Quantum Safety In Certified Cryptographic Modules

William Whyte, Lee Wilson

NTRU

SECURITY INNOVATION

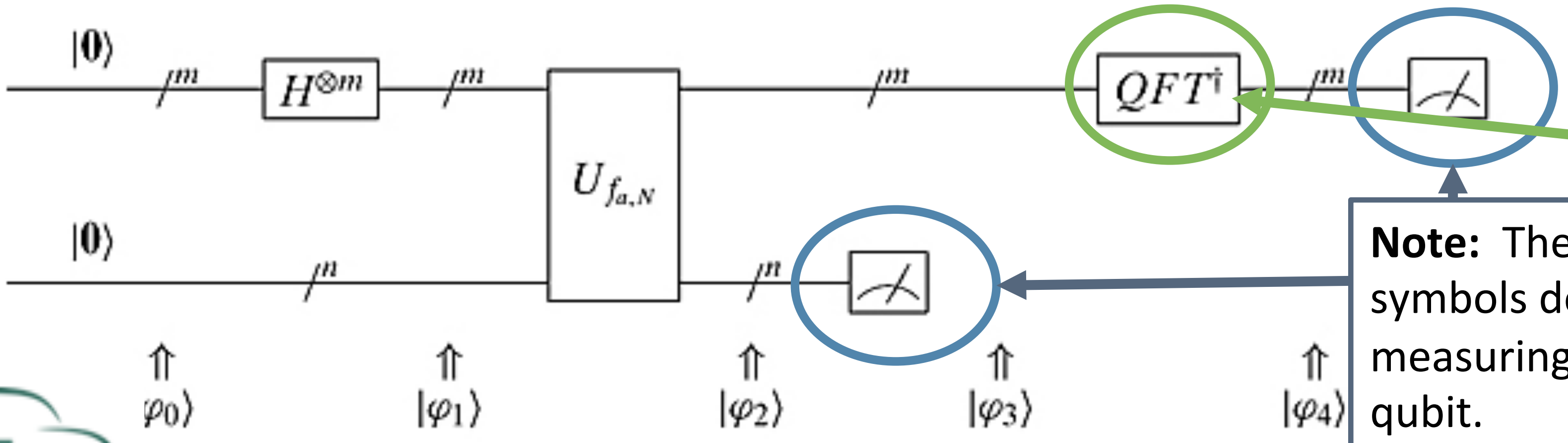
What’s Causing All the Fuss? Shor’s Algorithm

(From Quantum Computing for Computer Scientists by Noson Yanofsky and Mirco Mannucci)

Input: A positive integer N with n = [log2 N].

Output: A factor p of N if it exists.

1. Use a polynomial algorithm to determine if N is prime or a power of prime. If it is a prime, declare that it is and exit. If it is a power of a prime number, declare that it is and exit.
2. Randomly choose an integer a such that 1 < a < N. Perform Euclid’s algorithm to determine GCD(a, N). If the GCD is not 1, then return it and exit.
3. Use the quantum circuit below to find a period r.
4. If r is odd or if $a^r \equiv -1$ Mod N, then return to #2 and choose another a.
5. Use Euclid’s algorithm to calculate GCD(($a \uparrow r/2$ +1),N) and GCD(($a \uparrow r/2$ $-$1),N) . Return at least one of the nontrivial solutions.



$|0\rangle$
$/^m$
$H^{\otimes m}$
$/^m$
$U_{f_{a,N}}$
$/^m$
$QFT^\dagger$
$/^m$
$|0\rangle$
$/^n$
$/^n$
$\Uparrow$ $\varphi_0\rangle$
$\Uparrow$ $|\varphi_1\rangle$
$\Uparrow$ $|\varphi_2\rangle$
$\Uparrow$ $|\varphi_3\rangle$
$\Uparrow$ $|\varphi_4\rangle$

Note: These gate symbols denote measuring the qubit.

Note: The QFT is a “Quantum Fourier Transform” gate.

Insights from "Cybersecurity in an era with quantum computers: will we be ready?" – 5 Main Points

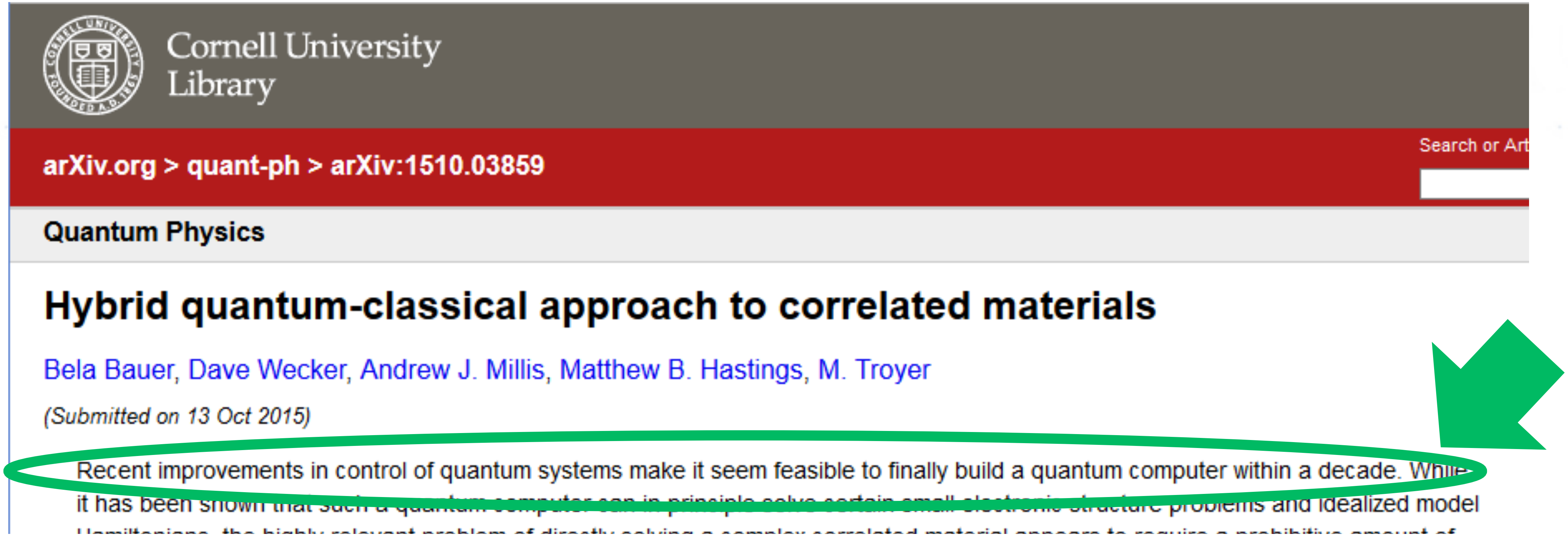
The referenced paper was written by ***Michele Mosca*** *(University of Waterloo, Chairman of the Institute for Quantum Computing, Canada Research Chair in Quantum Computation)*

1. **The transition to quantum-safety will take lots of time and energy.**
   - *"There is no quick fix and we cannot quickly make up lost time."*
2. **Quantum computer will arrive before we're ready.**
3. **A wake up call is needed… The main challenges aren't technical.**
   - *"Despite the many technical and scientific challenges to deploying quantum-safe cryptography,* ***the main challenges in my opinion are the business and policy decisions that would drive the adoption of quantum-safe cryptography….****"*
4. **Quantum computers will be of immense value to mankind, but the impact of quantum computers on cybersecurity will be catastrophic.**
   - *"Harnessing the power of quantum mechanics in large-scale quantum computers will allow us to solve many valuable problems for humanity,* ***but we must first take the catastrophic impact of breaking cybersecurity off the table by developing and deploying a suite of quantum-safe cryptographic tools before quantum computers arrive****."*
5. **Quantum-safe cryptography is not an option in the new age of quantum computing.**
   - *"Quantum-safe cryptography is a necessary part of cybersecurity in an era with quantum computers…"*

NTRU

SECURITY INNOVATION

Microsoft Quantum Computing Predictions



Cornell University Library

arXiv.org > quant-ph > arXiv:1510.03859

Search or Art

Quantum Physics

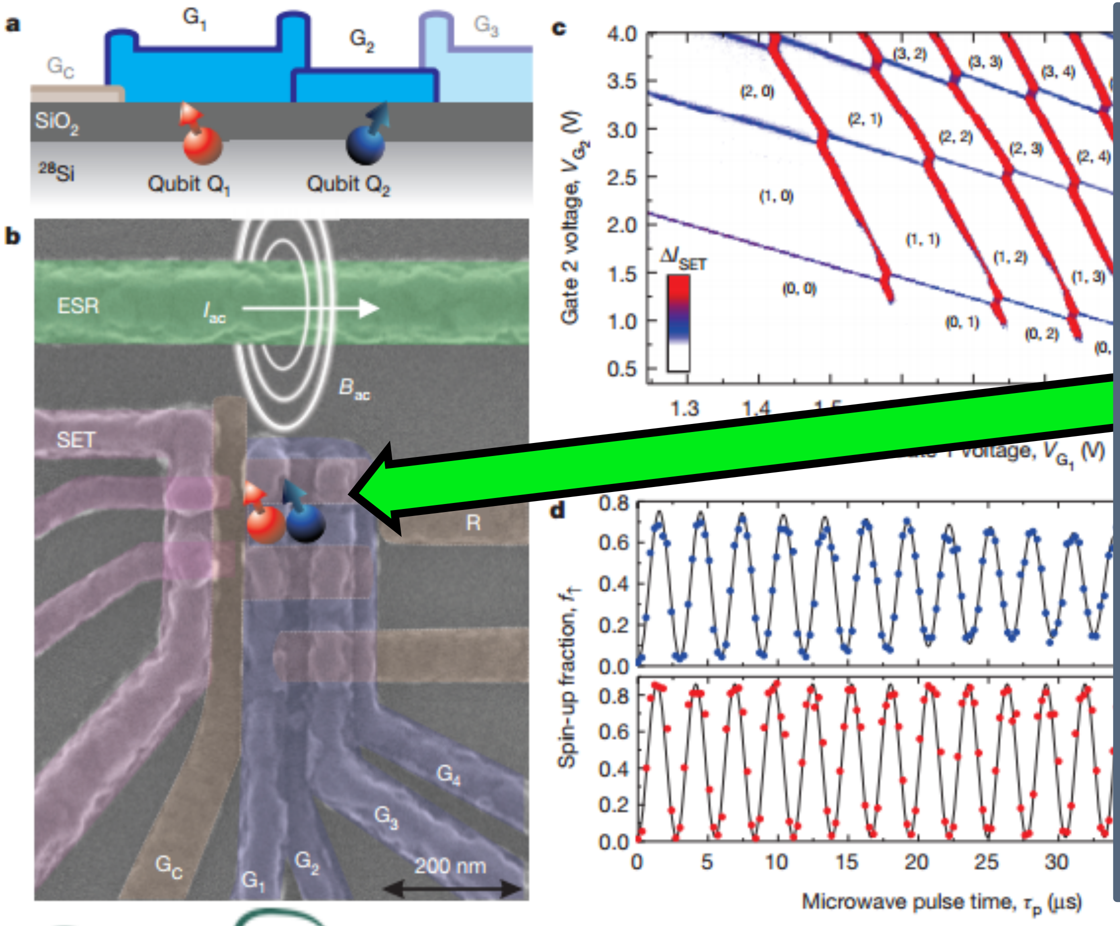
Hybrid quantum-classical approach to correlated materials

Bela Bauer, Dave Wecker, Andrew J. Millis, Matthew B. Hastings, M. Troyer

(Submitted on 13 Oct 2015)

Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer within a decade. While it has been shown that such a quantum computer can in principle solve certain small electronic structure problems and idealized model Hamiltonians, the highly relevant problem of directly solving a complex correlated material appears to require a prohibitive amount of

UNSW Can Now Make Qubits Using Standard CMOS Fabrication Technology….



