Post-Quantum Cryptography: Detours, delays, and disasters

Daniel J. Bernstein & Tanja Lange

University of Illinois at Chicago; Ruhr University Bochum
&
Eindhoven University of Technology

29 December 2022

Cryptographic tools used in TLS (`https`)

TLS relies critically on public-key cryptography for two reasons:

- Making sure the attacker can't pretend to be the server.
  Use public-key signatures: e.g., RSA-4096.
- Sending data as incomprehensible scrambled "ciphertexts".
  Use public-key encryption: e.g., NIST P-256.

Cryptographic tools used in TLS (`https`)

TLS relies critically on public-key cryptography for two reasons:

- Making sure the attacker can't pretend to be the server.
  Use public-key signatures: e.g., RSA-4096.
- Sending data as incomprehensible scrambled "ciphertexts".
  Use public-key encryption: e.g., NIST P-256.

For speed, TLS combines public-key crypto with symmetric crypto:

- Public-key encryption exchanges a key k.
- Public-key sigs $\Rightarrow$ attacker can't change k.
- Symm crypto uses k to protect user data.

Similar comments for SSH etc.

Cryptographic tools used in TLS (`https`)

TLS relies critically on public-key cryptography for two reasons:

- Making sure the attacker can't pretend to be the server.
  Use public-key signatures: e.g., RSA-4096.
- Sending data as incomprehensible scrambled "ciphertexts".
  Use public-key encryption: e.g., NIST P-256.

For speed, TLS combines public-key crypto with symmetric crypto:

- Public-key encryption exchanges a key k.
- Public-key sigs ⇒ attacker can't change k.
- Symm crypto uses k to protect user data.

Similar comments for SSH etc.

The problem

Quantum computers will break RSA-4096 and NIST P-256.

This assumes the attacker will have a big quantum computer, which isn't guaranteed but seems increasingly likely.
Large-scale attackers are already recording ciphertexts today in the hope of breaking them with future quantum computers.

The problem, and the main hope of a solution

Quantum computers will break RSA-4096 and NIST P-256.

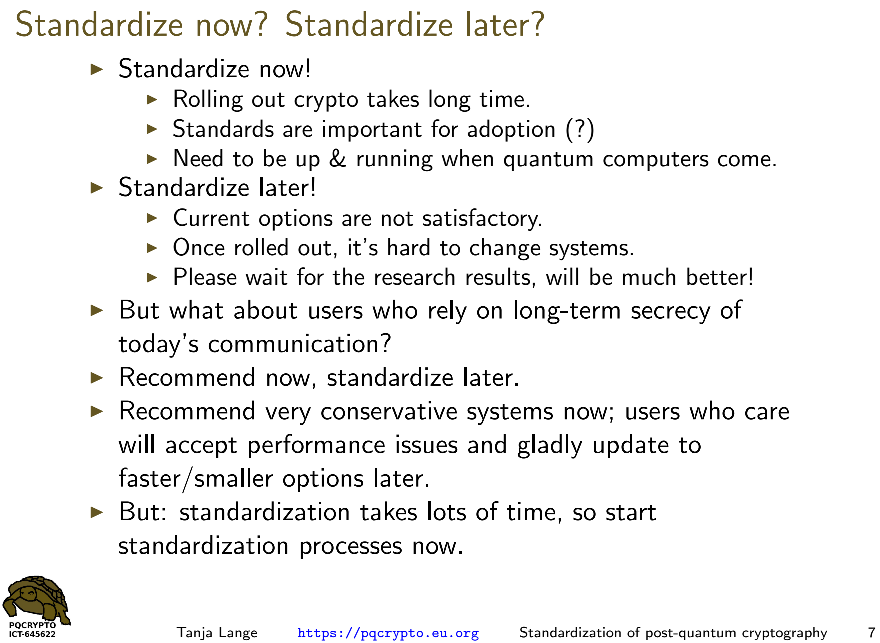
This assumes the attacker will have a big quantum computer, which isn't guaranteed but seems increasingly likely.
Large-scale attackers are already recording ciphertexts today in the hope of breaking them with future quantum computers.

Post-quantum cryptography: cryptography under the assumption that the attacker has a quantum computer.

