How to deal with annoying questions from Dan

Peter Schwabe

Eindhoven University of Technology

May 4, 2010

Africacrypt 2010, Rump Session

The problem

- Imagine you are a protocol designer
- Imagine you just gave a nice talk on a nice new protocol
- Of course you are prepared for many interesting questions about your protocol

The problem

- Imagine you are a protocol designer
- Imagine you just gave a nice talk on a nice new protocol
- Of course you are prepared for many interesting questions about your protocol

But...

- Imagine Dan Bernstein is in the audience
- You will get a question like...

The problem

- Imagine you are a protocol designer
- Imagine you just gave a nice talk on a nice new protocol
- Of course you are prepared for many interesting questions about your protocol

But...

- Imagine Dan Bernstein is in the audience
- You will get a question like...
  - How efficient is your protocol?

The problem

- Imagine you are a protocol designer
- Imagine you just gave a nice talk on a nice new protocol
- Of course you are prepared for many interesting questions about your protocol

But...

- Imagine Dan Bernstein is in the audience
- You will get a question like...
  - How efficient is your protocol?
  - Did you implement your protocol?

The problem

- Imagine you are a protocol designer
- Imagine you just gave a nice talk on a nice new protocol
- Of course you are prepared for many interesting questions about your protocol

But...

- Imagine Dan Bernstein is in the audience
- You will get a question like...
  - How efficient is your protocol?
  - Did you implement your protocol?
  - Is this protocol feasible in practice, how many cycles will it take on a Core 2 Quad Q6600, running at 2404.228 MHz?

Common answers...

- Would be very interesting to see, but we didn't implement it...
- I'm not really an implementor... hard to say...
- The protocol involves pairings so... we don't really know... but probably "yes"?!

The solution
(for pairing-based protocols)

Technische Universiteit Eindhoven University of Technology

- New pairing software available at http://cryptojedi.org/crypto/#dclxvi
- Joint work with Michael Naehrig and Ruben Niederhagen
- Requires 4451688 cycles for a pairing on a Core 2 Quad Q6600 running at 2404.228 MHz
- More than $2\times$ faster than previously published results
- Code is public domain (do with it what you like!)
- Paper describing the implementation: http://eprint.iacr.org/2010/186/