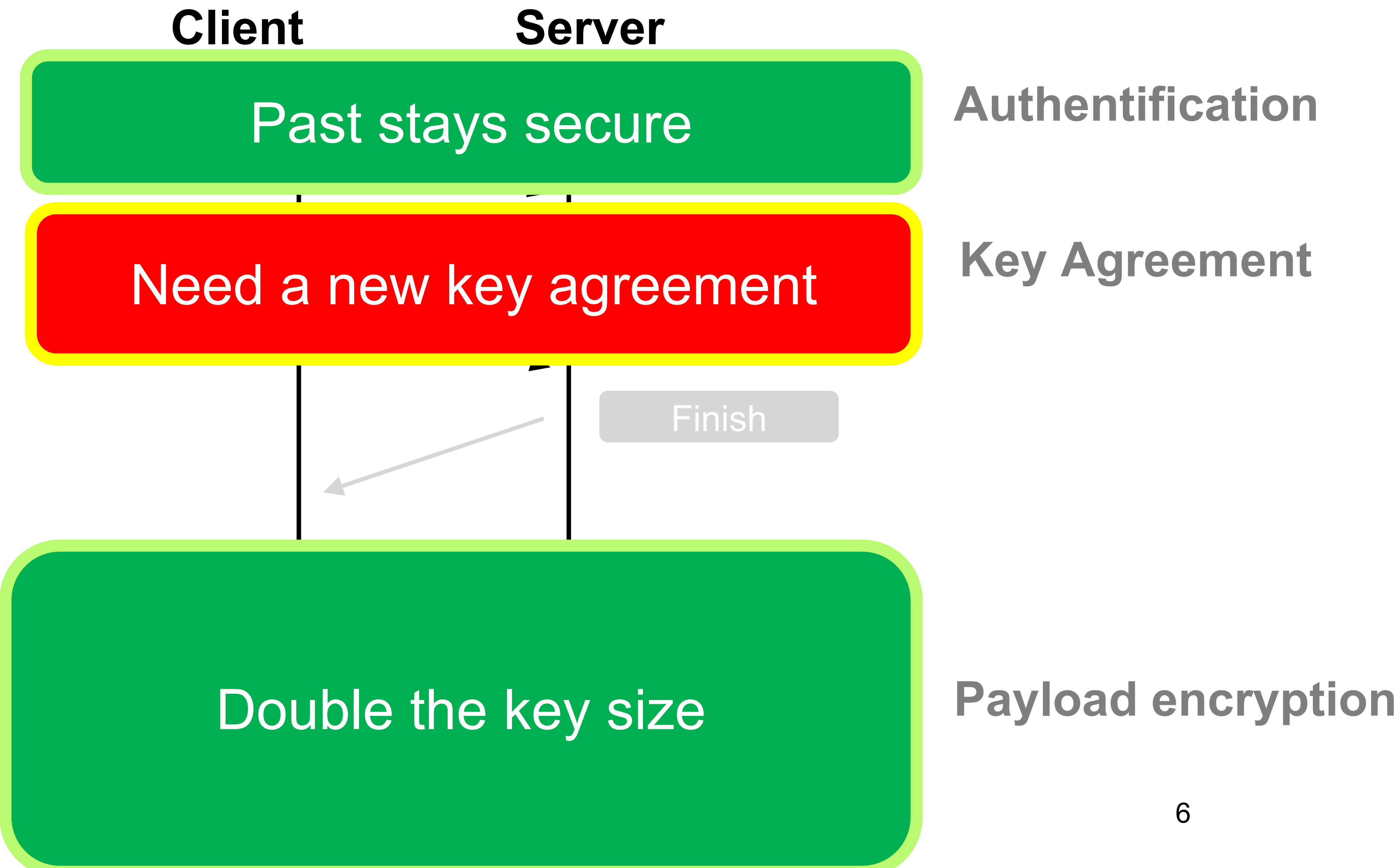
TLS protocol



TLS protocol



TLS protocol in the post-quantum world

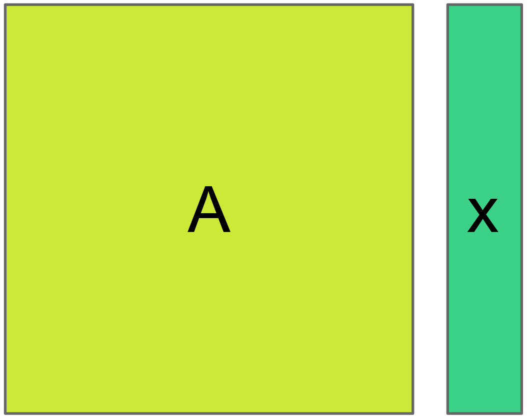


Should we expect a quantum computer?

