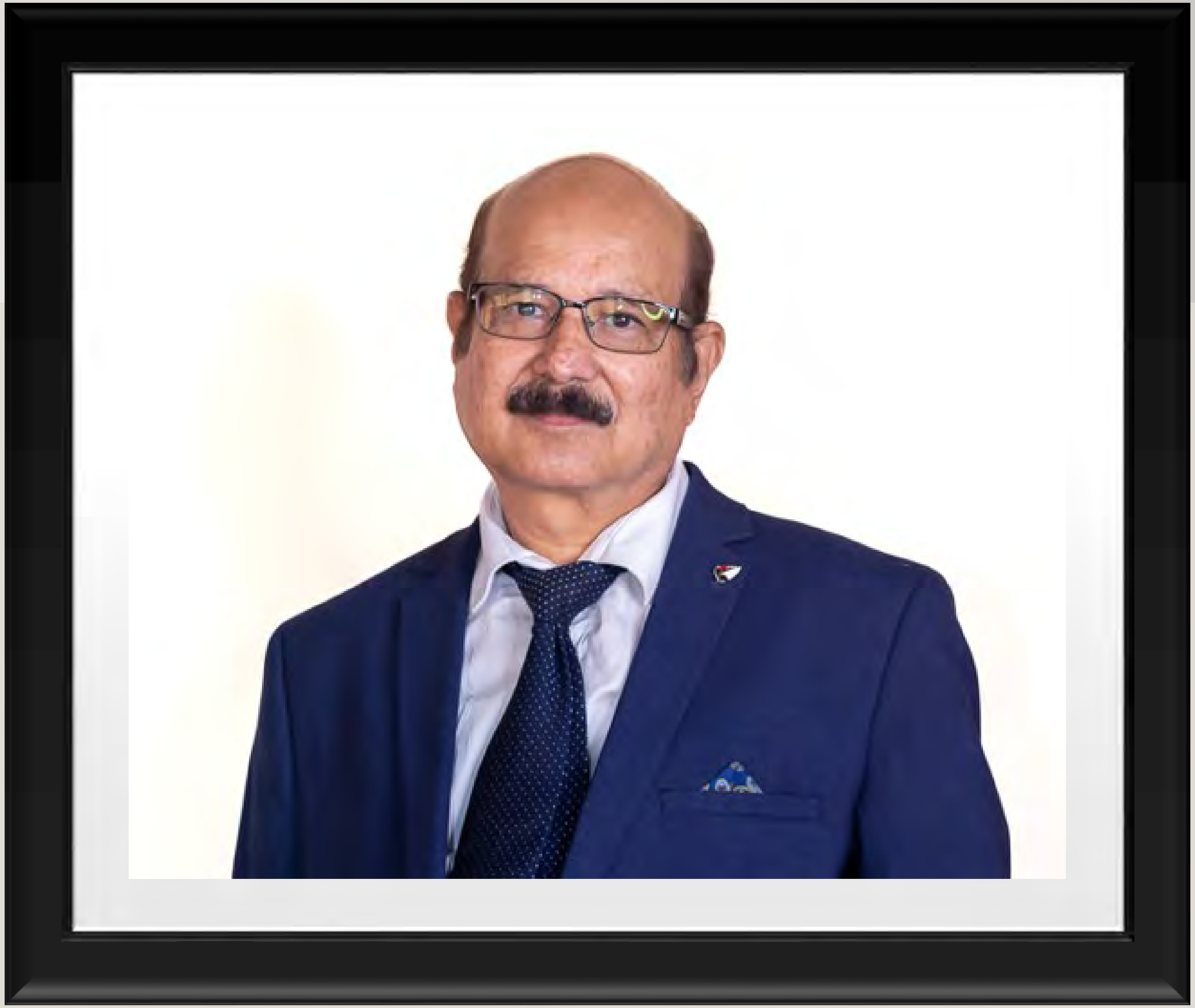
Challenges in Transitioning to Post quantum Cryptography

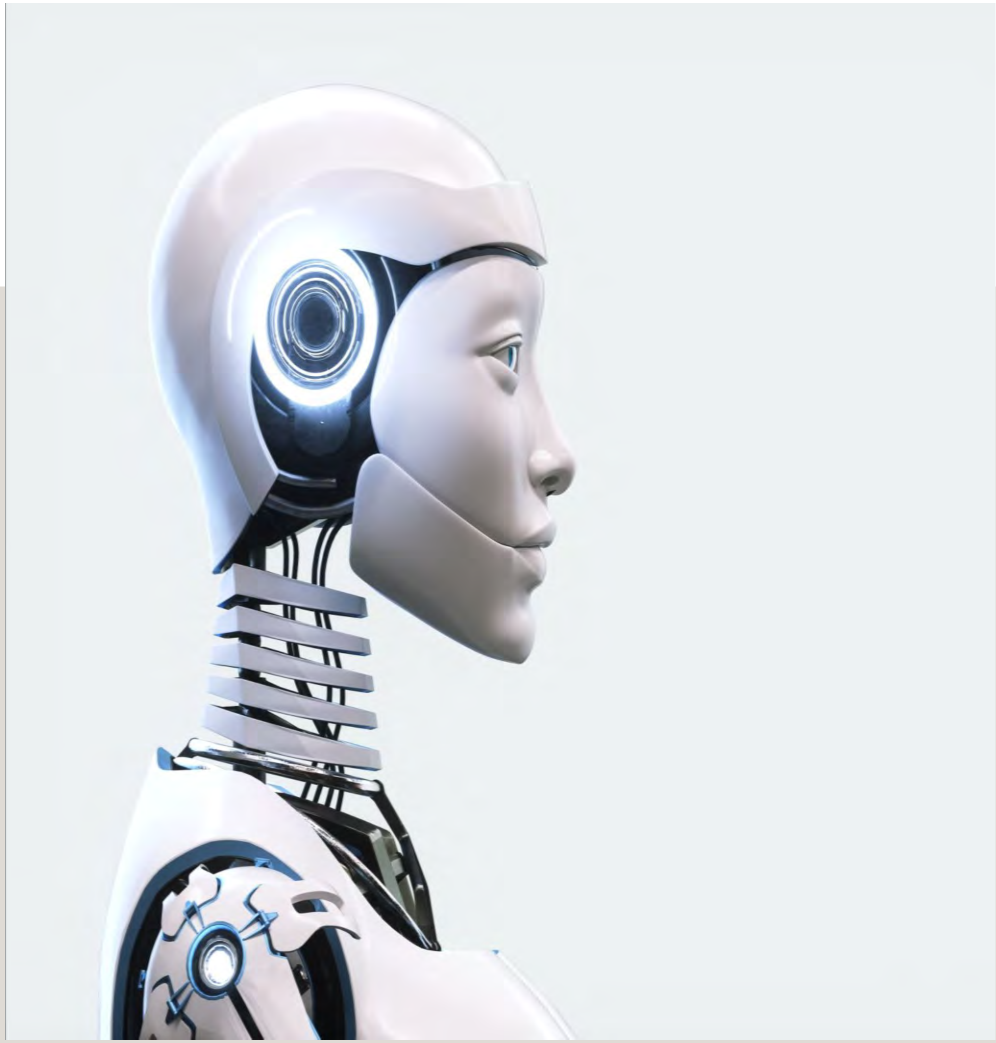
Dr. Bharat S. Rawal

Grambling State University

Dr. Bharat S. Rawal

D.Sc, M.Sc, M.B.A, SM-IEEE/EAI

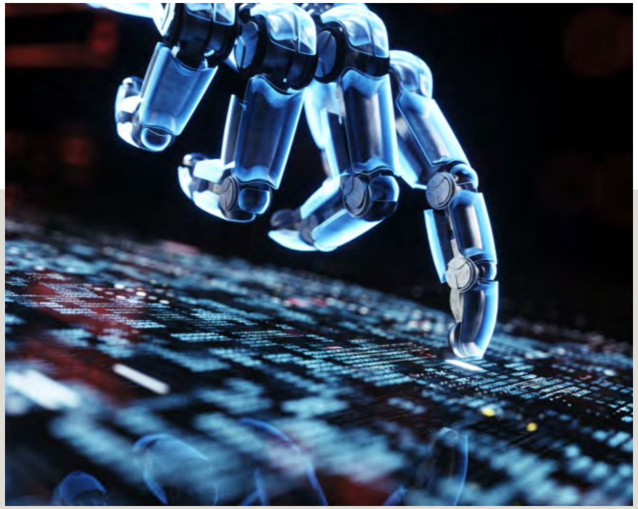




Educational Background

D.Sc. Information Technology, Towson University, December 2011.
M.B.A. UB/Towson University, December 2008.
M.Sc. Physics, South Gujarat University, India, May 1990.
B.Sc. Physics, South Gujarat University, India, May 1986.

