Sender-Anamorphic Encryption Reformulated: Achieving Robust and Generic Constructions

Yi Wang

※National University of Defense Technology, China

joint work with

Rongmao Chen※, Xinyi Huang#, Moti Yung*

#The Hong Kong University of Science and Technology (Guangzhou), China,

*Columbia University & Google LLC, USA

ASIACRYPT 2023

Background

Message Transmission

Sender-freedom assumption

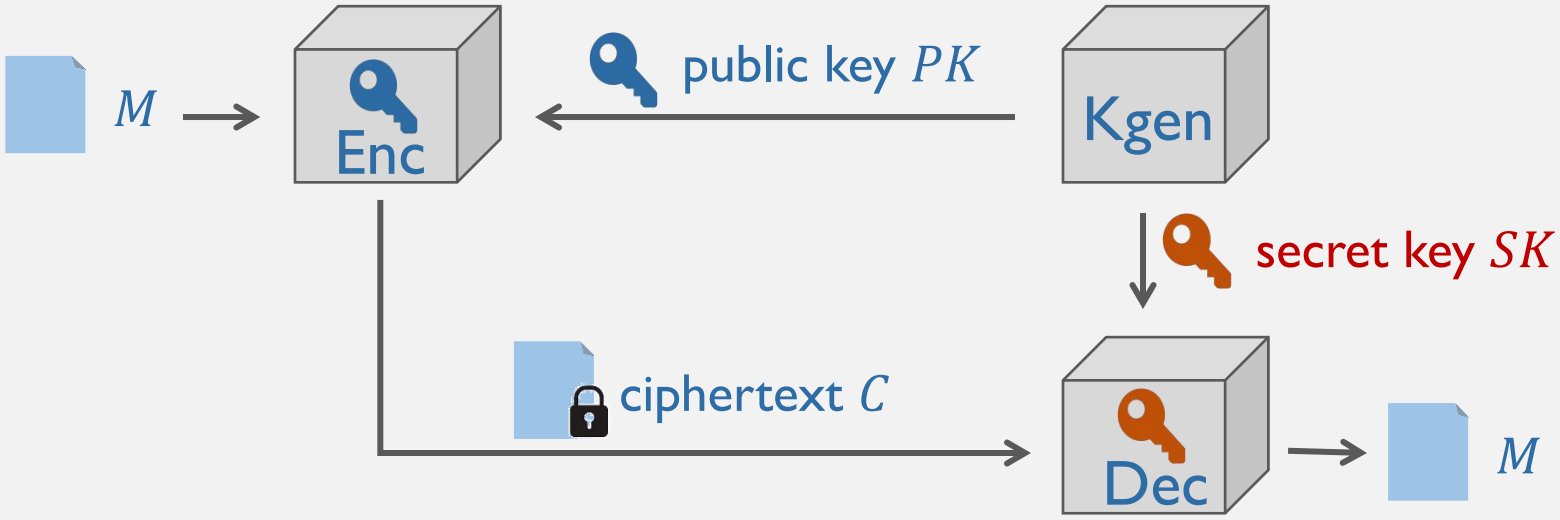
Free to choose message to be sent

Alice

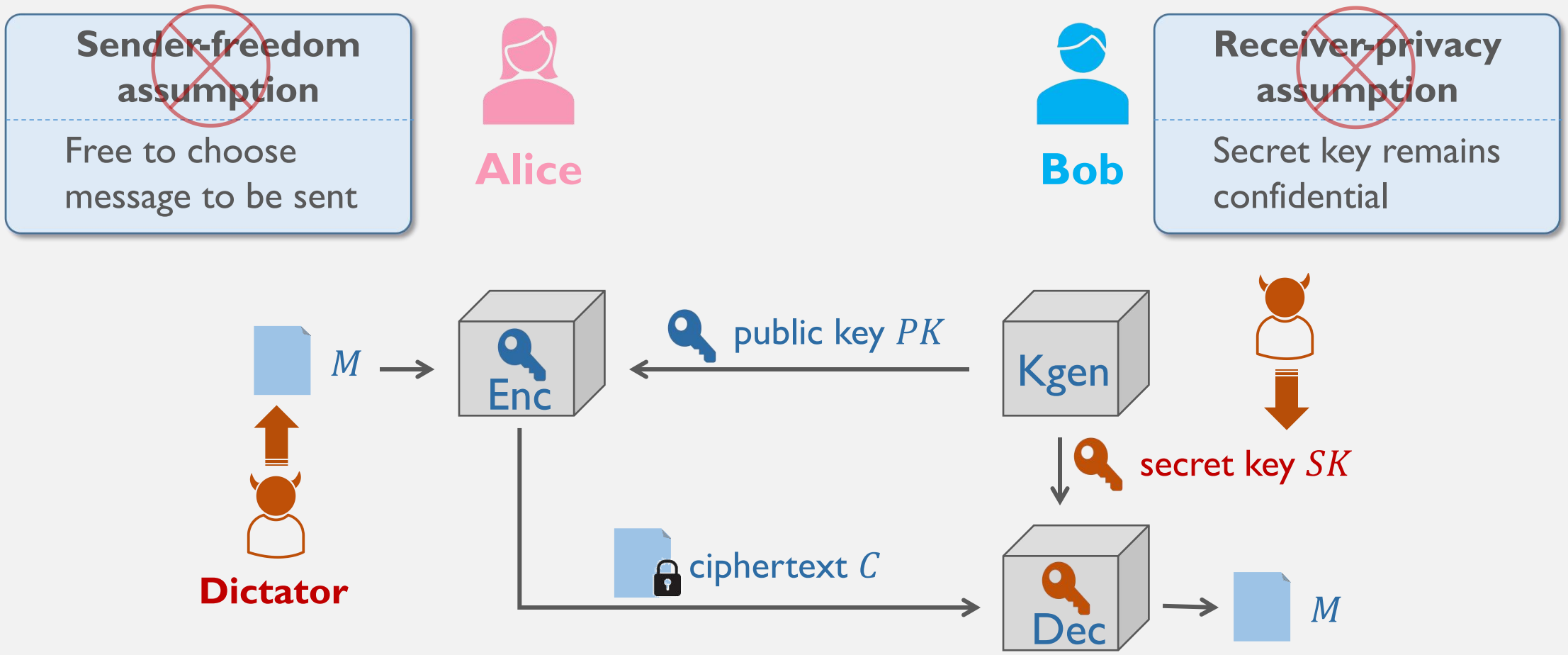
