CS171: Cryptography

Lecture 6

Sanjam Garg

All Photos are by Unknown Author and are licensed under CC BY-SA

Plan for Today

- Towards Practical Constructions of Encryption
- Chosen Ciphertext Attacks and Security
- New Proof Technique: Hybrid Arguments

Constructions are heuristic

Practical Constructions

Stream-Cipher (aka PRG with arbitrary output length) based

Block-cipher (aka PRF/PRP) based

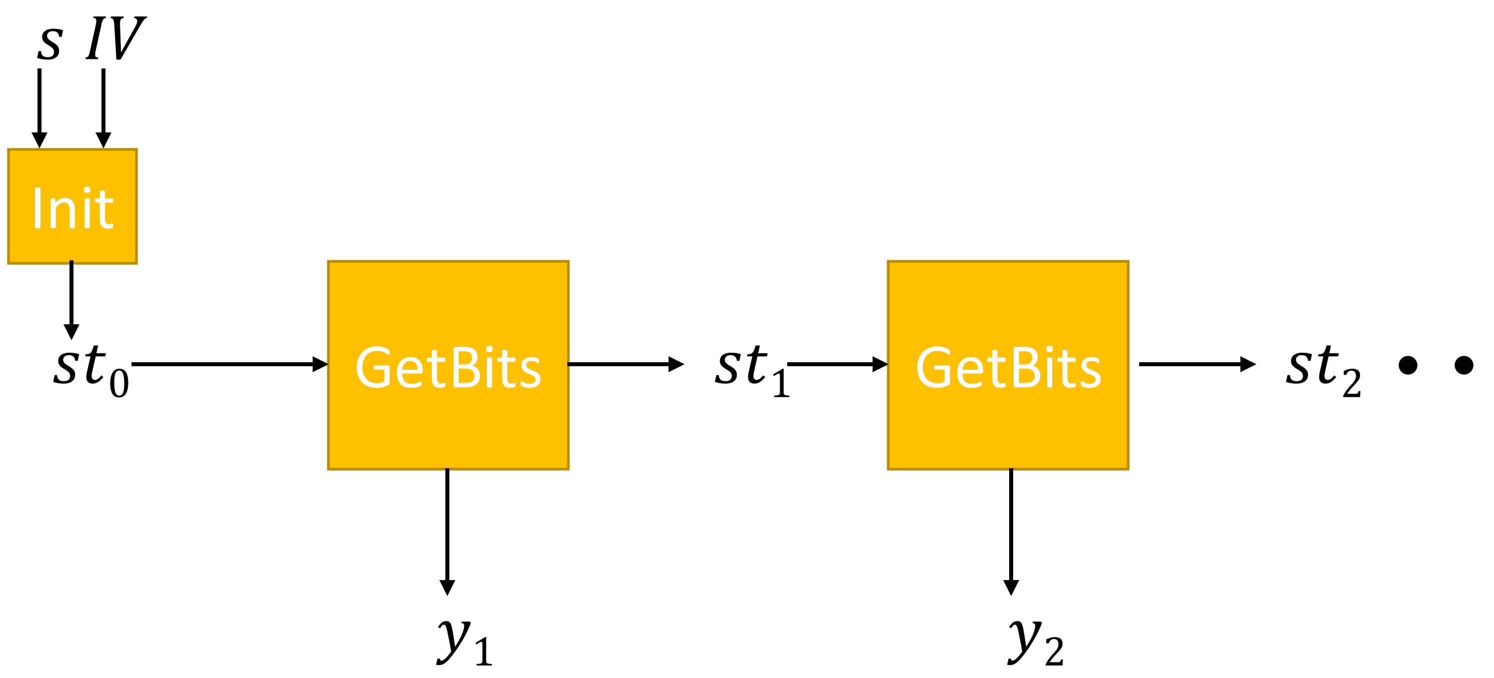
Stream Ciphers

- Init algorithm
  - Input: a key and an *optional* initialization vector (IV)
  - Output: initial state

- GetBits algorithm
  - Input: the current state
  - Output: next bit and updated state
  - Multiple executions allow for generation of desired number of bits
    - Enables encryption messages of different lengths

Stream Ciphers

- Use (Init, GetBits) to generate the desired number of output bits from the seed

