IEEE SA
STANDARDS
ASSOCIATION

IEEE P1943 (deferred) QuNET/WG

POST-QUANTUM NETWORK SECURITY WORKING GROUP

Jonathan J. Attia & Ludovic Perret

WebEx – May 12, 2022 #0

IEEE

PARTICIPANTS HAVE A DUTY TO INFORM THE IEEE

08 June 2021 – Slide 1/4

Participants shall inform the IEEE (or cause the IEEE to be informed) of the identity of each holder of any potential Essential Patent Claims of which they are personally aware if the claims are owned or controlled by the participant or the entity the participant is from, employed by, or otherwise represents

- **Participants should inform the IEEE (or cause the IEEE to be informed) of the identity of any other holders of potential Essential Patent Claims**

Early identification of holders of potential Essential Patent Claims is encouraged

WAYS TO INFORM IEEE

08 June 2021 – Slide 2/4

- **Cause an LOA to be submitted to the IEEE SA (patcom@ieee.org); or**
- **Provide the chair of this group with the identity of the holder(s) of any and all such claims as soon as possible; or**
- **Speak up now and respond to this Call for Potentially Essential Patents**

If anyone in this meeting is personally aware of the holder of any patent claims that are potentially essential to implementation of the proposed standard(s) under consideration by this group and that are not already the subject of an Accepted Letter of Assurance, please respond at this time by providing relevant information to the WG Chair

OTHER GUIDELINES FOR IEEE WORKING GROUP MEETINGS

08 June 2021 – Slide 3/4

- **All IEEE SA standards meetings shall be conducted in compliance with all applicable laws, including antitrust and competition laws.**
  - Don’t discuss the interpretation, validity, or essentiality of patents/patent claims.
  - Don’t discuss specific license rates, terms, or conditions.
    - Relative costs of different technical approaches that include relative costs of patent licensing terms may be discussed in standards development meetings.
      - Technical considerations remain the primary focus.
  - Don’t discuss or engage in the fixing of product prices, allocation of customers, or division of sales markets.
  - Don’t discuss the status or substance of ongoing or threatened litigation.
  - Don’t be silent if inappropriate topics are discussed. Formally object to the discussion immediately.

For more details, see *IEEE SA Standards Board Operations Manual*, clause 5.3.10 and *Antitrust and Competition Policy: What You Need to Know* at http://standards.ieee.org/develop/policies/antitrust.pdf

PATENT-RELATED INFORMATION

08 June 2021 – Slide 4/4

- **The patent policy and the procedures used to execute that policy are documented in the:**
  - ***IEEE SA Standards Board Bylaws***
    (http://standards.ieee.org/develop/policies/bylaws/sect6-7.html#6)
  - ***IEEE SA Standards Board Operations Manual***
    (http://standards.ieee.org/develop/policies/opman/sect6.html#6.3)

Material about the patent policy is available at
http://standards.ieee.org/about/sasb/patcom/materials.html

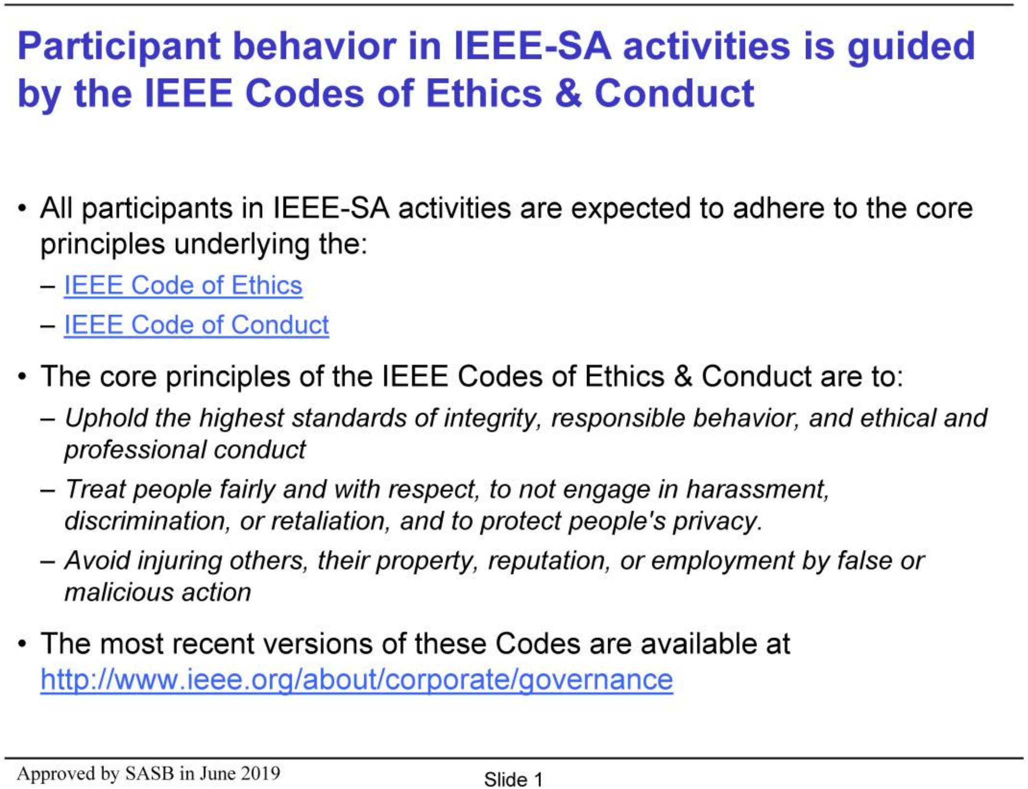
If you have questions, contact the IEEE SA Standards Board Patent Committee Administrator at patcom@ieee.org

IEEE SA COPYRIGHT POLICY

**By participating in this activity,
you agree to comply with the IEEE Code of Ethics,
all applicable laws, and all IEEE policies and procedures including,
but not limited to, the IEEE SA Copyright Policy.**

- Previously Published material (copyright assertion indicated) shall not be presented/submitted to the Working Group nor incorporated into a Working Group draft unless permission is granted.
- Prior to presentation or submission, you shall notify the Working Group Chair of previously Published material and should assist the Chair in obtaining copyright permission acceptable to IEEE SA.
- For material that is not previously Published, IEEE is automatically granted a license to use any material that is presented or submitted.

IEEE SA INDIVIDUAL WG PARTICIPANT BEHAVIOR



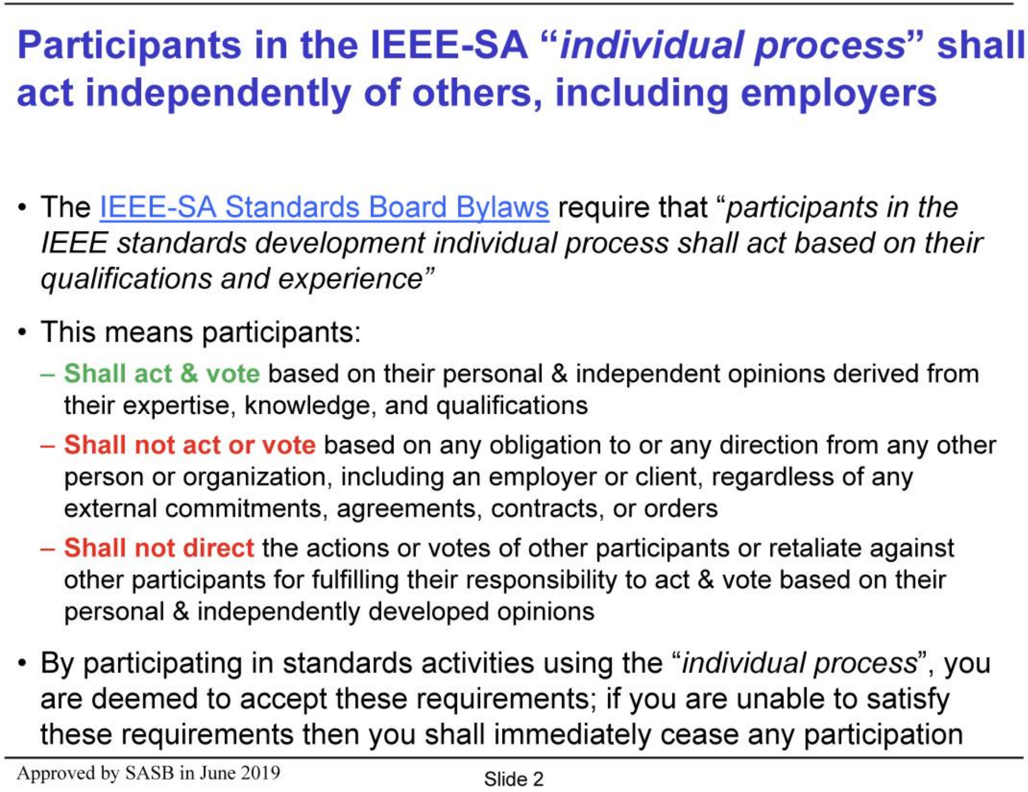
Participant behavior in IEEE-SA activities is guided by the IEEE Codes of Ethics & Conduct

- All participants in IEEE-SA activities are expected to adhere to the core principles underlying the:
  - IEEE Code of Ethics
  - IEEE Code of Conduct
- The core principles of the IEEE Codes of Ethics & Conduct are to:
  - *Uphold the highest standards of integrity, responsible behavior, and ethical and professional conduct*
  - *Treat people fairly and with respect, to not engage in harassment, discrimination, or retaliation, and to protect people's privacy.*
  - *Avoid injuring others, their property, reputation, or employment by false or malicious action*
- The most recent versions of these Codes are available at http://www.ieee.org/about/corporate/governance

