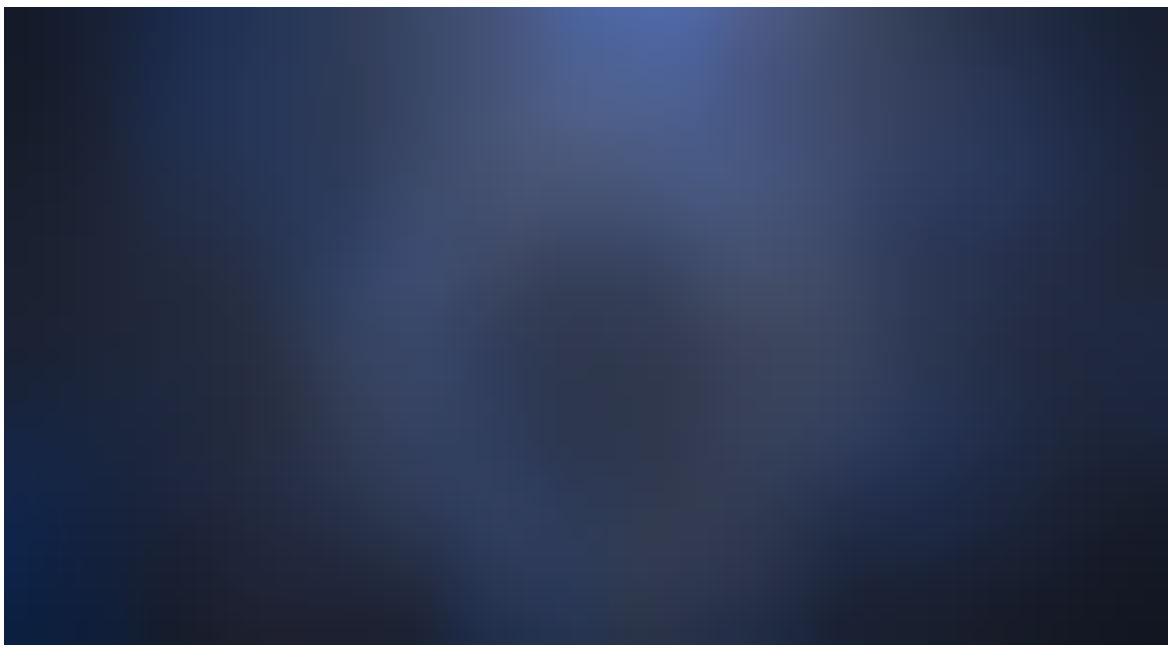
Post Quantum Cryptography Algorithms

Bhagvan Kommadi Follow
Jan 1 · 9 min read

Introduction



Financial institutions will be interested in securing their payment portals against potential future threats from future quantum computing capabilities. There is a need to make information systems "quantum resistant". There is a need for blockchain based products to improve the security using post-quantum cryptographic algorithms. The Quantum Resistant ledger is a cryptocurrency that strives to remain on the bleeding edge of security and functionality. "Quantum cryptography," also called "quantum key distribution," expands a short shared key into an effectively infinite shared stream. There is a need to improve the efficiency of post-quantum cryptography. Financial Firms need to have confidence in post-quantum cryptography. Software firms will continue to improve the usability of post-quantum cryptography. Blockchain security will be at risk when quantum computers emerge. Functioning cryptographic systems such as DES, Triple DES, AES, RSA, Merkle hash-tree signatures, Merkle–Hellman knapsack encryption, Buchmann–Williams class-group encryp-

tion, ECDSA, HFEv−, etc are going to break with a quantum computer. Shor's algorithm is the quantum-computer discrete-logarithm algorithm that breaks RSA and DSA and ECDSA cryptographic systems.

Quantum Algorithms

Quantum algorithms beat the classical computers not only because they run on faster hardware but also the quantum mechanical mathematics requires fewer steps. Quantum computers work on principles based on the behavior of subatomic particles as described by quantum mechanics. Quantum mechanics is a subfield of physics related to the complex behavior of subatomic particles such as electrons. Electrons can exist in multiple distinct states at the same time known as superposition. Heisenberg uncertainty principle states that a quantum system has complete knowledge of both an object's momentum and location. Any measurement of momentum will change the location because the act of observing the state changes it. Electrons can be "entangled". A change to one influences another when they are physically distant from each other. To capture these complexities, quantum mechanics describes the state of subatomic particles probabilistically using complex numbers.

