Curves – next steps

Kenny Paterson
CFRG co-chair
Royal Holloway, University of London

Where we are – 1

- We have selected two curves
  - Curve25519 – already deployed in several places.
  - Goldilocks – offers good performance-security trade-off at higher security level (approx 224 bits).

- These curves (and base points) are produced by a deterministic procedure that takes as its only input a prime *p* for the underlying field.

- http://www.ietf.org/internet-drafts/draft-irtf-cfrg-curves-02.txt

Where we are – 2

- We have defined how to do DH key exchange for both curves*.

- http://www.ietf.org/internet-drafts/draft-irtf-cfrg-curves-02.txt

  - *some detail missing from current draft for Goldilocks; endian-ness poll taking place now.

Where we are – 3

- We have submitted a short proposal to the NIST workshop as IETF/IRTF input.
- We have liaised with W3C.
- We need people's help to keep the mailing list discussion productive and respectful.

Where we are going next – 1

- The next major work item is to select and define a signature scheme for use with the new curves.

- We could stop now and deliver to TLS WG without that, since existing signature schemes could be used there.
  - RSA-PKCS, ECDSA, maybe RSA-PSS.

- But we might get significant performance and implementation security gains by adopting a different scheme.

Where we are going next – 2

- Some signature options (illustrative, not definitive):
  - ECDSA on the (twisted) Edwards form versions of the new curves.
    - Is that compliant with NIST standard for ECDSA?
    - Does that matter?
  - De-randomised ECDSA.
    - Avoids common failure mode of ECDSA.
    - Generate *r* for ECDSA by hashing message and private key.
    - OR generate *r* via PRF on message using separate key K; augment ECDSA private key to include K.

Where we are going next – 3

- Some signature options (illustrative, not definitive):
  - EdDSA [BDLSY'11]
    - Variant of Schnorr signature scheme, rather than DSA.
    - Uses derandomisation trick and a different verification equation.
    - Already deployed in OpenSSH.
  - Others?

Where we are going next – 4

- Some questions for the audience:
  - What other signature schemes should we be considering?
  - How much does NIST compliance matter for TLS?
  - How much does it matter for other applications?
  - (Meta:) How should we structure the discussion to make sure it reaches a useful conclusion in a timely fashion?