

Status Update on the Review of the NIST Block Cipher Modes

Nicky Mouha

Strativia

FrisiaCrypt 2022
Monday, September 26, 2022

- NIST commitment:
 - Periodical review of standards
- First review: AES (FIPS 197)
 - NISTIR 8319: Review of the AES (July 2021)
- Next review: Modes of operation (SP 800-38 Series)
 - Talk at Dagstuhl Symmetric Cryptography (April 2022)
 - This talk: 38 Series and 38A announcement explained!

NIST SP 800-38 Series

- NIST SP 800-38A + Add: ECB, CBC, CFB, OFB, CTR
 -
- NIST SP 800-38B: CMAC
 -
- NIST SP 800-38C: CCM
 -
- NIST SP 800-38D: GCM
 -
- NIST SP 800-38E: XTS-AES
 -
- NIST SP 800-38F: KW, KWP, TKW
 -
- NIST SP 800-38G: FF1, FF3
 -

NIST SP 800-38 Series

- NIST SP 800-38A + Add: ECB, CBC, CFB, OFB, CTR
 - CPA security (except ECB)
- NIST SP 800-38B: CMAC
 - MAC security
- NIST SP 800-38C: CCM
 - CPA + MAC = CCA security
- NIST SP 800-38D: GCM
 - CPA + MAC = CCA security
- NIST SP 800-38E: XTS-AES
 - CCA up-to-block (without MAC)
- NIST SP 800-38F: KW, KWP, TKW
 - CCA (without MAC)
- NIST SP 800-38G: FF1, FF3
 - CCA (without MAC)

NIST SP 800-38 Series

- NIST SP 800-38A + Add: ECB, CBC, CFB, OFB, CTR
 - CPA security (except ECB), IV (except ECB)
- NIST SP 800-38B: CMAC
 - MAC security
- NIST SP 800-38C: CCM
 - CPA + MAC = CCA security, nonce
- NIST SP 800-38D: GCM
 - CPA + MAC = CCA security, nonce
- NIST SP 800-38E: XTS-AES
 - CCA up-to-block (without MAC), tweak
- NIST SP 800-38F: KW, KWP, TKW
 - CCA (without MAC), no tweak
- NIST SP 800-38G: FF1, FF3
 - CCA (without MAC), tweak

- Note the evolution:
 - CPA \rightarrow CPA + MAC \rightarrow CCA
 - IV \rightarrow nonce \rightarrow tweak
- To understand the 38 Series and the 38A announcement, we need to explain these terms!

- FISMA defines “information security” as:
 - Confidentiality
 - Integrity (incl. nonrepudiation and authenticity)
 - Availability

- FISMA defines “information security” as:
 - Confidentiality
 - Integrity (incl. nonrepudiation and authenticity)
 - Availability
- We need two additional terms:
 - Semantic security: *“Can the attacker learn something by having the ciphertext that is not already known about the plaintext?”*

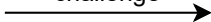
- FISMA defines “information security” as:
 - Confidentiality
 - Integrity (incl. nonrepudiation and authenticity)
 - Availability
- We need two additional terms:
 - Semantic security: *“Can the attacker learn something by having the ciphertext that is not already known about the plaintext?”*
 - Non-malleability: *“Can the attacker modify the ciphertext so that it decrypts to a related plaintext?”*

- FISMA defines “information security” as:
 - Confidentiality
 - Integrity (incl. nonrepudiation and authenticity)
 - Availability
- We need two additional terms:
 - Semantic security: *“Can the attacker learn something by having the ciphertext that is not already known about the plaintext?”*
 - Non-malleability: *“Can the attacker modify the ciphertext so that it decrypts to a related plaintext?”*
- Implications:
 - IND-CPA \rightarrow semantic security \rightarrow confidentiality
 - IND-CCA \rightarrow non-malleability \rightarrow integrity

