

High-speed cryptography

NSF Grant ITR-0716498

Daniel J. Bernstein

Center for Research and Instruction in Technologies for Electronic Security (RITES)

University of Illinois at Chicago



Why doesn't the Internet use cryptography?

“The Internet does use cryptography! I just made an SSL connection to my bank.”

Indeed, many connections use SSL, Skype, etc. But most connections don't.

Why is there so much unprotected Internet communication?

“Nobody cares about cryptography. Cryptography is pointless.”

Attackers are exploiting buffer overflows; they aren't intercepting or forging packets.”

In fact, attackers are forging packets and exploiting buffer overflows and doing much more.

Users want all of these problems fixed.

Why are typical Internet packets unencrypted and unauthenticated?

“It's too easy to write Internet software that exchanges data without any cryptographic protection.

Most Internet clients and servers don't know how to make cryptographic connections.”

True for most protocols. But let's focus on HTTP.

Most HTTP servers and browsers (Apache, Internet Explorer, Firefox, etc.) support SSL.

Why is SSL used for only a tiny fraction of all HTTP connections?

“Have you ever tried to set up SSL? I don't want to go through all these extra Apache configuration steps.

I don't want to pay for a certificate. I don't want to annoy my web-site visitors with self-signed certificates.”

Indeed, usability is a major issue; only about 1% of the Apache servers on the Internet have SSL enabled.

But let's focus on Google, which has paid for a certificate and uses SSL for https://mail.google.com.

If you connect to https://www.google.com, Google redirects you to http://www.google.com.

Why does Google actively turn off cryptographic protection?

“Enabling SSL for more than a small fraction of Google connections would overload the Google servers.

Google doesn't want to pay for a bunch of extra computers.”

Many companies sell SSL accelerators, but those cost money too.

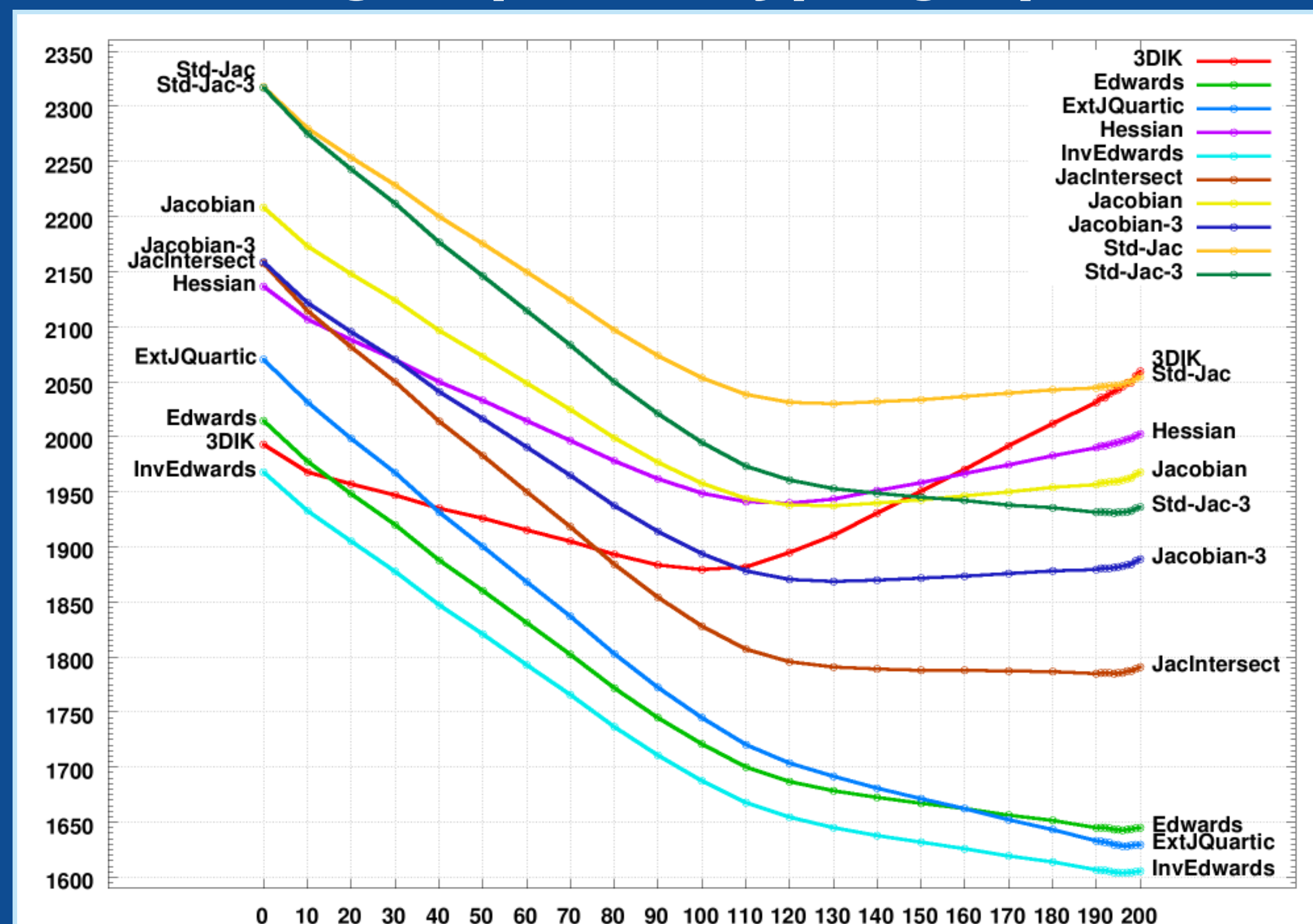
Does cryptography have to be so expensive?

Can we make it fast enough to protect all of Google's communications?

Can we make it fast enough to protect every Internet packet?

Expected results of project:

1. New tools for high-speed engineering of high-speed software.
2. New speed records for encryption, authentication, etc.
3. New high-speed cryptographic Internet software.



Latest news:

In joint work with Tanja Lange (Technische Universiteit Eindhoven) the PI has shown how to use

“Edwards curves”

to set new speed records for elliptic-curve cryptography.

Unexpected spinoff:

This work has also produced speedups in other elliptic-curve computations, including “ECM,” a critical part of “cofactorization” in the famous “NFS” attack on the RSA cryptosystem.