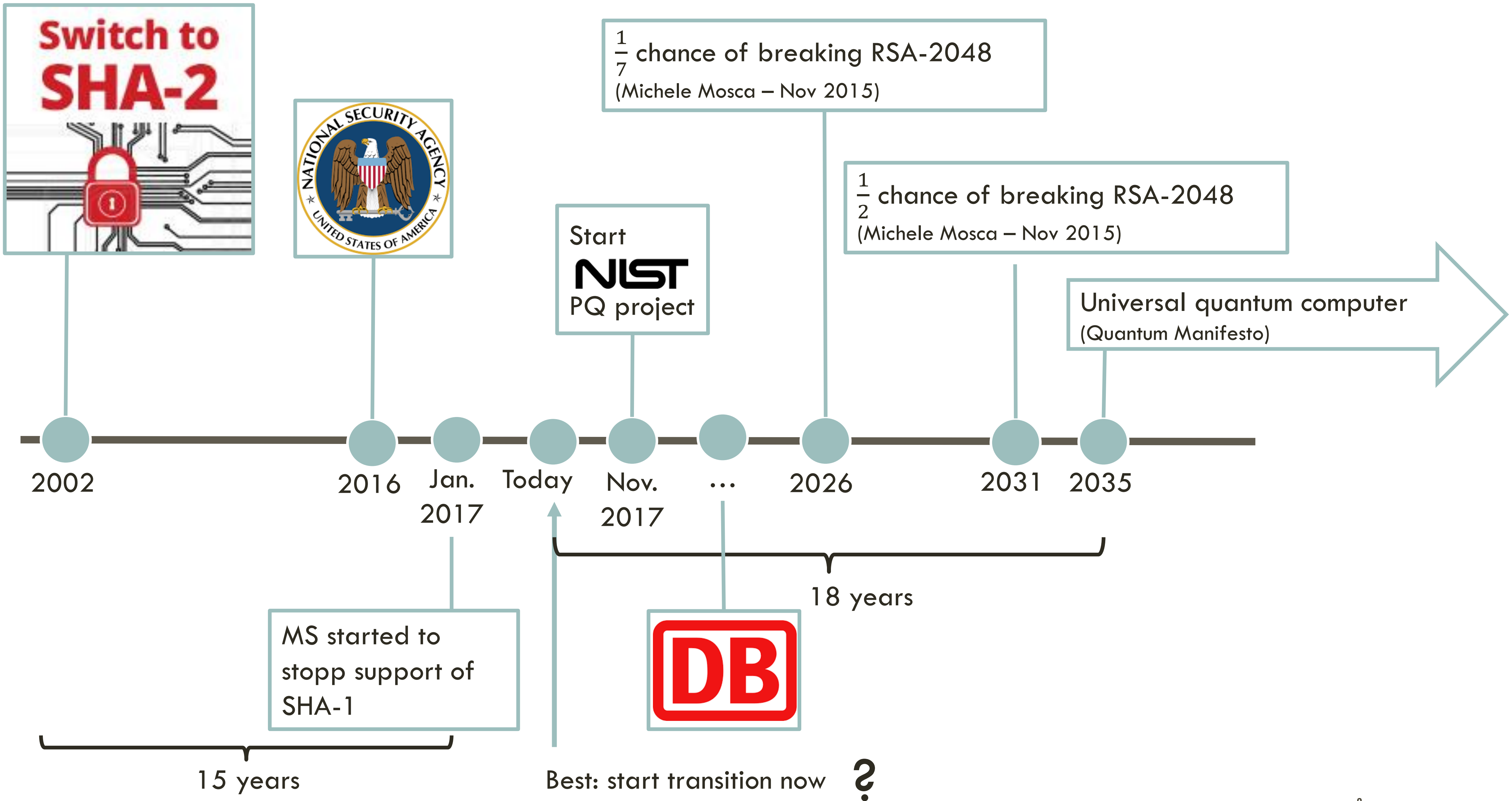
TRANSITIONING TO A QUANTUM-RESISTENT PUBLIC KEY INFRASTRUCTURE

