To Rijndael256 or not that is the question

Bart Preneel

1

Rijndael128/128-192-256 is AES

1. ~~Standardize Rijndael160/* or Rijndael224/*?~~
2. ~~Standardize Rijndael192/128 or Rijndael192/192 or Rijndael192/256?~~
3. ~~Standardize Rijndael256/192 or Rijndael256/128?~~
4. Standardize Rijndael256/256 ?

a) It was already in the selected Rijndael proposal
b) We need post-quantum proofs
c) BBB schemes are messy
d) Block ciphers are so 1990s
e) SHA-3 is better at MAC and AEAD and keywrap and variable length encryption

2

If we standardize Rijndael256/256

a) Keep it as is
b) Change the key schedule
   - If so, how?
c) Include MixColumns in the last round
d) Make changes to that it is easier to implement with AES-NI2
e) Change the number of rounds from 14

3

Update of standards using AES?

- GMAC and GCM
- CMAC and CCM
- KeyWrap
- XTS
- Wide-Block AES
- Accordion
- ISO 10118: Hash functions based on block ciphers

4

What else should we standardize?

- Accordion or AEAD based on SHA-3?

5