Urgency of post-quantum recommendations

- All currently used public-key systems on the Internet are broken by quantum computers.
- Today's encrypted communication can be (and is being!) stored by attackers and can be decrypted later with quantum computer – think of medical records, legal proceedings, and state secrets.
- Post-quantum secure cryptosystems exist (to the best of our knowledge) but are under-researched – we can recommend secure systems now, but they are big and slow hence the logo of the PQCRYPTO project.
- PQCRYPTO is an EU project in H2020, running 2015 – 2018.
- PQCRYPTO is designing a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet.

Screenshot from 8 May 2016



Standardize now? Standardize later?

- Standardize now!
  - Rolling out crypto takes long time.
  - Standards are important for adoption (?)
  - Need to be up & running when quantum computers come.
- Standardize later!
  - Current options are not satisfactory.
  - Once rolled out, it’s hard to change systems.
  - Please wait for the research results, will be much better!
- But what about users who rely on long-term secrecy of today’s communication?
- Recommend now, standardize later.
- Recommend very conservative systems now; users who care will accept performance issues and gladly update to faster/smaller options later.
- But: standardization takes lots of time, so start standardization processes now.

PQCRYPTO
ICT-645622

Screenshot from 8 May 2016

Initial recommendations of long-term secure post-quantum systems

Daniel Augot, Lejla Batina, Daniel J. Bernstein, Joppe Bos,
Johannes Buchmann, Wouter Castryck, Orr Dunkelman, Tim Güneysu,
Shay Gueron, Andreas Hülsing, Tanja Lange,
Mohamed Saied Emam Mohamed, Christian Rechberger,
Peter Schwabe, Nicolas Sendrier, Frederik Vercauteren, Bo-Yin Yang

Issued in 2015
by the PQCRYPTO project.

Initial recommendations

- **Symmetric encryption** Thoroughly analyzed:
  - AES-256
  - Salsa20 with a 256-bit key
- **Symmetric authentication** Information-theoretic MACs:
  - GCM using a 96-bit nonce and a 128-bit authenticator
  - Poly1305
- **Public-key encryption** McEliece with binary Goppa codes:
  - length $n = 6960$, dimension $k = 5413$, $t = 119$ errors
- **Public-key signatures** Hash-based (minimal assumptions):
  - XMSS with parameters from CFRG draft
  - SPHINCS-256

Some other systems listed as *under evaluation* for possible future recommendations.

So everyone lived happily ever after

So everyone lived happily ever after?

Critical post-quantum decisions in 2016

2016.07 Chrome adds `newhope1024` post-quantum option.
Used for an experiment with Google servers.

Critical post-quantum decisions in 2016

2016.07 Chrome adds `newhope1024` post-quantum option.
Used for an experiment with Google servers.

This encryption layer is *added* to X25519 encryption (ECC):
if `newhope1024` is broken, still have pre-quantum security.

Critical post-quantum decisions in 2016

2016.07 Chrome adds `newhope1024` post-quantum option.
Used for an experiment with Google servers.

This encryption layer is *added* to X25519 encryption (ECC):
if `newhope1024` is broken, still have pre-quantum security.

`newhope1024` is new: main pieces from 2010, 2014, 2015.

Critical post-quantum decisions in 2016

2016.07 Chrome adds `newhope1024` post-quantum option.
Used for an experiment with Google servers.

This encryption layer is *added* to X25519 encryption (ECC): if `newhope1024` is broken, still have pre-quantum security.

`newhope1024` is new: main pieces from 2010, 2014, 2015.

A patent holder contacts Google, asks for money. Oops!

Critical post-quantum decisions in 2016

2016.07 Chrome adds newhope1024 post-quantum option.
Used for an experiment with Google servers.

This encryption layer is *added* to X25519 encryption (ECC):
if newhope1024 is broken, still have pre-quantum security.

newhope1024 is new: main pieces from 2010, 2014, 2015.

A patent holder contacts Google, asks for money. Oops!

2016.11 Chrome removes newhope1024 option.

Critical post-quantum decisions in 2016, cont'd

2016.12 US National Institute of Standards and Technology (NIST) calls for submissions by 2017.11 of post-quantum systems for subsequent standardization.

Critical post-quantum decisions in 2016, cont'd

2016.12 US National Institute of Standards and Technology (NIST) calls for submissions by 2017.11 of post-quantum systems for subsequent standardization.

