CS 442
Introduction to Cryptography

Lecture 14: CPA Secure Encryption – II and Modes of Operation

Instructor: Aarushi Goel

Spring 2026

Agenda

* CPA-secure encryption from PRFs
* Proof of security
* Modes of Operation: Practical ways of encrypting long messages.

CPA Secure Encryption (Also called multi-message secure encryption)

Definition: A CPA-secure encryption scheme with message space $\mathcal{M}$, key space $\mathcal{K}$, ciphertext space $\mathcal{C}$, comprises of the following algorithms:

* $\text{KeyGen} \longrightarrow K$: This algorithm samples a key $K \in \mathcal{K}$.
* $\text{Enc}(K, m) \rightarrow c$: On input a key $K \in \mathcal{K}$ and a message $m \in \mathcal{M}$, it outputs ciphertext $c \in \mathcal{C}$.
* $\text{Dec}(K, c) \rightarrow m$: On input a key $K \in \mathcal{K}$ and a ciphertext $c \in \mathcal{C}$, it outputs message $m \in \mathcal{M}$.

These algorithms must satisfy the following:

→ Correctness: $\forall K \in \mathcal{K}$, $\forall m \in \mathcal{M}$, it holds that:

$$Pr[\text{Dec}(K, \text{Enc}(K, m)) = m] = 1$$

→ CPA-Security: For all PPT adversaries, there exists a negligible function $\nu(\cdot)$ such that the following holds in the game below:

$$Pr[b = b'] \leq \frac{1}{2} + \nu(|K|)$$

Adversary

Challenger

KeyGen → K

query polynomial no. of times { $m \rightarrow$, $\leftarrow c$ } Enc(K, .)