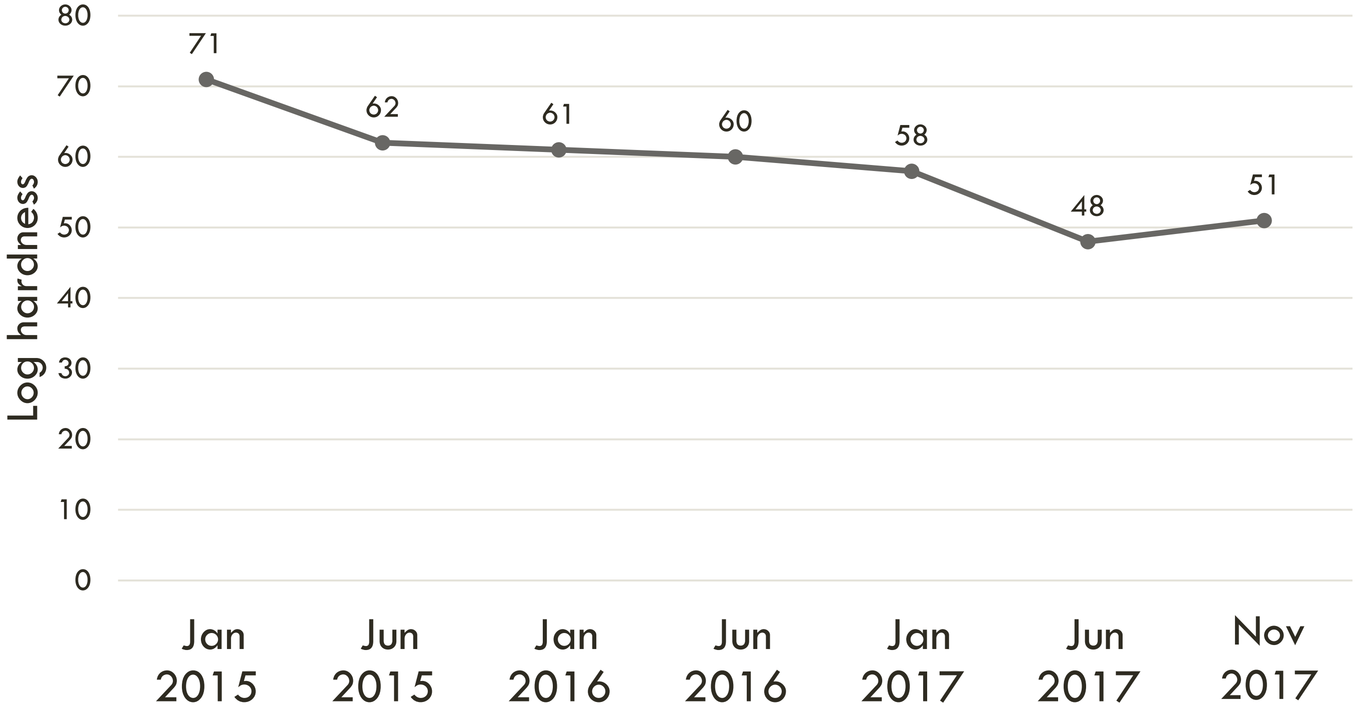
Cryptography for the IoT+Cloud
Bochum, Germany
11/06/2017

Nina Bindel
Udyani Herath
Matthew McKague
Douglas Stebila

TECHNISCHE UNIVERSITÄT DARMSTADT
CROSSING
QUT Queensland University of Technology
McMaster University


Switch to SHA-2
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
Start
NIST
PQ project
$\frac{1}{7}$ chance of breaking RSA-2048
(Michele Mosca – Nov 2015)
$\frac{1}{2}$ chance of breaking RSA-2048
(Michele Mosca – Nov 2015)
Universal quantum computer
(Quantum Manifesto)
2002
2016
Jan. 2017
Today
Nov. 2017
…
2026
2031
2035
18 years
MS started to stopp support of SHA-1
DB
15 years
Best: start transition now ?

