

Recent Advances in Post-Quantum Cryptography

Sedat Akleylek

Chair of Security and Theoretical Computer Science,
Institute of Computer Science,
University of Tartu, Estonia
sedat.akleylek@ut.ee

Outline

1 Post-Quantum Cryptography

2 Standardization

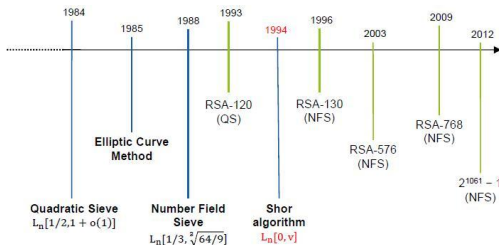
Post-Quantum Cryptography

- Post-quantum cryptography **does not** imply quantum cryptography.
- Post-quantum cryptography implies quantum safe public key cryptography.
- Post-quantum cryptographic algorithms are believed to be secure against an attack by a quantum computer.
- Post-quantum cryptography relies on mathematically unproven assumptions regarding the hardness of certain algorithmic problems.

1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 2680, 26

- RSA, ElGamal, Diffie-Hellman, DSA, ECDSA
- Security depends on *computationally hard problems*. There are several algorithms running with (sub-)exponential time to solve factorization problem, (elliptic curve) discrete problem by using traditional computing systems.
- Quadratic sieve, elliptic curve method, number field sieve, Pollard's Rho, index calculus, ...

Factorization Algorithms

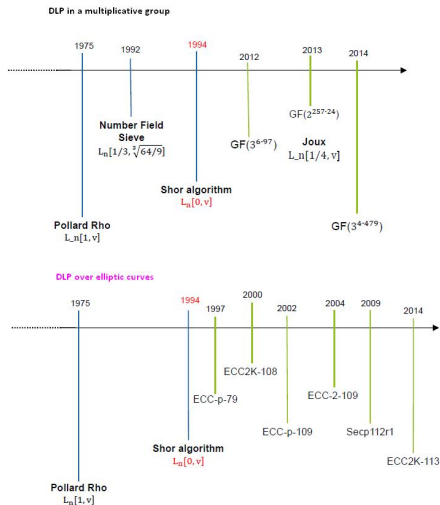


$$L_n[u, v] = e^{v(\log n)^u (\log \log n)^{(1-u)}}$$

$$L_n[0, v] = (\log n)^v \text{ polynomial}$$

$$L_n[1, v] = (e^{\log n})^v \text{ exponential}$$

Discrete Logarithm Problem Algorithms



100

believed to

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 at most a polynomial 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

- P.W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM J. Comput. Vol.26/5, pp.1484-1509, (1997).

What is Shor's Algorithm?

- Assume that we want to factorize N . We have two parts: classical arithmetic and quantum period finding. The steps are as follows:
 - 1 Compute $\gcd(m, N)$ for randomly selected m . If $\gcd(m, N) \neq 1$, N is factorized.
 - 2 Use a quantum computer to determine the period P of function $a \rightarrow m^a \pmod N$.
 - 3 If P is odd, then go to Step 1 (this probability is $1/4$ for RSA case).
 - 4 We have $(m^{P/2} - 1)(m^{P/2} + 1) = m^P - 1 \equiv 0 \pmod N$. If $(m^{P/2} + 1) \equiv 0 \pmod N$ then go to Step 1 (this probability is less than $1/2$ for RSA case).
 - 5 Compute $\gcd(m^{P/2} - 1, N)$ the non-trivial factor of N since $(m^{P/2} + 1) \not\equiv 0 \pmod N$.

Example

- What are the factors of $N = 91$?
 - 1 Choose $m = 3$, then $\gcd(91, 3) = 1$. $f(a) = 3^a \pmod{91}$.
 - 2 Quantum part (The period is $P = 6$, i.e., $3^6 \equiv 1 \pmod{91}$.)
 - 3 Since $P = 6$ is even, then proceed next step.
 - 4 $3^{P/2} = 27 \not\equiv -1 \pmod{91}$, then proceed next step.
 - 5 Compute $\gcd(3^{P/2} - 1, 91) = \gcd(26, 91) = 13$. Then,
 $N = 7 \times 13 = 91$.

Quantum Computing

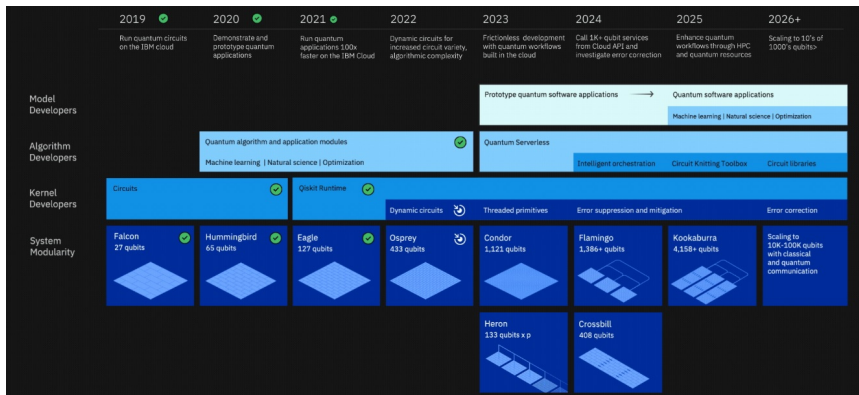
A banner for D-Wave Quantum Computing. On the left is a large, black, cube-shaped quantum computing system with the 'D:wave' logo on its side. The background is a gradient of blue and teal. On the right, the text 'Quantum computing has arrived.' is displayed in a large, white, sans-serif font. Below this, a smaller white text block states: 'D-Wave offers the first commercial quantum computing system on the market. If you are looking for a next-generation solution to difficult computational problems, we've got a pretty cool option for you.' At the top, a dark navigation bar contains the 'D:wave' logo and the text 'The Quantum Computing Company™' on the left, and a series of white links: 'HOME', 'PRODUCTS & SUPPORT', 'QUANTUM COMPUTING', 'OUR STORY', and 'DEVELOPER PORTAL' on the right.

Google moves toward quantum supremacy with 72-qubit computer

BY **EMILY CONOVER** 5:17PM, MARCH 5, 2018



Quantum Computing



Microsoft's Majorana 1 chip carves new path for quantum computing

Microsoft today [introduced Majorana 1](#), the world's first quantum chip powered by a new Topological Core architecture that it expects will realize quantum computers capable of solving meaningful, industrial-scale problems in years, not decades.

Written by

Catherine Bolgar

Published

February 19, 2025

Category

Innovation

It leverages the world's first topoconductor, a breakthrough type of material which can observe and control Majorana particles to produce more reliable and scalable qubits, which are the building blocks for quantum computers.