can include previously queried messages

$m_0, m_1 \in \mathcal{M}$ →

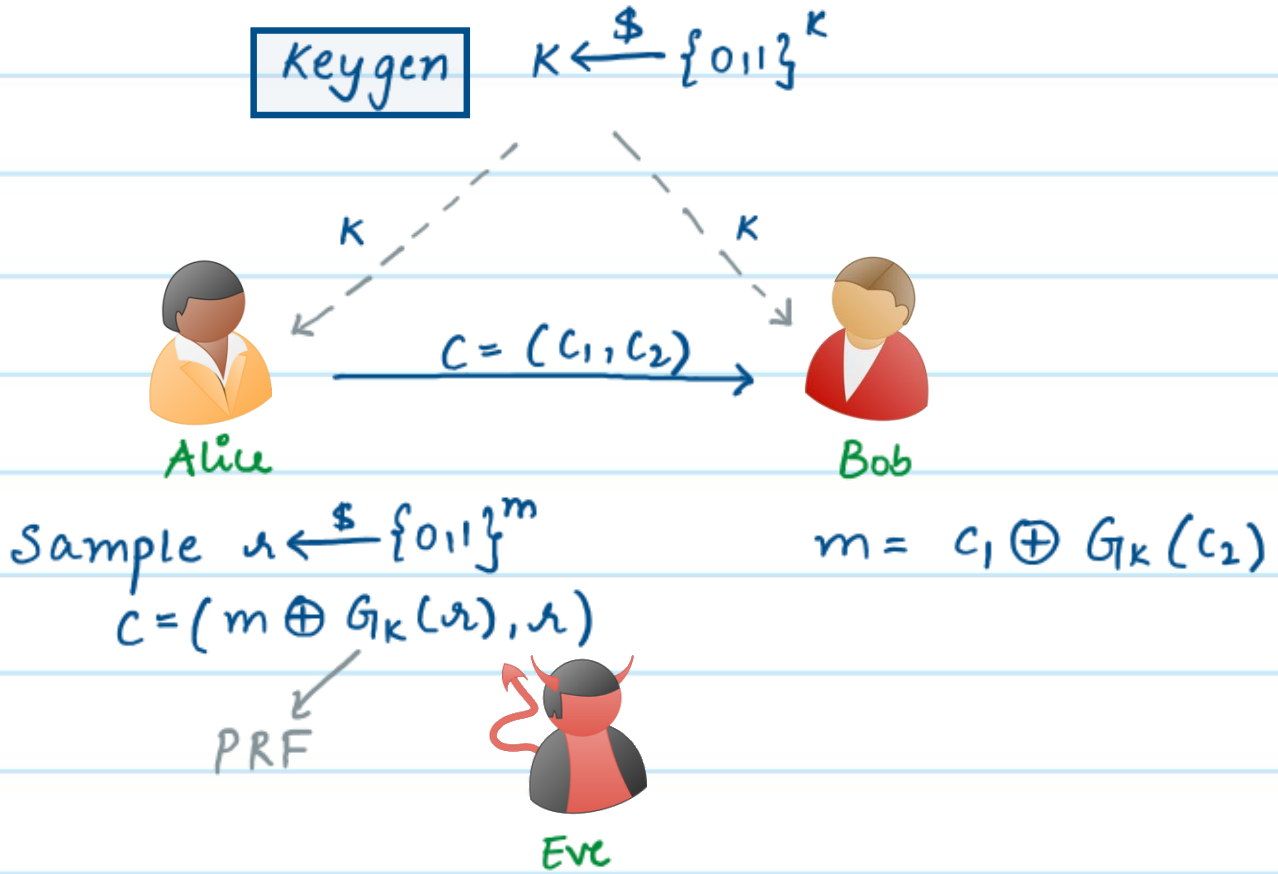
$\leftarrow c_b = Enc(K, m_b)$

$b \xleftarrow{\$} \{0,1\}$

query polynomial no. of times { $m \rightarrow$, $\leftarrow c$ } Enc(K, .)

$b' \rightarrow$

CPA Secure Encryption from PRFs



Proof of Security

Consider the following hybrids:

H_1: CPA-security game where the challenger chooses $b=0$.

H_2: Similar to H_1 except that the encryption algorithm uses a random function instead of a PRF

H_3: Similar to H_2 except that the encryption algorithm simply XORs a random value with the message

H_4: Similar to H_3 except that the challenger chooses $b=1$.

H_5: Similar to H_4 except that the encryption algorithm uses a random function

H_6: CPA-security game where the challenger chooses $b=1$.

Proof of Security

Consider the following hybrids:

H_1: CPA-security game where the challenger chooses $b=0$.

H_2: Similar to H_1 except that the encryption algorithm uses a random function instead of a PRF

H_3: Similar to H_2 except that the encryption algorithm simply XORs a random value with the message

H_4: Similar to H_3 except that the challenger chooses $b=1$.

H_5: Similar to H_4 except that the encryption algorithm uses a random function

H_6: CPA-security game where the challenger chooses $b=1$.

Indistinguishability between H_1 & H_2 follows from security of the PRF.

Proof of Security

Consider the following hybrids:

H_1: CPA-security game where the challenger chooses $b=0$.

H_2: Similar to H_1 except that the encryption algorithm uses a random function instead of a PRF

H_3: Similar to H_2 except that the encryption algorithm simply XORs a random value with the message

H_4: Similar to H_3 except that the challenger chooses $b=1$.

H_5: Similar to H_4 except that the encryption algorithm uses a random function

H_6: CPA-security game where the challenger chooses $b=1$.

H_2 and H_3 are identically distributed

Proof of Security

Consider the following hybrids:

H_1: CPA-security game where the challenger chooses $b=0$.

H_2: Similar to H_1 except that the encryption algorithm uses a random function instead of a PRF

H_3: Similar to H_2 except that the encryption algorithm simply XORs a random value with the message

H_4: Similar to H_3 except that the challenger chooses $b=1$.

H_5: Similar to H_4 except that the encryption algorithm uses a random function

H_6: CPA-security game where the challenger chooses $b=1$.

H_3 and H_4 are identically distributed (one-time pad security)

Proof of Security

Consider the following hybrids:

H_1: CPA-security game where the challenger chooses $b=0$.

H_2: Similar to H_1 except that the encryption algorithm uses a random function instead of a PRF

H_3: Similar to H_2 except that the encryption algorithm simply XORs a random value with the message

H_4: Similar to H_3 except that the challenger chooses $b=1$.