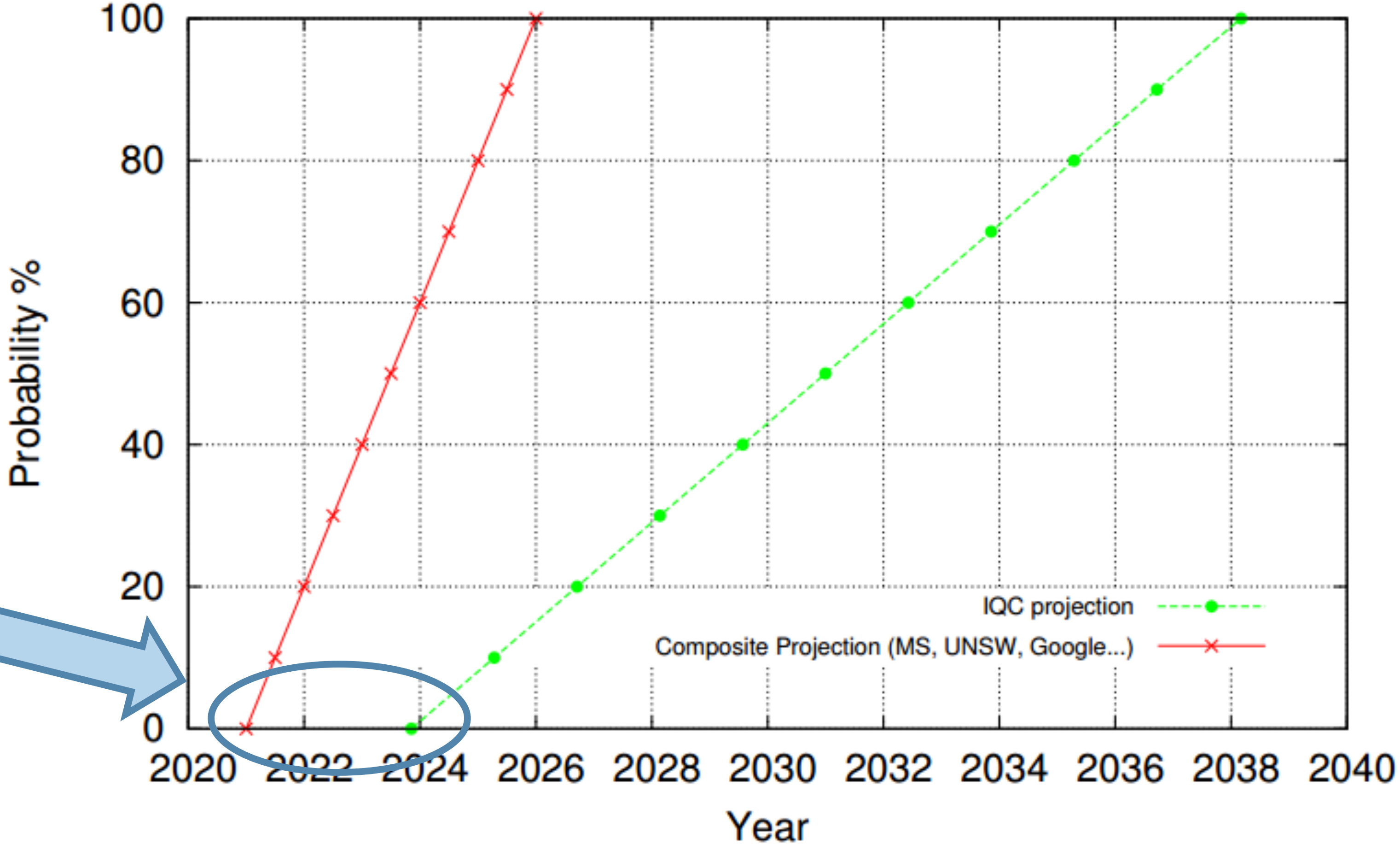
From "A Two-Qubit Logic Gate in Silicon", Nature Magazine, 10/15/15

"Although these **silicon qubits** represent the smallest scalable two-qubit system reported so far, the complete fabrication process is **compatible with standard CMOS (complementary metal – oxide–semiconductor) technology,** and is also consistent with current transistor feature sizes, offering the prospect of **realizing a large-scale quantum processor using the same silicon manufacturing technologies that have enabled the current information age**."

Projected Probability of General Purpose Quantum Computers Arriving By Year

The green graph is based on data from the IQC (Institute for Quantum Computing) provided earlier in 2015. The red graph is based on data after significant breakthroughs were achieved (Microsoft, UNSW, IBM, Google, etc.) since the beginning of 2H15.

Critical infrastructure and industries with fiduciary responsibilities <u>MUST</u> be re-tooled when the threat window opens!



NTRU

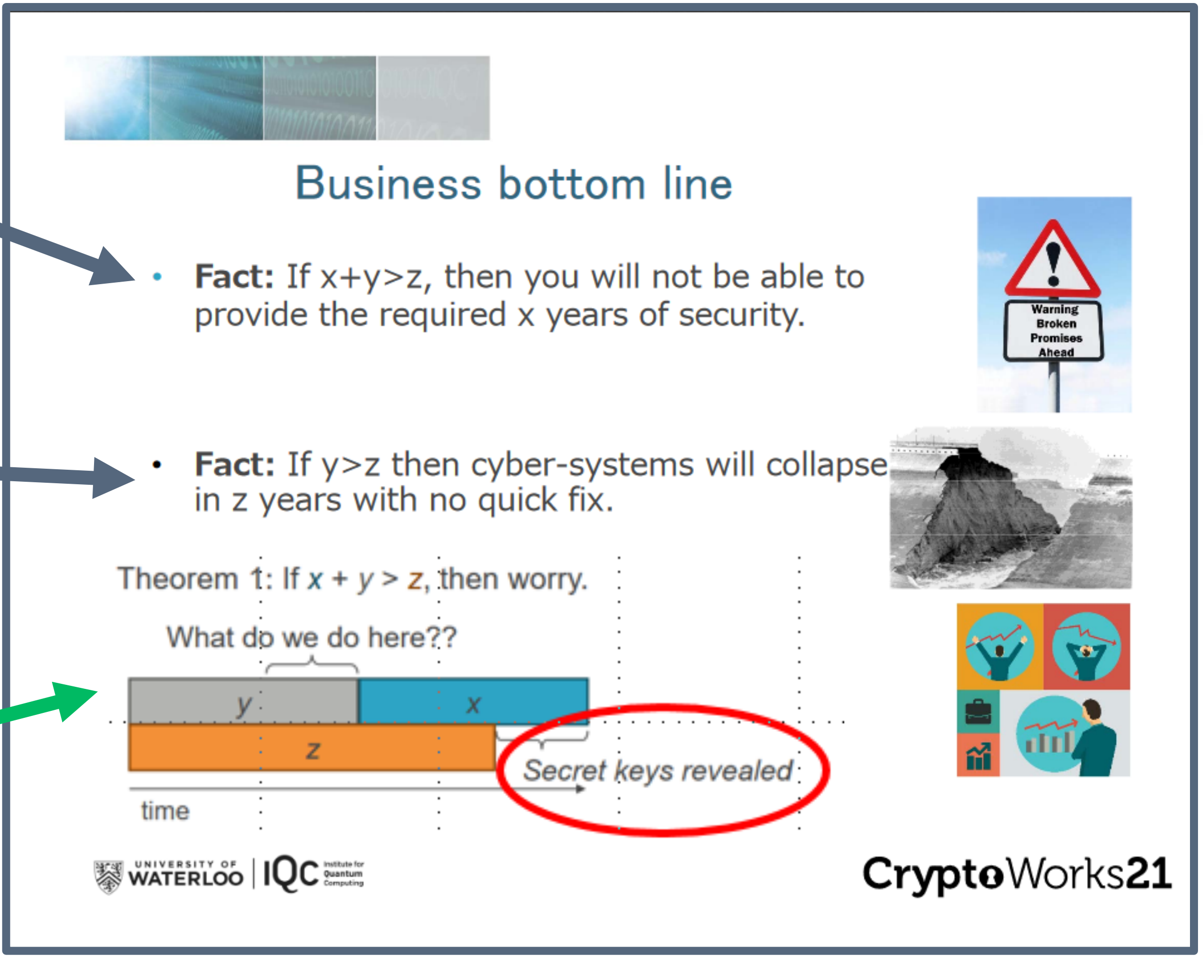
SECURITY INNOVATION

There are 2 Very Important Threats… The 1st Is Already Here… We Have a FIPS 140-2 Compliant Solution

Threat #1: If QC arrives before all your classically encrypted data reaches end of life – you've got a major security breach (data vaulting attack)

Threat #2: If QC arrives before you are retooled – the problem is even worse – your system's real time security will be completely exposed and the fix will probably not be quick.

X = "how many years does your data need to be secure"
Y = "how long will it take you to retool"
Z = "when will QC arrive"



Business bottom line

- **Fact:** If x+y>z, then you will not be able to provide the required x years of security.
- **Fact:** If y>z then cyber-systems will collapse in z years with no quick fix.

Theorem 1: If $x + y > z$, then worry.

What do we do here??

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

CryptoWorks21

NTRU

SECURITY INNOVATION

Applying the IQC "Panic" Equation

Time you need your current encryption to be secure (X)	Time needed to retool crypto, standards and IT infrastructure (Y)	Assessment on when QC threat arrives (see chart 5) (Z)	Time Your Keys (and Confidential Data) are Exposed
15	10	10	15 Years
15	10	15	10 Years
15	3	5	13 Years
15	3	10	10 Years
15	3	15	10 Years
30	5	12	23 Years

- Ten years is aggressive but achievable retooling.
- Fifteen years of data confidentiality (x) is low for many govt, health, financial … institutions

- Three years is extremely aggressive retooling – effectively mass panic mode.

- More realistic confidentiality period for banks, healthcare, govt., etc.
- Aggressive retooling time
- Assumption that QC will arrive fairly slowly

NTRU

SECURITY INNOVATION

From A New Study: “Most Organizations Can’t Protect Digital Information in the Long-Term”

“New research has revealed that the majority of organizations DO NOT have a coherent long-term strategy for their vital digital information even though virtually all of them (98%) are required to keep information for ten years or longer.”