Approved by SASB in June 2019

Slide 1

IEEE SA INDIVIDUAL WG PARTICIPANT BEHAVIOR



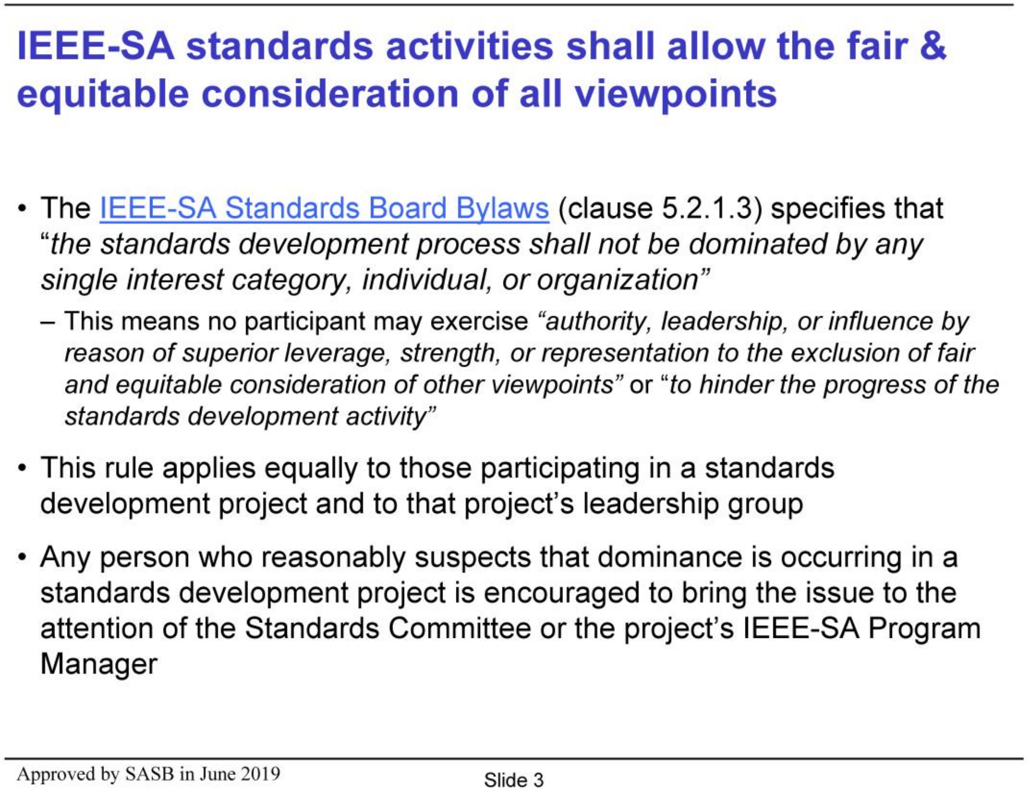
Participants in the IEEE-SA “*individual process*” shall act independently of others, including employers

- The IEEE-SA Standards Board Bylaws require that “*participants in the IEEE standards development individual process shall act based on their qualifications and experience*”
- This means participants:
  - **Shall act & vote** based on their personal & independent opinions derived from their expertise, knowledge, and qualifications
  - **Shall not act or vote** based on any obligation to or any direction from any other person or organization, including an employer or client, regardless of any external commitments, agreements, contracts, or orders
  - **Shall not direct** the actions or votes of other participants or retaliate against other participants for fulfilling their responsibility to act & vote based on their personal & independently developed opinions
- By participating in standards activities using the “*individual process*”, you are deemed to accept these requirements; if you are unable to satisfy these requirements then you shall immediately cease any participation

Approved by SASB in June 2019

Slide 2

IEEE SA INDIVIDUAL WG PARTICIPANT BEHAVIOR



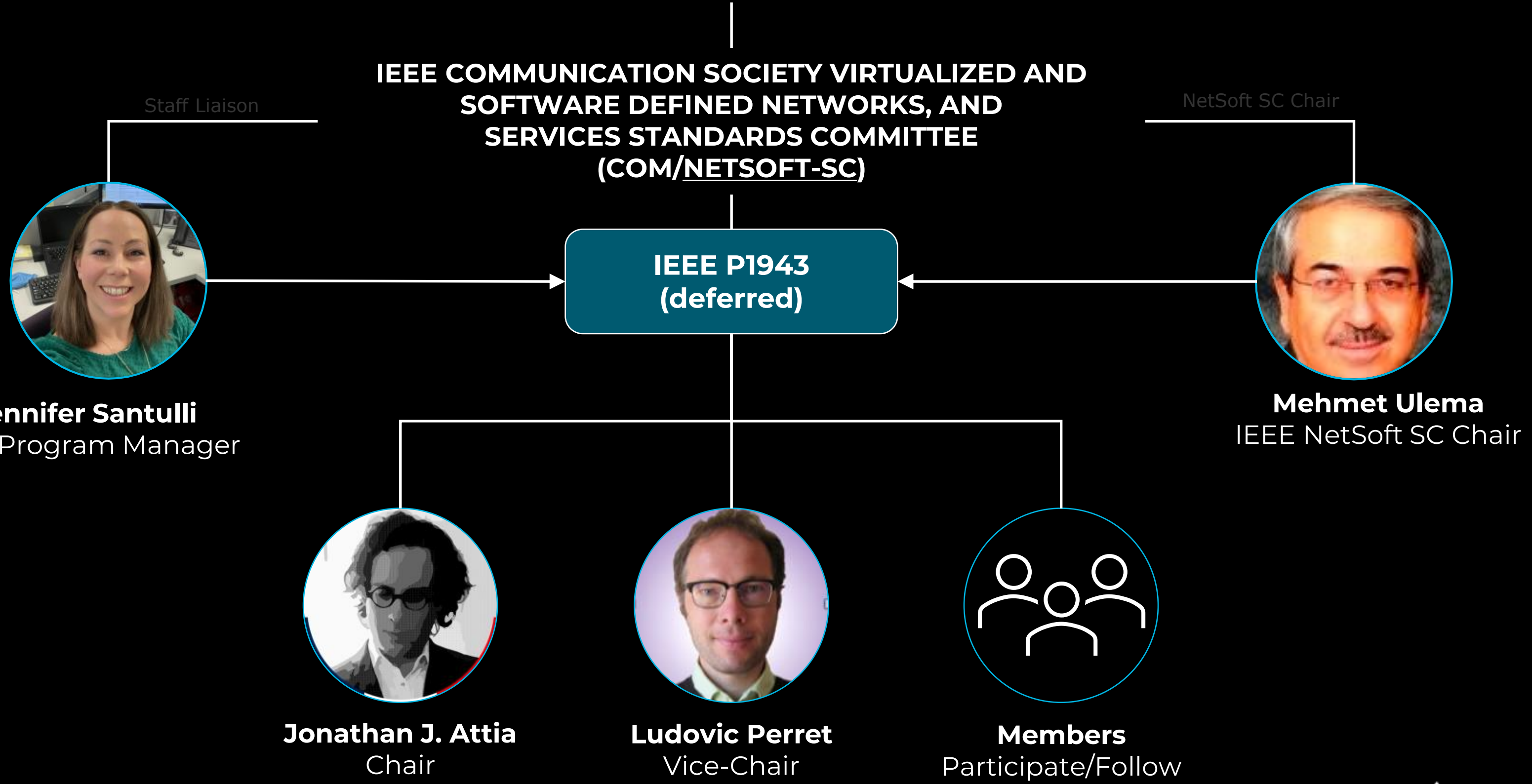
IEEE-SA standards activities shall allow the fair & equitable consideration of all viewpoints

- The IEEE-SA Standards Board Bylaws (clause 5.2.1.3) specifies that "*the standards development process shall not be dominated by any single interest category, individual, or organization*"
  - This means no participant may exercise "*authority, leadership, or influence by reason of superior leverage, strength, or representation to the exclusion of fair and equitable consideration of other viewpoints*" or "*to hinder the progress of the standards development activity*"
- This rule applies equally to those participating in a standards development project and to that project's leadership group
- Any person who reasonably suspects that dominance is occurring in a standards development project is encouraged to bring the issue to the attention of the Standards Committee or the project's IEEE-SA Program Manager

Approved by SASB in June 2019 Slide 3

ORGANIZATION PLAN

IEEE ComSoc
IEEE Communications Society



IEEE COMMUNICATION SOCIETY VIRTUALIZED AND SOFTWARE DEFINED NETWORKS, AND SERVICES STANDARDS COMMITTEE (COM/NETSOFT-SC)

Staff Liaison

NetSoft SC Chair

IEEE P1943 (deferred)

