Transitioning to post-quantum cryptography

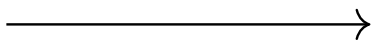
Dr Chloe Martindale

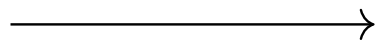
University of Bristol

29th June 2022

What is this all about?

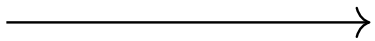
Cryptography

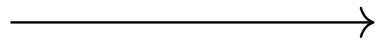




Sender Channel with eavesdropper ‘Eve’ Receiver

Cryptography





Sender Channel with eavesdropper 'Eve' Receiver

Problems:

- Communication channels store and spy on our data
- Communication channels are modifying our data

Cryptography

Sender — Channel with eavesdropper 'Eve' — Receiver

Problems:

- Communication channels store and spy on our data
- Communication channels are modifying our data

Goals:

- Confidentiality despite Eve's espionage.
- Integrity: recognising Eve's espionage.

Post-quantum cryptography

Sender Channel with eavesdropper ‘Eve’ Receiver

Post-quantum cryptography

Sender Channel with eavesdropper ‘Eve’ Receiver

- Eve has a quantum computer.
- Harry and Meghan don’t have a quantum computer.

Post-quantum cryptography

Sender Channel with eavesdropper 'Eve' Receiver

- Eve has a quantum computer.
- Harry and Meghan don't have a quantum computer.

Post-quantum cryptography $\neq$ quantum cryptography

- In quantum cryptography, Harry and Meghan also have access to quantum technology.

Why does Eve need a quantum computer?

- Asymmetric cryptography typically relies on the discrete logarithm problem being slow to solve:
  with Shor's quantum algorithm this is no longer true.

Why does Eve need a quantum computer?

- Asymmetric cryptography typically relies on the discrete logarithm problem being slow to solve:
  with Shor's quantum algorithm this is no longer true.
  $\rightsquigarrow$ will make current asymmetric algorithms obselete.

Why does Eve need a quantum computer?

- Asymmetric cryptography typically relies on the discrete logarithm problem being slow to solve:
  with Shor's quantum algorithm this is no longer true.
  $\rightsquigarrow$ will make current asymmetric algorithms obselete.
- Symmetric cryptography typically has less mathematical structure so quantum computers are less devastating,
  but Grover's quantum algorithm still speeds up attacks.

Why does Eve need a quantum computer?

- Asymmetric cryptography typically relies on the discrete logarithm problem being slow to solve:
  with Shor's quantum algorithm this is no longer true.
  $\rightsquigarrow$ will make current asymmetric algorithms obselete.
- Symmetric cryptography typically has less mathematical structure so quantum computers are less devastating,
  but Grover's quantum algorithm still speeds up attacks.
  $\rightsquigarrow$ reduces security of current symmetric algorithms.

Why does Eve need a quantum computer?

- Asymmetric cryptography typically relies on the discrete logarithm problem being slow to solve:
  with Shor's quantum algorithm this is no longer true.
  $\rightsquigarrow$ will make current asymmetric algorithms obselete.
- Symmetric cryptography typically has less mathematical structure so quantum computers are less devastating,
  but Grover's quantum algorithm still speeds up attacks.
  $\rightsquigarrow$ reduces security of current symmetric algorithms.

Main goal: replace the use of the discrete logarithm problem in asymmetric cryptography with something quantum-resistant.

Alternatives

Ideas to replace the discrete logarithm problem:

Alternatives

Ideas to replace the discrete logarithm problem:

- Code-based encryption: uses error correcting codes. Short ciphertexts, large public keys.

Alternatives

Ideas to replace the discrete logarithm problem:

- Code-based encryption: uses error correcting codes.
  Short ciphertexts, large public keys.
- Hash-based signatures: uses hard-to-invert functions.
  Well-studied security, small public keys.

Alternatives

Ideas to replace the discrete logarithm problem:

- Code-based encryption: uses error correcting codes.
  Short ciphertexts, large public keys.
- Hash-based signatures: uses hard-to-invert functions.
  Well-studied security, small public keys.
- Isogeny-based encryption and signatures: based on finding maps between (elliptic) curves.
  Smallest keys, slow encryption.