H_5: Similar to H_4 except that the encryption algorithm uses a random function

H_6: CPA-security game where the challenger chooses $b=1$.

H_5 and H_6 are identically distributed

Proof of Security

Consider the following hybrids:

H_1: CPA-security game where the challenger chooses $b=0$.

H_2: Similar to H_1 except that the encryption algorithm uses a random function instead of a PRF

H_3: Similar to H_2 except that the encryption algorithm simply XORs a random value with the message

H_4: Similar to H_3 except that the challenger chooses $b=1$.

H_5: Similar to H_4 except that the encryption algorithm uses a random function

H_6: CPA-security game where the challenger chooses $b=1$.

Indistinguishability between H_5 & H_6 follows from security of the PRF.

How to Build PRFs?

Two Approaches

Theoretical

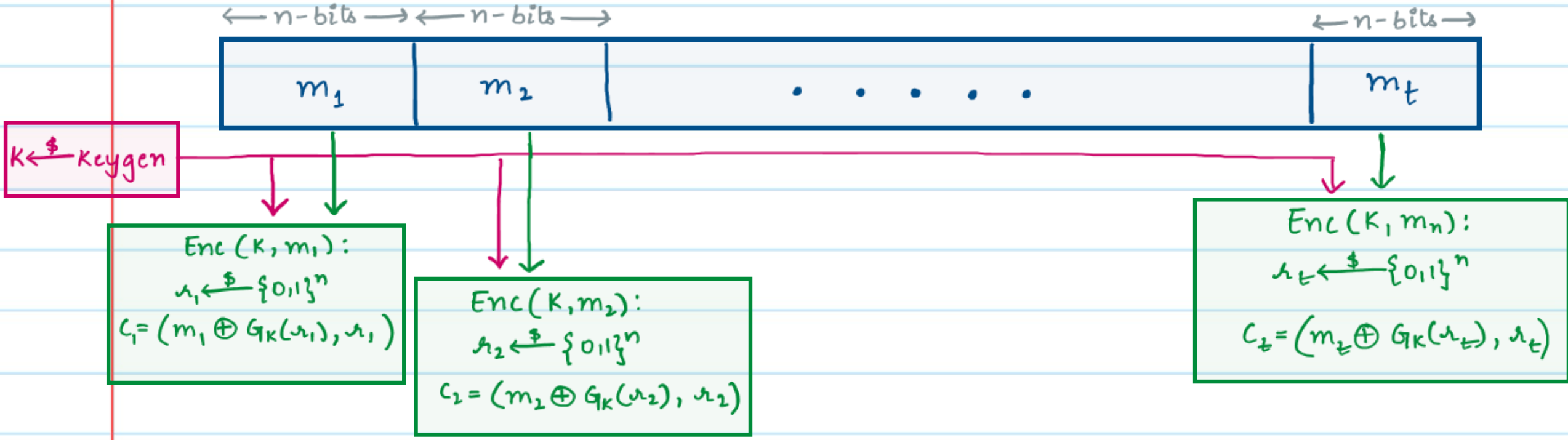
* PRG $\Rightarrow$ PRF
* PRGs can be constructed using well-studied computational hardness assumptions.
* Provably secure but far from practical.

Practical Constructions

* Start from some design framework ("Appropriately chosen" functions, composed "appropriately many times" look random)
* Build a candidate construction
* Do extensive cryptanalysis.
* Practical but not provably secure (eg. AES, DES etc.)

CPA - Secure Encryption for Arbitrary Length Messages

* Let's start with a PRF $G_K : \{0,1\}^m \to \{0,1\}^n$. This PRF yields a CPA-secure encryption for encrypting n-bit messages.
* What if we want to encrypt a tn-bit message?



