Report on the Block Cipher Modes of Operation in the NIST SP 800-38 Series

Nicky Mouha Morris Dworkin

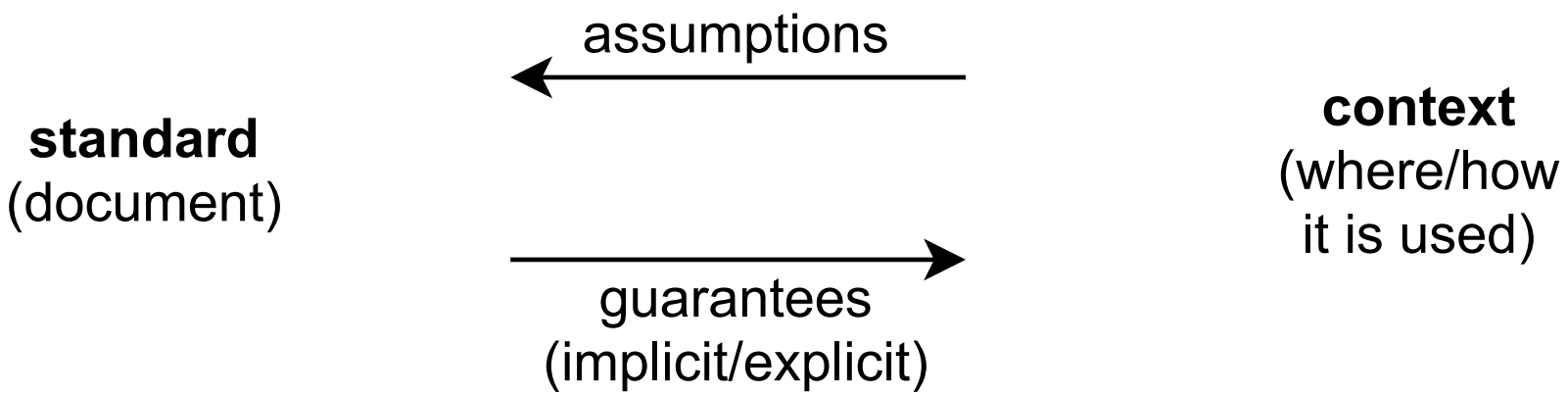
NIST Workshop on Block Cipher Modes of Operation 2023
Tuesday, October 3, 2023

Standards Review

- NIST commitment:
  - Periodical review of standards
- First review: AES (FIPS 197)
  - NISTIR 8319: Review of the AES (July 2021)
- Next: Modes of operation (SP 800-38 Series)
  - Draft NISTIR 8459: Modes Report (March 2023)

Methodology

- Where is the standard used?
- What security properties are required there?
- Does failure of security properties lead to **attacks**?



