IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PQC SG 21 April 2025 Teleconference Meeting Minutes | | | | |
| Date: 2025-04-25 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Alex Lungu | SAMSUNG | OCS, CB4 0AE, U.K. | +44 1223 434600 | da.lungu@samsung.com |

Abstract

This document containes the minutes for the PQC SG teleconference that took place on the 21st of April 2025.

# 

1. The Chair, Stephen Orr (Cisco), calls the meeting to order at 09:31 ET.
2. Chair provides reminders:
   1. Please record your attendance during the session by using the IMAT system.
   2. No recordings are allowed.
   3. Please use the mute function unless addressing the group.
   4. Please announce your affiliation when you first address the group during a meeting slot.
3. Policy and procedures

Chair informs that participants have a duty to inform the IEEE 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 also inform the IEEE (or cause the IEEE to be informed) of the identity of any other holders of potential Essential Patent Claims.

**Nobody speaks up.**

1. Chair presents:
   1. Patent-related information.
   2. IEEE SA Copyright Policy. Chair requests the secretary to ensure the presentation of the **Copyright Policy** is minuted.
   3. Other guidelines for IEEE WG meetings.
   4. Participant behavior in IEEE-SA activities is guided by the IEEE Codes of Ethics & Conduct
   5. Participants in the IEEE-SA “individual process” shall act independently of others, including employers.
   6. IEEE-SA standards activities shall allow the fair & equitable consideration of all viewpoints.
2. For documentation the “PQC SG” repository in <http://mentor.ieee.org> shall be used for submissions.
3. Meeting minutes for the previous meeting can be found at [11-25/0642r0](https://mentor.ieee.org/802.11/dcn/25/11-25-0642-00-0PQC-pqc-sg-07-april-2025-teleconference-meeting-minutes.docx).
   1. Meeting minutes approved with unanimous consent.
4. Agenda for the meeting can be found at [11-25/0671r0](https://mentor.ieee.org/802.11/dcn/25/11-25-0671-00-0PQC-pqc-sg-agenda-04-21-2025.pptx).
   1. Agenda approved with unanimous consent.
5. Meeting plan
   1. 2 meeting time slots are planned for face to face meetings in Warsaw
6. View on PQC - [11-25/0528r1](https://mentor.ieee.org/802.11/dcn/25/11-25-0528-01-0PQC-view-on-pqc.pptx)
   1. Question on the work envisioned to allow supporting legacy devices: will PQC not be transparent to legacy devices by default as it will use an AKM unknown to these devices?
      1. To be considered off-line.
   2. Question on hybrid algorithms: don’t these algorithms cover both PQC and classic cryptography and thus remain incompatible with legacy devices?
      1. To be considered off-line. There is a backwards-compatibility concern, but this needs to be re-considered.
7. PQC Draft proposed PAR - [11-25/0597r1](https://mentor.ieee.org/802.11/dcn/25/11-25-0597-01-0PQC-pqc-draft-proposed-par.docx)
   1. Changes done to incorporate feedback provided before the meeting were presented.
   2. Some comments received off-line were conflicting between themselves.
   3. Question on the addition of point e) to section 5.2.b.
      1. There was a conflicting comment during the last meeting that this text could be added to section 8.1.
      2. Text was added to section 5.2.b.
   4. Comment on moving the “symmetric” keyword from section 5.2.b, point d).
      1. The intent is to leave a door open so we can update multiple handshakes, as the group doesn’t need to fulfil everything in scope.
      2. The scope remains quite limited regardless of how wide point d) leaves us.
      3. The conclusion was to remove the keyword.
   5. Question on section 5.2.b: Does point e) of cover work done by the 11bc group, or does another point cover it?
      1. This should be resolved / the PAR should be open to this.
      2. The PAR draft is not envisioned to be too narrow to handle 11bc.
   6. Question on point e) to section 5.2.b: Why is it needed if AES remains quantum resistant?
      1. While no concrete example is offered, this point was suggested as a “maybe”.
      2. There is a concern that point e) may be mis-interpreted as replacing the symmetric pairwise cipher.
      3. There is a risk to out-scope the group from its goal, so the point is best left in.
   7. Question on section 5.3: are we not dependent on any other standards?
      1. No standards on which the group is dependent were identified.
      2. Enough work is believed to have been done by other standards’ groups to enable us to satisfy the PAR.
8. PQC Draft Proposed CSD - [11-25/0598r1](https://mentor.ieee.org/802.11/dcn/25/11-25-0598-01-0PQC-pqc-draft-proposed-csd.docx)
   1. Changes done to incorporate feedback provided before the meeting were presented.
   2. A few editoral changes were performed during the meeting.
   3. Question on the CSD being required at all from the SG.
      1. The CSD is required for LMSC’s consideration, the Coexistence Assesment is not.
   4. Question on “the USA entity” wording – which entity is this?
      1. NSA is the entity, text was updated.
9. An opportunity presents itself - [11-25/0631r0](https://mentor.ieee.org/802.11/dcn/25/11-25-0631-00-0PQC-an-opportunity-presents-itself.pptx)
   1. Comment on 11bi, which is more mature than the PQC SG, being in the process of doing somthing similar, protecting Association frames. There is overlap in result and in technique with the proposal at hand.
      1. 11bi is doing something similar, and duplication of work is not welcomed. If the 11bi work is mature, it can simply be re-used for PQC – especially for association. There is also a concern that the 11bi group is violating IEEE’s code of ethics by block voting.
      2. There are also suggestions in the contribution at hand that are not captured in 11bi.
   2. Straw poll at slide 8 of the contribution:
      1. The PQ TG, once formed, should:
         1. Leave the unfortunate architecture alone, just define new PQ algorithms; or
         2. Rearchitect things for PQC protocols only to integrate the 4way HS into the new protocols and avoid clunkiness
      2. Results:
         1. 5 votes for option a);
         2. 12 votes for option b);
         3. 3 votes for newly added option c) Don’t know.
      3. Note: One of the votes for option a) was captured on Webex chat as the contributor could not access Slido.
10. Progress on the PAR and CSD will be considered, and a meeting may be scheduled during the week commencing May 5th if required.
    1. 10 days notice would be required in this case.
11. Otherwise, next meeting will be in Warsaw on the 13th of May.
12. Adjourned at 11:10 ET.