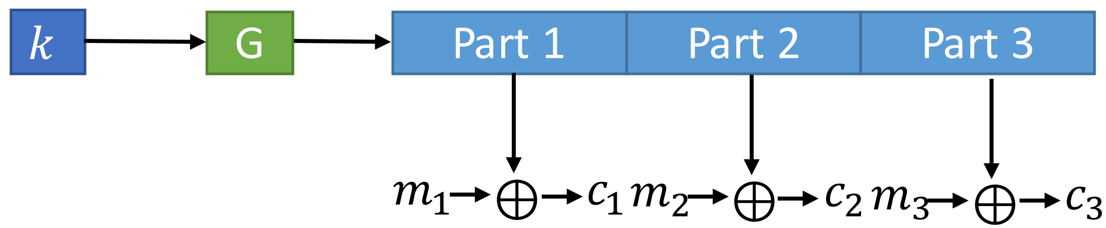


Security

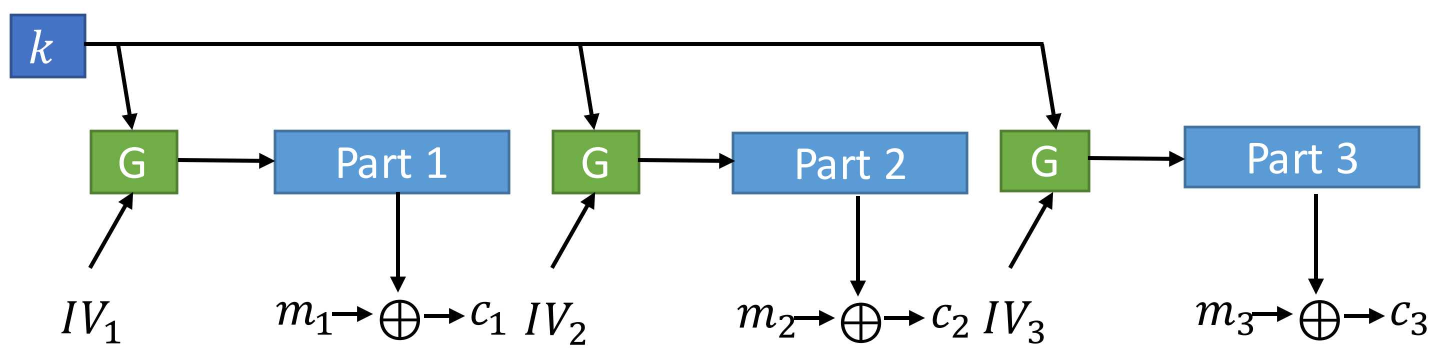
- Without IV: For a uniform key, output of GetBits should a pseudorandom stream of bits
- With IV: : For a uniform key, and uniform IVs (a*vailable to the attacker*), output of GetBits should be pseudorandom streams of bits (weak PRF)

Stream-Cipher Mode of Operation

Synchronized Mode



Unsynchronized Mode



- G is used as a weak PRF whose output is expanded.
- Communicate IV as well.

Pseudorandom Permutations/Block Ciphers

- What is a permutation?

  a bijective function $f: \{0,1\}^n \to \{0,1\}^n$

  - $\forall\, x, x' f(x) \neq f(x')$

- Let $Perm_n$ be the set of all permutations from n-bits to n-bits.
  - What is the size?
  - $2^n!$

Pseudorandom Permutations/Block Ciphers

Let $F: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be an efficient, length-preserving, keyed permutation. F is a PRP if for all PPT distinguishers D, there is a negligible function $negl(\cdot)$ such that:

$$\left|\Pr\left[D^{F_k(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot)}(1^n) = 1\right]\right| \leq negl(n)$$

where $k \leftarrow U_n$ and $f \leftarrow Perm_n$.

Every PRP is also a PRF!

Pseudorandom Permutations/Block Ciphers

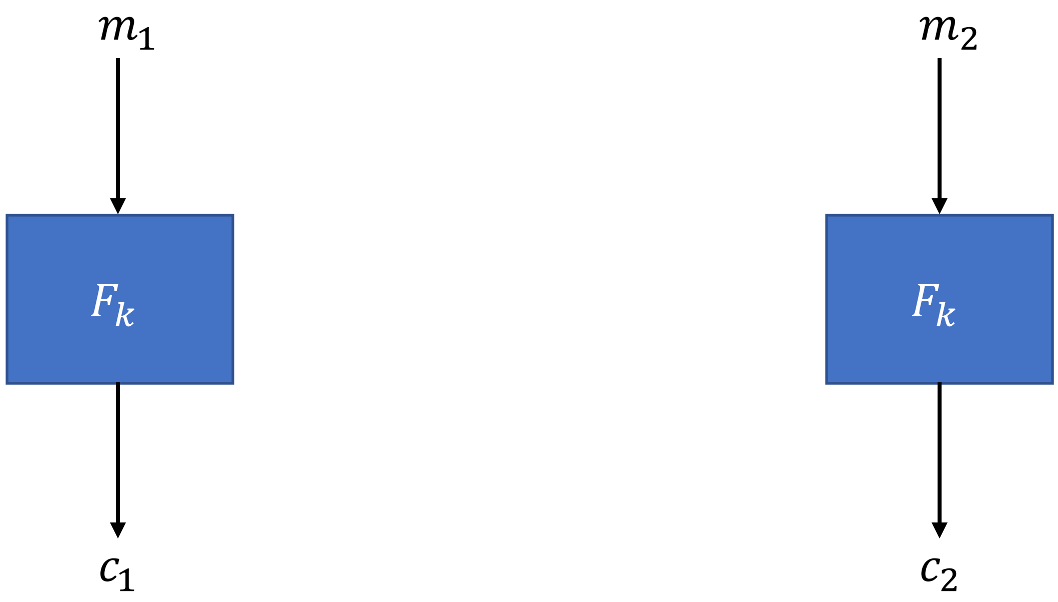
Both computing and inverting!

Let F: $\{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be an efficient, length-preserving, keyed permutation. F is a (strong) PRP if for all PPT distinguishers D, there is a negligible function $negl(\cdot)$ such that:

$$\left|\Pr\left[D^{F_k(\cdot),F_k^{-1}(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot),f^{-1}(\cdot)}(1^n) = 1\right]\right| \leq negl(n)$$

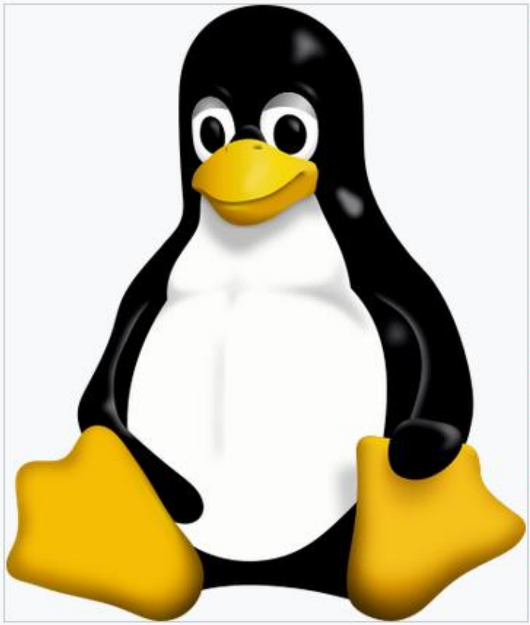
where $k \leftarrow U_n$ and $f \leftarrow Perm_n$.