Alternatives

Ideas to replace the discrete logarithm problem:

- Code-based encryption: uses error correcting codes.
  Short ciphertexts, large public keys.
- Hash-based signatures: uses hard-to-invert functions.
  Well-studied security, small public keys.
- Isogeny-based encryption and signatures: based on finding maps between (elliptic) curves.
  Smallest keys, slow encryption.
- Lattice-based encryption and signatures: based on finding short vectors in high-dimensional lattices.
  Fastest encryption, huge keys, slow signatures.

Alternatives

Ideas to replace the discrete logarithm problem:

- Code-based encryption: uses error correcting codes.
  Short ciphertexts, large public keys.
- Hash-based signatures: uses hard-to-invert functions.
  Well-studied security, small public keys.
- Isogeny-based encryption and signatures: based on finding maps between (elliptic) curves.
  Smallest keys, slow encryption.
- Lattice-based encryption and signatures: based on finding short vectors in high-dimensional lattices.
  Fastest encryption, huge keys, slow signatures.
- Multivariate signatures: based on solving simulateneous multivariate equations.
  Short signatures, large public keys, slow.

What can we do?

We have:

- KEM/Encryption and signatures*
  (many options from NIST competition).
- Diffie-Hellman-style / non-interactive key exchange
  (only option is with CSIDH).

What can we do?

We have:

- KEM/Encryption and signatures*
  (many options from NIST competition).
- Diffie-Hellman-style / non-interactive key exchange
  (only option is with CSIDH).

*What is wrong with signatures?

- Ward Beullens found a new attack on multivariate cryptography after finalists were announced.

What can we do?

We have:

- KEM/Encryption and signatures*
  (many options from NIST competition).
- Diffie-Hellman-style / non-interactive key exchange
  (only option is with CSIDH).

*What is wrong with signatures?

- Ward Beullens found a new attack on multivariate cryptography after finalists were announced.
  - Breaking the (lowest) original Rainbow parameters takes a weekend on Ward's laptop.
  - Security of MV schemes now under question.

What can we do?

We have:

- KEM/Encryption and signatures*
  (many options from NIST competition).
- Diffie-Hellman-style / non-interactive key exchange
  (only option is with CSIDH).

*What is wrong with signatures?

- Ward Beullens found a new attack on multivariate cryptography after finalists were announced.
  - Breaking the (lowest) original Rainbow parameters takes a weekend on Ward's laptop.
  - Security of MV schemes now under question.
- Daniel J. Bernstein and Tanja Lange have a (contested) attack avenue on structured lattice-based schemes.

What can we do?

We have:

- KEM/Encryption and signatures*
  (many options from NIST competition).
- Diffie-Hellman-style / non-interactive key exchange
  (only option is with CSIDH).

*What is wrong with signatures?

- Ward Beullens found a new attack on multivariate cryptography after finalists were announced.
  - Breaking the (lowest) original Rainbow parameters takes a weekend on Ward's laptop.
  - Security of MV schemes now under question.
- Daniel J. Bernstein and Tanja Lange have a (contested) attack avenue on structured lattice-based schemes.
  - Applies to all finalists, but not all alternates.

What can we do?

We have:

- KEM/Encryption and signatures*
  (many options from NIST competition).
- Diffie-Hellman-style / non-interactive key exchange
  (only option is with CSIDH).

*What is wrong with signatures?

- Ward Beullens found a new attack on multivariate cryptography after finalists were announced.
  - Breaking the (lowest) original Rainbow parameters takes a weekend on Ward's laptop.
  - Security of MV schemes now under question.
- Daniel J. Bernstein and Tanja Lange have a (contested) attack avenue on structured lattice-based schemes.
  - Applies to all finalists, but not all alternates.
- NIST may re-open submissions for signature schemes.

What next?

Exciting research directions in 2022:

- How to transition to post-quantum in the real world?
- New ideas for signature schemes?
- Hertzbleed: Effect on each post-quantum *and* classical scheme?
- Lattices: How much structure is too much?
- Isogenies: What more can we do? Are they really secure?
- Multivariate: Can Beullen's attack be pushed further? Are there other attacks?

What next?

Exciting research directions in 2022:

- How to transition to post-quantum in the real world?
- New ideas for signature schemes?
- Hertzbleed: Effect on each post-quantum *and* classical scheme?
- Lattices: How much structure is too much?
- Isogenies: What more can we do? Are they really secure?
- Multivariate: Can Beullen's attack be pushed further? Are there other attacks?

Thank you!