IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501

Vol.14, No 3 Sep 2024

Application for Quantum Secure Email Client

Mr. V. Arun Kumar [1], M. Praisy [2], P. Anusha [3], S. Dhanandhuka [4]

[1] Assistant Professor, Malla Reddy Engineering College for Women (Autonomous Institution) Hyderabad.

[2] [3] [4] Student, Malla Reddy Engineering College for Women (Autonomous Institution) Hyderabad.

ABSTRACT:

The future of public-key cryptography systems is uncertain in light of recent developments in the capabilities of quantum computers and Shor's groundbreaking work on the prime factorization of integers using quantum algorithms. When it comes to protecting cryptographic systems from quantum computers, there are two separate but related fields of study: post-quantum cryptography and quantum cryptography. With these technologies becoming more accessible, it is important to integrate them into various applications to learn about their features, benefits, and drawbacks, as well as to evaluate them. Here, we go into the topic of secure messaging apps that use quantum-resistant encryption. Our focus is on the open-source messaging program Delta Chat, which provides end-to-end security. The end-to-end secure messaging properties of the system are maintained by integrating post-quantum secure digital signature schemes and public-key encryption schemes. Additionally, server-to-server communication is secured via secret keys provided by a metropolitan quantum key distribution network. Because Delta Chat uses users' email accounts to transmit messages, we also get an email infrastructure that is immune to quantum computing. In light of this, we also examine the methods often used to encrypt email and the necessary measures to establish a quantum-system for S/MIME and OpenPGP users.

INTRODUCTION

With the rise of electronic communication, secure messaging has become an essential component of the modern digital world. The primary objective of secure messaging apps is to provide a safe environment for users to transmit sensitive information without worrying about prying eyes. The reasons behind utilizing encrypted messaging solutions might differ based on the circumstances. Secure messaging offers a technological solution to the problem of

eavesdropping and spying by unauthorized parties, such as government agencies and cybercriminals. Businesses, nonprofits, and even government entities are considering implementing encrypted communications systems. Without worrying about information leakage, employees of these firms may safely communicate and discuss sensitive data, trade secrets, intellectual property, financial records, and legal problems via these platforms. So, encrypted messaging services lessen the possibility of sensitive data leaks. Many apps that allow for encrypted chat have been more popular in the past few years. On top of the X3DH key agreement system, Signal provides asynchronous end-to-end secure messaging for both individuals and groups. Protocols like off-the-record (OTR) messaging offered encrypted communications to users of Internet Relay Chat (IRC) networks, Extensible Messaging and Presence Protocol (XMPP), and others long before messaging apps like Signal or WhatsApp were popular. Even while OTR is seen as a forerunner of the protocol used in Signal, it should be remembered that at first, OTR only provided secure messaging for two participants in a synchronous scenario, meaning that both sides had to be online simultaneously. Group communication was later introduced. There is a plethora of secure messaging apps available today, each with its own set of advantages and disadvantages in terms of security assurances, on-premise deployment choices, and supported functionality.

RELATED WORK

"Let's Encrypt: A Web-wide Automated Certificate Authority."

When it comes to promoting HTTPS adoption throughout the Web, one option is Let's Encrypt, a free, open, and automated HTTPS certificate authority (CA). After launching at the tail end of 2015, Let's Encrypt has developed into the biggest HTTPS CA in the world, with more valid certificates than any other browser-trusted CA put together. Over 223 million domain names had their certificates granted by January 2019. Including the design of the CA software system (Boulder) and the structure of the organization that runs it (ISRG), we detail how we constructed Let's Encrypt and talk about what we learnt along the way. We also take a look at the varied ecosystem of ACME clients, including Certbot, a software agent we developed to automate HTTPS deployment, and explain the architecture of ACME, an IETF-standard protocol that we built to simplify CA--server interactions and

certificate issuing. Lastly, we assess how the CA ecosystem and the Web have been affected by Let's Encrypt. If Let's Encrypt is successful, it will hopefully serve as a template for future improvements to the Web PKI and the security architecture of the Internet.

"Process for Standardizing Post-Quantum Cryptography by the NIST,"

By means of a public, competition-like procedure, the National Institute of Standards and Technology is now choosing public key cryptography algorithms. To supplement Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard (DSS), and NIST Special Publication (SP) 800-56A, the new public key cryptography standards will include further algorithms for digital signatures, public key encryption, and key setup. Third Revision: SP 800-56B and Discrete Logarithm Cryptography for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography for Pair-Wise Key Establishment, Second Revision! The goal is for these algorithms to continue securing sensitive data even when quantum computers are available, for the foreseeable future. The third-round candidates for the NIST Post-Quantum Cryptography Standardization were evaluated and selected based on public comments and internal examination, as detailed in this paper. This report provides a brief overview of all fifteen candidate algorithms from the third round of evaluation, details which ones were chosen for standardization, and announces which ones will be further tested in the fourth round. Cryptographic has chosen CRYSTALS-KYBER as the standard for public-key encryption and key setup. Cryptographic Signatures—Dilithium, Falcon, and SPHINCS+ are the digital signatures that will be standardized. Although other signature techniques were considered, NIST suggests using CRYSTALS-Dilithium. Finally, a total of four algorithms that were considered for alternative key establishment will move on to the next screening: the Classic McElwee, BIKE, HQC, and SIKE brands. For potential future standardization, these choices are still under consideration. To further expand and enhance its signature portfolio, NIST will also make public-key digital signature algorithms the subject of a new Call for Proposals.