Jennifer Santulli
IEEE Program Manager

Mehmet Ulema
IEEE NetSoft SC Chair

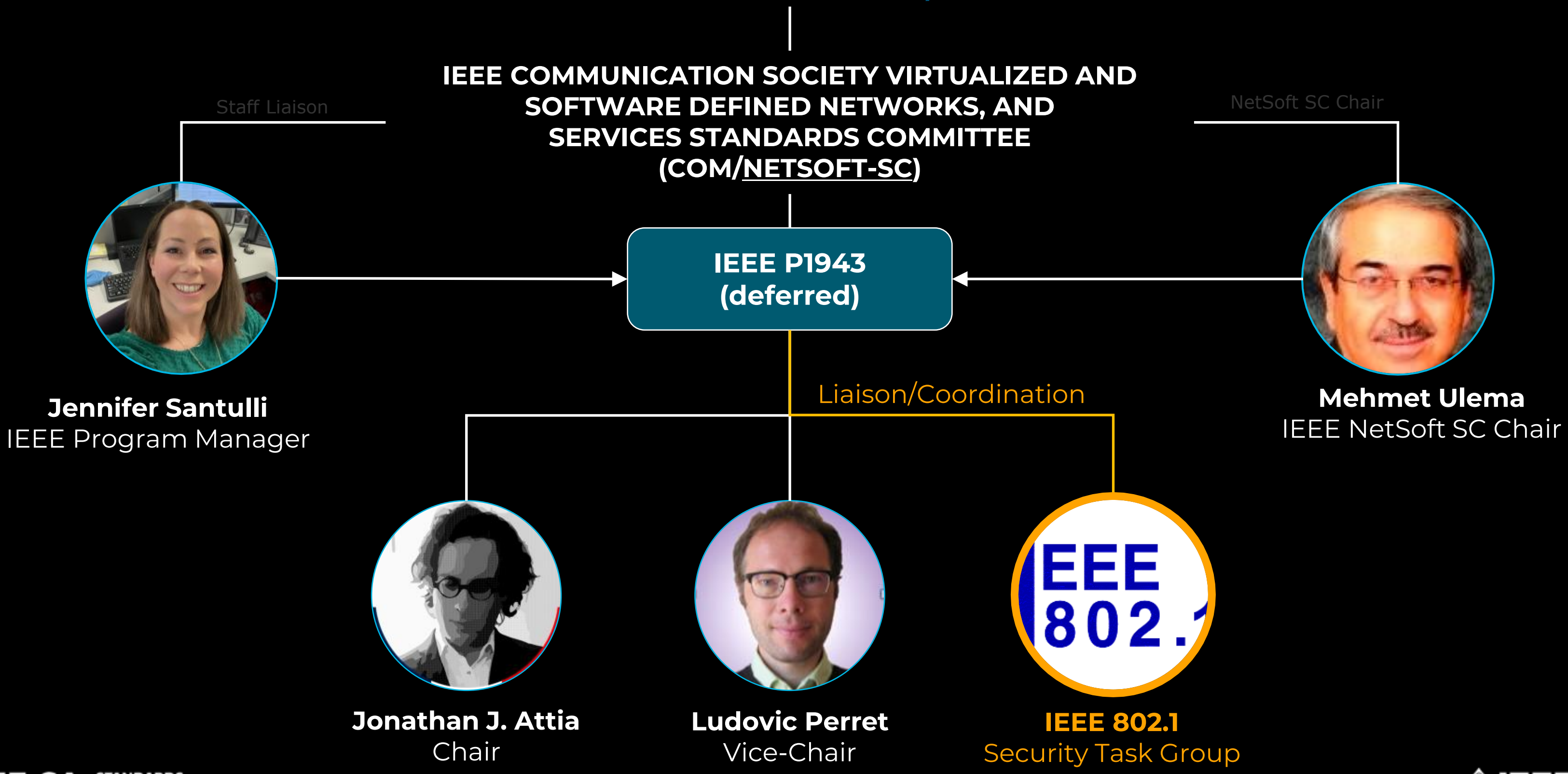
Jonathan J. Attia
Chair

Ludovic Perret
Vice-Chair

Members
Participate/Follow

ORGANIZATION PLAN

IEEE ComSoc
IEEE Communications Society



IEEE COMMUNICATION SOCIETY VIRTUALIZED AND SOFTWARE DEFINED NETWORKS, AND SERVICES STANDARDS COMMITTEE (COM/NETSOFT-SC)

Staff Liaison

NetSoft SC Chair

IEEE P1943 (deferred)

Liaison/Coordination

Jennifer Santulli
IEEE Program Manager

Mehmet Ulema
IEEE NetSoft SC Chair

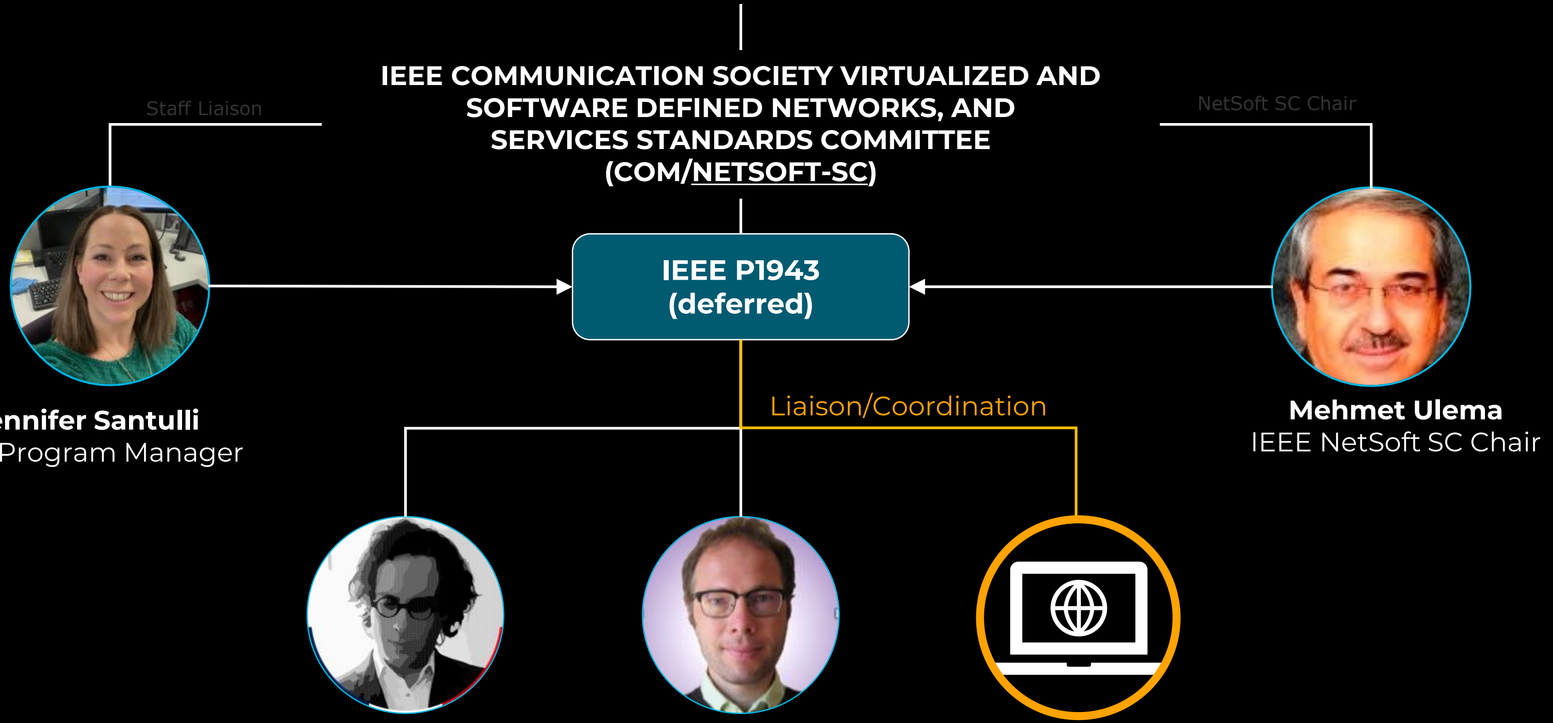
Jonathan J. Attia
Chair

Ludovic Perret
Vice-Chair

IEEE 802.1
Security Task Group

ORGANIZATION PLAN

IEEE ComSoc
IEEE Communications Society



IEEE COMMUNICATION SOCIETY VIRTUALIZED AND SOFTWARE DEFINED NETWORKS, AND SERVICES STANDARDS COMMITTEE (COM/NETSOFT-SC)

Staff Liaison

NetSoft SC Chair

IEEE P1943 (deferred)

Liaison/Coordination

Jennifer Santulli
IEEE Program Manager

Mehmet Ulema
IEEE NetSoft SC Chair

Jonathan J. Attia
Chair
(QIRG Member)

Ludovic Perret
Vice-Chair
(IETF Member)

IETF & IRTF
CFRG, LAMPS, TLS,
IPSECME, QIRG

FROM SHOR'S ALGORITHM TO MOSCA'S THEOREM

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor[†]

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

*A preliminary version of this paper appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20–22, 1994, IEEE Computer Society Press, pp. 124–134.

[†] AT&T Research, Room 2D-149, 600 Mountain Ave., Murray Hill, NJ 07974.

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2]

[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

We significantly reduce the cost of factoring integers and computing discrete logarithms in finite fields on a quantum computer by combining techniques from Shor 1994, Griffiths-Niu 1996, Zalka 2006, Fowler 2012, Ekerå-Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney-Fowler 2019, Gidney 2019. We estimate the approximate cost of our construction using plausible physical assumptions for large-scale superconducting qubit platforms: a planar grid of qubits with nearest-neighbor connectivity, a characteristic physical gate error rate of 10^{-3}, a surface code cycle time of 1 microsecond, and a reaction time of 10 microseconds. We account for factors that are normally ignored such as noise, the need to make repeated attempts, and the spacetime layout of the computation. When factoring 2048 bit RSA integers, our construction's spacetime volume is a hundredfold less than comparable estimates from earlier works (Van Meter et al. 2009, Jones et al. 2010, Fowler et al. 2012, Gheorghiu et al. 2019). In the abstract circuit model (which ignores overheads from distillation, routing, and error correction) our construction uses $3n + 0.002n \lg n$ logical qubits, $0.3n^3 + 0.0005n^3 \lg n$ Toffolis, and $500n^2 + n^2 \lg n$ measurement depth to factor n-bit RSA integers. We quantify the cryptographic implications of our work, both for RSA and for schemes based on the DLP in finite fields.

1 Introduction

Peter Shor's introduction in 1994 of polynomial time quantum algorithms for factoring integers and computing discrete logarithms [79, 89] was a historic milestone that greatly increased interest in quantum computing. Shor's algorithms were the first quantum algorithms that achieved a superpolynomial speedup over classical algorithms, applied to problems outside the field of quantum mechanics, and had obvious applications. In particular, Shor's algorithms may be used to break the RSA cryptosystem [73] based on the hardness of factoring integers that are the product of two similarly-sized primes (hereafter "RSA integers"), and cryptosystems based on the discrete logarithm problem (DLP), such as the Diffie-Hellman key agreement protocol [19] and the Digital Signature Algorithm [59].

The most expensive operation performed by Shor's factoring algorithm is a modular exponentiation. Modern classical computers can perform modular exponentiations on numbers with thousands of bits in under a second. These two facts may at first glance appear to suggest that factoring a thousand bit number with Shor's algorithm should only take seconds, but unfortunately (or perhaps fortunately), that is not the case. The modular exponentiation in Shor's algorithm is performed over a superposition of exponents, meaning a quantum computer is required, and quantum hardware is expected to be many orders of magnitude noisier than classical hardware [3, 48, 78]. This noise necessitates the use of error correction, which introduces overheads that ultimately make performing reliable arithmetic on a quantum computer many orders of magnitude more expensive than on classical computers [15, 28].

Craig Gidney: craiggidney@google.com

Accepted in Quantum 2021-03-29, click title to verify. Published under CC-BY 4.0.

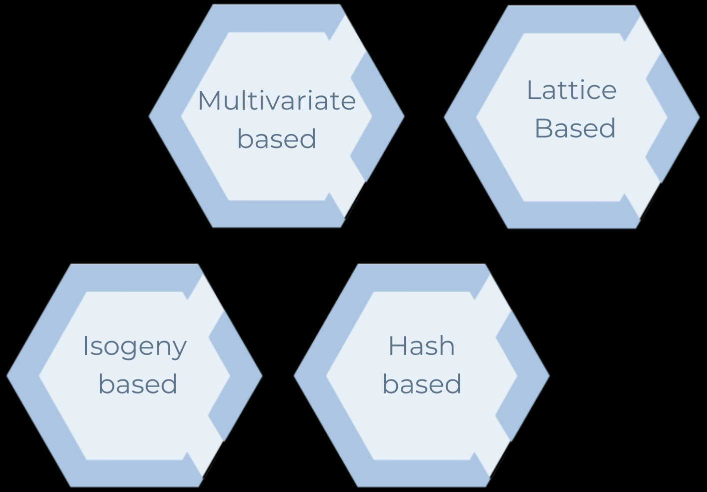
POST-QUANTUM CRYPTOGRAPHY

Current public-key cryptographic standards (RSA - ECC) are based on mathematical problems difficult to solve for classical computers but easy to solve for a quantum computer.

