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+forgery.

$$
\begin{tikzcd}
 & k \arrow[rr] \arrow[d] & & k \arrow[d] \\
m \arrow[r, "\text{Alice}"'] & c \arrow[r, "\text{Eve}"'] & c' \arrow[r, "\text{Bob}"'] & m \text{ if } c' = c
\end{tikzcd}
$$

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.

$$
\begin{tikzcd}
a \arrow[r, "\text{Alice}"] \arrow[dr] & A \arrow[dr] \arrow[drr, bend left] & & \\
m \arrow[r, "\text{Alice}"'] & c \arrow[r, "\text{Eve}"'] & c' \arrow[r, "\text{Bob}"'] & m \text{ if } c' = c
\end{tikzcd}
$$

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.

$$
\begin{tikzcd}
a \arrow[r, "\text{Alice}"] \arrow[dr] & A \arrow[dr] \arrow[drr, bend left] & & B \arrow[dll, bend right] \arrow[dl] & b \arrow[l, "\text{Bob}"'] \arrow[dl] \\
m \arrow[r, "\text{Alice}"'] & c \arrow[r, "\text{Eve}"'] & c' \arrow[r, "\text{Bob}"'] & m \text{ if } c' = c &
\end{tikzcd}
$$

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.

$\Rightarrow$ 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.

$\Rightarrow$ 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.

$\Rightarrow$ Hundreds of papers on
side-channel defenses.

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

$\Rightarrow$ Hundreds of papers on
post-quantum cryptography.

Post-quantum secret-key crypto

$$\begin{tikzcd} & k \arrow[rr] \arrow[d] & & k \arrow[d] \\ m \arrow[r, "\text{Alice}"'] & c \arrow[r, "\text{Eve}"'] & c' \arrow[r, "\text{Bob}"'] & m \text{ if } c' = c \end{tikzcd}$$

Very easy solutions if k is long uniform random string.

Post-quantum secret-key crypto

$$
\begin{array}{ccccccc}
 & & k & \longrightarrow & k & & \\
 & & \downarrow & & \downarrow & & \\
m & \xrightarrow[\text{Alice}]{} & c & \xrightarrow[\text{Eve}]{} & c' & \xrightarrow[\text{Bob}]{} & m \text{ if } c' = c
\end{array}
$$

Very easy solutions if k is long uniform random string.

Already standardized method to expand short k into string indistinguishable from long k: 1998 Daemen–Rijmen "Rijndael" cipher ("AES") using 256-bit key. Security analyzed in papers by dozens of cryptanalysts.

Post-quantum public-key signatures

$$\begin{tikzcd}
a \arrow[r, "\text{Alice}"] \arrow[dr] & A \arrow[dr] \arrow[drr, bend left] & & \\
m \arrow[r, "\text{Alice}"'] & c \arrow[r, "\text{Eve}"'] & c' \arrow[r, "\text{Bob}"'] & m \text{ if } c' = c
\end{tikzcd}$$

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

$$
\begin{tikzcd}
a \arrow[r, "\text{Alice}"] \arrow[dr] & A \arrow[dr] \arrow[drr, bend left] & & B \arrow[dl] \arrow[dll, bend right] & b \arrow[l, "\text{Bob}"'] \arrow[dl] \\
m \arrow[r, "\text{Alice}"'] & c \arrow[r, "\text{Eve}"'] & c' \arrow[r, "\text{Bob}"'] & m & \text{if } c' = c
\end{tikzcd}
$$

Safe, ready for standardization:
1978 McEliece encryption
using binary Goppa codes.

Main security-analysis papers:
1981, 1988, 1988, 1989, 1989,
1989, 1990, 1990, 1991, 1991,
1993, 1993, 1994, 1994, 1998,
1998, 2008, 2009, 2009, 2009,
2010, 2011, 2011, 2012, 2013.

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