Quantum Threats to the TLS 1.3 Protocol

Presenter:
Luiz Filipi Anderson de Sousa Moura
(filipi_lfsm@hotmail.com)
Federal University of Santa Catarina

More article authors:
Dr. Alexandre Augusto Giron
Federal University of Technology-Paraná
Dr. Ricardo Felipe Custódio
Federal University of Santa Catarina

Presenter's short résumé:

Field of research: quantum computing and its implications on cybersecurity

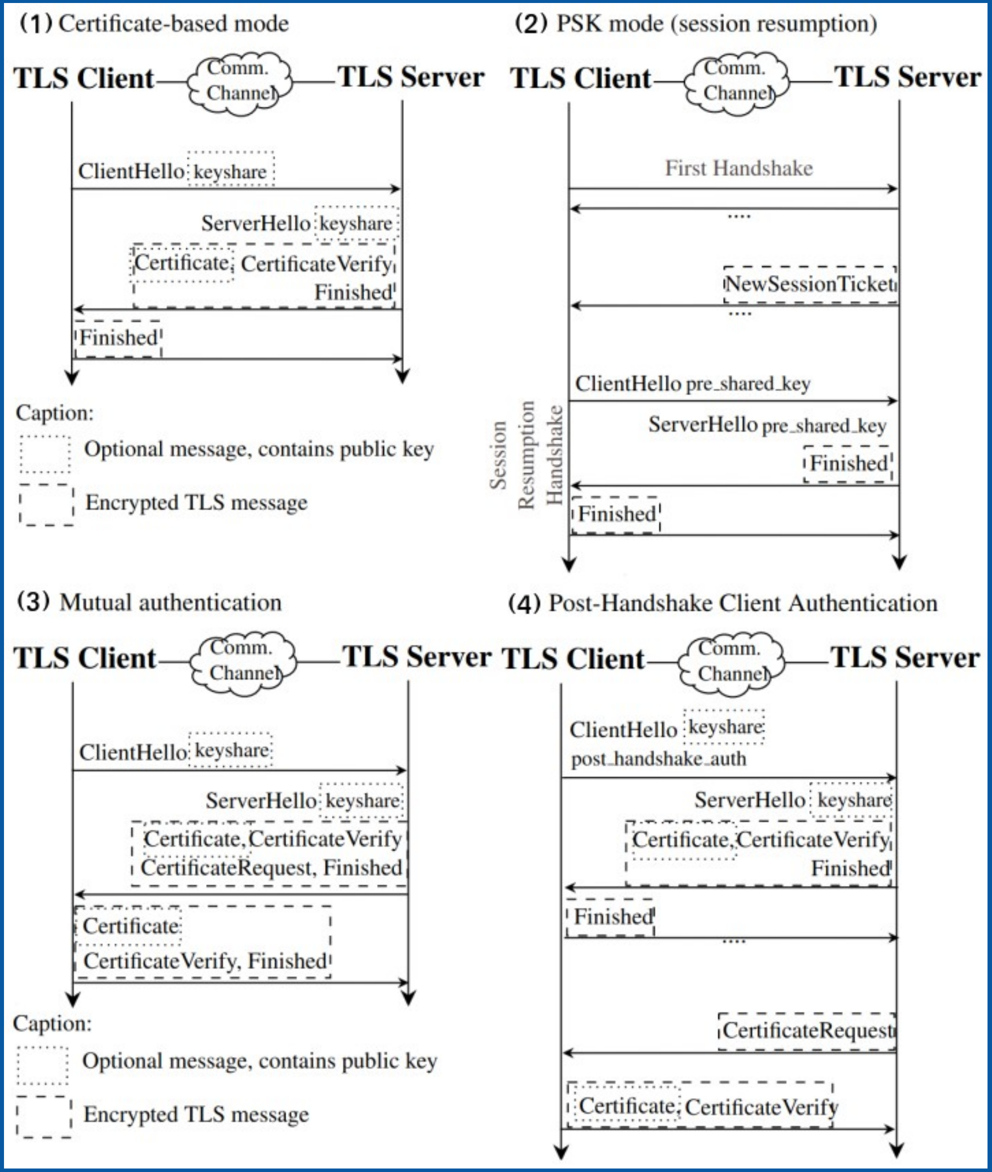
M.Sc. in Computer Science (ABD)
PG Certificate in Algorithms and Data Structures
PG Certificate in Software Engineering
B.Sc. in Physics/Biological Physics

The TLS 1.3

— Transport Layer Security (TLS) 1.3, defined in RFC 8446 [3], is a notorious internet security protocol, present in more than 60% of all internet connections based on HTTPS [1], [2].

