Preparing for post-quantum and hybrid cryptography on the Internet

Douglas Stebila McMaster University

Funding acknowledgements:

NSERC CRSNG

University of Kent • Workshop on Quantum CyberSecurity • June 22, 2017

Motivation

Quantum CyberSecurity 2017

https://www.cs.kent.ac.uk/events/2017/qcs2017/program.html

QCS 2017
Workshop on Quantum CyberSecurity
22 – 23 June, 2017, Canterbury, UK

Home | Program | Registration | Venue | Organising Committee

Banner photography © Mark Wheadon

Program

Thursday 22 June

09:00 – 10:00 Registration, Tea and Coffee

Quantum CyberSecurity 2017

https://www.cs.kent.ac.uk/events/2017/qcs2017/program.html

Secure Connection

The connection is secure.

www.cs.kent.ac.uk

Hide details

First Visited: **No previous visits recorded**

Certificate: **www.cs.kent.ac.uk (QuoVadis Limited)**

Connection: **TLS 1.0 AES_128_CBC HMAC-SHA1 RSA**

QCS 2017
Workshop on Quantum CyberSecurity
22 – 23 June, 2017, Canterbury, UK

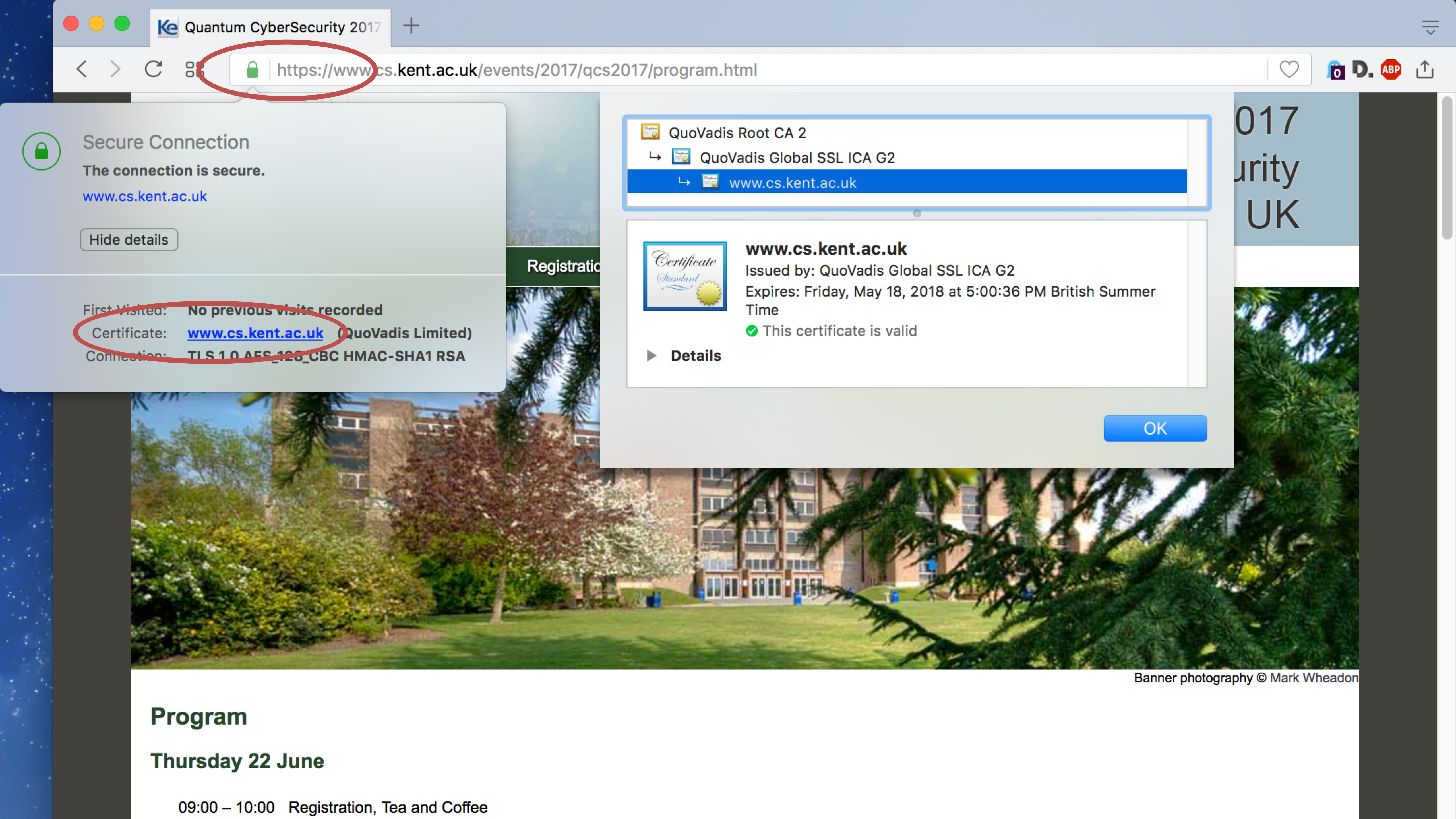
Registration | Venue | Organising Committee

Banner photography © Mark Wheadon

Program

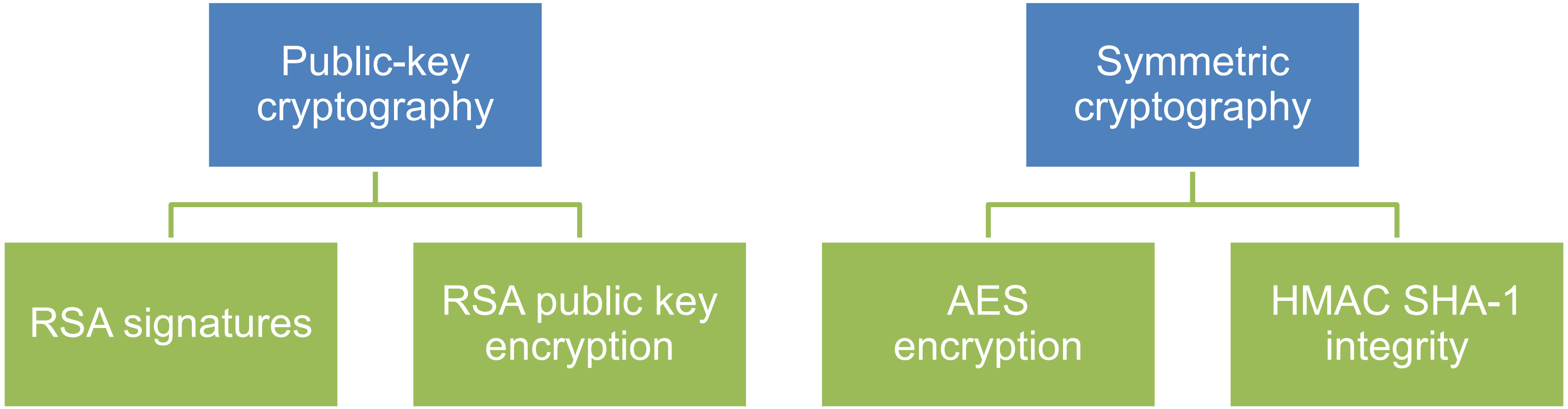
Thursday 22 June

09:00 – 10:00 Registration, Tea and Coffee


Quantum CyberSecurity 2017
https://www.cs.kent.ac.uk/events/2017/qcs2017/program.html
Secure Connection
The connection is secure.
www.cs.kent.ac.uk
Hide details
First Visited: No previous visits recorded
Certificate: www.cs.kent.ac.uk (QuoVadis Limited)
Connection: TLS 1.0 AES_128_CBC HMAC-SHA1 RSA
QuoVadis Root CA 2
QuoVadis Global SSL ICA G2
www.cs.kent.ac.uk
Certificate Standard
www.cs.kent.ac.uk
Issued by: QuoVadis Global SSL ICA G2
Expires: Friday, May 18, 2018 at 5:00:36 PM British Summer Time
This certificate is valid
Details
OK
Registratio
017
urity
UK
Banner photography © Mark Wheadon
Program
Thursday 22 June
09:00 – 10:00 Registration, Tea and Coffee