In the same way that the invention of semiconductors made today's smartphones, computers and electronics possible, topoconductors and the new type of chip they enable offer a path to developing quantum systems that can scale to a million qubits and are capable of tackling the most complex industrial and societal problems. Microsoft said,

Qubit Count

<https://quantumcomputingreport.com/scorecards/qubit-count/>

Univ. of Wisconsin	Gate	Neutral Atoms	49	TBD
Harvard/MIT	Quantum Simulator	Rydberg Atoms	51	TBD
Univ. of Maryland / NIST	Quantum Simulator	Ion Trap	53	TBD
D-Wave	Annealing	Superconducting	2048	5000
iARPA QEO Research Program	Annealing	Superconducting	N/A	100
NTT/Univ. of Tokyo/Japan NII	Qtm Neural Network	Photonic	2048	>20,000
Fujitsu	Digital Annealer	Classical	1024	8192
Alibaba/Univ. of Michigan	Software Simulator	Classical	144	N/A

How Many Qubits Are Needed?

Factoring algorithm (RSA)			EC discrete logarithm (ECC)			Classical
n	$\approx \#$ qubits	time	n	$\approx \#$ qubits	time	time
	$2n$	$4n^3$		$f'(n) (f(n))$	$360n^3$	
512	1024	$0.54 \cdot 10^9$	110	700 (800)	$0.5 \cdot 10^9$	$C \cdot 10^3$
1024	2048	$4.3 \cdot 10^9$	163	1000 (1200)	$1.6 \cdot 10^9$	$C \cdot 10^6$
2048	4096	$34 \cdot 10^9$	224	1300 (1600)	$4.0 \cdot 10^9$	$C \cdot 10^{12}$
3072	6144	$120 \cdot 10^9$	256	1500 (1800)	$6.0 \cdot 10^9$	$C \cdot 10^{18}$
15360	30720	$1.5 \cdot 10^{12}$	512	2800 (3600)	$50 \cdot 10^9$	$C \cdot 10^{40}$

How Many Qubits Are Needed?

- Quantum Attack Resource Estimate: Using Shor's Algorithm to Break RSA vs DH/DSA vs ECC, Kudelski Security, August 2021.
- Craig Gidney and Martin Eker, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, April 2021.
- Mark Webber, Vincent Elfving, Sebastian Weidt, and Winfried K. Hensinger, The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime, January 2022.

We investigate how hardware specifications can impact the final run time and the required number of physical qubits to achieve a quantum advantage in the fault tolerant regime. Within a particular time frame, both the code cycle time and the number of achievable physical qubits may vary by orders of magnitude between different quantum hardware designs. We start with logical resource requirements corresponding to a quantum advantage for a particular chemistry application, simulating the FeMo-co molecule, and explore to what extent slower code cycle times can be mitigated by using additional qubits. We show that in certain situations, architectures with considerably slower code cycle times will still be able to reach desirable run times, provided enough physical qubits are available. We utilize various space and time optimization strategies that have been previously considered within the field of error-correcting surface codes. In particular, we compare two distinct methods of parallelization: Game of Surface Code's Units and AutoCCZ factories. Finally, we calculate the number of physical qubits required to break the 256-bit elliptic curve encryption of keys in the Bitcoin network within the small available time frame in which it would actually pose a threat to do so. It would require 317×10^6 physical qubits to break the encryption within one hour using the surface code, a code cycle time of $1 \mu\text{s}$, a reaction time of $10 \mu\text{s}$, and a physical gate error of 10^{-3} . To instead break the encryption within one day, it would require 13×10^6 physical qubits.

Quantum Algorithms

math.nist.gov/quantum/zoo/

Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at stephen.jordan@nist.gov. Your help is appreciated and will be [acknowledged](#).

Algebraic and Number Theoretic Algorithms

Algorithm: Factoring

Speedup: Superpolynomial

Description: Given an n -bit integer, find the prime factorization. The quantum algorithm of Peter Shor solves this in $\tilde{O}(n^3)$ time [82–125]. The fastest known classical algorithm for integer factorization is the general number field sieve, which is believed to run in time $2^{\tilde{O}(n^{1/3})}$. The best rigorously proven upper bound on the classical complexity of factoring is $O(2^{n^{1/3+o(1)}})$ [252]. Shor's factoring algorithm breaks RSA public-key encryption and the closely related quantum algorithms for discrete logarithms break the DSA and ECDSA digital signature schemes and the Diffie-Hellman key-exchange protocol. A quantum algorithm even faster than Shor's for the special case of factoring "semiprimes", which are widely used in cryptography is given in [271]. There are proposed classical public-key cryptosystems not believed to be broken by quantum algorithms, cf. [248]. At the core of Shor's factoring algorithm is order finding, which can be reduced to the Abelian hidden subgroup problem, which is solved using the quantum Fourier transform. A number of other problems are known to reduce to integer factorization including the membership problem for matrix groups over fields of odd order [253], and certain diophantine problems relevant to the synthesis of quantum circuits [254].

Algorithm: Discrete-log

Speedup: Superpolynomial

Description: We are given three n -bit numbers a , b , and N , with the promise that $b = a^* \pmod N$ for some s . The task is to find s . As shown by Shor [82], this can be achieved on a quantum computer in $\text{poly}(n)$ time. The fastest known classical algorithm requires time superpolynomial in n . By similar techniques to those in [82], quantum computers can solve the discrete logarithm problem on elliptic curves, thereby breaking elliptic curve cryptography [109, 14]. The superpolynomial quantum speedup has also been extended to the discrete logarithm problem on semigroups [203, 204]. See also Abelian Hidden Subgroup.

[illegible]

Algorithm	Key Length	Effective Key Strength / Security Level	
		Conventional Computing	Quantum Computing
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

Crypto is Inside!

- Sim cards,
- Mobile phones,
- Remote controllers,
- Online banking
- Online shopping,
- Cloud



Transition to Post-Quantum Cryptography

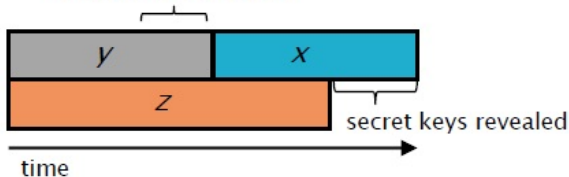
- NIST IR 8547 was published on January 10, 2025.
- Traditional public-key algorithms such as RSA, ECDSA, EdDSA are deprecated after 2030. The algorithm and key length/strength may be used, but there is some security risk.
- The data owner must examine this risk potential.
- The usage of traditional public-key algorithms will be disallowed after 2035. The scheme is no longer allowed for the stated purpose.