"A survey on the use of quantum key distribution in cryptography"

From a cryptography perspective, one attractive aspect of quantum key distribution (QKD) is the capacity to demonstrate the information-theoretic security (ITS) of the previously established keys. While QKD is

useful as a key setup basic, it is not a security service in and of itself. Subsequent cryptographic applications often make use of the secret keys produced by QKD, and these applications' needs, contexts, and security features might differ. So, looking at how QKD may be used with other cryptographic primitives is vital for incorporating it into security infrastructures. Contributing to such an analysis is the primary goal of this survey article, which mostly focuses on research results from Europe. We begin by taking a look at the current primary establishment approaches, including QKD, and comparing their features. We delve deeper into two practical applications of QKD in cryptographic infrastructures, examining two generic scenarios: 1) utilizing QKD as a key renewal technique for a symmetric cipher over a point-to-point link, and 2) implementing QKD in a network with multiple users to provide any-to-any key establishment service. We go over the possible benefits and drawbacks of applying QKD in various settings. We conclude with a review of the difficulties associated with expanding QKD technology, which may lead to new directions in cryptography.

"WireGuard after quantum"

The authors of this work introduce PQ-WireGuard, a post-quantum version of the WireGuard VPN protocol's handshake (NDSS 2017). This variation goes beyond most prior work on post-quantum security for real-world protocols by taking post-quantum authentication and post-quantum confidentiality (or forward secrecy) into consideration simultaneously. A less specific method relying solely on key-encapsulation mechanisms (KEMs) was used by the author to do this instead of a handshake based on Diffie-Hellman. The author establishes PQ-WireGuard's security by modifying the standard and symbolic models' security proofs for WireGuard to fit our build. After that, the author uses concrete post-quantum safe KEMs—which we pick with care—to instantiate this generic architecture, resulting in great security and speed. By providing comprehensive benchmarking data compared to commonly deployed VPN systems, the author demonstrates that PQ-WireGuard is competitive.

METHODOLOGY

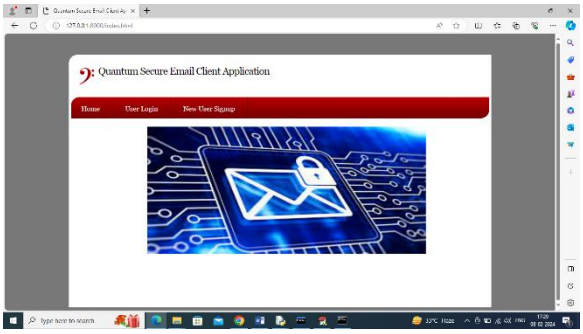
To implement this project we have designed following modules

1) User Sign up: using this module user can sign up with the application
2) User Login: can be used to login to systems

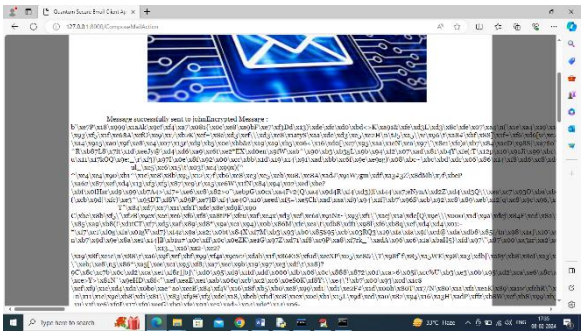
3) Compose Mails: after login sender can select desired receiver to send mails and while sending application will apply quantum computing to generate keys and to encrypt messages and then send to receiver account

4) View Mails: receiver can view list of mails and then can click on ‘Decrypt Message’ link to decrypt and view messages. Can click on download file to decrypt and download attachment file.

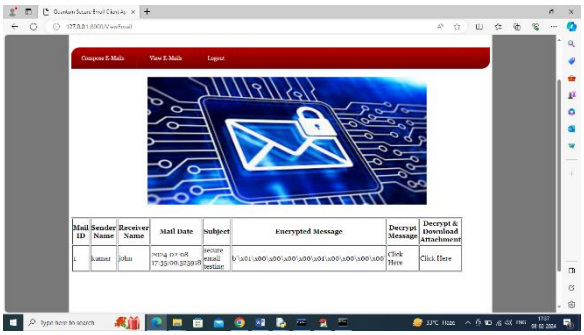
RESULT AND DISCUSSION



In above screen click on ‘New User Sign up’ link to get below page



The specifics of the encrypted message delivered to the receiver are visible on the screen above, and no one will be able to decipher or hack it because of how complicated it is. Before you can access your inbox, you must log out and then log in as John.