Security Models

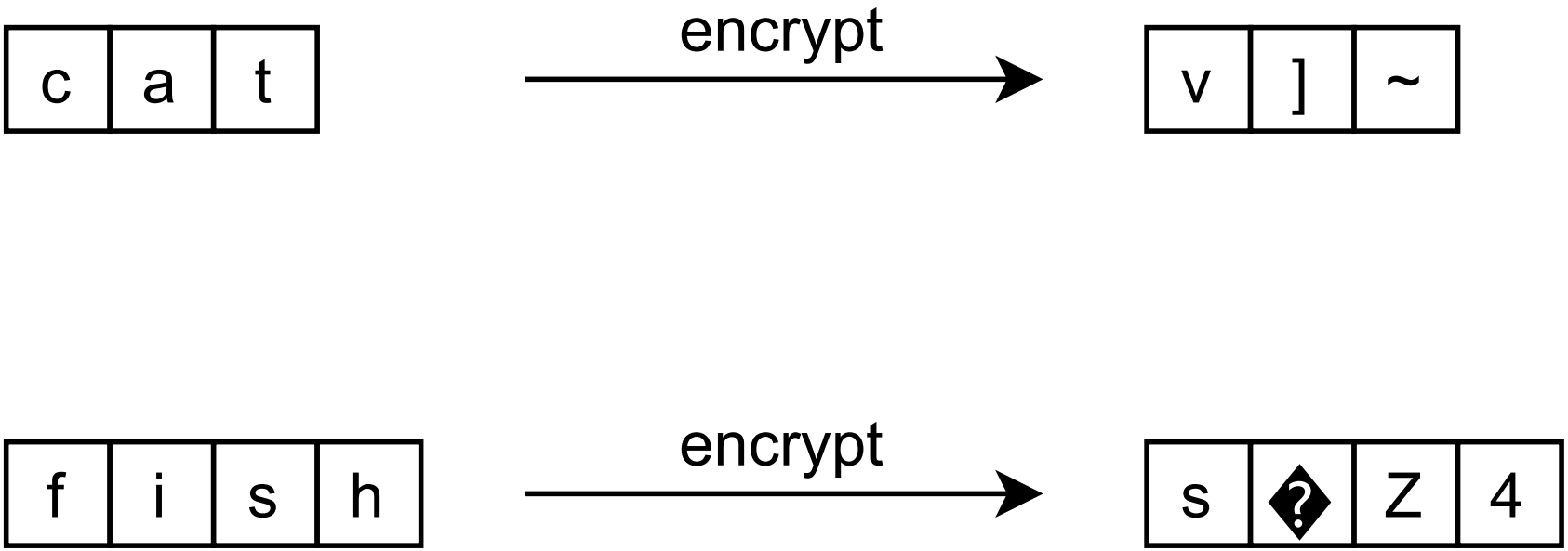
- E.g., known/chosen plaintext attacks, but...
  - Purpose of encryption if attacker already knows the plaintext?
  - How can an attacker choose the plaintext?

Security Models

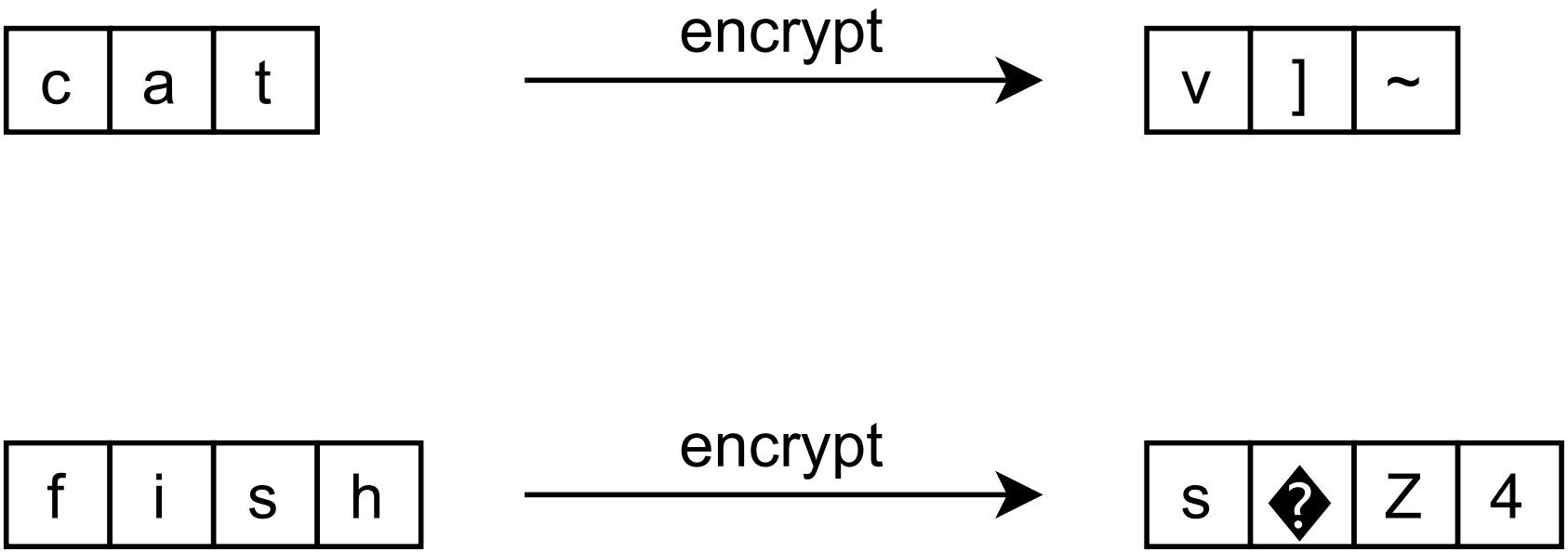
- E.g., known/chosen plaintext attacks, but...
  - Purpose of encryption if attacker already knows the plaintext?
  - How can an attacker choose the plaintext?