“While 97% of information professionals understand the need for a specialized approach to these assets, only 11% are storing them in systems specifically designed to ensure long-term protection and access. This gap has economic, legal, and business competitiveness implications. The research, conducted by think tank the Information Governance Initiative (IGI), provides a new benchmark for organizations to evaluate their capability and outlines tactics for closing this critical gap. It also reports on how leading organizations like Associated Press, HSBC, and the State of Texas have addressed this challenge.”

“The research, conducted by think tank the Information Governance Initiative (IGI), provides a new benchmark for organizations to evaluate their capability and outlines tactics for closing this critical gap. It also reports on how leading organizations like Associated Press, HSBC, and the State of Texas have addressed this challenge.”

https://www.helpnetsecurity.com/2016/05/17/protect-digital-information/

NTRU

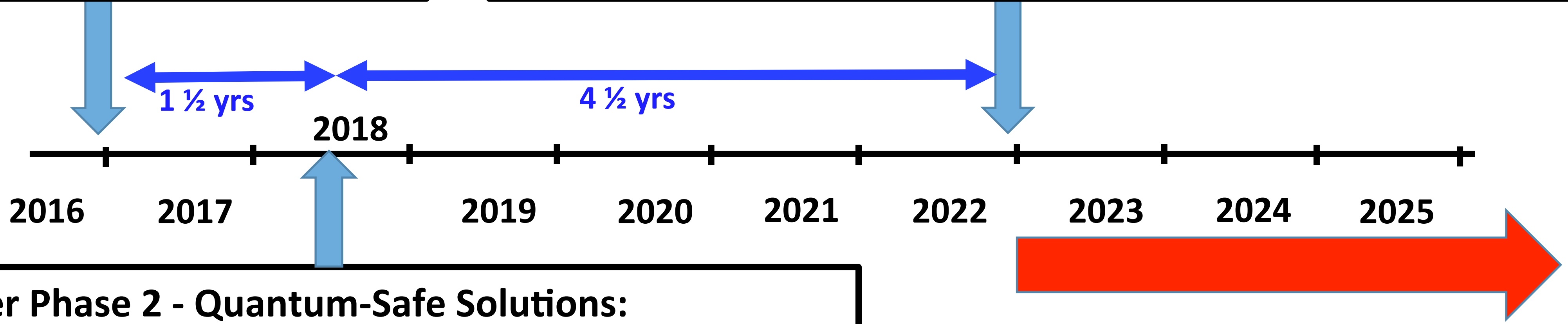
SECURITY INNOVATION

A Common Sense Timeline to Quantum Safety – Building a Quantum Risk Mgmt. Plan (QRMP)

Deliver Phase 1 - Quantum Risk Management Plan as an RFP Response

Deliver Phase 3 – Complete Quantum-Safety

- **Quantum-Safe Standardized PKI**
- **Quantum-Safe Authentication, Key Management, etc.**



Deliver Phase 2 - Quantum-Safe Solutions:

- **Quantum-safe TLS to combat data vaulting threat**
- **Quantum-safe code signing**
- **Quantum-safe symmetric keys**

Probability of general purpose QC doing crypto breaking is very real after 2022 – it could occur sooner…

Template for a “Quantum Risk Management Plan” (QRMP)

NTRU

SECURITY INNOVATION

NTRU and pqNTRUsign Algorithm Summary

Quantum Bit Strength	NTRU Encryption Algorithm	pqNTRUsign Signature Algorithm
128	**NTRU-443** (Private key size = 396 bits Public key size = 665 bytes)	**pqNTRUsign-563** (Private Key Size= 540 bits, Public key size =1056 bytes, signature size = 1056 bytes)
192	**NTRU-587** (Private key size = 504 bits Public key size = 881 bytes)	**pqNTRUsign-743** (Private Key Size= 560 bits, Public key size =1486 bytes, signature size = 1486 bytes)
256	**NTRU-743** (Private key size = 740 bits Public key size = 1115 bytes)	**pqNTRUsign-907** (Private Key Size = 640 bits, Public key size =1814 bytes, signature size = 1814 bytes)

Notes:

1. *For post-quantum cryptography you need to know their quantum bit strengths – not the classical bit strengths.*
2. *The suffixes on the NTRU and pqNTRUsign algorithms designate their polynomial which is one-half of the NTRU lattice size they use.*
3. *For NTRU private keys, store the seed and compute it on demand for decryption. (private keys are less than 100 bytes). The seed size is 2x the security level (quantum bit strength) (e.g. for NTRU-443 it is 256 bits.)*

NTRU

SECURITY INNOVATION

NTRU Standardization and Adoption

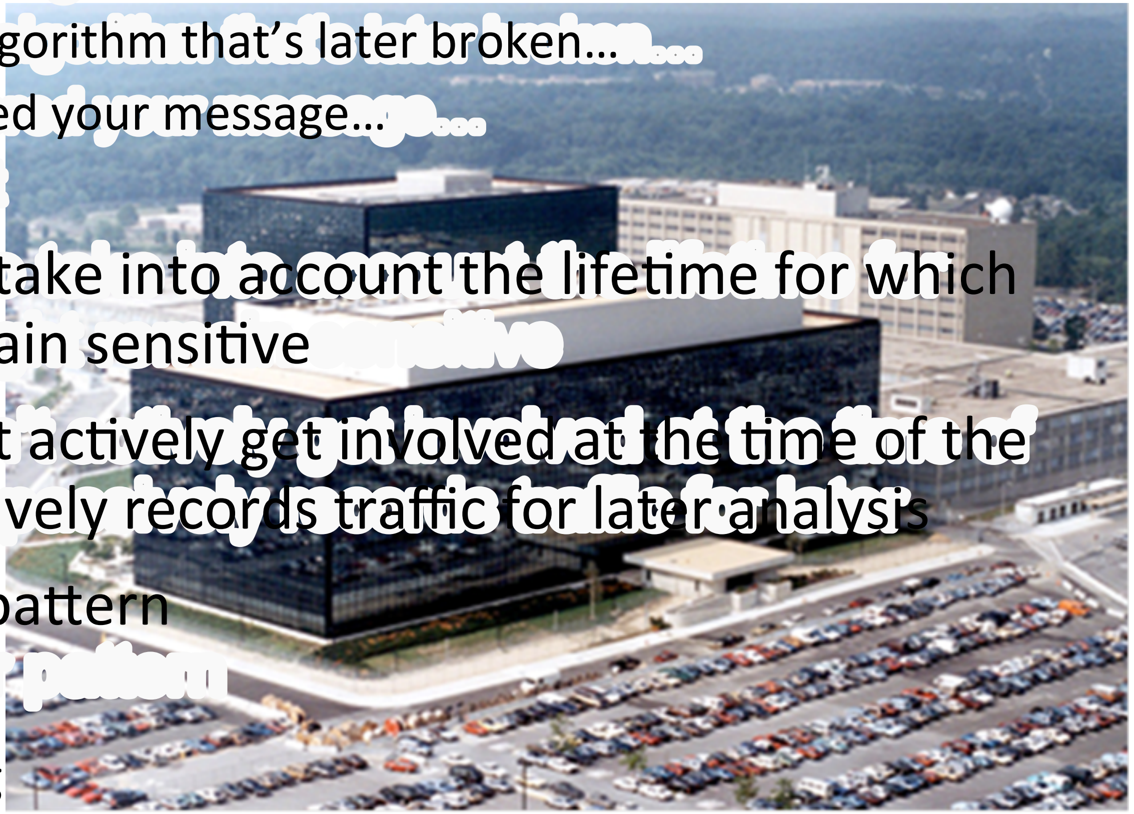
- NTRUEncrypt
  - 2008: IEEE standard 1363.1 – NTRUEncrypt
  - 2010: X9 standard X9.98 – NTRUEncrypt
  - Quantum-Safe Hybrid (QSH) Internet Draft – Standalone RFC in Progress
  - Involved with quantum-safe standardization work with NIST, ISO, ETSI.
  - Implemented in:
    - wolfSSL (wolfSSL supports 1 billion TLS connections worldwide)
    - Cyph (IM), Imprivata (Healthcare IT), Unseen (IM), Texas Instruments OMAP chip (cellphone technology), WikID (2FA) , EchoSat (POS credit card devices)
    - Following the NSA Announcement, 2015 technical breakthroughs, etc. … Interest has understandably skyrocketed.

NTRU

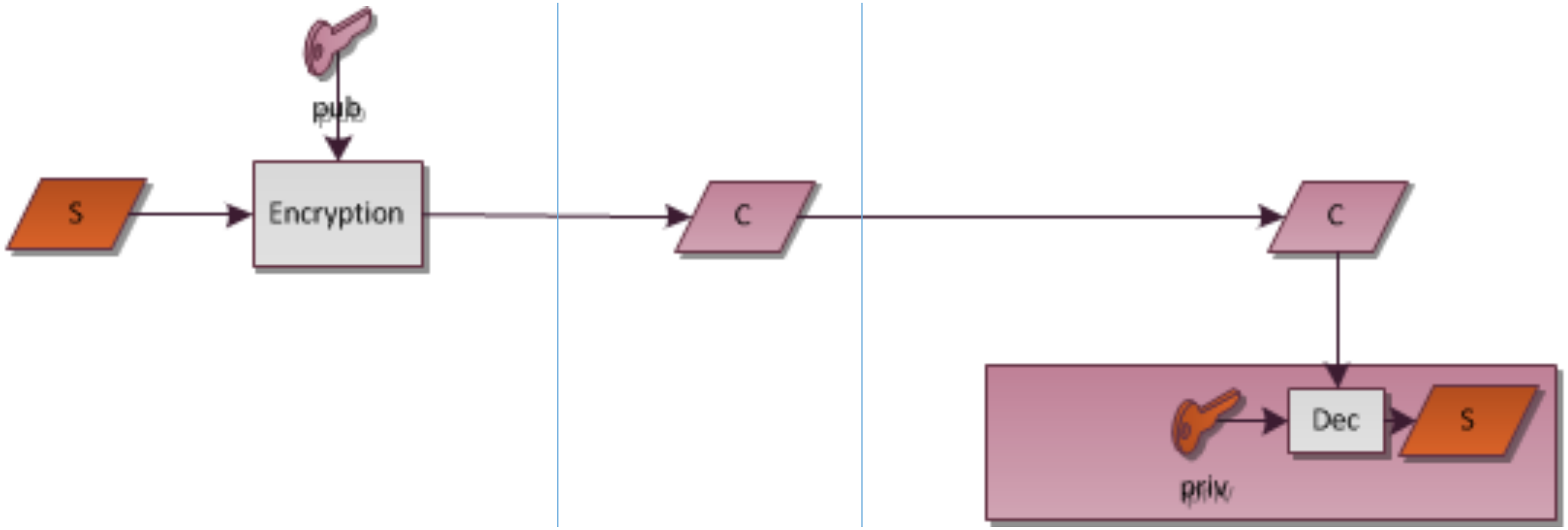
SECURITY INNOVATION

How long do your secrets need to live?

