NIST Announcements

Computer Security Division

Crypto 2011 Rump Session
Available for public comments

- Draft 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.

Close date: October 1, 2011
Available for public comments

- Draft 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.
  Close date: October 1, 2011

- Draft 800-133: Recommendation for Cryptographic Key Generation
  Close date: September 30, 2011
Available for public comments

- Draft 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.
  
  Close date: October 1, 2011

- Draft 800-133: Recommendation for Cryptographic Key Generation
  
  Close date: September 30, 2011

Find the links at http://csrc.nist.gov/publications/PubsDrafts.html
Workshop on Cryptography for Emerging Technologies and Applications
November 7-8, 2011
NIST Campus in Gaithersburg, MD, USA
NIST Upcoming Workshop and Conference

Workshop on Cryptography for Emerging Technologies and Applications
November 7-8, 2011
NIST Campus in Gaithersburg, MD, USA

The Third SHA-3 Candidate Conference
March 22-23, 2012
Washington DC, USA (co-located with FSE March 19-21)
A PUBLIC RANDOMNESS SOURCE.
THREAT MODEL.
Threat Model Rene.
Threat Model Kelsey.
NIST Beacon
Nixed!
Will broadcast full-entropy bit-strings.
- Will broadcast full-entropy bit-strings.
- Will do it in blocks of 512 bits per minute.
- Will broadcast full-entropy bit-strings.
- Will do it in blocks of 512 bits per minute.
- Will sign and time-stamp.
- Will broadcast full-entropy bit-strings.
- Will do it in blocks of 512 bits per minute.
- Will sign and time-stamp.
- Will link the sequence of blocks with a secure hash.
Will broadcast full-entropy bit-strings.

Will do it in blocks of 512 bits per minute.

Will sign and time-stamp.

Will link the sequence of blocks with a secure hash.

As for source of entropy, we are talking to NIST physicists.
Prototype architecture.

- DRBG Engine (SP 800-90)
- HTTP Server
- Database
- Client (HTTP Client)
- Firewall

Crosslinks:
- Special Pubs.
- Meetings
- NIST Beacon
- Architecture
- Team applications
NIST Beacon

Team: Larry Basham, Michaela Iorga, Michael Fischer (Yale), John Kelsey, Rene Peralta.

Timeframe: this year we plan to complete a prototype.

Contact: michaela.iorga@nist.gov
My favorite application: Given additively-homomorphic bit-commitment, produce 4-tuples of bit-commitments guaranteed to be in the set

\[ U = \{0111, 1011, 1101, 1110\} \]
My favorite application: Given additively-homomorphic bit-commitment, produce 4-tuples of bit-commitments guaranteed to be in the set

\[ U = \{0111, 1011, 1101, 1110\} \]

(BDP 1996) : There is a linear transformation from U to correct input-output bits of any binary linear gate.
My favorite application: Given additively-homomorphic bit-commitment, produce 4-tuples of bit-commitments guaranteed to be in the set

\[ U = \{0111, 1011, 1101, 1110\} \]

(BDP 1996) : There is a linear transformation from U to correct input-output bits of any binary linear gate.

Use this until practical fully homomorphic encryption is available.