- Again, focus on **attacks**...
  - Exhaustive search is infeasible, but...
    ...side-channel attacks recover key in minutes?
  - Block cipher secure against related-key attacks, or...
    ...disallow generating keys with known relations?
  - Vulnerabilities (CVE numbers)?

Plaintext Length



Plaintext Length

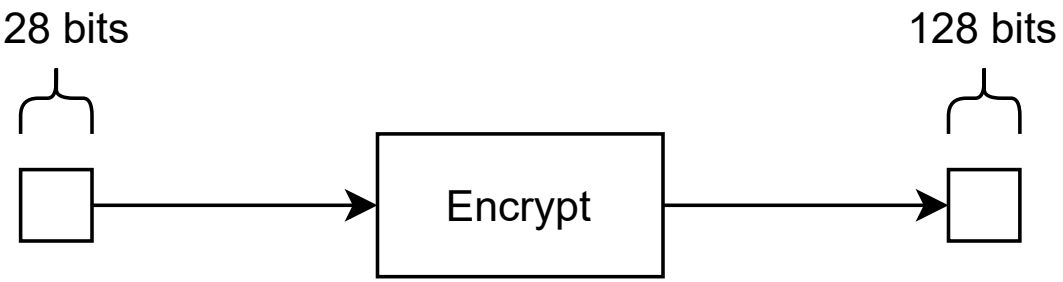


- Guessing attack $\rightarrow$ minimum plaintext size for FF1/FF3 (38G)

Why Modes? Limitations of AES

- AES

  (all keys sizes)



Domain Extension

- CTR, OFB

  ($k \geq 0$)