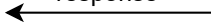
A Simple Challenge-Response Protocol



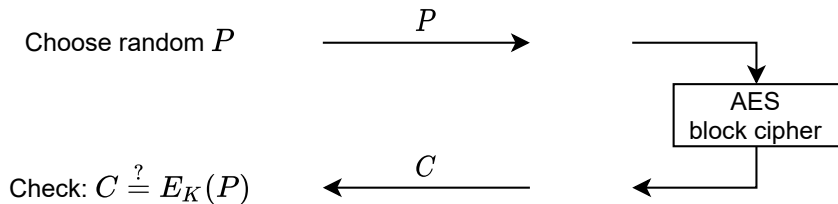
challenge



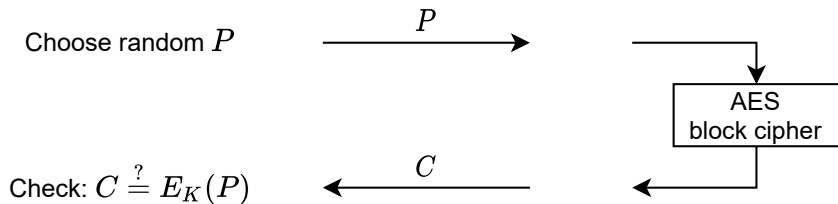
response



A Simple Challenge-Response Protocol



A Simple Challenge-Response Protocol



- Chosen Plaintext Attacks (CPA) are realistic!
- Used in SP 800-73-4 Part 2 for PIV cards (with ECB!)

- Achieving CPA security is the basis
 - Requires block cipher (AES) and any IV-based mode of operation
 - Without IV: we know if plaintexts are equal (or much more!)
 - IV may require unpredictability, nonces just need to be unique!

- Achieving CPA security is the basis
 - Requires block cipher (AES) and any IV-based mode of operation
 - Without IV: we know if plaintexts are equal (or much more!)
 - IV may require unpredictability, nonces just need to be unique!
- Achieving CCA security is usually done with a MAC
 - If a ciphertext is modified, it will not decrypt! (38C/38D)

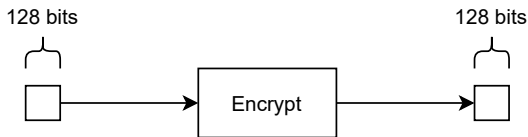
- Achieving CPA security is the basis
 - Requires block cipher (AES) and any IV-based mode of operation
 - Without IV: we know if plaintexts are equal (or much more!)
 - IV may require unpredictability, nonces just need to be unique!
- Achieving CCA security is usually done with a MAC
 - If a ciphertext is modified, it will not decrypt! (38C/38D)
- But... repeated nonce or no space for MAC?
 - “Misuse resistance”: nonce becomes tweak
 - Achieve CCA directly without MAC (38E/38F/38G)
 - If MAC is used: pad-then-encipher (38F/38G)

Announcement on 38A

- Announcement to revise SP 800-38A
 - Website: <https://csrc.nist.gov/News/2022/proposal-to-revise-sp-800-38a>
 - Public comments available
- In a nutshell
 - (Sort of) deprecate ECB
 - Many problems with 38A, recently Fujita et al. (ACNS 2020)
 - Revision of 38A with guidance on how to use them
- Problems with 38A
 - Predictable IVs, IV reuse, ciphertext malleability, insecurely combining CBC + MAC (padding oracles),...
 - Next slides: some intuition

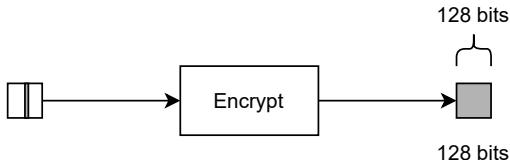
Why Modes? Limitations of AES

- AES
(all key sizes)

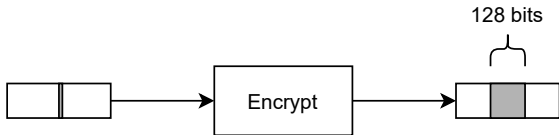


Bit Flips (Encryption, Same IV)

