Classic McEliece:
conservative code-based cryptography

Daniel J. Bernstein, Tung Chou,
Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram,
Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen,
Edoardo Persichetti, Christiane Peters, Nicolas Sendrier, Jakub Szefer,
Cen Jung Tjhai, Martin Tomlinson, Wen Wang

https://classic.mceliece.org/

10 – 12 Apr. 2024
Fifth NIST PQC workshop

Stability

Classic McEliece is the paramount conservative code-based encryption scheme.

Stability

Classic McEliece is the paramount conservative code-based encryption scheme.

Classic McEliece is **stable**:

Stability

Classic McEliece is the paramount conservative code-based encryption scheme.

Classic McEliece is **stable**:

- The McEliece cryptosystem has been stable for over 40 years now.

Stability

Classic McEliece is the paramount conservative code-based encryption scheme.

Classic McEliece is **stable**:

- The McEliece cryptosystem has been stable for over 40 years now.
  Nothing has changed in the asymptotics of OW-Passive security for McEliece.

Stability

Classic McEliece is the paramount conservative code-based encryption scheme.

Classic McEliece is **stable**:

- The McEliece cryptosystem has been stable for over 40 years now.
  Nothing has changed in the asymptotics of OW-Passive security for McEliece.

- Classic McEliece inherits this impressive security history.

Stability

Classic McEliece is the paramount conservative code-based encryption scheme.

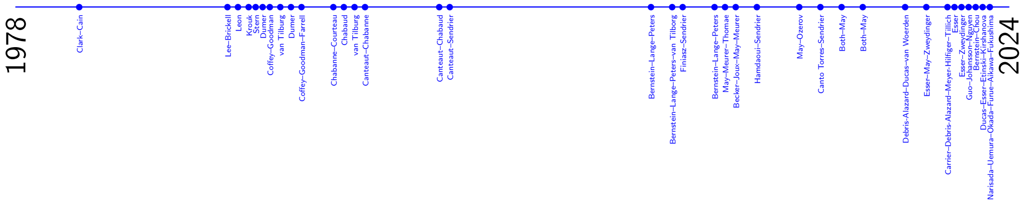
Classic McEliece is **stable**:

- The McEliece cryptosystem has been stable for over 40 years now.
  Nothing has changed in the asymptotics of OW-Passive security for McEliece.

- Classic McEliece inherits this impressive security history.
  We follow McEliece's original approach (binary Goppa codes) and use best practices (e.g. implicit rejection) to obtain an IND-CCA2 secure KEM with a tight QROM proof assuming OW-Passive security for original McEliece.

McEliece security stability

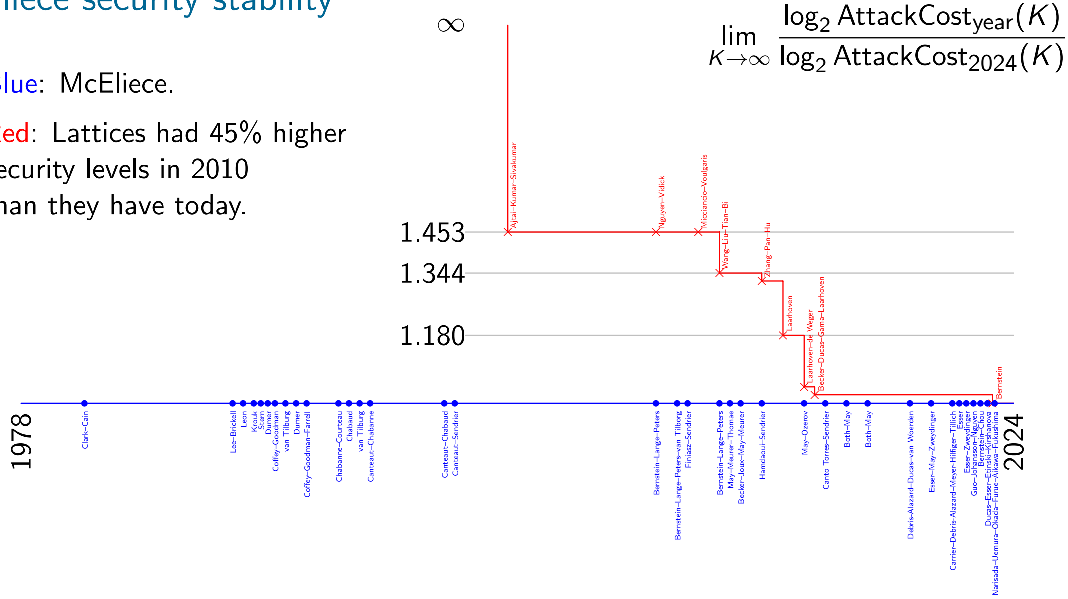
$$\lim_{K \to \infty} \frac{\log_2 \mathrm{AttackCost}_{\mathrm{year}}(K)}{\log_2 \mathrm{AttackCost}_{2024}(K)}$$