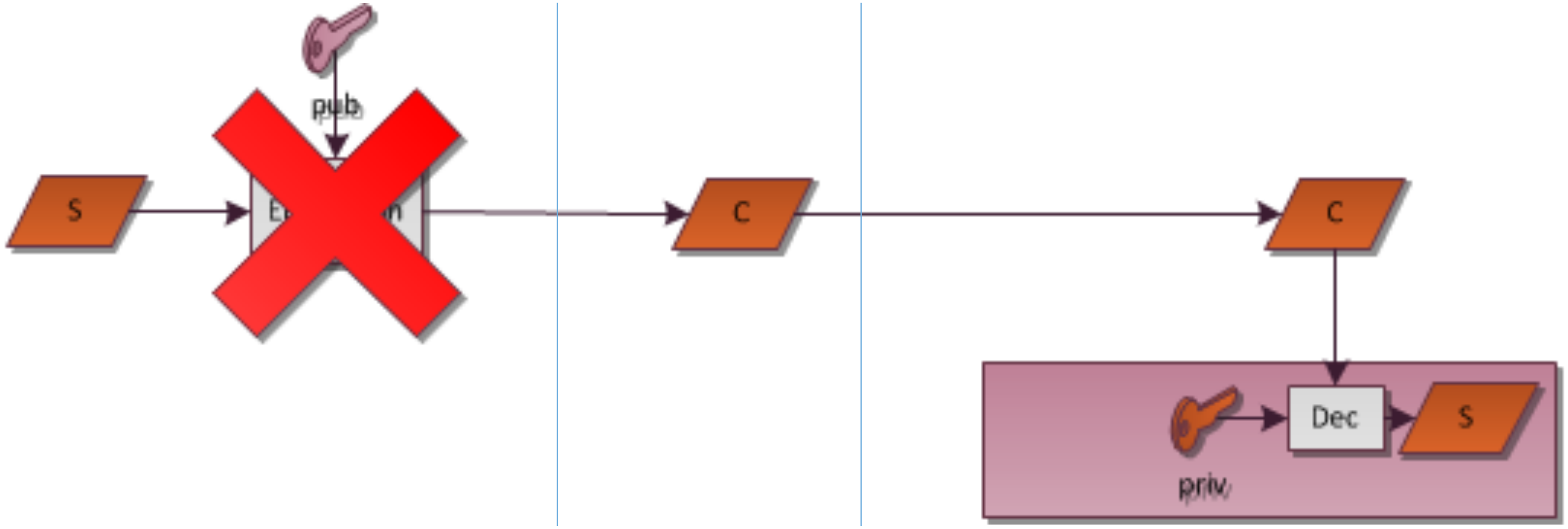
- If you send something now…
  - Encrypted with an algorithm that’s later broken…
  - And someone’s stored your message…
  - They can decrypt it
- Encryption needs to take into account the lifetime for which your data might remain sensitive
- Attacker who doesn’t actively get involved at the time of the interaction, but passively records traffic for later analysis
- Fits known attacker pattern
- Attacks:
  - Quantum computing
  - Other yet-to-be-discovered classical