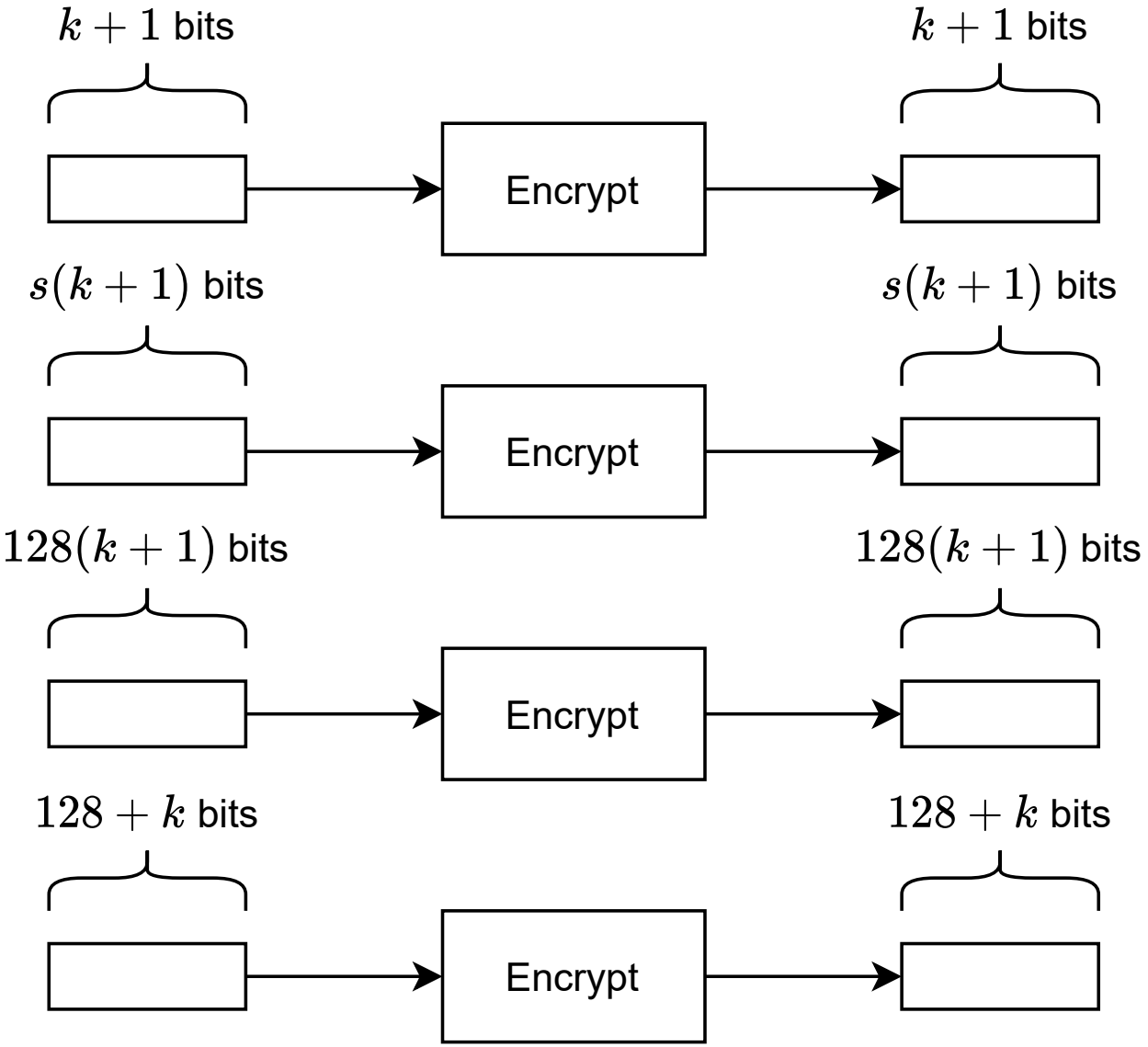
- CFB

  (s = size of segment)

- ECB, CBC

- CBC-CS

  (CS1, CS2, CS3)



Bit Flips (Encryption, Same IV)

- AES

  (best achievable)