Security in an Era with Quantum Computers

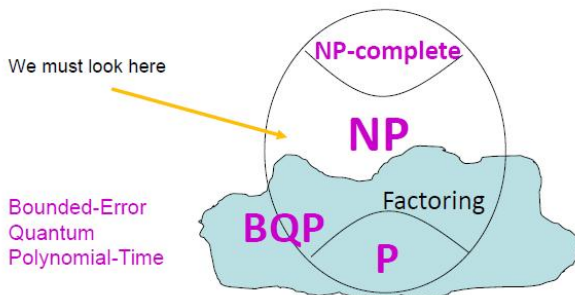
- **x:** How long do you need your cryptographic keys to be remain secure?
- **y:** How long will it take to deploy a set of tools that are quantum-safe?
- **z:** How long will it be before a quantum computer, or some other method, breaks the currently deployed public-key cryptography tools?

Theorem (Mosca): If $x + y > z$, then worry

What do we do here??



Cryptographically Hard Problems



Cryptosystems That Resist to Quantum Algorithms

- **Code-based**: efficient, large key sizes
- **Hash-based**: very efficient, large signatures
- **Multivariate quadratic**: very efficient, large key sizes
- **Lattice-based**: efficient, small key sizes.
- **Curve-based**: efficient, no formal security proof.
- **Symmetric-based**: efficient, large signature sizes, small key sizes

Parameters to Build Quantum Resistant Cryptographic Scheme

- Quantum resistant problem
- Cryptographic primitive
- Security analysis
- Parameter sets for different security level
- Optimizing performance

1. **Introduction**

1. *Journal of the American Medical Association*, 1997; 277: 1039-1043.

Computationally Hard Problems - Multivariate-based

Definition (Decisional Multivariate Quadratic Polynomial Problem)

Given a finite field \mathbb{F} and a system of m quadratic polynomials of n variables x_i :

$$f_k(x_1, \dots, x_n) = \sum_{1 \leq i < j \leq n} a_{ij}^{(k)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(k)} x_i + c^k,$$

for $k = 1, \dots, m$, where $a_{ij}^{(k)}, b_i^{(k)}, c^{(k)} \in \mathbb{F}$, determine if there exists a solution in \mathbb{F}^n .

- Multivariate Quadratic Polynomial Problem was shown to be NP-hard in all fields.
- MinRank problem was shown to be NP-hard.

Computationally Hard Problems - Lattice-based 1

Definition (The Short Integer Solution (SIS) Problem)

Let $n, m, q \in \mathbb{Z}^+$ and let β be a positive real number. Given a matrix $A \in \mathbb{Z}_q^{n \times m}$, chosen uniformly at random, find a nonzero integer vector $z \in \mathbb{Z}^m$ of Euclidean norm $\|z\| \leq \beta$ such that $Az = 0 \in \mathbb{Z}_q^n$.

Definition (The Search-NTRU Problem)

Let $q \in \mathbb{Z}^+$ and let γ be a positive real number. Let $R = \mathbb{Z}_q[x]/m(x)$, where $m(x)$ is a monic polynomial. Given an element $h \in R$ drawn from some distribution \mathbf{D} , such that there exists nonzero $(f, g) \in R^2$ that satisfy $h \cdot f \equiv g \pmod{q}$ and have small Euclidean norms $\|f\|, \|g\| \leq \sqrt{q}/\gamma$, find such a pair (f, g) .

Computationally Hard Problems - Lattice-based 2

For a vector $s \in \mathbb{Z}_q^n$ and error distribution ξ , define the Learning with Errors (LWE) distribution $A_{s,\xi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ by choosing $a \in \mathbb{Z}_q^n$ uniformly at random, choosing $e \leftarrow \xi$ over \mathbb{Z} , and outputting the pair (a, b) where $b = \langle s, a \rangle + e \pmod{q}$.

Definition (The Search-Learning with Errors (LWE) Problem)

Let $s \in \mathbb{Z}_q^n$ be chosen from some distribution \mathbf{B} . Given m samples $(a_1, b_1), \dots, (a_m, b_m) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ drawn independently at random from the distribution $A_{s, \xi}$, find s .

Definition (The Search-NTRU Problem)

Given m vectors of polynomials $a_1, \dots, a_m \in R_q^k$, chosen uniformly at random, let us view them as the rows of a matrix $A \in R_q^{m \times k}$. Then find a nonzero polynomial vector $z \in R_q^k$ of $\|z\| \leq \beta$ such that $A \cdot z = 0$.

1

- An encryption scheme is semantically secure if by observing a ciphertext c the adversary learns nothing about the plaintext.
- A CPA is an attack model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts.
- An encryption scheme is IND-CPA secure if and only if it's semantically secure.
- IND-CPA security implies that k and x cannot be obtained from $c \leftarrow E_k(x)$.
- The adversary gains access to a decryption oracle which decrypts arbitrary ciphertexts at the adversary's request, returning the plaintext. The challenger selects a bit $b \in \{0, 1\}$ uniformly at random, and sends the "challenge" ciphertext $c = E_k(m_b)$ back to the adversary. The adversary is free to perform any number of additional computations or

Security Definitions

- In the non-adaptive case (IND-CCA), the adversary may not make further calls to the decryption oracle before guessing
- In the adaptive case (IND-CCA2), the adversary may make further calls to the decryption oracle, but may not submit the challenge ciphertext c .
- A cryptosystem is indistinguishable under chosen ciphertext attack if no adversary can win the above game with probability $p > 1/2 + \epsilon$, where ϵ is a negligible function in the security parameter k .

Definition (EUF-CMA security)

A signature scheme is existential unforgeability under chosen message attacks (EUF-CMA) secure if the advantage of any probabilistic polynomial time adversary \mathbf{A} in the following game is negligible. The advantage of an adversary \mathbf{A} is defined as the function $Adv_A^{EUF-CMA}(\ell) = Pr[Succ_A^{EUF-CMA}]$, where $Succ_A^{EUF-CMA}$ is the event that \mathbf{A} wins.

1

- **Setup:** The challenger runs the key generation to obtain a key pair (pk, sk) and hands the public key pk to **A**.
- **Queries:** The adversary **A** is given access to a signing oracle. When queried for message m , the challenger runs algorithm **Sign** on input m and sk , and returns the corresponding output σ to the adversary
- **Forgery:** The adversary **A** outputs a pair (μ, σ) and wins if and only if $\text{Verify}_{sk}(\sigma, \mu) = 1$ and no query for a signature on μ was asked.

Security Definitions

- **Random Oracle Model (ROM):** A uniformly random function H is sampled at the beginning of time, and all parties are provided blackbox access to H ; any evaluations of the hash function in the real setting are then replaced with queries to H . Proving security of a cryptographic scheme in the ROM can be interpreted as indicating security against certain kinds of attacks (e.g., ones that do not exploit special structural properties of the hash function).

