Cost-benefit analysis of quantum cryptography

D. J. Bernstein
University of Illinois at Chicago

NSF ITR–0716498

2004 Paterson–Piper–Schack:
"Why quantum cryptography?"

2007 Alléaume et al.: "SECOQC white paper on quantum key distribution and cryptography."

2008 Schneier:
"Quantum cryptography:
as awesome as it is pointless."

2009 Stebila–Mosca–Lütkenhaus:
"The case for quantum key distribution. . . . We argue that QKD will be an important part of future cryptographic infrastructures."

Different authors have come
to wildly different conclusions
regarding the value
of quantum cryptography.

Two sources of variability:

1. Analyses often contain
implicit differences in
models of what users value.

My response: Unified analysis;
model as explicit parameter.

2. Analyses often contain easily correctable errors.

My response: Education! Explain how future authors can recognize and avoid the most common pitfalls.

2. Analyses often contain easily correctable errors.

My response: Education! Explain how future authors can recognize and avoid the most common pitfalls.

Warning: Education fails when errors are malicious, economically motivated, etc.

Example: "If a quantum computer is created . . . then the levels of security that we now have to protect our information on computers will be worthless. It is absolutely essential that quantum cryptography be developed out before quantum computers become a reality."

Calgary press release, 2004. Author not clearly identified. Barry Sanders named as contact.

2005 id Quantique white paper "Future-proof Data Confidentiality with Quantum Cryptography":

"Finally, it is already proven that quantum computers[5] will allow to break public key cryptography."

"[5]Quantum computers are computers that exploit the laws of quantum physics to process information. They are still in the realm of experimental research, but will eventually be built."

In fact, quantum computers are not believed to break 1978 McEliece, 1979 Merkle, et al.

SECOQC white paper, page 20:

"As noted in [68], 'If powerful quantum computers could be built, most asymmetric cryptographic protocols in use today would no longer be secure, which would present a serious challenge for open networks and cryptographers should be prepared for this situation'."

[68] is a 15-author ECRYPT deliverable "Challenges for Cryptology Research in Europe for 2007–2013 and beyond."

What the deliverable actually said:
"If powerful quantum computers could be built, most asymmetric cryptographic protocols in use today would no longer be secure, which would present a serious challenge for open networks (for which quantum cryptology is not a solution either). We need to be prepared for this situation."

SECOQC authors removed
"for which quantum cryptology is not a solution either."

Pointed out by Tanja Lange.

What are we comparing?

Many critical variations in quantum key distribution.

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.)

What is the competition?

Many critical variations
in non-quantum cryptography.

Often cryptography is designed
for busy Internet servers
handling millions of users.
Cost drives many decisions.

Example: 2009 Kaminsky
complains that "10,000 ECC
operations per second" isn't
fast enough for DNS servers.

Does anyone claim that quantum cryptography is suitable for such applications?

Does anyone claim that quantum cryptography is suitable for such applications?

Let's focus on applications that aren't so cost-sensitive.

What can Alice and Bob do without quantum cryptography?

1. Use 16384-bit RSA *and* 512-bit ECC.

2. *Also* sign data
using Merkle hash trees
and "HFEv−" signatures.

Note: can easily build
secure public-key signatures
from *any* one-way function.

3. *Also* share secrets
using McEliece encryption
and lattice-based encryption.

See Tanja Lange's talk
for an introduction to
post-quantum cryptography.

4. 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.

5. *Also* share secrets
via trusted couriers.

6. Change secrets frequently,
overwriting s with $H(s)$.
Subsequent compromise of $H(s)$
does not reveal s.

7. Use 100 rounds of Salsa20
and 100 rounds of AES
and triple Luby–Rackoff.

Stebila–Mosca–Lütkenhaus:
"QKD is a new tool in the cryptographers toolbox: it allows for secure key agreement where the output key is entirely independent from any input value, a task that is impossible using classical cryptography."

Stebila–Mosca–Lütkenhaus:
"QKD is a new tool in the cryptographers toolbox: it allows for secure key agreement where the output key is entirely independent from any input value, a task that is impossible using classical cryptography."

"Impossible"? Really?
I generate new randomness, send it by trusted courier.

"If we live in a world where public key cryptography can no longer be employed safely, we must revert to shared secret key authentication or trusted third party authentication before we can use QKD. Here QKD still offers a benefit over an entirely classical solution because the key agreed upon by QKD is independent of the authentication keys, eliminating the ability of trusted third parties to later compromise information protected by QKD."

Understanding this "ability":

Suppose Alice and Bob
were using a shared AES key
to protect all their messages.

Eavesdropper records everything.

A month later,
eavesdropper sees opportunity
to sneak into Bob's office;
physically access encrypting
computer; copy the AES key.

Compromises future messages
and old messages.

But that isn't what
Alice and Bob are doing!

Once per second,
Alice and Bob overwrite
the AES key k with $H(k)$.

Sneaking into Bob's office
does not compromise old k.

Future traffic is compromised,
but that is also true
for quantum cryptography.

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 QKD 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.)

Variations in models, part 1:

Is there a secret-key cryptosystem unbreakable in 2^{400} operations?

Variations in models, part 1:

Is there a secret-key cryptosystem unbreakable in 2^{400} operations?