— It provides end-to-end secure channels, and, like many others, uses public key cryptography (PKC).

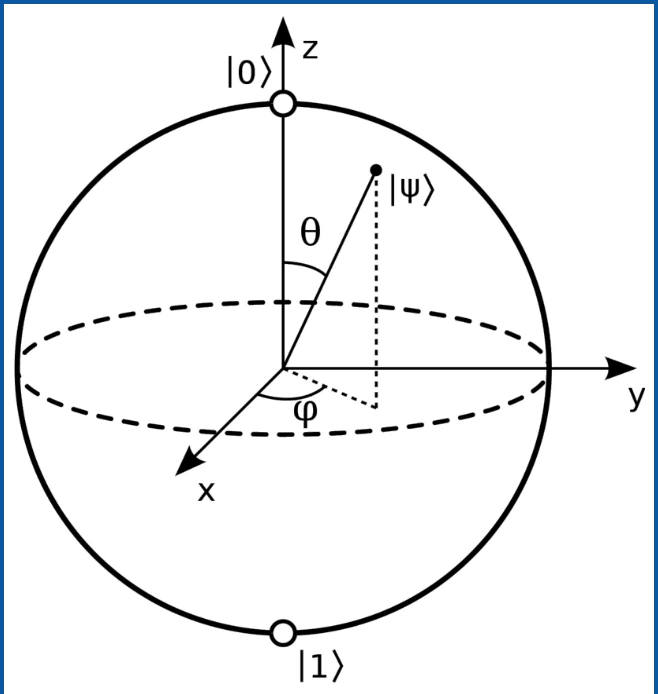
The TLS 1.3


(1) Certificate-based mode
TLS Client
Comm. Channel
TLS Server
ClientHello keyshare
ServerHello keyshare
Certificate, CertificateVerify
Finished
Finished
Caption:
Optional message, contains public key
Encrypted TLS message
(2) PSK mode (session resumption)
TLS Client
Comm. Channel
TLS Server
First Handshake
....
NewSessionTicket
....
Session Resumption Handshake
ClientHello pre_shared_key
ServerHello pre_shared_key
Finished
Finished
(3) Mutual authentication
TLS Client
Comm. Channel
TLS Server
ClientHello keyshare
ServerHello keyshare
Certificate, CertificateVerify
CertificateRequest, Finished
Certificate
CertificateVerify, Finished
Caption:
Optional message, contains public key
Encrypted TLS message
(4) Post-Handshake Client Authentication
TLS Client
Comm. Channel
TLS Server
ClientHello keyshare
post_handshake_auth
ServerHello keyshare
Certificate, CertificateVerify
Finished
Finished
....
CertificateRequest
Certificate, CertificateVerify

The quantum computer

— Qubit: $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$

— Normalization: $|a|^2 + |b|^2 = 1$



The quantum computer

— Register: $|q\rangle = |q_1\rangle \otimes |q_0\rangle =$

$c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$

— Gate model: $|q_n\rangle = G^n|q_{n-1}\rangle$

— Adiabatic model: applies an adiabatically slow time evolution of the state of the initial register (suitable for minimization problems)

Quantum algorithms for a PKC attack

— Shor's period finding algorithm, 1994 [4]: exponential speedup for solving factorization and DLP based problems [7], [14] with some newer implementations extending its usability to ECDLP [15], [16]

Best implementation of Shor's algorithm [17]	To break RSA-2048
2n+1 qubits	4097 qubits
Roughly $n^3\log(n)$ gates	Billions of gates

Quantum algorithms for a PKC attack

— However, due to errors in the measurements, the calculations have to be done multiple times or circa 1568 noisy qubits have to be used to simulate each perfect logical qubit [19]

— Other things to consider are gate and coherence times. Adding gates makes the total execution time longer and it cannot be longer than the coherence time.

Superconducting	Neutral atoms	Trapped ions
25 ns	19 μs	32 μs

Quantum algorithms for a PKC attack

— There are also good adiabatic implementations for factoring algorithms [21], [22], [23], and for DLP [24]

— The table is adapted from [14], [17], [25]

Year	Key length	Algorithm
2001	4 bits	Shor
2012	5 bits	Shor
2012	16 bits	Adiabatic
2016	18 bits	Adiabatic
2018	19 bits	Adiabatic
2019	20 bits	Adiabatic
2020	41 bits	Adiabatic

Threat model

Quantum eras	Description
Pre-quantum	The era we are now, when QC are still not powerful enough for an effective break on cryptography;
Post-quantum initial	Quantum hardware is primitive and expensive, demanding a high skill level to break even short keys;
Post-quantum intermediate	Quantum hardware, price, and skill level to perform an attack are at an intermediate stage;
Post-quantum advanced	QC is fully established and available at a lower cost.