McEliece security stability

Blue: McEliece.

Red: Lattices had 45% higher security levels in 2010 than they have today.



McEliece security stability

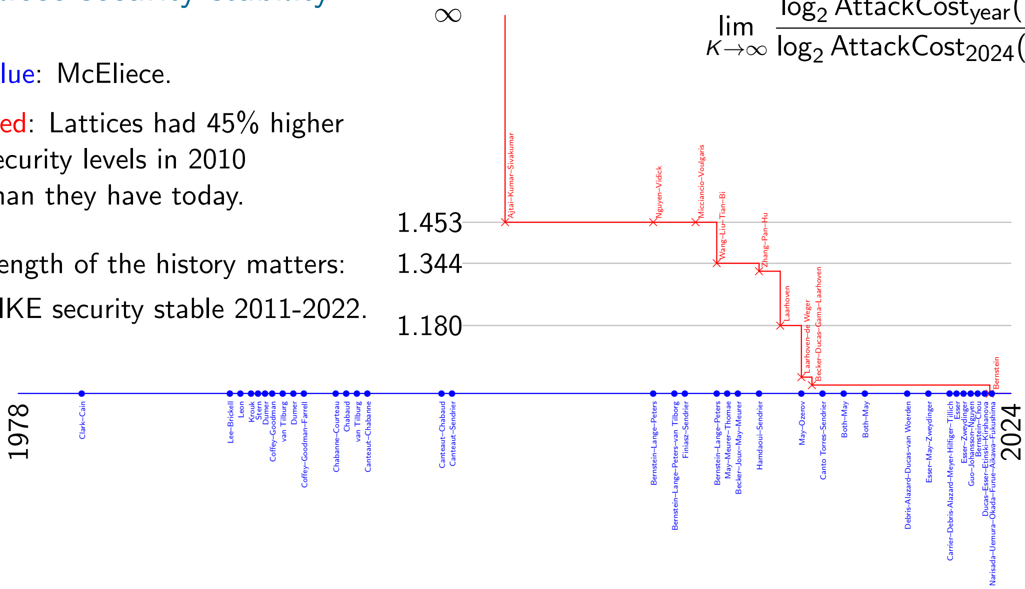
Blue: McEliece.

Red: Lattices had 45% higher security levels in 2010 than they have today.

Length of the history matters:

SIKE security stable 2011-2022.

$$\lim_{K\to\infty} \frac{\log_2 \mathrm{AttackCost}_{\mathrm{year}}(K)}{\log_2 \mathrm{AttackCost}_{2024}(K)}$$



Performance

Classic McEliece has the shortest ciphertext in the competition, and fast encapsulation/decapsulation algorithms.

Performance

Classic McEliece has the shortest ciphertext in the competition, and fast encapsulation/decapsulation algorithms.

Classic McEliece also has a very large key, and a slow key generation algorithm.

Performance

Classic McEliece has the shortest ciphertext in the competition, and fast encapsulation/decapsulation algorithms.

Classic McEliece also has a very large key, and a slow key generation algorithm.

How serious are these two issues in practice?

Performance

Classic McEliece has the shortest ciphertext in the competition, and fast encapsulation/decapsulation algorithms.

Classic McEliece also has a very large key, and a slow key generation algorithm.

How serious are these two issues in practice?