Security Definitions

- **Quantum Random Oracle Model (QROM):** A classical adversary who knows a circuit for some function f can certainly evaluate that function in black-box form by locally implementing the circuit for f . A quantum adversary who knows a circuit for f has the added ability to implement a certain unitary circuit associated to f , enabling queries in superposition.
- The relevance of this model is justified by the existence of nontrivial quantum attacks that use such quantum queries but no specific properties of the hash function itself. A standard example is the use of Grover's algorithm to find preimages with quadratically fewer queries than is possible in the classical-query model.

We may think in a different way

- This work claimed “Quantum Secure” Key Exchange, but indeed it uses post-quantum primitives (i.e., lattice) to realize a key exchange construction. In general, we cannot say lattice assumptions are quantum secure, since **no one can guarantee** the such assumptions withstand quantum attacks in the future!

CONCLUSIONS

- We need time to improve the **efficiency** of post-quantum cryptography.
- We need time to build **confidence** in post-quantum cryptography.
- We need time to improve the **usability** of post-quantum cryptography.

Milestones of Code-based Cryptography

- McEliece public key encryption scheme, 1978 (for 128-bit security it uses of (6960, 5413, 119-errors) almost 1MB)
- Niederreiter public key encryption scheme, 1986 (difference to McEliece is to encode the message into the error vector by a function instead of representing it as a codeword)
- Courtois, Finiasz, Sendrier McEliece-based signature scheme, 2001

Milestones of Hash-based Cryptography

The security of hash-based digital signature schemes depends on the collision resistance of that hash function.

- Merkle signature scheme (MSS) 1989
- Buchmann, Dahmen, Huelsing, extended Merkle signature scheme (XMSS) 2011 (IETF draft standard; for 80-bit security signatures are 2.4KB, public key is 0.9KB and secret key is 1.6KB)
- Bernstein et. al, SPHINCS: Stateless, practical, hash-based, incredibly nice cryptographic signatures 2015 (for 256-bit security signatures are 41KB, private and public keys are 1KB)

Milestones of Multivariate Quadratic Based Signature Schemes

- *Oil and Vinegar (OV)*: Rainbow, 2005 (for 80-bit security public key is 27.9KB, secret key is 19.6KB), partially cyclic UOV, 2011 (for 80-bit security public key is 8.9KB, secret key is 75.3KB)
- *Matsumoto-Imai*: C^* , 1988
- *Hidden Field Equations (HFE)*: HFEv-, 2001 (for 80-bit security public key is 3.9KB, secret key is 71KB)
- *MQDSS*

References

- Goldreich, Goldwasser, Halevi, GGH (lattice analogue of McEliece cryptosystem) 1997
- Hoffstein, Pipher, Silverman, NTRU (closest vector problem) 1998
- Regev, Learning with errors (LWE) based on shortest vector problem 2005
- Lyubashevsky, Micciancio, Peikert, Rosen, SWIFFT: A Modest Proposal for FFT Hashing 2008

Standardization Efforts in Cryptography by NIST

- **Block Cipher** : AES - 15 candidates, 2 rounds, 5 finalists, 3 years + 1 year for standard.
- **Hash Function** : SHA3 - 64 submissions, 51 accepted, 3 rounds, 14 Round 2 candidates, 5 finalists, 5 years + 3 years for standard.
- **Lightweight Crypto** : 57 submissions, 3 years ?
- **Post-Quantum Cryptography** : in progress

NOTES

Post-Quantum Cryptography Project

April 2015	Workshop on Cybersecurity in a Post-Quantum World, NIST, Gaithersburg, MD
February 2016	PQC Standardization: Announcement and outline of NIST's Call for Submissions presentation given at PQCrypto 2016
April 2016	NISTIR 8105, <i>Report on Post-Quantum Cryptography</i> [8], released
December 2016	Federal Register Notice – Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms [4]
November 30, 2017	Submission Deadline for NIST PQC Standardization Process
December 2017	First-round candidates announced. The public comment period on the first-round candidates began.
April 2018	First NIST PQC Standardization Conference, Ft. Lauderdale, FL
January 2019	Second-round candidates announced. NISTIR 8240, <i>Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process</i> [6], released. The public comment period on the second-round candidates began.
August 2019	Second NIST PQC Standardization Conference, Santa Barbara, CA
April 2020	NIST invited comments from submitters and the community to inform its decision-making process for the selection of third-round candidates.
July 2020	Third-round finalists and alternate candidates announced. NIST-IR 8309, <i>Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process</i> [7], released. The public comment period on the third-round candidates began.
June 2021	Third NIST PQC Standardization Conference, held virtually
July 2022	Candidate algorithms to be standardized are announced, along with alternate candidates advancing to the fourth round. NIST-IR 8413, <i>Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process</i> , released.

Post-Quantum KEM and DSS

- On August 13, 2024, the standards were published.
- FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard
- FIPS 204, Module-Lattice-Based Digital Signature Standard
- FIPS 205, Stateless Hash-Based Digital Signature Standard

NIST Standards

Algorithm	Quantum-safe	Public Key	Ciphertext / Signature
ECDH P-384	✗	48	48
Kyber-512	✓	800	768
Kyber-768	✓	1184	1088
ECDSA P-384	✗	48	96
RSA-3072	✗	387	384
Falcon-512	✓	897	666
Dilithium-2	✓	1312	2420
Falcon-1024	✓	1793	1280
Dilithium-3	✓	1952	3293
SPHINCS+-128s	✓	32	7856
SPHINCS+-192s	✓	48	16224

Table 1. Classical and post-quantum cryptographic schemes selected by NIST for standardization, ordered by ciphertext/signature size.

Post-Quantum Cryptography Competition

- Scope:
 - Digital Signatures
 - EUF-CMA up to 2^{64} signature queries
 - Public-key Encryption / Key-Encapsulation Mechanisms (KEMs)
 - IND-CCA up to 2^{64} decryption/decapsulation queries
 - IND-CPA option
- Open and transparent process
- Unlike previous AES and SHA-3 competitions, there will not be a single “winner”

Evaluation Criteria

- **Security** – against both classical and quantum attacks

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

- NIST asked submitters to focus on levels 1,2, and 3. (Levels 4 and 5 are for very high security)
- **Performance** – measured on various classical platforms
- **Other properties:** Drop-in replacements, Perfect forward secrecy, Resistance to side-channel attacks, Simplicity and flexibility, Misuse resistance, etc.