Consensus of cryptographers:

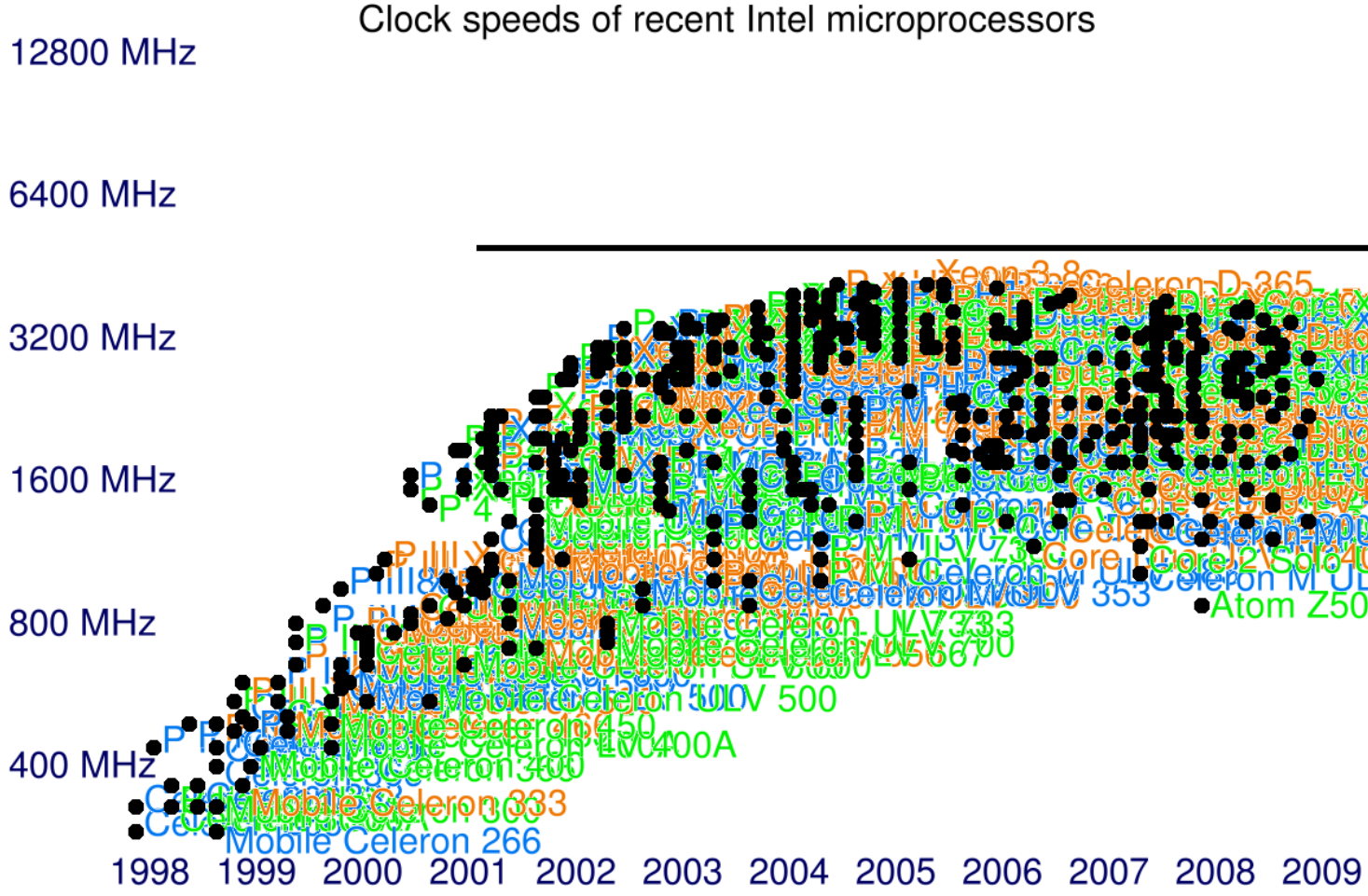
"Yes . . . and here it is!"

Variations in models, part 1:
Is there a secret-key cryptosystem unbreakable in 2^{400} operations?

Consensus of cryptographers:
"Yes . . . and here it is!"

Another possibility: "No."

Another possibility: "Maybe, but we're still looking for it."


Clock speeds of recent Intel microprocessors
12800 MHz
6400 MHz
3200 MHz
1600 MHz
800 MHz
400 MHz
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
Xeon 3.8
Celeron D 365
Core 2 Solo
Atom Z50
Mobile Celeron 266
Mobile Celeron 333
Mobile Celeron 300
Mobile Celeron 450
ULV 500
ULV 353
ULV 733
ULV 667
ULV 900
ULV 400A

Variations in models, part 2:
Is there a *public-key* cryptosystem unbreakable in 2^{400} operations?

Consensus of cryptographers:
"Yes . . . and here it is!"

Another possibility: "No."

Another possibility: "Maybe, but we're still looking for it."

If our strongest cryptosystems are unbreakable
then QKD has no benefits.

If our strongest cryptosystems
are unbreakable
then QKD has no benefits.

If our strongest cryptosystems
are very easily breakable
then QKD has no benefits.

If our strongest cryptosystems
are unbreakable
then QKD has no benefits.

If our strongest cryptosystems
are very easily breakable
then QKD has no benefits.

The only remaining case:
our strongest cryptosystems
are broken but not quickly.

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

QKD isn't completely useless if
(1) our strongest cryptosystems
are broken but not quickly;
(2) Alice and Bob
can afford the costs of QKD; and
(3) they cannot afford a courier.
In this "winning" situation,
without QKD, attacker
eventually sees old messages;
with QKD, attacker does not.