Threat model

Available resources	Skill level	Becomes a threat at which post-quantum era?
Governments and large organizations	3 2 1	Initial Intermediate Advanced
Hacker groups and small organizations	3 2 1	Intermediate Advanced ∞
Individuals	3 2 1	Advanced ∞ ∞

Attack scenarios

— Break confidentiality: passive or active attack

—Impersonation: active attack only

Attack scenarios: Breaking confidentiality

— On certificate-based (server) mode:

1) collect Client and ServerHello, extracting the public keys epk_{CH} and epk_{SH} present in keyshare messages;

2) use Shor's algorithm for ECDLP to break the KEX: it computes the private key from epk_{CH} or epk_{SH} in order to recover the ephemeral private key;

3) use the recovered ephemeral key to derive the symmetrical keys, using the TLS Key Schedule [3], allowing to decrypt the whole communication

Attack scenarios: Breaking confidentiality

— On mutual authentication mode: same as previous

Attack scenarios: Breaking confidentiality

— On post-handshake authentication mode: same as previous

Attack scenarios: Breaking confidentiality

— On PSK-based resumption mode:

1) use previous steps on the First Handshake;
2) use the recovered ephemeral key to derive the symmetrical keys used throughout the communication;
3) decrypt the NewSessionTicket message, recovering the ticket information;
4) use the recovered information to derive the resumption PSK;
5) use the PSK to derive the second handshake's symmetrical keys

Attack scenarios: Impersonation

— On certificate-based (server) mode:
1) collect Client and ServerHello, extracting the public keys epk_{CH} and epk_{SH} present in keyshare messages;
2) use Shor's algorithm for ECDLP to break the KEX: it computes the private key from epk_{CH} or epk_{SH} in order to recover the ephemeral private key;
3) use one of the recovered private keys to derive the symmetrical keys, using the TLS Key Schedule [3], and then decrypt the authentication messages;

Attack scenarios: Impersonation

4) use one of the alternatives to attack the Certificate message and return the certificate private key:

— use Shor's algorithm or adiabatic QC to solve the factorization problem on the RSA public key; or

— use Shor for ECDLP on the public key based on elliptic curves

Attack scenarios: Impersonation

— On mutual authentication mode: same as for server authentication mode, but the attacker can choose to impersonate server or client. The main difference is the target Certificate message (from the server or client)

Attack scenarios: Impersonation

— On post-handshake authentication mode: impersonate the server is similar to the previous modes, but to impersonate client:

1) check the presence of the post_handshake_auth extension;

2) use the steps 1-2 of the Certificate-based authentication (server);

3) decrypt the communication using the recovered symmetric keys, searching for the CertificateRequest message;

Attack scenarios: Impersonation

4) use one of the alternatives to attack the client's Certificate message and return the private key:

– solve the factorization problem with Shor's algorithm or adiabatic QC; or

– use Shor for ECDLP instead

Attack scenarios: Impersonation

— On PSK-based resumption mode: similar steps as used for server authentication mode, but the steps should be applied to the First Handshake. Having the PSK information, the attacker can impersonate both peers. However, PSKs duration time can be limited up to 7 days [3], so the attack window is limited

Attack scenarios: SNDL resources

Site	1h of captured packets (MB)	Expected storage cost for 24h (GB)	Expected storage cost for 1y (TB)
Instagram.com	835.4	19.6	7
Youtube.com	723.7	17	6
Amazon.com	272.6	6.4	2.3
Gmail.com	124.8	2.9	1

Mitigation: QKD

— Quantum cryptography: the use of physics to create a different class of cryptography. QKD is the most common.

— QKD pros:

— the mathematics of quantum mechanics guarantees the key exchange is perfectly secure;

— the no-copy property of quantum mechanics ensures there will be no man-in-the-middle attack, because a measurement of the system would modify it

Mitigation: QKD

- QKD cons:
  - no-copy property makes it impossible to re-rout or broadcast a qubit, making it necessary special network channels and hardware;
  - it is affected by decoherence and most of the current QKD systems do not allow travels further than 200 km [28];
  - implementation costs immensely for large networks. Making it a viable solution only for limited use cases

Mitigation: PQC

— PQC: classical devices with math problems hard for a QC to solve.