NIST Submissions - Round 1

- 82 submissions received.
- 69 accepted as “complete and proper” (5 withdrew)

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Symmetric-based	3		3
Other	2	5	7
Total	19	45	64

NIST Submissions

• BIG QUAKE	• Gravity-SPHINCS	• LUOV	• QC-MDPC-KEM
• BIKE	• Guess Again	• McNie	• qTESLA
• CFPKM	• Gui	• Mersenne-756839	• RaCoSS
• Classic McEliece	• HILA5	• MQDSS	• Rainbow
• Compact LWE	• HiMQ-3	• NewHope	• Ramstake
• CRYSTALS-DILITHIUM	• HK-17	• NTRUEncrypt	• RankSign
• CRYSTALS-KYBER	• HQC	• NTRU-HRSS-KEM	• RLCE-KEM
• DAGS	• KCL	• NTRU Prime	• Round2
• Ding Key Exchange	• KINDI	• NTS-KEM	• RQC
• DME	• LAC	• Odd Manhattan	• RVB
• DRS	• LAKE	• Ouroboros-R	• SABER
• DualModeMS	• LEDAkem	• Picnic	• SIKE
• Edon-K	• LEDApkc	• Post-quantum RSA Encryption	• SPHINCS+
• EMBLEM/R.EMBLEM	• Lepton	• Post-quantum RSA Signature	• SRTPI
• FALCON	• LIMA	• pqNTRUSign	• Three Bears
• FrodoKEM	• Lizard	• pqsigRM	• Titanium
• GeMSS	• LOCKER		• WalnutDSA
• Giophantus	• LOTUS		

	Signatures		KEM/Encryption		Overall	
Lattice-based	5	3	24	9	26	12
Code-based	2	0	17	7	19	7
Multi-variate	7	4	2	0	9	4
Symmetric-based	3	2			3	2
Other	2	0	5	1	7	1
Total	19	9	45	17	64	26

NIST Status Report - Round 1

- NIST IR 8240 - Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, January 2019.
- The purpose of this document is **to report on the first round** of the NIST PQC Standardization Process.
- This report describes the evaluation criteria and selection process, based on **public feedback** and **internal review** of the first-round candidates, and summarizes the 26 (17 KEM/PKE, 9 DS) candidate algorithms announced on January 30, 2019 for moving forward to the second round of the competition.

NIST Status Report - Round 1

- The criteria included provisions for reference and optimized C code implementations, known-answer tests, a written specification, and required intellectual property statements. In addition, **the algorithms were required to be implementable in a wide range of hardware and software platforms.**
- The three aspects are: **1)** security, **2)** cost and performance, and **3)** algorithm and implementation characteristics.

NIST Status Report - Round 1

- **NIST studied the security arguments** presented in the submission package, as well as external cryptanalysis submitted to NIST or published elsewhere. NIST researchers also conducted internal cryptanalysis.
- NIST considered not only attacks that directly demonstrated that a candidate fell short of NIST's stated security targets, but also attacks that brought the candidate's underlying security assumptions into question, or that gave the appearance of room for improvement.
- NIST also considered the overall quantity, quality, and maturity of analysis relevant to each candidate, including analysis of similar schemes.

NIST Status Report - Round 1

- **NIST did not use the implementation performance numbers as a primary factor in its decision.**
- When evaluating the performance of the candidates, NIST considered both the key/ciphertext/signature sizes as well as the computational estimates.
- In a few cases, a submitted design was selected in part for its **uniqueness** and **elegance**.

NIST Submissions - Round 2

[illegible]

NIST Submissions

Biting the Bullet

Crystals-Kyber	Lattice MLWE	
KINDI	Lattice MLWE	
Saber	Lattice MLWR	
FrodoKEM	Lattice LWE	
Lotus	Lattice LWE	
Lizard	Lattice LWE/RLWE	
Emblem/R.emblem	Lattice LWE/RLWE	
KCL	Lattice LWE/RLWE/LWR	
Round 2	Lattice LWR/RLWR	
Hila5	Lattice RLWE	
Ding's key exchange	Lattice RLWE	
LAC	Lattice RLWE	
Lima	Lattice RLWE	
NewHope	Lattice RLWE	
Three Bears	Lattice IMLWE	
Mersenne-756839	Lattice ILWE	
Titanium	Lattice MP-LWE	
Ramstake	Lattice LWE like	
Odd Manhattan	Lattice Generic	
NTRU Encrypt	Lattice NTRU	
NTRU-HRSS-KEM	Lattice NTRU	
NTRUprime	Lattice NTRU	

Crystals-Kyber	Lattice MLWE	
Saber	Lattice MLWR	
FrodoKEM	Lattice LWE	
Round 5	Lattice LWR/RLWR	
LAC	Lattice RLWE	
NewHope	Lattice RLWE	
Three Bears	Lattice IMLWE	
NTRU	Lattice NTRU	
NTRUprime	Lattice NTRU	

Big Quake	Codes	Goppa	
Classic McEliece	Codes	Goppa	
NTS-KEM	Codes	Goppa	
BIKE	Codes	short Hamming	
HQC	Codes	short Hamming	
LEDAkem	Codes	short Hamming	
LEDApkc	Codes	short Hamming	
QC-MDPC KEM	Codes	short Hamming	
LAKE	Codes	low rank	
LOCKER	Codes	low rank	
Oursborers-R	Codes	low rank	
RQC	Codes	low rank	
SIKE	Isogeny	Isogeny	

Classic McEliece	Codes	Goppa	
NTS-KEM	Codes	Goppa	
BIKE	Codes	short Hamming	
HQC	Codes	short Hamming	
LEDAcrypt	Codes	short Hamming	
Rollo	Codes	low rank	
RQC	Codes	low rank	
SIKE	Isogeny	Isogeny	

Signatures			
CRYSTALS-Dilithium	Lattice	Fiat-Shamir	
qTesla	Lattice	Fiat-Shamir	
Falcon	Lattice	Hash then sign	
poNTRUSign	Lattice	Hash then sign	

Gravity-SPHINCS	Symm	Hash	
SPHINCS+	Symm	Hash	
Picnic	Symm	ZKP	
GeMMS	MultiVar	HFE	
Gul	MultiVar	HFE	
HIMQ-3	MultiVar	UOV	
LUOV	MultiVar	UOV	
Rainbow	MultiVar	UOV	
MQDSS	MultiVar	Fiat-Shamir	

Signatures			
CRYSTALS-Dilithium	Lattice	Fiat-Shamir	
qTesla	Lattice	Fiat-Shamir	
Falcon	Lattice	Hash then sign	
SPHINCS+	Symm	Hash	
Picnic	Symm	ZKP	
GeMMS	MultiVar	HFE	
LUOV	MultiVar	UOV	
Rainbow	MultiVar	UOV	
MQDSS	MultiVar	Fiat-Shamir	

NIST Status Report - Round 2

- NIST IR 8309 - Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, July 2020.
- This report describes the evaluation and selection process, based on public feedback and internal review, of the second-round candidates. The report summarizes the 26 second-round candidate algorithms and identifies those selected to move forward to the third round of the competition.