Bob

Receiver-privacy assumption

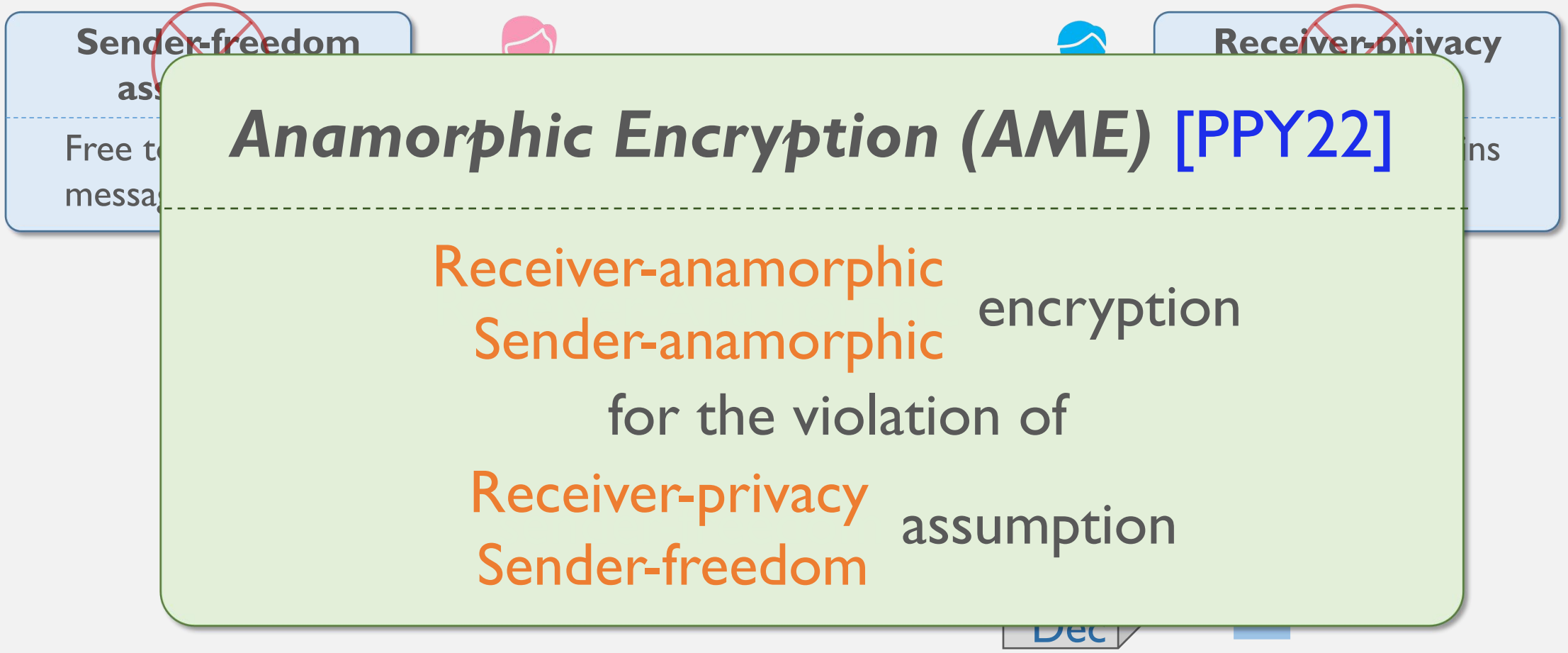
Secret key remains confidential



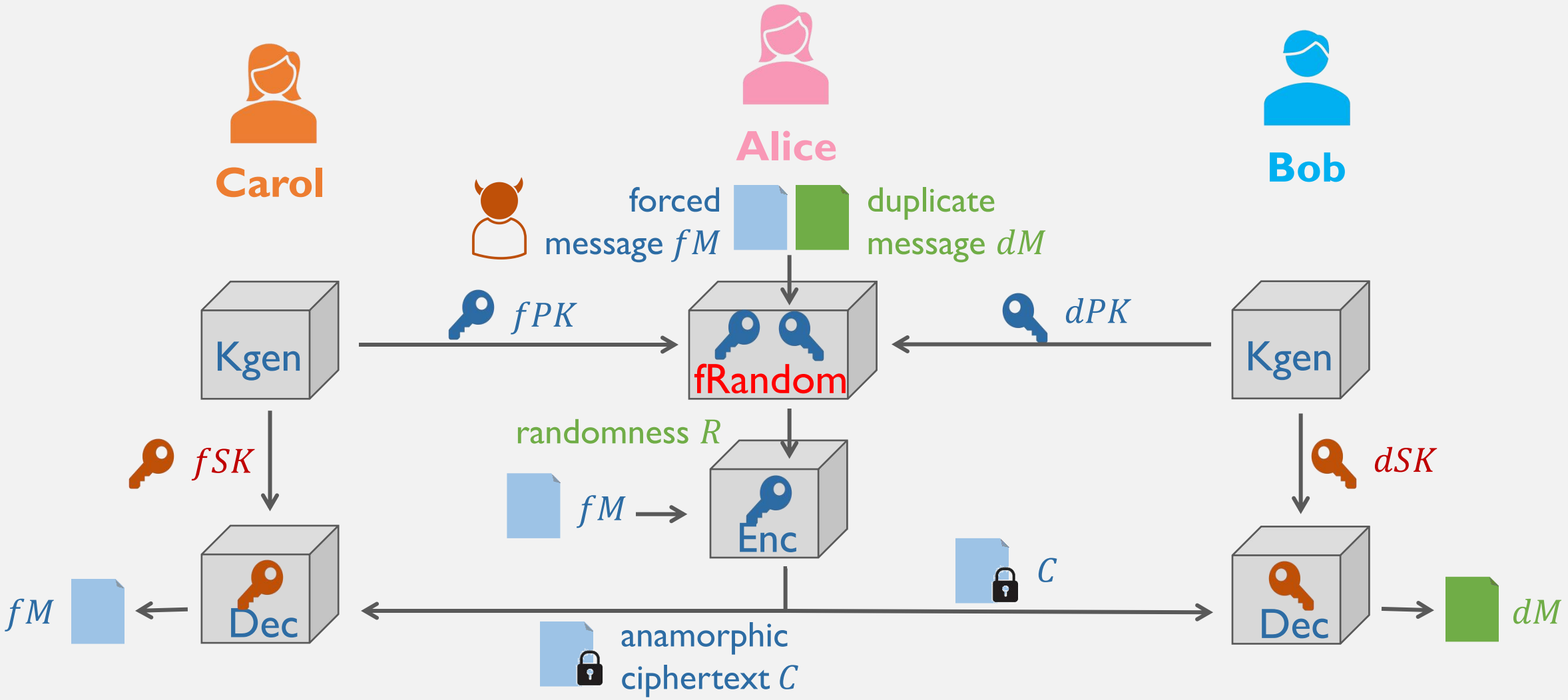
Message Transmission



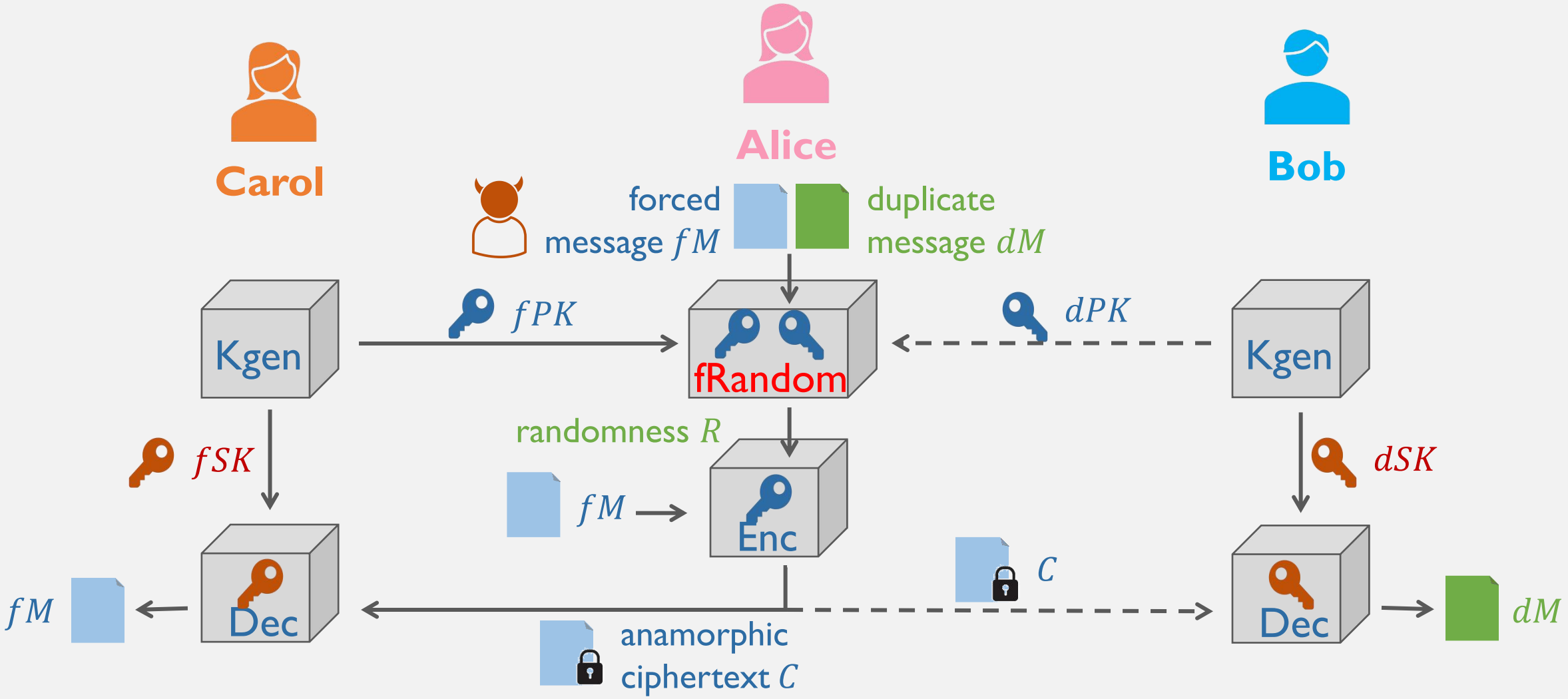
Message Transmission



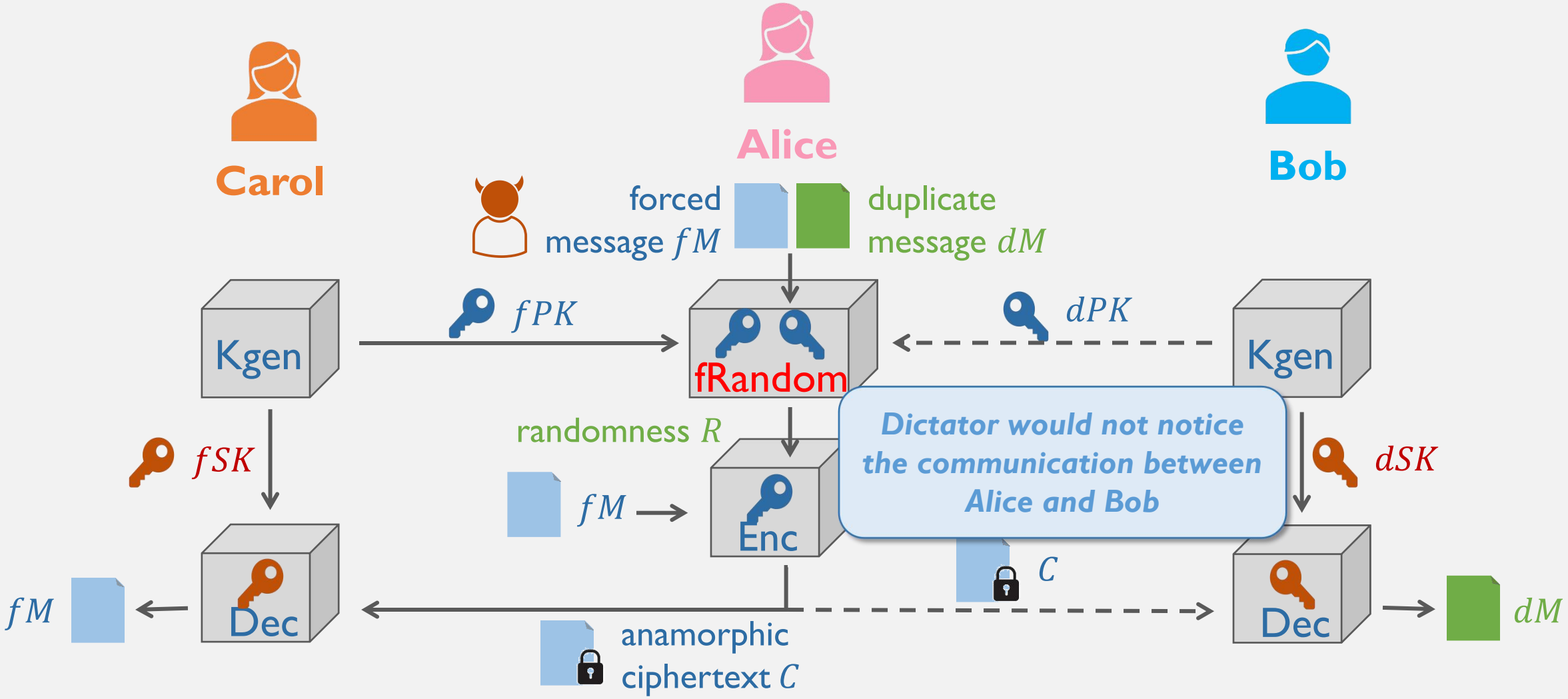
Sender-Anamorphic Encryption [PPY22]



Sender-Anamorphic Encryption [PPY22]



Sender-Anamorphic Encryption [PPY22]

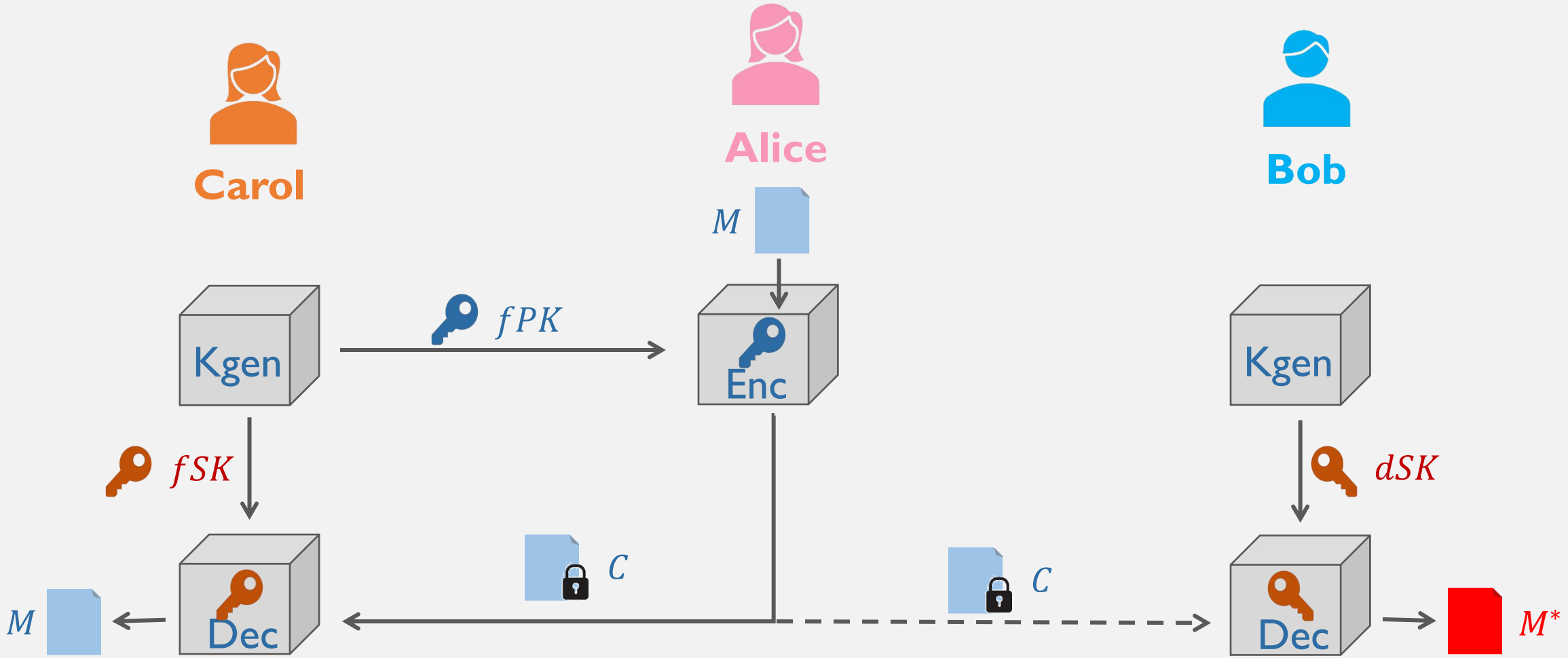


Sufficient Conditions for 1-bit Sender-AME [PPY22]