- *We have been recommending parameter sets with 1MB keys.*
  More and more users will be able to afford 1MB keys. Average webpage size is over 2MB now according to httparchive.org (≈ 55% growth rate since 2017).

Performance

Classic McEliece has the shortest ciphertext in the competition, and fast encapsulation/decapsulation algorithms.

Classic McEliece also has a very large key, and a slow key generation algorithm.

How serious are these two issues in practice?

- *We have been recommending parameter sets with 1MB keys.*
  More and more users will be able to afford 1MB keys. Average webpage size is over 2MB now according to httparchive.org (≈ 55% growth rate since 2017).
- *Having CCA security means that key pairs can be reused.*
  A long-term identity key is generated once and reused for any number of ciphertexts. If **forward secrecy** is desired, once per hour, spend a fraction of a second generating a new short-term key.

Updates

Various items to report with regards to use cases, analysis, and applications:

Updates

Various items to report with regards to use cases, analysis, and applications:

- *isdbitops*: now a bigger CryptAttackTester project, available online.
  This means there is now auditable computer-tested bit-operation counts for a wide range of fully-defined attacks in a fully-defined model of computation.

Updates

Various items to report with regards to use cases, analysis, and applications:

- *isdbitops*: now a bigger CryptAttackTester project, available online.
  This means there is now auditable computer-tested bit-operation counts for a wide range of fully-defined attacks in a fully-defined model of computation.
- *decoding formulas*: now featuring formally verified proofs of correctness.

Updates

Various items to report with regards to use cases, analysis, and applications:

- *isdbitops*: now a bigger CryptAttackTester project, available online.
  This means there is now auditable computer-tested bit-operation counts for a wide range of fully-defined attacks in a fully-defined model of computation.
- *decoding formulas*: now featuring formally verified proofs of correctness.
- *networks*: included by Adva in high-speed optical network. Encrypted layer 1 optical transport solutions (OTNsec) with 10-400 Gbit/s including BSI approval.

Updates

Various items to report with regards to use cases, analysis, and applications:

- *isdbitops*: now a bigger CryptAttackTester project, available online. This means there is now auditable computer-tested bit-operation counts for a wide range of fully-defined attacks in a fully-defined model of computation.
- *decoding formulas*: now featuring formally verified proofs of correctness.
- *networks*: included by Adva in high-speed optical network. Encrypted layer 1 optical transport solutions (OTNsec) with 10-400 Gbit/s including BSI approval.
- *hardware*: Crypto4A uses Classic McEliece in all of its HSMs for three important use cases (transfer of sensitive items), in hybrid mode.

Updates

Various items to report with regards to use cases, analysis, and applications:

- *isdbitops*: now a bigger CryptAttackTester project, available online.
  This means there is now auditable computer-tested bit-operation counts for a wide range of fully-defined attacks in a fully-defined model of computation.
- *decoding formulas*: now featuring formally verified proofs of correctness.
- *networks*: included by Adva in high-speed optical network. Encrypted layer 1 optical transport solutions (OTNsec) with 10-400 Gbit/s including BSI approval.
- *hardware*: Crypto4A uses Classic McEliece in all of its HSMs for three important use cases (transfer of sensitive items), in hybrid mode.
- *software*: available in multiple libraries, such as Bouncy Castle, classic-mceliece-rust, gcrypt-mceliece, libmceliece (now included in Debian), liboqs, node-mceliece-nist, openssh-mceliece, and more.

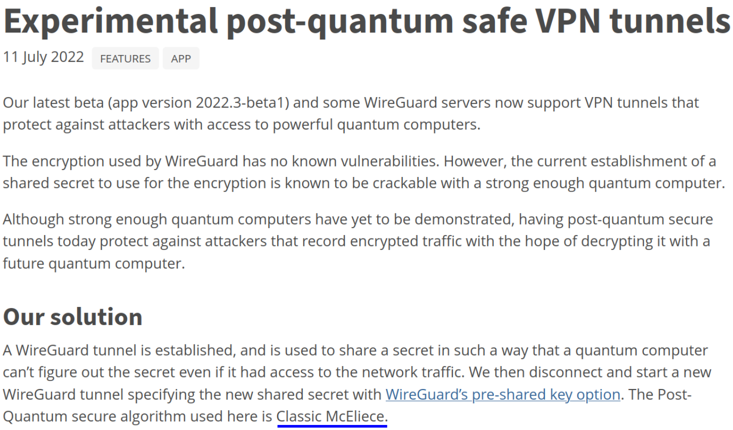
Updates

Various items to report with regards to use cases, analysis, and applications:

- *isdbitops*: now a bigger CryptAttackTester project, available online.
  This means there is now auditable computer-tested bit-operation counts for a wide range of fully-defined attacks in a fully-defined model of computation.
- *decoding formulas*: now featuring formally verified proofs of correctness.
- *networks*: included by Adva in high-speed optical network. Encrypted layer 1 optical transport solutions (OTNsec) with 10-400 Gbit/s including BSI approval.
- *hardware*: Crypto4A uses Classic McEliece in all of its HSMs for three important use cases (transfer of sensitive items), in hybrid mode.
- *software*: available in multiple libraries, such as Bouncy Castle, classic-mceliece-rust, gcrypt-mceliece, libmceliece (now included in Debian), liboqs, node-mceliece-nist, openssh-mceliece, and more.
- *VPNs*: (next slides)

Applications – MULLVAD VPN

https://mullvad.net/en/blog/2022/7/11/experimental-post-quantum-safe-vpn-tunnels/



Experimental post-quantum safe VPN tunnels

11 July 2022 FEATURES APP

Our latest beta (app version 2022.3-beta1) and some WireGuard servers now support VPN tunnels that protect against attackers with access to powerful quantum computers.

The encryption used by WireGuard has no known vulnerabilities. However, the current establishment of a shared secret to use for the encryption is known to be crackable with a strong enough quantum computer.

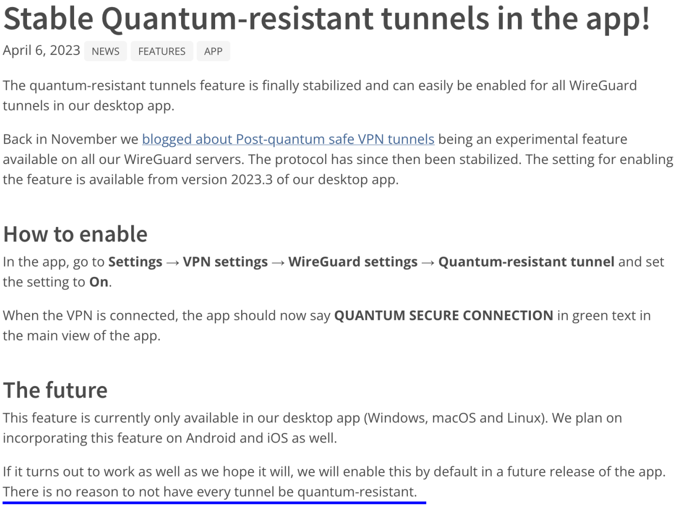
Although strong enough quantum computers have yet to be demonstrated, having post-quantum secure tunnels today protect against attackers that record encrypted traffic with the hope of decrypting it with a future quantum computer.

Our solution

A WireGuard tunnel is established, and is used to share a secret in such a way that a quantum computer can't figure out the secret even if it had access to the network traffic. We then disconnect and start a new WireGuard tunnel specifying the new shared secret with WireGuard's pre-shared key option. The Post-Quantum secure algorithm used here is Classic McEliece.

Applications – MULLVAD VPN

https://mullvad.net/en/blog/stable-quantum-resistant-tunnels-in-the-app



Stable Quantum-resistant tunnels in the app!

April 6, 2023 NEWS FEATURES APP

The quantum-resistant tunnels feature is finally stabilized and can easily be enabled for all WireGuard tunnels in our desktop app.

Back in November we blogged about Post-quantum safe VPN tunnels being an experimental feature available on all our WireGuard servers. The protocol has since then been stabilized. The setting for enabling the feature is available from version 2023.3 of our desktop app.

How to enable

In the app, go to **Settings** → **VPN settings** → **WireGuard settings** → **Quantum-resistant tunnel** and set the setting to **On**.