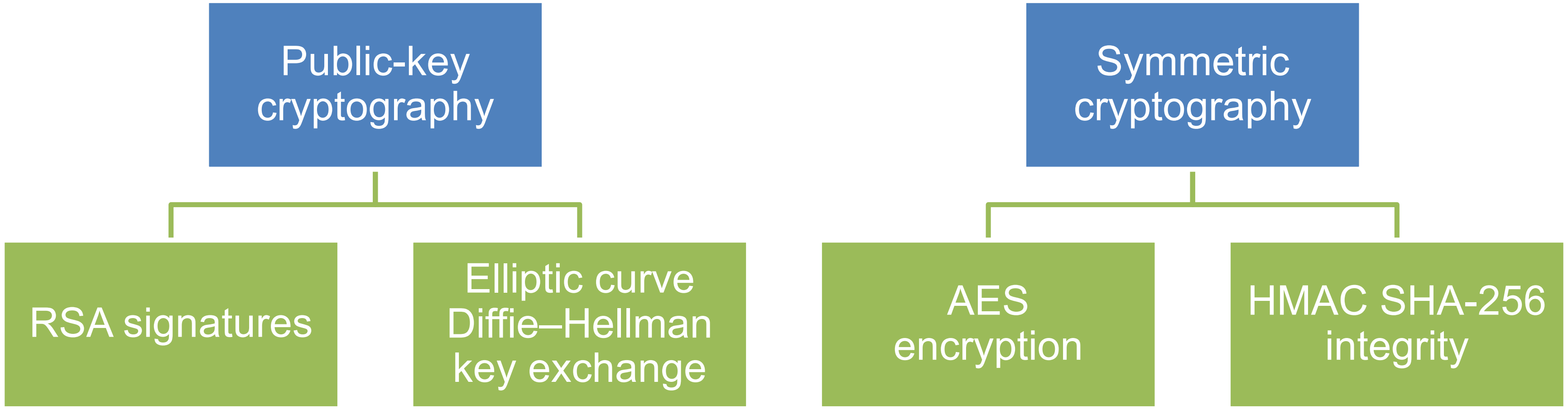
Contemporary cryptography

TLS 1.0 AES_128_CBC HMAC-SHA1 RSA

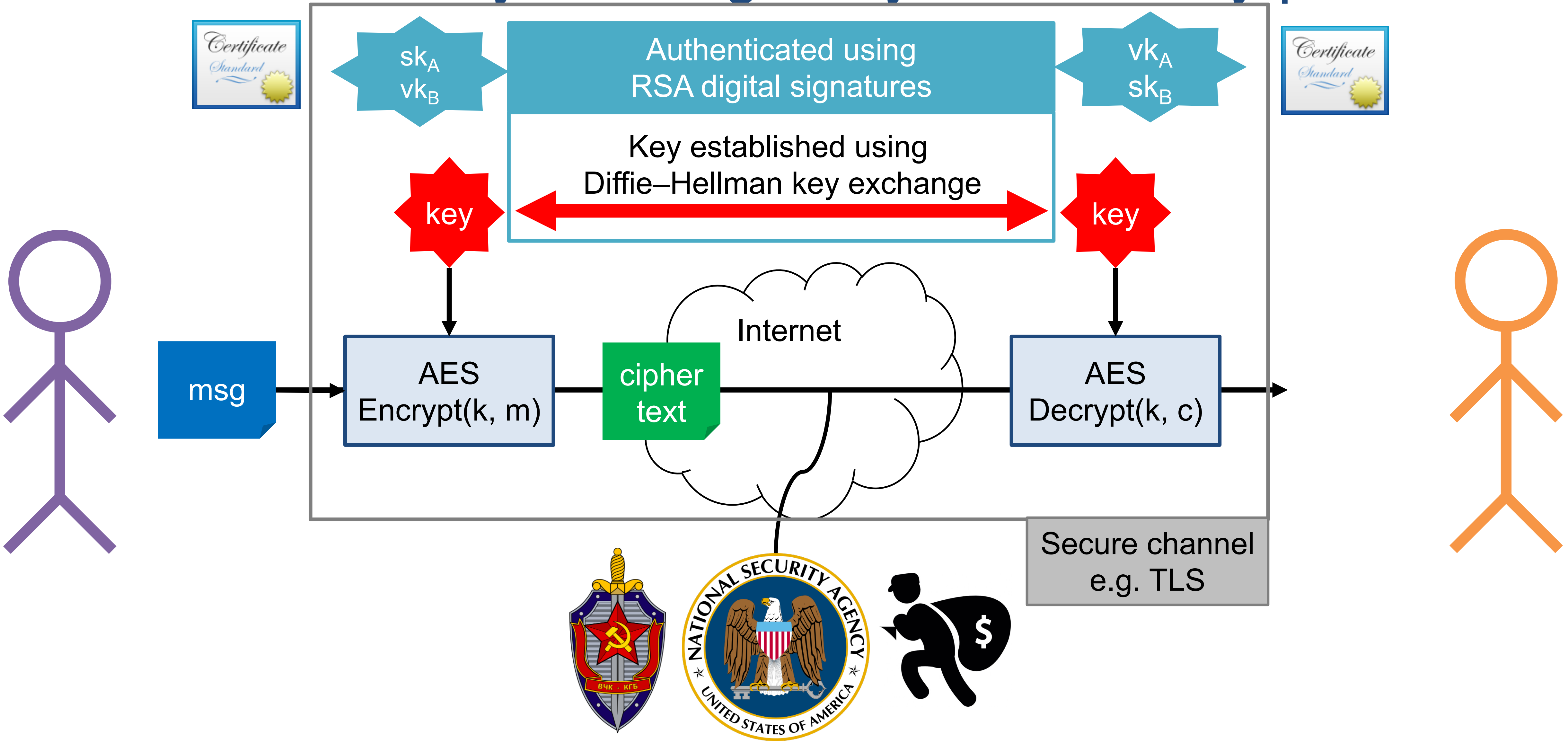


Contemporary cryptography

`TLS 1.2 AES_128_GCM HMAC-SHA256 RSA + ECDH`

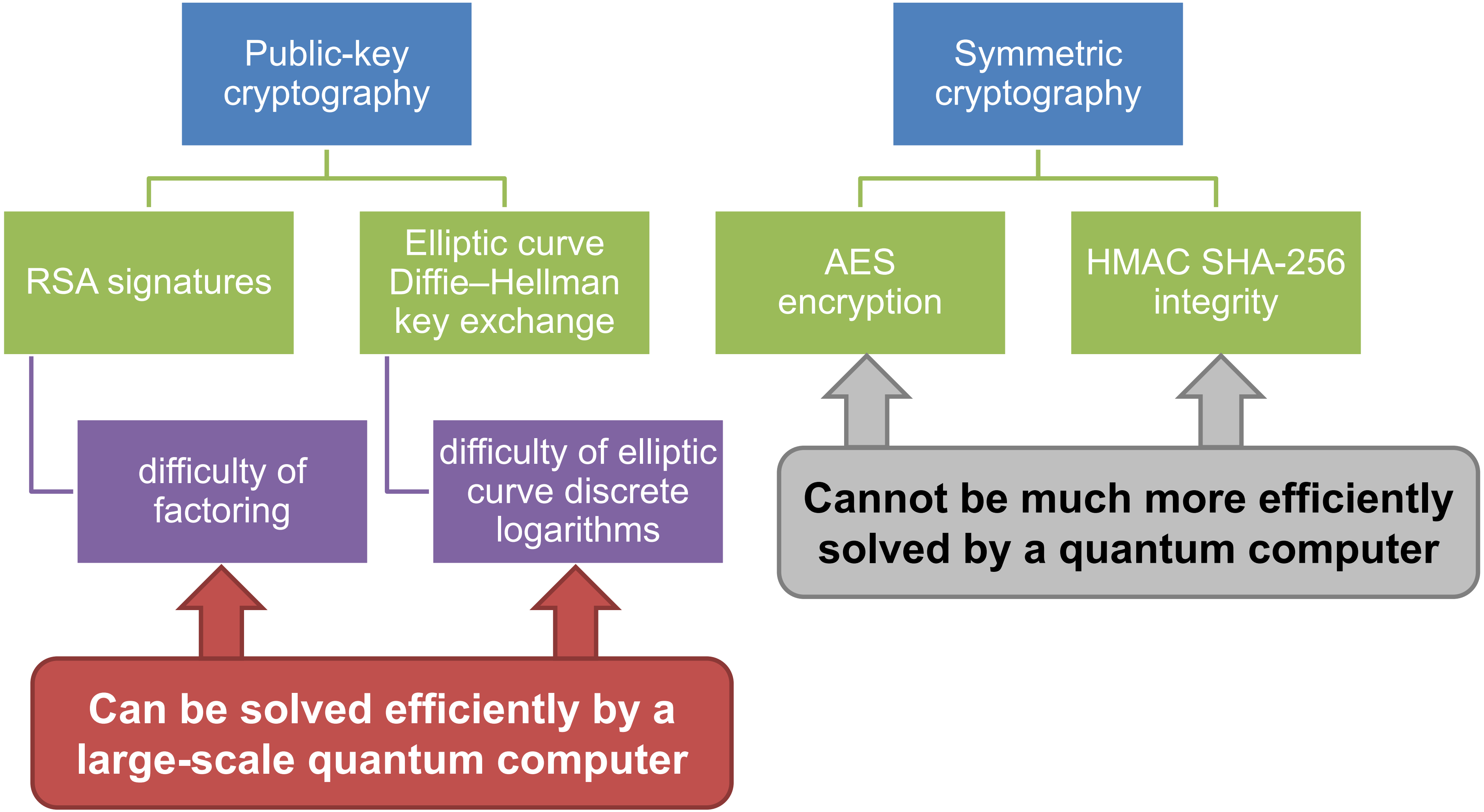


Authenticated key exchange + symmetric encryption