(Theoretical Construction)

No. of message blocks = t
size of each message block = n

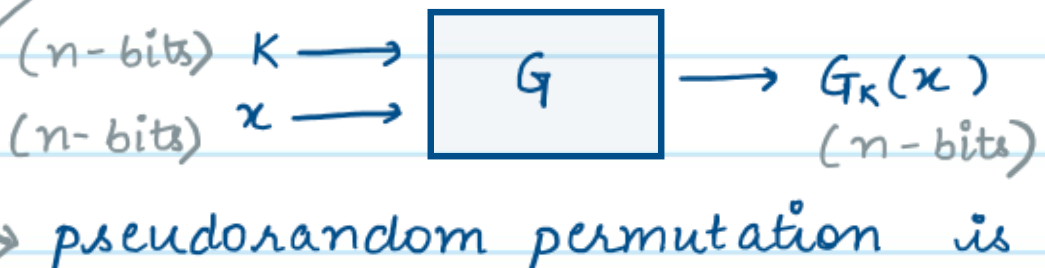
How Good Is This?

	Theoretical Construction				Ideal Goal
Randomness Used	tn - bits				n - bits
Ciphertext Size	2tn - bits				tn+n - bits
Parallelizable ciphertext computation	Yes				Yes
Reusable Randomness	No				Yes
Minimal Assumption	PRF				PRF
CPA Secure?	Yes				Yes

Block-Cipher Modes of Operation

Practical Ways of encrypting long messages.

* **Given:** Let $\{G_K\}$ be a family of length-preserving family of PRFs (or a PRP) with block-length n



pseudorandom permutation is function that is indistinguishable from a random permutation.

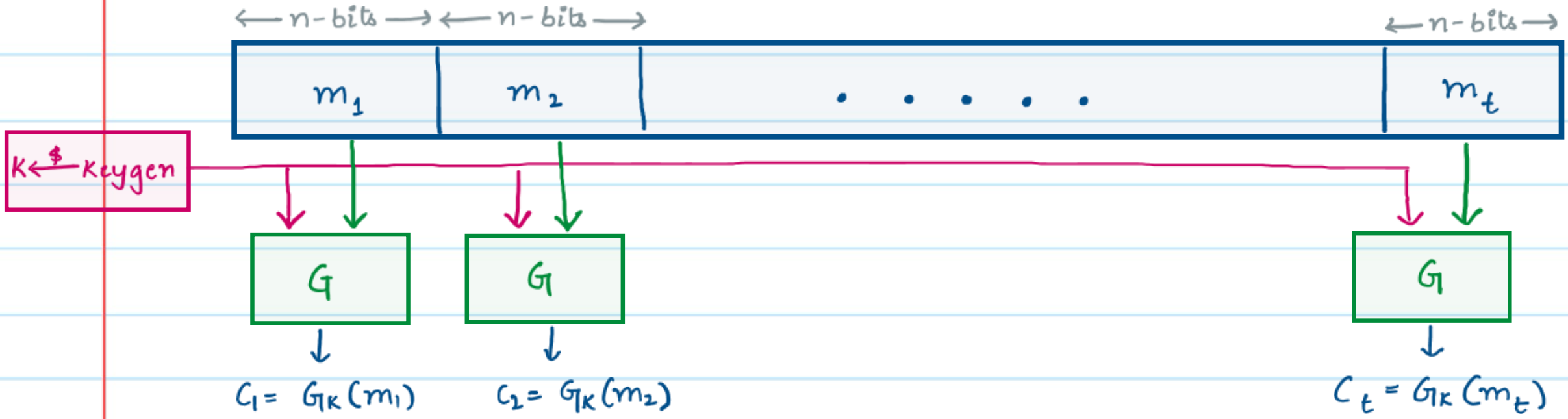
we will assume that G_K^{-1} is also known.

* **Goal:** We want to encrypt $m = m_1, \ldots, m_t$ using G_K with ciphertext length as small as possible and as less randomness as possible.

What can we do if the message length is not a multiple of n?

Electronic Code Book (ECB) Mode

Let $\{G_K\}$ be a family of PRPs.