Electronic Code Book (Insecure)

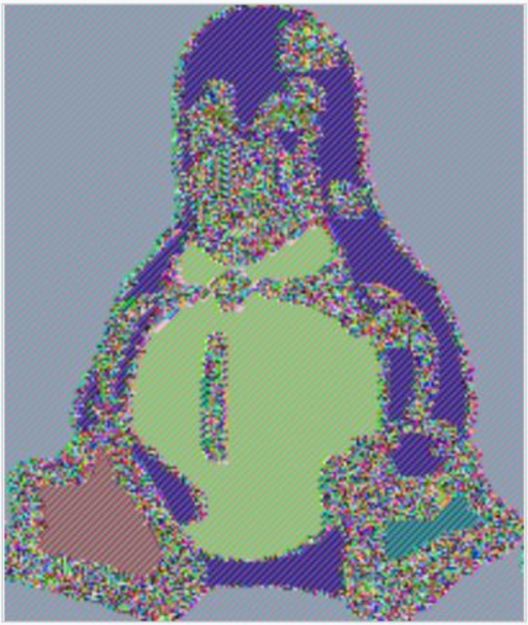


- Decryption done using F_k^{-1}
- Not CPA secure

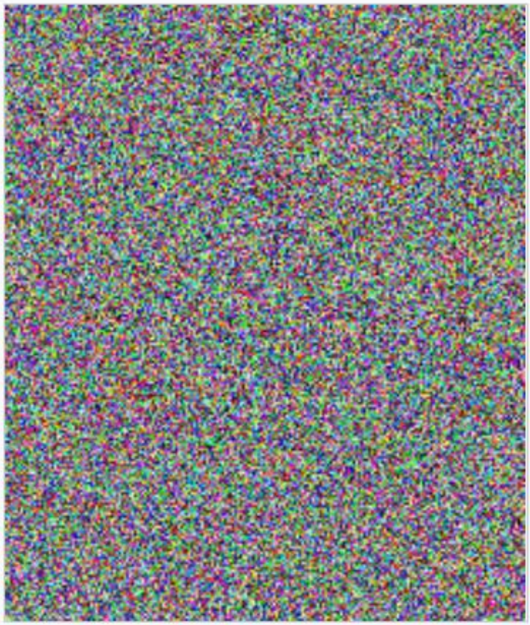
Visibly Insecure



Original image



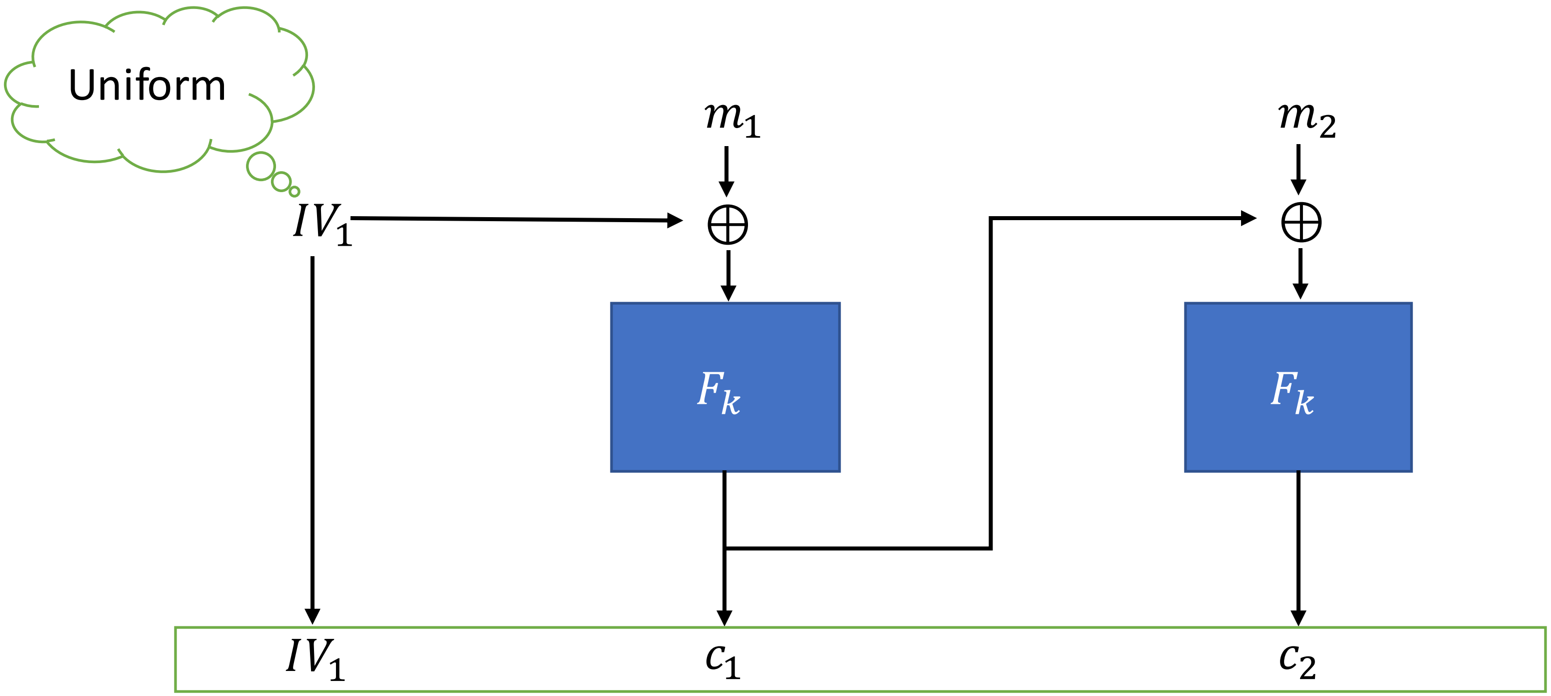
Using ECB allows patterns to be easily discerned