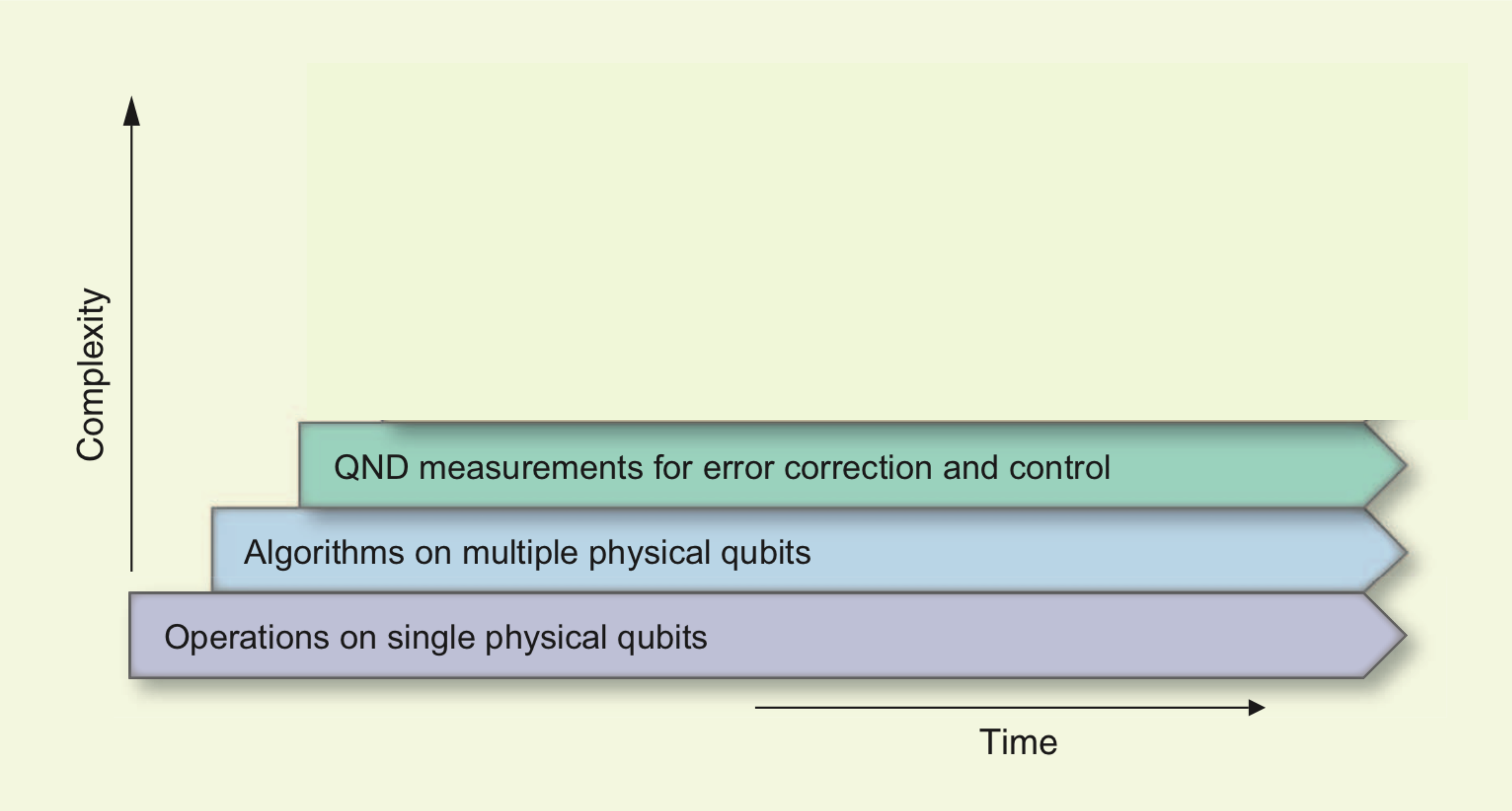


Contemporary cryptography

`TLS 1.2 AES_128_GCM HMAC-SHA256 RSA + ECDH`

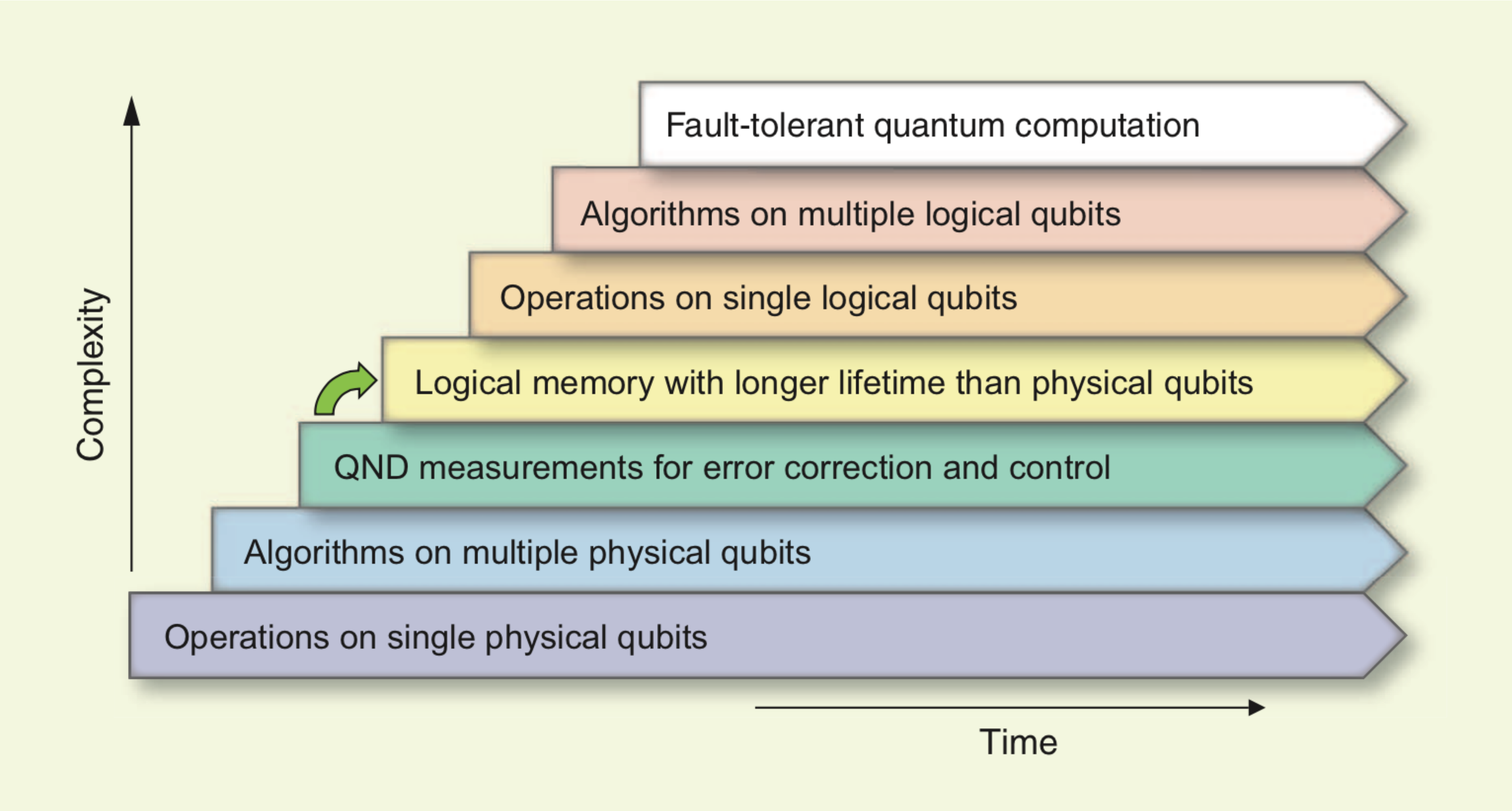


When will a large-scale quantum computer be built?



Devoret, Schoelkopf. *Science* 339:1169–1174, March 2013.

When will a large-scale quantum computer be built?