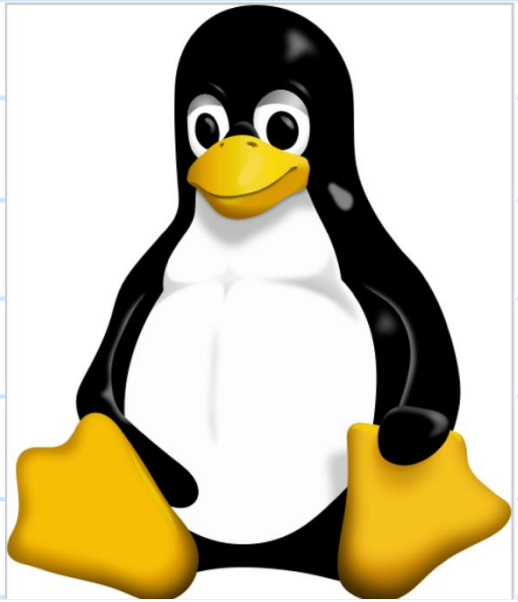
* Decryption: $\forall i \in [t]$, compute $m_i = G_K^{-1}(c_i)$.

Is this CPA-secure? Why NOT?

How Good Is This?

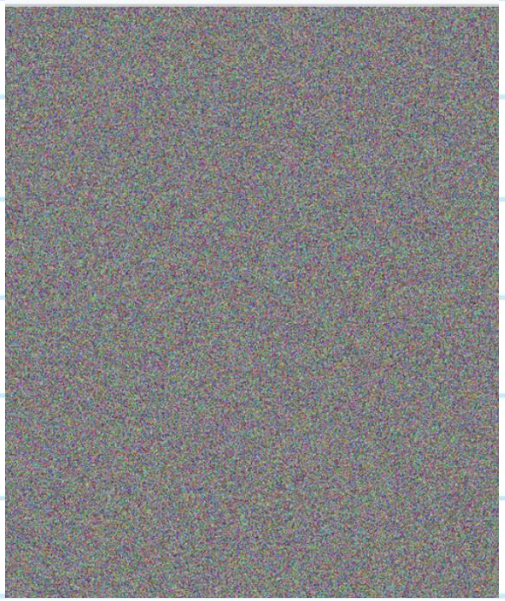
	Theoretical Construction	ECB			Ideal Goal
Randomness Used	tn - bits	0 - bits			n - bits
Ciphertext Size	2tn - bits	tn - bits			tn+n - bits
Parallelizable ciphertext computation	yes	yes			yes
Reusable Randomness	No	–			Yes
Minimal Assumption	PRF	PRP			PRF
CPA Secure?	Yes	No			Yes