Oct 2014: predicts a quantum computer in **15 years** (Matteo Mariantoni)

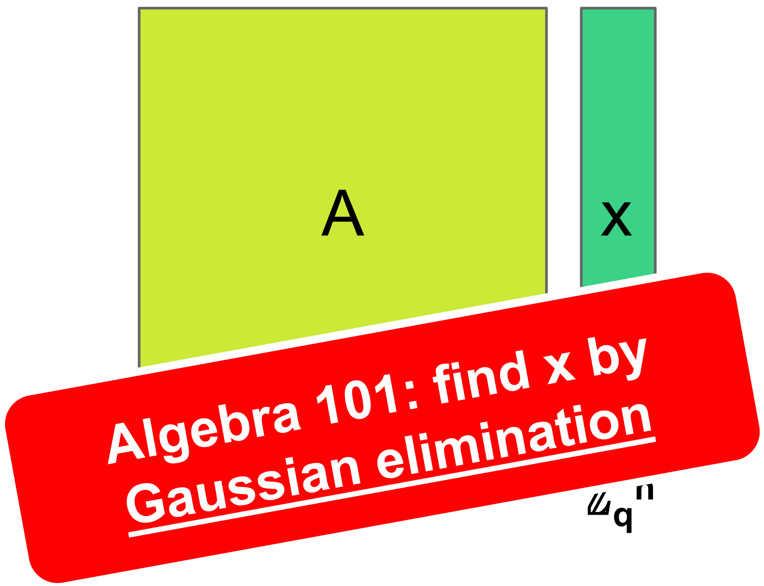
Jan 2014: **invested $80 million** (E. Snowden through Washington Post)
Aug 2015: **suggests moving towards quantum-secure crypto!**

Learning with Errors (LWE): new foundation for key agreement



$\mathbb{Z}_q^{n \times n}$ $\mathbb{Z}_q^{n}$

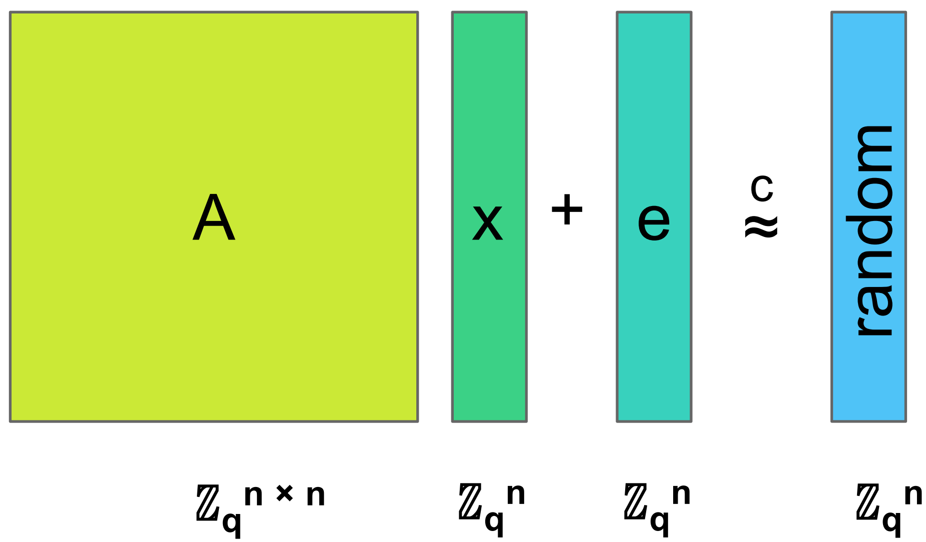
Learning with Errors (LWE): new foundation for key agreement



Learning with Errors (LWE): new foundation for key agreement

For a random A, random small x and e

(A, Ax+e) looks like (A, random) [Regev05]

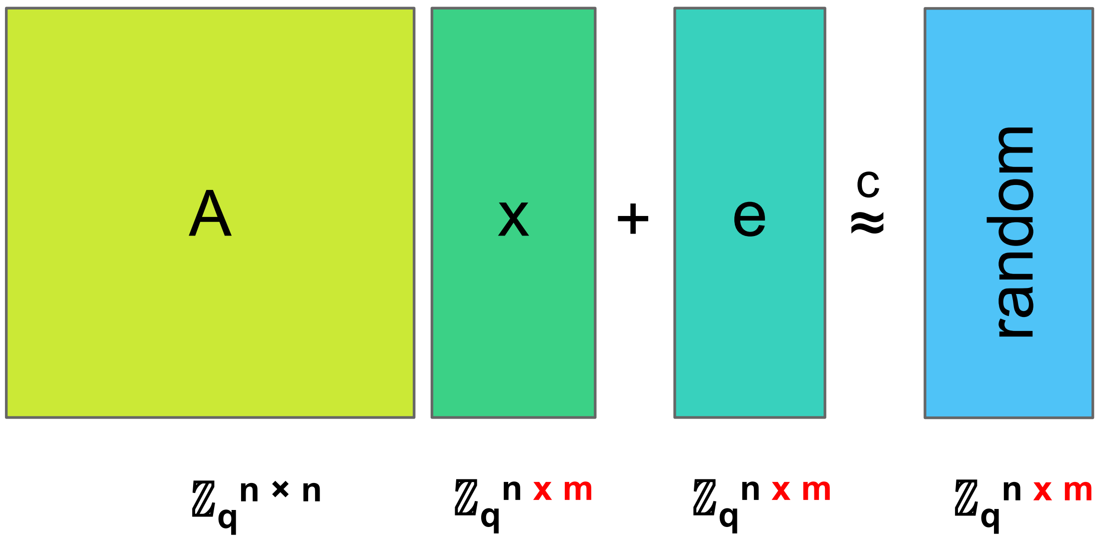


O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC 2005.