- ECB, XTS

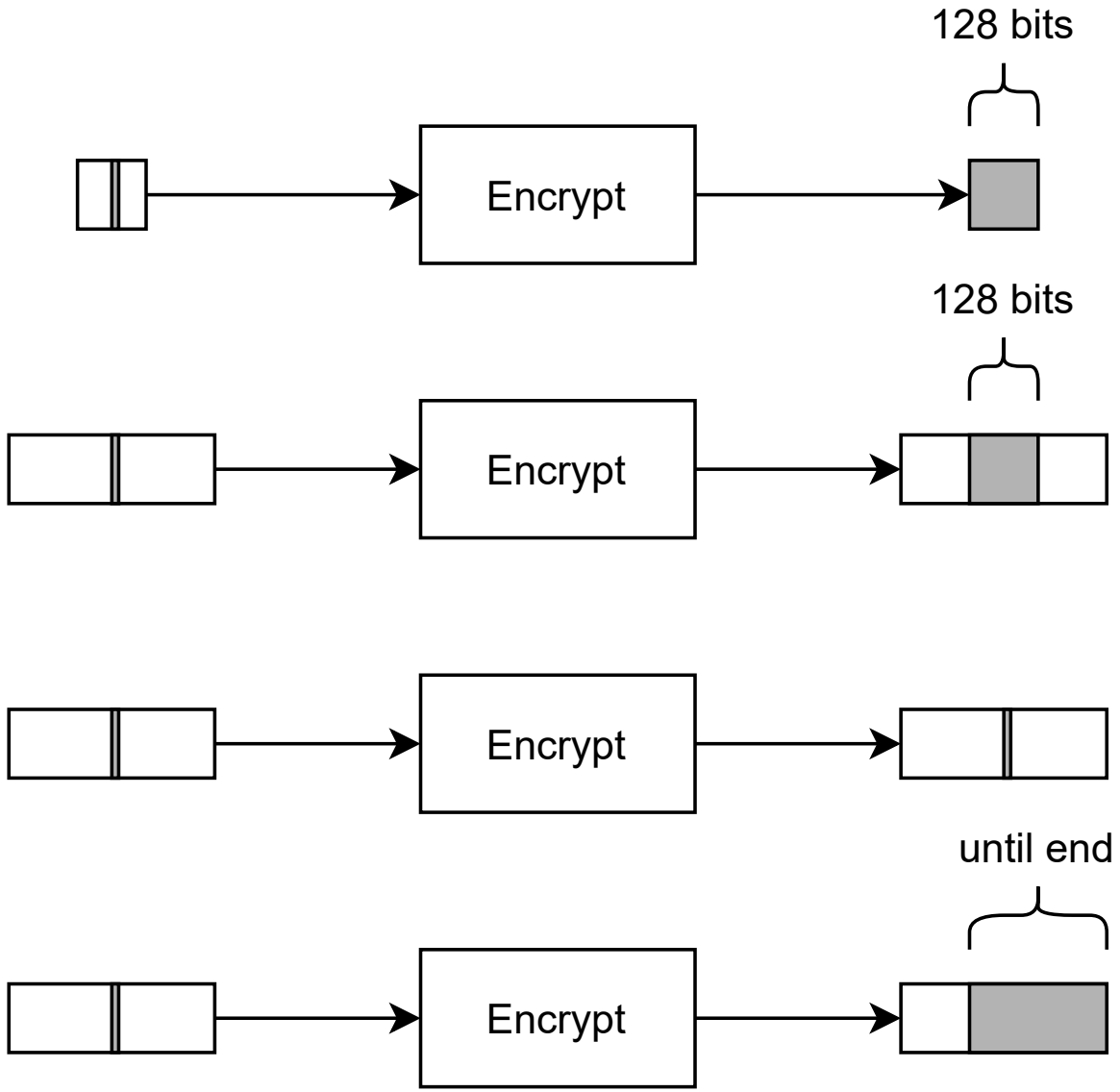
  (corresponding block)

- CTR, OFB

  (corresponding bit)

- CBC

  (best for single-pass)



Bit Flips (Decryption, No MAC)

- AES

  (best achievable)