Visible Insecurity of ECB



Plain Image

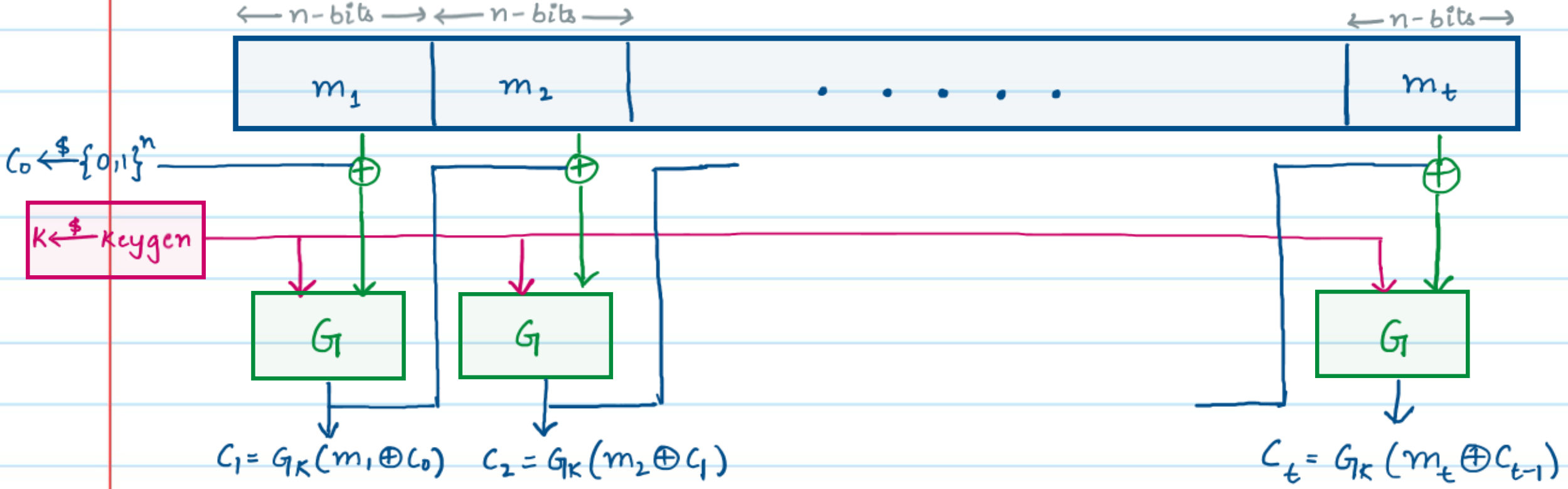
ECB Encrypted



Securely Encrypted

Cipher Block Chaining (CBC) Mode (used in SSL 3.0 and TLS 1.0)

Let $\{G_K\}$ be a family of PRPs.



* Decryption: $\forall i \in [t]$, compute $m_i = G_K^{-1}(C_i) \oplus C_{i-1}$

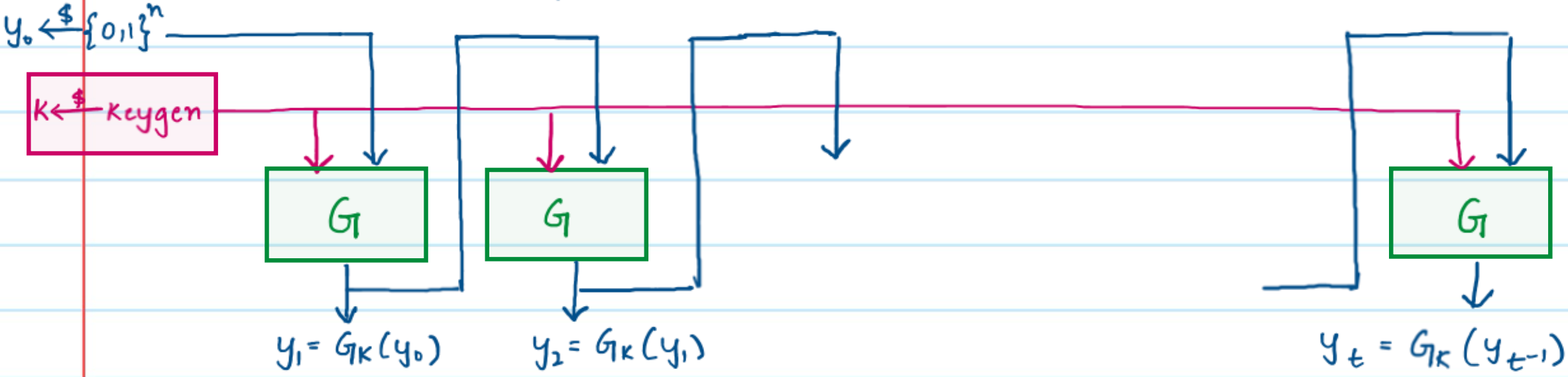
Is this CPA-secure? Can we reuse C_0?

How Good Is This?

	Theoretical Construction	ECB	CBC		Ideal Goal
Randomness Used	tn-bits	0-bits	n-bits		n-bits
Ciphertext Size	2tn-bits	tn-bits	tn+n-bits		tn+n-bits
Parallelizable ciphertext computation	yes	yes	No		yes
Reusable Randomness	No	–	–		Yes
Minimal Assumption	PRF	PRP	PRP		PRF
CPA Secure?	Yes	No	yes		Yes

