Overview of post-quantum cryptography

D. J. Bernstein
University of Illinois at Chicago & Technische Universiteit Eindhoven

Cryptography = “secret writing”.

Achieve various security goals by secretly transforming messages.

Major theme of research:
Users have cost constraints. Can be challenging to reach acceptable security levels.
Secret-key cryptography

Prerequisite: Alice and Bob share a short secret key \( k \) not known to eavesdropper Eve.

Security goals:
Confidentiality and integrity for any number of messages exchanged by Alice and Bob, despite Eve’s espionage and forgery.

\[
\begin{array}{ccc}
  k & \rightarrow & k \\
  \downarrow & & \downarrow \\
  m & \rightarrow & c \\
  Alice & & Eve \\
  \downarrow & & \downarrow \\
  & \rightarrow & c' \\
  & Eve & Bob \\
  \downarrow & & \downarrow \\
  & \rightarrow & m \\
  & & if \ c' = c
\end{array}
\]
Public-key signatures

Prerequisite:
Alice has a short secret key $a$, corresponding public key $A$.
Everyone knows $A$.
Eve does not know $a$.

Security goal: Integrity
for any number of messages
published by Alice.

```
\[
\begin{align*}
\text{Alice} & \quad \rightarrow \quad A \\
\text{Alice} & \quad \rightarrow \quad c \\
\text{Eve} & \quad \rightarrow \quad c' \\
\text{Bob} & \quad \rightarrow \quad m \quad \text{if } c' = c
\end{align*}
\]
```
Public-key encryption (DH form)

Prerequisite:
Alice has $a$, $A$; Bob has $b$, $B$.
Public knows $A$ and $B$.
Eve does not know $a$, $b$.

Security goals:
Confidentiality and integrity
for any number of messages exchanged by Alice and Bob.

Alice \(\rightarrow\) $A$ \(\rightarrow\) Bob

Bob \(\leftarrow\) $b$ \(\leftarrow\) Alice

Alice \(\rightarrow\) $c$ \(\rightarrow\) Eve

Eve \(\rightarrow\) $c'$ \(\rightarrow\) Bob

Bob \(\leftarrow\) $m$ if $c' = c$
Advanced security goals

Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.
Advanced security goals

Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.

But I’ll focus on the most fundamental operations: secret-key cryptography, public-key signatures, public-key encryption.
The impact of physics

Critical for cryptography: attackers exploit physical reality.

1996 Kocher: typical crypto is broken by side channels.
The impact of physics

Critical for cryptography: attackers exploit physical reality.

1996 Kocher: typical crypto is broken by side channels.

⇒ Hundreds of papers on side-channel defenses.
The impact of physics

Critical for cryptography: attackers exploit physical reality.

1996 Kocher: typical crypto is broken by side channels.

⇒ Hundreds of papers on side-channel defenses.

1994 Shor, 1996 Grover: typical crypto will be broken by large quantum computers.
The impact of physics

Critical for cryptography: attackers exploit physical reality.

1996 Kocher: typical crypto is broken by side channels.

⇒ Hundreds of papers on side-channel defenses.

1994 Shor, 1996 Grover: typical crypto will be broken by large quantum computers.

⇒ Hundreds of papers on post-quantum cryptography.
Post-quantum secret-key crypto

Very easy solutions if $k$ is long uniform random string.
Post-quantum secret-key crypto

Very easy solutions if $k$ is long uniform random string.

Already standardized method to expand short $k$ into string indistinguishable from long $k$:

Post-quantum public-key signatures

Safe, ready for standardization: 1979 Merkle hash-tree public-key signature system.

Modern variants of system are guaranteed to be as secure as the underlying hash function.

Reasonable choice of function: Keccak with 576-bit capacity.
Post-quantum public-key encryption


Examples of post-quantum research

Better secret-key crypto: smaller, faster, easier to protect against side channels, etc.

Lattice-based cryptography: similar idea to code-based; maybe allows smaller keys; security analysis not as mature.

Signatures using codes/lattices.

Multivariate quadratics: very short signatures; maybe tolerable for encryption.

http://pqcrypto.org