What is a use case for quantum key exchange? Part II

D. J. Bernstein
University of Illinois at Chicago

What is QKE?

Many critical variations in quantum key exchange.

Highest cost: Alice and Bob have direct fiber-optic link (expensive!) between two quantum devices (expensive!).
Share initial secret using trusted couriers (expensive!).
Use shared secret to authenticate quantum key exchange.
Use quantum key (slowly!) for information-theoretic encryption, authentication.

Lower cost: Alice and Bob expand quantum key using AES.

Lower cost: Alice and Bob expand quantum key using AES.

2008 SECOQC: “This prototype network will run some well known applications like VoIP or Web Services in an unconditionally secure regime on a 24/7 basis.” Public demo included “video conferencing.”

Lower cost: Alice and Bob expand quantum key using AES.

2008 SECOQC: “This prototype network will run some well known applications like VoIP or Web Services in an unconditionally secure regime on a 24/7 basis.” Public demo included “video conferencing.”

Demo actually used AES to encrypt the video. Does SECOQC think AES is “unconditionally secure”?

Lower cost: Alice and Bob establish initial shared secret using public-key cryptography.

Paterson–Piper–Schack: "For example, if RSA digital signatures are used for authentication, a system of this type would become insecure if quantum computers became available."

Lower cost: Alice and Bob don't have direct link.

Trust intermediate "repeaters."

(Or "quantum repeaters": higher cost, less security loss.)

Standard security metrics

Confidentiality despite espionage:
Who can acquire data?

Integrity despite corruption:
Who can change data?

Availability despite sabotage:
Who can destroy data?

Example: Alice hears from Bob, Charlie, and Dave that Fred's public key is 8675309.

Alice uses public key 8675309 to check signed email from Fred.

Integrity analysis:
Email can be modified by anyone who can break into Fred's mail-handling computer; anyone who can break the public-key system; Bob, Charlie, and Dave acting in concert; etc.

The critical question,
assuming that the costs
of quantum cryptography
aren't prohibitive:

"How does QKE help security?"
Which attackers are stopped
only by quantum cryptography?

(Outside the scope of this talk:
Which attackers are stopped
only by non-quantum
cryptography?
Many important answers:
saboteurs, repeaters, et al.)

Searching for a QKE market

A courier can carry a key
of practically infinite length.

Searching for a QKE market

A courier can carry a key
of practically infinite length.

If Alice and Bob
can afford a courier
then QKE has no benefits.

Searching for a QKE market

A courier can carry a key
of practically infinite length.

If Alice and Bob
can afford a courier
then QKE has no benefits.

"Courier can break
confidentiality,
integrity, availability!"

Searching for a QKE market

A courier can carry a key of practically infinite length.

If Alice and Bob can afford a courier then QKE has no benefits.

"Courier can break confidentiality, integrity, availability!"