Modes other than ECB result in pseudo-randomness

Source: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

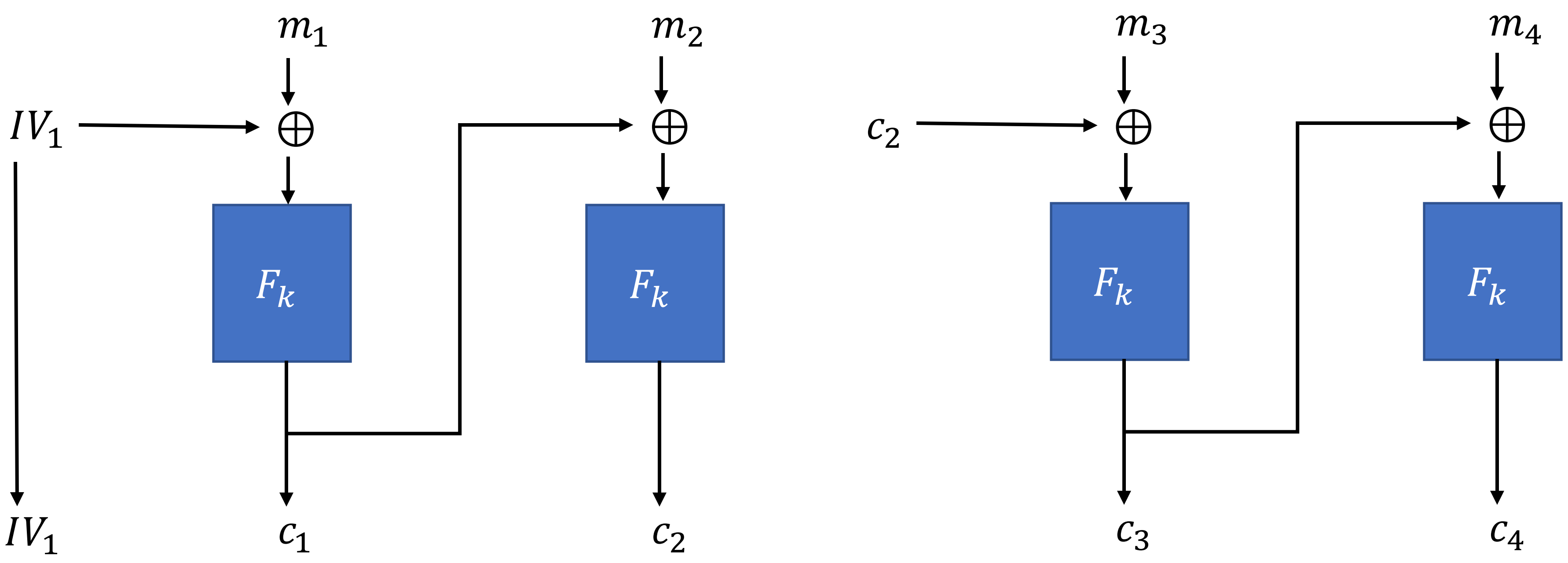
Cipher Block Chaining (CBC) Mode



Attack if IV_1 is not uniform (but distinct across multiple ciphers). E.g. IV is a counter.

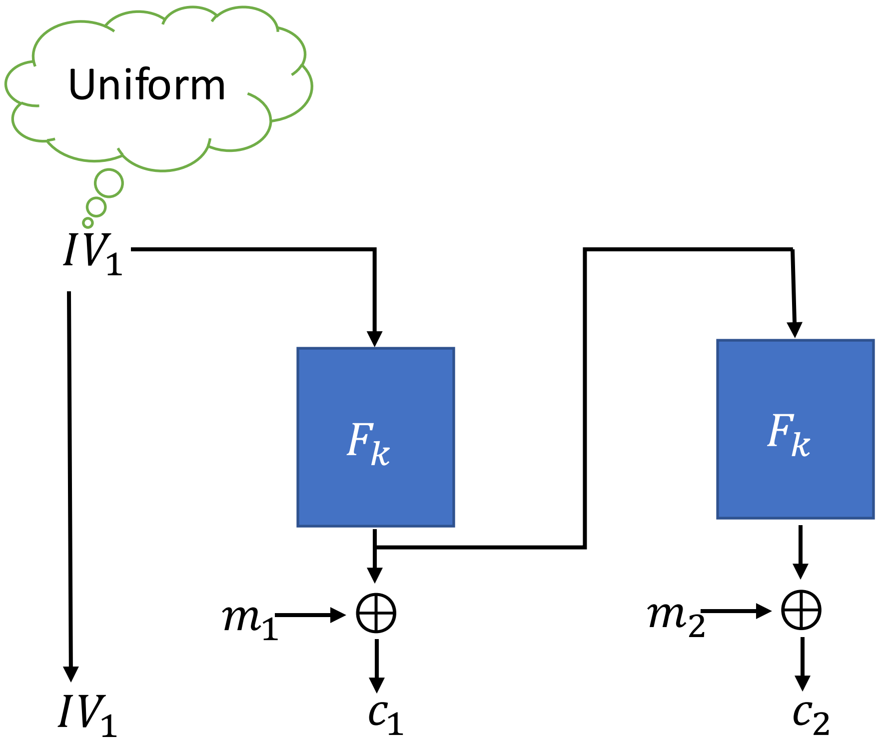
$$m_1' = IV_1' \oplus IV_1 \oplus m_1$$

Is Chaining in CBC Mode secure?