Learning with Errors (LWE): new foundation for key agreement

For a random A, random small x and e

(A, Ax+e) looks like (A, random) [Regev05]



LWE ≦ "Frodo" key agreement

O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC 2005.

Ring-Learning with Errors (RLWE):

$\mathbb{Z}_{17}^{4\times 4}$

A =

4	1	11	6
-6	4	1	11
-11	-6	4	1
-1	-11	-6	4

- Each row is a cyclic shift of the row above (x wraps to –x mod 17)

Ring-Learning with Errors (RLWE):

$\mathbb{Z}_{17}^{4\times4}$

a =

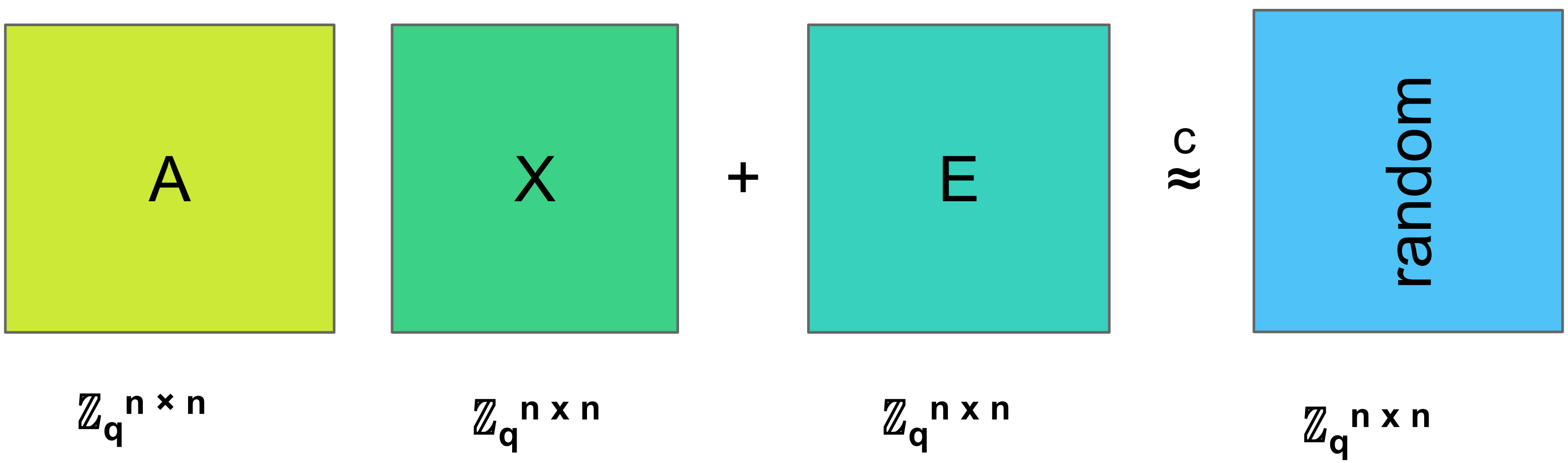
4	1	11	6

- Each row is a cyclic shift of the row above (x wraps to –x mod 17)
- Can only sent the first row => saves **communication**
- Saves **computation** (NTT instead of matrix-matrix product)

Ring-Learning with Errors (**RLWE**):