- ECB, XTS

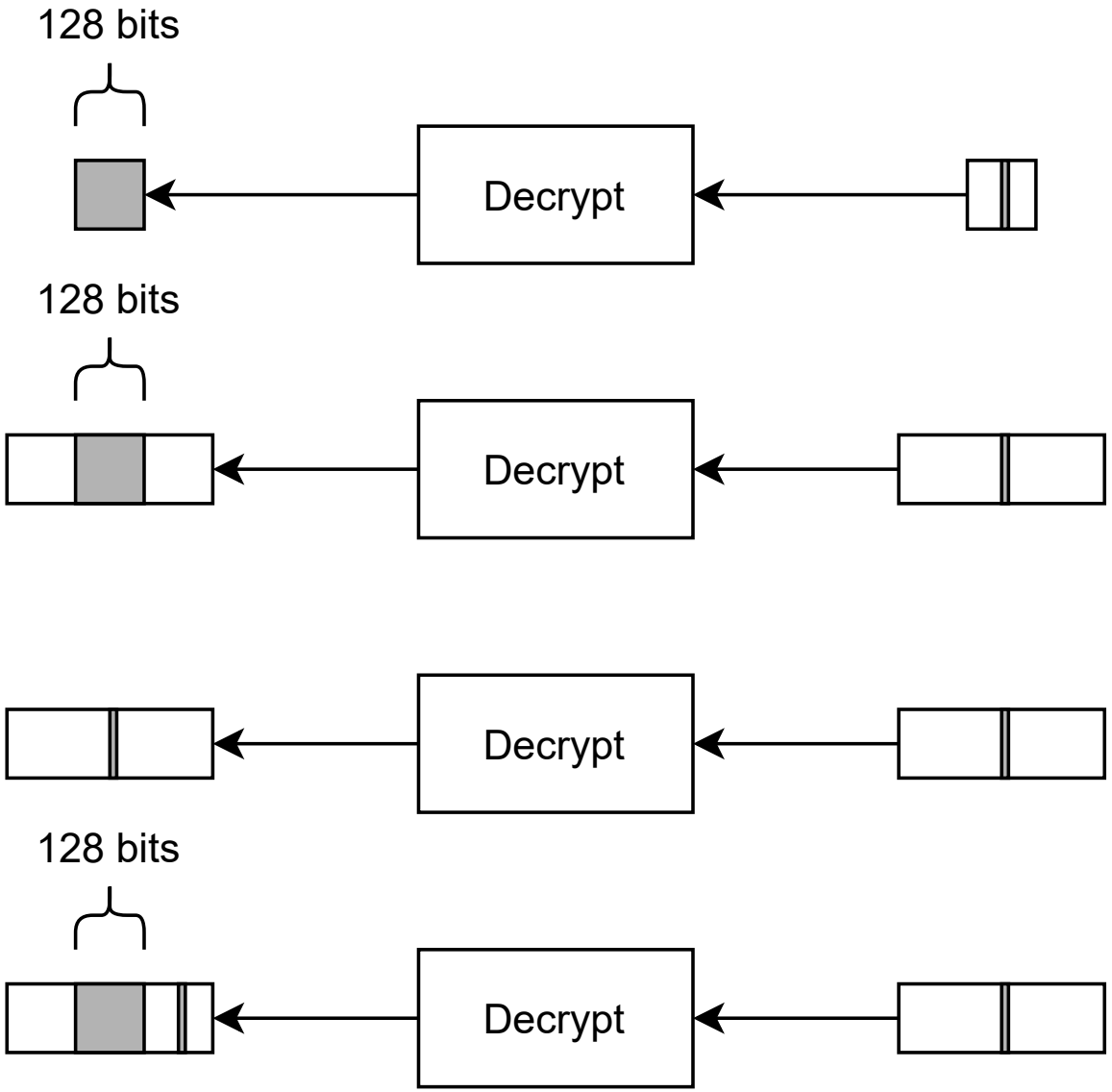
  (corresponding block)

- CTR, OFB

  (corresponding bit)

- CBC

  (one block + one bit)



Best Achievable

- AES

  (random ciphertext)