NIST Status Report - Round 2

- NIST selected 15 of the second-round candidates to move onto the third round of the standardization process. Of the 15 advancing candidates, seven have been selected as **finalists** and eight as **alternate candidates**.
- The set of finalists are algorithms that NIST considers to be the most promising to fit the majority of use cases and most likely to be ready for standardization soon after the end of the third round.
- In NIST's current view, structured lattice schemes appear to be **the most promising general-purpose algorithms** for public-key encryption/KEM and digital signature schemes.

NIST Status Report - Round 2

- The alternate candidates are regarded as potential candidates for future standardization, most likely after another round of evaluation.
- Some of the alternate candidates have worse performance than the finalists but might be selected for standardization based on NIST's high confidence in their security.
- Some alternate candidates were **selected based either on NIST's desire for diversity** in future post-quantum security standards or on their potential for further improvement.

NIST Status Report - Round 2

- New standards are needed to provide security for all of TLS, SSH, IKE, IPsec, and DNSSEC, as well as for certificates, software code signing, and secure bootloaders applications.
- More information about the computational efficiency of the algorithms became available. Faster, constant-time implementations on Intel x64 processors were provided for many of the algorithms, as were ARM Cortex-M4 and hardware implementations.
- NIST also sees diversity of computational hardness assumptions as an important long-term security goal for its standards. NIST hopes to **standardize practically efficient schemes from different families of cryptosystems** to reduce the risk that a single breakthrough in cryptanalysis.

NIST Status Report - Round 2

- NIST does **not** feel the need to choose these standards **all at once** but will rather prioritize those schemes which seem closest to being ready for standardization and wide adoption.
- **For general-purpose use**, the evaluation of overall performance considered the cost of transferring the public key in addition to the signature or ciphertext during each transaction.
- **For special-purpose uses**, the performance requirements can be somewhat different, and different algorithms may be preferable.

NIST Submissions - Round 3

- 1+2 code-based KEM/Encryption
- 3+2 lattice-based KEM/Encryption
- 0+1 isogeny KEM/Encryption
- 1+1 multivariate digital signature
- 2 lattice-based digital signature
- 0+1 hash-based digital signature
- 0+1 other digital signature

NIST Selected Algorithms 2022

- Crystals-Kyber (KEM)
- Crystals-Dilithium (digital signature)
- FALCON (digital signature)
- SPHINCS+ (digital signature)

NIST Submissions - Round 4 (KEM)

- BIKE
- Classic McEliece
- **HQC** was selected on March 2025.
- SIKE

NIST Status Report - Round 3

- NIST IR 8413 - Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, July 2022.
- The report summarizes each of the 15 third-round candidate algorithms and identifies those selected for standardization, as well as those that will continue to be evaluated in a fourth round of analysis.

NIST Status Report - Round 3

- The NIST security strength categories are defined in a way that leaves open the relative cost of various computational resources, including quantum gates/memory, classical gates/memory, hardware, energy, and time.
- Even if one has agreed upon a model or a range of models for evaluating the relative cost of various computational resources, there may still be uncertainty how much of a given resource an attack actually requires.
- NIST continues to see diversity of computational hardness assumptions as an important **long-term security** goal for its standards.

NIST Status Report - Round 3

- **NIST will standardize practically efficient schemes from different families of cryptosystems.**
- The computational efficiency of key generation and public and private key operations, the transmission costs for public keys and signatures or ciphertexts, and the implementation costs in terms of RAM (random-access memory) or gate counts are as the second most important criterion when evaluating candidate algorithms.

NIST Status Report - Round 3

- For **general-purpose use**, the evaluation of overall performance considered the cost of transferring the public key in addition to the signature or ciphertext during each transaction.
- For KEMs, the cost of key generation was also taken into account, since many applications use a new KEM key pair for each transaction to provide forward secrecy.
- For signature algorithms, the cost of key generation was considered less important.
- It is NIST's hope and expectation that more side-channels work will continue, especially with regard to protecting the implementations of the algorithms announced for standardization.

NIST Status Report - Round 3

- Simplicity was an important factor in NIST's evaluation of FALCON, with the concern that the use of floating point arithmetic and more complex implementation could lead to errors that might affect security. In contrast, the simpler design of Dilithium was viewed positively.
- The security of Picnic is not better than that of SPHINCS+, and NIST feels that while SPHINCS+ is a mature design, Picnic and related schemes would continue to benefit from future research and improvements.
- They each have much higher cost and much worse performance in comparison to Dilithium and FALCON, making these criteria less important.
- In selecting a cryptographic algorithm for standardization, an evaluation factor is whether a patent might hinder adoption of the cryptographic standard.

NIST Status Report - Round 3

- As NIST will standardize one of the (structured lattice) finalist KEMs, NTRU Prime was not selected to continue on in the process.
- One of the differences between KYBER, Saber, and NTRU is the specific security assumption each relies upon for security. NIST finds the MLWE problem, which KYBER depends upon, marginally **more convincing** than the other assumptions like MLWR or the NTRU problem.
- FrodoKEM has generally worse performance than these three and so will not be considered further for standardization.

Note on the Selections

- CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications.
- Falcon is standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large.
- SPHINCS+ is standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

1. Introduction

- BIKE
- Classic McEliece
- **HQC**

SIGNATURE ALGORITHMS

What NIST Wants?

- Security (applied and theoretical)
- Performance (hardware and software)

What the Industry Wants?

- Performance ?
- Key sizes ?
- Energy consumption ?
- Avoid transmitting large public keys across slow links ?
- Avoid storing large public keys on endpoints ?
- ?

KEM Selected for Standardization

- **CRYSTALS-Kyber:** MLWE-based KEM.
- $R = \mathbb{Z}[x]/(x^{256} + 1)$, the module rank k is set to 2, 3 or 4.
 $q = 3329$.
- KYBER has excellent performance overall in software, hardware and many hybrid settings.
- **Why Kyber?** A significant factor in the decision to choose KYBER over NTRU was NTRU's performance (particularly key generation), which was not quite as efficient as that of KYBER. There is arguably more evidence to support the MLWE problem (which KYBER is based upon) than the MLWR or NTRU assumptions which Saber and NTRU respectively rely upon.

KEMs Advancing to the 4th Round

- **BIKE**: Bit Flipping Key Encapsulation. Binary linear quasi-cyclic moderate density parity check (QC-MDPC) codes.
- Security depends on quasi-cyclic codeword finding (QCCF) problem.
- BIKE PKE follows Neiderreitter-style encryption.
- **Why BIKE?** The quasi-cyclic structure of BIKE enables public key and ciphertext sizes comparable to – though slightly larger – than the structured lattice KEMs.
- BIKE remains under consideration due to its overall performance and substantially different security assumption from the currently selected KEM.

9

- **Classic McEliece:** Binary Goppa code in the Niederreiter variant of the McEliece cryptosystem combined with standard techniques to achieve CCA security
- Classic McEliece has a very large public key size and fairly slow key generation. This is likely to make Classic McEliece undesirable in many common settings. However, in settings where a public key is reused many times and does not need to be retransmitted for each new communication
- **Why McEliece?** There has been no significant cryptanalysis on Classic McEliece. Classic McEliece has the smallest ciphertext sizes of any of the NIST PQC candidates.