For a random **cyclic** A, random small **cyclic** X and E

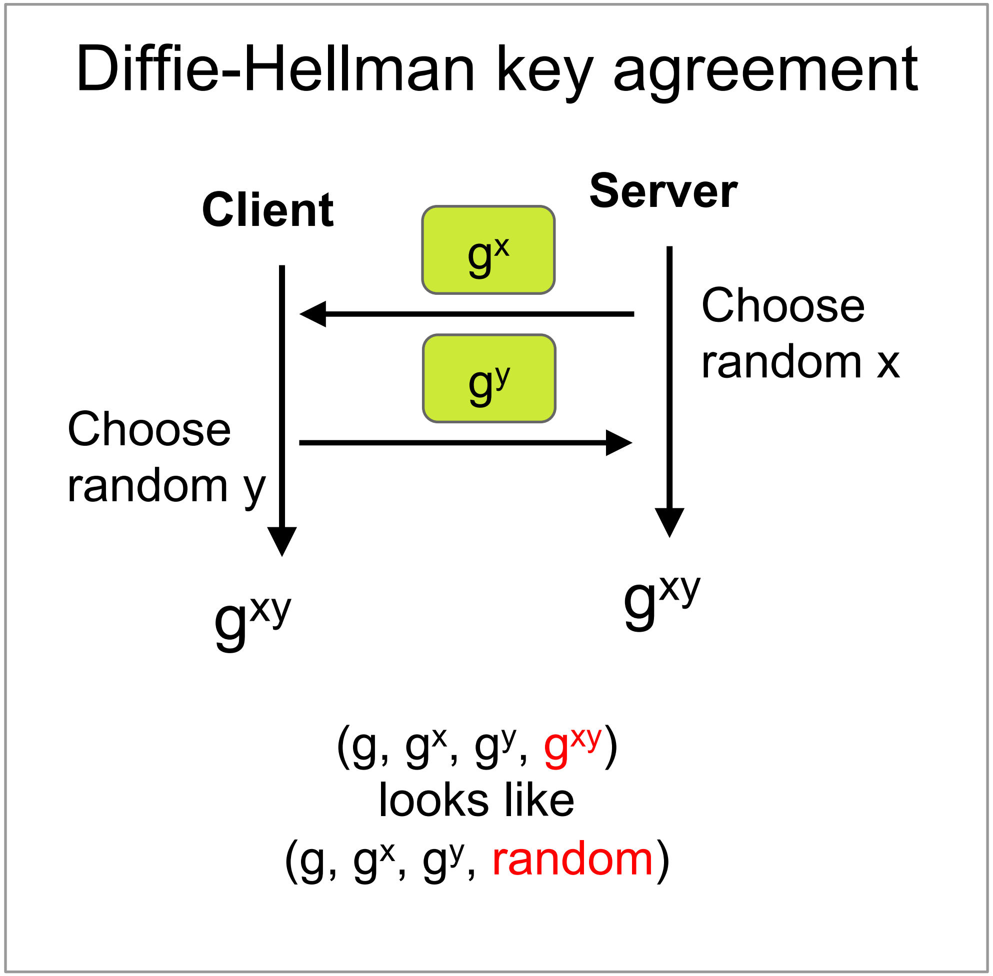
(A, AX+E) looks like (A, random) [LyubashevskyPR10]



Ring-LWE ≦ "New Hope" key agreement

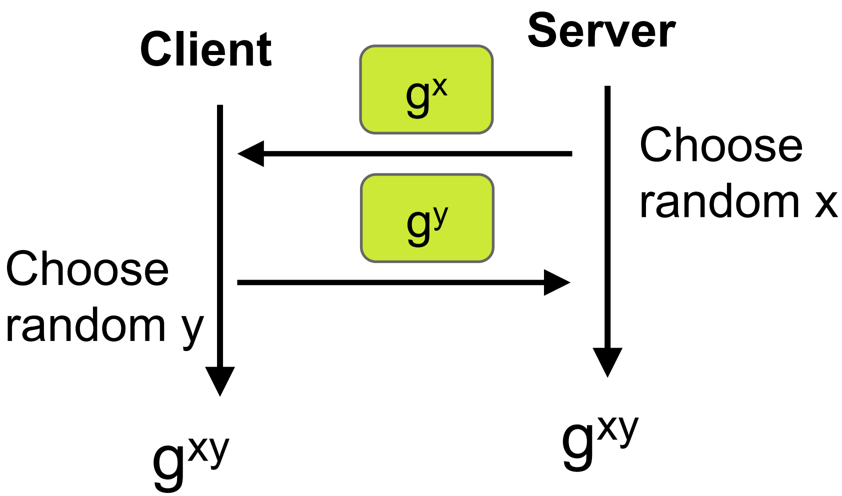
[LyubashevskyPR10]: "On Ideal Lattices and Learning with Errors Over Rings" EUROCRYPT 2010"