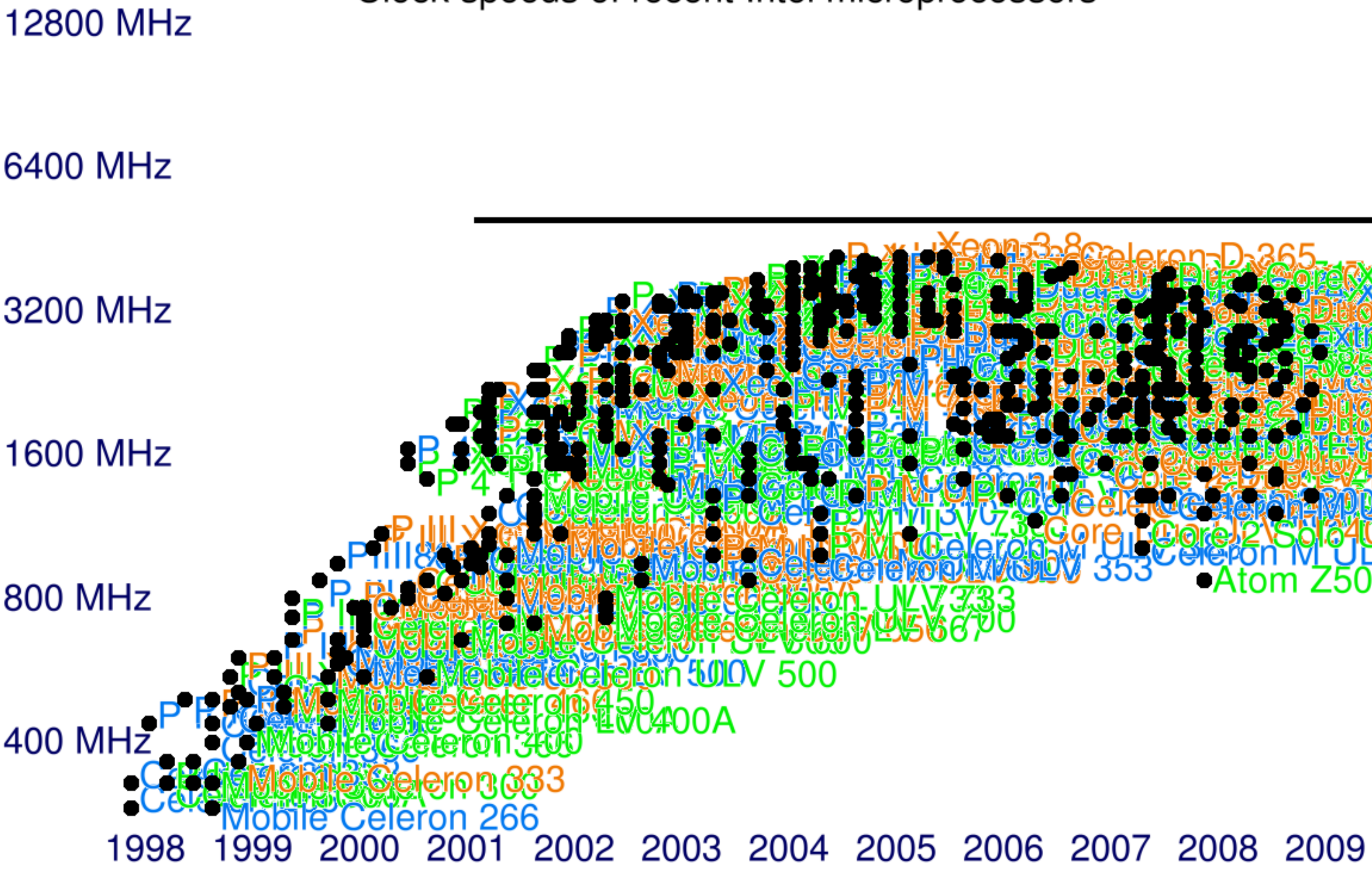
— True, but QKE doesn't protect against courier.