The recipient may see the sender's name and the subject line on the above screen, but the message is in encrypted format; to decrypt it, click the "Click Here" link. Then, the following output will appear.

CONCLUSION

Our results demonstrate that post-quantum and quantum cryptography, or a mix of the two, are prepared for application in systems and use cases beyond the traditional usage of

secure channel protocols for client-server communication, including Transport Layer Security (TLS). Although there is still more to do, particularly in terms of updating all applicable standards and RFCs, many cryptography libraries are based on extensible software designs that can accommodate new cryptographic algorithms. But we found certain problems with OpenPGP implementations that will need further effort to make them quantum-safe. Key management systems, as well as the user's and program's interactions with them, may necessitate further development for QKD encryption in order to guarantee asynchronous and long-term access to encrypted communications. Key rates are currently inadequate to meet demand, especially for QKD key integration into non-site-to-site VPN systems. This issue could be resolved by deriving several keys from a single key that is first supplied by QKD. It is possible, for instance, to employ a single QKD key with message-specific keys for all messages exchanged between two fixed participants on a given day. Even while it's important to think about key compromise at the QKD key level, not all messages would be encrypted using independent keys. We can reduce this danger by incorporating PQC-based encryption. There is need for further study in this area to investigate other key derivation methods.

REFERENCES

[1] Josh Aas, Richard Barnes, Benton Case, Zakir Durumeric, Peter Eckersley, Alan Flores-López, J. Alex Halderman, Jacob Hoffman-Andrews, James Kasten, Eric Rescorla, Seth D. Schoen, and Brad Warren. 2019. Let’s Encrypt: An Automated Certificate Authority to Encrypt the Entire Web. In ACM CCS 2019, Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz (Eds.). ACM Press, 2473–2487.
https://doi.org/10.1145/3319535.3363192

[2] Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Yi-Kai Liu. 2022. NISTIR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8413-upd1

[3] Romain Alléaume, Cyril Branciard, Jan Bouda, Thierry Debuisschert, Mehrdad Dianati, Nicolas Gisin, Mark Godfrey, Philippe Grangier, Thomas Länger, Norbert Lütkenhaus, Christian Monyk, Philippe Painchault, Momtchil Peev, Andreas Poppe,

Thomas Pornin, John G. Rarity, Renato Renner, Gregoire Ribordy, Michel Riguidel, Louis Salvail, Andrew J. Shields, Harald Weinfurter, and Anton Zeilinger. 2014. Using quantum key distribution for cryptographic purposes: A survey. Theor. Comput. Sci. 560 (2014), 62–81. https://doi.org/10.1016/j.tcs.2014.09.018

[4] Andreas Hülsing, Kai-Chun Ning, Peter Schwabe, Florian Weber, and Philip R. Zimmermann. 2021. Post-quantum WireGuard. In 2021 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 304–321. https://doi.org/10.1109/SP40001.2021.00030

[5] Jacqueline Brendel, Rune Fiedler, Felix Günther, Christian Janson, and Douglas Stebila. 2022. Post-quantum Asynchronous Deniable Key Exchange and the Signal Handshake. In PKC 2022, Part II (LNCS), Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe (Eds.), Vol. 13178. Springer, Heidelberg, 3–34. https://doi.org/10.1007/978-3-030-97131-1_1

[6 Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. 2018. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. In 2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018. IEEE, 353–367. https://doi.org/10.1109/EuroSP.2018.00032

[7] Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. 2018. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. IACR TCHES 2018, 1 (2018), 238–268. https://doi.org/10.13154/tches.v2018.i1.238-268 https://tches.iacr.org/index.php/TCHES/article/ view/839.

[8] Nik Unger, Sergej Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl, Ian Goldberg, and Matthew Smith. 2015. SoK: Secure Messaging. In 2015 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 232–249. https://doi.org/10.1109/SP.2015.22

[9] Daniel J. Bernstein, Billy Bob Brumley, Ming-Shing Chen, Chitchanok Chuengsatiansup, Tanja Lange, Adrian Marotzke, Bo-Yuan Peng, Nicola Tuveri, Christine van Vredendaal, and Bo-Yin Yang. 2020. NTRU Prime. Technical Report. National Institute of Standards and Technology. available at

https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[10] Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. 2019. The SPHINCS+ Signature Framework. In ACM CCS 2019, Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz (Eds.). ACM Press, 2129–2146. https://doi.org/10.1145/3319535.3363229

[11] Nina Bindel, Udyani Herath, Matthew McKague, and Douglas Stebila. 2017. Tran_sitioning to a Quantum-Resistant Public Key Infrastructure. In Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Tanja Lange and Tsuyoshi Takagi (Eds.). Springer, Heidelberg, 384–405. https://doi.org/10.1007/ 978-3-319-59879-6_22

[12] Nikita Borisov, Ian Goldberg, and Eric A. Brewer. 2004. Off-the-record communication, or, why not to use PGP. In Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, WPES 2004, Washington, DC, USA, October 28, 2004, Vijay Atluri, Paul F. Syverson, and Sabrina De Capitani di Vimercati (Eds.). ACM, 77–84. https://doi.org/10.1145/1029179.1029200