CFRG Work on Curves

Stephen Farrell (IETF Security Area Director)
Kathleen Moriarity (IETF Security Area Director)
Alexey Melnikov (CFRG co-chair)
Kenny Paterson (CFRG co-chair)

Genesis – “Elephant, meet room”

- IETF has been overly dependent on NIST for crypto
  - Not surprising given excellent history starting from AES competition
- There is ongoing mostly-silly speculation about the seeds for NIST curves
  - That NIST has not issued any statement doesn't help. Even one saying “we wish we did remember, but we don't, sorry;-)”
  - Dual-ec-dbrg did damage: wild speculation gains credence, even if only amongst the gullible
- But, the real motivation for work in CFRG is the better performance and side-channel resistance of new curves developed by academic cryptographers over the last decade

Genesis

- CFRG list announcement July 15th relaying request for new curve recommendations from TLS WG chairs.

- CFRG chairs announced a 2-part process:
  - Reach rough consensus on requirements (2 wks).
  - Reach rough consensus on curves (4 wks).
  - Finalise recommendations (2 wks).

Genesis

- This was rather naïve on the part of the chairs.

- What ensued was a wide-ranging and sometimes heated discussion about different curves and schemes.

Requirements where Consensus was Reached

- Protection against side-channel attacks strongly desired.
- Basic elements of curve selection – defined over prime field; prime or near-prime order; twist security.
  - Not always needed, but we can achieve these at no real cost.
- Need to support existing algorithms.
  - Strong steer from TLS WG.
  - ECDHE, EC-DSA, and maybe ECDH.
  - Interoperability with existing wire formats desirable, not essential.
  - Versus potential performance gains from adopting new algorithms.
- Need for *rigidity* in curve generation process.
  - Trustable curve generation process is important.
  - It was a primary motivation for this work.

Curves

We have selected two curves:

- Curve25519 – approx 128 bits of security; already deployed in several places.
- Goldilocks – offers good performance-security trade-off at higher security level (approx 224 bits of security).
- These curves (and base points) are produced by a deterministic procedure that takes as its only input a prime *p* for the underlying field.
- We have defined procedures for generating curves in (twisted) Edwards form from these curves (for signatures).

https://tools.ietf.org/html/draft-irtf-cfrg-curves

Diffie-Hellman Key Exchange

- We have defined how to do DH key exchange for both curves.
- Deciding on low-level issues such as endian-ness was surprisingly time-consuming.
- In principal, these curves can be deployed “as is” in TLS in combination with existing signature schemes.

Signatures

- Our current work is focussed on selecting a signature scheme for use with the new curves.
- Existing schemes supported in TLS are RSA and ECDSA.
- We expect to achieve significant performance and implementation security gains over existing schemes.

Signatures

- Decisions so far:
  - Compatibility with NIST signature schemes not required.
  - Use a deterministic scheme to avoid common failure modes of curve-based signature schemes.
  - Adopt a IUF interface for signing.
    - Reflects common implementation practice, enables signatures for long messages to be computed in constant space.

More General Outlook

- CFRG hopefully finish work in a timely fashion and that gets adopted by IETF working groups
  - For TLS, DNSSEC, PGP, …
- CFRG have already done good work on chacha20-poly1305 which seems like a fine replacement for RC4 ciphersuites in TLS
  - For those w/o AES h/w
- From an IETF perspective we hope CFRG continue to be a place from which the IETF can get timely advice on algorithms and specifications of algorithms that we want to make MTI
  - MTI = mandatory to implement

Even More General Outlook

- We (slideware authors:-) hope NIST also adopt what CFRG produces that gets deployed, both for curves and more generally
- We fully understand that NIST have a different constituency and different processes, and that's ok
- The IETF seem very unlikely to want to wait for a NIST outcome on curves
  - Mainly because of the security & performance benefits of the new curves

Thanks

- Feel free to send queries to whichever of these addresses you find most appropriate
  - stephen.farrell@cs.tcd.ie
  - kenny.Paterson@rhul.ac.uk
  - alexey.melnikov@isode.com
  - kathleen.moriarty.ietf@gmail.com
  - cfrg@irtf.org