POST QUANTUM CRYPTOGRAPHY (PQC) : NEW HARDER QUANTUM-RESISTANT MATHEMATICAL PROBLEMS

Example : Multivariate cryptography → hard problem solving a system of non-linear equations

$$
\begin{aligned}
p^{(1)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)} \\
&\vdots \\
p^{(m)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}
\end{aligned}
$$



Multivariate based

Lattice Based

Isogeny based

Hash based

POST-QUANTUM CRYPTOGRAPHY

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

"Quantum risk is now simply too high and can no longer be ignored« , US NIST, 2016.

ON GOING PROCESS OF NEW QUANTUM RESISTANT CRYPTOGRAPHIC STANDARDS THROUGH NIST

Several cryptographic functions selected for standardization in 2022

NIST step 1 - 2016 - 2018

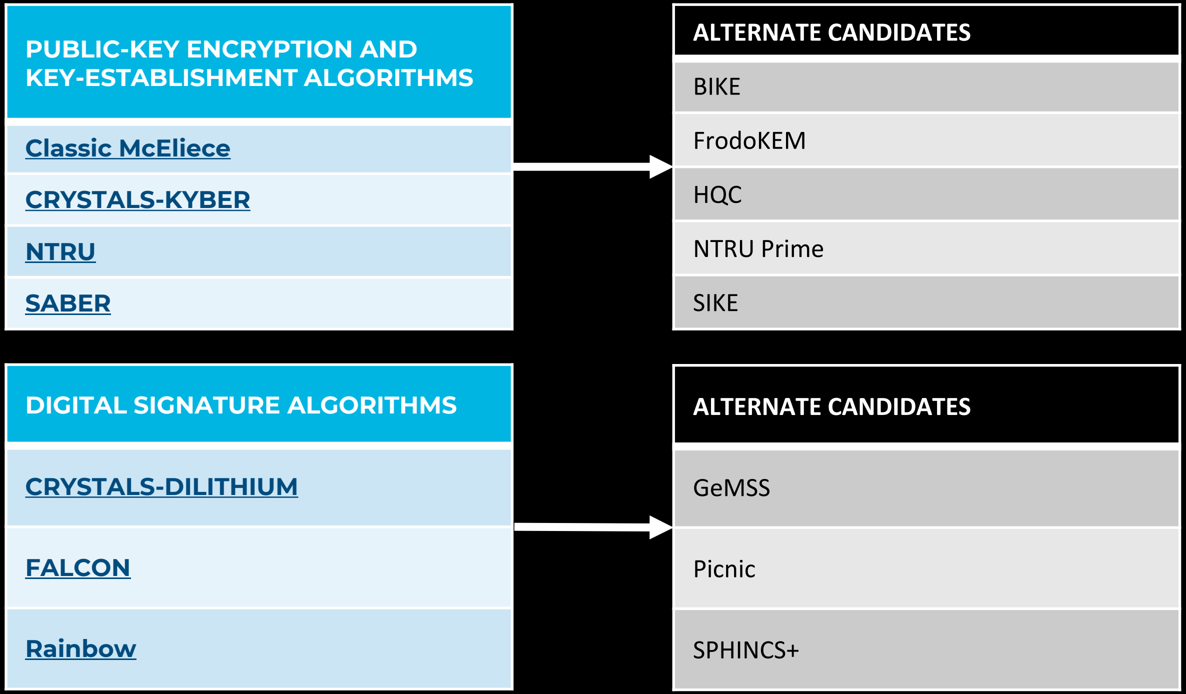
NIST step 2 - 2019 - 2020

NIST step 3 - Final - 2020 - 2022

NEW POST-QUANTUM VERSION OF PROTOCOLS NEED TO BE PROPOSED

afnor GROUPE ISO ETSI CENELEC IEEE SA STANDARDS ASSOCIATION IETF Accredited Standards Committee X9 Inc. Financial Industry Standards

Third Round Candidate Announcement (July 22, 2020)



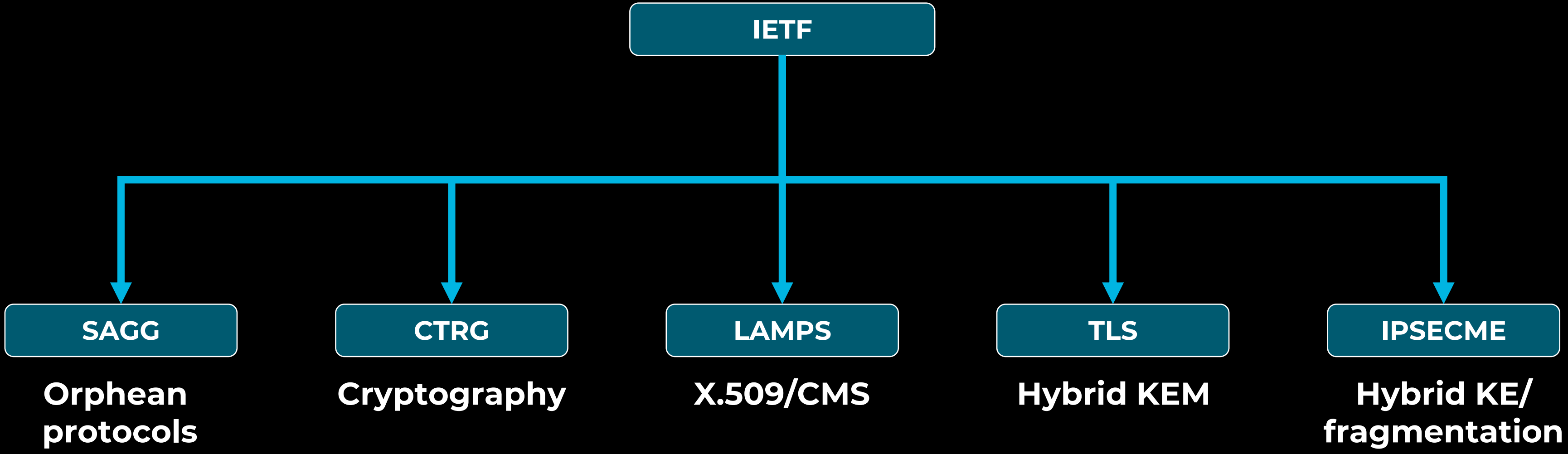
PUBLIC-KEY ENCRYPTION AND KEY-ESTABLISHMENT ALGORITHMS
Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

ALTERNATE CANDIDATES
BIKE
FrodoKEM
HQC
NTRU Prime
SIKE

DIGITAL SIGNATURE ALGORITHMS
CRYSTALS-DILITHIUM
FALCON
Rainbow

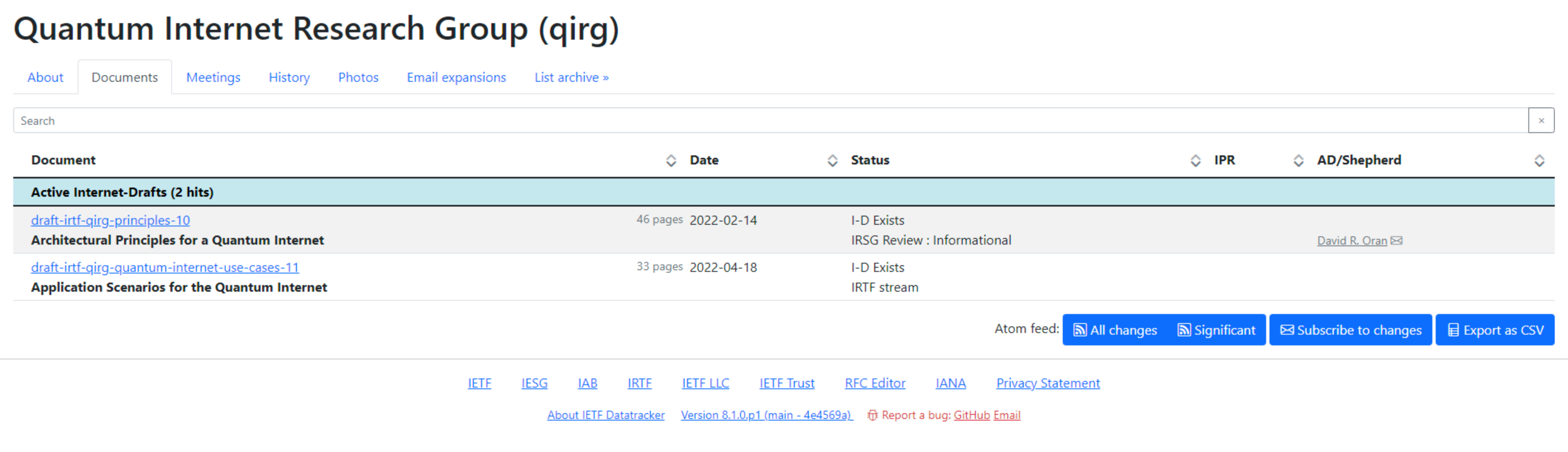
ALTERNATE CANDIDATES
GeMSS
Picnic
SPHINCS+

PQC@IETF (1/2)


IETF
SAGG
Orphean protocols
CTRG
Cryptography
LAMPS
X.509/CMS
TLS
Hybrid KEM
IPSECME
Hybrid KE/ fragmentation

PQC@IETF (2/2)