When the VPN is connected, the app should now say **QUANTUM SECURE CONNECTION** in green text in the main view of the app.

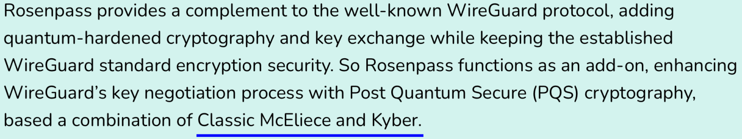
The future

This feature is currently only available in our desktop app (Windows, macOS and Linux). We plan on incorporating this feature on Android and iOS as well.

If it turns out to work as well as we hope it will, we will enable this by default in a future release of the app. There is no reason to not have every tunnel be quantum-resistant.

Applications – ROSENPASS VPN

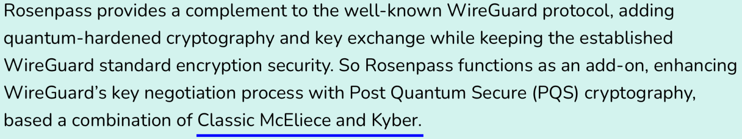
https://rosenpass.eu/about/



Rosenpass provides a complement to the well-known WireGuard protocol, adding quantum-hardened cryptography and key exchange while keeping the established WireGuard standard encryption security. So Rosenpass functions as an add-on, enhancing WireGuard's key negotiation process with Post Quantum Secure (PQS) cryptography, based a combination of Classic McEliece and Kyber.

Applications – ROSENPASS VPN

https://rosenpass.eu/about/

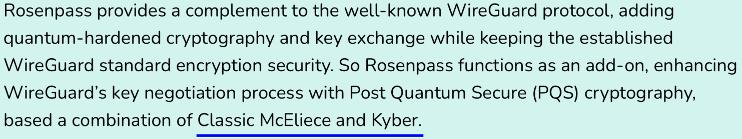


Rosenpass provides a complement to the well-known WireGuard protocol, adding quantum-hardened cryptography and key exchange while keeping the established WireGuard standard encryption security. So Rosenpass functions as an add-on, enhancing WireGuard's key negotiation process with Post Quantum Secure (PQS) cryptography, based a combination of Classic McEliece and Kyber.

Uses Classic McEliece for long-term keys, the foundation of security for identifying and authenticating the server, as well as for encrypting data.

Applications – ROSENPASS VPN

https://rosenpass.eu/about/



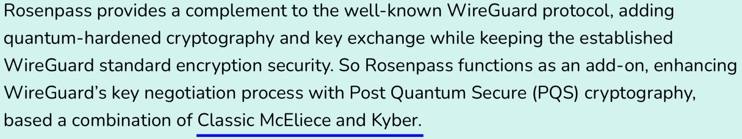
Rosenpass provides a complement to the well-known WireGuard protocol, adding quantum-hardened cryptography and key exchange while keeping the established WireGuard standard encryption security. So Rosenpass functions as an add-on, enhancing WireGuard's key negotiation process with Post Quantum Secure (PQS) cryptography, based a combination of Classic McEliece and Kyber.

Uses Classic McEliece for long-term keys, the foundation of security for identifying and authenticating the server, as well as for encrypting data.

Uses Kyber just for forward secrecy: a break of the lattice system does not damage security unless the attacker can also steal secret keys through, e.g., hardware theft.

Applications – ROSENPASS VPN

https://rosenpass.eu/about/



Rosenpass provides a complement to the well-known WireGuard protocol, adding quantum-hardened cryptography and key exchange while keeping the established WireGuard standard encryption security. So Rosenpass functions as an add-on, enhancing WireGuard's key negotiation process with Post Quantum Secure (PQS) cryptography, based a combination of Classic McEliece and Kyber.

Uses Classic McEliece for long-term keys, the foundation of security for identifying and authenticating the server, as well as for encrypting data.

Uses Kyber just for forward secrecy: a break of the lattice system does not damage security unless the attacker can also steal secret keys through, e.g., hardware theft.

Interestingly, trying to use a lattice system for the long-term keys would damage efficiency, since ciphertexts are continually sent to those keys, while the keys themselves are basically always cached.