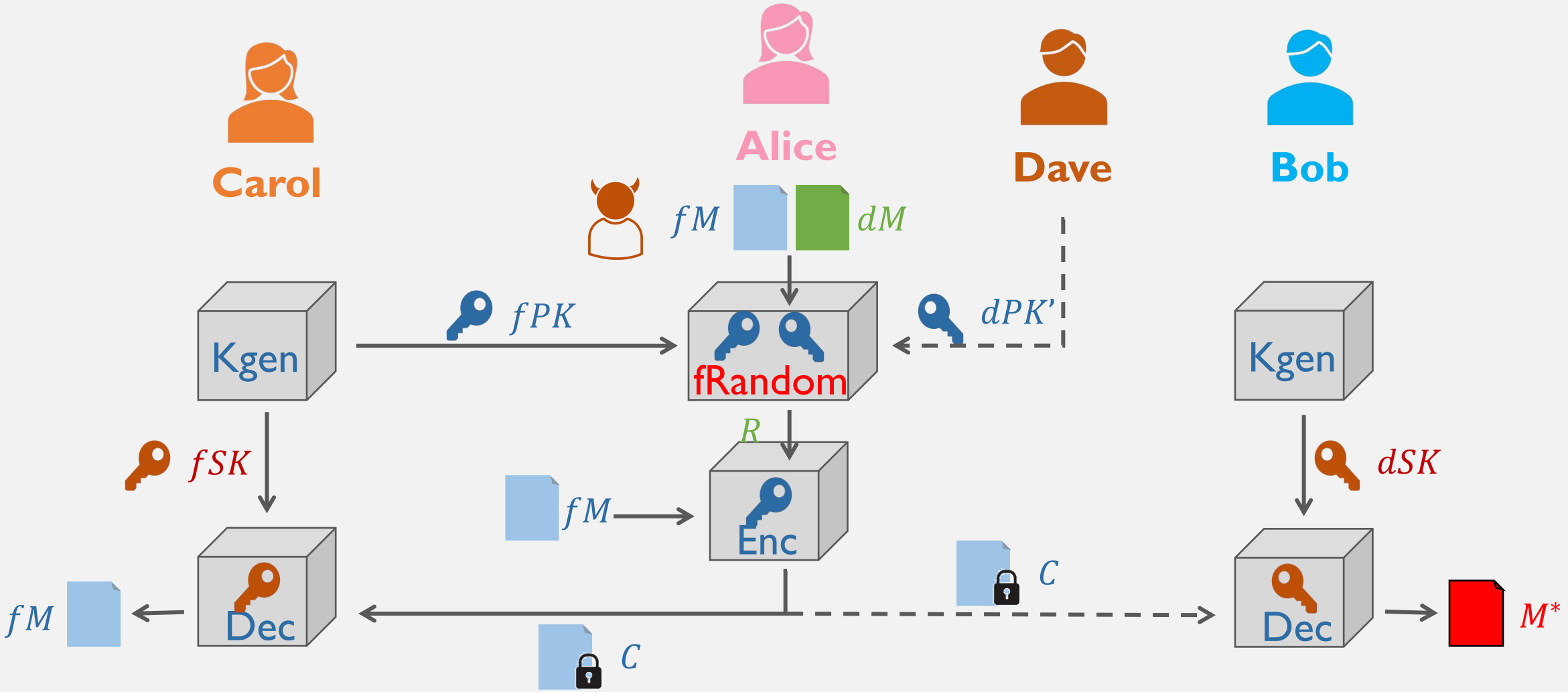
- Common Randomness
  - $C \leftarrow \mathsf{Enc}(PK_0, M_0; R) \Rightarrow\ C \leftarrow \mathsf{Enc}(PK_1, M_1; R)$
- Message Recovery from Randomness
  - $M \leftarrow \mathsf{Rec}(C, PK, R)$
- Equal Distribution of Plaintext
  - $C \leftarrow_{\$} \mathcal{C}, (PK, SK) \leftarrow_{\$} \mathsf{Kgen}(1^n) \Rightarrow\ \mathbf{Pr}[\mathsf{Dec}(SK, C) = 0] = 1/2$

The only known sender-AMEs are the LWE and the Dual LWE cryptosystems.

Misreading of Normal Ciphertext



Misreading of Anamorphic Ciphertext



Sender-AME with Robustness

- Robustness
  - Decrypting normal ciphertext in anamorphic way or anamorphic ciphertext with wrong duplicate secret key should produce an explicit abort signal.
- Contradiction
  - An anamorphic ciphertext is a normal ciphertext with proper randomness.
  - Decryption algorithm always returns a bit for normal ciphertext.

Sender-AME with Robustness

- Robustness
  - Decrypting normal ciphertext in anamorphic way or anamorphic ciphertext with wrong duplicate secret key should produce an explicit abort signal.
- Contradiction
  - An anamorphic ciphertext is a normal ciphertext with proper randomness.
  - Decryption algorithm always returns a bit for normal ciphertext.

It seems impossible to construct "robust" sender-AME.

Our Work

- New Formalization
- Generic Constructions
- Relation Exploration

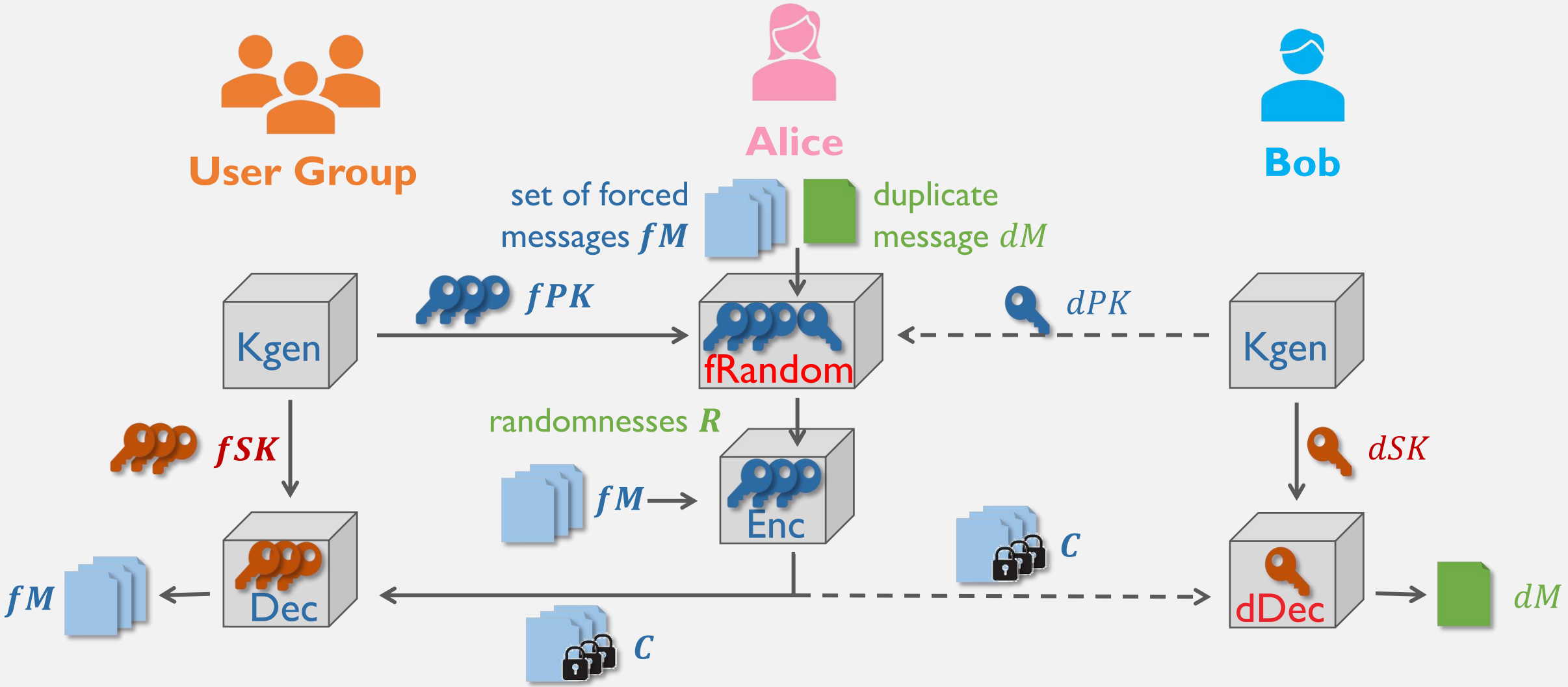
Our Work

- New Formalization
- Generic Constructions
- Relation Exploration

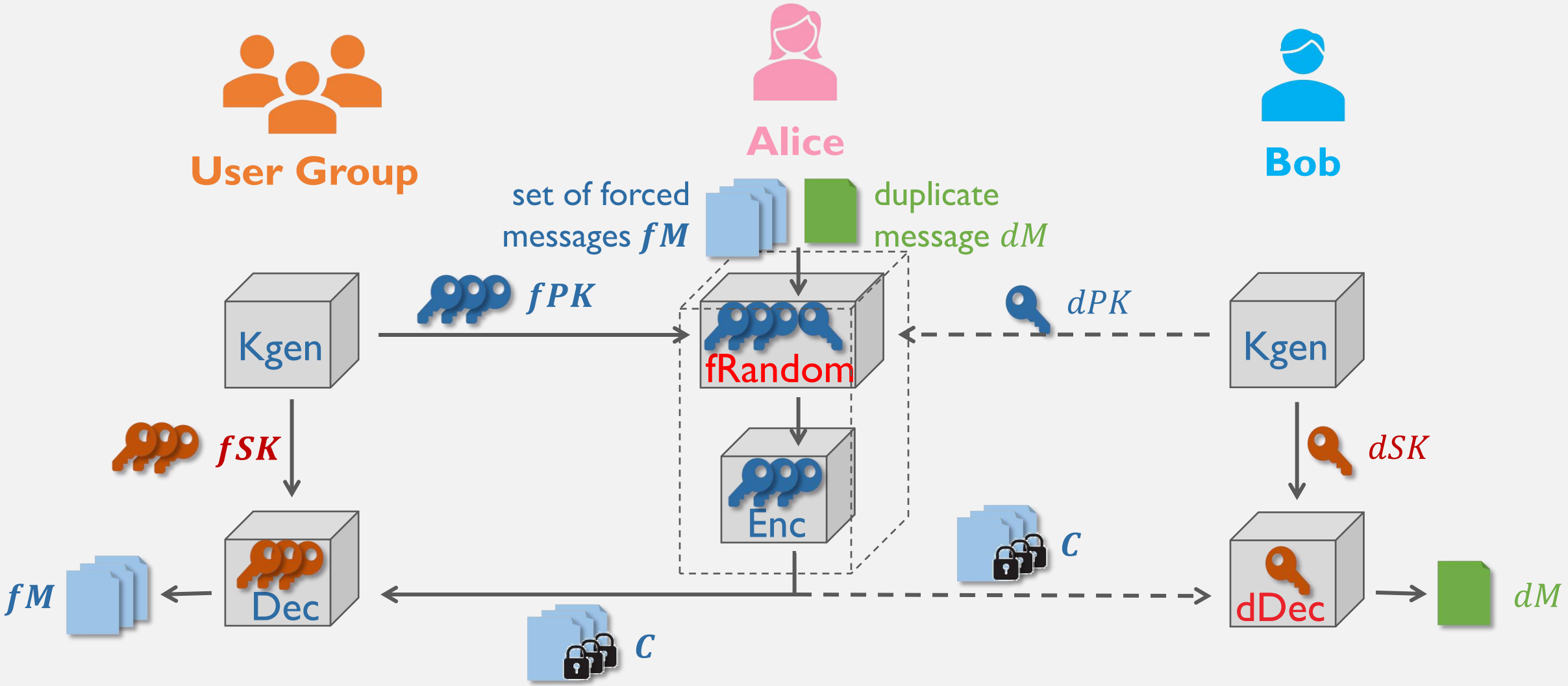
Reformulate Sender-AME

- Observation
  - User usually sends more than one ciphertext to the others
- Relaxation
  - Encoding both forced and duplicate messages into one anamorphic ciphertext
  - Encoding duplicate message across multiple anamorphic ciphertexts
- Modification
  - Coin-toss faking algorithm takes as input multiple forced message and public key pairs
  - Alternative decryption algorithm extracts duplicate message from multiple anamorphic ciphertexts