NIST *prohibits* submissions of PQ+ECC hybrids: "The algorithms shall not incorporate major components that are believed to be insecure against quantum computers. (For example, hybrid schemes that include encryption or signatures based on factoring or discrete logs will not be considered for standardization by NIST in this context.)"

NIST creates incentives for industry to wait

NIST promises to collect information about patents
and to select strong patent-free post-quantum standards.

- Strong: "The security provided by a cryptographic scheme is the most important factor in the evaluation."
- Patent-free: "NIST believes it is critical that this process leads to cryptographic standards that can be freely implemented in security technologies and products."

Other standardization bodies decide to wait

IRTF CFRG, 2017.03: “the current CFRG approach is to define RFCs for a few relatively mature post-quantum primitives, such as hash-based signatures, but to wait for the results of the NIST process for everything else.”

ISO internal discussions: ISO will wait for NIST.

Other standardization bodies decide to wait

IRTF CFRG, 2017.03: “the current CFRG approach is to define RFCs for a few relatively mature post-quantum primitives, such as hash-based signatures, but to wait for the results of the NIST process for everything else.”

ISO internal discussions: ISO will wait for NIST.

Exception: China runs its own competition!

Other standardization bodies decide to wait

IRTF CFRG, 2017.03: "the current CFRG approach is to define RFCs for a few relatively mature post-quantum primitives, such as hash-based signatures, but to wait for the results of the NIST process for everything else."

ISO internal discussions: ISO will wait for NIST.

Exception: China runs its own competition!
But nobody cares what China does.

2017.12: 69 submissions from 260 people

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRU Prime. NTRU-HRSS-KEM. NTRUEncrypt. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqNTRUSign. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

NIST competition timeline

- 2019.01: NIST selects 26 round-2 candidates.

NIST competition timeline

- 2019.01: NIST selects 26 round-2 candidates.
- 2020.07: NIST selects 15 round-3 candidates.

NIST competition timeline

- 2019.01: NIST selects 26 round-2 candidates.
- 2020.07: NIST selects 15 round-3 candidates.
- Of course, NIST prioritizes the strongest candidates *except* for applications that need something more efficient.

NIST competition timeline

- 2019.01: NIST selects 26 round-2 candidates.
- 2020.07: NIST selects 15 round-3 candidates.
- ~~Of course, NIST prioritizes the strongest candidates *except* for applications that need something more efficient.~~
— Wait, no, it's the other way around: e.g. NIST says it will delay SPHINCS+ *unless* "NIST's confidence in better performing signature algorithms is shaken by new analysis".

NIST competition timeline

- 2019.01: NIST selects 26 round-2 candidates.
- 2020.07: NIST selects 15 round-3 candidates.
- ~~Of course, NIST prioritizes the strongest candidates *except* for applications that need something more efficient.~~ — Wait, no, it's the other way around: e.g. NIST says it will delay SPHINCS+ *unless* "NIST's confidence in better performing signature algorithms is shaken by new analysis".
- 2022.07: NIST selects 4 standards (including SPHINCS+) and 4 round-4 candidates.

2017.12: 69 submissions from 260 people

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRU Prime. NTRU-HRSS-KEM. NTRUEncrypt. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqNTRUSign. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

2022.12: Many submissions have been attacked

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRU Prime. NTRU-HRSS-KEM. NTRUEncrypt. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqNTRUSign. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Legend: Still in the NIST competition.
Less security than claimed. Really broken. Attack scripts.

2019: Some popular software adds pq options

Incentives for industry are starting to change by 2019:

- Urgency of protecting users is becoming more obvious.
- NIST has already collected and published patent statements.

2019.04 OpenSSH 8.0 adds `sntrup4591761`+ECC option (copying TinySSH). Used if client and server configure it.

2019: Some popular software adds pq options

Incentives for industry are starting to change by 2019:

- Urgency of protecting users is becoming more obvious.
- NIST has already collected and published patent statements.

2019.04 OpenSSH 8.0 adds `sntrup4591761`+ECC option (copying TinySSH). Used if client and server configure it.

2019.07 Google + Cloudflare run a new post-quantum experiment.
Option 1: CECPQ2, encrypting with `ntruhrss701`+ECC.
Option 2: CECPQ2b, encrypting with `sikep434`+ECC.