BIT-HARDNESS ESTIMATIONS WITH LWE-ESTIMATOR [APS15]



Difference of ~20 bit in 2.5 years

LWE Instance - Regev(128)
$n=128$, $q=16411$, $\sigma=29.6$

CURRENT SITUATION

Quantum threat against RSA- and discrete log

Unstable hardness estimations of “PQ assumptions“

NOT ENOUGH TO CARE ABOUT THE PRIMITIVES…

CHALLENGES DURING TRANSITION

- Security
- Compatibility

HYBRID SIGNATURE SCHEMES

Given: Σ_1 and Σ_2
Construct: Σ_C s.t. Σ_C is secure if Σ_1 or Σ_2 secure

Example:

- Σ_1 PQ scheme and Σ_2 classical scheme
- 2 PQ schemes based on different assumptions

Q

- What means “secure“ ?
- How to construct Σ_C ?
- Can we use hybrids in current protocols and standards?

SECURITY DEFINITION

Intuition:

- eUF-CMA with 2-stage adversary $\mathrm{A} = (A_1, A_2)$
- A_1, A_2 different access to quantum computer
- A_1 classical/quantum access to sign oracle

$\mathrm{EXPT}_{\Sigma}^{\mathrm{EUF-CMA}}(A)$:

$q_s \leftarrow 0$

$(sk, vk) \leftarrow \Sigma.\mathrm{KeyGen}()$

$(m_1, \sigma_1), \dots, (m_{q_s+1}, \sigma_{q_s+1}) \leftarrow A(vk)$

$A(vk) \leftrightarrow O_S()$: $q_s \leftarrow q_s + 1$

If $\Sigma.\mathrm{Verify}(vk, m_i, \sigma_i) = 1$

Return 1

Else

Return 0

$\mathrm{EXPT}_{\Sigma}^{\mathrm{EUF-CMA}}(A_1, A_2)$:

$q_s \leftarrow 0$

$(sk, vk) \leftarrow \Sigma.\mathrm{KeyGen}()$

$st \leftarrow A_1(vk)$

$(m_1, \sigma_1), \ldots, (m_{q_s+1}, \sigma_{q_s+1}) \leftarrow A_2(st)$

If $\Sigma.\mathrm{Verify}(vk, m_i, \sigma_i) = 1$

    Return 1

Else

    Return 0

$O_S()$

$q_s \leftarrow q_s + 1$

010…1/ ?

010…1/ ?

010…1/ ?

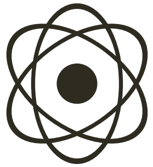
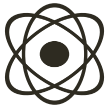
ADVERSARY MODEL

$\mathbf{C^cC}$ - Fully classical (eUF-CMA)

$\mathbf{C^cQ}$ - Future quantum

$\mathbf{Q^cQ}$ - Quantum adversary

$\mathbf{Q^qQ}$ - Fully quantum (also in [BZ13]) $\longleftarrow$

- A_1: 
- A_2:
- Access O_S: 

THEOREM

$$
\begin{tikzcd}
\mathbf{Q^qQ} \arrow[r, bend left] & \mathbf{Q^cQ} \arrow[l, bend left, "/" marking] \arrow[r, bend left] & \mathbf{C^cQ} \arrow[l, bend left, "/" marking] \arrow[r, bend left] & \mathbf{C^cC} \arrow[l, bend left, "/" marking]
\end{tikzcd}
$$