Professional Experience

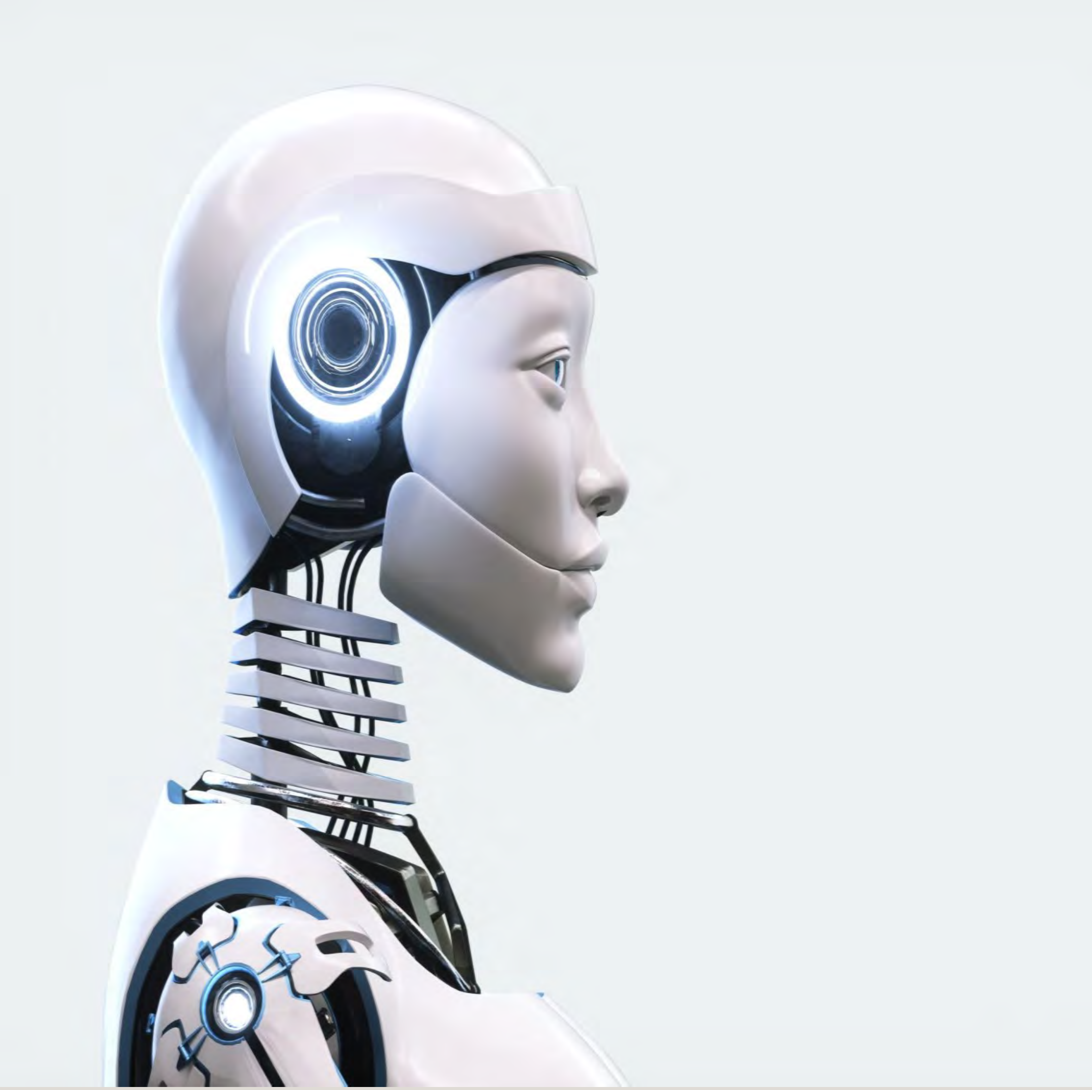


Industries : (Health Care / Pharmaceuticals) CEO/Chairman

IT/Cybersecurity, Quantum Computing CEO/ President

Academia: Assistant Professor / Associate Professor / Full Professor

Administrative: Program Co-Ordinator, Program Director, Department Chair



Scholarly Works

US Patents

Bharat S Rawal, Selvi, S. Sharmila, **Methods and systems for secure sharing of data between user devices using a Proxy Re-Encryption Key (PRE**)." U.S. Patent Application 16/688,642 filed September 3, 2020. Granted 2022

Bharat S Rawal, Dhananjay Singh." **Methods and systems for providing reward-based verified recommendations.** Published & Granted

U.S. Patent 11,386,444, issued July 12, 2022.

Books

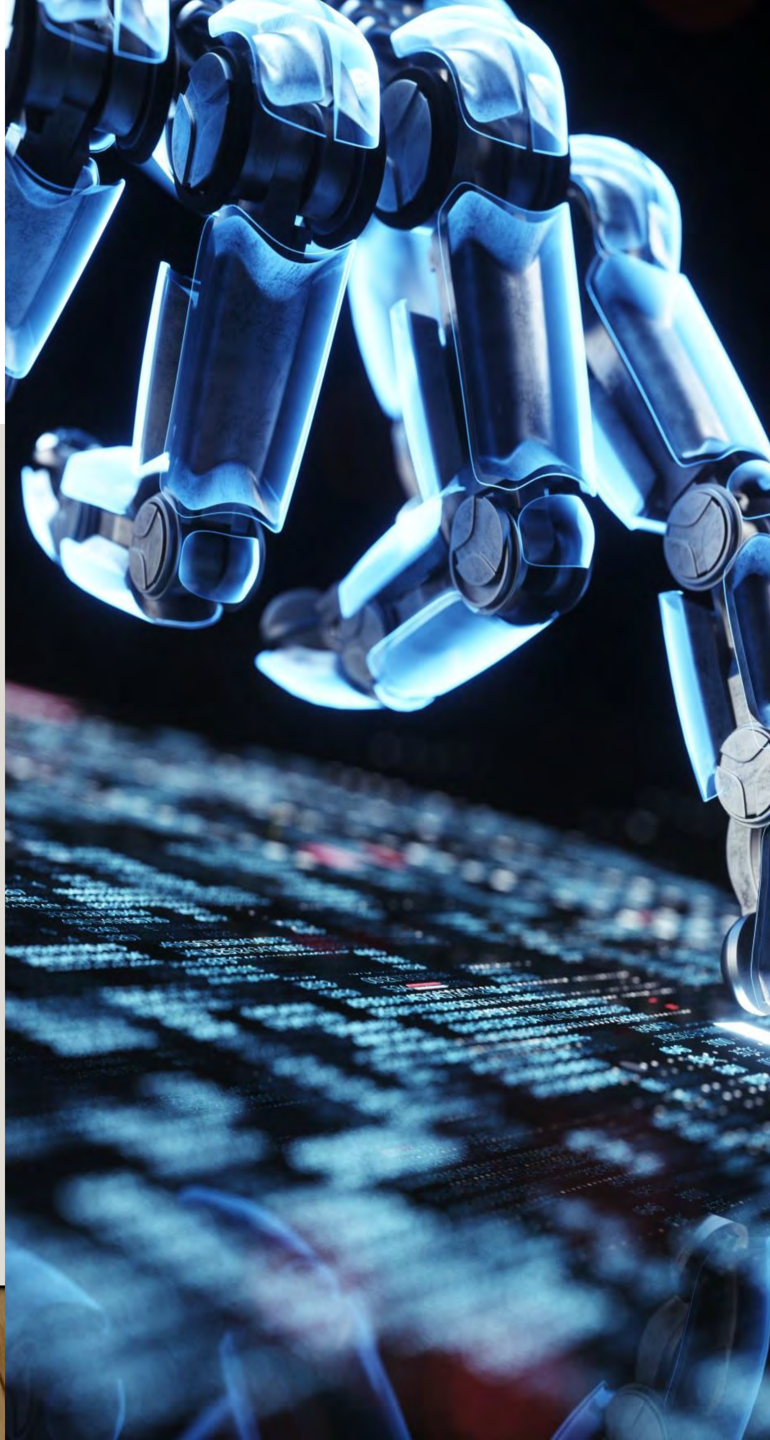
- Rawal, Bharat S., Gunasekaran Manogaran, and M. Poongodi. "Implementing and Leveraging Blockchain Programming." (2022).
  Authorship: First Author

- Rawal, Bharat S., Gunasekaran Manogaran, and Alexender Peter. "Cybersecurity and Identity Access Management." (2022).
- Authorship: First Author

- IET Book “Intelligent Multimedia Technologies for Financial Risk Management: Trends, Tools" - In press (2023).
- Authorship: Co-Author

- Springer’s Book “Artificial Intelligence in IoT and Cyborgization" (2023).
- Authorship: Co-Author