2019: Some popular software adds pq options

Incentives for industry are starting to change by 2019:

- Urgency of protecting users is becoming more obvious.
- NIST has already collected and published patent statements.

2019.04 OpenSSH 8.0 adds `sntrup4591761`+ECC option (copying TinySSH). Used if client and server configure it.

2019.07 Google + Cloudflare run a new post-quantum experiment.
Option 1: CECPQ2, encrypting with `ntruhrss701`+ECC.
Option 2: CECPQ2b, encrypting with `sikep434`+ECC.

2019.10 Google claims “quantum supremacy”.

NTRU, NTRU Prime: deployment accelerates

2021.03 OpenSSH 8.5 upgrades `sntrup4591761` → `sntrup761`.

2021.05 OpenBSD adds `sntrup761`+ECC option for IPsec. Used if client and server configure it.

2022.02 OpenSSH 8.9 enables `sntrup761`+ECC on server by default. Used if client configures it.

2022.04 OpenSSH 9.0 enables `sntrup761`+ECC on client *and* server by default.

2022.11 Google internal communication enables `ntruhrss701`+ECC by default.

US ANSI X9: use post-quantum hybrids

2021.10 “Simultaneous use of both classical cryptography and PQC methods for both security and acceptance is required during a transition and may be required long term as well.”

French ANSSI: use post-quantum hybrids

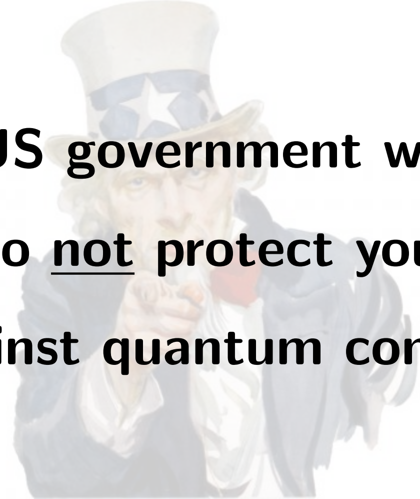
2021.12 "Acknowledging the immaturity of PQC is important: ANSSI will not endorse any direct drop-in replacement of currently used algorithms in the short/medium term. However, this immaturity should not serve as an argument for postponing the first deployments."

Here's where the story gets really weird

The US government wants YOU

https://www.publicdomainpictures.net/en/view-image.php?image=76327

Here's where the story gets really weird



The US government wants YOU

to not protect yourself

against quantum computers.

https://www.publicdomainpictures.net/en/view-image.php?image=76327

NIST vs. post-quantum deployment

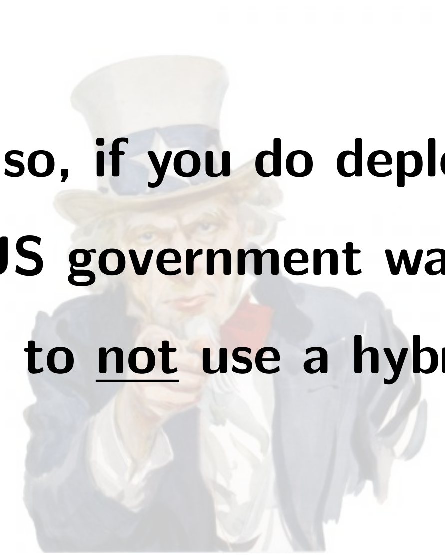
2021.07 Matthew Scholl, Chief of the Computer Security Division in NIST's Information Technology Laboratory, on videotape: "Don't let folks start to buy and implement unstandard, unknown, potentially unsecured implementations before we as a general community have agreed upon standardization."

NSA vs. post-quantum deployment

2021.08 NSA says: “NSS customers are reminded that NSA does not recommend and policy does not allow implementing or using unapproved, non-standard or experimental cryptographic algorithms. The field of quantum-resistant cryptography is no exception.”

DHS vs. post-quantum deployment

2021.09 DHS says: Do not use “any post-quantum cryptographic industry products until standardization, implementation, and testing of replacement products with approved algorithms are completed by NIST.”

