Development of SP 800–38 Series for Block Cipher Modes

Morris Dworkin
May 29, 2014

Computer Security Division
National Institute of Standards and Technology (NIST)
• Transformation of fixed-length data blocks
• Parameterized by the choice of a secret, symmetric key, $K$
• Invertible
Block Cipher Mode of Operation

- A function that features a block cipher for
  - confidentiality/encryption
  - data integrity/source authentication
  - authenticated encryption w/associated data (AEAD)
- Other types of modes are possible, e.g.,
  - hash functions
  - random number generators
  - key derivation functions
- Variety of performance/security properties
  - Analogy to a vehicle built around a block cipher “engine”
Advanced Encryption Standard (AES)

- Public competition for new block cipher
  - initiated in 1997
  - compared to [Triple] Data Encryption Standard (DES)
    - increase key sizes from 56/112/168 to 128/192/256
    - increase block size from 64 bits to 128 bits

- The AES was published in FIPS Pub 197 in 2001
  - NIST Special Publications authorized as a source for new modes of operation

- Watershed in NIST cryptography standards
  - public participation and widespread acceptance
NIST Block Cipher & Modes Pubs

1977    FIPS Pub 46: DES
1980    FIPS Pub 81: ECB, CBC, CFB, OFB
1998    FIPS Pub 46–3: Triple DES
2001    FIPS Pub 197: AES
         SP 800–38A: Updated DES modes & CTR
2004    SP 800–38C: CCM
2005    SP 800–38B: CMAC
2007    SP 800–38D: GCM, GMAC
         SP 800–38A Addendum: CBC–CS variants
2012    SP 800–38F: KW, KWP, TKW
Outline of Process

- Open invitation to public to submit modes
- Submitted proposals are posted for public review
- NIST decides to pursue a proposal
- NIST develops a draft Special Publication for public review in consultation with submitters
- NIST decides whether to
  - finalize and publish the document
  - revise the draft for further public review
  - withdraw plan to approve proposal
# The 800–38 Series of NIST Special Publications

<table>
<thead>
<tr>
<th>Pub.</th>
<th>38A</th>
<th>38B</th>
<th>38C</th>
<th>38D</th>
<th>38E</th>
<th>38F</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode(s)</strong></td>
<td>ECB, CBC, CFB, OFB, CTR, CBC–CS*</td>
<td>CMAC</td>
<td>CCM</td>
<td>GCM (GMAC)</td>
<td>XTS–AES</td>
<td>KW, KWP, TKW</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>confid.</td>
<td>authent’n</td>
<td>AEAD</td>
<td>AEAD</td>
<td>confid.</td>
<td>key wrap</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>NIST, NSA, Ind., Acad.</td>
<td>Acad.</td>
<td>Ind.</td>
<td>Ind.</td>
<td>Ind.</td>
<td>NSA, Ind.</td>
</tr>
<tr>
<td><strong>Impetus</strong></td>
<td>update FIPS 81 modes for AES</td>
<td>improve CBC–MAC</td>
<td>WLANs</td>
<td>Internet routers</td>
<td>storage</td>
<td>gen. key managem’t, S/MIME</td>
</tr>
</tbody>
</table>

* ciphertext stealing variants in addendum
Some Other Proposals

- OCB, IAPM
  - efficient, general purpose AEAD modes
  - intellectual property complications
- EAX, SIV
  - AEAD modes, submitted as alternatives to CCM, KW
- EAXPrime
  - variant of EAX specified in ANS C12.22 for Smart Grid
  - NIST had planned to approve
  - security concern for short messages
- Format-preserving encryption (FPE) modes
  - pending in draft SP 800–38G
- 32 modes currently posted at csrc.nist.gov
Main Selection Considerations

- whether the mode serves an important need
  - for U.S. Government or
  - in promoting commerce

- whether existing modes in the NIST toolkit, or other submitted modes, can adequately provide the desired properties/functionality

- whether the mode provides adequate security

- for patented modes, whether acceptable royalty-free alternatives are available.
Vetting Security of Modes

- Expertise of designers
- Public review
  - many instances of useful input
  - meaningful consideration not ensured
- Historic reliance on NSA
- NIST in-house capability improving over time
- Security “proofs”
  - fundamentally rely on security of underlying block cipher
  - assumptions/model are important
  - desirable, but not a requirement, e.g., KW
    - arguably over-engineered for security
    - does not appear to lend itself to reduction proofs
NSA Involvement

- NIST statutory responsibility to consult with NSA
  - review modes proposals, indicate security concerns
  - two specific instances
    - advice to propose RMAC for 800-38B
    - support for GCM proposal
- NSA-designed modes
  - CFB mode in FIPS 81, updated in SP 800-38A
  - KW (at NIST’s request) and KWP in SP 800-38F
  - DCM proposed and quickly withdrawn
- Opportunities to comment on draft 800-38 series publications
  - before and after release for public comment
  - one instance of contributing extended text
    - guidance for short tags for GCM in SP 800-38D
Opportunities for Public Input

- Public workshops in 2000 and 2001
- NIST requested input on several modes decisions
  - a plan for revising the draft specification of RMAC
  - choice between CWC and GCM
  - whether to pursue XTS–AES
  - whether to develop format–preserving encryption modes
- Periods of public comment on draft 800–38 series publications
  - announced on csrc.nist.gov, ASC X9, IETF, etc.
  - normally 30–60 days
- Public comments posted on csrc.nist.gov
Responsiveness to Comments

- Replaced RMAC with CMAC in second draft SP 800–38B
- Choose GCM over CWC for draft SP 800–38D
  - included support from CWC submitter
- Proceeded with plan to propose approval XTS–AES by reference to IEEE Std. 1619
  - NIST insisted that IEEE provide the relevant excerpt free-of-charge during the period of public review
- Withdrawal of plan to approve EAXPrime
Difficult Decisions

- **Draft SP 800–38D specifying GCM**
  - Security concerns identified in public comments
    - Some authentication weaknesses
    - Significant vulnerability to misuse (nonce repetition)
  - Decision to revise draft with additional guidance
    - Can be implemented securely, a powerful/useful mode
    - Support from NSA

- **Draft SP 800–38E specifying XTS–AES by ref.**
  - Use–case, other technical concerns in public comments
  - Close decision to publish, to support IEEE P1619 SISWG

- **Incompatibility of CMAC with ANS X9.24**
  - Encryption of 0: secret value or public value?
  - ASC X9 could develop new key check method for AES
  - Avoid further delay of SP 800–38B
Two Concluding Thoughts

• In modes work, NIST has cultivated ties with a variety of stakeholders in government, academia, and industry, while also considering the interests of the general public.

• Flexibility in approaches/processes has been valuable as modes work has evolved to meet emerging needs.