# Appendix A - Attendance:

|  |  |  |  |
| --- | --- | --- | --- |
| **Breakout** | **Timestamp** | **Name** | **Affiliation** |
| PQC SG | 04/21/2025 | Wang, Zisheng | ZTE Corporation |
| PQC SG | 04/21/2025 | Sun, Bo | Sanechips |
| PQC SG | 04/21/2025 | Sevin, Julien | Canon Research Centre France |
| PQC SG | 04/21/2025 | Sambasivan, Sam | AT&T |
| PQC SG | 04/21/2025 | Rosdahl, Jon | Qualcomm Technologies, Inc |
| PQC SG | 04/21/2025 | Patwardhan, Gaurav | Hewlett Packard Enterprise |
| PQC SG | 04/21/2025 | Orr, Stephen | Cisco Systems, Inc. |
| PQC SG | 04/21/2025 | Lungu, Alexandru | SAMSUNG ELECTRONICS |
| PQC SG | 04/21/2025 | Li, Weiyi | Spreadtrum Communication USA, Inc |
| PQC SG | 04/21/2025 | Yang, Jay | ZTE Corporation |
| PQC SG | 04/21/2025 | Levy, Joseph | InterDigital, Inc. |
| PQC SG | 04/21/2025 | Koo, Jonghoe | SAMSUNG ELECTRONICS |
| PQC SG | 04/21/2025 | Kim, Sang Gook | LG ELECTRONICS |
| PQC SG | 04/21/2025 | Jang, Insun | LG ELECTRONICS |
| PQC SG | 04/21/2025 | Hunt, Preston | Intel |
| PQC SG | 04/21/2025 | Harkins, Daniel | Aruba Networks, Inc. |
| PQC SG | 04/21/2025 | Hamilton, Mark | Ruckus/CommScope |
| PQC SG | 04/21/2025 | Dharap, Anuj | Cisco Systems, Inc. |
| PQC SG | 04/21/2025 | DeLaOlivaDelgado, Antonio | Universidad Carlos III Madrid |
| PQC SG | 04/21/2025 | Baykas, Tuncer | Self |
| PQC SG | 04/21/2025 | Kuo, Chih-Chun | MediaTek Inc. |
| PQC SG | 04/21/2025 | Yee, Peter | NSA-CSD |
| PQC SG | 04/21/2025 | Zhou, Lei | New H3C Technologies Co., Limited |
| PQC SG | 04/21/2025 | Zuniga, Juan Carlos | Cisco Systems, Inc. |
| PQC SG | 04/21/2025 | Zhou, RenFang | TP-Link Systems Inc. |