Basic model of public-key encryption

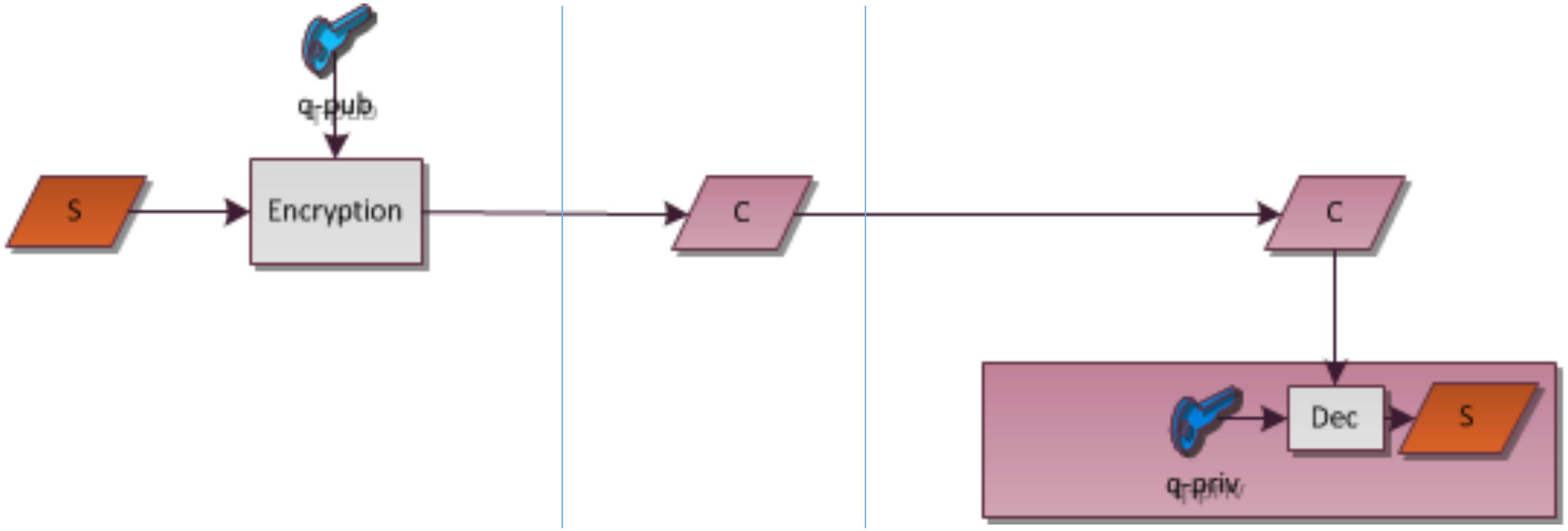


Post-quantum problem

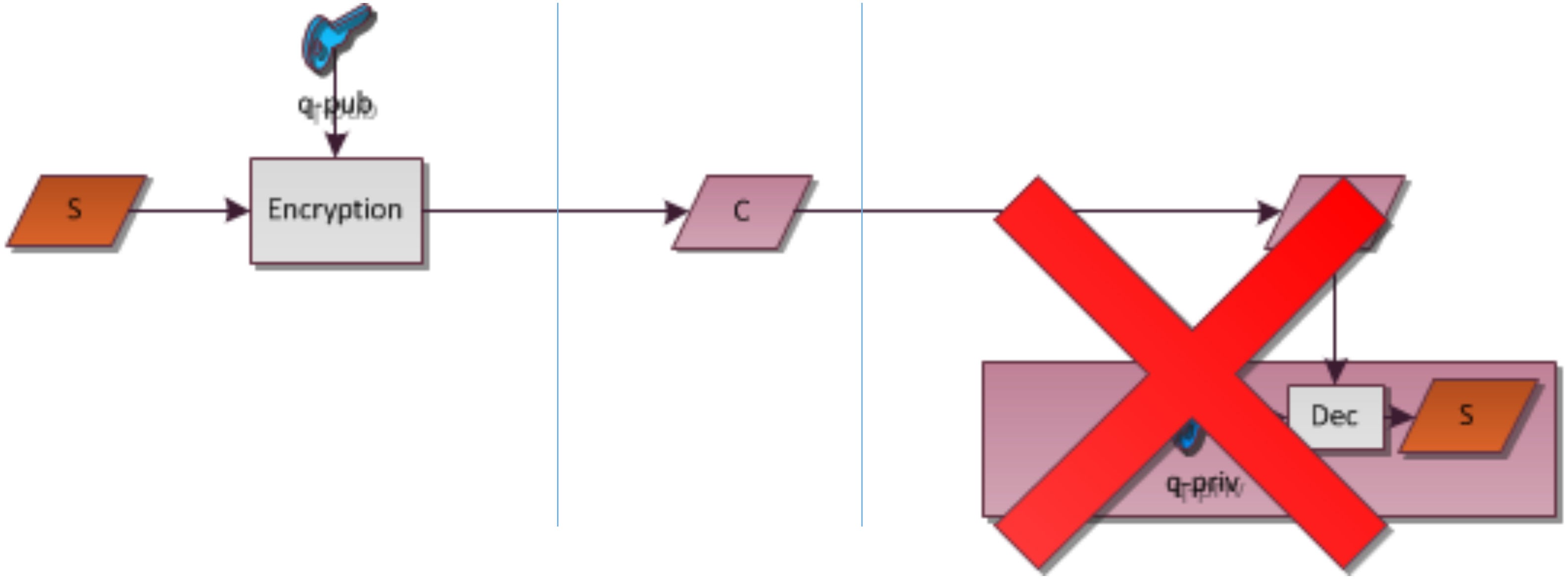


SECURITY INNOVATION

Solution 1

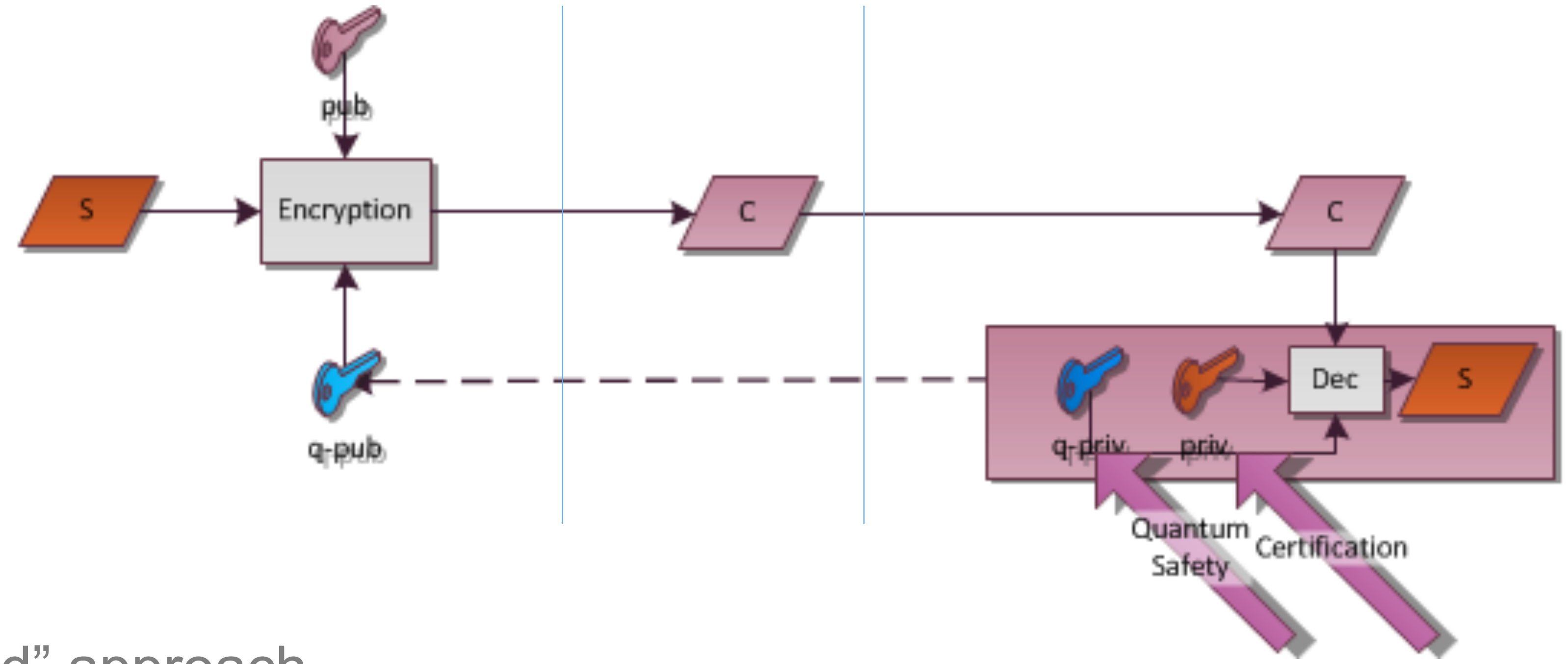


~~Solution 1~~



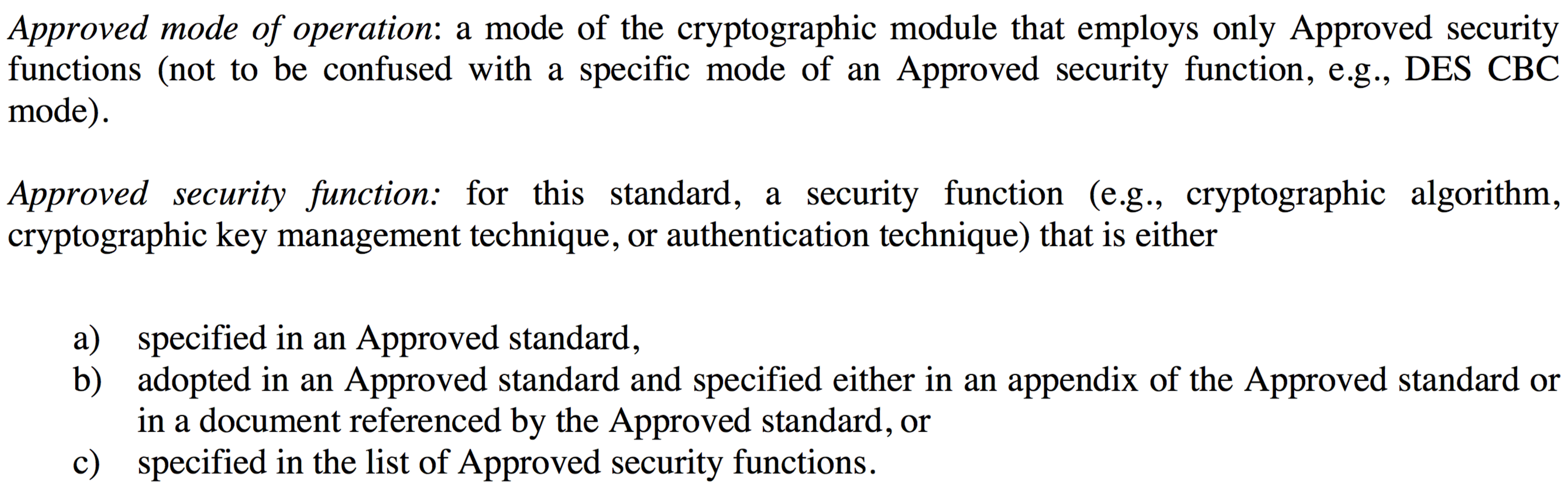
- No FIPS-approved quantum-safe algorithms

Potential transitional solution



- “Hybrid” approach
- FIPS-approved algorithm for conformance, quantum-safe algorithm for quantum-safety
- But isn’t it still not allowed to run a non-Approved algorithm in Approved mode?

Approved mode



Approved mode of operation: a mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., DES CBC mode).

Approved security function: for this standard, a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either

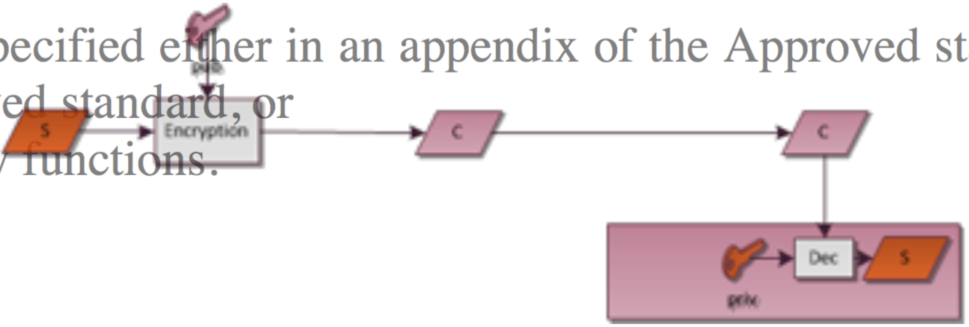
a) specified in an Approved standard,
b) adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or
c) specified in the list of Approved security functions.

Approved mode

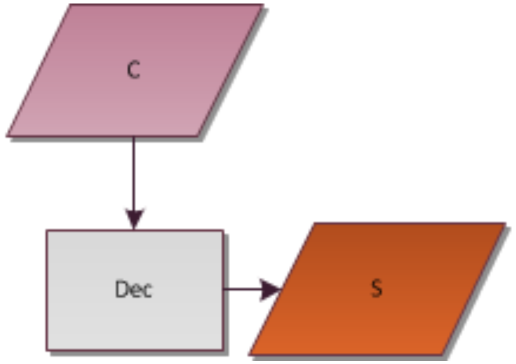
Approved mode of operation: a mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., DES CBC mode).

Approved security function: for this standard, a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either

a) specified in an Approved standard,
b) adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or
c) specified in the list of Approved security functions.

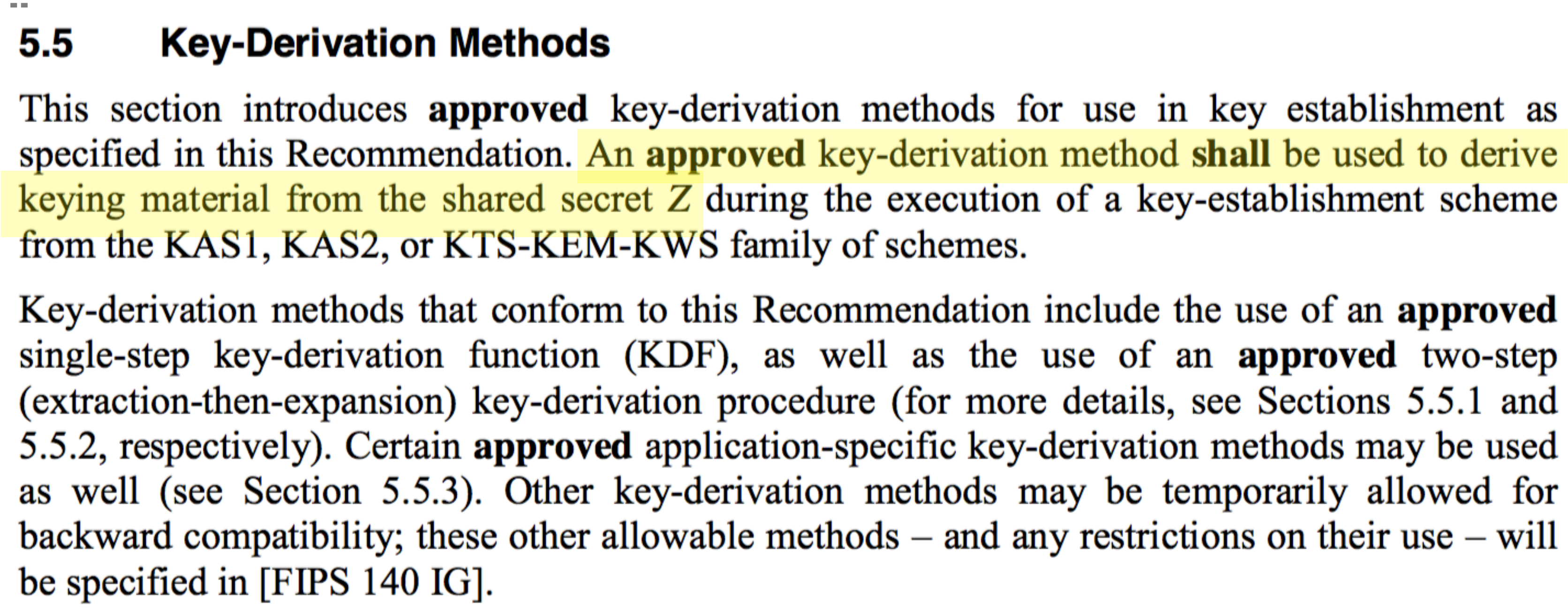


Looking closer at decryption (1)



Key Derivation methods

- SP 800-56B, “Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptograph

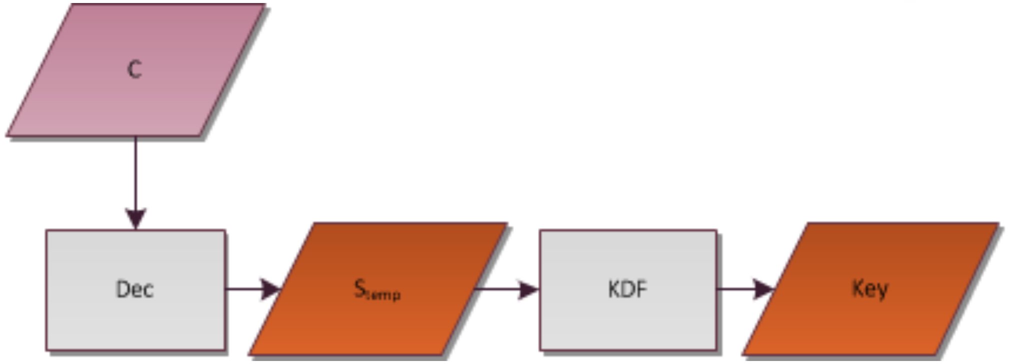


5.5 Key-Derivation Methods

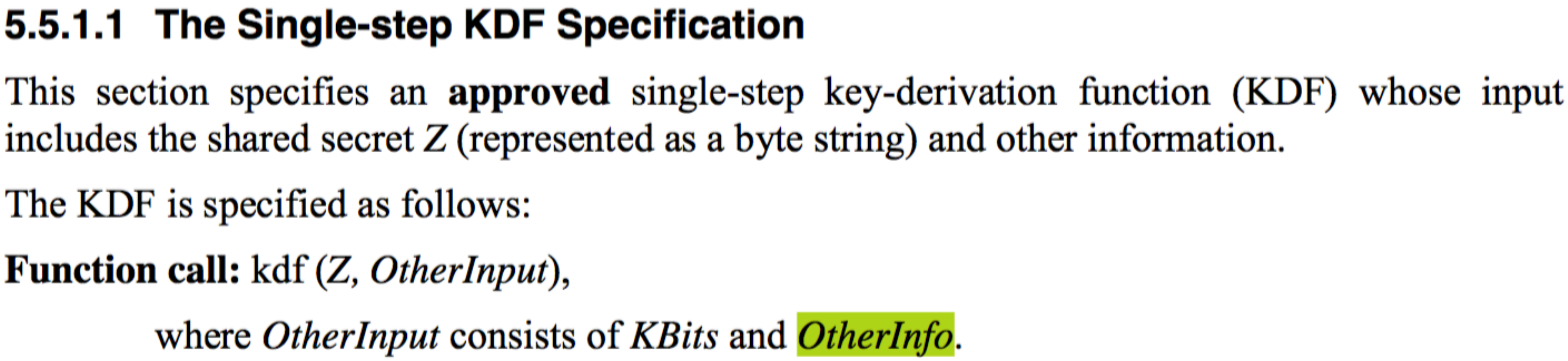
This section introduces **approved** key-derivation methods for use in key establishment as specified in this Recommendation. An **approved** key-derivation method **shall** be used to derive keying material from the shared secret *Z* during the execution of a key-establishment scheme from the KAS1, KAS2, or KTS-KEM-KWS family of schemes.