— NIST, 2022, announced 4 algorithms promissed to be quantum-safe:

- — CRYSTALS-Kyber [29], a key encapsulation mechanism that can be used to establish symmetric keys;
- — CRYSTALS-Dilithium [30], a DSA;
- — Falcon [31], another DSA;
- — SPHINCS+ [32], a hash-based DSA

Mitigation: PQC

— PQC pros:

— more viable for KEX than QKD;

— there are also implementations for digital signatures

— PQC cons:

— have been tested for years, but it’s still impossible to tell for how long they will remain unbreakable [28];

– Most of them are slower than the traditional algorithms for KEX or digital signature, impacting in slower page loads and a risk of packet loss

Mitigation: Hybrid

— Hybrid implementations combine pre- and post-quantum cryptography.

— E.g.:

  — Combining the output of a pre- and a post-quantum algorithm with XOR in a KEX;

  — Creating 2 signatures, one with a pre- and another with a post-quantum algorithm

Mitigation: ROI

— Key length requires more gates, hence, longer execution time.

— Adding encryption layers, since the QC has to be used for each one of them [25];

— PFS, PCS, key management, short-term certificates can diminish the data recovered on each attack or shorten the window for an attack;

— Because the amount of storage necessary for a SNDL attack is huge, company have to be aware of social engineering attacks

Conclusion

— The paper exposed:
- — The threats of QC on TLS 1.3;
- — Existing quantum algorithms for an attack against PKC;
- — Achievements of these algorithms;
- — Detailed steps for a quantum attack in different handshake modes;
- — Approximate requirements for SNDL;
- — Mitigation methods

References

[1] C.-l. Chan, R. Fontugne, K. Cho, S. Goto, Monitoring tls adoption using backbone and edge traffic, in: IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2018, pp. 208–213.
[2] D. Sikeridis, P. Kampanakis, M. Devetsikiotis, Post-quantum authentication in tls 1.3: a performance study, Cryptology ePrint Archive.
[3] E. Rescorla, The transport layer security (tls) protocol version 1.3, RFC 8446, RFC Editor (August 2018).
[4] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th annual symposium on foundations of computer science, Ieee, 1994, pp. 124–134.
[5] J.-P. Aumasson, The impact of quantum computing on cryptography, Computer Fraud & Security 2017 (6) (2017) 8–11.

References

[6] L. K. Grover, A fast quantum mechanical algorithm for database search, in: Proceedings of the twentyeighth annual ACM symposium on Theory of computing, 1996, pp. 212–219.
[7] V. Mavroeidis, K. Vishi, M. D. Zych, A. Jøsang, The impact of quantum computing on present cryptography, arXiv preprint arXiv:1804.00200.
[8] M. Mosca, M. Piani, Quantum threat timeline report 2022, Global Risk Institute, Toronto, ON.
[9] G. Mone, The quantum threat, Communications of the ACM 63 (7) (2020) 12–14.
[10] H. Krawczyk, H. Wee, The optls protocol and tls 1.3, in: 2016 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, 2016, pp. 81–96.

References

[11] P. I. Hagouel, I. G. Karafyllidis, Quantum computers: Registers, gates and algorithms, in: 2012 28th International Conference on Microelectronics Proceedings, IEEE, 2012, pp. 15–21.
[12] C. R. Laumann, R. Moessner, A. Scardicchio, S. L. Sondhi, Quantum annealing: The fastest route to quantum computation?, The European Physical Journal Special Topics 224 (1) (2015) 75–88.
[13] S. Yarkoni, E. Raponi, T. Bäck, S. Schmitt, Quantum annealing for industry applications: Introduction and review, Reports on Progress in Physics.
[14] A. Petrenko, Applied Quantum Cryptanalysis, CRC Press, 2023.
[15] J. Proos, C. Zalka, Shor's discrete logarithm quantum algorithm for elliptic curves, arXiv preprint quant-ph/0301141.