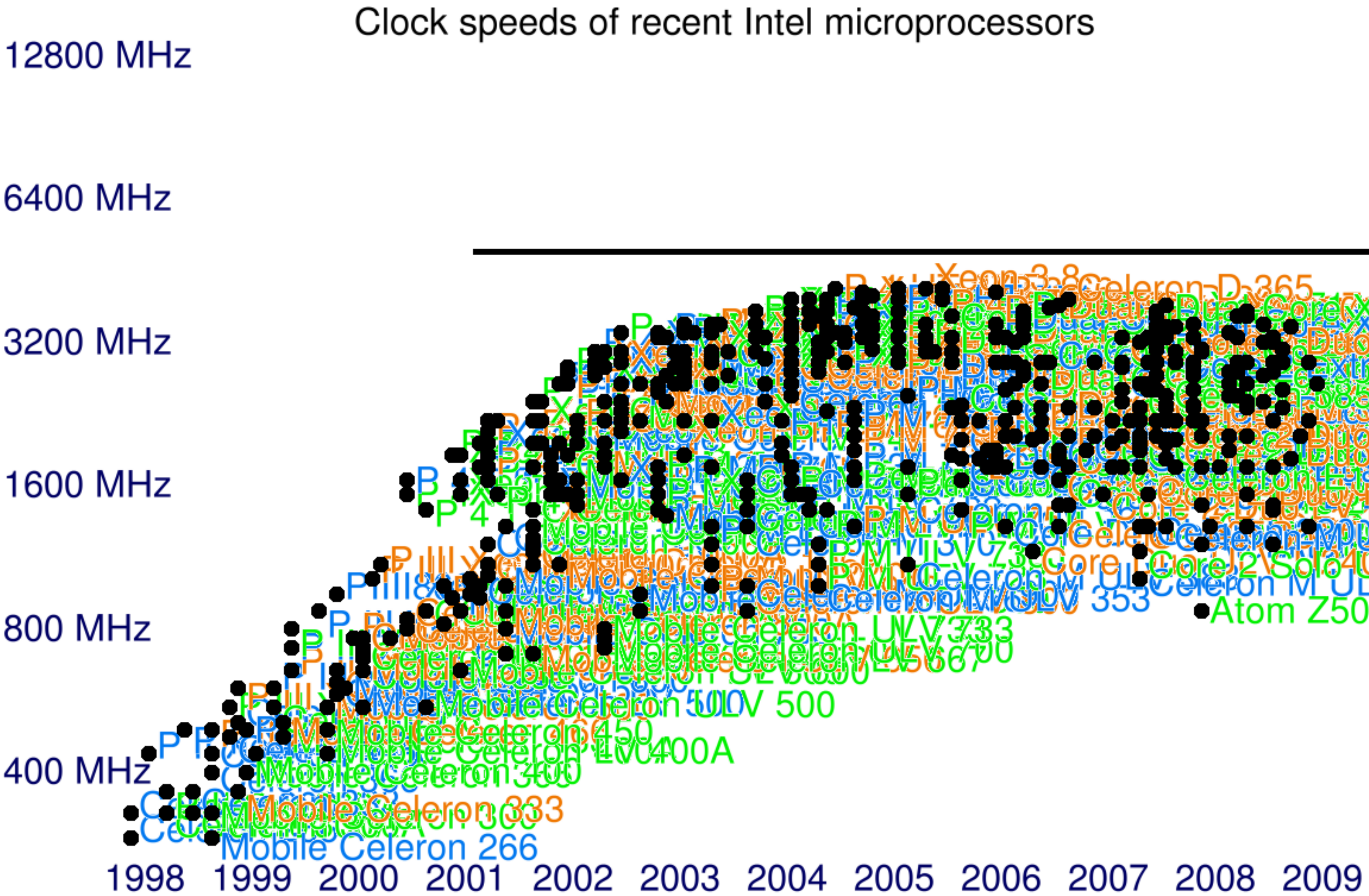
“Courier can break QKE,
but only by carrying out
a man-in-the-middle attack!
He needs to put his own
quantum device on the fiber
between Alice and Bob!”

“Courier can break QKE,
but only by carrying out
a man-in-the-middle attack!
He needs to put his own
quantum device on the fiber
between Alice and Bob!”

— Yes, have $\approx$1:1 ratio
between attacker’s costs
and Alice+Bob’s costs.
This isn’t security;
it doesn’t stop attacks.
We need much larger ratios.

Clock speeds of recent Intel microprocessors





General principle:

Computer power has a limit.

Consensus: $< 2^{400}$ operations.

Public-key cryptosystems that take $> 2^{400}$ operations to break will be secure forever.

If we have such systems then QKE has no benefits.

If we have such systems
then QKE has no benefits.

If every public-key cryptosystem
is *instantly* breakable
then QKE has no benefits.

If we have such systems
then QKE has no benefits.

If every public-key cryptosystem
is *instantly* breakable
then QKE has no benefits.

Intermediate possibility:
our strongest public-key system
is breakable but not instantly.

Alice+Bob can use this system
to share initial secret;
use initial secret
to authenticate QKE.
Subsequent break doesn't
compromise QKE security.

In the same situation,
Alice and Bob can achieve
integrity *without* QKE.

In the same situation,
Alice and Bob can achieve
integrity *without* QKE.

How? Standard technique:
Switch keys frequently.

Generate new secret key;
transmit corresponding public key
using current authentication;
discard previous key k.

Subsequent compromise of k
does not violate integrity.

Conclusion

QKE market needs
the following situation:
(1) our strongest cryptosystems
are broken but not quickly;
(2) Alice and Bob
can afford the costs of QKE; and
(3) they cannot afford a courier.

In this “winning” situation,
QKE does not improve integrity,
but does improve confidentiality:
without QKE, attacker
eventually sees old messages;
with QKE, attacker does not.