Key-derivation methods that conform to this Recommendation include the use of an **approved** single-step key-derivation function (KDF), as well as the use of an **approved** two-step (extraction-then-expansion) key-derivation procedure (for more details, see Sections 5.5.1 and 5.5.2, respectively). Certain **approved** application-specific key-derivation methods may be used as well (see Section 5.5.3). Other key-derivation methods may be temporarily allowed for backward compatibility; these other allowable methods – and any restrictions on their use – will be specified in [FIPS 140 IG].

Looking closer at decryption (2)



OtherInfo in KDF



5.5.1.1 The Single-step KDF Specification

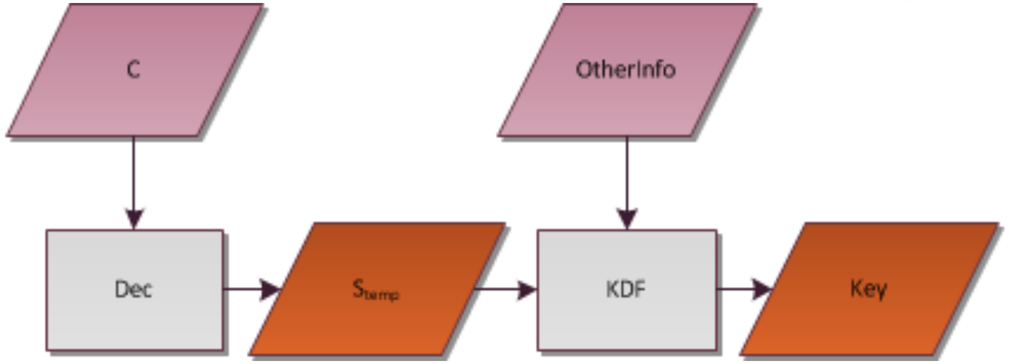
This section specifies an **approved** single-step key-derivation function (KDF) whose input includes the shared secret *Z* (represented as a byte string) and other information.

The KDF is specified as follows:

Function call: kdf (*Z*, *OtherInput*),

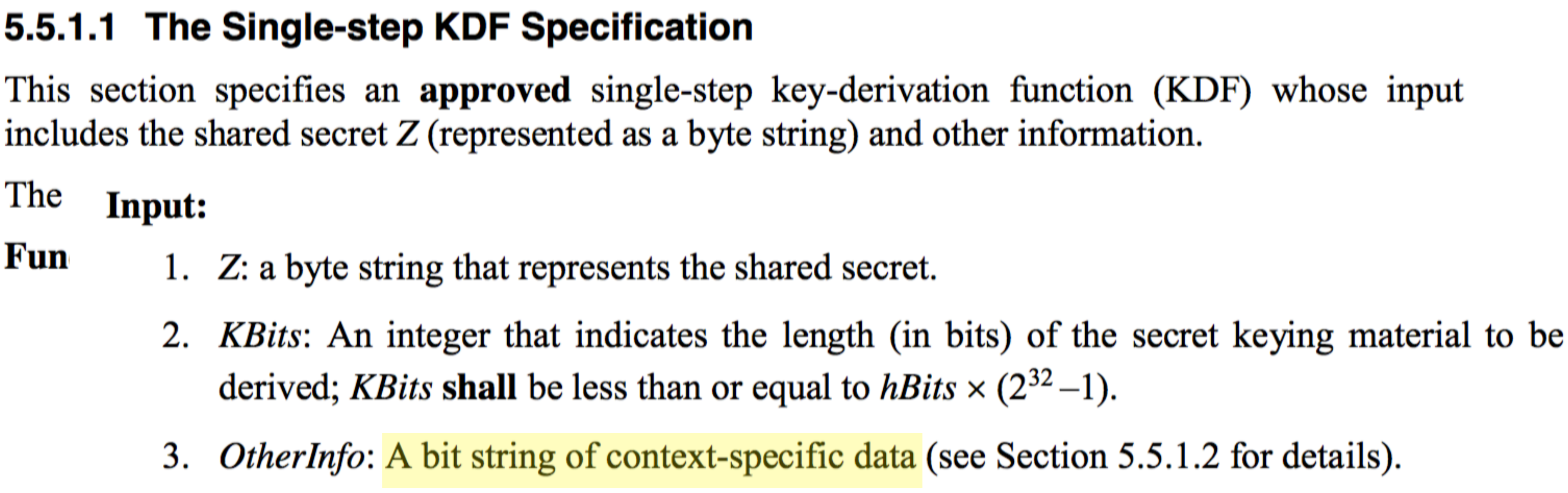
where *OtherInput* consists of *KBits* and *OtherInfo*.

Looking closer at decryption (3)



- The field “OtherInfo” is input to the KDF and FIPS 140-2 puts no constraints on where it comes from
- Idea: Use this to quantum-safe our exchange
- Question: Is this permissible?

OtherInfo in KDF



5.5.1.1 The Single-step KDF Specification

This section specifies an **approved** single-step key-derivation function (KDF) whose input includes the shared secret *Z* (represented as a byte string) and other information.

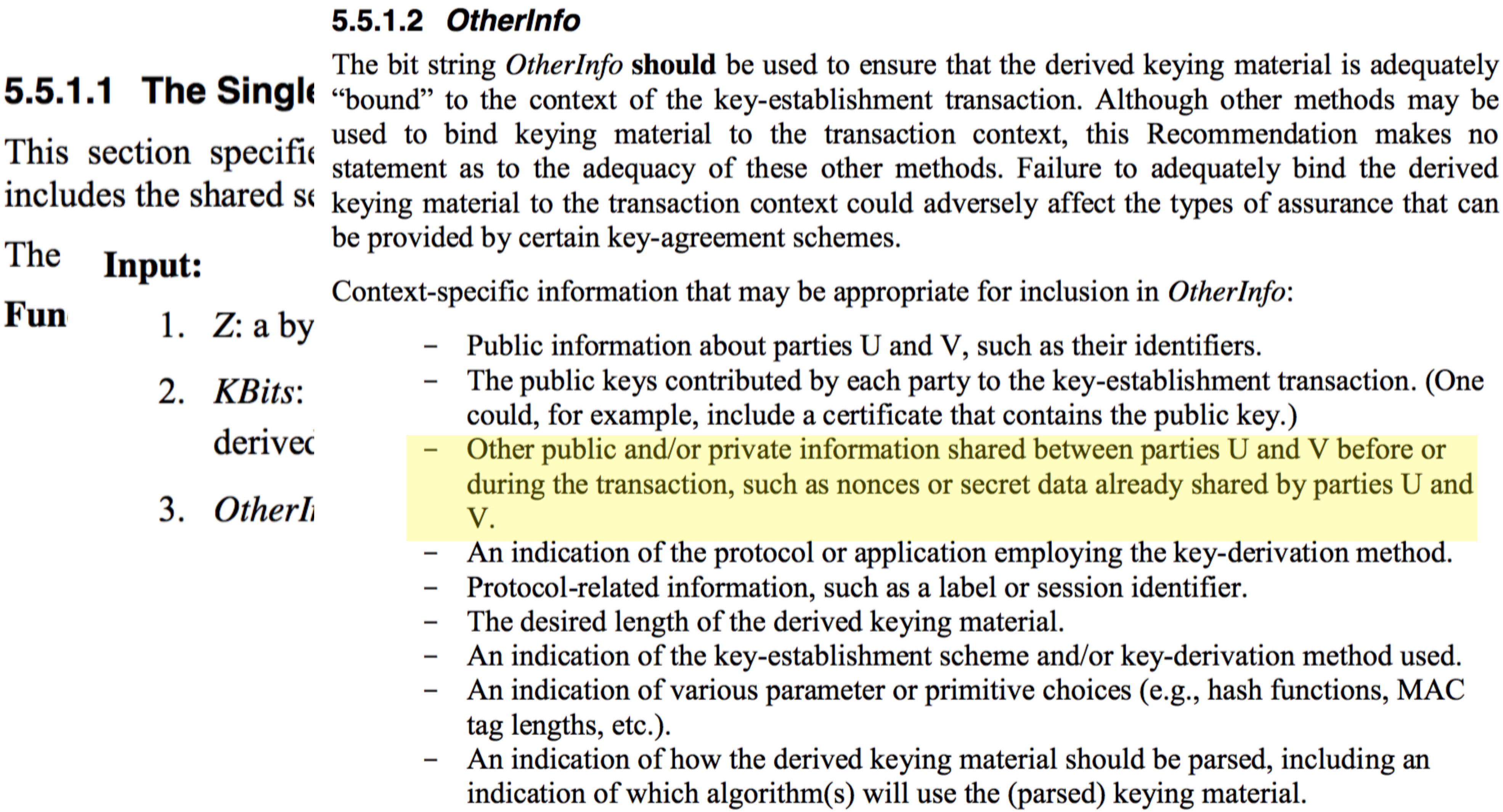
The

Input:

Fun

1. *Z*: a byte string that represents the shared secret.
2. *KBits*: An integer that indicates the length (in bits) of the secret keying material to be derived; *KBits* **shall** be less than or equal to *hBits* × (2^{32} –1).
3. *OtherInfo*: A bit string of context-specific data (see Section 5.5.1.2 for details).

