Standardization efforts for PQC in OpenPGP

Stephan Ehlen\textsuperscript{BSI}, Andreas Hülsing\textsuperscript{TU/e}, Evangelos Karatsiolis\textsuperscript{MTG}, Stavros Kousidis\textsuperscript{BSI}, Johannes Roth\textsuperscript{MTG}, Falko Strenzke\textsuperscript{MTG}, Christian Tobias\textsuperscript{MTG}, Aron Wussler\textsuperscript{Proton}

BSI: German Federal Office for Information Security
MTG: MTG AG, Germany
Proton: Proton AG, Swiss
TU/e: Eindhoven University of Technology
OpenPG PQC Draft

- draft-wussler-openpgp-pqc-02
- public repository
  - https://github.com/openpgp-pqc/draft-openpgp-pqc
Recent developments / changes to 02

- KEM construction:
  - Now **hashing the public key** in the KDF within all the component schemes\(^1\) and not anymore feeding it into the key combiner

- Discussed at OpenPGP E-Mail Summit:
  - Now **allow more flavours of PQC encryption** additionally to v6 keys / v6 PKESK:
    - with v4 keys
    - with v6 keys and v3 PKESK
  - Alignment of security levels traditional and PQC in composites. *(Keep security margins for structured lattices.)*

---

\(^1\) was the case already for Kyber and now added EC schemes as well
Feedback / comments ?
backup ...
Algorithm and Parameter Choices

Algorithm Choices

**Kyber768 + X25519**  MUST  192/128
Kyber1024 + X448  SHOULD  256/224
Kyber768 + ECDH-NIST-P-256  MAY  192/128
Kyber1024 + ECDH-NIST-P-384  MAY  256/192
Kyber768 + ECDH-brainpoolP256r1  MAY  192/128
Kyber1024 + ECDH-brainpoolP384r1  MAY  256/192

**Dilithium3 + Ed25519**  MUST  192/128
Dilithium5 + Ed448  SHOULD  256/224
Dilithium3 + ECDSA-NIST-P-256  MAY  192/128
Dilithium5 + ECDSA-NIST-P-384  MAY  256/192
Dilithium3 + ECDSA-brainpoolP256r1  MAY  192/128
Dilithium5 + ECDSA-brainpoolP384r1  MAY  256/192

SPHINCS\(^+\)-simple-SHA2  SHOULD
SPHINCS\(^+\)-simple-SHAKE  MAY

\(^2\)classical security levels PQC/EC
## SPHINCS$^+$ Parameters

| SPHINCS$^+$-simple-\texttt{SHA2}-128s | SHOULD |
| SPHINCS$^+$-simple-\texttt{SHA2}-128f | SHOULD |
| SPHINCS$^+$-simple-\texttt{SHA2}-192s | SHOULD |
| SPHINCS$^+$-simple-\texttt{SHA2}-192f | SHOULD |
| SPHINCS$^+$-simple-\texttt{SHA2}-256s | SHOULD |
| SPHINCS$^+$-simple-\texttt{SHA2}-256f | SHOULD |
| SPHINCS$^+$-simple-\texttt{SHAKE}-128s | MAY |
| SPHINCS$^+$-simple-\texttt{SHAKE}-128f | MAY |
| SPHINCS$^+$-simple-\texttt{SHAKE}-192s | MAY |
| SPHINCS$^+$-simple-\texttt{SHAKE}-192f | MAY |
| SPHINCS$^+$-simple-\texttt{SHAKE}-256s | MAY |
| SPHINCS$^+$-simple-\texttt{SHAKE}-256f | MAY |