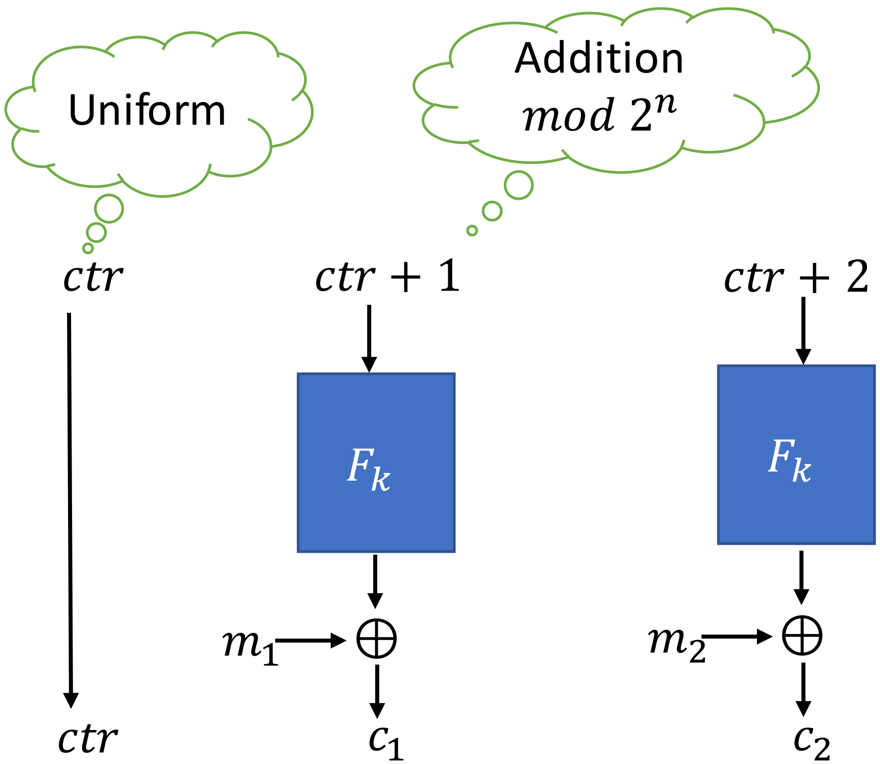
Not CPA secure! Adversary could use the following challenge messages for m_3 : $IV_1 \oplus c_2 \oplus m_1$ and 0^ℓ.

Output Feedback (OFB) Mode



- No need of F_k^{-1}
- Positive: All F_k can be made before the message is known
- Negative: Encryption and Decryption is sequential

Counter (CTR) Mode

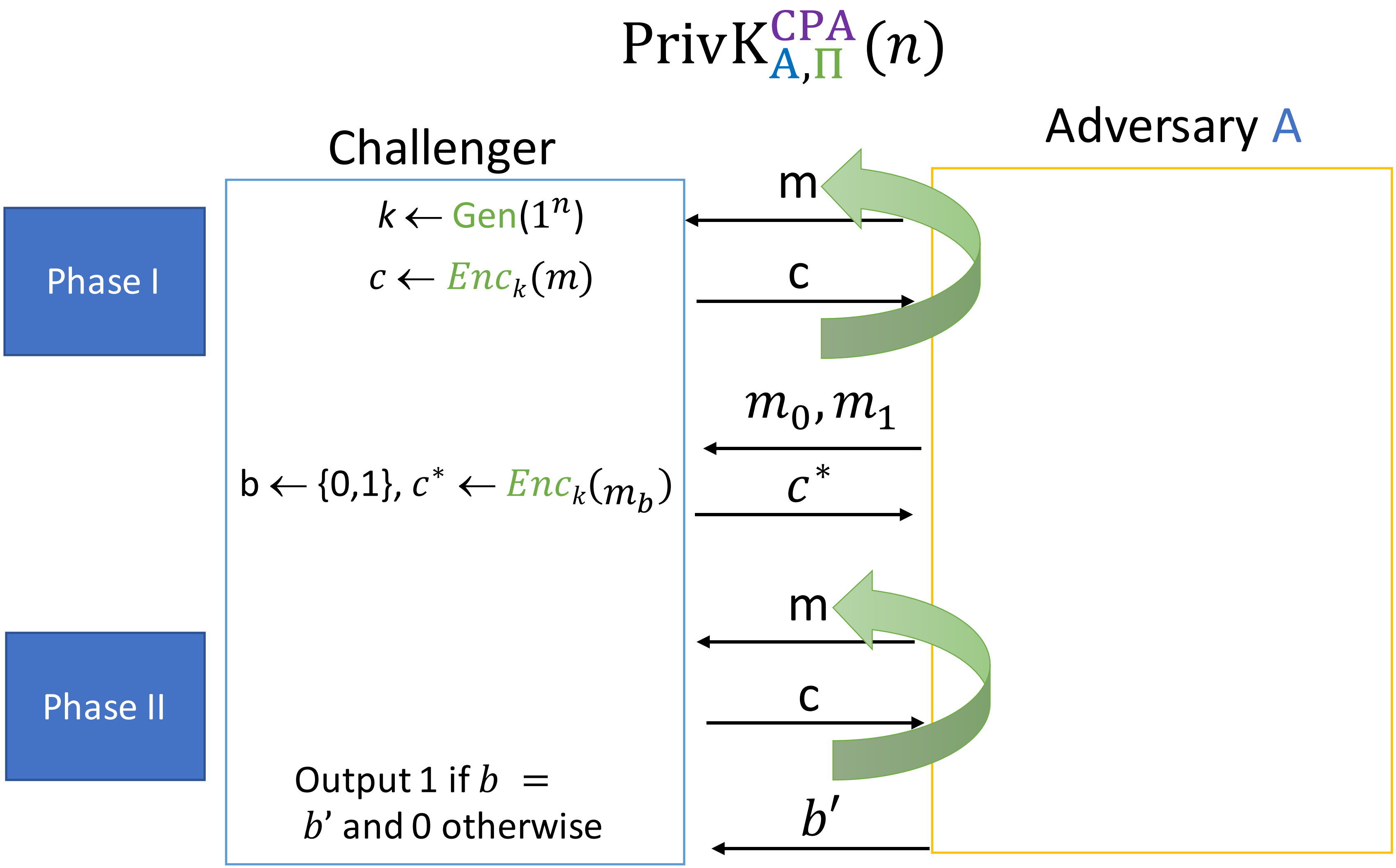


- Again no need of F_k^{-1}
- Positive: Easy to parallelize
- Possible to decrypt only the i-th block

Can be proved to be CPA secure (DIY). Argument similar to the CPA security of PRF based OTP. Now we need the guarantee that the values $(ctr^*, \ldots ctr^* + t^*)$ are not used in any other adversarial queries.

