Qrypt

Technology Reference & Bibliography

Qrypt

1. Introduction

Secure encryption requires an adversarial approach to identifying weaknesses in algorithms, protocols, and the implementations of cryptographic systems. Qrypt subscribes to these principles and develops, licenses, and validates technology that has been subject to peer review and inspection. This is evident in our collaborative research with the world's leading research laboratories, as well as through the publications and presentations in quantum and cryptography conferences and journals. This reference is intended to act as a resource to provide an understanding of the technology that Qrypt relies upon to provide secure technology for our users.

2. Messaging Protocols

References describing how Qrypt key generation protocols can be combined with techniques such as one-time pad encryption, double-ratchet encryption with epoch key exchange, and implemented as a derivative of the Signal protocol to achieve everlasting encryption.

a. USPTO 10,412,063: End-To-End Double-Ratchet Encryption with Epoch Key Exchange

b. Joel Alwen, Sandro Coretti and Yevgeniy Dodis, "The Double Ratchet: Security Notions, Proofs, and Modularization for the Signal Protocol", *Advances in Cryptology - EUROCRYPT*, May 2019.

3. Key Generation Protocols

References describing the underlying technology and principles of how Qrypt ensures that generated keys are secure, including the basis of extracting keys from random pools.

a. Yevgeniy Dodis and Kevin Yeo, "Doubly-Affine Extractors, and their Applications", *Conference on Information-Theoretic Cryptography (ITC)*, July 2021.

b. USPTO 11,095,442: Generating Unique Cryptographic Keys from A Pool Of Random Elements

c. Yevgeniy Dodis et al., "Online Linear Extractors for Independent Sources"

d. Yevgeniy Dodis et al., “Extracting Randomness from Extractor-Dependent Sources”

e. Sandro Coretti et al., “Seedless Fruit is the Sweetest: Random Number Generation, Revisited“

f. Yevgeniy Dodis et al., “Towards Defeating Backdoored Random Oracles: Indifferentiability with Bounded Adaptivity”

4. Quantum Random Number Generator Technology

Select references describing the underlying technology and principles of how entropy is measured and extracted, both in production and in the advanced roadmap. These references are not exhaustive.

a. General patents applicable to all source types
   i. USPTO 10,402,172 Multi-Source Entropy and Randomness Aggregation And Distribution Network

b. Quantum sources based on heterodyne laser phase diffusion developed at the Institute for Photonic Sciences (ICFO), in Barcelona, and now manufactured by Quside.
   i. USPTO 9,218,160 Ultrafast Quantum Random Number Generation Process and System Therefore
   ii. USPTO 10,302,560 Process for Quantum Random Number Generation in a Multimode Laser Cavity
   iii. C. Abellan et al “Generation of Fresh And Pure Random Numbers For Loophole-Free Bell Tests” Phys. Rev. Lett. 115, 250403 – Published 16 December 2015
   iv. C. Abellan, "Quantum entropy source on an InP photonic integrated circuit for random number generation," Optica, vol. 3, no. 9, pp. 989-994, 2016.

c. Quantum sources based on homodyne detection of quantum noise developed in collaboration with and exclusively licensed from Oak Ridge National Laboratories (ORNL)
   i. USPTO 11,118,964 Noiseless AC Coupling for Balanced Detection Using a Common Adjustable Current Sink - "Balance Light Detector"
   ii. USPTO 10,635,403 Quantum Random Number Generator

   iii. F. Raffaelli, "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," Optics Express, vol. 26, no. 16, pp. 19730-19741, 2018.

d. Quantum sources based on the quantum photon bunching from a thermal light source, developed in collaboration with and exclusively licensed from Los Alamos National Laboratories (LANL)
   i. "Quantum Random Number Generators" US20160328211 A1 USPTO, 11/10/2016.

e. Quantum sources based on SPAD array approach, developed in collaboration with EPFL
   i. D. Stucki, "Towards a high-speed quantum random number generator," EPFL, 27 Jan 2018.
   ii. S. Burri, "Architecture and applications of a high resolution gated SPAD image sensor," Optics Express, vol. 22, no. 14, pp. 17573-17589, 2014.
   iii. M. Stipcevic, "Spatio-temporal optical random number generator," Optics Express, vol. 23, no. 9, pp. 11619-11631, 2015.
   iv. X. Guo, "Enhancing quantum entropy in vacuum-based quantum random number generator," arXiv, 26 May 2018.