Devoret, Schoelkopf. *Science* 339:1169–1174, March 2013.

When will a large-scale quantum computer be built?

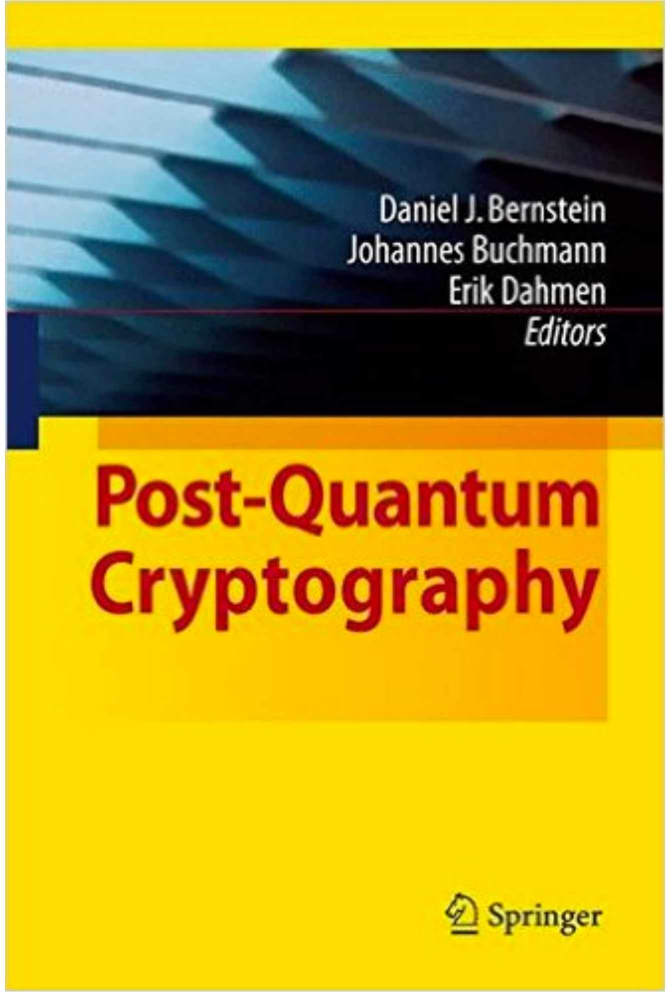
“I estimate a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031.”

— Michele Mosca, November 2015
https://eprint.iacr.org/2015/1075

Post-quantum cryptography in academia

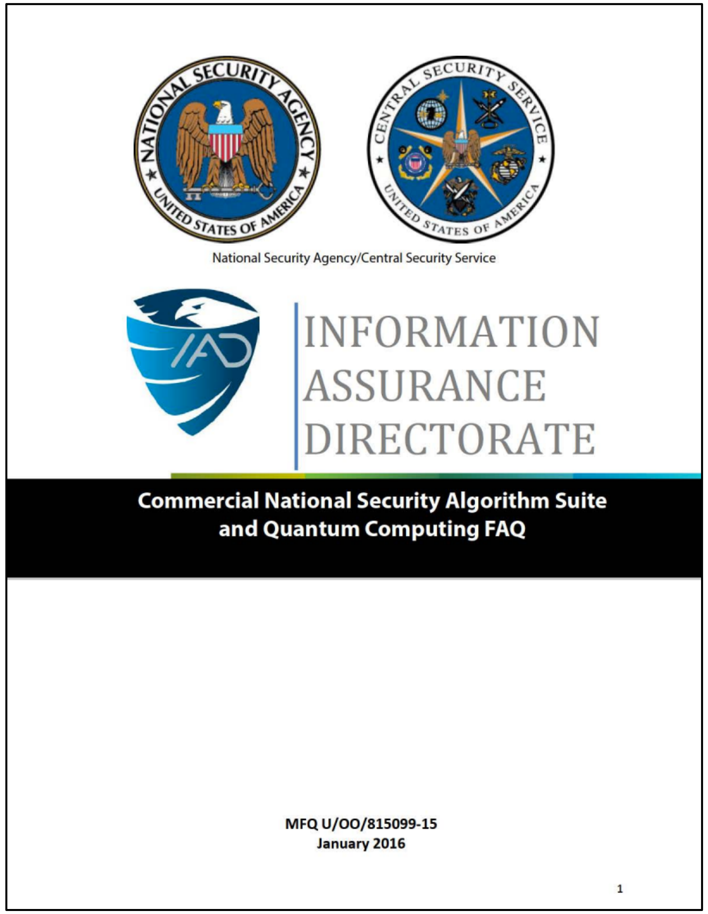
<u>Conference series</u>

- PQCrypto 2006
- PQCrypto 2008
- PQCrypto 2010
- PQCrypto 2011
- PQCrypto 2013
- PQCrypto 2014
- PQCrypto 2016
- PQCrypto 2017



2009

Post-quantum cryptography in government


National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

Commercial National Security Algorithm Suite and Quantum Computing FAQ

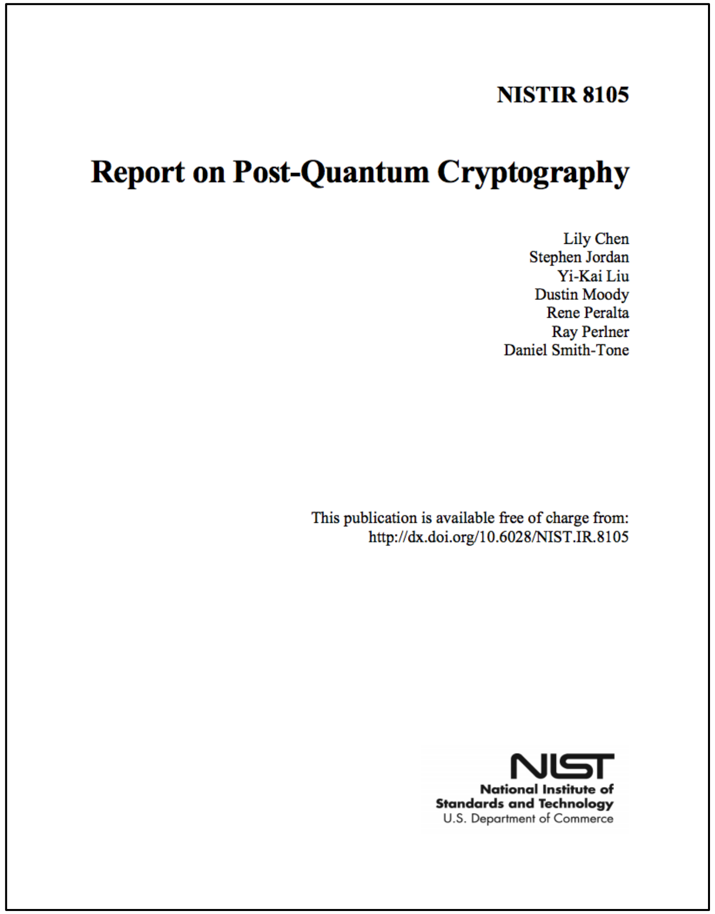
MFQ U/OO/815099-15
January 2016

1

Aug. 2015 (Jan. 2016)

"IAD will initiate a transition to quantum resistant algorithms in the not too distant future."