10

- **HQC:** Hamming Quasi-Cyclic.
- The quasi-cyclic structure of HQC enables small public key and ciphertext sizes, although they are noticeably larger than the structured lattice KEMs.
- Although the bandwidth of HQC exceeds that of BIKE, HQC's key generation and decapsulation only require a fraction of the kilocycles required by BIKE. When factoring in the bandwidth with performance numbers, HQC is one of the top two alternate KEMs advancing for overall performance in software
- **Why HQC?** HQC offers strong security assurances and a mature decryption failure rate analysis. HQC public keys and ciphertexts are larger than all of the other remaining structured code- and structured lattice-based KEMs.

- Both BIKE and HQC are based on structured codes, and either would be suitable as a **general-purpose** KEM that is not based on lattices. NIST expects to select **at most one of these** two candidates for standardization at the conclusion of the fourth round.
- Although Classic McEliece is widely regarded as secure, NIST does not anticipate it being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

KEMs Advancing to the 4th Round

- **SIKE**: Supersingular Isogeny Key Encapsulation
- SIKE is an unusual candidate, as it relies on a different hard problem than all of the other post-quantum cryptosystems. However, there is a recent attack showing this is not secure.

Signatures Selected for Standardization

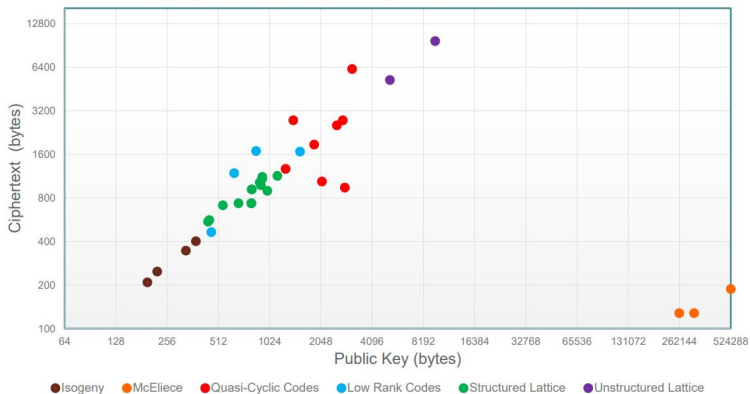
- **CRYSTALS-Dilithium:** Module-LWE sample of the form $(A, t := As_1 + s_2)$. Fiat-Shamir paradigm.
- $R = \mathbb{Z}[x]/(x^{256} + 1)$, $q = 2^{23} - 2^{13} + 1$.
- Pseudorandomness and truncated storage techniques are used to improve the performance of Dilithium.
- **Why Dilithium?** Dilithium is a signature scheme with high efficiency, relatively simple implementation, a strong theoretical security basis, and an encouraging cryptanalytic history.

Signatures Selected for Standardization

- **FALCON:** Fast Fourier Lattice-based Compact Signatures over NTRU. Hash-and-sign paradigm.
- The theoretical security of FALCON is established by a proof of unforgeability in the QROM, based on the hardness of the SIS Problem over NTRU lattices
- Signing is somewhat slower than Dilithium and key generation is significantly slower.
- Pseudorandomness and truncated storage techniques are used to improve the performance of Dilithium.
- **Why FALCON?** FALCON has the smallest bandwidth (public key size + signature size). There is no known attack.

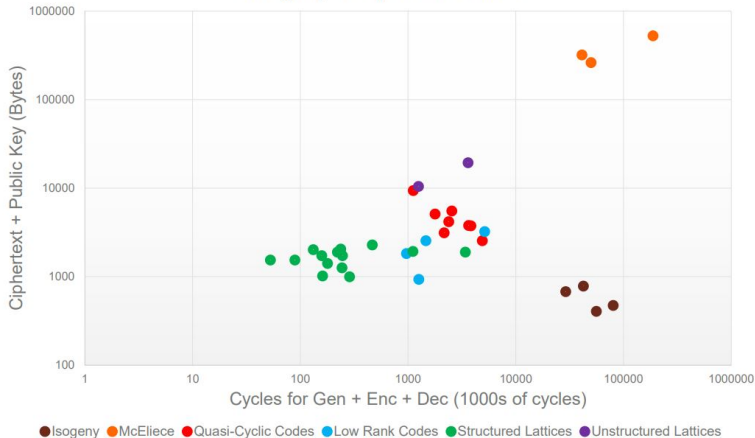
- **SPHINCS⁺**: is a stateless hash-based signature scheme.
- **Why SPHINCS⁺**? There is no known attack.

Category 1: Public Key vs Ciphertext size - PKE/KEMs

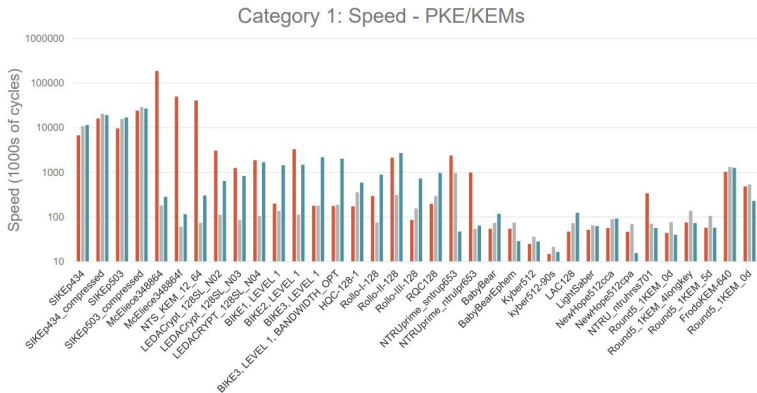


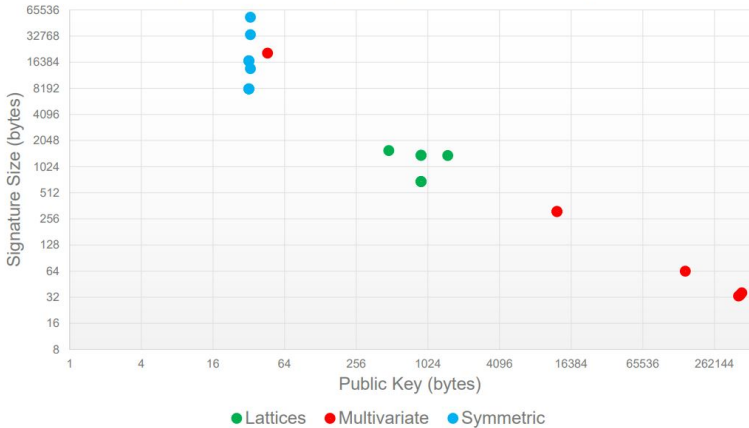
NIST Submissions - S1 Speed vs Sizes - PKE/KEMs