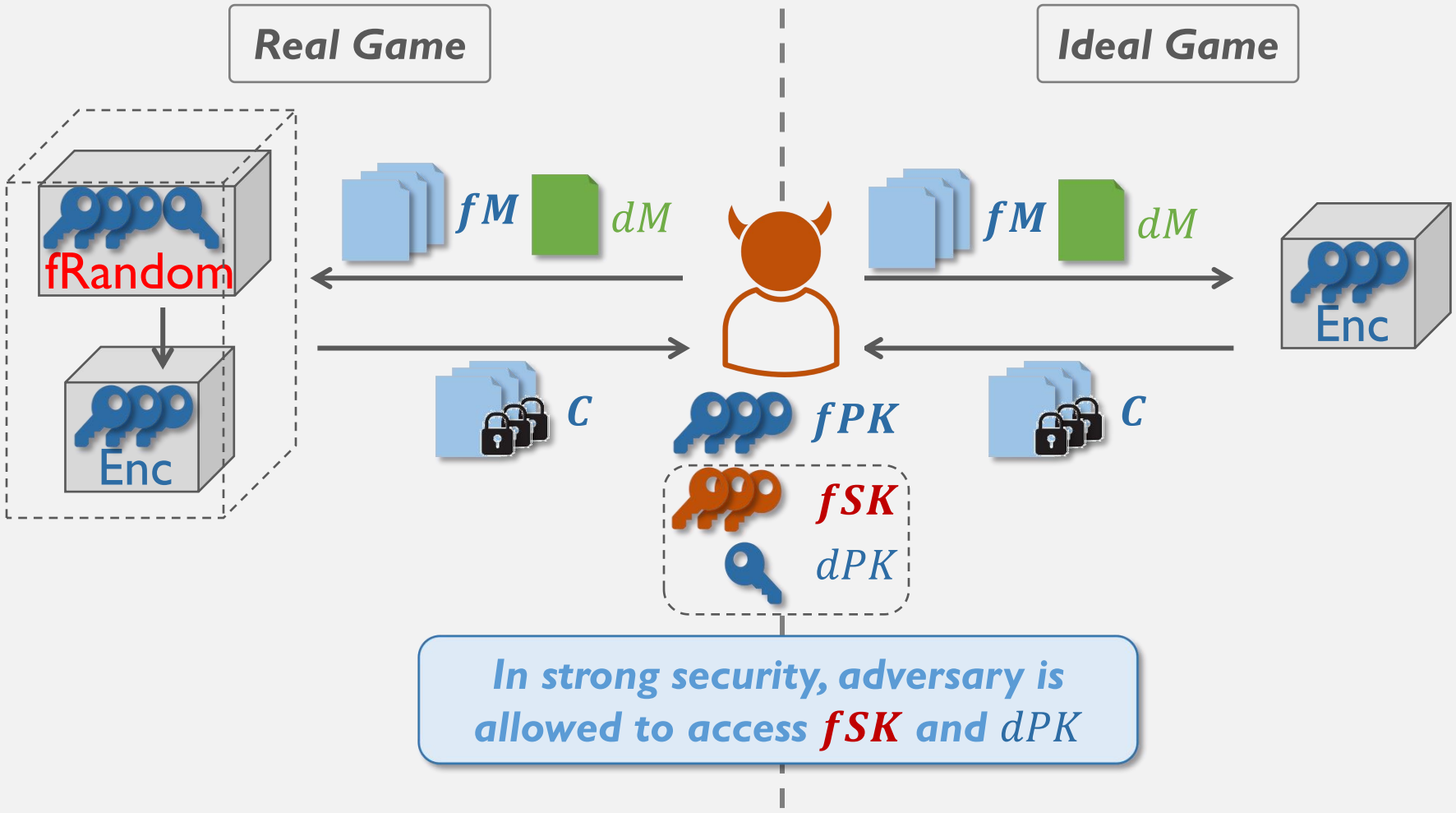
ℓ-Sender-Anamorphic Encryption



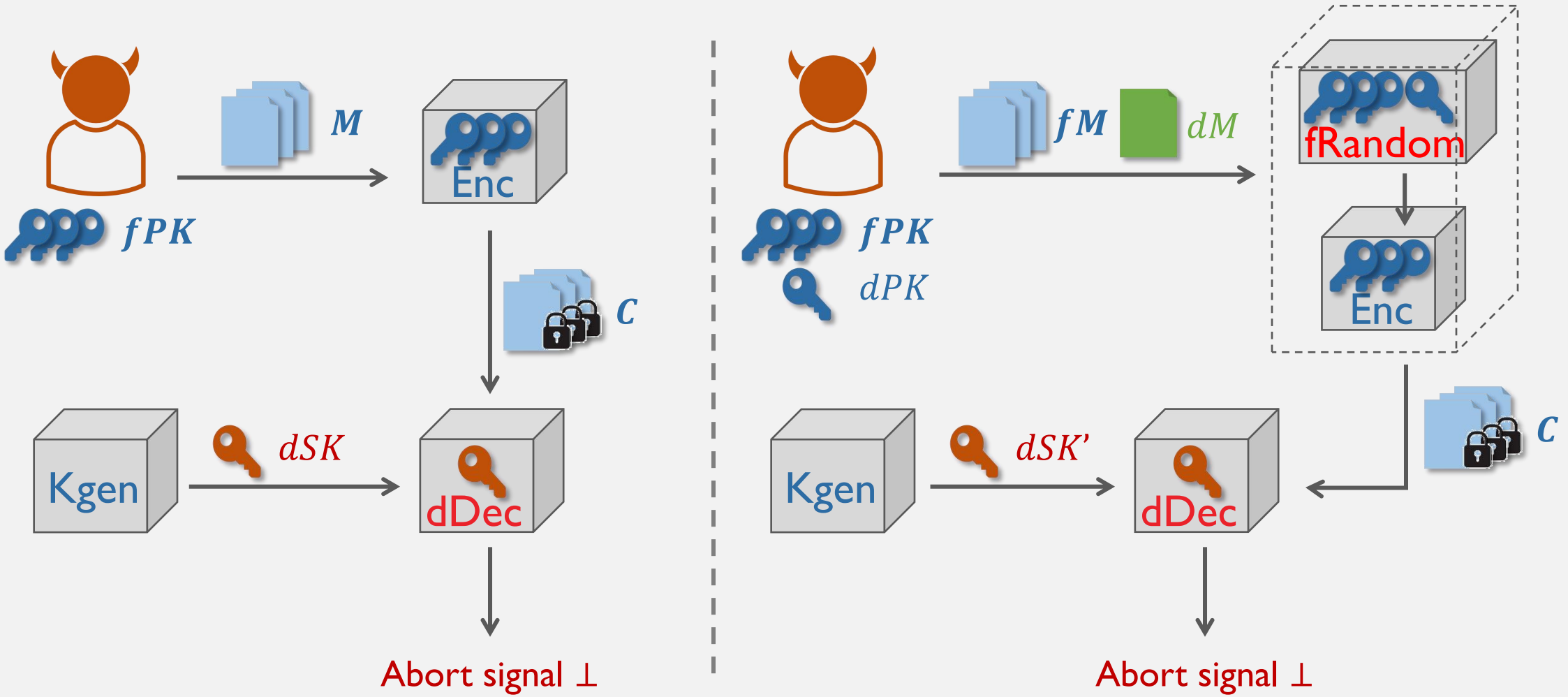
ℓ-Sender-Anamorphic Encryption



ℓ-Sender-AME : Security



ℓ-Sender-AME : Robustness



Our Work

- New Formalization
- Generic Constructions
- Relation Exploration

Construction I : Pseudorandom and Robust PKE

➢Pseudorandomness [vAH04]

Challenger **Adversary**

PK →

← M

$C_0 \leftarrow_{\$} \mathrm{Enc}(PK, M)$

$C_1 \leftarrow_{\$} \{0,1\}^{\ell}$

C_b →

← b'

$|\mathbf{Pr}[b' = b] - 1/2| \leq \mathbf{negl}(n)$

➢Robustness [ABN10]

Challenger **Adversary**

$\boldsymbol{PK}$ →

← (M, i, j)

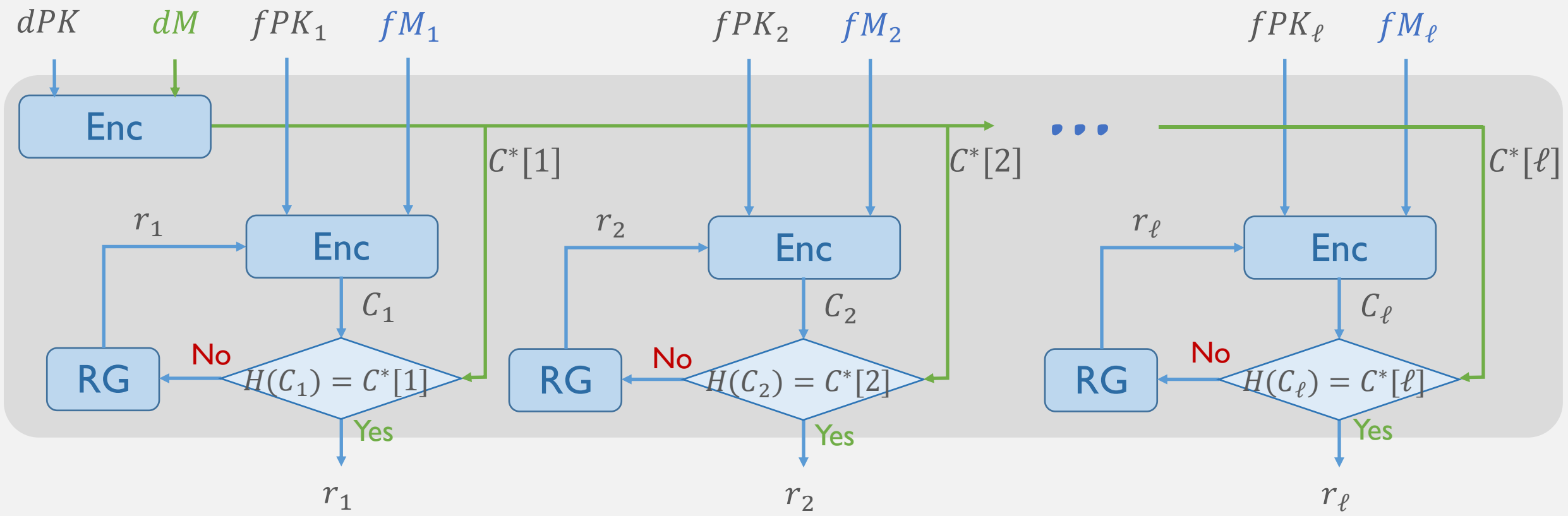
$C \leftarrow_{\$} \mathrm{Enc}(PK_i, M)$