Output Feedback (OFB) Mode

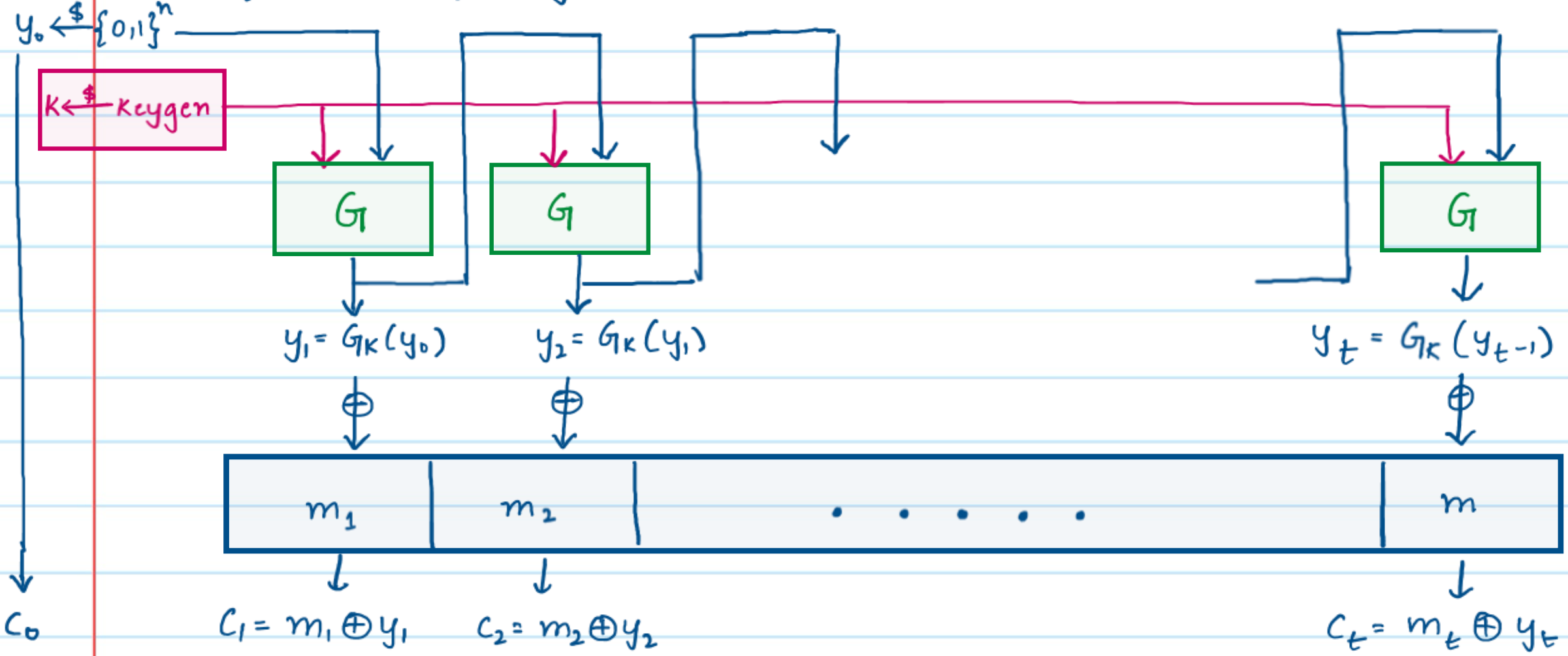
Let $\{G_K\}$ be a family of PRFs



* Generate a pseudorandom stream of one-time pads.

Output Feedback (OFB) Mode (Used in multimedia streaming)

Let $\{G_K\}$ be a family of PRFs.