DH key agreement



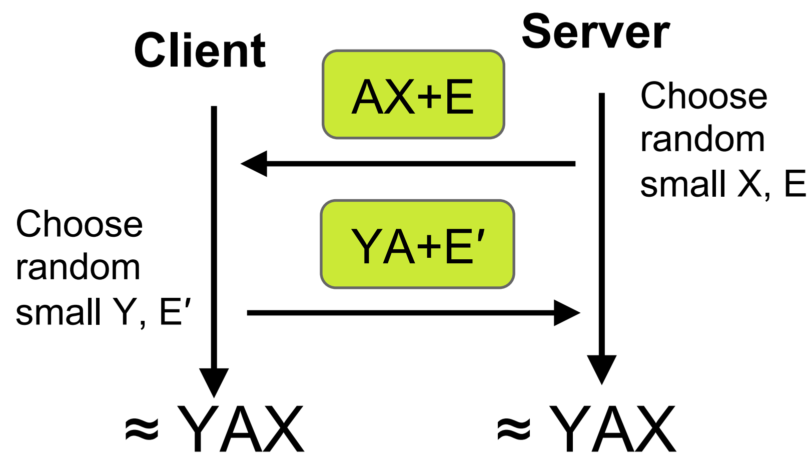
DH key agreement translates to (R)LWE

Diffie-Hellman key agreement



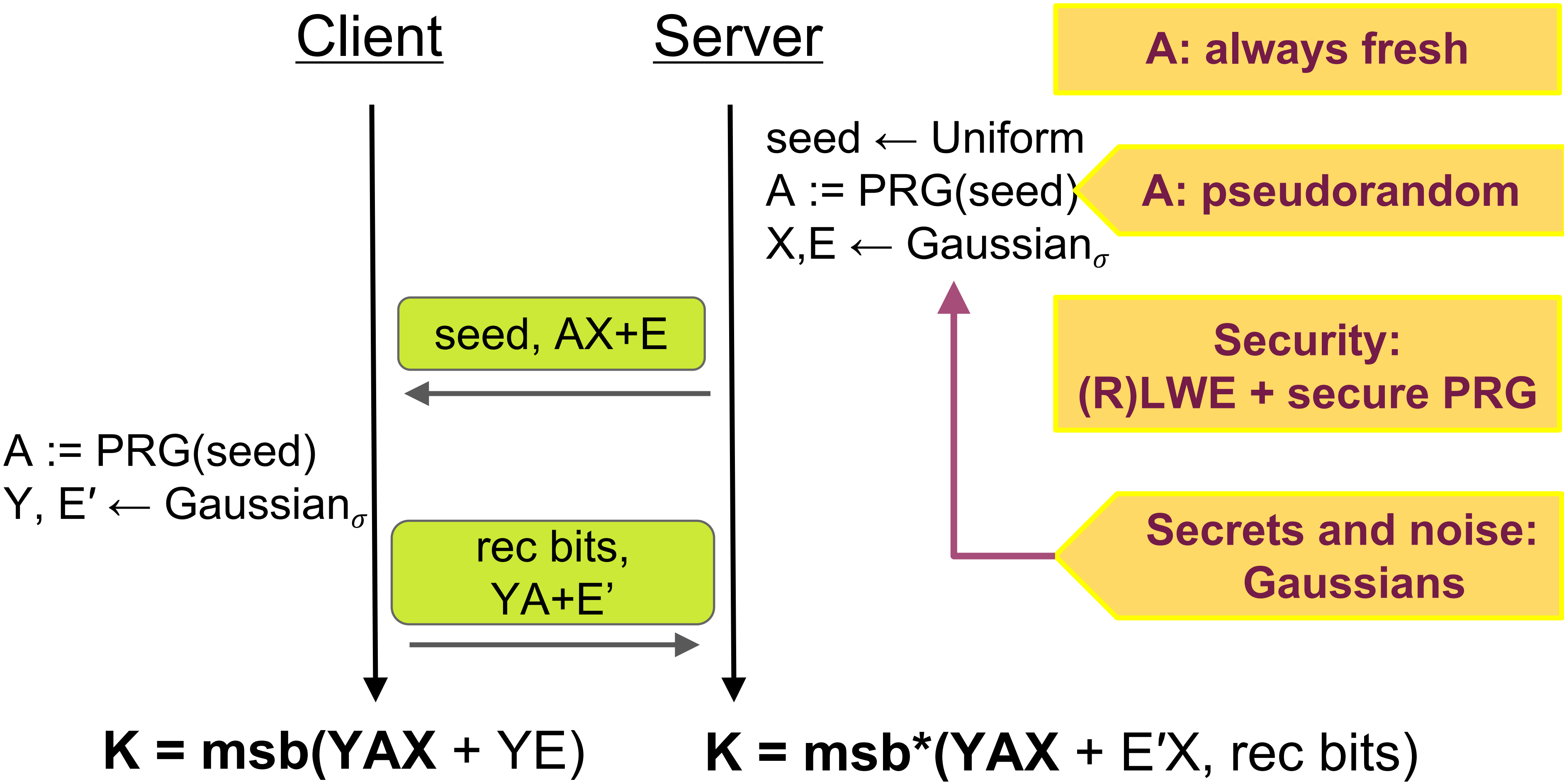
(g, g^x, g^y, g^{xy})
looks like
$(g, g^x, g^y, \text{random})$

(R)LWE key agreement



(A, AX+E, YA+E′, msb*(YAX))
looks like
(A, AX+E, YA+E′, random)

