DNSCurve: Usable security for DNS

D. J. Bernstein
University of Illinois at Chicago

Thanks to: NSF ITR–0716498

How do web browsers find `http://certicom.com` or `http://brightsight.com`?

How do mail programs find `microsoft.com`?

They ask the Domain Name System.

How do web browsers find
`http://certicom.com` or
`http://brightsight.com`?

How do mail programs find
`microsoft.com`?

They ask the Domain Name System.
DNS has no security whatsoever.

Cryptography is used for private tunnels and for a small fraction of web pages but everybody knows that it's too slow to protect *all* communication.

DNSSEC tries to minimize server costs by *precomputing* signatures.

DNSSEC tries to minimize client costs by using 1024-bit RSA.

Unfortunately, this precomputation causes severe usability problems.

Unfortunately, this precomputation causes severe usability problems.

“Fifteen years.

Unfortunately, this precomputation causes severe usability problems.

“Fifteen years. Ten million dollars of grants.

Unfortunately, this precomputation causes severe usability problems.

"Fifteen years. Ten million dollars of grants. More than 100 users."

Actually, crypto isn't so slow!
New project, DNSCurve:

1. Use state-of-the-art ECDH.

2. Reuse secret for subsequent packets exchanged between same parties.

3. Integrate carefully with DNS to avoid other usability problems.