OtherInfo in KDF



5.5.1.1 The Singl

This section specifi
includes the shared s

The

Input:

Fun

1. *Z*: a by
2. *KBits*:
derived
3. *OtherI*

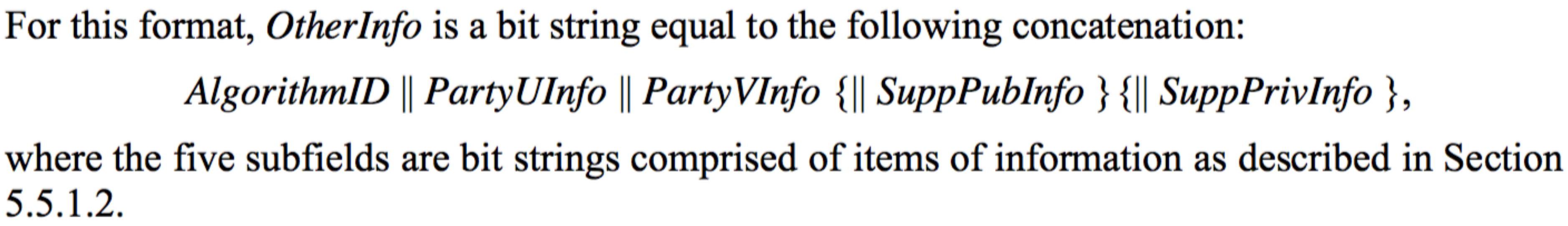
5.5.1.2 *OtherInfo*

The bit string *OtherInfo* **should** be used to ensure that the derived keying material is adequately "bound" to the context of the key-establishment transaction. Although other methods may be used to bind keying material to the transaction context, this Recommendation makes no statement as to the adequacy of these other methods. Failure to adequately bind the derived keying material to the transaction context could adversely affect the types of assurance that can be provided by certain key-agreement schemes.

Context-specific information that may be appropriate for inclusion in *OtherInfo*:

- Public information about parties U and V, such as their identifiers.
- The public keys contributed by each party to the key-establishment transaction. (One could, for example, include a certificate that contains the public key.)
- Other public and/or private information shared between parties U and V before or during the transaction, such as nonces or secret data already shared by parties U and V.
- An indication of the protocol or application employing the key-derivation method.
- Protocol-related information, such as a label or session identifier.
- The desired length of the derived keying material.
- An indication of the key-establishment scheme and/or key-derivation method used.
- An indication of various parameter or primitive choices (e.g., hash functions, MAC tag lengths, etc.).
- An indication of how the derived keying material should be parsed, including an indication of which algorithm(s) will use the (parsed) keying material.

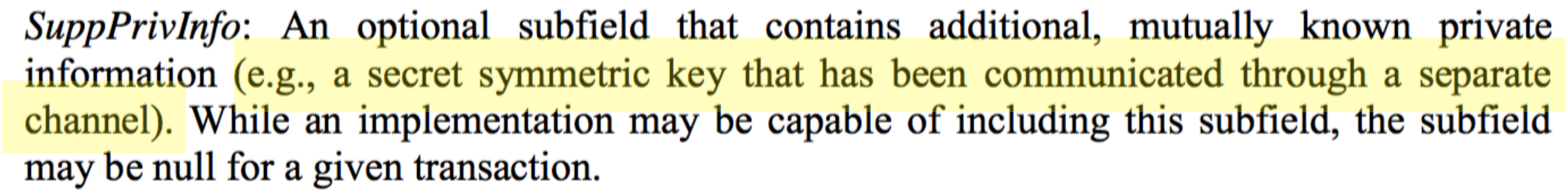
Can we include symmetric keys in OtherInfo?



For this format, *OtherInfo* is a bit string equal to the following concatenation:

AlgorithmID || *PartyUInfo* || *PartyVInfo* {|| *SuppPubInfo* } {|| *SuppPrivInfo* },

where the five subfields are bit strings comprised of items of information as described in Section 5.5.1.2.



SuppPrivInfo: An optional subfield that contains additional, mutually known private information (e.g., a secret symmetric key that has been communicated through a separate channel). While an implementation may be capable of including this subfield, the subfield may be null for a given transaction.

SECURITY INNOVATION

Suitable schemes in SP 800-56B

Scheme	Section	Uses KDF
KAS1 Key Agreement (basic or with confirmation)	8.2	✔
KAS2 Key agreement (basic or with any form of confirmation)	8.3	✔
KTS-OAEP (basic or with confirmation)	9.2	NO
KTS-KEM-KWS	9.3	✔

KDF	Section	Allows OtherInfo
Single-step Key-Derivation Function	5.8.1	✔
Extraction-then-Expansion Key-Derivation Procedure	5.8.2	✔
Application-Specific Key-Derivation Methods	5.8.2	

… all but one scheme, and both baseline KDFs, in SP 800-56B support OtherInfo
==> all but one scheme, if used with either baseline KDF, supports quantum-safe hybrid

Suitable Schemes in SP 800-56A

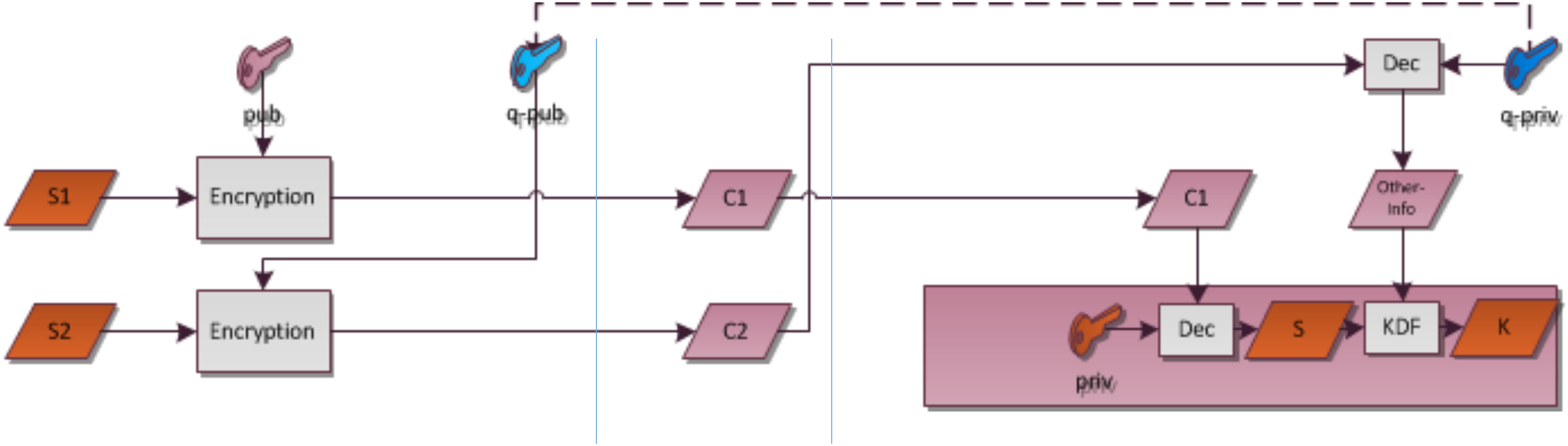
Scheme	Section	Uses KDF
dhHybrid1	6.1.1.1	✔
(Cofactor) Full Unified Model	6.1.1.2	✔
MQV2	6.1.1.3	✔
Full MQV	6.1.1.4	✔
dhEphem	6.1.2.1	✔
(Cofactor) Ephemeral Unified Model	6.1.2.2	✔
dhHybridOneFlow	6.2.1.1	✔
(Cofactor) One-Pass Unified Model	6.2.1.2	✔
MQV1	6.2.1.3	✔
One-Pass MQV	6.2.1.4	✔
dhOneFlow	6.2.2.1	✔
(Cofactor) One-Pass Diffie-Hellman	6.2.2.2	✔
dhStatic	6.3.1	✔
(Cofactor) Static Unified Model	6.3.2	✔

KDF	Section	Allows OtherInfo
Single-step Key-Derivation Function	5.8.1	✔
Extraction-then-Expansion Key-Derivation Procedure	5.8.2	✔
Application-Specific Key-Derivation Methods	5.8.2	

… every single scheme, and both baseline KDFs, in SP 800-56A support OtherInfo
==> every scheme, if used with either baseline KDF, supports quantum-safe hybrid

SECURITY INNOVATION

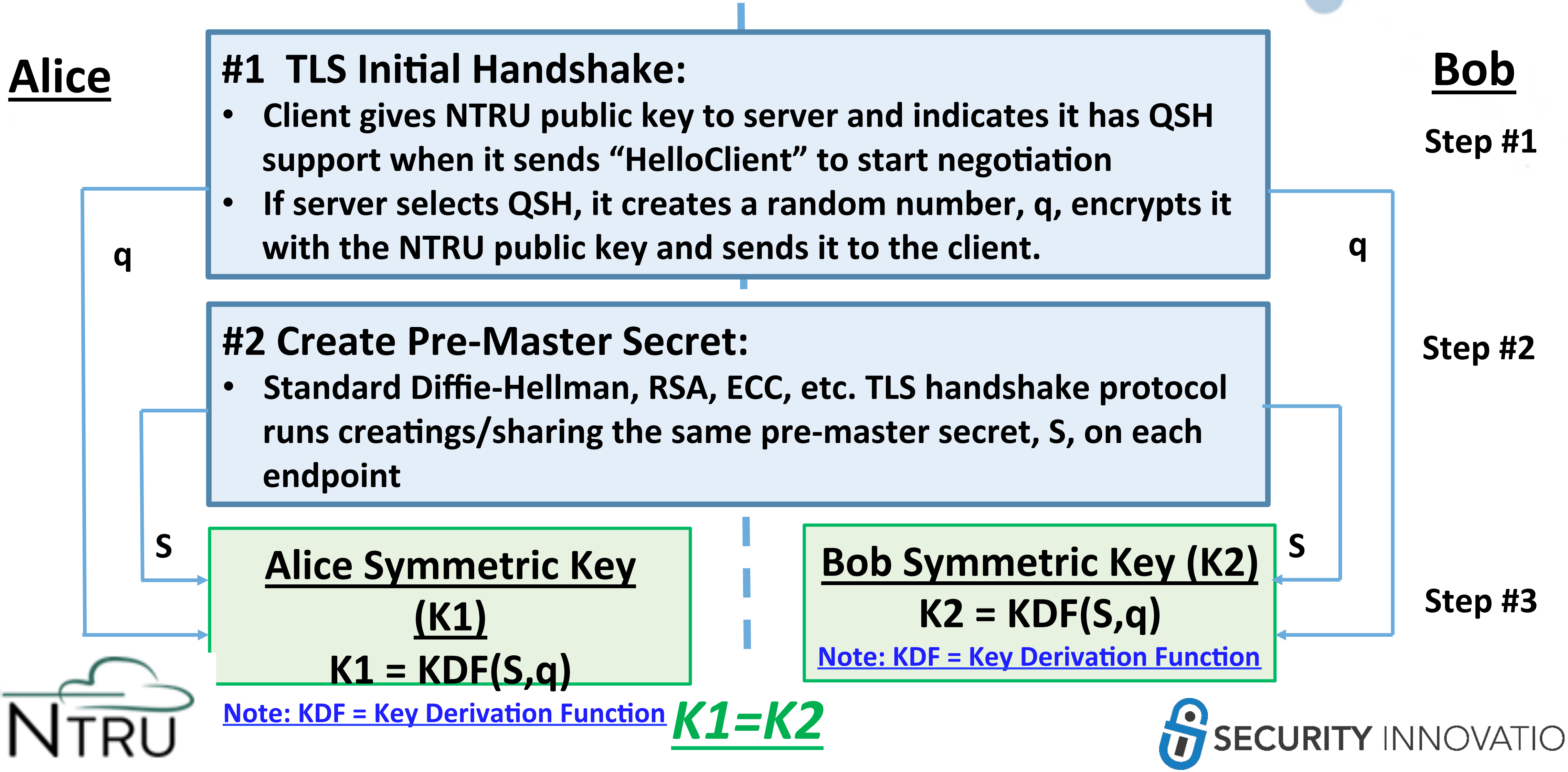
This is clearly okay



- q-pub/q-priv are *ephemeral* keys to the greatest extent possible – ideally, they are used for a single exchange and then deleted
- It is clear that a FIPS-approved module, running in FIPS mode, can do this
- You can construct a security proof showing that this “doesn’t make things worse”

SECURITY INNOVATION

TLS Negotiation with QSH (Quantum Safe Hybrid)



Alice

Bob

Step #1

#1 TLS Initial Handshake:

- Client gives NTRU public key to server and indicates it has QSH support when it sends “HelloClient” to start negotiation
- If server selects QSH, it creates a random number, q, encrypts it with the NTRU public key and sends it to the client.