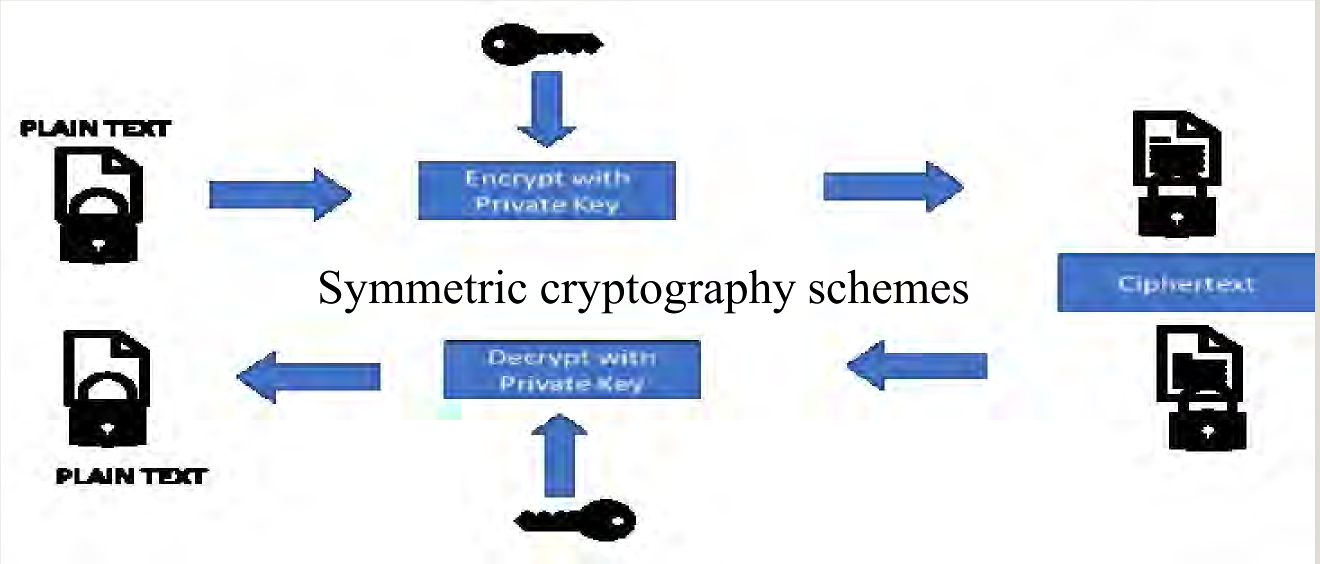
- Introduction to Quantum Computing Springer Book (2024) In Press
- Authorship: Co-Author



CRYPTOGRAPHY

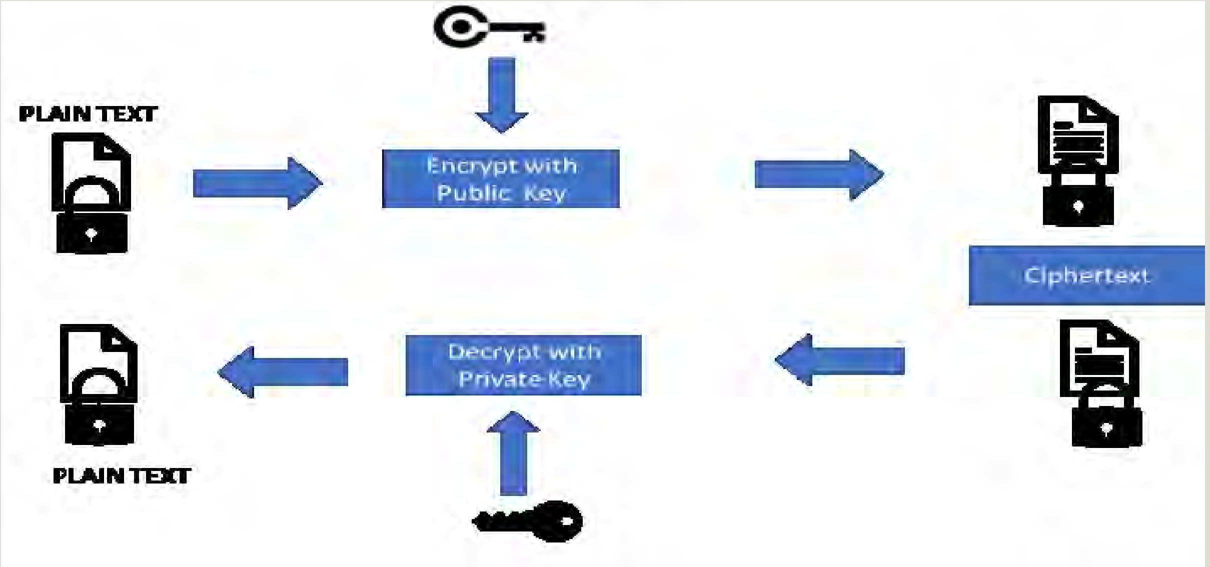
Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior. It involves constructing and analyzing protocols that prevent third parties or the public from reading private messages.

SYMMETRIC CRYPTOGRAPHY SCHEMES



Symmetric cryptography schemes

ASYMMETRIC CRYPTOGRAPHY SCHEMES



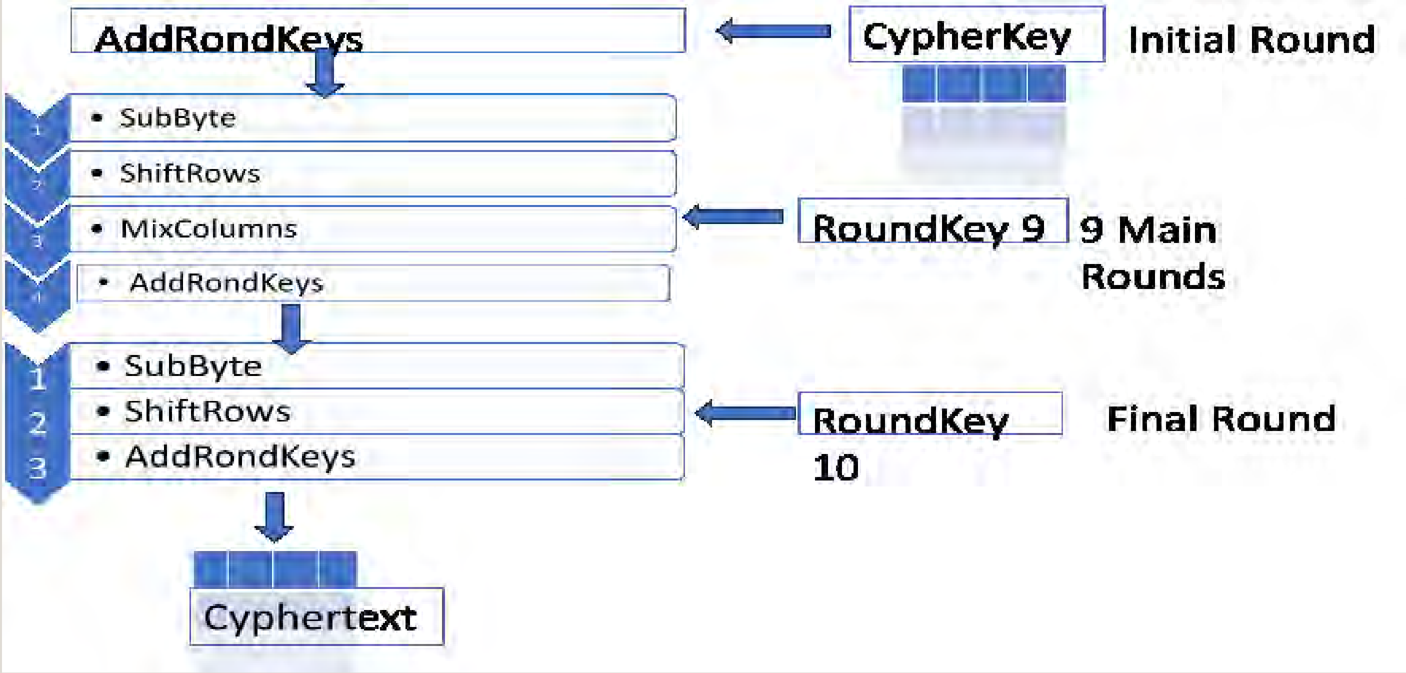
TYPES OF CRYPTOGRAPHY

- Hash-based Cryptography
- Code-based Cryptography
- Lattice-based Cryptography
- Elliptic Curve Cryptography (ECC)
- Homomorphic Encryption