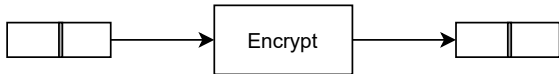
- AES
(best achievable)



- ECB, XTS
(corresponding block)



- CTR, OFB
(corresponding bit)



- CBC
(best for single-pass)



Bit Flips (Decryption, No MAC)

- AES

(best achievable)

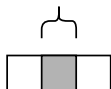
128 bits



- ECB, XTS

(corresponding block)

128 bits



- CTR, OFB

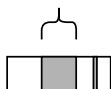
(corresponding bit)



- CBC

(one block + one bit)

128 bits



Detecting Bit Errors

- Bit errors in ciphertext:
 - “the existence of such bit errors may be detected by their randomizing effect on their decryption” (NIST SP 800-38A)
- So: 128 random plaintext bits → checksum failure?
 - “SSH insertion attack” CBC/CFB + CRC-32 (CVE-1999-1085)

Where Are 38A Modes Used?

- Length-preserving encryption
 - XTS (38E): only for storage devices
(but 38A modes “continue to be approved for such devices”)
 - Applications exist where ciphertext cannot be expanded...
- Building block for AEAD
 - Authentication-only mode: CMAC (38B), HMAC (FIPS 198-1)
 - Generic AEAD: e.g., CBC + HMAC
 - CCM (38C) and GCM (38D): AEAD based on CTR!

Always Use AEAD Modes?

- GCM (38C) and CCM (38D)
 - Based on **CTR**
- Nonce reuse:
 - Deduce plaintext from ciphertext difference!
- Short tag / no tag:
 - Control plaintext through ciphertext difference!

Alternatives?

- Nonce reuse: KW/KWP/TKW (38F) or FF1/FF3 (38G)
 - “Misuse resistant” AEAD
 - Most suitable for key wrapping (38F) or formatted data (38G)
 - Very slow for general use...
- No tag: XTS (38E)
 - ECB-like mode: independently encrypts every block...
 - Only for storage devices
 - CBC (38A): sometimes preferable?

Conclusion

- Deprecate 38A modes?
 - Secure alternative not always available...
- To discuss
 - Applications where “misuse” is unavoidable?
 - Which requirements?

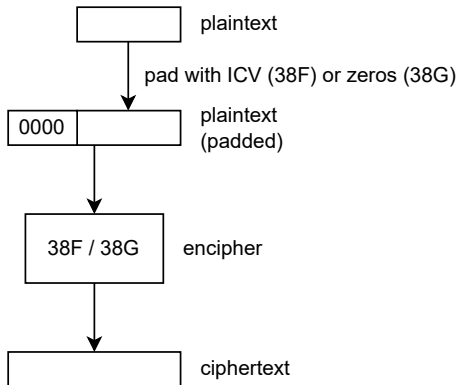
Conclusion

- Deprecate 38A modes?
 - Secure alternative not always available...
- To discuss
 - Applications where “misuse” is unavoidable?
 - Which requirements?
- Questions?

Backup Slides

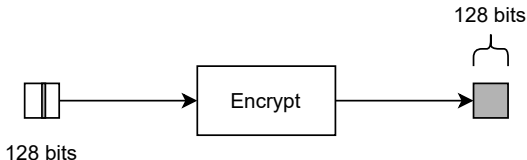
Pad-Then-Encipher (Rogaway-Shrimpton, Eurocrypt 2006)

- Encipher requires CCA security (next slide)

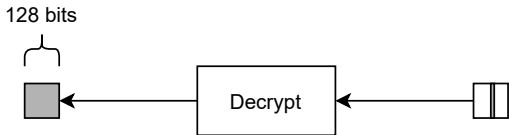


CCA Security

- AES
(random ciphertext)



- AES
(random plaintext)



- 38F, 38G
(random ciphertext)



- 38F, 38G
(random plaintext)