(R)LWE-based key agreement



History of (R)LWE

- [HoffsteinPS 96]: NTRU cryptosystem
- [AjtaiD 97]: First cryptosystem from GapSVP
- [Regev 05]: Introduce of LWE encryption
- [LyubashevskyPR 10]: Introduce ring-LWE encryption
- [DingXL 12]: Key agreement from LWE and ring-LWE
- [Peikert 14]: Improved ring-LWE key agreement
- [BosCNS 15]: Instantiated and implemented Peikert's key agreement in OpenSSL
- [AlkimDPS 16] ("NewHope"): Improved the performance of [BosCNS 15]
- [BosCDMNNRS 16] ("Frodo"): Key agreement from LWE, implementation, improvements, experiments

Ring-LWE cipher in Chrome Canary

LWE/RLWE: new foundation for key agreement

- (R)LWE considered to be **quantum resistant**
- (R)LWE has **worst- to average-case** reductions
- A new **(3rd) type** of assumption
  (RSA: factoring, DH: solving discrete logarithm)
- **Other crypto** primitives from (R)LWE
  (FHE, ABE, etc.)

“Frodo” vs. “New Hope”: relations to worst-case lattice problems

“Frodo”

Based on LWE

(matrices are random)

Gap-SVPγ $\leqq$ LWE $\leqq$ “Frodo”

“New Hope”

Based on Ring-LWE

(matrices are cyclic)

Ideal-SVPγ $\leqq$ Ring-LWE $\leqq$ “New Hope”

[Cramer Ducas Wesolowski’16]:
Recent quantum poly-time algorithm for sub-exponential γ.

“Frodo” vs. “New Hope”: relations to worst-case lattice problems

<u>“Frodo”</u>

Based on LWE

(matrices are random)

<u>“New Hope”</u>

Based on Ring-LWE

(matrices are cyclic)

Choosing parameters made simple

- modulus **q**
- dimension **n**
- **distribution** for small matrices

Search for (q, n, distribution) that minimizes communication and computation and

  - classical/quantum attacks run in $> 2^{128}$
  - failure probability $< 2^{-32}$
  - can extract a 256-bits key

“Frodo” vs. “NewHope”: parameters

“Frodo”

Based on LWE

Recommended parameters:

- $q = 2^{15}$
- $n = 752$
- failure probability: **2^{-36}**
- quantum security: **130** bits

“New Hope”

Based on Ring-LWE

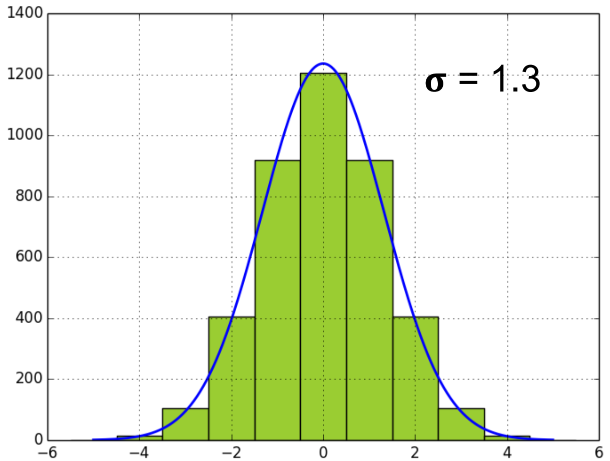
Recommended parameters:

- $q = 12289$ (13 bits prime)
- $n = 1024$
- failure probability: **2^{-60}**
- quantum security: **255** bits

"Frodo" vs. "NewHope": distributions

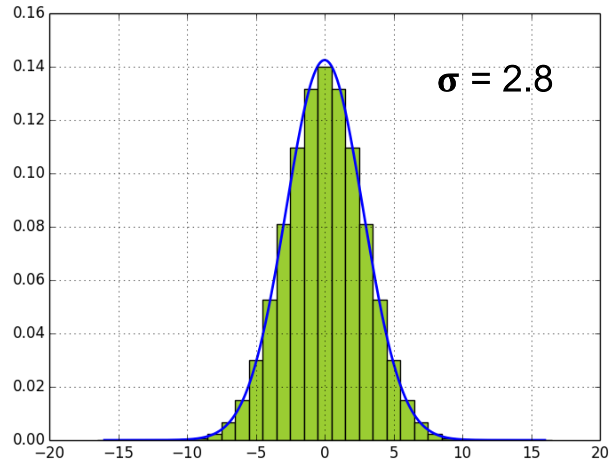
"Frodo"

- **Table distribution**
- Needs only 12 random bits per sample
- Scans the table of size 14 Bytes (constant time)



"New Hope"

- **Binomial distribution**
- Needs 32 random bits per sample
- Constant time



[BaiLLSS15]: techniques to substitute distributions

[BaiLLSS15] S. Bai, A. Langlois, T. Lepoint, D. Stehlé, and R. Steinfeld. Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. ASIACRYPT 2015

Implementation

- Constant time, pure C based on OQS framework[1]
- Compare:
  - RSA 3072
  - ECDHE nistp256
  - **all** available quantum resistant protocols
- New lattice ciphersuites in OpenSSL:

  (R)LWE_(RSA or ECDSA)_WITH_AES_256_GCM_SHA384

  (R)LWE_**ECDHE**_(RSA or ECDSA)_WITH_AES_256_GCM_SHA384

[1] Open Quantum Safe project by Michele Mosca and Douglas Stebila
openquantumsafe.org

Standalone performance of key agreement

Group		Speed → (ms)	Network ↔ (KiB)	Quantum security
Most widely used ciphers	RSA 3072	4	0.77	-
	ECDHE nistp256 (unoptimized)	0.7	0.06	-
Lattice based ciphers	NTRU EES743EP1	0.3–1.2	2.05	128
	New Hope (Ring-LWE)	0.2	3.87	255
	Frodo (LWE)	1.4	22.67	130
Others	SIDH	35–400	1.13	128
	McBits (McEliece)	0.5	360	161

First 6 rows: x86_64, 2.6GHz Intel Xeon E5 (Sandy Bridge) - Google n1-standard-4
McBits results from source paper [BCS13]

Comparison of lattice-based key agreements to ECDHE

	Speed →	Network ↔
ECDHE (unoptimized nistp256)	**0.7ms**	**0.06 KiB**
NTRU EES743EP1	**0.3–1.2ms**	**2.1 KiB**
NewHope (Ring-LWE)	**0.2ms**	**3.9 KiB**
Frodo (LWE)	**1.4ms**	**22.7 KiB**

Cert chain for https://www.google.com is **3KiB**

x86_64, 2.6GHz Intel Xeon E5 (Sandy Bridge) - Google n1-standard-4

Switching to Hybrids

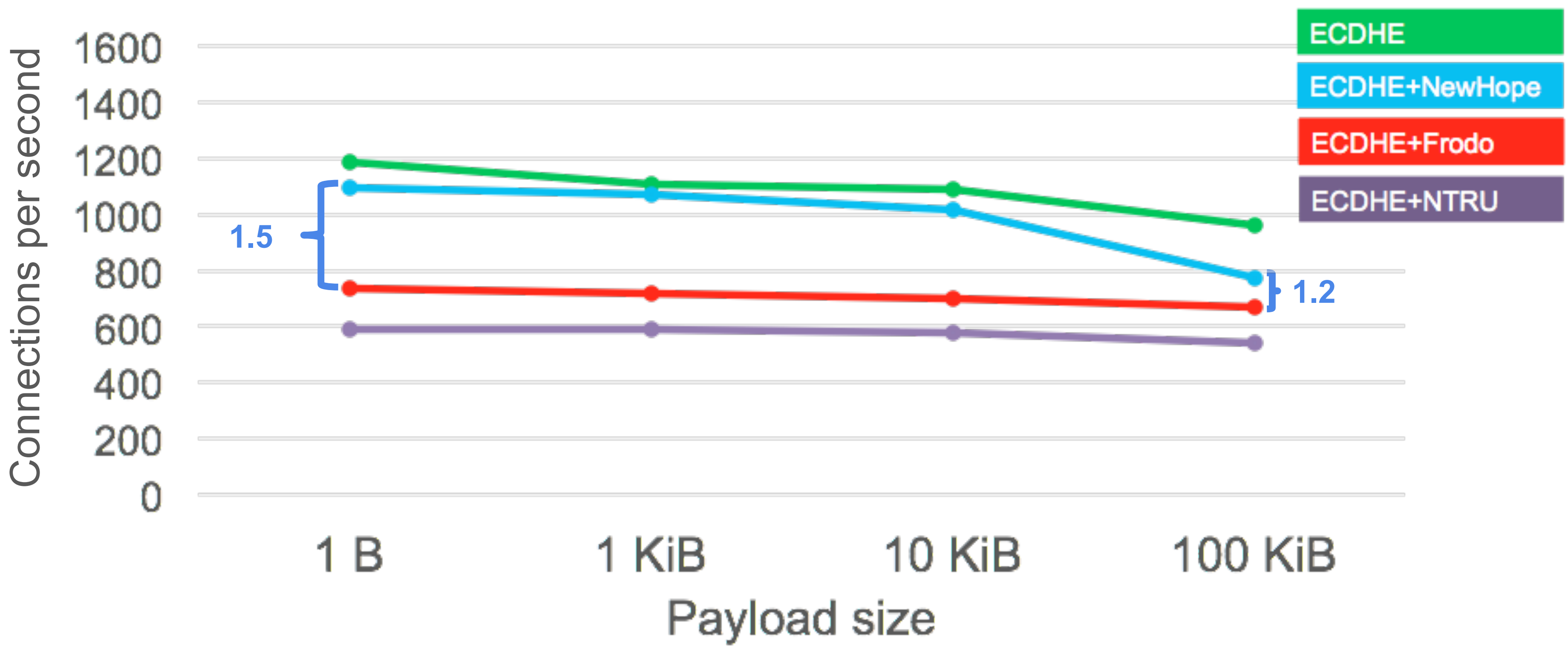
(R)LWE_**ECDHE**_(RSA or ECDSA)_WITH_AES_256_GCM_SHA384