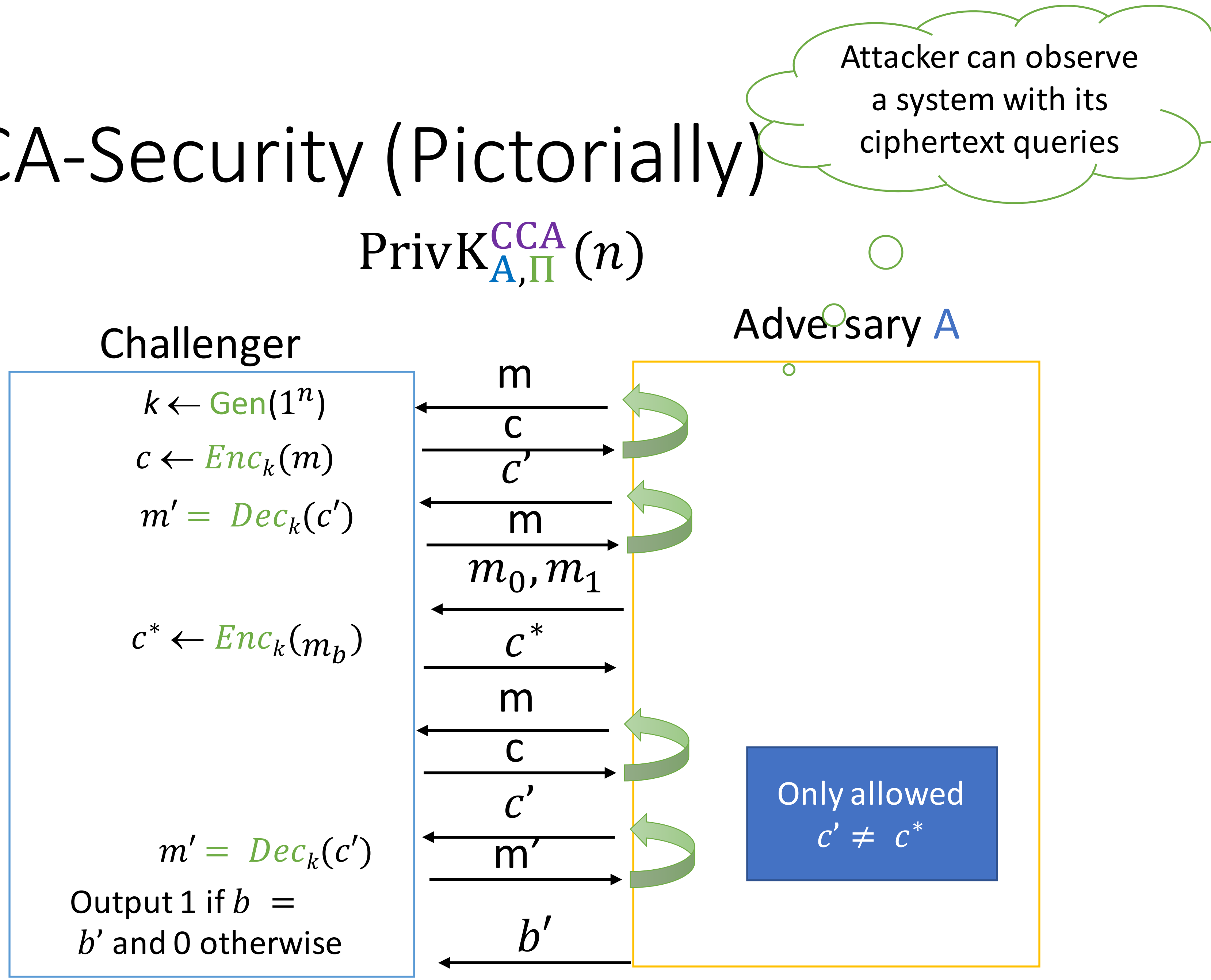
CCA Security

CPA-Security (Pictorially)



CCA-Security (Pictorially)

$\text{PrivK}^{\text{CCA}}_{A,\Pi}(n)$



Is PRF based OTP CCA secure?

Let F be a PRF: $\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$.

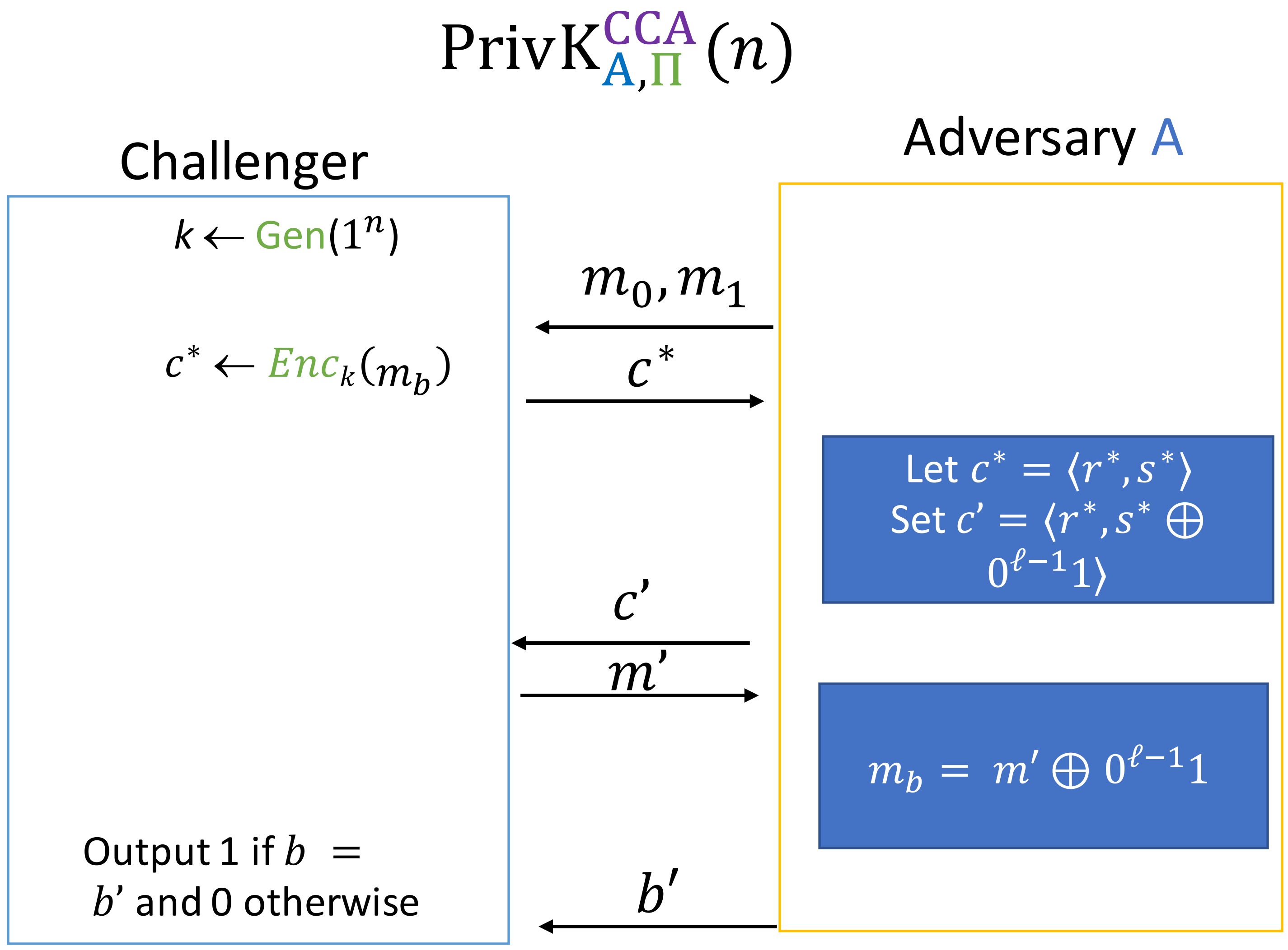
- $Gen(1^n)$: Choose uniform $k \in \{0,1\}^n$ and output it as the key
- $Enc_k(m)$: On input a message $m \in \{0,1\}^n$, sample $r \leftarrow U_n$ output the ciphertext c as