– NSA Information Assurance Directorate, Aug. 2015


NISTIR 8105

Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8105

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Apr. 2016

NIST Post-quantum Crypto Project timeline

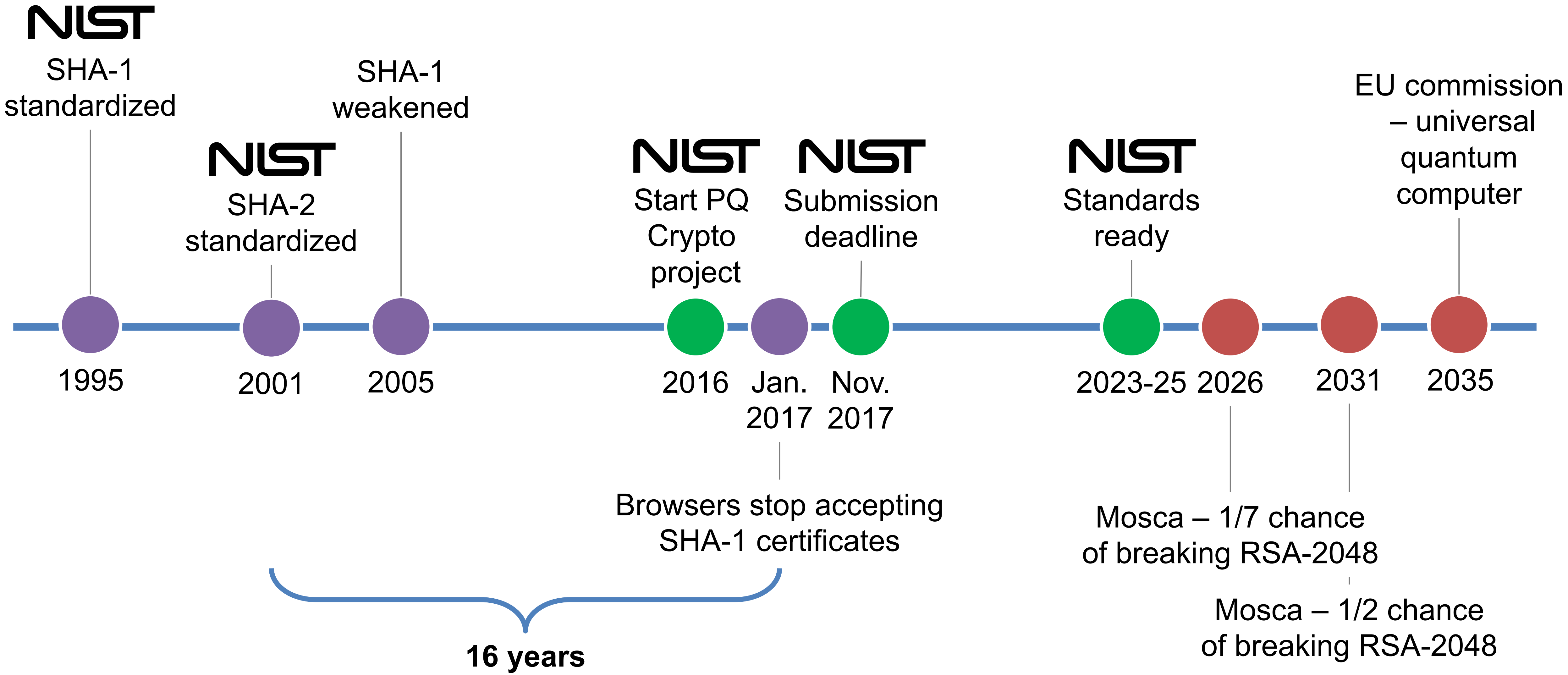
http://www.nist.gov/pqcrypto

December 2016	Formal call for proposals
November 2017	**Deadline for submissions**
3-5 years	Analysis phase
2 years later (2023-2025)	Draft standards ready

"**Our intention is to select a couple of options** for more immediate standardization, as well as to eliminate some submissions as unsuitable. … The goal of the process is **not primarily to pick a winner**, but to document the strengths and weaknesses of the different options, and to analyze the possible tradeoffs among them."

http://csrc.nist.gov/groups/ST/post-quantum-crypto/faq.html#Q7

Timeline


NIST
SHA-1 standardized
1995
NIST
SHA-2 standardized
2001
SHA-1 weakened
2005
NIST
Start PQ Crypto project
2016
Jan. 2017
Browsers stop accepting SHA-1 certificates
NIST
Submission deadline
Nov. 2017
NIST
Standards ready
2023-25
2026
Mosca – 1/7 chance of breaking RSA-2048
2031
Mosca – 1/2 chance of breaking RSA-2048
EU commission – universal quantum computer
2035
16 years

Post-quantum crypto

Post-quantum crypto

Classical crypto with no known exponential quantum speedup

Hash-based

- Merkle signatures
- Sphincs

Code-based

- McEliece

Multivariate

- multivariate quadratic

Lattice-based

- NTRU
- learning with errors
- ring-LWE

Isogenies

- supersingular elliptic curve isogenies

Quantum-safe crypto

Classical post-quantum crypto

Hash-based
- Merkle signatures
- Sphincs

Code-based
- McEliece

Multivariate
- multivariate quadratic

Lattice-based
- NTRU
- learning with errors
- ring-LWE

Isogenies
- supersingular elliptic curve isogenies

Quantum crypto

Quantum key distribution

Quantum channels

Quantum blind computation

Post-quantum crypto research agenda

- Design better post-quantum schemes
- Improve classical and quantum attacks
- Pick parameter sizes
- Develop fast, secure implementations
- Integrate them into the existing infrastructure

This talk

- Frodo
  - Key exchange protocol from the learning with errors problem
- Open Quantum Safe project
  - A library for comparing post-quantum primitives
  - Framework for easing integration into applications like OpenSSL
- Hybrid key exchange and digital signatures
  - In TLS
  - In X.509v3, S/MIME

Learning with errors problems

Solving systems of linear equations

$$\underbrace{\begin{bmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{bmatrix}}_{\mathbb{Z}_{13}^{7\times 4}} \times \underbrace{\begin{bmatrix} \\ \\ \\ \end{bmatrix}}_{\text{secret } \mathbb{Z}_{13}^{4\times 1}} = \underbrace{\begin{bmatrix} 4 \\ 8 \\ 1 \\ 10 \\ 4 \\ 12 \\ 9 \end{bmatrix}}_{\mathbb{Z}_{13}^{7\times 1}}$$

Linear system problem: given **blue**, find **red**

Solving systems of linear equations

$$\underbrace{\begin{bmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{bmatrix}}_{\mathbb{Z}_{13}^{7\times 4}} \times \underbrace{\begin{bmatrix} 6 \\ 9 \\ 11 \\ 11 \end{bmatrix}}_{\text{secret } \mathbb{Z}_{13}^{4\times 1}} = \underbrace{\begin{bmatrix} 4 \\ 8 \\ 1 \\ 10 \\ 4 \\ 12 \\ 9 \end{bmatrix}}_{\mathbb{Z}_{13}^{7\times 1}}$$

Easily solved using Gaussian elimination (Linear Algebra 101)

Linear system problem: given blue, find red

Learning with errors problem

$$
\begin{array}{ccccccc}
\textbf{random} & & \textbf{secret} & & \textbf{small noise} & & \\
\mathbb{Z}_{13}^{7\times 4} & & \mathbb{Z}_{13}^{4\times 1} & & \mathbb{Z}_{13}^{7\times 1} & & \mathbb{Z}_{13}^{7\times 1} \\
\begin{bmatrix}
4 & 1 & 11 & 10 \\
5 & 5 & 9 & 5 \\
3 & 9 & 0 & 10 \\
1 & 3 & 3 & 2 \\
12 & 7 & 3 & 4 \\
6 & 5 & 11 & 4 \\
3 & 3 & 5 & 0
\end{bmatrix}
& \times &
\begin{bmatrix}
6 \\ 9 \\ 11 \\ 11
\end{bmatrix}
& + &
\begin{bmatrix}
0 \\ -1 \\ 1 \\ 1 \\ 1 \\ 0 \\ -1
\end{bmatrix}
& = &
\begin{bmatrix}
4 \\ 7 \\ 2 \\ 11 \\ 5 \\ 12 \\ 8
\end{bmatrix}
\end{array}
$$

Learning with errors problem

$$\begin{array}{ccccccc}
\textbf{random} & & \textbf{secret} & & \textbf{small noise} & & \\
\mathbb{Z}_{13}^{7\times 4} & & \mathbb{Z}_{13}^{4\times 1} & & \mathbb{Z}_{13}^{7\times 1} & & \mathbb{Z}_{13}^{7\times 1} \\
\begin{bmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{bmatrix} & \times & \begin{bmatrix} \ \\ \ \\ \ \\ \ \end{bmatrix} & + & \begin{bmatrix} \ \\ \ \\ \ \\ \ \\ \ \\ \ \\ \ \end{bmatrix} & = & \begin{bmatrix} 4 \\ 7 \\ 2 \\ 11 \\ 5 \\ 12 \\ 8 \end{bmatrix}
\end{array}$$

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

Decision learning with errors problem

$$
\underset{\mathbb{Z}_{13}^{7\times 4}}{\textbf{random}}\;\begin{bmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{bmatrix} \times \underset{\mathbb{Z}_{13}^{4\times 1}}{\textbf{secret}}\begin{bmatrix} \, \\ \, \\ \, \\ \, \end{bmatrix} + \underset{\mathbb{Z}_{13}^{7\times 1}}{\textbf{small noise}}\begin{bmatrix} \, \\ \, \\ \, \\ \, \\ \, \\ \, \\ \, \end{bmatrix} = \underset{\mathbb{Z}_{13}^{7\times 1}}{\textbf{looks random}}\begin{bmatrix} 4 \\ 7 \\ 2 \\ 11 \\ 5 \\ 12 \\ 8 \end{bmatrix}
$$

Decision LWE problem: given **blue**, distinguish **green** from random

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

$\mathbb{Z}_{2^{15}}^{752\times 8}$

8

752

2738	3842	3345	2979	…
2896	595	3607		
377	1575			
2760				
…				

752 × 8 × 15 bits = **11 KiB**

Ring learning with errors problem

random

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

4	1	11	10
10	4	1	11
11	10	4	1
1	11	10	4
4	1	11	10
10	4	1	11
11	10	4	1

Each row is the cyclic shift of the row above

Ring learning with errors problem

random

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

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

Each row is the cyclic shift of the row above

…

with a special wrapping rule: *x* wraps to –*x* mod 13.