WIDELY USED CRYPTOGRAPHY

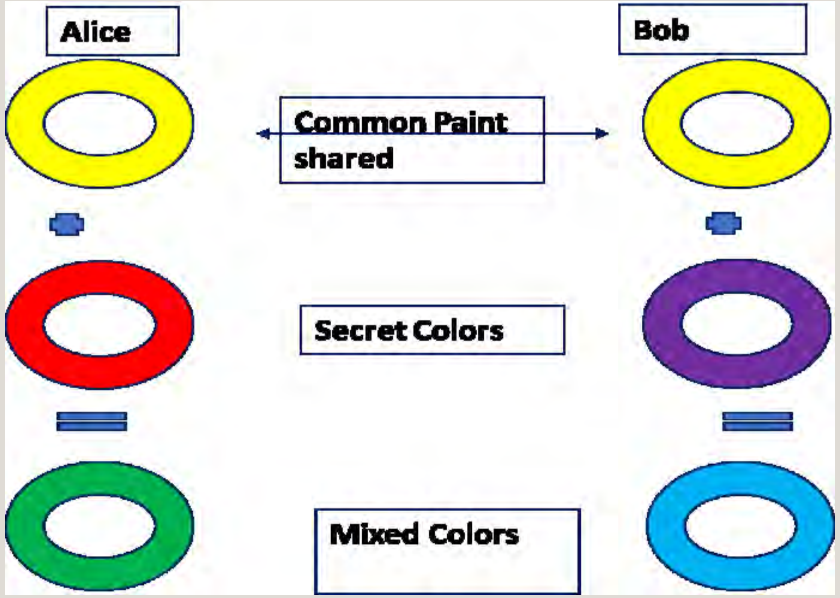
- Advanced Encryption Standard (AES): Known for its security and efficiency, AES comes in three key sizes: AES-128, AES-192, and AES-2561.
- Triple Data Encryption Algorithm (TDEA/Triple DES): DES is used three times in a row with distinct keys in symmetric encryption1.
- Blowfish: A symmetric block cipher that operates on 64-bit blocks.
- Twofish: Another symmetric block cipher designed as a successor to Blowfish.
- ChaCha20: A stream cipher known for its speed and security.
- RC4: A widely used stream cipher, although it has some vulnerabilities.
- Serpent: A symmetric block cipher with a 128-bit block size.
- Camellia: A symmetric block cipher developed jointly by Japan and NTT.
- IDEA (International Data Encryption Algorithm): A block cipher used in some legacy systems.

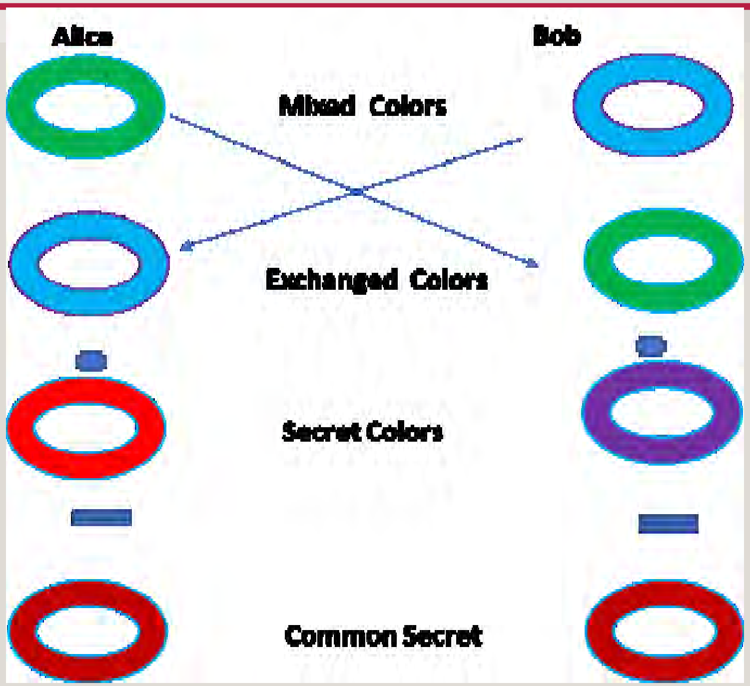
SYMMETRIC CRYPTOGRAPHY SCHEMES AES



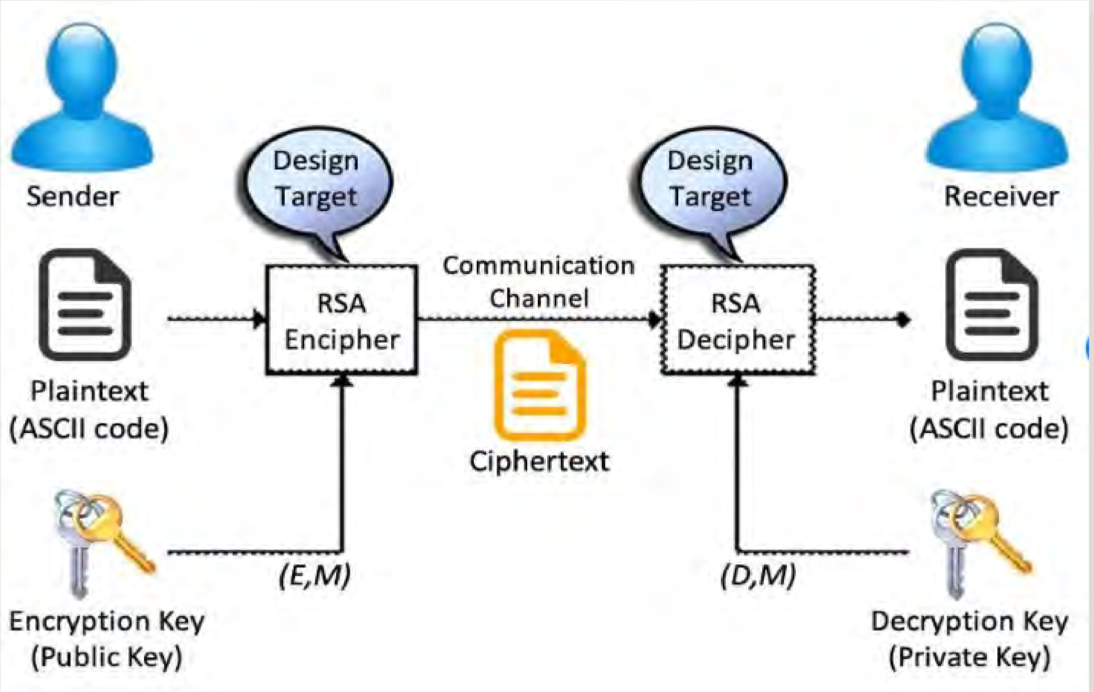
ASYMMETRIC CRYPTOGRAPHY SCHEMES

Diffie Helman Key Exchange





ASYMMETRIC CRYPTOGRAPHY SCHEMES
RIVEST–SHAMIR–ADLEMAN (RSA)



RSA algorithm structure

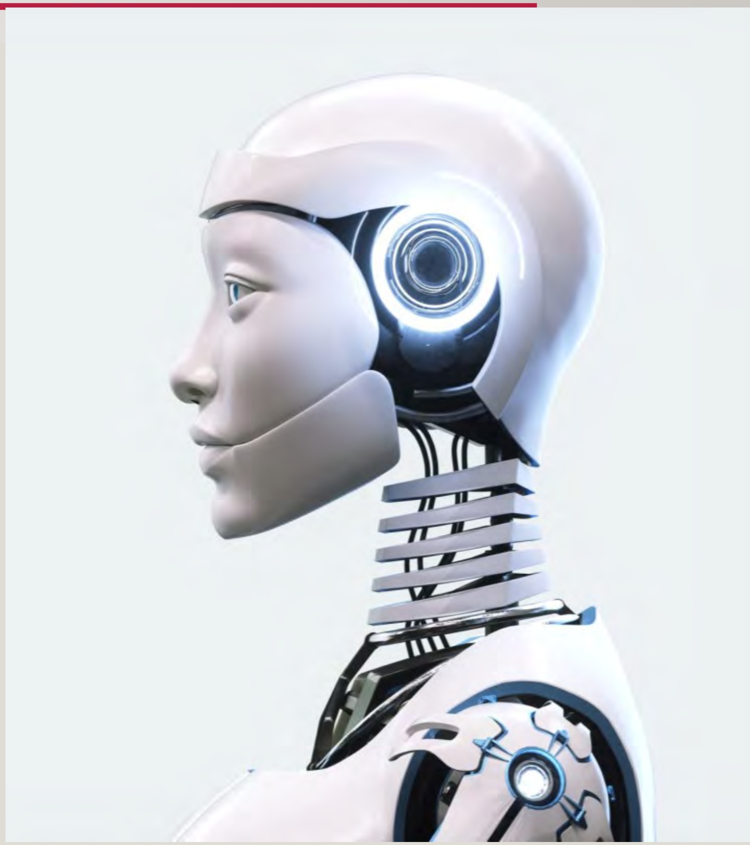
POST QUANTUM CRYPTOGRAPHY NOW

Shor's algorithms can break the following cryptosystems.
RSA
Diffie- Hellman key -exchange
Elliptical Curve Cryptosystem
Buchmann-William's Key exchange
Algebraic Homomorphic
When are we expecting the availability of large quantum computers? 10, 15, or 20 years, depending on the speed of technological advancements.
Why do we have to act now?