$$c := \langle r, F_k(r) \oplus m \rangle$$

- Dec$_k(c)$: On input a ciphertext $c = \langle r, s \rangle$ output the message

$$m := F_k(r) \oplus s$$

No! CCA Attack



New proof strategy:
hybrid arguments

CPA-Security => Mult-Security

CPA-Security => Mult-Security

$\mathrm{PrivK}_{A,\Pi}^{\mathrm{CPA}}(n)$

1. Sample $k \leftarrow \mathsf{Gen}(1^n)$, $A^{Enc_k(\cdot)}$ outputs $m_0, m_1 \in \{0,1\}^*, |m_0| = |m_1|$.
2. $\mathrm{b} \leftarrow \{0,1\}, c \leftarrow Enc_k(m_b)$
3. c is given to $A^{Enc_k(\cdot)}$
4. $A^{Enc_k(\cdot)}$ output b'
5. Output 1 if $b = b'$ and 0 otherwise

$\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult}}(n)$

1. A for $i \in \{1 \dots t\}$ outputs $m_{0,i}, m_{1,i} \in \{0,1\}^*, |m_{0,i}| = |m_{1,i}|$.
2. $\mathrm{b} \leftarrow \{0,1\}, k \leftarrow \mathsf{Gen}(1^n), c_i \leftarrow Enc_k(m_{b,i})$
3. $c_1 \dots c_t$ is given to A
4. A output b'
5. Output 1 if $b = b'$ and 0 otherwise

Step 1: Assume an attacker

$\Pr\left[\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult},0} = 1\right] \geq \frac{1}{2} + \epsilon$

$\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult}}(n)$

1. A for $i \in \{1 \ldots t\}$ outputs $m_{0,i}, m_{1,i} \in \{0,1\}^*, |m_{0,i}| = |m_{1,i}|$.
2. $\mathrm{b} \leftarrow \{0,1\}, k \leftarrow \mathrm{Gen}(1^n)$, $c_i \leftarrow Enc_k(m_{b,i})$
3. $c_1 \ldots c_t$ is given to A
4. A output b'
5. Output 1 if $b = b'$ and 0 otherwise

$\exists$ PPT A it holds that:

$$\Pr\left[\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult}} = 1\right] \geq \frac{1}{2} + \epsilon$$

$\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult,j}}(n)$ $j \in \{0, \ldots t\}$

…Same as $\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult}}$

$i > j$: $c_i \leftarrow Enc_k(m_{b,i})$

$i \leq j$: $c_i \leftarrow Enc_k(0^{|m_{b,i}|})$

…Same as $\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult}}$

Step 2: Hybrid Steps

$$\delta_i = \Pr\left[\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult},i} = 1\right] - \Pr\left[\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult},i-1} = 1\right]$$

$m_{b,1}$	$0^{\lvert m_{b,1}\rvert}$	$0^{\lvert m_{b,1}\rvert}$
$m_{b,2}$	$m_{b,2}$	$0^{\lvert m_{b,2}\rvert}$
$m_{b,3}$	$m_{b,3}$	$0^{\lvert m_{b,3}\rvert}$
⋮	⋮	⋮
$m_{b,t}$	$m_{b,t}$	$0^{\lvert m_{b,t}\rvert}$

δ_1 δ_2 δ_{t-1}

$\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult},0}(n)$ $\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult},1}(n)$ $\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult},t}(n)$

$$\Pr\left[\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult},0} = 1\right] \geq \frac{1}{2} + \epsilon$$

Why?