$M' \leftarrow \mathrm{Dec}(SK_j, C)$

$\mathbf{Pr}[(M \neq \perp) \wedge (M' \neq \perp)] \leq \mathbf{negl}(n)$

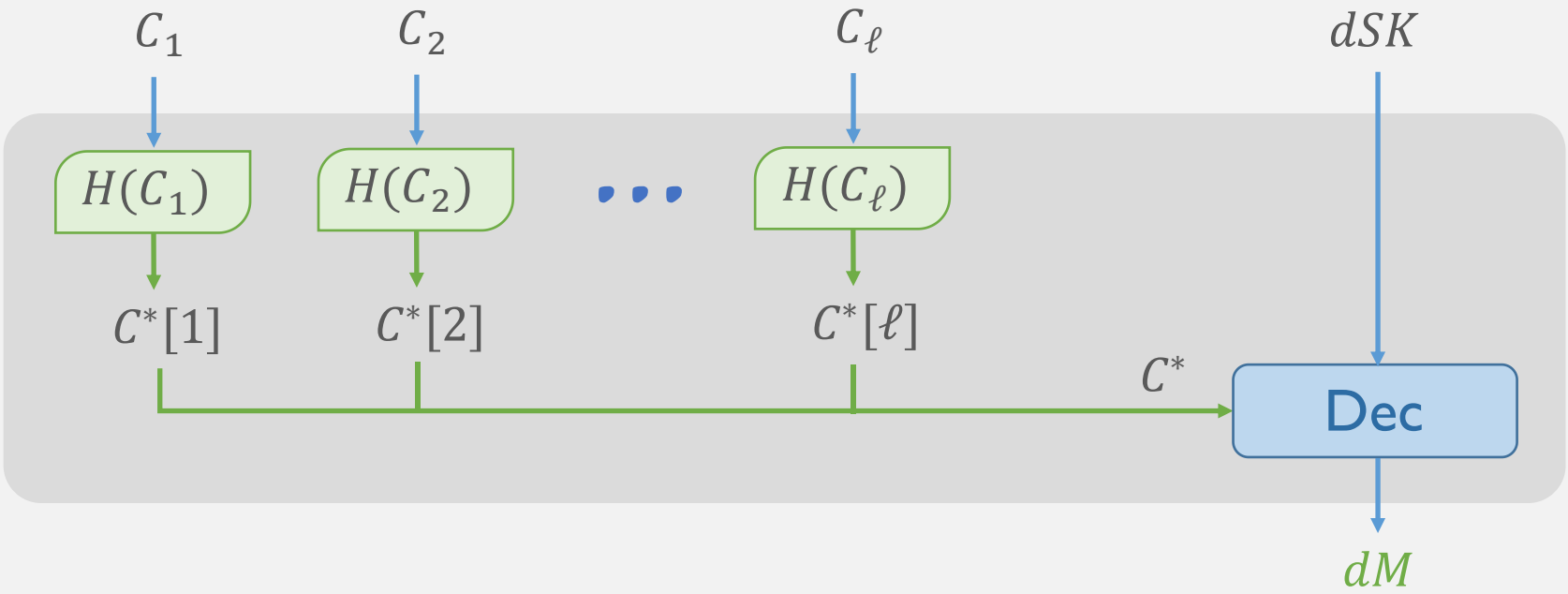
Construction I : Pseudorandom and Robust PKE