- AES

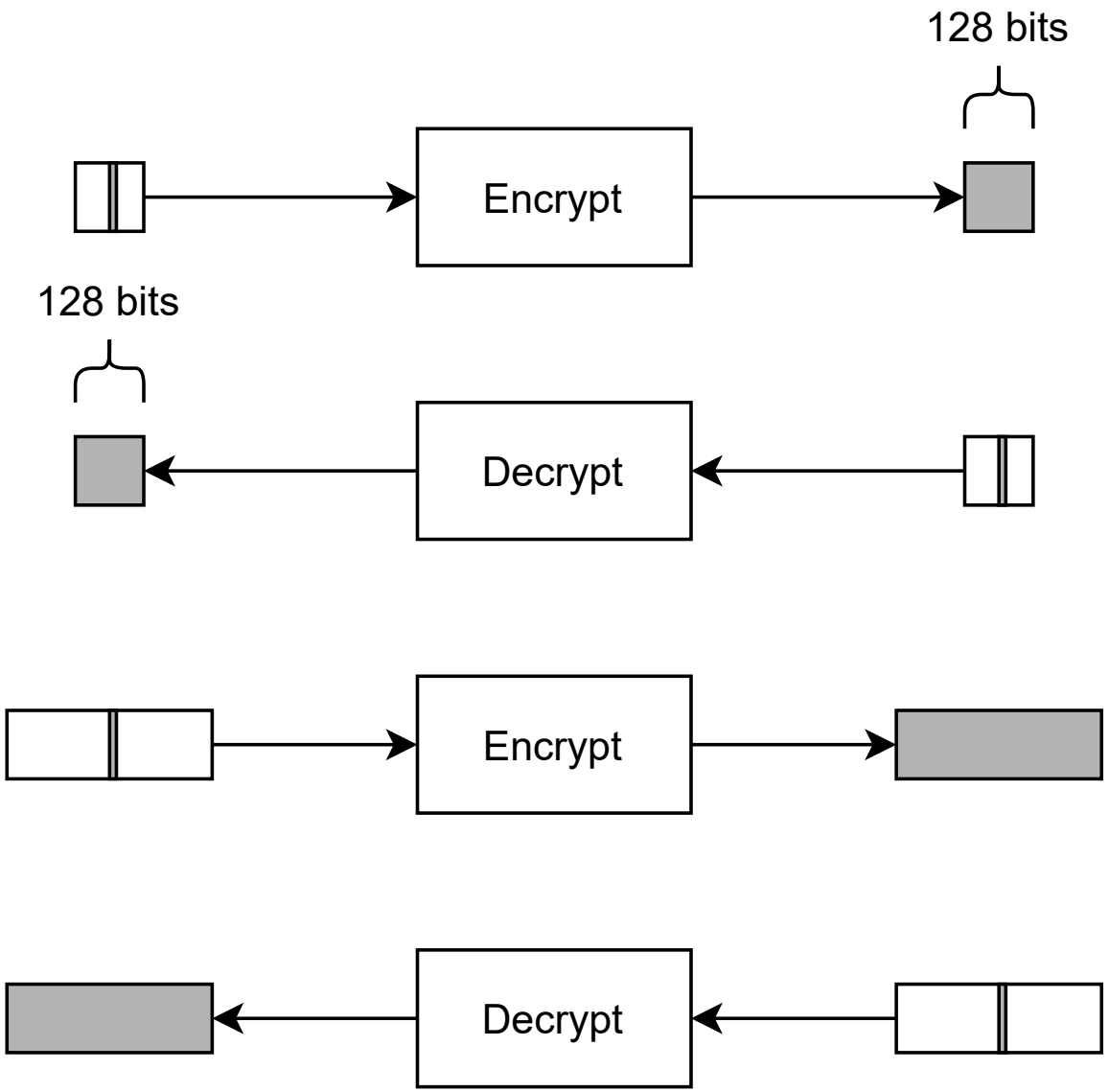
  (random plaintext)

- 38F, 38G

  (random ciphertext)

- 38F, 38G

  (random plaintext)



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

Information Security

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

Information Security

- 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?"*

Information Security

- 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?"*

Information Security

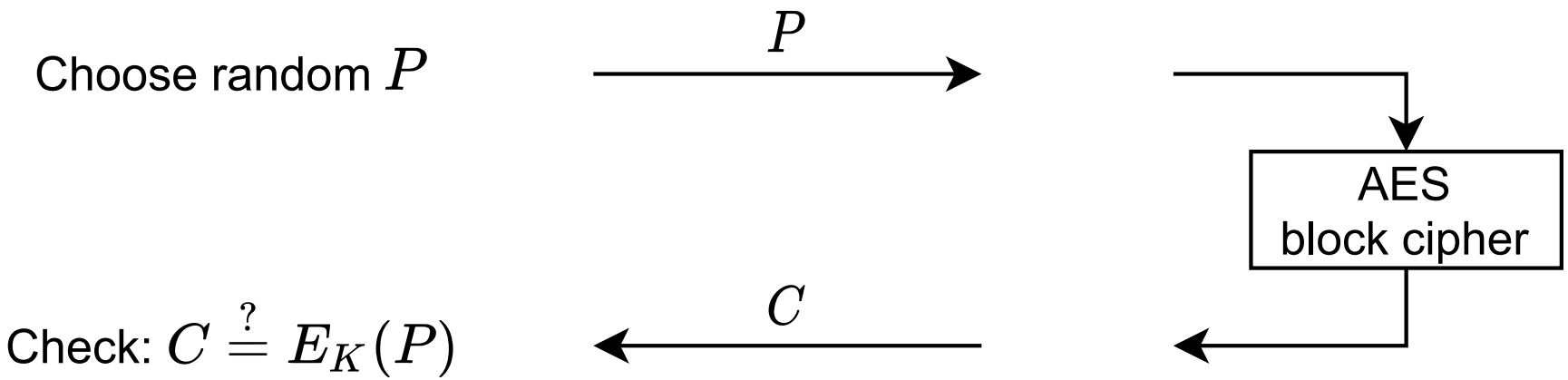
- FISMA defines "information security" as:
  - Confidentiality
  - Integrity (incl. nonrepudiation and authenticity)
  - Availability
- We need two additional terms:
  - Semantic security: *"Can the attacker learn something by having the ciphertext that is not already known about the plaintext?"*
  -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