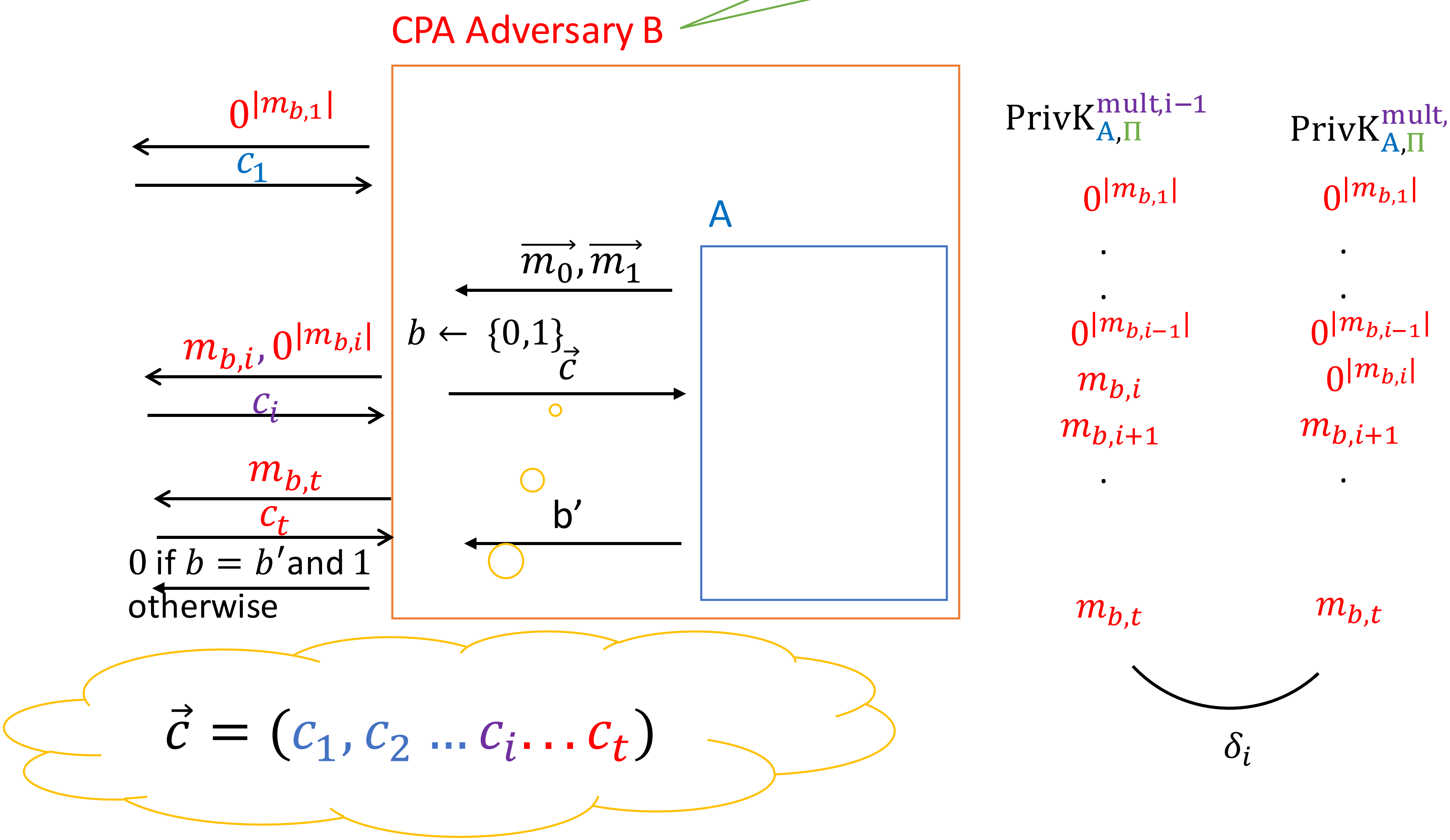
Claim: $\Pr\left[\mathrm{PrivK}_{A,\Pi}^{\mathrm{mult},t} = 1\right] = \frac{1}{2}$

Step 3: Arguing for every 'hybrid pair'

- $|\Pr[\mathrm{PrivK}^{\mathrm{mult},0}_{\mathrm{A},\Pi} = 1]$ - $\Pr[\mathrm{PrivK}^{\mathrm{mult},\mathrm{t}}_{\mathrm{A},\Pi} = 1]| =$ $\left|\sum_{i=1}^{t-1} \delta_i\right| \geq \epsilon$
- We will argue that $\forall\, i$ we have that δ_i is $negl(n)$.
- This would be a contradiction.
- Say for some i, $|\Pr[\mathrm{PrivK}^{\mathrm{mult},\mathrm{i}}_{\mathrm{A},\Pi} = 1]$ - $\Pr[\mathrm{PrivK}^{\mathrm{mult},\mathrm{i}-1}_{\mathrm{A},\Pi} = 1]| = \delta_i$ is non-negligible.
- Use this A that distinguishes $\mathrm{PrivK}^{\mathrm{mult},\mathrm{i}}_{\mathrm{A},\Pi}$ and $\mathrm{PrivK}^{\mathrm{mult},\mathrm{i}-1}_{\mathrm{A},\Pi}$ to break CPA security.

Step 4: Reduction

$$\left|\Pr[\mathrm{PrivK}^{\mathrm{CPA}}_{\mathrm{B},\Pi}=1]-\frac{1}{2}\right|\geq\delta'(n)$$



Step 5: Probability Calculation

- Note: Pr[b=b'|c_i is an encryption $m_{b,i}$]= $\Pr\left[\mathrm{PrivK}_{\mathrm{A},\Pi}^{\mathrm{mult,i-1}}=1\right]$
- Note: Pr[b=b'|c_i is an encryption $0^{|m_{b,i}|}$]= $\Pr\left[\mathrm{PrivK}_{\mathrm{A},\Pi}^{\mathrm{mult,i}}=1\right]$
- Say $\Pr\left[\mathrm{PrivK}_{\mathrm{A},\Pi}^{\mathrm{mult,i}}=1\right]=p$
- Then: $\Pr\left[\mathrm{PrivK}_{\mathrm{A},\Pi}^{\mathrm{mult,i-1}}=1\right]=p+\delta_i$
- Compute: Pr[B's guess is correct] $=\frac{1}{2}(p+\delta_i)+\frac{1}{2}\cdot(1-p)=\frac{1}{2}+\frac{\delta_i}{2}$

Thank You!