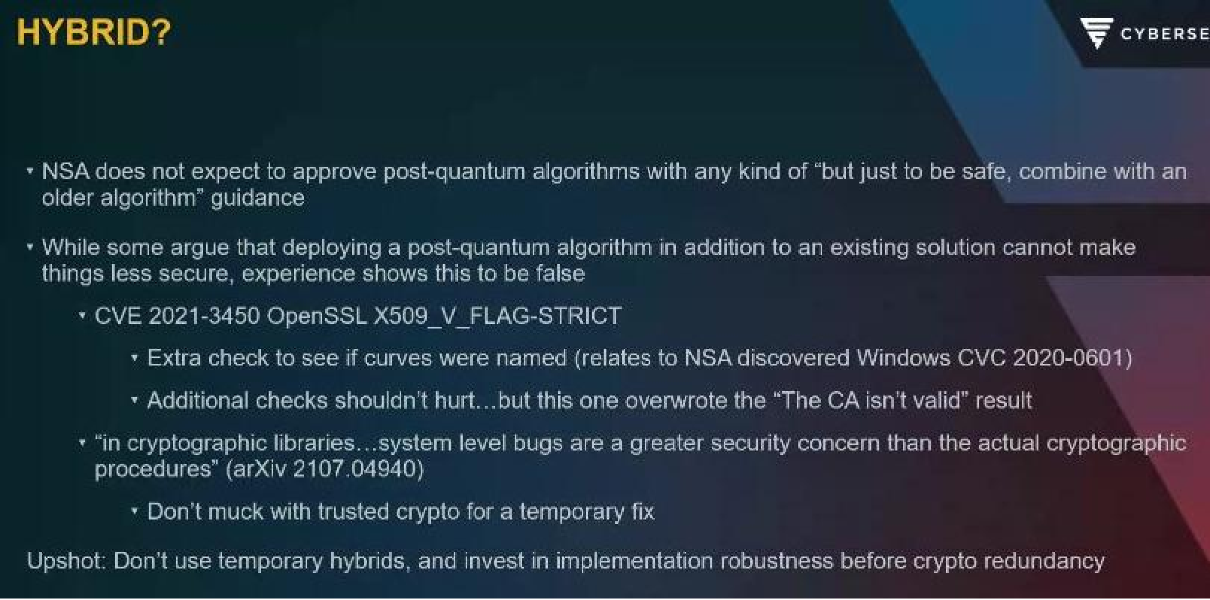


Also, if you do deploy pq,

the US government wants YOU

to not use a hybrid.

https://www.publicdomainpictures.net/en/view-image.php?image=76327



HYBRID?

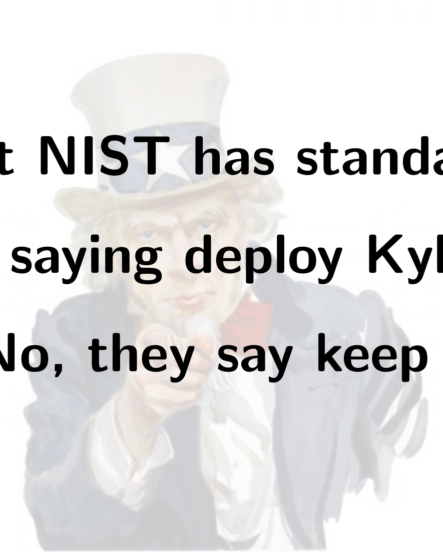
- NSA does not expect to approve post-quantum algorithms with any kind of "but just to be safe, combine with an older algorithm" guidance
- While some argue that deploying a post-quantum algorithm in addition to an existing solution cannot make things less secure, experience shows this to be false
  - CVE 2021-3450 OpenSSL X509_V_FLAG-STRICT
    - Extra check to see if curves were named (relates to NSA discovered Windows CVC 2020-0601)
    - Additional checks shouldn't hurt…but this one overwrote the "The CA isn't valid" result
  - "in cryptographic libraries…system level bugs are a greater security concern than the actual cryptographic procedures" (arXiv 2107.04940)
    - Don't muck with trusted crypto for a temporary fix

Upshot: Don't use temporary hybrids, and invest in implementation robustness before crypto redundancy

Picture credit: Markku Saarinen capturing screenshot from NSA talk
https://twitter.com/mjos_crypto/status/1433443198534361101

“Now that NIST has standardized Kyber, they’re saying deploy Kyber, right?”

https://www.publicdomainpictures.net/en/view-image.php?image=76327



“Now that NIST has standardized Kyber, they’re saying deploy Kyber, right?”