➢ fRandom algorithm

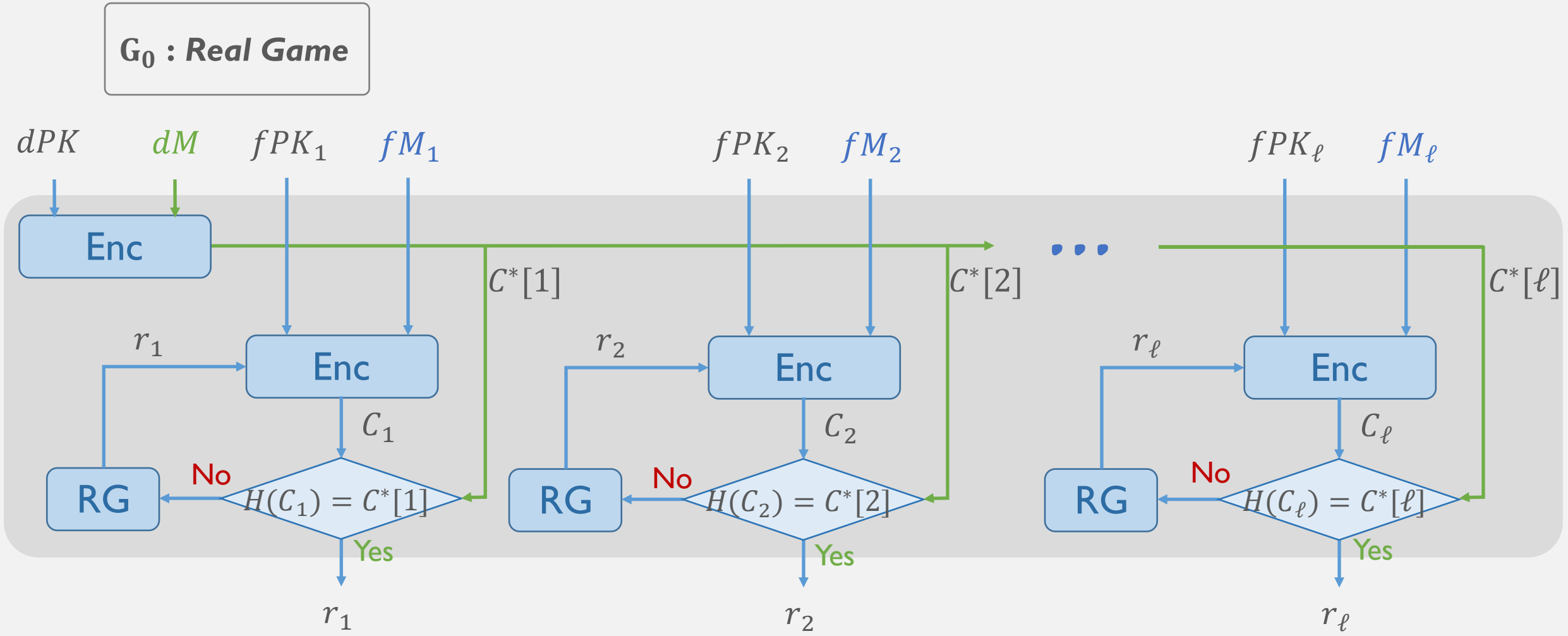


Construction I : Pseudorandom and Robust PKE

➢ dDec algorithm



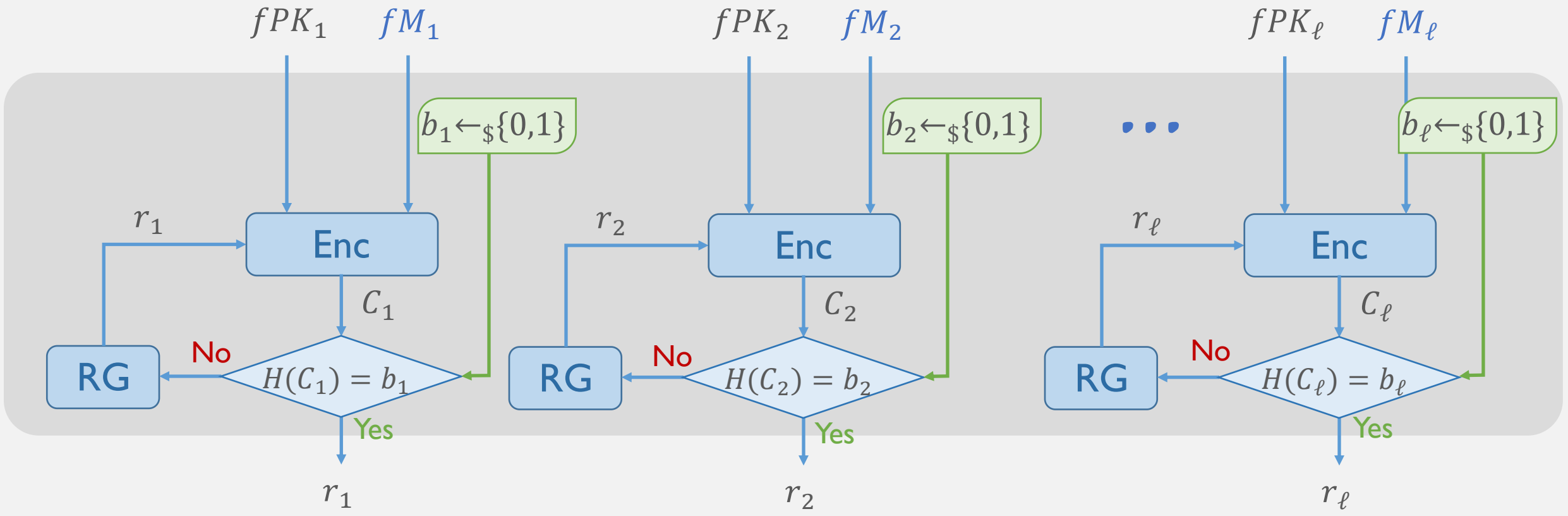
Construction I : Security



Construction I : Security

G_1 : *Replace* C^* *with random string*

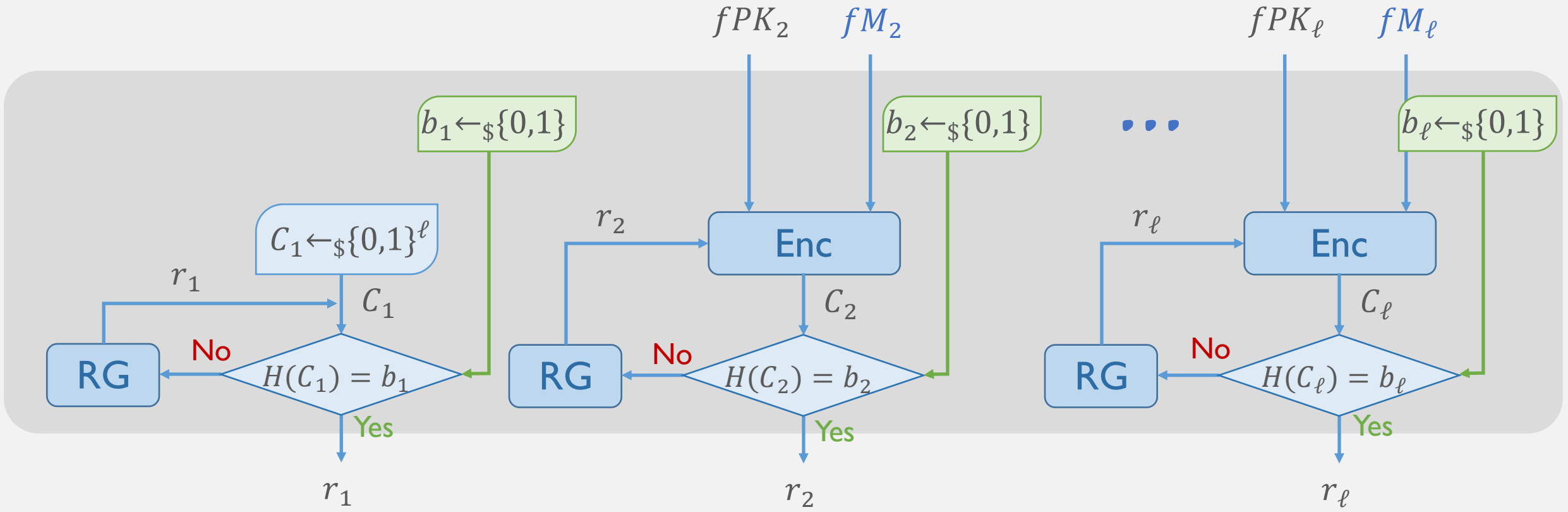
Pseudorandomness of PKE



Construction I : Security

G_2 : *Replace* C_1 *with random string*

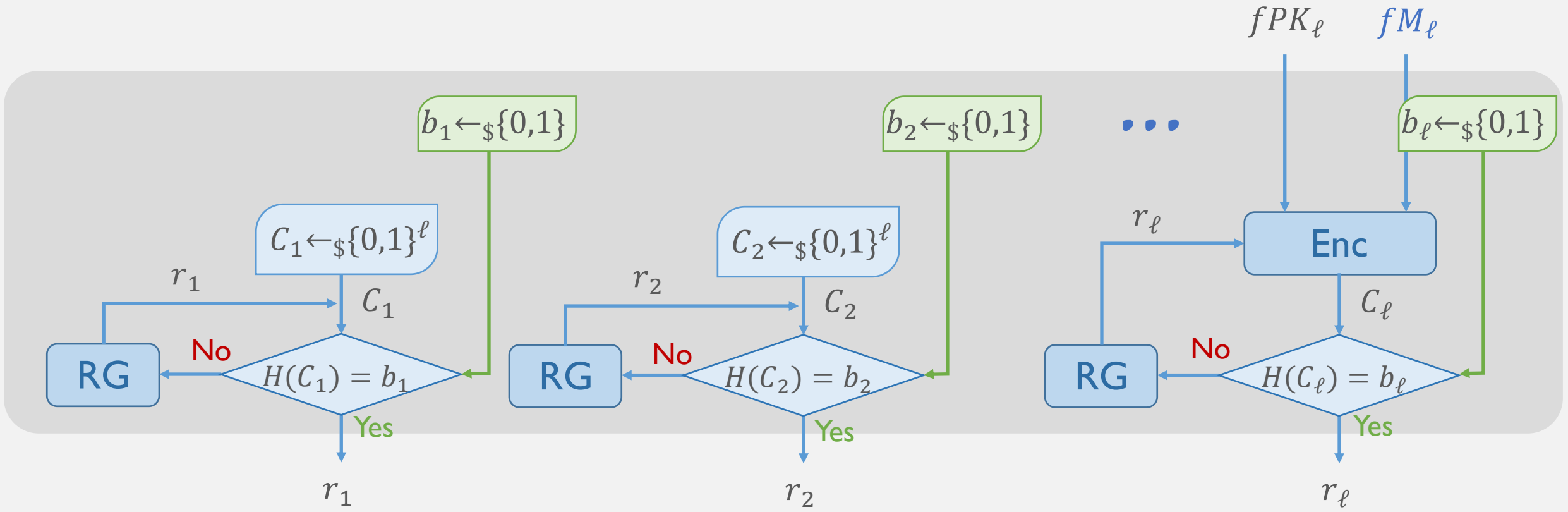
Pseudorandomness of PKE



Construction I : Security

G_3 : *Replace* C_2 *with random string*

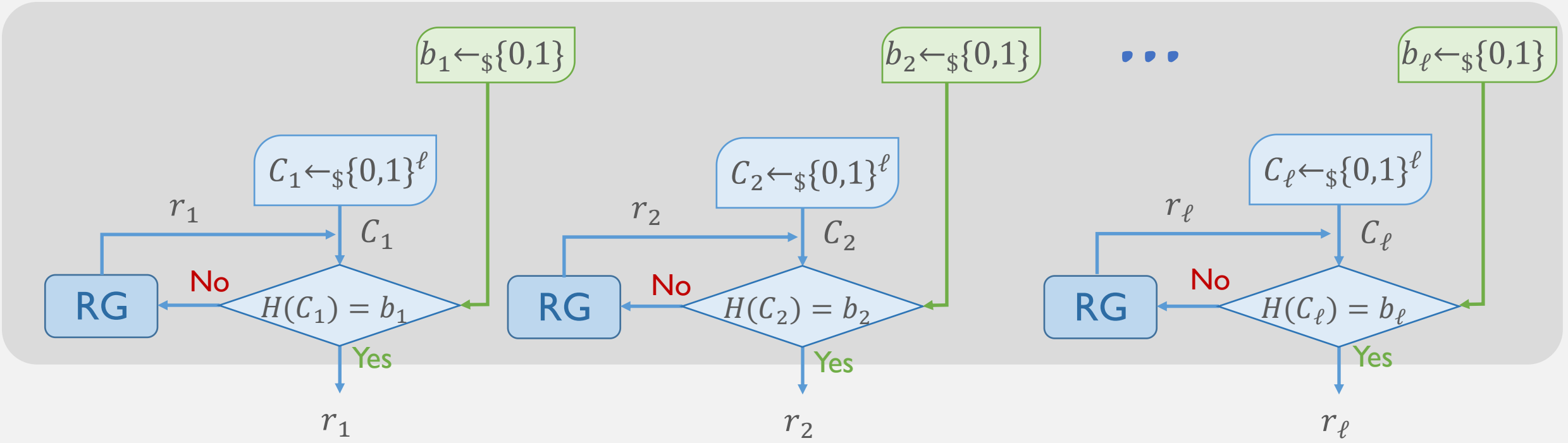
Pseudorandomness of PKE



Construction I : Security

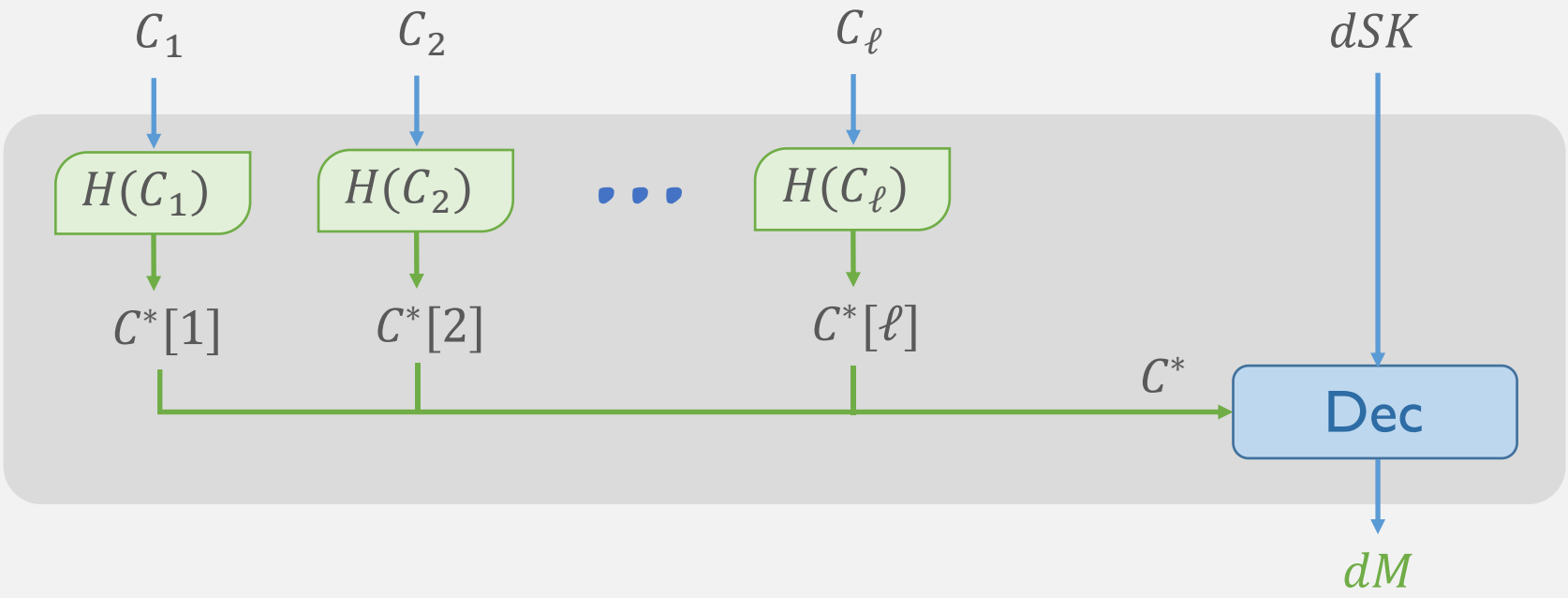
$\mathbf{G}_{\ell+1}$: ***Replace*** C_ℓ ***with random string (Ideal Game)***