1) Development and standardization take time.
2) Improvement also takes time.
3) Take time to build confidence in PQC.
4) It takes time to improve the usability of PQC.
5) Last year 2022 NIST announces the list of PQC.

POST QUANTUM CRYPTOGRAPHY

Recently NIST has selected four cryptosystems: CRYSTALS-Kyber, Dilithium, FALCON, and SPHINCS+. CRYSTALS-Kyber is for use in general encryption. It offers several benefits including two parties can exchange relatively modest encryption keys and maintain the required speed of operation. It is faster among cross-platforms, and it is designed for efficient constant time implementation, same optimized routines across all parameters sets.



CRYSTALS-KYBER

CRYSTALS-Kyber uses a set of parameters to define the security level and efficiency of the scheme. The parameters include the dimension of the underlying lattice, the number of rounds for the encryption algorithm, and the number of bits used for public keys, secret keys, and ciphertexts. The specific values of these parameters can be chosen based on the desired security level.

Crystal-Kyber = [A; Public Key] [s; secrete key] + [e: (α, β, θ) small error terms]
= [t; public key]
$V = t\alpha, + \beta + m$
$U = A\alpha + \theta$
$D = V - sU$

FALCON

The snapshot of the Falcon cryptosystem is reproduced here under.
Falcon work over the cyclotomic ring R = Z q[x]/ (x^n + 1).
Keygen (): Generate matrices A, B with coefficients in R such that.
--> BA = 0
--> B has small coefficients
pk ←A
sk ← B

Sign (m, sk) (Performed using FFT)
Compute c such that cA = H(m)
v ← "a vector in the lattice Λ(B), close to c"
s ← c − v
The signature sig is s = (s1, s2)

Verify (m, pk sig)
Accept if:
s is short
sA = H(m)
The main design goal is compactness: to minimize |pk| + |sig

CRYSTALS-Dilithium

The signature scheme is reproduced here

Gen

$A \leftarrow Rq(k \times l)$

$(s1, s2) \leftarrow Sl\eta \times Sk\,\eta$

$t := As1 + s2$

return $(pk = (A, t), sk = (A, t, s1, s2))$

Sign (**sk**, **M**)

$z := \perp$

While $z = \perp$ do

$y \leftarrow S\,l\,\gamma1 - 1$

$w1 := \text{HighBits}(Ay, 2\gamma2)$

$c \in B60 := H(M \parallel w1)$

$z := y + cs1$

if $\|z\|\infty \geq \gamma1 - \beta$ or $\|\text{LowBits}(Ay - cs2, 2\gamma2)\|\infty \geq \gamma2 - \beta$, then $z := \perp$

return $\sigma = (z, c)$

Verify $(pk, M, \sigma = (z, c))$

$w'1 := \text{HighBits}(Az - ct, 2\gamma2)$

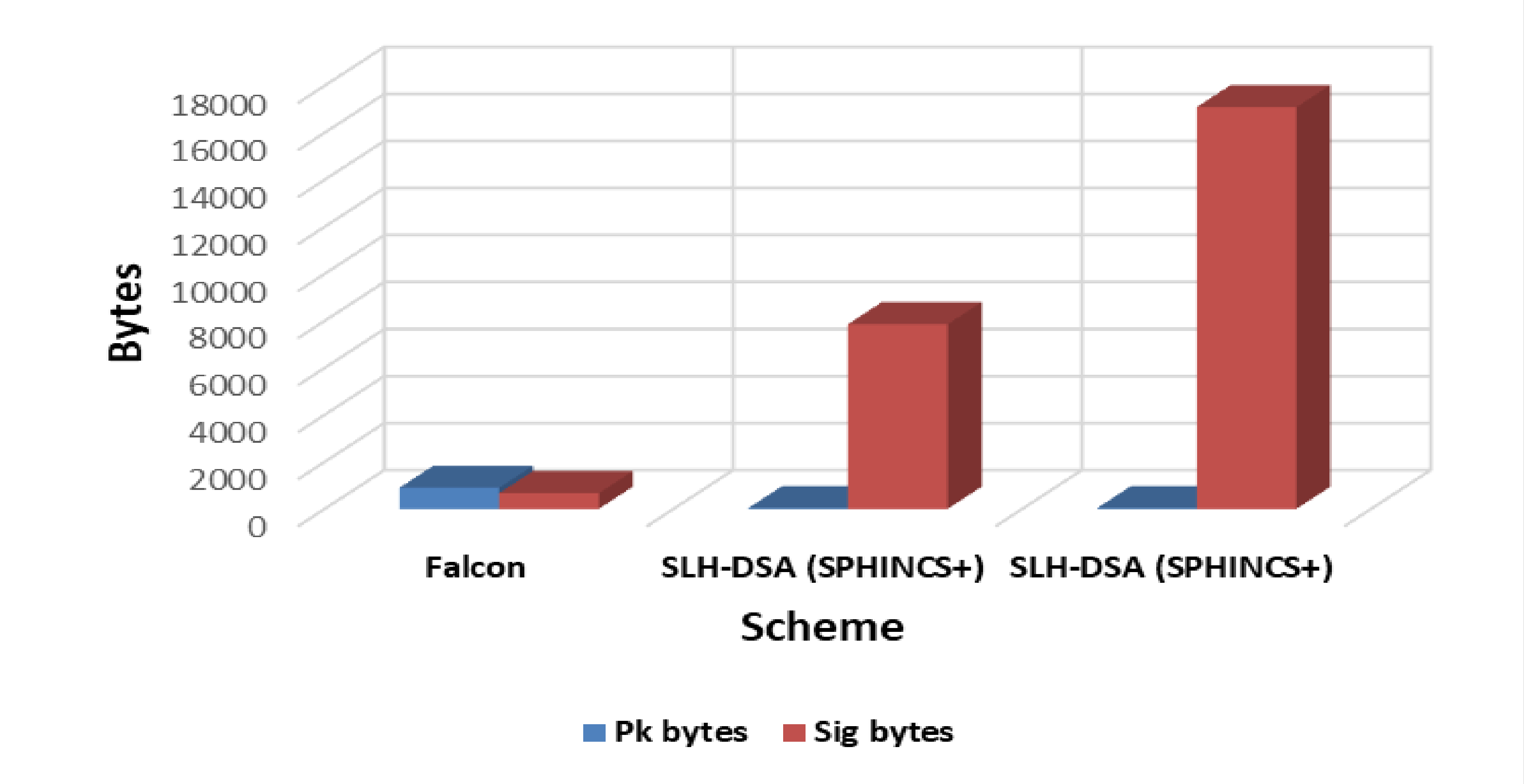
if return $[\ \|z\|\infty < \gamma1 - \beta]$ and $[c = H(M \parallel w'1)]$