Ring learning with errors problem

random

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

4	**1**	**11**	**10**

Each row is the cyclic shift of the row above

…

with a special wrapping rule: *x* wraps to –*x* mod 13.

So I only need to tell you the first row.

Ring learning with errors problem

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

	$4 + 1x + 11x^2 + 10x^3$	**random**
×	$6 + 9x + 11x^2 + 11x^3$	**secret**
+	$0 - 1x + 1x^2 + 1x^3$	**small noise**
=	$10 + 5x + 10x^2 + 7x^3$	

Ring learning with errors problem

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

	$4 + 1x + 11x^2 + 10x^3$	**random**
×		**secret**
+		**small noise**
=	$10 + 5x + 10x^2 + 7x^3$	

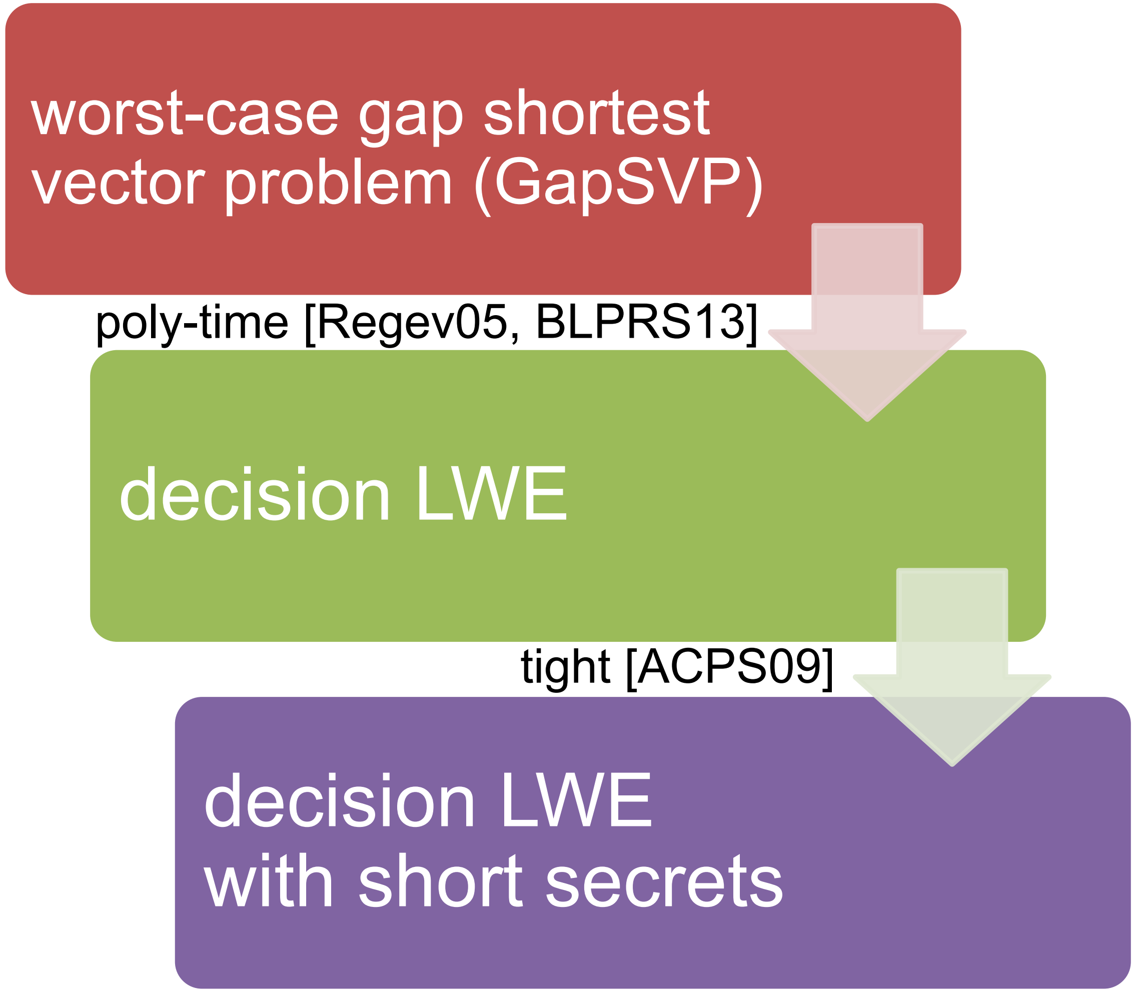
Computational ring-LWE problem: given **blue**, find **red**

Problems

Computational LWE problem	Decision LWE problem
Computational ring-LWE problem	Decision ring-LWE problem

with or without short secrets

Hardness of decision LWE



<u>Practice:</u>

- Assume the best way to solve DLWE is to solve LWE.
- Assume solving LWE involves a lattice reduction problem.
- Estimate parameters based on runtime of lattice reduction algorithms.
- (Ignore non-tightness.)

Key agreement from LWE

Bos, Costello, Ducas, Mironov, Naehrig, Nikolaenko, Raghunathan, Stebila.
Frodo: Take off the ring! Practical, quantum-safe key exchange from LWE.
ACM Conference on Computer and Communications Security (CCS) 2016.

https://eprint.iacr.org/2016/659

Basic LWE-DH key agreement (unauthenticated)

Based on Lindner–Peikert LWE public key encryption scheme

public: "big" A in $\mathbf{Z}_q^{n \times m}$

Alice

secret:
random "small" s, e in $\mathbf{Z}_q^m$

Bob

secret:
random "small" s', e' in $\mathbf{Z}_q^n$

$b = As + e$ →

← $b' = s'A + e'$

Alice shared secret:
$b's = s'As + e's \approx s'As$

Bob shared secret:
$s'b \approx s'As$

These are only approximately equal ⇒ need rounding

Parameters

“Recommended”

- 144-bit classical security, 130-bit quantum security, 103-bit plausible lower bound
- $n = 752$, $m = 8$, $q = 2^{15}$
- χ = approximation to rounded Gaussian with 11 elements
- Failure: $2^{-38.9}$
- Total communication: 22.6 KiB

“Paranoid”

- 177-bit classical security, 161-bit quantum security, 128-bit plausible lower bound
- $n = 864$, $m = 8$, $q = 2^{15}$
- χ = approximation to rounded Gaussian with 13 elements
- Failure: $2^{-33.8}$
- Total communication: 25.9 KiB

LWE and ring-LWE public key encryption and key exchange

Regev
STOC 2005
- Public key encryption from LWE

Lyubashevsky, Peikert, Regev
Eurocrypt 2010
- Public key encryption from ring-LWE

Lindner, Peikert
ePrint 2010, CT-RSA 2011
- Public key encryption from LWE and ring-LWE
- Approximate key exchange from LWE

Ding, Xie, Lin
ePrint 2012
- Key exchange from LWE and ring-LWE with single-bit reconciliation

Peikert
PQCrypto 2014
- Key encapsulation mechanism based on ring-LWE and variant single-bit reconciliation

Bos, Costello, Naehrig, Stebila
IEEE S&P 2015
- Implementation of Peikert's ring-LWE key exchange, testing in TLS 1.2

"NewHope"