Step #2

#2 Create Pre-Master Secret:

- Standard Diffie-Hellman, RSA, ECC, etc. TLS handshake protocol runs creatings/sharing the same pre-master secret, S, on each endpoint

Step #3

Alice Symmetric Key (K1)

K1 = KDF(S,q)

Note: KDF = Key Derivation Function

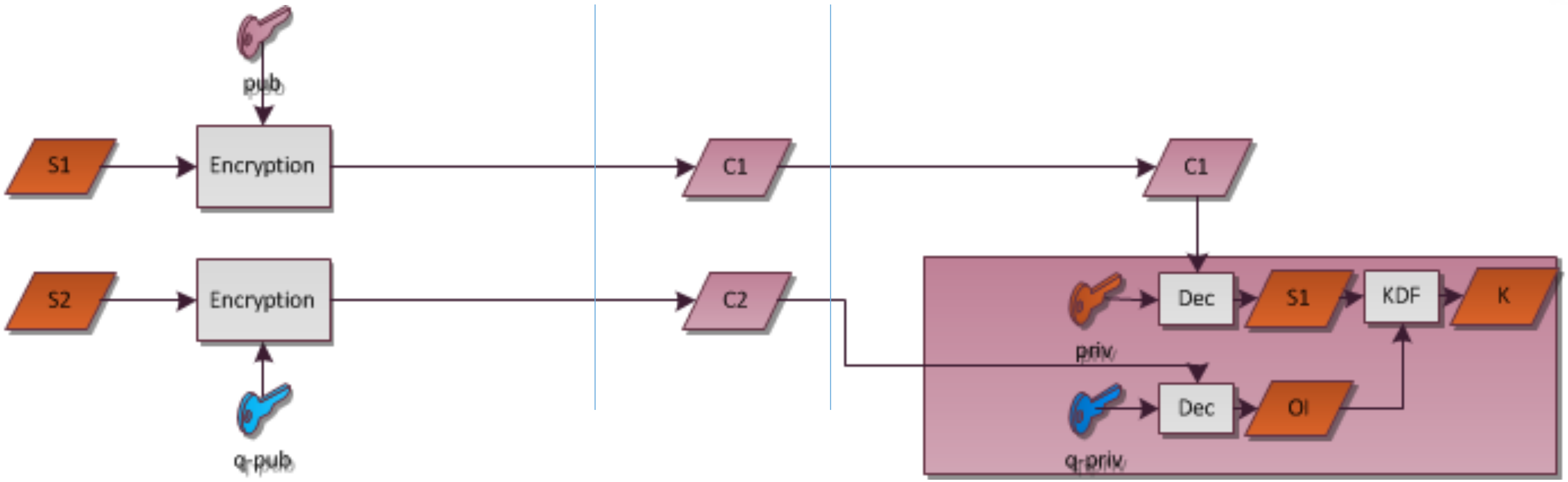
Bob Symmetric Key (K2)

K2 = KDF(S,q)

Note: KDF = Key Derivation Function

K1=K2

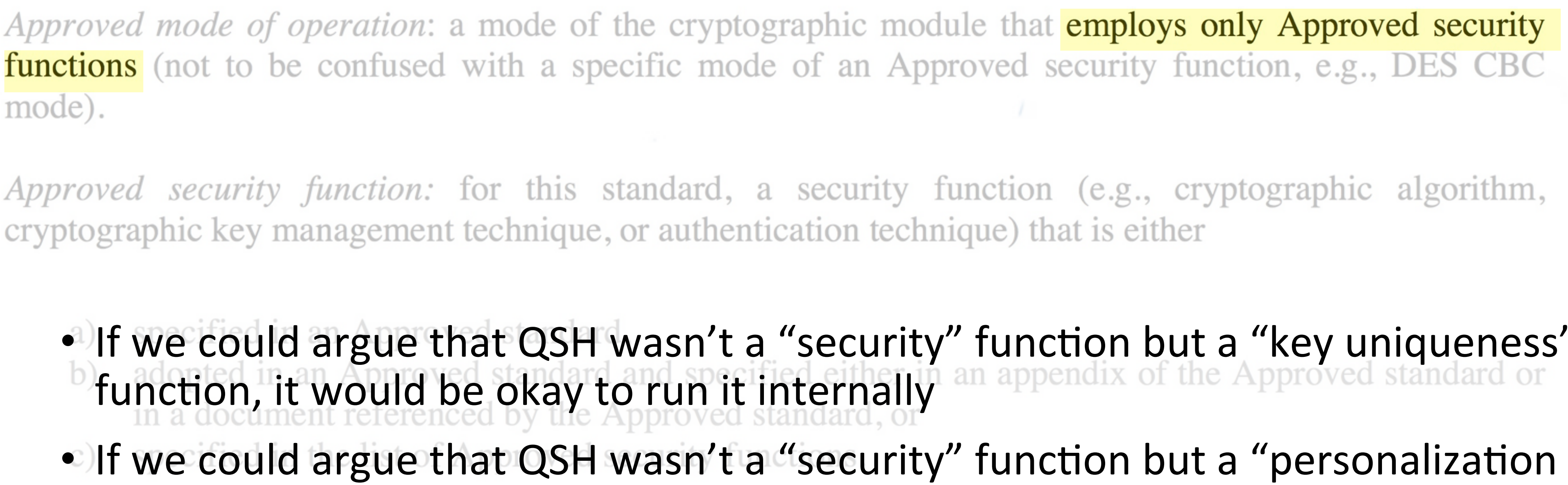
What about this?



- Same as previous, except the quantum-safe decryption runs inside the secured boundary
- Clearly more secure…
- ... But can it be done in Approved mode?

SECURITY INNOVATION

Approved mode



Approved mode of operation: a mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., DES CBC mode).

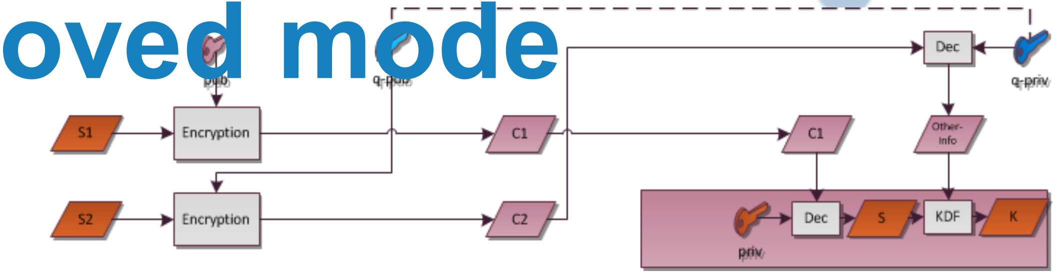
Approved security function: for this standard, a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either

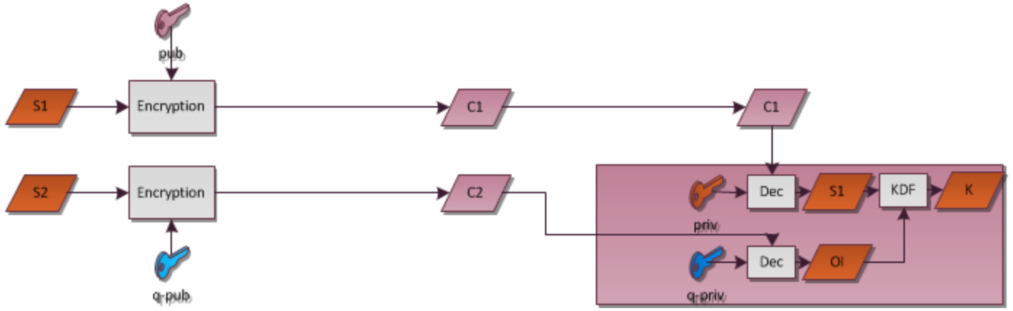
a) specified in an Approved standard,
b) adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or
c) specified in the list of Approved security functions.

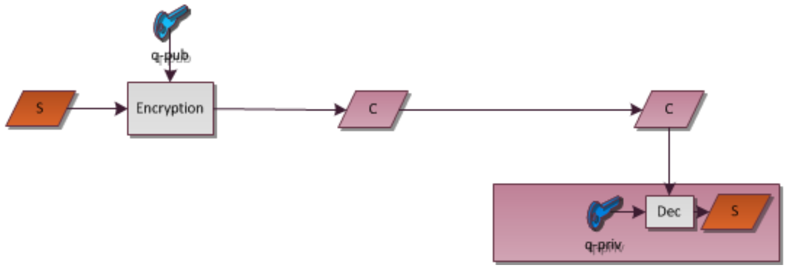
- If we could argue that QSH wasn’t a “security” function but a “key uniqueness” function, it would be okay to run it internally
- If we could argue that QSH wasn’t a “security” function but a “personalization function”, it would be okay to run it internally
- If NIST changed this to “employs only Approved security functions, except to derive the OtherInfo field”; or simply issued guidance that using non-Approved functions to derive the OtherInfo field is okay, it would be okay to run it internally

Roadmap to quantum-safe devices running in FIPS Approved mode

- Tomorrow: QSH via ephemeral keys in software outside the FIPS device, shared secret entered via OtherInfo
- Two years (?): NIST issues guidance allowing OtherInfo to be obtained using non-Approved security mechanisms; FIPS-approved devices, running in FIPS Approved Mode, can carry out QSH
- Five years (?): NIST approves quantum-safe algorithms: FIPS-approved devices can be in FIPS mode while only running quantum-safe algorithms







NIST Position on QSH and FIPS 140-2

pq
PQCrypto 2016
Seventh International Conference
on Post-Quantum Cryptography, Fukuoka, Japan
Post-Quantum Cryptography:
NIST's Plan for the Future
Dustin Moody
Post Quantum Cryptography Team
National Institute of Standards and Technology (NIST)
NTU