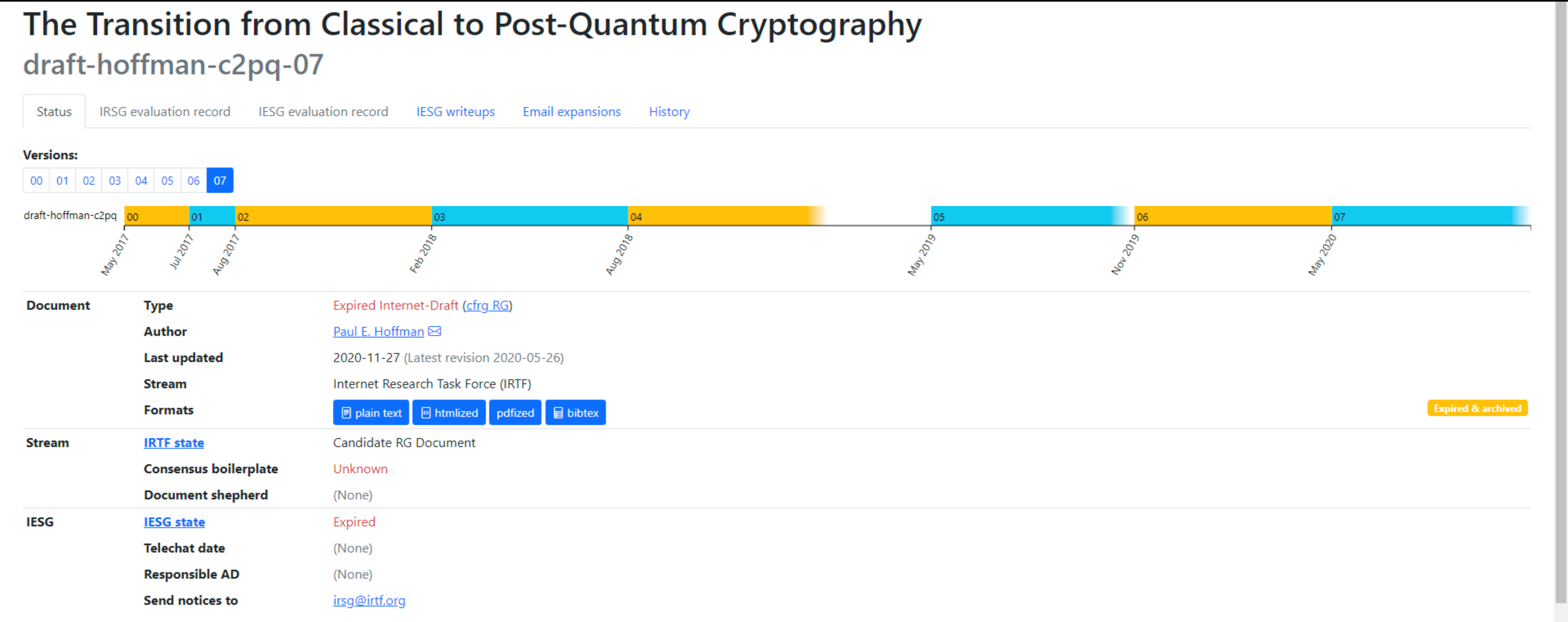
- ✓ Hybrid : post-quantum and classical
  - ✓ Gap : no standard for hybrid
- ✓ Global strategy
  - ✓ First step using a PSK
  - ✓ Second step hybrid KEM
  - ✓ Last step full post-quantum ! Authentication+Key-Exhange
    - ✓ Trend : KEM-based authentication (TLS)



Quantum Internet Research Group (qirg)

Document		Date	Status	IPR	AD/Shepherd
Active Internet-Drafts (2 hits)					
draft-irtf-qirg-principles-10 **Architectural Principles for a Quantum Internet**	46 pages	2022-02-14	I-D Exists IRSG Review : Informational		David R. Oran
draft-irtf-qirg-quantum-internet-use-cases-11 **Application Scenarios for the Quantum Internet**	33 pages	2022-04-18	I-D Exists IRTF stream		

Atom feed:



The Transition from Classical to Post-Quantum Cryptography

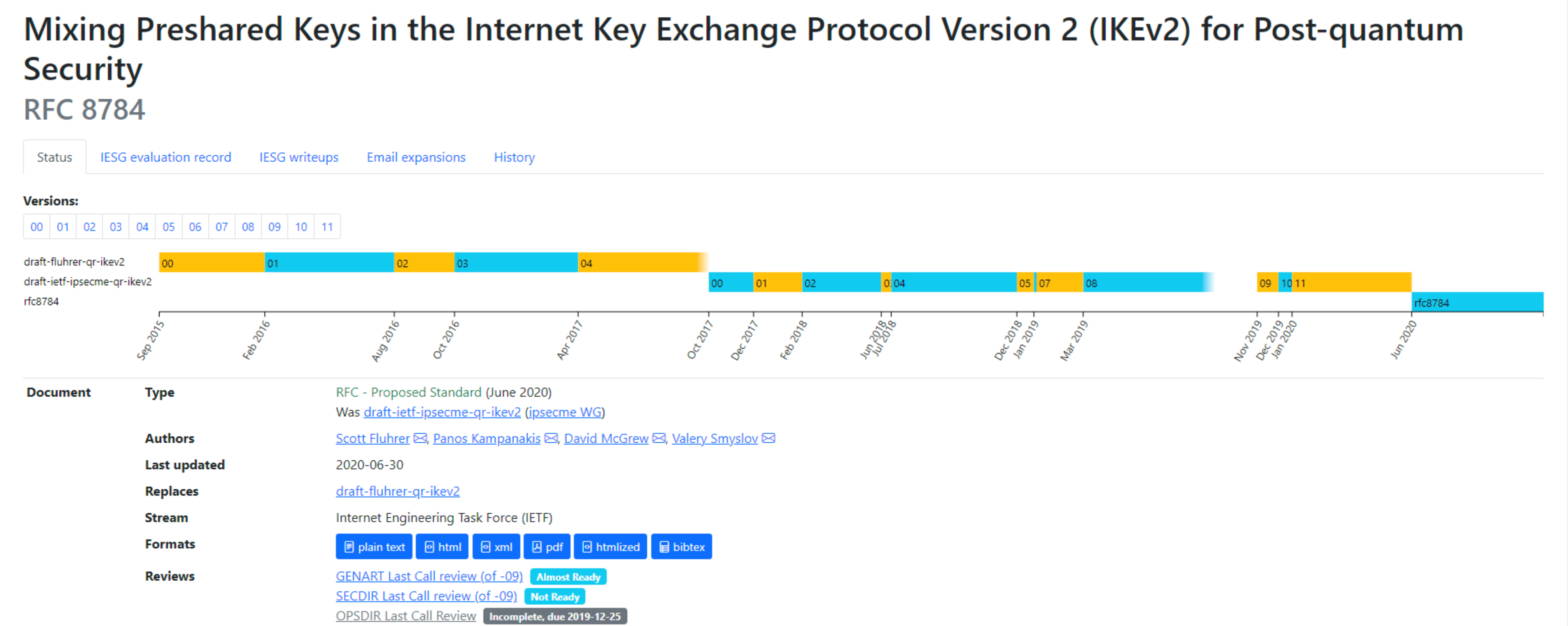
draft-hoffman-c2pq-07

Versions:

00 01 02 03 04 05 06 07

Document	**Type**	Expired Internet-Draft (cfrg RG)
	Author	Paul E. Hoffman ✉
	Last updated	2020-11-27 (Latest revision 2020-05-26)
	Stream	Internet Research Task Force (IRTF)
	Formats	plain text htmlized pdfized bibtex
Stream	**IRTF state**	Candidate RG Document
	Consensus boilerplate	Unknown
	Document shepherd	(None)
IESG	**IESG state**	Expired
	Telechat date	(None)
	Responsible AD	(None)
	Send notices to	irsg@irtf.org

Expired & archived

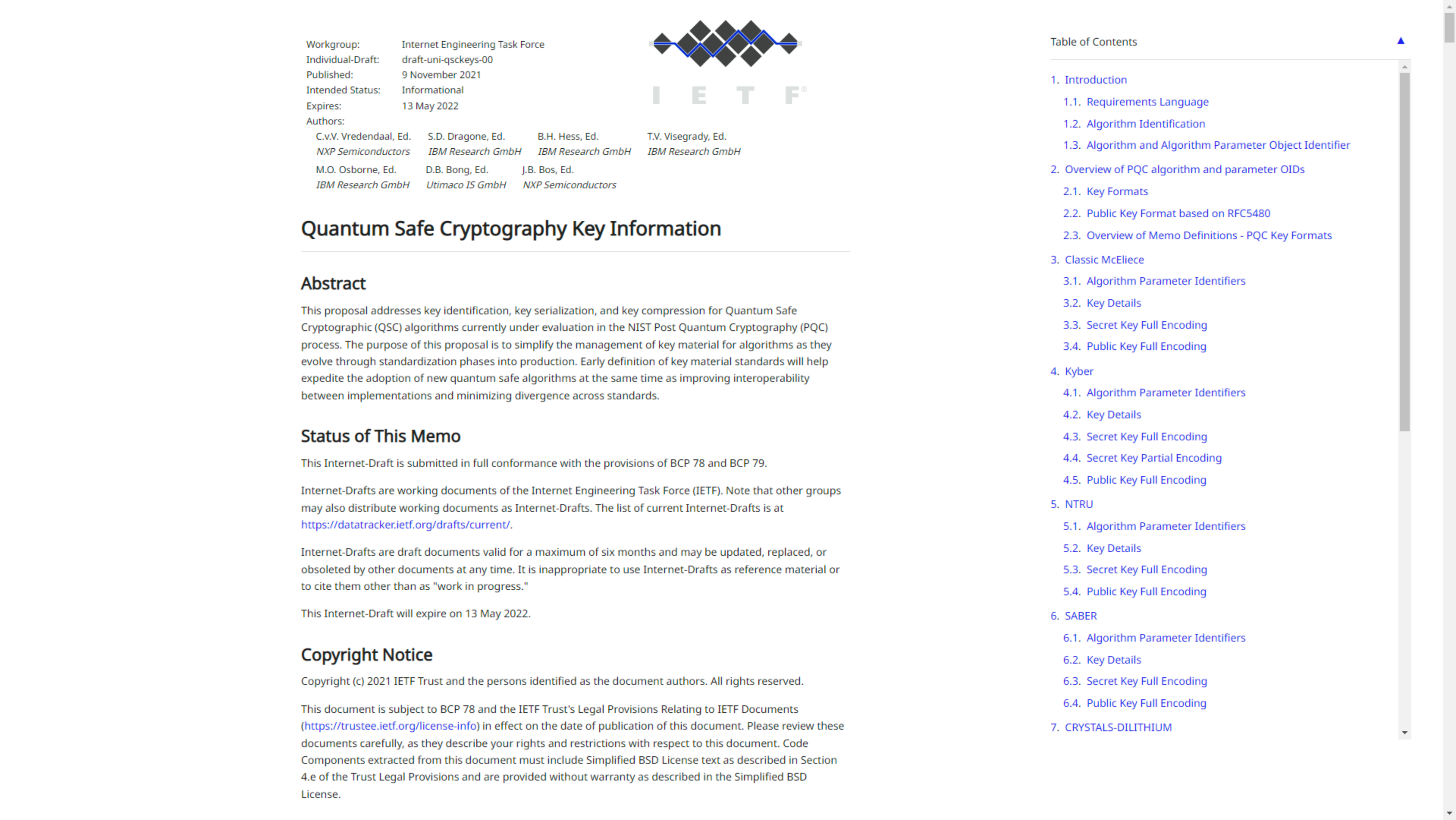


Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

RFC 8784

Versions:

Document		
	Type	RFC - Proposed Standard (June 2020) Was draft-ietf-ipsecme-qr-ikev2 (ipsecme WG)
	Authors	Scott Fluhrer ✉, Panos Kampanakis ✉, David McGrew ✉, Valery Smyslov ✉
	Last updated	2020-06-30
	Replaces	draft-fluhrer-qr-ikev2
	Stream	Internet Engineering Task Force (IETF)
	Formats	plain text · html · xml · pdf · htmlized · bibtex
	Reviews	GENART Last Call review (of -09) Almost Ready SECDIR Last Call review (of -09) Not Ready OPSDIR Last Call Review Incomplete, due 2019-12-25



Workgroup: Internet Engineering Task Force
Individual-Draft: draft-uni-qsckeys-00
Published: 9 November 2021
Intended Status: Informational
Expires: 13 May 2022

Authors:
C.v.V. Vredendaal, Ed. *NXP Semiconductors*
S.D. Dragone, Ed. *IBM Research GmbH*
B.H. Hess, Ed. *IBM Research GmbH*
T.V. Visegrady, Ed. *IBM Research GmbH*
M.O. Osborne, Ed. *IBM Research GmbH*
D.B. Bong, Ed. *Utimaco IS GmbH*
J.B. Bos, Ed. *NXP Semiconductors*

Quantum Safe Cryptography Key Information

Abstract

This proposal addresses key identification, key serialization, and key compression for Quantum Safe Cryptographic (QSC) algorithms currently under evaluation in the NIST Post Quantum Cryptography (PQC) process. The purpose of this proposal is to simplify the management of key material for algorithms as they evolve through standardization phases into production. Early definition of key material standards will help expedite the adoption of new quantum safe algorithms at the same time as improving interoperability between implementations and minimizing divergence across standards.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

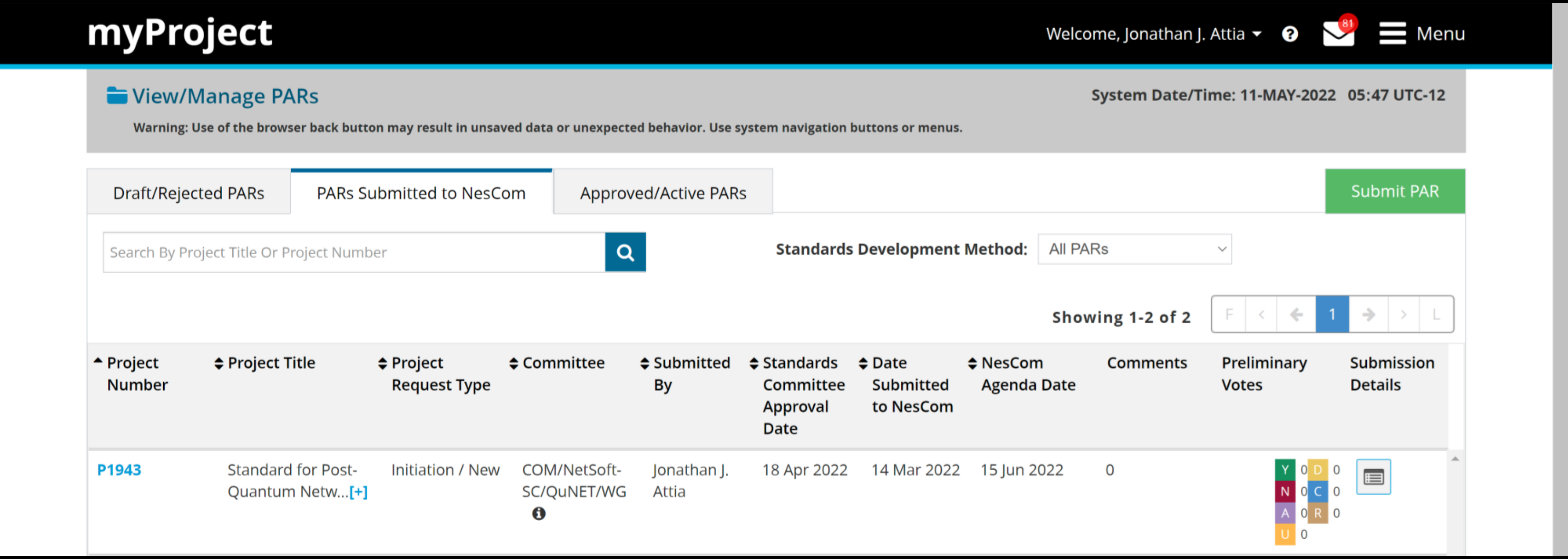
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 13 May 2022.

Copyright Notice

Table of Contents



View/Manage PARs

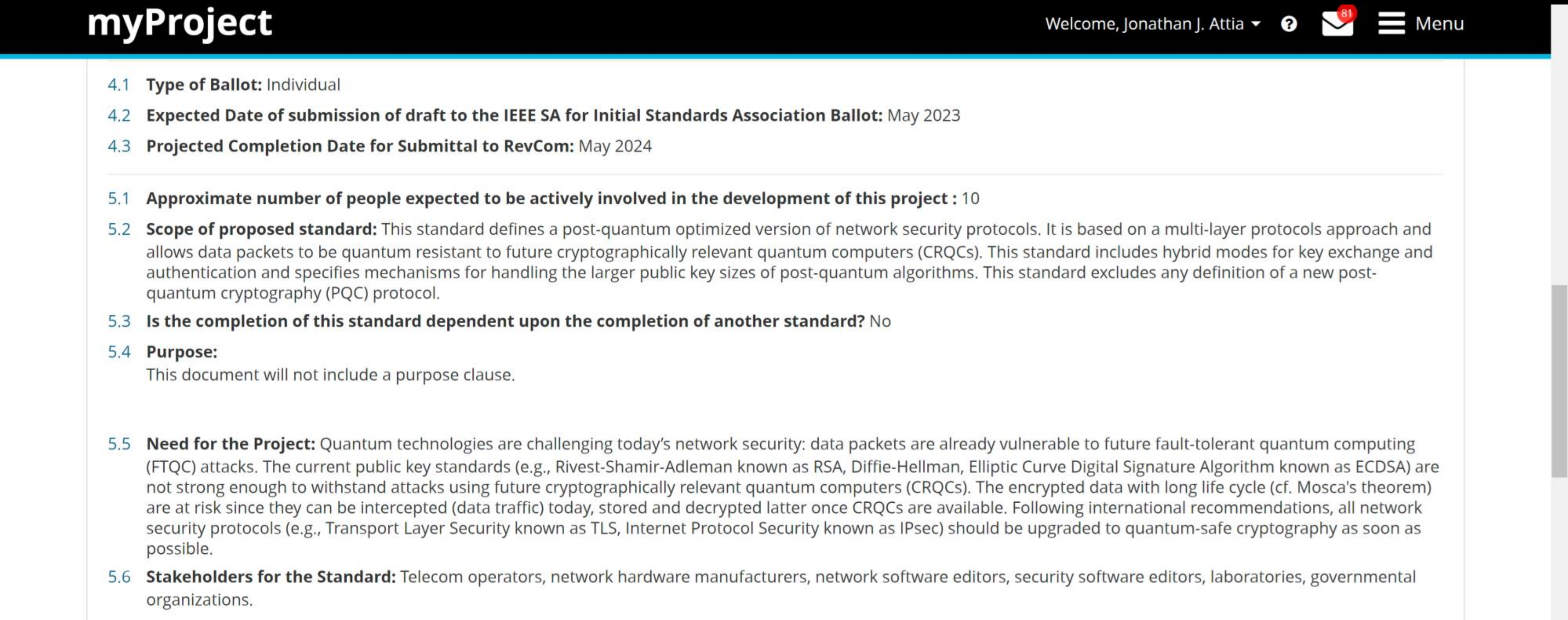
System Date/Time: 11-MAY-2022 05:47 UTC-12

Warning: Use of the browser back button may result in unsaved data or unexpected behavior. Use system navigation buttons or menus.

Standards Development Method: All PARs

Showing 1-2 of 2

Project Number	Project Title	Project Request Type	Committee	Submitted By	Standards Committee Approval Date	Date Submitted to NesCom	NesCom Agenda Date	Comments	Preliminary Votes	Submission Details
P1943	Standard for Post-Quantum Netw...[+]	Initiation / New	COM/NetSoft-SC/QuNET/WG	Jonathan J. Attia	18 Apr 2022	14 Mar 2022	15 Jun 2022	0	Y 0 D 0 N 0 C 0 A 0 R 0 U 0	



4.1 **Type of Ballot:** Individual

4.2 **Expected Date of submission of draft to the IEEE SA for Initial Standards Association Ballot:** May 2023

4.3 **Projected Completion Date for Submittal to RevCom:** May 2024

5.1 **Approximate number of people expected to be actively involved in the development of this project :** 10