Alkim, Ducas, Pöppelman, Schwabe.
USENIX Security 2016

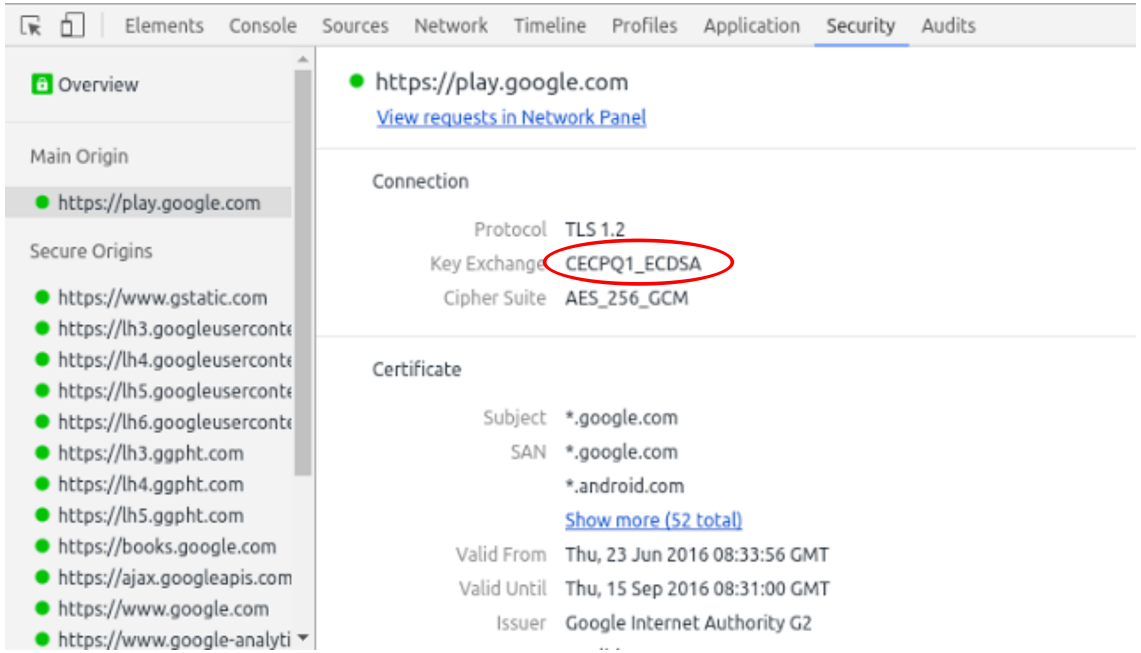
- New parameters
- Different error distribution
- Improved performance
- Pseudorandomly generated parameters

- Further performance improvements by others [GS16,LN16,AOPPS17,…]

Google Security Blog

Experimenting with Post-Quantum Cryptography

July 7, 2016



https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html

Ring-LWE

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

4	1	11	10

Cyclic structure

$\Rightarrow$ Save communication,
more efficient computation

4 KiB representation

LWE

$$\mathbb{Z}_{2^{15}}^{752\times 8}$$

$$752\left\{\overbrace{\begin{array}{ccccc} 2738 & 3842 & 3345 & 2979 & \ldots \\ 2896 & 595 & 3607 & & \\ 377 & 1575 & & & \\ 2760 & & & & \\ \ldots & & & & \end{array}}^{8}\right.$$

752 × 8 × 15 bits = **11 KiB**

Why consider (slower, bigger) LWE?

Generic vs. ideal lattices

- Ring-LWE matrices have additional structure
  - Relies on hardness of a problem in **ideal** lattices
- LWE matrices have no additional structure
  - Relies on hardness of a problem in **generic** lattices
- NTRU also relies on a problem in a type of ideal lattices

- Currently, best algorithms for ideal lattice problems are essentially the same as for generic lattices
  - Small constant factor improvement in some cases
  - Very recent quantum polynomial time algorithm for Ideal-SVP (http://eprint.iacr.org/2016/885) but not immediately applicable to ring-LWE

If we want to eliminate this additional structure, can we still get an efficient protocol?

Implementations

Our implementations

- Ring-LWE BCNS15
- LWE Frodo

Pure C implementations

Constant time

Compare with others

- RSA 3072-bit (OpenSSL 1.0.1f)
- ECDH `nistp256` (OpenSSL)

Use assembly code

- Ring-LWE NewHope
- NTRU `EES743EP1`
- SIDH (Isogenies) (MSR)

Pure C implementations

Post-quantum key exchange performance

	Speed		Communication	
RSA 3072-bit	Fast	4 ms	Small	0.3 KiB
ECDH `nistp256`	Very fast	0.7 ms	Very small	0.03 KiB
Code-based	Very fast	0.5 ms	Very large	360 KiB
NTRU	Very fast	0.3–1.2 ms	Medium	1 KiB
Ring-LWE	Very fast	0.2–1.5 ms	Medium	2–4 KiB
LWE	Fast	1.4 ms	Large	11 KiB
SIDH	Slow	35–400 ms	Small	0.5 KiB

See [Bos, Costello, Ducas, Mironov, Naehrig, Nikolaenko, Raghunathan, Stebila, ACM CCS 2016] for details/methodology

Post-quantum signature sizes

	Public key		Signature	
RSA 3072-bit	Small	0.3 KiB	Small	0.3 KiB
ECDSA `nistp256`	Very small	0.03 KiB	Very small	0.03 KiB
Hash-based (stateful)	Small	0.9 KiB	Medium	3.6 KiB
Hash-based (stateless)	Small	1 KiB	Large	32 KiB
Lattice-based (ignoring tightness)	Medium	1.5–8 KiB	Medium	3–9 KiB
Lattice-based (respecting tightness)	Very large	1330 KiB	Small	1.2 KiB
SIDH	Small	1.5 KiB	Very large	704 KiB

See [Bindel, Herath, McKague, Stebila PQCrypto 2017] for details

Open Quantum Safe

https://openquantumsafe.org/

Open Quantum Safe

- MIT-licensed open-source project on Github
  - https://openquantumsafe.org/
  - https://github.com/open-quantum-safe/

- liboqs: C language library, common API

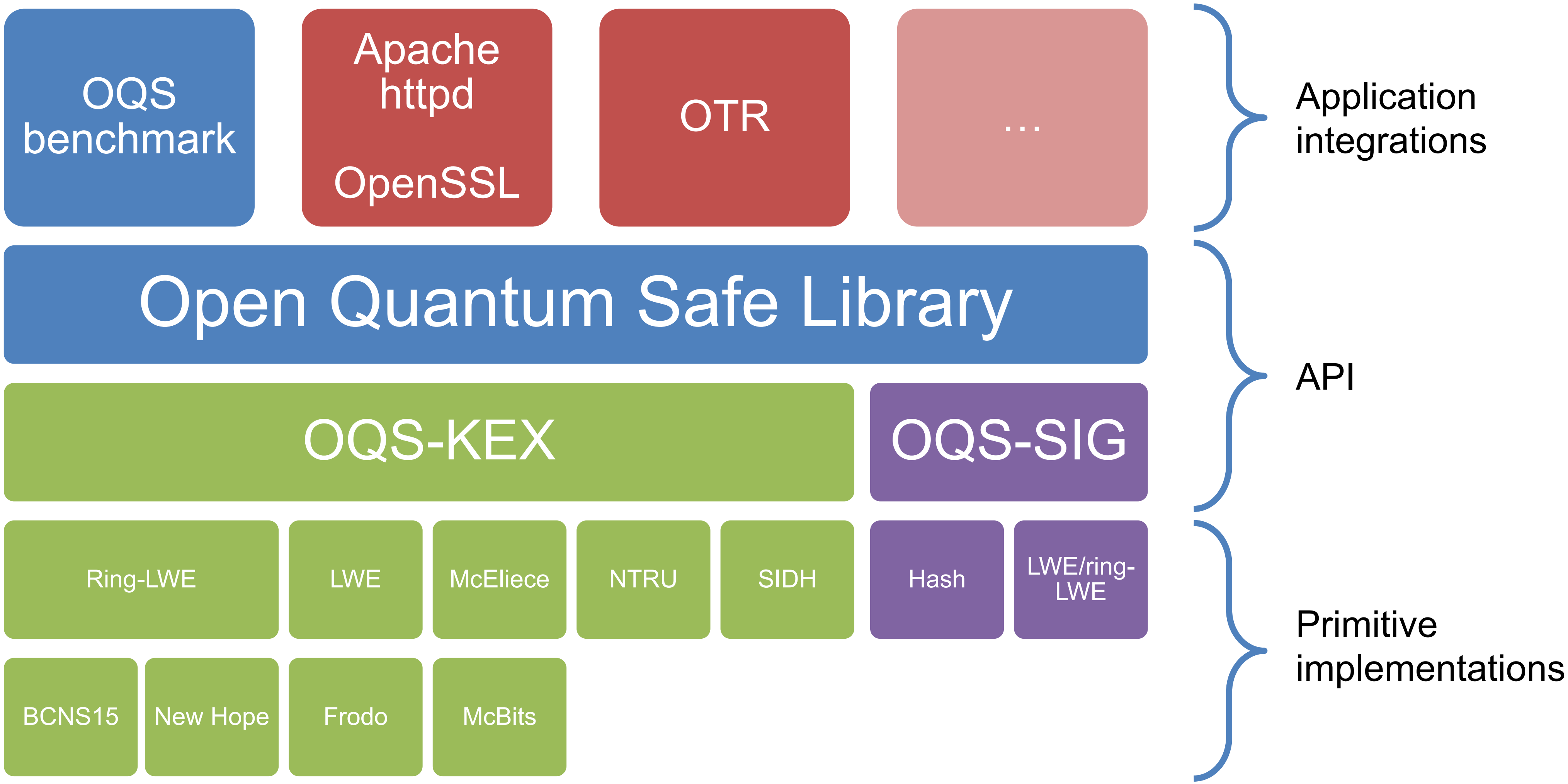
Open Quantum Safe

1. Collect post-quantum implementations together
    - Our own software
    - Thin wrappers around existing open source implementations
    - Contributions from others

2. Enable direct comparison of implementations

3. Support prototype integration into application level protocols
    - Don’t need to re-do integration for each new primitive – how we did Frodo experiments

Open Quantum Safe architecture



liboqs: Current key exchange algorithms

- **Ring-LWE**:
  - BCNS15
  - NewHope
  - MSR NewHope improvements
- **LWE**: Frodo
- **NTRU**
- **SIDH (Supersingular isogeny Diffie–Hellman)**:
  - MSR
  - IQC
- **Code**: McBits

liboqs: Benchmarking

- Built-in key exchange benchmarking suite
  - `./test_kex --bench`
- Gives cycle counts and ms runtimes

liboqs: Application integrations

OpenSSL v1.0.2:

- Ciphersuites using key exchange algorithms from liboqs
- Integrated into `openssl speed` benchmarking command and `s_client` and `s_server` command-line programs

- Track OpenSSL 1.0.2 stable with regular updates
  - https://github.com/open-quantum-safe/openssl

- Successfully used in Apache httpd and OpenVPN (with no modifications!)