SPHINCS+

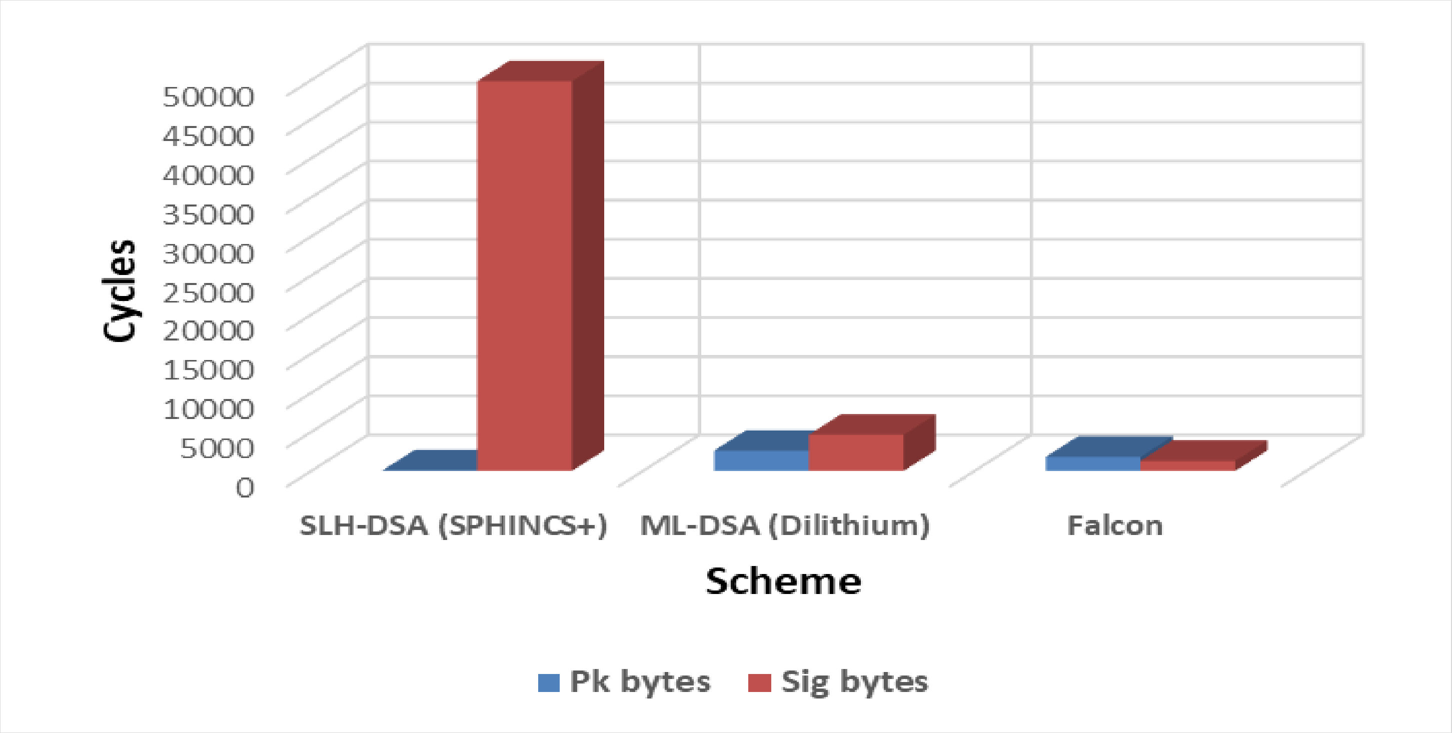
SPHINCS+ cryptography which utilizes FTS schemes [24]. This method uses a so-called hyper tree to authenticate a large number of key pairs with few-time signatures. Signature schemes known as "few-time signatures' enable a key pair to generate a limited quantity of signatures. For every new communication, a pseudo-random FTS key pair is chosen to sign it. The FTS signature and the authentication data for that FTS key pair make up the signature. A hyper tree signature, or a signature using a certification tree of a Merkle tree signature, represents the authentication information.

PQC

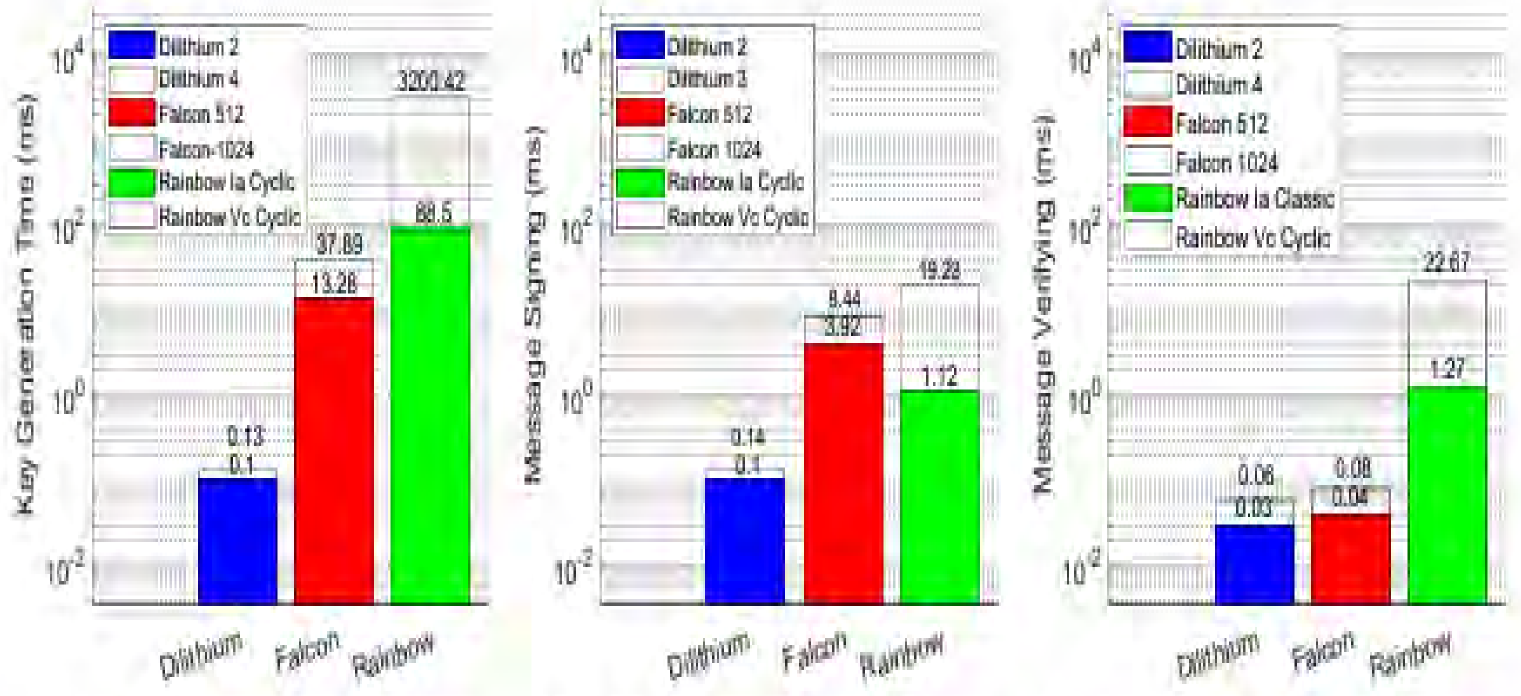
The comparison of key size with Falcon for security level 1.



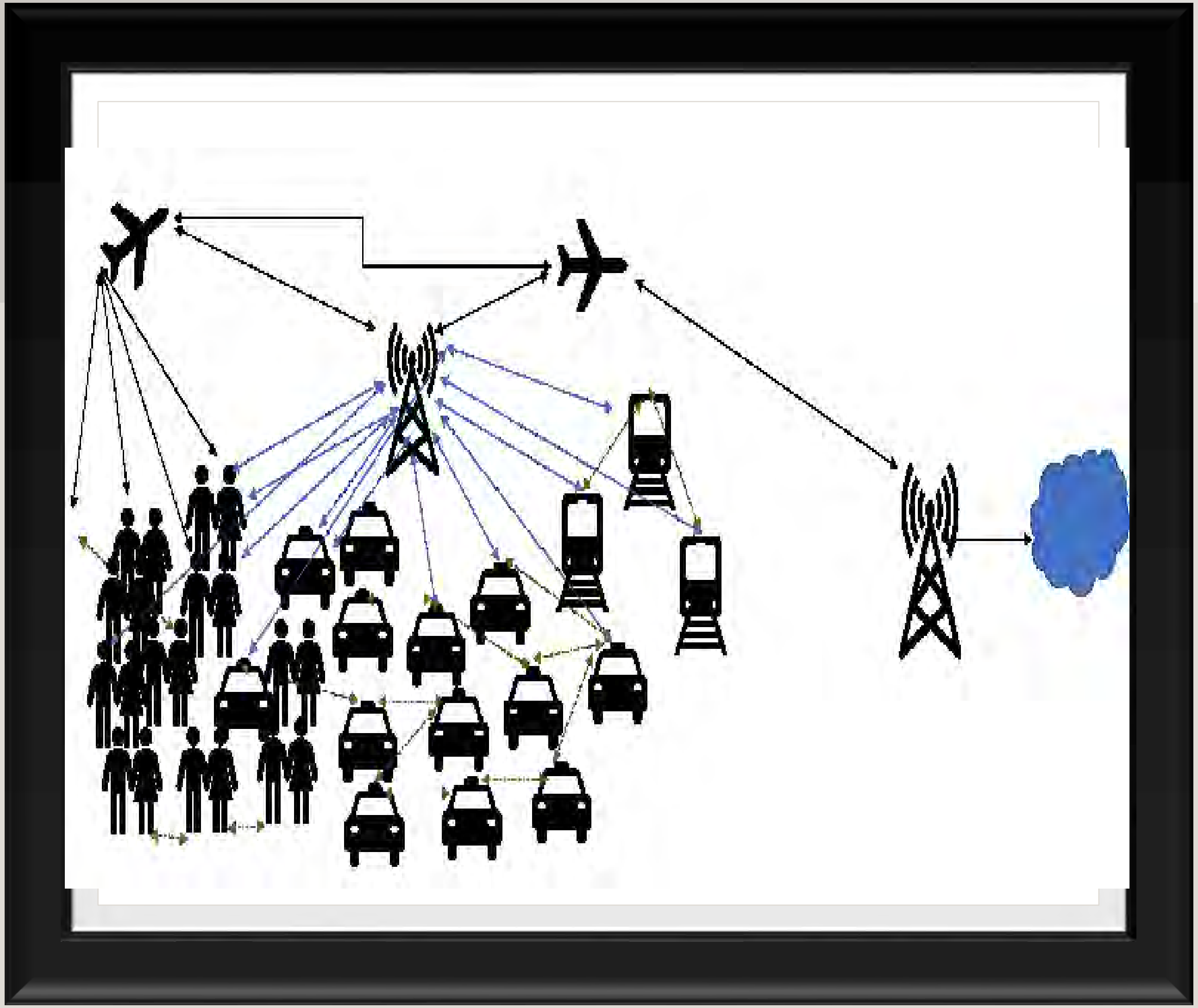
Comparisons the public key sizes and signature bytes of Falcon and SPHINICS+ and Dilithium at NIST security level 5.