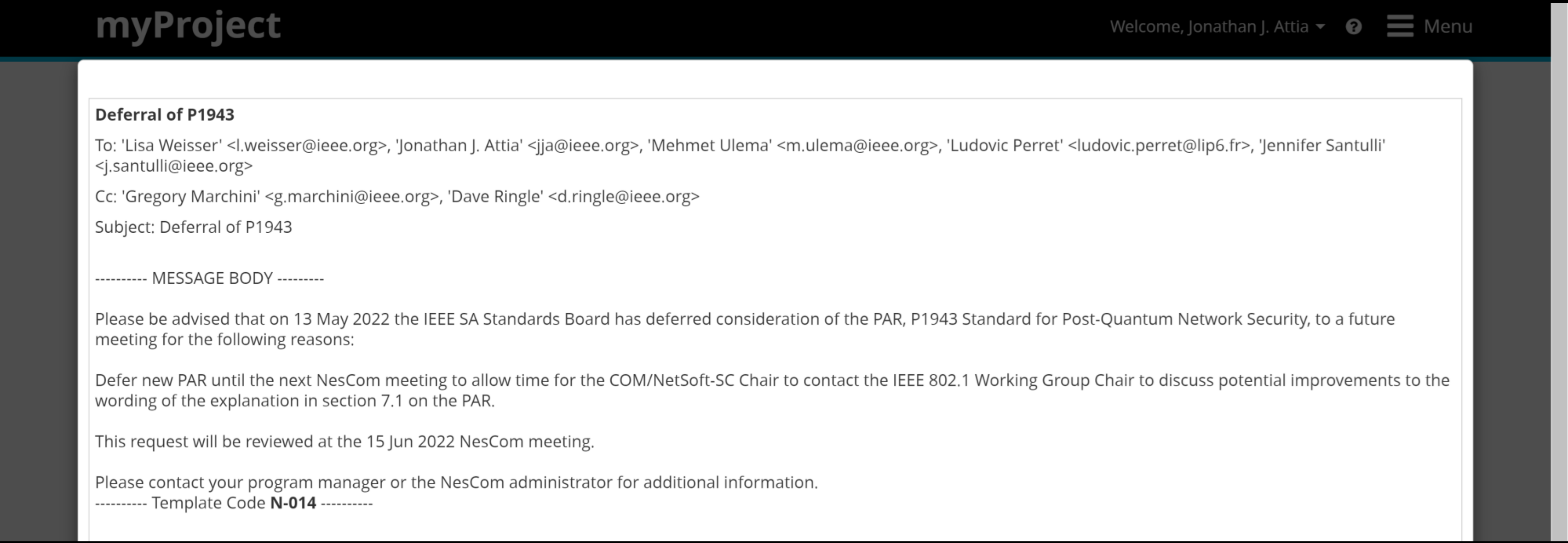
5.2 **Scope of proposed standard:** This standard defines a post-quantum optimized version of network security protocols. It is based on a multi-layer protocols approach and allows data packets to be quantum resistant to future cryptographically relevant quantum computers (CRQCs). This standard includes hybrid modes for key exchange and authentication and specifies mechanisms for handling the larger public key sizes of post-quantum algorithms. This standard excludes any definition of a new post-quantum cryptography (PQC) protocol.

5.3 **Is the completion of this standard dependent upon the completion of another standard?** No

5.4 **Purpose:**
This document will not include a purpose clause.

5.5 **Need for the Project:** Quantum technologies are challenging today's network security: data packets are already vulnerable to future fault-tolerant quantum computing (FTQC) attacks. The current public key standards (e.g., Rivest-Shamir-Adleman known as RSA, Diffie-Hellman, Elliptic Curve Digital Signature Algorithm known as ECDSA) are not strong enough to withstand attacks using future cryptographically relevant quantum computers (CRQCs). The encrypted data with long life cycle (cf. Mosca's theorem) are at risk since they can be intercepted (data traffic) today, stored and decrypted latter once CRQCs are available. Following international recommendations, all network security protocols (e.g., Transport Layer Security known as TLS, Internet Protocol Security known as IPsec) should be upgraded to quantum-safe cryptography as soon as possible.

5.6 **Stakeholders for the Standard:** Telecom operators, network hardware manufacturers, network software editors, security software editors, laboratories, governmental organizations.



Deferral of P1943

To: 'Lisa Weisser' <l.weisser@ieee.org>, 'Jonathan J. Attia' <jja@ieee.org>, 'Mehmet Ulema' <m.ulema@ieee.org>, 'Ludovic Perret' <ludovic.perret@lip6.fr>, 'Jennifer Santulli' <j.santulli@ieee.org>

Cc: 'Gregory Marchini' <g.marchini@ieee.org>, 'Dave Ringle' <d.ringle@ieee.org>

Subject: Deferral of P1943

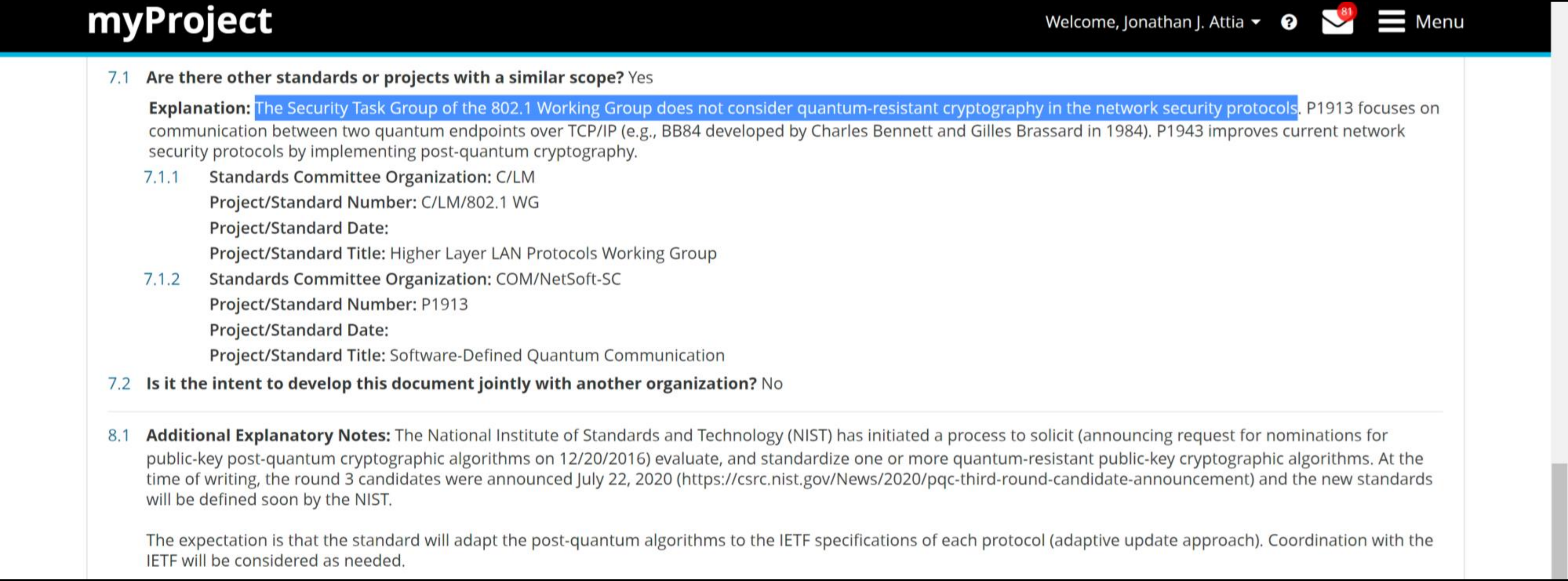
---------- MESSAGE BODY ---------

Please be advised that on 13 May 2022 the IEEE SA Standards Board has deferred consideration of the PAR, P1943 Standard for Post-Quantum Network Security, to a future meeting for the following reasons:

Defer new PAR until the next NesCom meeting to allow time for the COM/NetSoft-SC Chair to contact the IEEE 802.1 Working Group Chair to discuss potential improvements to the wording of the explanation in section 7.1 on the PAR.

This request will be reviewed at the 15 Jun 2022 NesCom meeting.

Please contact your program manager or the NesCom administrator for additional information.
---------- Template Code **N-014** ----------



7.1 **Are there other standards or projects with a similar scope?** Yes

Explanation: The Security Task Group of the 802.1 Working Group does not consider quantum-resistant cryptography in the network security protocols. P1913 focuses on communication between two quantum endpoints over TCP/IP (e.g., BB84 developed by Charles Bennett and Gilles Brassard in 1984). P1943 improves current network security protocols by implementing post-quantum cryptography.

7.1.1 **Standards Committee Organization:** C/LM
Project/Standard Number: C/LM/802.1 WG
Project/Standard Date:
Project/Standard Title: Higher Layer LAN Protocols Working Group

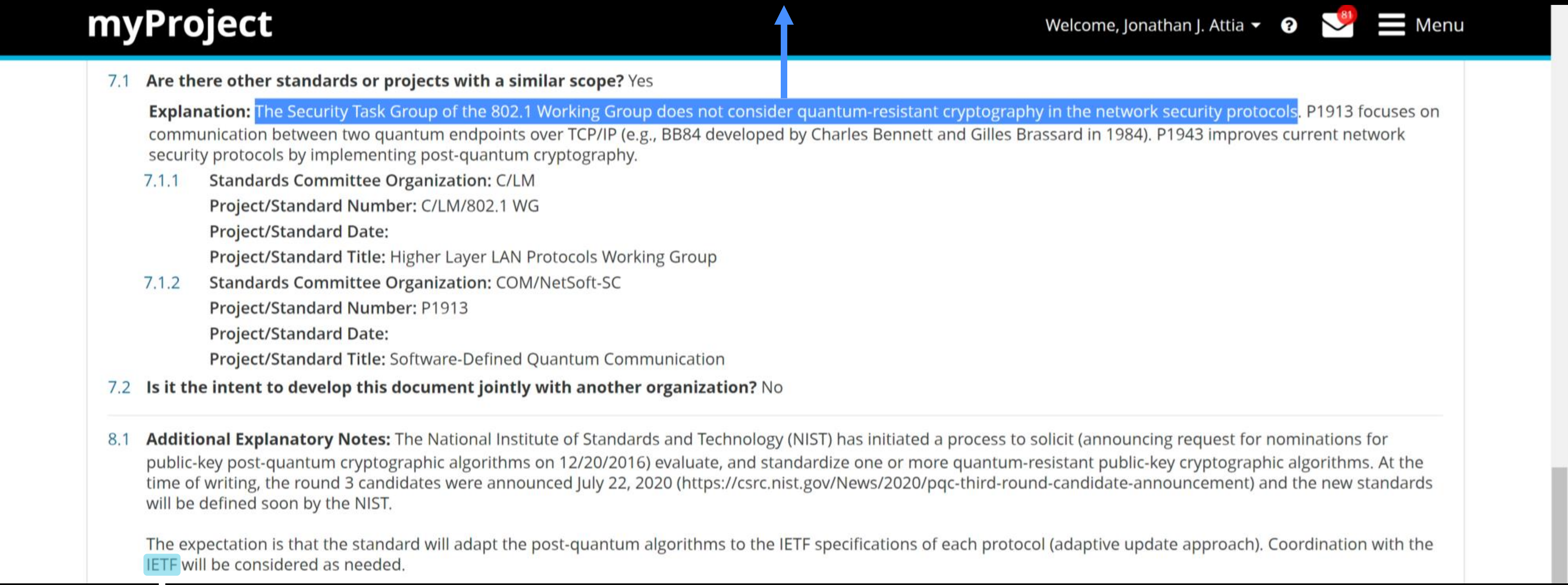
7.1.2 **Standards Committee Organization:** COM/NetSoft-SC
Project/Standard Number: P1913
Project/Standard Date:
Project/Standard Title: Software-Defined Quantum Communication

7.2 **Is it the intent to develop this document jointly with another organization?** No

8.1 **Additional Explanatory Notes:** The National Institute of Standards and Technology (NIST) has initiated a process to solicit (announcing request for nominations for public-key post-quantum cryptographic algorithms on 12/20/2016) evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. At the time of writing, the round 3 candidates were announced July 22, 2020 (https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement) and the new standards will be defined soon by the NIST.