- Use both post-quantum key-agreement and traditional key-agreement together
- Example:
  - ECDHE + NewHope

    Tested in Chrome Canary:

  - ECDHE + Frodo
- Session key is secure if at least one problem is hard

Throughput for TLS - hybrid (with ECDHE)



x86_64, 2.6GHz Intel Xeon E5 (Sandy Bridge) - Google n1-standard-4

Take-aways

- Candidate **key-agreement protocols** from LWE and Ring-LWE
- Implemented and integrated into **OpenSSL**
- New methods for **noise sampling**
- Tricks to **save communication**
- All code is **open source** (including scripts!):
  github.com/open-quantum-safe
  github.com/lwe-frodo
  github.com/tpoeppelmann/newhope
- Micro/macro **benchmarks:**
  the OQS framework [1] simplifies the benchmarks

[1] Open Quantum Safe project by Michele Mosca and Douglas Stebila
openquantumsafe.org

Thank you!

RLWE algebraic notation

$R_q = Z_q[x]/(x^n + 1)$

For a random $a \in R_q$, random small $s,e \in R_q$

$(a, as+e)$ looks like $(a, \text{random } r \in R_q)$

$$(a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + 1)$$

$$\times$$

$$(s_{n-1}x^{n-1} + s_{n-2}x^{n-2} + \ldots + 1)$$

$$+$$

$$(e_{n-1}x^{n-1} + e_{n-2}x^{n-2} + \ldots + 1)$$

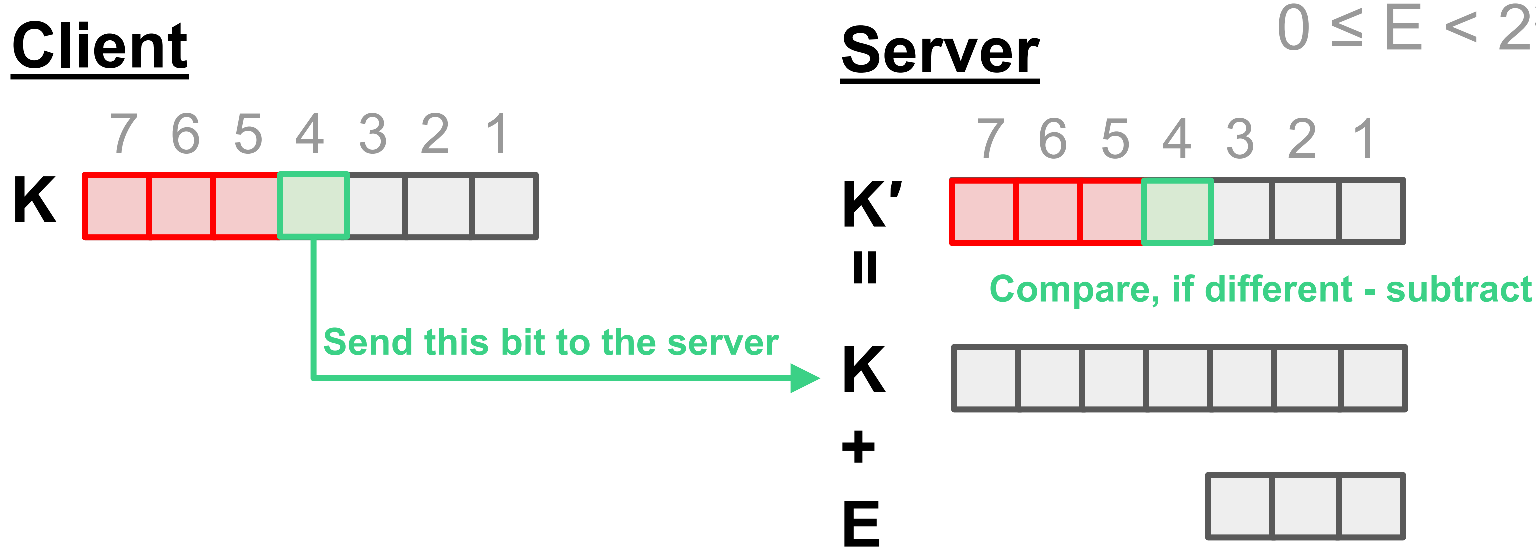
$$\approx r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \ldots + 1$$

mod x^n+1

"New Hope": $q = 12289$, $n = 1024$

Generalized rounding equalizes the keys

Toy example:
$q = 2^7$
$0 \leq E < 2^3$



TASK: derive a common key from K and K′, where E = K′ - K is small
SOLUTION: take the most significant bits

PROBLEM: they can be altered by the carry from E
FIX: make the client send an indicator bit*

* A generalized and simplified idea of [Pei14] C. Peikert. Lattice cryptography for the Internet. In Post-Quantum Cryptography. Springer, 2014.