U.S. activities in post-quantum cryptography

Daniel J. Bernstein

University of Illinois at Chicago;
Ruhr University Bochum;
Academia Sinica

Institute of Electrical and Electronics Engineers

1884: American Institute of Electrical Engineers is founded.
1912: Institute of Radio Engineers founded.
1963: AIEE + IRE $\rightarrow$ IEEE.

Expanded internationally: today 400000 members, including 160000 U.S. members. Revenues: 500 million USD/year, mostly for journals/conferences (300000 articles/year), about 10% for standards.

1200 active standards. 600 new standards under development.

IEEE P1363: standardizing public-key cryptography

1994: New P1363 committee chaired by Kaliski from RSA company.
1999: New P1363 chair, Singer from **NTRU company**.
2000: P1363-2000 standard on DL, ECDL, RSA.
2001: New P1363 chair, Whyte from **NTRU company**.
2004: P1363a-2004 update with more DL/ECDL/RSA variants.
2008: **P1363.1-2008 standard for NTRU.**
2008: P1363.2-2008 standard for PAKE.
2013: P1363.3-2013 standard for identity-based cryptography.
2014: Last email (out of thousands) on P1363 mailing list.

Note: IEEE NTRU standard differs from what NIST is considering.

American National Standards Institute

1918: American Engineering Standards Committee is founded.
1928: → American Standards Association.
1966: → USA Standards Institute.
1969: → ANSI.

ANSI doesn't develop its own standards.
ANSI accredits 243 organizations
developing standards, and promotes
"U.S. Leadership Role in the Regional
and International Standardization Community".
Revenues: 80 million USD/year.

Accredited Standards Committee X9

1974: ANSI approves the X9 Standards Committee on Banking.
1976: $\rightarrow$ X9, Financial Services.
1984: ANSI accredits X9.

X9 maintains 120 financial standards, including 26 cryptography standards. e.g., ANSI X9.92-1-2009 (R2017) is specifically "Digital Signature Algorithms Giving Partial Message Recovery—Part 1: Elliptic Curve Pintsov-Vanstone Signatures (ECPVS)".

ANSI X9.98-2010 (R2017) is a standard for NTRU.

X9 Call For Experts on post-quantum hybrids

2021: "As we transition from classical cryptography to post-quantum cryptography (PQC), there is a need to understand the proper ways to use both methods simultaneously. PQC methods will not be able to be used as a direct replacement in all cases. And the confidence and broad acceptance of PQC methods will not be as great as classical cryptography. **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. There are improper and insecure ways of implementing a hybrid of classical and PQC methods. Specifying the proper methods of using both are required." (emphasis added)

National Quantum Initiative (quantum.gov)

2019: NQI funding begins. "QIS research includes transformative new types of computers, sensors, and networks that can improve the Nation's prosperity and security."

U.S. government spent 672 million USD on quantum research+development in 2020. Approximately 0% for post-quantum crypto.

National Strategic Overview for Quantum Information Science says "DHS, NIST, NSA" are engaged in post-quantum crypto.

Department of Homeland Security

2003: 22 agencies merge, creating DHS.

2021 speech: Transition to post-quantum crypto depends on development and adoption. "Planning for the latter remains in its infancy. We must prepare for it now to protect the confidentiality of data that already exists today and remains sensitive in the future."

2021 memo: **Do not use** "post-quantum cryptographic industry products until standardization, implementation, and testing of replacement products with approved algorithms are completed by NIST."

National Institute of Standards and Technology

1901: National Bureau of Standards is founded.
1988: $\rightarrow$ NIST.
2021: Budget 1034 million USD.

NIST's Cryptographic Technology Group maintains >30 standards, including Federal Information Processing Standards for AES, DSA/ECDSA, HMAC, SHA-2, SHA-3.

NIST ran the competitions that produced AES, SHA-3, and is now running a **competition for post-quantum crypto**.

National Security Agency (NSA)

1919: Black Chamber is founded by Army and State Department.
1929: Secretary of State terminates funding.
"Gentlemen do not read each other's mail."
1930: → Signal Intelligence Service.
1949: → Armed Forces Security Agency.
1952: → NSA.
1967: NSA's Project Minaret starts
spying on anti-war protesters.
1968: NBS asks NSA for help
creating an encryption standard.

NSA's goals for cryptographic standardization

NSA internal history book (public release forced in 2013):

> *Narrowing the encryption problem to a single, influential algorithm might* ***drive out competitors****, and that would reduce the field that NSA had to be concerned about. Could a* ***public encryption standard*** *be made secure enough to protect against everything but a massive brute force attack, but* ***weak enough to still permit an attack of some nature*** *using very sophisticated (and expensive) techniques?*

(Emphasis added.)

Examples of NSA influence on standards

1975: IBM's DES is published. Key sizes are too small.
NSA had convinced IBM to reduce key size to 56 bits.

1991: NIST proposes DSA. Key sizes are too small.
Lawsuit later revealed that NSA had secretly designed DSA.

2005: ISO 18031 standardizes Dual EC. Has an NSA back door.
2013 report: NSA "wrote the standard and aggressively pushed it [on ISO], privately calling the effort 'a challenge in finesse.' "

2006, 2007: NIST SP 800-90, ANSI X9.82 standardize Dual EC.
Internally, Dual EC had been proposed to ANSI X9 first,
but ISO was the fastest organization to standardize it.

NSA on post-quantum cryptography

2013: NSA spends 250 million USD/year to "covertly influence and/or overtly leverage" cryptography to make it "exploitable".

2015: NSA "recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite".

2015–2020: NSA is secretly coordinating with NIST on PQC.
2020.07.22 13:02:49: NSA publicly thanks NIST for its PQC work.
2020.07.22 20:51:25: NIST announces round-3 PQC candidates.
2020.07.29: NSA recommends specifically lattices.

2021.09: NSA says it will approve only *non-hybrid* lattice systems. To sell to the U.S. government, will have to **turn off ECC**.