5. Relevant References

a. Videos

   i. Craig Costello TED Talk "Cryptographers, quantum computers, and the war for information"
   ii. Educational video by Yevgeniy Dodis on the use of extractors (45 min)
   iii. A Wikipedia article on the numbers stations that broadcast to the intelligence community in foreign countries.

b. Popular news articles – General Quantum Threat

   i. Today's encryption crackable by quantum computing in five years, 73% of cybersecurity pros say, verdict.co.uk
   ii. The race for quantum-proof cryptography, csoonline.com

iii. Quantum knows what you did last summer, Todd Moore on securityboulevard.com

iv. Traditional cryptography doesn't stand a chance against the quantum age, inverse.com

v. Race is on to build quantum-proof encryption by Adam Green on ft.com

vi. What can be done — today — to keep quantum computing from killing encryption

vii. The quantum computing threat to American security, The Wall Street Journal

viii. The Day When Computers Can Break All Encryption Is Coming, Wall Street Journal

ix. The CIO's guide to quantum computing, Gartner

x. Quantum computers will break the encryption that protects the internet, The Economist

xi. Quantum computing will break your encryption in a few years, networkworld.com

xii. The Race for Quantum Resistant Cryptography, National Defense Magazine

c. Popular news articles – Quantum Cryptography and Post Quantum Cryptography

i. Blazing New Paths in Quantum Security by Arthur Herman on Forbes.com

ii. Is our Data Actually Safe? By Kenna Castleberry on The Quantum Insider

iii. How Peter Shor's Algorithm Dooms RSA Encryption to Failure, interestingengineering.com

iv. Experts say it's high time to create new cryptography for quantum computing age

v. Quantum Cryptography: The next generation of secure data transmission

vi. Post-Quantum Cryptography Becoming Relevant in Pre-Quantum World

vii. Start Preparing Now for the Post-Quantum Future

viii. Quantum Cryptography and the Future of Security

d. News Articles/Blogs - Addressing Implications to Flawed Randomness

i. The Register article covering the Reductor malware and how it hijacks the random number generation function, so that TLS traffic can be decrypted

ii. A blog post and subsequent reporting exposing keys derived without sufficient randomness allowing them to break 250k certificates.

iii. Research presented at RWC (YouTube) as proof of IDQuantiq's Quantis is not quantum or random, based on the full paper submitted to IACR "Bias in a Family of Quantum Random Number Generators"

iv. Reporting on a critical vulnerability in random number generators used in billions of Internet of Things (IoT) devices, undermining their security and putting them at risk of attacks.

v. A survey published to Forbes of the risks of flawed randomness, and history of compromises by Denis Mandich, Qrypt CTO

vi. An essay analyzing failures in random number generation and which may have been intentionally inserted backdoors.

vii. Washington Post coverage of the historical project Rubicon, where the CIA deliberately contaminated random sources to compromise cryptography, using Crypto AG.

viii. Reports by Sophos and Register article on the Yubico FIPS series randomness flaw

ix. A flaw in Ethereum wallet random resulting in $54M losses, reported on Sophos and ISE

x. An approachable blog by Carlos Abellan, discussing cryptography and randomness

e. Academic Papers - Addressing Implications to Flawed Randomness

i. A Formal Treatment of Backdoored Pseudorandom Generators, by Yevgeniy Dodis et al. (Qrypt/NYU)

ii. When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography by Thomas Ristenpart et al (UCSD)

iii. A publication on the vulnerability in the 2008 Debian Linux version of OpenSSL, resulting in predictable random numbers,

iv. Detection of Widespread Weak Keys in Network Devices, by Nadia Heninger et al

v. Factoring RSA keys from certified smart cards, by Daniel Berstein et al, “This paper explains how an attacker can efficiently factor 184 distinct RSA keys out of more than two million 1024-bit RSA keys”

vi. Not-So-Random Numbers in Virtualized Linux and the Whirlwind RNG, by Adam Everspaugh et al

f. News Articles - Harvest Now and Decrypt Later, and threats to intellectual property

i. ‘Hack now, decrypt later’ is here today; by Dan O’Shea on Fierce Electronics

ii. Reporting on re-routing of internet traffic for collection through China in 2019 and Russia in 2017

iii. Reporting of the FBI having over 1000 probes into intellectual property theft, “nearly all” originating in China
iv. 'Quantum supremacy' demands prioritization of crypto protections