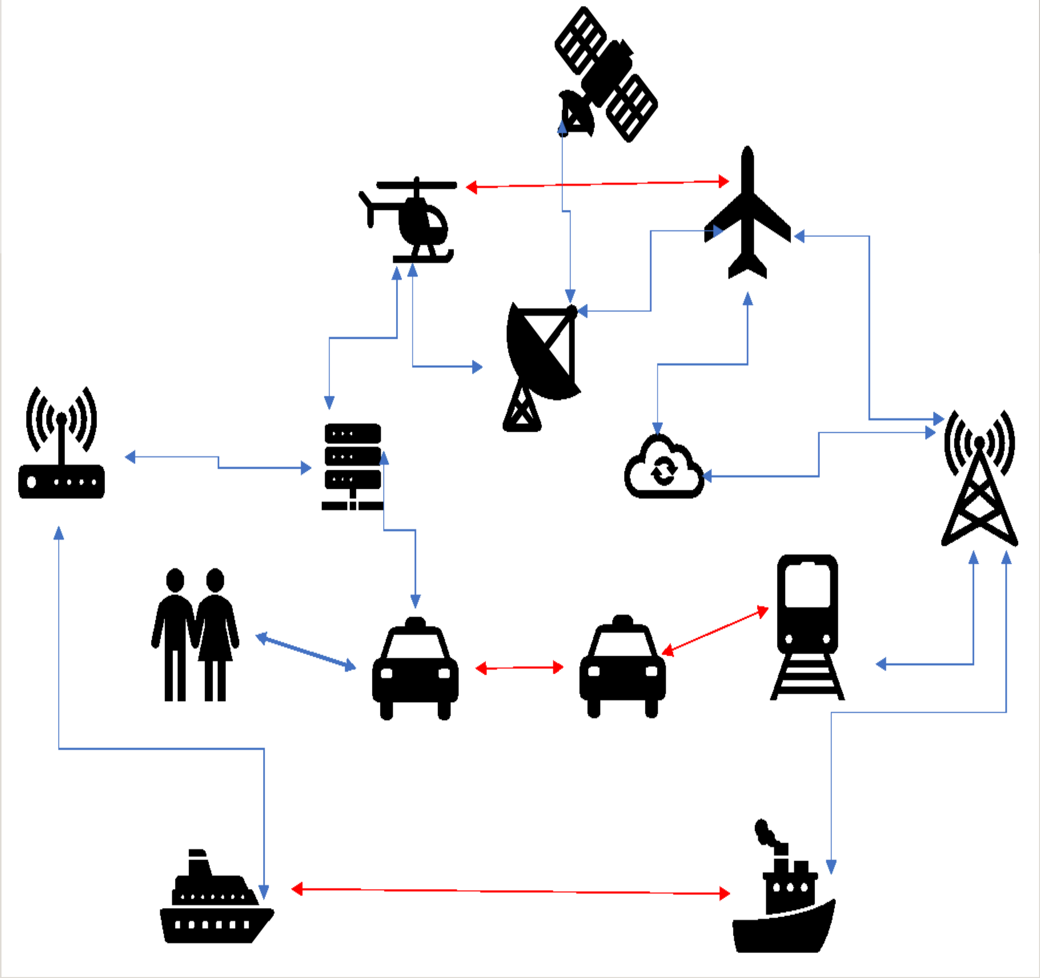


The fastest (colored bar) and slowest (outlined bar) signature candidates from each family cross the three signature phases, with a message length of 100 Bytes



(a) Key generation time (b) Message signing time (c) Message verifying time





No-Sum Sequence

We reproduce a quick overview of the NS sequence here [45,46]. If any element cannot be represented as a sum of any subset in a given set, this sequence can be termed an NS sequence. Each of its elements cannot equate to the sum of any combinations of the other non-repeated elements in the sequence where any element is a positive number. The NS sequence reproduced here could be mathematically represented as given in the equation under [37].

No-Sum Sequence

1	3
2	4
3	5
4	6
5	16
6	17
7	49
8	50
9	148
10	149
11	445
12	446
13	1336
14	1337
15	4009
16	4010
17	12028
18	12029
19	36085
20	36086

PQC Share

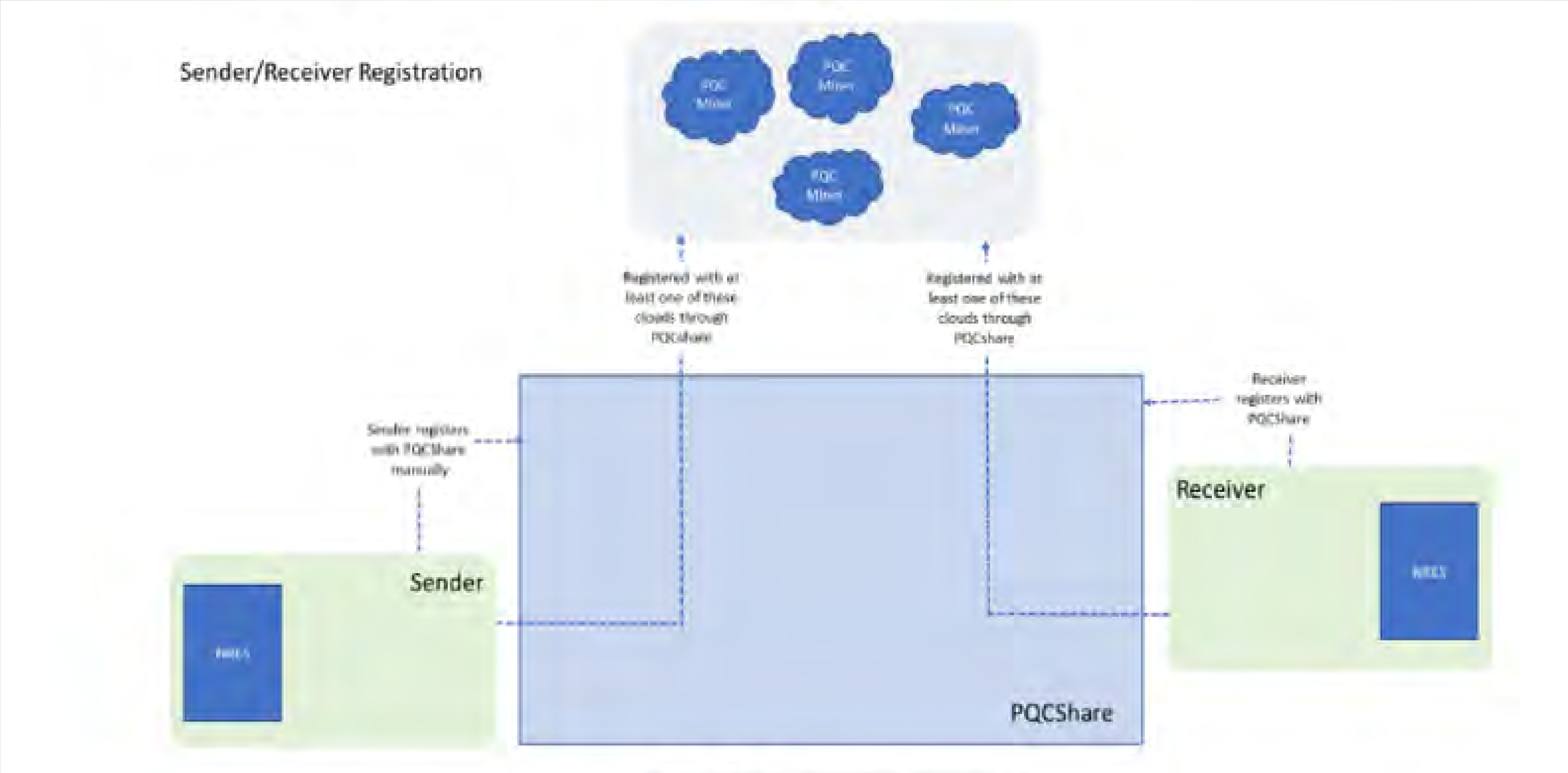


FIG. 24 Registration process

It is too early to draw a conclusion since we are in the preliminary stages of exploration and standardization, but we observed in PQC that great security comes with an increase in key length, which could delay the handshake process and has an impact on the performance the system. Also, we expect the hardware to scale in performance and hard speed. We can see several solutions exist to overcome the large key sizes, software, and hard hardware faults, and malfunctions due to the complex implementation of PQC.