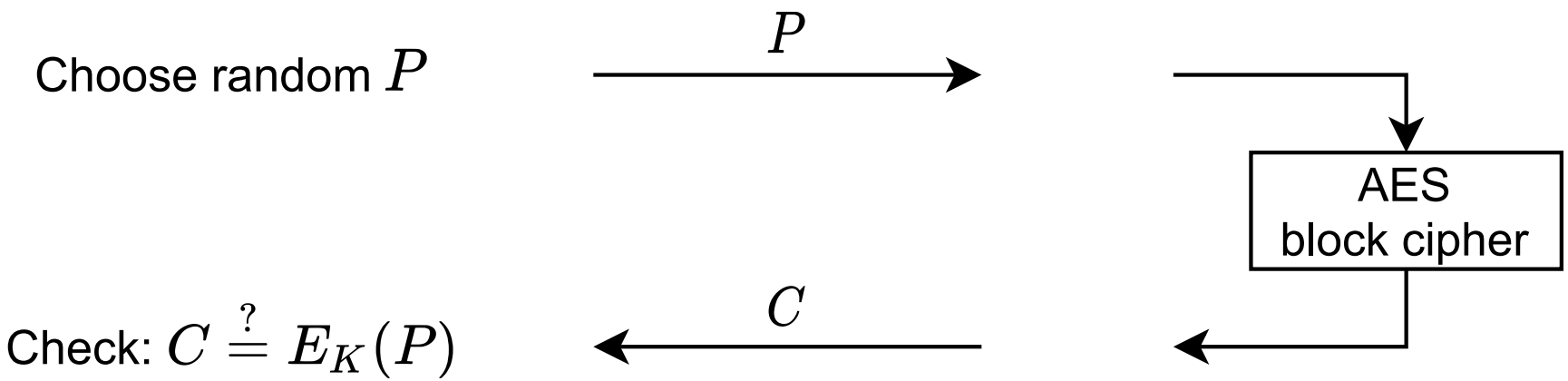
challenge

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!)

Notions Explained

- 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!

Notions Explained

- 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)

Notions Explained

- 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)

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 $\rightarrow$ 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?

New Encryption Primitive?

- "Conventional" Authenticated Encryption
  - Use GCM or CCM
  - Secure in commonly-used protocols such as TLS

New Encryption Primitive?

- "Conventional" Authenticated Encryption
  - Use GCM or CCM
  - Secure in commonly-used protocols such as TLS
- Other Encryption Applications?
  - Low-latency encryption?
  - Lightweight encryption?
  - SHA-3-based encryption?
  - Insecure uses of CBC, GCM, CCM?
  - Other?

New Encryption Primitive?

- "Conventional" Authenticated Encryption
  - Use GCM or CCM
  - Secure in commonly-used protocols such as TLS
- Other Encryption Applications?
  - ~~Low-latency encryption?~~
  - ~~Lightweight encryption?~~
  - ~~SHA-3-based encryption?~~
  - Insecure uses of CBC, GCM, CCM? ← This talk!
  - ~~Other?~~

New Encryption Primitive?

- "Conventional" Authenticated Encryption
  - Use GCM or CCM
  - Secure in commonly-used protocols such as TLS
- Other Encryption Applications?
  - ~~Low-latency encryption?~~
  - ~~Lightweight encryption?~~
  - ~~SHA-3-based encryption?~~
  - Insecure uses of CBC, GCM, CCM? $\leftarrow$ This talk!
  - ~~Other?~~
- Why?
  - IV reuse, short or no tags, no key commitment, release of unverified plaintext,...
  - Many applications: disk encryption, packet encryption, message franking,...