Category 1: Speed vs Sizes

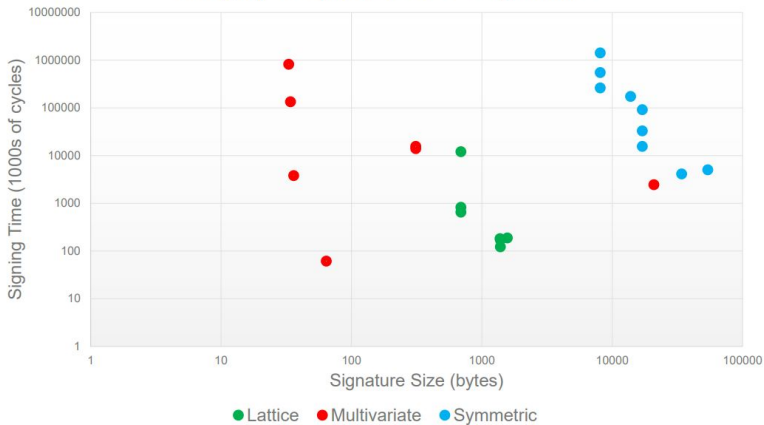


NIST Submissions - S1 Speed - PKE/KEMs

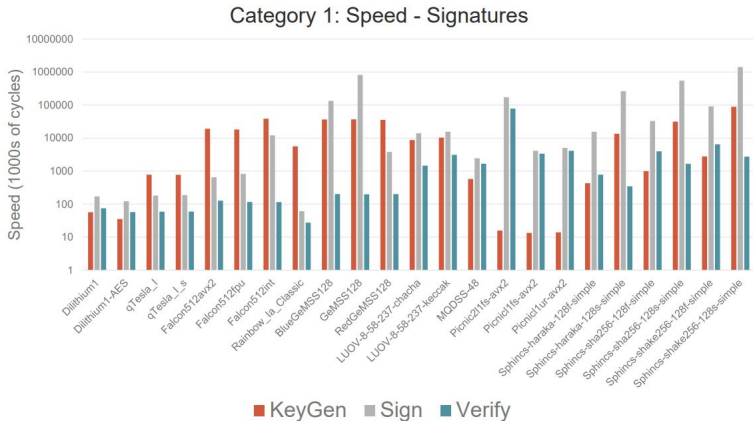




1. *Journal of Management Studies*, 1991, 28, 1, 1-14.



NIST Submissions - S1 Speed - Signature Schemes



Next Steps

- 1977. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems” RSA 23600 citations (4100 since 2015)
- 1978. McEliece, “A Public-Key Cryptosystem Based On Algebraic Coding Theory” 1920 citations (666 since 2015)
- 1998. NTRU, “NTRU: A Ring-Based Public Key Cryptosystem ” 1610 citations (624 since 2015)
- 2005. LWE, “On lattices, learning with errors, random linear codes, and cryptography” 2243 citations (1380 since 2015)
- 2010. Ring-LWE, “On ideal lattices and learning with errors over rings” 1245 citations (876 since 2015)

Next Steps

- “At the industry panel of the 2nd NIST PQC conference, there seemed to have been a consensus agreement that a hybrid mode (in which a post-quantum scheme is combined with an EC scheme so that the resulting scheme is at least as classically secure as the EC one) should be the default option for the foreseeable future.”, Vadim Lyubashevsky.
- “Integration of the os vendors, smart card vendors, piv card users to write the business requirements for pqc. We need to have more than cryptographic criteria documented for the selection.”

- “I think it is potentially worth standardizing “big” systems for use cases where online key exchange is rare (email, maybe). But I don’t see the case for using them in TLS on the web.”, Mike Hamburg.

What Should We Do?

- “NIST **should not** be aiming to conclude the process and have standards written by 2022. This is simply too fast to get proper answers? Much more research is needed.”
- “NIST should hold off creating any standard before 2025 and fund research efforts to look at all the candidates until that time. The process to date has provided the basis for a number of years of research. It is time to **give researchers a chance to innovate.**”

Recent Cryptanalysis Methods

- Breaking Rainbow Takes a Weekend on a Laptop, June 2022.
- An Efficient Key Recovery Attack on SIDH: SIKE is broken, August 2022.
- What is next?

Big Problem!

- **Quantum Algorithms for Lattice Problems** by Yilei Chen, April 10, 2024.
- We show a polynomial time quantum algorithm for solving LWE with certain polynomial modulus-noise ratios. Combining with the reductions from lattice problems to LWE shown by Regev, we obtain polynomial time quantum algorithms for solving the GapSVP and the (SIVP) for all n -dimensional lattices within approximation factors.

What will NIST do?

- NIST will create new draft standards for these algorithms, with coordination of the submission teams to ensure that the standards are in agreement with the specifications.
- The fourth round of evaluation and analysis will proceed similar to the earlier rounds.
- NIST would be interested in a **general-purpose digital signature** scheme which is not based on structured lattices.
- Even though the third round is ending and NIST will begin to draft the first PQC standards, standardization efforts in this area will continue for some time. **This should not be interpreted to mean that users should wait to adopt post-quantum algorithms.**

What will NIST do?

- NIST plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms in the summer of 2022.
- NIST primarily seeks to diversify its signature portfolio with non-structured lattice signature schemes.
- NIST may also be interested in signature schemes that have **short signatures** and **fast verification** (e.g., UOV).
- NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.

Post-Quantum Cryptography: Digital Signature Schemes

- NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices.
- For certain applications, such as certificate transparency, NIST may also be interested in signature schemes that have short signatures and fast verification.
- NIST is open to receiving additional submissions based on structured lattices, but is intent on diversifying the post-quantum signature standards.
- As such, any structured lattice-based signature proposal would need to significantly outperform CRYSTALS-Dilithium and FALCON in relevant applications and/or ensure substantial additional security properties to be considered for standardization
- There are 40 submissions.

Round 2

- NIST announced Round 2 Additional Digital Signature Candidates on October 24, 2024.
- HAWK, **FAEST**, CROSS, LESS, **MQOM**, **Mirath (merger of MIRA/MiRith)**, **PERK**, **RYDE**, **SDitH**, SQIsign, MAYO, SNOVA, QR-UOV, UOV.

Next Steps

- PQC key formats are not clearly specified.
- How to store / load the key from key formats (ordering)?
- Interoperability gets challenging.

Thank you for your attention!

Cordially invited to the **30th Nordic Conference on Secure IT Systems (NordSec)**, Tartu, Estonia, November 12-13, 2025

<https://nordsec2025.cs.ut.ee/>