References

[16] D. Maslov, J. Mathew, D. Cheung, D. K. Pradhan, An o (m2)-depth quantum algorithm for the elliptic curve discrete logarithm problem over gf (2m) a, Quantum Information & Computation 9 (7) (2009) 610–621.
[17] J. Suo, L. Wang, S. Yang, W. Zheng, J. Zhang, Quantum algorithms for typical hard problems: a perspective of cryptanalysis, Quantum Information Processing 19 (2020) 1–26.
[18] C. Q. Choi, Ibm's quantum leap: The company will take quantum tech past the 1,000-qubit mark in 2023, IEEE Spectrum 60 (1) (2023) 46–47.
[19] C. Gidney, M. Ekerå, How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits, Quantum 5 (2021) 433.
[20] M. Suchara, A. Faruque, C.-Y. Lai, G. Paz, F. T. Chong, J. Kubiatowicz, Comparing the overhead of topological and concatenated quantum error correction, arXiv preprint arXiv:1312.2316.

References

[21] Z. Li, N. S. Dattani, X. Chen, X. Liu, H. Wang, R. Tanburn, H. Chen, X. Peng, J. Du, High-fidelity adiabatic quantum computation using the intrinsic hamiltonian of a spin system: Application to the experimental factorization of 291311, arXiv preprint arXiv:1706.08061.
[22] S. Jiang, K. A. Britt, A. J. McCaskey, T. S. Humble, S. Kais, Quantum annealing for prime factorization, Scientific reports 8 (1) (2018) 17667.
[23] W. Peng, B. Wang, F. Hu, Y. Wang, X. Fang, X. Chen, C. Wang, Factoring larger integers with fewer qubits via quantum annealing with optimized parameters, SCIENCE CHINA Physics, Mechanics & Astronomy 62 (2019) 1–8.
[24] M. Wroński, Practical solving of discret logarithm problem over prime fields using quantum annealing, in: Computational Science–ICCS 2022: 22nd International Conference, London, UK, June 21–23, 2022, Proceedings, Part IV, Springer, 2022, pp. 93–106.
[25] T. Runge, Dismantling the quantum threat, Ph.D. thesis, Technische Hochschule Brandenburg (2023).

References

[26] V. Padamvathi, B. V. Vardhan, A. Krishna, Quantum cryptography and quantum key distribution protocols: a survey, in: 2016 IEEE 6th International Conference on Advanced Computing (IACC), IEEE, 2016, pp. 556–562.
[27] G. Brassard, C. H. Bennett, Quantum cryptography: Public key distribution and coin tossing, in: International conference on computers, systems and signal processing, 1984, pp. 175–179.
[28] G. Xu, J. Mao, E. Sakk, S. P. Wang, An overview of quantum-safe approaches: Quantum key distribution and post-quantum cryptography, in: 2023 57th Annual Conference on Information Sciences and Systems (CISS), IEEE, 2023, pp. 1–6.
[29] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, D. Stehlé, Crystals-kyber: a cca-secure module-lattice-based kem, in: 2018 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, 2018, pp. 353–367.
[30] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, D. Stehlé, Crystals-dilithium: A lattice-based digital signature scheme, IACR Transactions on Cryptographic Hardware and Embedded Systems (2018) 238–268.

References

[31] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang, et al., Falcon: Fast-fourier lattice-based compact signatures over ntru, Submission to the NIST's post-quantum cryptography standardization process 36 (5).
[32] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, P. Schwabe, The sphincs+ signature framework, in: Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, 2019, pp. 2129–2146.
[33] D. Stebila, M. Mosca, Post-quantum key exchange for the internet and the open quantum safe project, in: International Conference on Selected Areas in Cryptography, Springer, 2016, pp. 14–37.
[34] D. Stebila, S. Fluhrer, S. Gueron, Hybrid key exchange in TLS 1.3, Internet-Draft draft-ietf-tls-hybrid-design-06, Internet Engineering Task Force, work in Progress (Feb. 2023).
[35] W. Beullens, J.-P. D'Anvers, A. T. Hülsing, T. Lange, L. Panny, C. de Saint Guilhem, N. P. Smart, Post-quantum cryptography: Current state and quantum mitigation, Tech. rep., Eindhoven University of Technology (2021).

References

[36] K. Li, Q.-y. Cai, Practical security of rsa against ntc-architecture quantum computing attacks, International Journal of Theoretical Physics 60 (8) (2021) 2733–2744.
[37] M. Marlinspike, T. Perrin, The x3dh key agreement protocol, Open Whisper Systems 283 (2016) 10.
[38] T. Perrin, M. Marlinspike, The double ratchet algorithm, GitHub wiki (2016) 10.
[39] Y. Sheffer, D. Lopez, O. G. de Dios, A. Pastor, T. Fossati, Support for short-term, automatically renewed (star) certificates in the automated certificate management environment (acme), RFC 8739.