Grover demonstrated that a quantum computer could solve a phone book search problem proportional to the square root of the number of phone book entries in O(√n) time. Grover's algorithm could find you in a

phone book with 100 million names with just 10,000 operations. One area in which quantum computing is already having an impact is encryption. The most widely used techniques for encrypting and protecting transactions depend on the impossibility of quickly finding the prime factors of large numbers. A quantum computer could conceivably break this type of encryption. The algorithm reduces the security of symmetric key cryptography by a root factor. AES-256 will offer 128-bits of security. Finding a pre-image of a 256-bit hash function would only take 2128 time. We can increase the security of a hash function or AES by a factor of two is not very burdensome. Researchers have set a new record for the quantum factorization of the largest number to date, 56,153, smashing the previous record of 143 that was set in 2012.

According to Scientific American research paper in 1977, it would take 40 quadrillion years to crack a message asymmetrically encrypted with the RSA-129 cipher. It was cracked around 1996 within six months by using a distributed network of computers. Ever increasingly larger asymmetric keys are required to securely distribute symmetric keys.

There is a need to make information systems “quantum resistant”.The first robust encryption protocol prototype showed a slow down of cracking process by 21 percent than the versions using elliptic curve cryptography. The mathematical operation of the new protocol is based upon multiplying polynomials together and adding some random noise. In 1994 Peter Shor developed a quantum algorithm for integer factorization that runs in polynomial time.

There are upcoming products and solutions in the post-quantum security area related to Data at rest, Data in transit, Access to data, Business Processes, Multi-party authentication, and Multi-Party Authorisation. They present algorithms and techniques to tackle Man-in-middle detection, quantum security encryption, Phishing resistance, Biometric Security, Accountability and segregation of Duties. Data at rest can be breached by an insider or an external attacker. Data in transit can be intercepted and tampered by malicious insiders and external aggressors across networks. Confidential business data and personally identifiable information are scenarios related to data in transit. Mission critical data cannot be protected by using simple role-based access and rigid role-based controls. Data governance need to be enforced across the organization.

POST QUANTUM CRYPTOGRAPHY

A classic problem in security solutions is to encrypt, decrypt, sign and verify transactions and data. On a classical computer using $< 2n$ operations, an attacker tries to intercept and steal the secure data like credit card numbers and social security of the customers. With a quantum computer, an attacker has a higher processing power and quantum algorithms like Shors to break the cryptographic systems. The goal of post-quantum cryptographic designers is improving the efficiency and usability & build the usability of the new algorithms. Complete hybrid systems and high-speed resistant algorithms are required to strengthen post-quantum cryptography based security solutions. McEliece public key encryption, NTRU public key encryption and lattice-based public key encryption systems are not yet broken by quantum algorithms.

The important classes of post-quantum cryptographic systems are hash-based, code based, lattice-based, multivariate quadratic equations and secret key cryptography. These are secure against both quantum and classical computers. These systems can interoperate with different communications protocols and networks. The goal for post-quantum cryptography research is to meet demands for cryptographic usability & flexibility and win the confidence from security experts.

POST QUANTUM SCHEMES

Post-quantum schemes protect confidentiality and provide integrity, authenticity, and non-repudiation. The post-quantum schemes related to post-quantum cryptography are elliptic curves, lattices, isogenies, multivariate, codes, hash functions, and hybrids.

MultiVariate algorithms refer to asymmetric cryptographic primitives based on multivariate polynomials over a finite field F. Multivariate quadratics which are polynomials of degree two are considered to be good candidates for post-quantum cryptography. They have a public and a private key. The private key consists of two affine transformations, S and T.

$S(x) = MSx + vS$ and $T(y) = MTy' + vT$ where vS is a shift vector. (S-1, P'-1,T-1) is the private key. The public key is the composition $P = S \circ P' \circ T$. Signatures are generated using the private key and are verified using the public key. The message is hashed using a hash function y. The signature is :

$x = P\text{-}1(y) = T\text{-}1\ (P'\text{-}1(S\text{-}1(y)))$

The receiver of the signed document must have the public key P in possession. Hash is computed using the function y which fulfills $P(x) = y$.

Hybrid schemes are using pre-quantum methods to establish the authenticated link and a mutual key. The key exchange is done using post-quantum algorithms. The protocol used for key exchanges is New Hope. Lattices and codes based algorithms require slight modification of NP-hard problems. Their weakness is that keys are large matrices. Crystals constructions based cryptographic systems are Kyber and Dilithium.

Kyber is a key-encapsulation mechanism uses algebraic number theory. Key sizes are approximately 1kb for reasonable security parameters. Encryption and decryption time is on the order of .075 ms. The Kyber KEM seems promising for post-quantum key exchange. Dilithium is a digital signature scheme which achieves quite good performance. Public key sizes are around 1kb and signatures are 2kb. The average number of cycles required to compute a signature was around 2 million and verification took 390,000 cycles on average.