Pseudorandomness of PKE



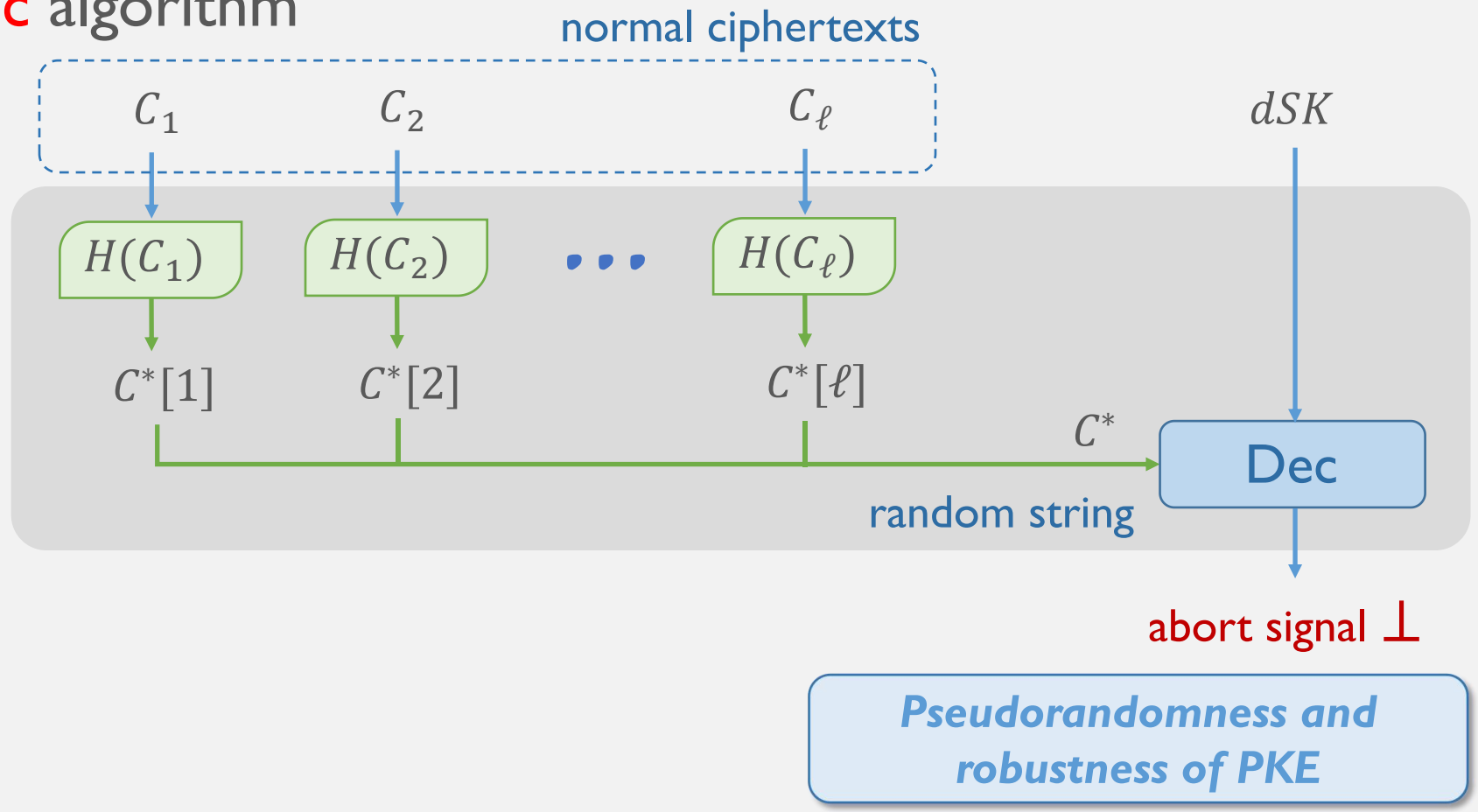
Construction I : Robustness

- dDec algorithm



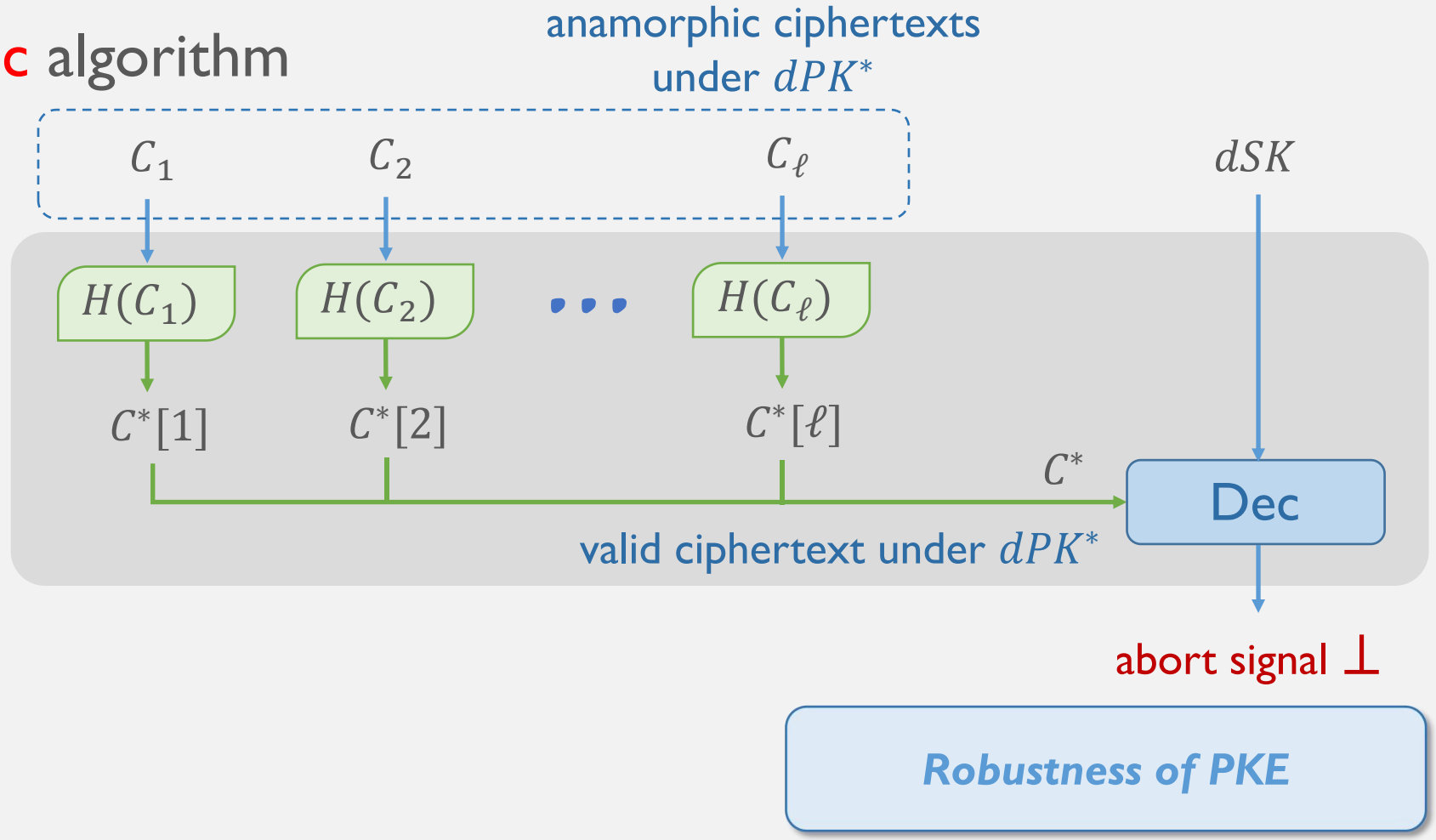
Construction I : Robustness

- dDec algorithm



Construction I : Robustness

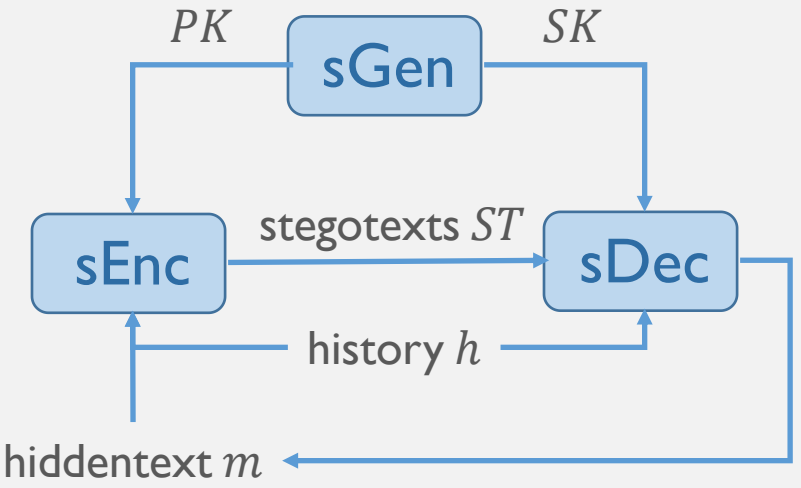
➢ dDec algorithm



Robustness of PKE

Construction I : Conclusion

➢ Public-Key Stegosystem (PKS)



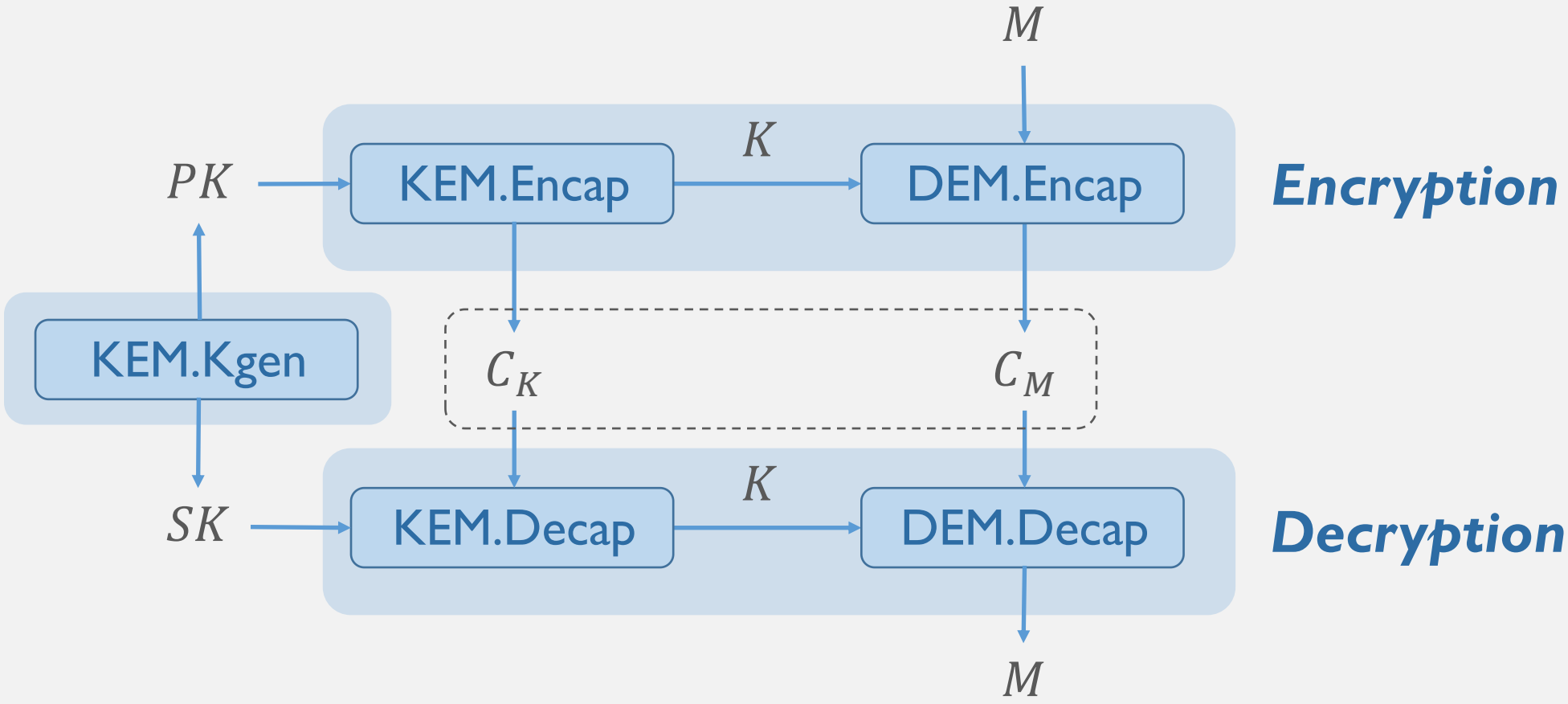
sEnc *also has access to a* ***channel oracle*** *which can sample from the channel distribution* $\mathcal{C}_h$