EXAMPLES OF HYBRID SIGNATURES

Σ_1 X^yZ-secure
Σ_2 U^vW-secure

Combiner	$\boldsymbol{\sigma = (\sigma_1, \sigma_2)}$	Unforgeability	Non-separability
$C_{\|\|}$	$\sigma_1 \leftarrow \mathrm{Sign}_1(m)$ $\sigma_2 \leftarrow \mathrm{Sign}_2(m)$	max$\{X^yZ, U^vW\}$	No
C_{nest}	$\sigma_1 \leftarrow \mathrm{Sign}_1(m)$ $\sigma_2 \leftarrow \mathrm{Sign}_2(m, \sigma_1)$	max$\{X^yZ, U^vW\}$	Depending on U^vW
$C_{dual-nest}$	$\sigma_1 \leftarrow \mathrm{Sign}_1(m_1)$ $\sigma_2 \leftarrow \mathrm{Sign}_2(m_1, \sigma_1, m_2)$	X^yZ wrt to m_1, U^vW	Depending on U^vW

APPLICABLE TO CURRENT PKI?

- Certificates: X.509v3
- Secure channels: TLS (not in this talk)
- Secure email: S/MIME

Q

(1) How can hybrid combiners be used in current standards?

(2) What about backwards-compatibility?

(3) Do large key and siganture size raise problems?

HYBRID SIGNATURE IN S/MIME EMAIL

Idea:

- Use concatenation combiner
- S/MIME data structures allow multiple parallel signatures
- Disadvantage: Verification of all signatures

  → backwards-compatibility?

2nd Idea:

- Use nested combiner
- Use optional attributes

HYBRID SIGNATURES IN X.509V3 CERT

Idea:

- Use dual nested combiner
- **PQ** cert **=** extension of **RSA** cert
- Hybrid software recognizes and processes PQ cert **and** RSA cert
- Older softeware ignores non-critical ext.

$$(sk_{PQ}^{CA}, vk_{PQ}^{CA}), (sk_{RSA}^{CA}, vk_{RSA}^{CA}) \leftarrow \mathrm{KeyGen}_{dual-nest}$$

$$(sk_{PQ}^{Sub}, vk_{PQ}^{Sub}), (sk_{RSA}^{Sub}, vk_{RSA}^{Sub}) \leftarrow \mathrm{KeyGen}_{dual-nest}$$

Certificate c_2 (RSA)

tbsCertificate m_2:

CA, subject, vk_{RSA}^{Sub}

$c_2 = \mathrm{Sign}_{RSA}(sk_{RSA}^{CA}, (m_2, vk_{RSA}^{Sub}, c_1, m_1))$

Extensions:

Ext. id. = non-critical

Certificate c_1 (PQ)

tbsCertificate m_1:

CA, subject, vk_{PQ}^{Sub}

$c_1 = \mathrm{Sign}_{PQ}(sk_{PQ}^{CA}, (m_1, vk_{PQ}^{Sub}))$

COMPATIBILITY OF HYBRID X.509V3 CERTS

	Application	Extension size [KB]				
		1.5	3.5	9.0	43.0	1333.0
Libraries	GnuTLS	✓	✓	✓	✓	✗
	Java SE	✓	✓	✓	✓	✓
	mbedTLS	✓	✓	✓	✗	✗
	NSS	✓	✓	✓	✓	✗
	OpenSSL	✓	✓	✓	✓	✗
Web browsers	Apple Safari	✓	✓	✓	✓	✓
	Google Chrome	✓	✓	✓	✓	✗
	MS Edge	✓	✓	✓	✗	✗
	MS IE	✓	✓	✓	✗	✗
	Mozilla Firefox	✓	✓	✓	✓	✗
	Opera	✓	✓	✓	✓	✗

SUMMARY

- 2-stage adversary
- Adversary model wrt quantum power
- Construction hybrid signatures
- Compatibility of with current PKI:
  - Nested single message in S/MIME
  - Nested dual message in X.509 cert

IACR ePrint Archive: Report 2017/460

OPEN QUESTIONS

- Our combiners used in PKI still either secure **or** compatible
  - Better combiners/application in PKI ?
  - Change protocols ?
  - No compatibility ?
- Define other hybrids (work in progress)

TECHNISCHE UNIVERSITÄT DARMSTADT

CROSSING

THANKS