OQC contributors and acknowledgements

Project leaders

- Michele Mosca and Douglas Stebila

Planning & discussions

- Scott Vanstone and Sherry Shannon Vanstone (Trustpoint)
- Matthew Campagna (Amazon Web Services)
- Alfred Menezes, Ian Goldberg, and Guang Gong (University of Waterloo)
- William Whyte and Zhenfei Zhang (Security Innovation)
- Jennifer Fernick, David Jao, and John Schanck (University of Waterloo)

Software contributors

- Mike Bender
- Tancrède Lepoint (SRI)
- Shravan Mishra (IQC)
- Christian Paquin (MSR)
- Alex Parent (IQC)
- Douglas Stebila (McMaster)
- Sebastian Verschoor (IQC)

+ Existing open-source code

Getting involved and using OQS

https://openquantumsafe.org/

If you're writing post-quantum implementations:

- We'd love to coordinate on API
- And include your software if you agree

If you want to prototype or evaluate post-quantum algorithms in applications:

- Maybe OQS will be helpful to you

We'd love help with:

- Code review and static analysis
- Signature scheme implementations
- Additional application-level integrations

Hybrid cryptography

Hybrid TLS: joint work with John Schanck

Hybrid signatures: joint work with Nina Bindel, Udyani Herath, Matthew McKague

Retroactive decryption

- A passive adversary that records today's communication can decrypt once they get a quantum computer
  - Not a problem for some people
  - Is a problem for other people

- How to provide potential post-quantum security to early adopters?

Hybrid ciphersuites

- Use pre-quantum and post-quantum algorithms together
- Secure if either one remains unbroken

Need to consider backward compatibility for non-hybrid-aware systems

Why hybrid?

- Potential post-quantum security for early adopters
- Maintain compliance with older standards (e.g. FIPS)
- Reduce risk from uncertainty on PQ assumptions/parameters

Hybrid ciphersuites

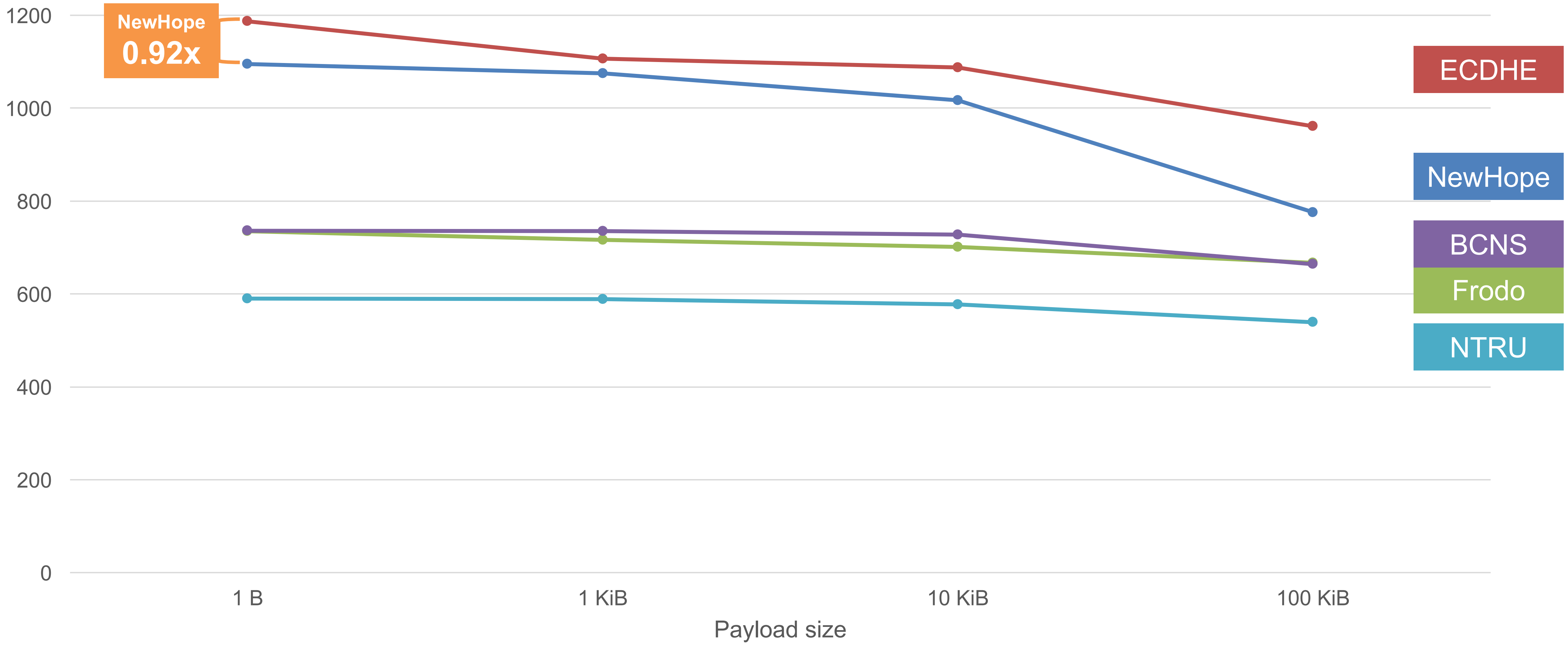
	Key exchange	Digital signature
1	Hybrid traditional + PQ	Single traditional
2	Hybrid traditional + PQ	Hybrid traditional + PQ
3	Single PQ	Single traditional
4	Single PQ	Single PQ

Likely focus
for next 10 years

TLS connection throughput – hybrid w/ECDHE

ECDSA signatures

bigger (top) is better



x86_64, 2.6 GHz Intel Xeon E5 (Sandy Bridge) – server Google `n1-standard-4`, client `-32`

Note somewhat incomparable security levels

Compatibility of large extensions in certs in TLS

	Extension size in KiB				
	1.5	3.5	9.0	43.0	1333.0
Libraries (library's command-line client talking to library's command-line server)					
GnuTLS 3.5.11	✓	✓	✓	✓	×
Java SE 1.8.0_131	✓	✓	✓	✓	✓
mbedTLS 2.4.2	✓	✓	✓	×	×
NSS 3.29.1	✓	✓	✓	✓	×
OpenSSL 1.0.2k	✓	✓	✓	✓	×
Web browsers (talking to OpenSSL's command-line server)					
Apple Safari 10.1 (12603.1.30.0.34)	✓	✓	✓	✓	✓
Google Chrome 58.0.3029.81	✓	✓	✓	✓	×
Microsoft Edge 38.14393.1066.0	✓	✓	✓	×	×
Microsoft IE 11.1066.14393.0	✓	✓	✓	×	×
Mozilla Firefox 53.0	✓	✓	✓	✓	×
Opera 44.0.2510.1218	✓	✓	✓	✓	×

[Bindel, Herath, McKague, Stebila, PQCrypto 2017]

Summary

Preparing for post-quantum and hybrid cryptography on the Internet

Douglas Stebila
McMaster University

- **Learning with Errors (LWE)** can achieve reasonable key sizes and runtime with more conservative assumption

- **Open Quantum Safe** project allows for prototyping and comparison on post-quantum algorithms

- **Hybrid cryptography** will probably play a role in the transition

LWE key exchange (Frodo)
- https://github.com/lwe-frodo
- https://eprint.iacr.org/2016/659

Open Quantum Safe
- https://openquantumsafe.org/
- https://eprint.iacr.org/2016/1017

Hybrid PKI
- https://eprint.iacr.org/2017/460