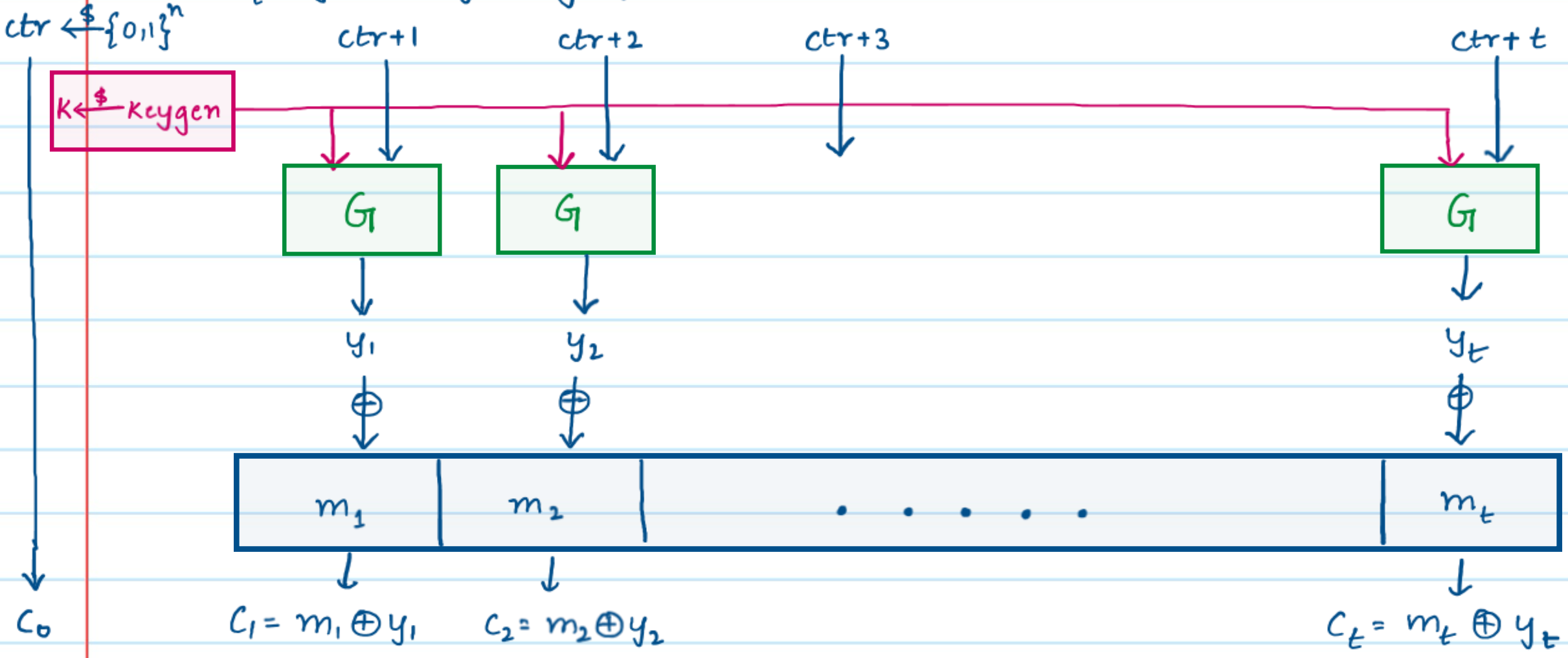
* Use the pseudorandom stream to mask messages

How Good Is This?

	Theoretical Construction	ECB	CBC	OFB	Ideal Goal
Randomness Used	tn-bits	0-bits	n-bits	n-bits	n-bits
Ciphertext Size	2tn-bits	tn-bits	tn+n-bits	tn+n-bits	tn+n-bits
Parallelizable ciphertext computation	yes	yes	No	No, but pre-computable	yes
Reusable Randomness	No	–	–	–	Yes
Minimal Assumption	PRF	PRP	PRP	PRF	PRF
CPA Secure?	Yes	No	yes	yes	Yes

Counter (CTR) Mode (Used in VPNs, cloud computing etc.)

Let $\{G_K\}$ be a family of PRFs.



How Good Is This?

	Theoretical Construction	ECB	CBC	OFB	CTR / Ideal Goal
Randomness Used	tn-bits	0-bits	n-bits	n-bits	n-bits
Ciphertext Size	2tn-bits	tn-bits	tn+n-bits	tn+n-bits	tn+n-bits
Parallelizable ciphertext computation	Yes	Yes	No	No, but pre-computable	Yes
Reusable Randomness	No	–	–	–	–
Minimal Assumption	PRF	PRP	PRP	PRF	PRF
CPA Secure?	Yes	No	Yes	Yes	Yes