We proposed other cryptographic primitives to make the most popular cryptosystems quantum safe. We suggest adding additional security for smaller lattice based PQC systems so that our current network system can handle them without significant delays. Also, we explore the technique for verifying the source of the QKD transmission solving NS sequence puzzle at both ends.

Questions ????

REFERENCES

1. Valentijn, Ashley. "Goppa codes and their use in the McEliece cryptosystems." (2015).
2. Post-Quantum Cryptography | CSRC. (2017, January 3). Post-Quantum Cryptography | CSRC. https://csrc.nist.gov/projects/post-quantum-cryptography
3. https://www.cryptomathic.com/news-events/blog/summary-of-cryptographic-algorithms-according-to-nist
4. Joseph, D. Paul, M. Krishna, and K. Arun. "Cognitive analytics and comparison of symmetric and asymmetric cryptography algorithms." Int. J. Adv. Res. Computer. Sci 6, no. 3 (2015): 51-56.
5. B. S. Rawal, "Quantum Integrated (C+G+Q)PU Split Architecture," 2023 International Wireless Communications and Mobile Computing (IWCMC), Marrakesh, Morocco, 2023, pp. 1466-1471, doi: 10.1109/IWC
6. Ducas, Léo, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "Crystals-dilithium: A lattice-based digital signature scheme." IACR Transactions on Crypto
7. Aguilera, A. Cano, X. Arnal I. Clemente, D. C. Lawo, I. Tafur Monroy, and JJ Vegas Olmos. "First end-to-end PQC protected DPU-to-DPU communications." Electronics Letters 59, no. 17 (2023): e12901.
8. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/W2VOzy0wz_E/m/XLBCDKYjBQAJ?utm_medium=email&utm_source=footer&pli=1.
9. Zeng, Pei, You Zhou, and Zhenhuan Liu. "Quantum gate verification and its application in property testing." Physical Review Research 2, no. 2 (2020): 023306.
10. Rawal, Bharat, and Alexander Peter. "Quantum-Safe Cryptography and Security." Implementing and Leveraging Blockchain Programming (2022): 35-51
11. J. Wang, M. Zhang, J. -S. Lai, W. -Y. Zhao and H. -Y. Zhang, "Analysis on noise impact in algorithm-based quantum computing benchmark," 2022 20th International Conference on Optical Communications ar
12. Zhang, Shan, Jiayin Chen, Feng Lyu, Nan Cheng, Weisen Shi, and Xuemin Shen. "Vehicular communication networks in the automated driving era." IEEE Communications Magazine 56, no. 9 (2018): 26-32.
13. Wang, Rui, Obada Alia, M. J. Clark, Sima Bahrani, Siddarth Koduru Joshi, D. Aktas, George T. Kanellos et al. "A dynamic multi-protocol entanglement distribution quantum network." In 2022 Optical Fiber Com
14. R. Nejabati, R. Wang and D. Simeonidou, "Dynamic Quantum Network: from Quantum Data Centre to Quantum Cloud Computing," 2022 Optical Fiber Communications Conference and Exhibition (OFC), 202
15. Ioannidis, Sotiris, Angelos D. Keromytis, Steve M. Bellovin, and Jonathan M. Smith. "Implementing a distributed firewall." In Proceedings of the 7th ACM conference on Computer and communications security
16. BOS, J. W., COSTELLO, C., NAEHRIG, M., AND STEBILA, D. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In 2015 IEEE Symposium on Security and Privacy (
17. DE CLERCQ, R., ROY, S. S., VERCAUTEREN, F., AND VERBAUWHEDE, I. Efficient software implementation of ring-LWE encryption. In Design, Automation & Test in Europe Conference & Exhibition, DATE
18. ALBRECHT, M., BAI, S., AND DUCAS, L. A subfield lattice attack on overstretched NTRU assumptions. IACR Cryptology ePrint Archive report 2016/127, 2016. http://eprint.iacr. org/2016/127. 8, 10
19. Moon, J., Jung, I.Y. and Park, J.H., 2018. IoT application protection against power analysis attack. Computers & Electrical Engineering, 67, pp.566-578.
20. Kumar, Adarsh, Carlo Ottaviani, Sukhpal Singh Gill, and Rajkumar Buyya. "Securing the future Internet of things with post-quantum cryptography." Security and Privacy 5, no. 2 (2022): e200.
21. Suhail, S., Hussain, R., Khan, A., & Hong, C. S. (2020). On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions. IEEE Internet of Things Journal, 8(1), 1
22. Introduction to post-quantum cryptography) By Daniel J, Bernstein, Johannes Buchmann, Erik Dahemen: By Springer
23. Sajimon, P. C., Kurunandan Jain, and Prabhakar Krishnan. "Analysis of post-quantum cryptography for internet of things." In 2022 6th International Conference on Intelligent Computing and Control Systems (I
24. Peikert, Chris. "Public-key cryptosystems from the worst-case shortest vector problem." In Proceedings of the forty-first annual ACM symposium on Theory of computing, pp. 333-342. 2009.
25. https://pqshield.github.io/nist-sigs-zoo/wide.html
26. Overbeck, Raphael, and Nicolas Sendrier. "Code-based cryptography." In Post-quantum cryptography, pp. 95-145. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.
27. Elias, Peter. "Universal codeword sets and representations of the integers." IEEE transactions on information theory 21, no. 2 (1975): 194-203.
28. NISTIR 8105 Report on Post-Quantum Cryptography 10

REFERENCES

29. https://www.nist.gov/cryptography#:~:text=NIST%20continues%20to%20lead%20public,encrypting%20large%20amounts%20of%20data Accessed on 12/28/2023.30
30. https://quantum- computing.ibm.com/composer/docs/iqx/guide/shors-algorithm.
31. Bernstein, Daniel J. "Curve25519: new Diffie-Hellman speed records." In Public Key Cryptography-PKC 2006: 9th International Conference on Theory and Practice in Public-Key Cryptography, New York, NY, USA, April 24-26, 2006. Proceedings 9, pp. 207-228. Springer Berlin Heidelberg, 2006.
32. Yang, Yipei, Zongyue Wang, Jing Ye, Junfeng Fan, Shuai Chen, Huawei Li, Xiaowei Li, and Yuan Cao. "Chosen ciphertext correlation power analysis on Kyber." Integration 91 (2023): 10-22. https://www.youtube.com/watch?v=FUb75AUXMvw&t=1694s. Accessed on 06/28/2023.
33. Kampanakis, Panos, and Dimitrios Sikeridis. "Two post-quantum signature use-cases: non-issues, challenges, and potential solutions." In Proceedings of the 7th ETSI/IQC Quantum Safe Cryptography Workshop, Seattle, WA, USA, vol. 3. 2019
34. https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/) Accessed on 10/28/2023.
35. https://cryptopedia.dev/posts/kyber/ Accessed on 12/28/2023.36.
36. Rawal, Bharat S., Songjie Liang, Shiva Gautam, Harsha Kumara Kalutarage, and Pandi Vijayakumar. "Nth order binary encoding with split-protocol." International Journal of Rough Sets and Data Analysis (IJRSDA) 5, no. 2 (2018): 95-118.37.
37. Giacomo Pope, CRYSTALS-Kyber Python Implementation [here]
38. Fernandez-Carames, Tiago M., and Paula Fraga-Lamas. "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks." IEEE Access 8 (2020): 21091-21116
39. https://csrc.nist.gov/CSRC/media/Presentations/falcon-round-2-presentation/images-media/falcon-prest.pdf
40. Ducas, Léo, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "Crystals-dilithium: A lattice-based digital signature scheme." IACR Transactions on Cryptographic Hardware and Embedded Systems (2018): 238-268.
41. B. Shi, D. Leo, E. Kiltz, et al., "Crystals-dilithium algorithm specifications and supporting documentation," 2020, https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.
42. https://cryptobook.nakov.com/key-exchange/diffie-hellman-key-exchange
43. Rawal, Bharat S., and Gunasekaran Manogaran. "Implementation of a secure multi-cloud storage framework with next-generation cryptosystems and split-protocol." In 2021 International Symposium on Networks, Computers, and Communications (ISNCC), pp. 1-6. IEEE, 2021.
44. Rawal, Bharat S., and Sai Tarun Gollapudi. "No-Sum IPsec Lite: Simplified and lightweight Internet security protocol for IoT devices." In 2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 4-9. IEEE, 2021.
45. Rawal, Bharat, and Alexander Peter. "Quantum-Safe Cryptography and Security." Implementing and Leveraging Blockchain Programming (2022): 35-51.