Isogenies are functions that transform one elliptic curve into another. They use a Diffie-Hellman type protocol. The Supersingular Isogeny Diffie-Hellman scheme uses secret keys which are a chain of isogenies and public keys are curved. Isogenies traverse through a sequence of elliptic curves themselves. The group structure of the first curve is reflected in the second during transformation by isogenies. This is similar to a group homomorphism with some added structure dealing with the geometry of each curve. Supersingular elliptic curves are guaranteed to have a fixed number of isogenies from it to other supersingular curves. Isogeny-based cryptography has extremely small key sizes in the range of 330 bytes for public keys.

Hash-based constructions techniques are related to good hash functions. Hash signatures use inputs to a hash function as secret keys and outputs as public keys. Hash-based signatures are not post-quantum cryptography schemes because one cannot build a public key encryption scheme out of hashes. Hash signatures are not space efficient.

Lamport Diffie one time signature system signs a message generating uniform random string and computes the bits using a cryptographic hash function. Chaining is the technique to sign more than one message. The signer includes in the signed message a generated public key to sign the next message. The verifier checks the signed message and a new public

key is used to check the signature of next messages. The signature of the nth message consists all n-1 previous signed messages. Hash-based cryptography helps in securing post-quantum public key signature systems. Codes which can be considered for error correction cryptographic algorithms are Goppa, alternate, GRS, Gabidulin, Reed-Muller, Algebraic, BCH and Graph-based codes.

Most promising of all is Mceliece public key cryptosystem with Goppa codes. Mceliece is based on the difficult problem of decoding the unknown error-correcting code. Goppa codes have a fast polynomial-time decoding algorithm. From the family of Goppa codes, a private key is chosen from a generator matrix. The generator matrix is from the key space which consists of invertible binary matrix and permutation matrix. Different families are suggested for Goppa codes such as Generalized Reed-Solomon Codes, Gabidulin Codes and Reed Muller Codes. Pierre Loidreau modified by using automorphism group of Goppa codes. He did not increase the size of the public key. As the number of Goppa Codes increases exponentially with the length of the code and generating polynomial degree, the structural attacks against the system will be tough to penetrate. The work factor for the attacks would increase exponentially.

McEliece public key cryptography system has generator matrix G with parameters n, t to generate code G over F of dimension k and minimum distance d >= 2t +1. S is a k x k random binary non-singular matrix. P is a n x n random permutation matrix. SGP is computed by the matrix Gpub k x n matrix for Public key. A private key is based on S, Decoding algorithm DG and P the permutation matrix. To encrypt the message, use E(Gpub,t) function and decryption is done by using D(S,DG ,P) function.

QUANTUM KEY DISTRIBUTION

Quantum key distribution consists of a fiber or free space quantum channel to send the quantum state of light between transmitter and receiver. The channel may not be secured and communication link between two parties is authenticated and public. The key exchange protocol exploits quantum properties to ensure security. Error correction and privacy application are the post-processing steps to remove errors and information leakage. The quantum key distribution overcomes the challenges from a classic such as weak security because of random number generators, advances to CPU power, new attack strategies and the emergence of quantum computers.

Different approaches to quantum key distribution are Discrete Variable and continuous variable methods. The example protocols are Silberhorn and Grangier. Microsoft has been developing key exchange and signature algorithms. Key exchange algorithms are Frodo and Sike. These key exchange algorithms are based on the hardness of Learning with errors (lattices) problem and supersingular isogeny Diffie Hellman protocol respectively. Picnic and Tesla are signature schemes for post-quantum cryptography. The post-quantum digital signature algorithms are designed to provide security against attacks. These algorithms are built using a zero-knowledge proof system and symmetric key primitives.

CONCLUSION

Post Quantum cryptography is catching up and different types of cryptosystems such as multivariate, elliptic curves, lattices, isogenies, hash, hybrid based signatures are grabbing attention in academia and NIST. McEliece with Goppa codes is the reliable cryptosystem. Using a Shor's algorithm variant, quantum computer underpins the security of blockchain. Quantum cryptographic codes can secure block chains and the transactions. Quantum key distribution algorithms are evolving and post-quantum cryptography communities are proactively looking to come up with innovative techniques to tackle quantum computing process power.

REFERENCES

1. NIST Post Quantum Cryptography Project
2. Block Chain Research Institute Quantum Proofing Block Chain
3. European Telecommunications Standards Institute Quantum Safe Cryptography
4. Quantum Safe Security Working Group

First Name

Email

Give me access!

I agree to leave Medium.com and submit this