— No, they say keep waiting!

https://www.publicdomainpictures.net/en/view-image.php?image=76327

Remember Google's patent problem?

NIST's 4 selected standards include Kyber as the only encryption option (with no backup option in case Kyber is broken).

Remember Google's patent problem?

NIST's 4 selected standards include Kyber as the only encryption option (with no backup option in case Kyber is broken).

Kyber is in the middle of a patent minefield.

Remember Google's patent problem?

NIST's 4 selected standards include Kyber as the only encryption option (with no backup option in case Kyber is broken).

Kyber is in the middle of a patent minefield.

2022.07 "NIST negotiated with several third parties to enter into various agreements to overcome potential adoption challenges posed by third-party patents."

Remember Google's patent problem?

NIST's 4 selected standards include Kyber as the only encryption option (with no backup option in case Kyber is broken).

Kyber is in the middle of a patent minefield.

2022.07 "NIST negotiated with several third parties to enter into various agreements to overcome potential adoption challenges posed by third-party patents."

2022.07 Fluhrer (Cisco): "... until we get the text of the licenses [Cisco] cannot use Kyber. If continues to be true, we will need to seek an alternative solution."

NIST *partially* bought out two of the patents

2022.11 license excerpt: "1.11. 'PQC ALGORITHM' shall mean: (a) any **standard prescribed by NIST in a NIST Special Publication or Federal Information Processing Standard** that is based on the CRYSTALS-KYBER public-key encryption and key-establishment algorithm . . . **any modification**, extension, or derivation of the parameters of the PQC ALGORITHM, **is not an implementation** or use of the PQC algorithm."
(Emphasis added.)

Kyber will likely be standardized **in 2024**

2022.07 NIST is “aiming to complete
the initial PQC standards by around 2024.”

Kyber will likely be standardized **in 2024**

2022.07 NIST is "aiming to complete the initial PQC standards by around 2024."

2022.12 Kyber team: "Several questions, **possible tweaks**, and ideas have been proposed by members of the team, by researchers and future users from the community, and by NIST." (Emphasis added.)

Kyber will likely be standardized **in 2024**

2022.07 NIST is "aiming to complete the initial PQC standards by around 2024."

2022.12 Kyber team: "Several questions, **possible tweaks**, and ideas have been proposed by members of the team, by researchers and future users from the community, and by NIST." (Emphasis added.)

So the license allows use of Kyber-STD starting (likely) in 2024.
Maybe in 2023 we'll know what Kyber-STD is.
Maybe the other 5 patents don't apply.

It's 2022 and PQC is still not widely deployed.

That's the real disaster!

Questions?

Happy to answer now or reach out to us at

`authorcontact-fireshonks22@box.cr.yp.to`

What can you do now? Deploy hybrids!

Combine one (or more) post-quantum schemes with ECC or RSA.

Public-key signatures: All individual signatures must be valid for the hybrid signature to be valid.

Public-key encryption: Use multiple systems to jointly generate key for use in symmetric cryptography.

Choice of systems depends on risk profile:

- Use most efficient systems (hybrid with ECC or RSA), to ease usage and gain familiarity.
- Use most conservative systems (hybrid with ECC or RSA), to ensure that data really remains secure.

Some PQ libraries exist, quality is getting better.

Further information

- NIST PQC competition.
- Quantum Threat Timeline, 2019; 2021 update.
- Status of quantum computer development (by German BSI).
- ENISA studies: Post-quantum cryptography: Integration study, Post-quantum cryptography: current state and quantum mitigation
- YouTube channel Tanja Lange: Post-quantum cryptography.
- `https://2017.pqcrypto.org/school`: PQCRYPTO summer school with 21 lectures on video; slides; exercises.
- Less math, more perspective: `https://2017.pqcrypto.org/exec` and `https://pqcschool.org`.
- PQCrypto 2016, 2017, 2018, 2019, 2020, 2021, 2022 slides + videos.