The expectation is that the standard will adapt the post-quantum algorithms to the IETF specifications of each protocol (adaptive update approach). Coordination with the IETF will be considered as needed.

The Security Task Group of the 802.1 WG considers the PQC for MACsec (Media Access Control Security): MKA (MACsec Key Agreement) and EAP (Extended Authentication Protocol). A coordination is already initiated and needed between 802.1 WG and P1943.



7.1 **Are there other standards or projects with a similar scope?** Yes

Explanation: The Security Task Group of the 802.1 Working Group does not consider quantum-resistant cryptography in the network security protocols. P1913 focuses on communication between two quantum endpoints over TCP/IP (e.g., BB84 developed by Charles Bennett and Gilles Brassard in 1984). P1943 improves current network security protocols by implementing post-quantum cryptography.

7.1.1 **Standards Committee Organization:** C/LM
Project/Standard Number: C/LM/802.1 WG
Project/Standard Date:
Project/Standard Title: Higher Layer LAN Protocols Working Group

7.1.2 **Standards Committee Organization:** COM/NetSoft-SC
Project/Standard Number: P1913
Project/Standard Date:
Project/Standard Title: Software-Defined Quantum Communication

7.2 **Is it the intent to develop this document jointly with another organization?** No

8.1 **Additional Explanatory Notes:** The National Institute of Standards and Technology (NIST) has initiated a process to solicit (announcing request for nominations for public-key post-quantum cryptographic algorithms on 12/20/2016) evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. At the time of writing, the round 3 candidates were announced July 22, 2020 (https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement) and the new standards will be defined soon by the NIST.

The expectation is that the standard will adapt the post-quantum algorithms to the IETF specifications of each protocol (adaptive update approach). Coordination with the IETF will be considered as needed.

IETF (Internet Engineering Task Force)/IRTF (Internet Research Task Force)

TOWARDS POST-QUANTUM MACSEC

Configuring Post-Quantum MACsec in Cisco Switches

Summary

A quantum computer could break essentially all of the public key cryptography standards in use today: RSA, Diffie-Helman (DH), and Elliptic Curve Diffie-Hellman (ECDH). Since these algorithms are widely used for key exchange in various encryption protocols, a quantum computer could threaten data encryption protocols of today. Someone could store encrypted communications today and decrypt them later, if, and when, a quantum computer was available. In this whitepaper, we discuss the quantum-resistance of MACsec, which is standard for authenticating and encrypting packets between two MAC-layer, directly connected devices. We explain how quantum-resistant MACsec can be deployed in Cisco routers today, and further enhancements that can be made to improve the protocol's quantum-resistance.

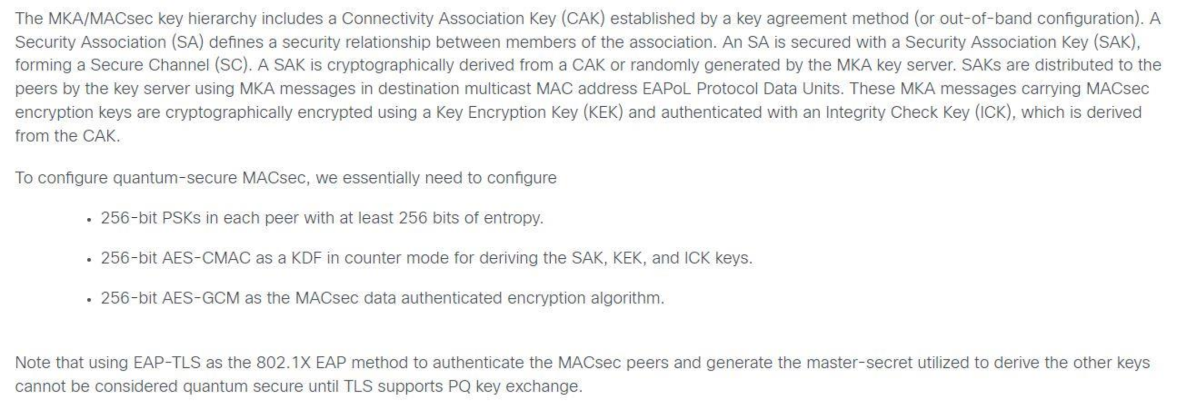
Contents

Using a Pre-Shared Key

Security

Post-quantum MACsec in Cisco switches

Panos Kampanakis



The MKA/MACsec key hierarchy includes a Connectivity Association Key (CAK) established by a key agreement method (or out-of-band configuration). A Security Association (SA) defines a security relationship between members of the association. An SA is secured with a Security Association Key (SAK), forming a Secure Channel (SC). A SAK is cryptographically derived from a CAK or randomly generated by the MKA key server. SAKs are distributed to the peers by the key server using MKA messages in destination multicast MAC address EAPoL Protocol Data Units. These MKA messages carrying MACsec encryption keys are cryptographically encrypted using a Key Encryption Key (KEK) and authenticated with an Integrity Check Key (ICK), which is derived from the CAK.

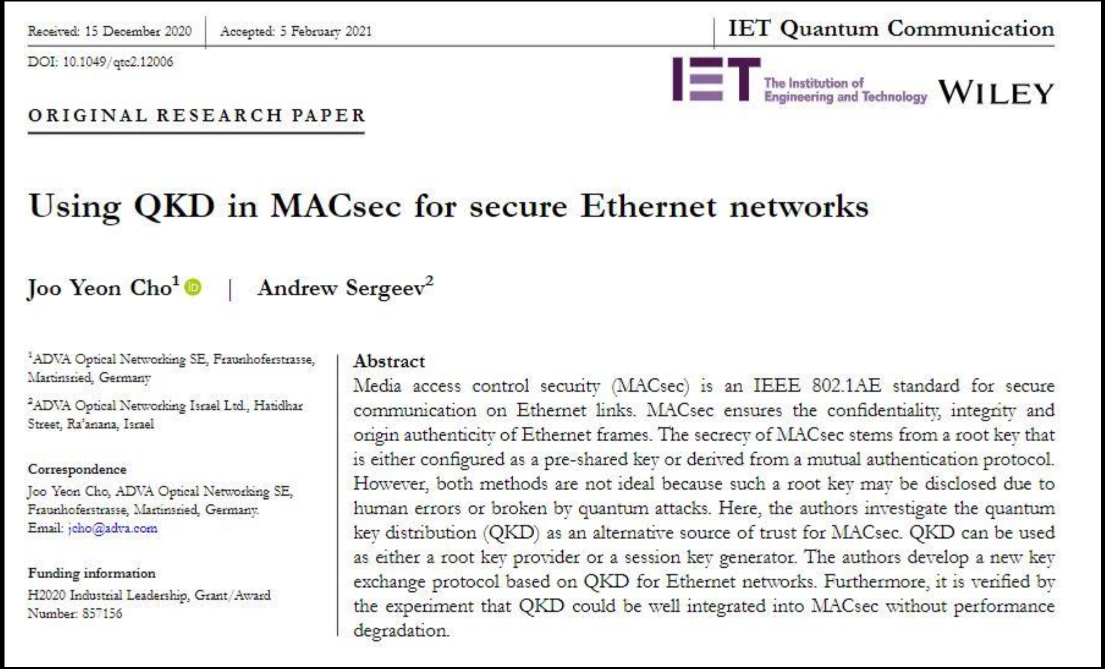
To configure quantum-secure MACsec, we essentially need to configure

- 256-bit PSKs in each peer with at least 256 bits of entropy.
- 256-bit AES-CMAC as a KDF in counter mode for deriving the SAK, KEK, and ICK keys.
- 256-bit AES-GCM as the MACsec data authenticated encryption algorithm.

Note that using EAP-TLS as the 802.1X EAP method to authenticate the MACsec peers and generate the master-secret utilized to derive the other keys cannot be considered quantum secure until TLS supports PQ key exchange.

TOWARDS POST-QUANTUM MACSEC

Using QKD to secure MacSec



Received: 15 December 2020 | Accepted: 5 February 2021

IET Quantum Communication

DOI: 10.1049/qtc2.12006

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH PAPER

Using QKD in MACsec for secure Ethernet networks

Joo Yeon Cho[1] | Andrew Sergeev[2]

[1] ADVA Optical Networking SE, Fraunhoferstrasse, Martinsried, Germany

[2] ADVA Optical Networking Israel Ltd., Hatidhar Street, Ra'anana, Israel

Correspondence

Joo Yeon Cho, ADVA Optical Networking SE, Fraunhoferstrasse, Martinsried, Germany.
Email: jcho@adva.com

Funding information

H2020 Industrial Leadership, Grant/Award Number: 857156

Abstract

Media access control security (MACsec) is an IEEE 802.1AE standard for secure communication on Ethernet links. MACsec ensures the confidentiality, integrity and origin authenticity of Ethernet frames. The secrecy of MACsec stems from a root key that is either configured as a pre-shared key or derived from a mutual authentication protocol. However, both methods are not ideal because such a root key may be disclosed due to human errors or broken by quantum attacks. Here, the authors investigate the quantum key distribution (QKD) as an alternative source of trust for MACsec. QKD can be used as either a root key provider or a session key generator. The authors develop a new key exchange protocol based on QKD for Ethernet networks. Furthermore, it is verified by the experiment that QKD could be well integrated into MACsec without performance degradation.

DURING THIS MEETING

- NIST Standards are coming soon
- IETFs protocols are being adapted
- Proposals already exist for pqMACsec
- Need for unification of transition methods and hybrid architecture

FOR THE NEXT WG MEETING

- Join the 802.1 WG as a Member
- Set up a liaison between 802.1 WG and P1943