➢ Relation between ℓ-Sender-AME and PKS

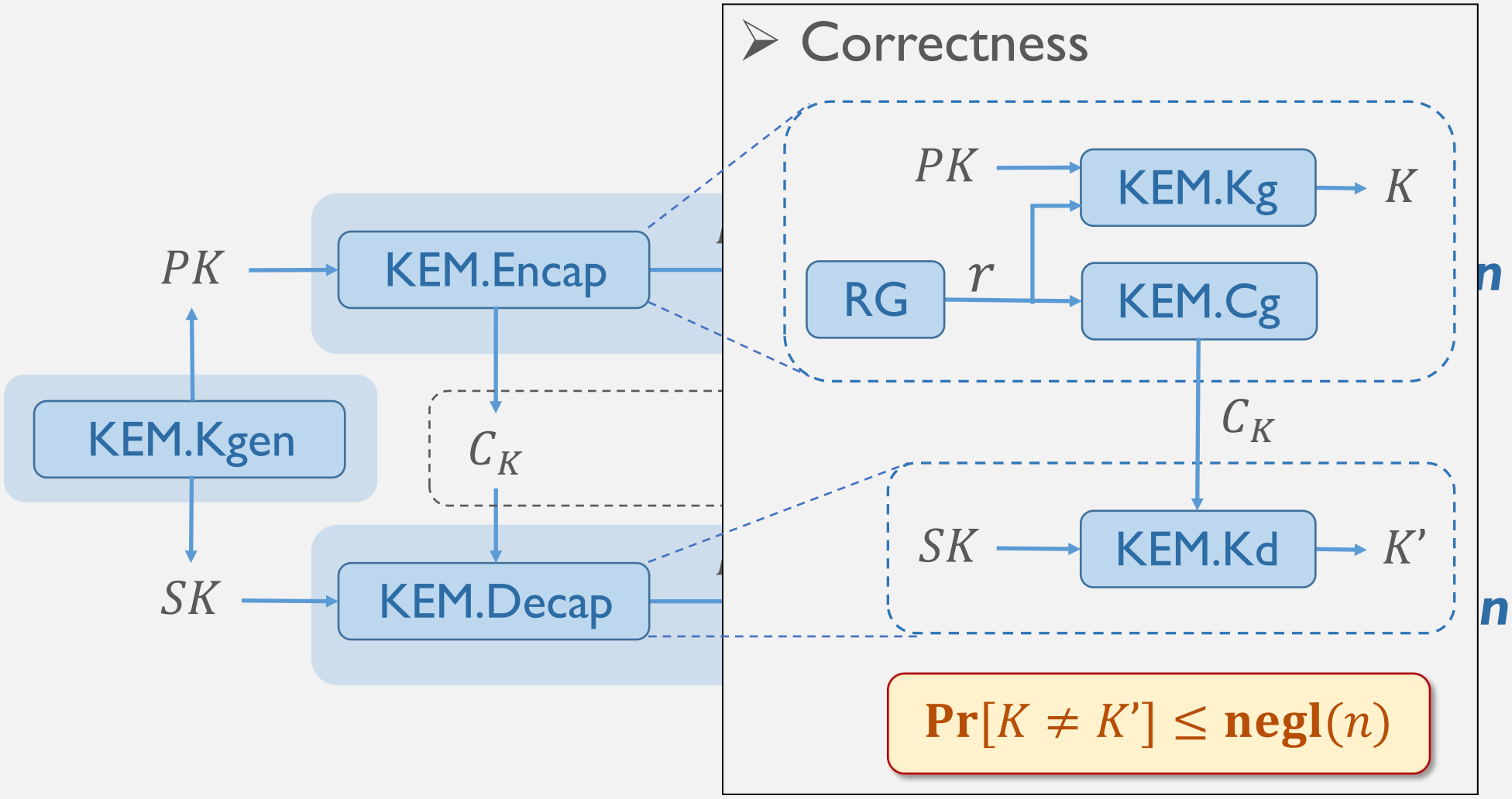
- ℓ-Sender-AME ⇒ PKS (Theorem 7.1)
- PKS ⇏ ℓ-Sender-AME

Construction II : Hybrid PKE with Special KEM

➢ Hybrid PKE : KEM + DEM (Key / Data Encapsulation Mechanism)



Construction II : Hybrid PKE with Special KEM



Construction II : Hybrid PKE with Special KEM

➢ Key Pseudorandomness

Challenger

Adversary

$r \leftarrow_{\$} \text{RG}$

$C_K \leftarrow \text{KEM.Cg}\ (r)$

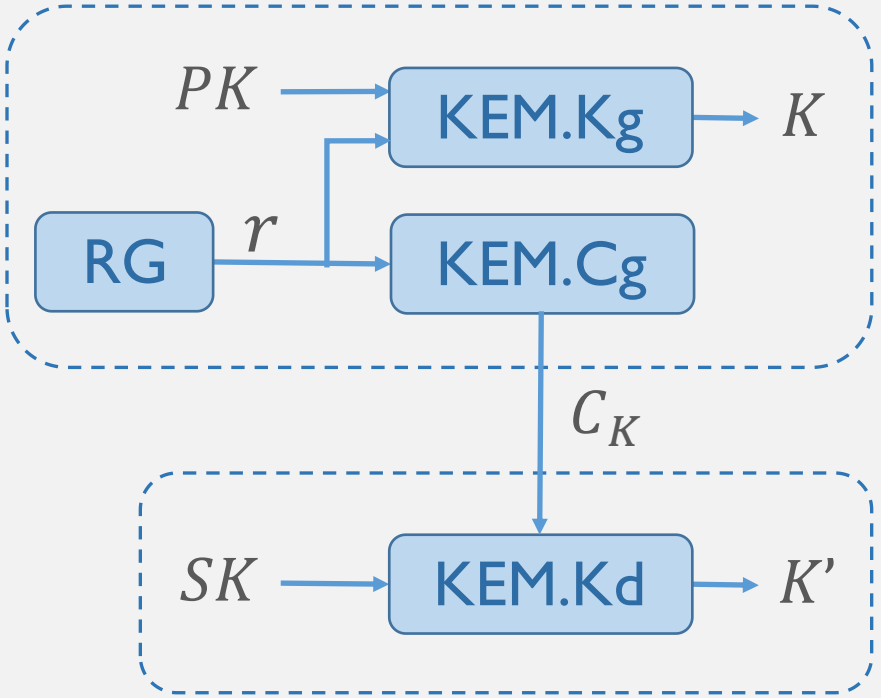
$K_0 \leftarrow \text{KEM.Kg}\ (PK, r)$

$K_1 \leftarrow_{\$} \mathcal{K}$

$C_K, PK, K_b \rightarrow$

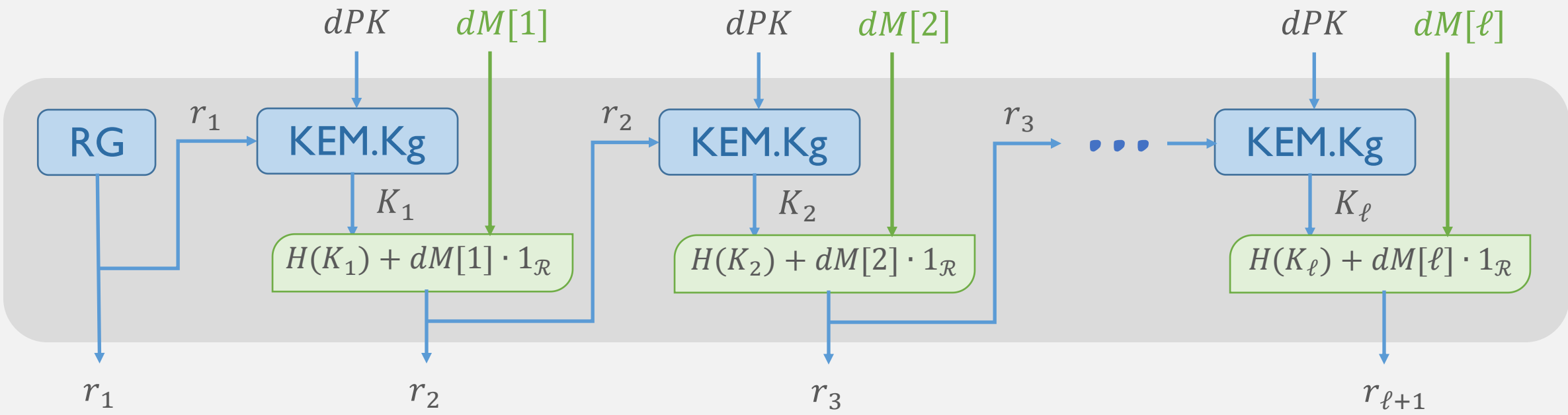
$\leftarrow b'$

$$|\mathbf{Pr}[b' = b] - 1/2| \leq \mathbf{negl}(n)$$



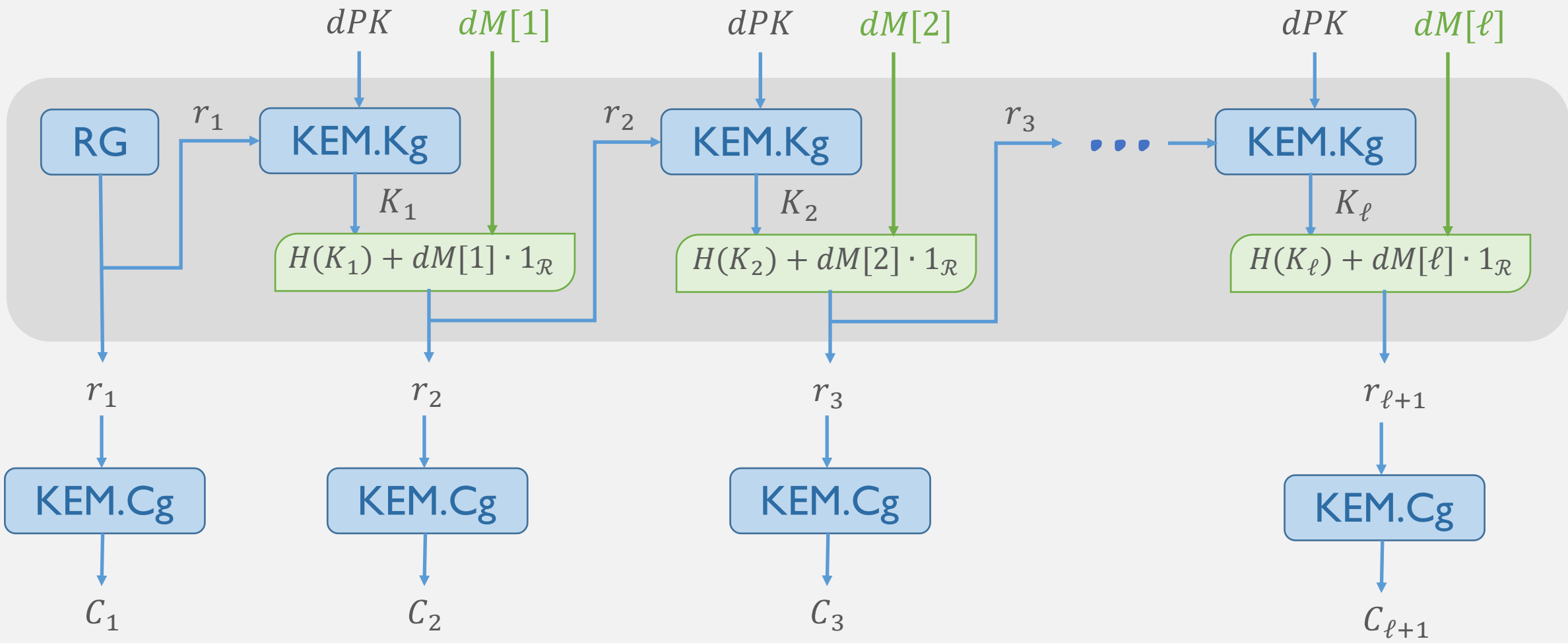
Construction II : Hybrid PKE with Special KEM

- fRandom algorithm



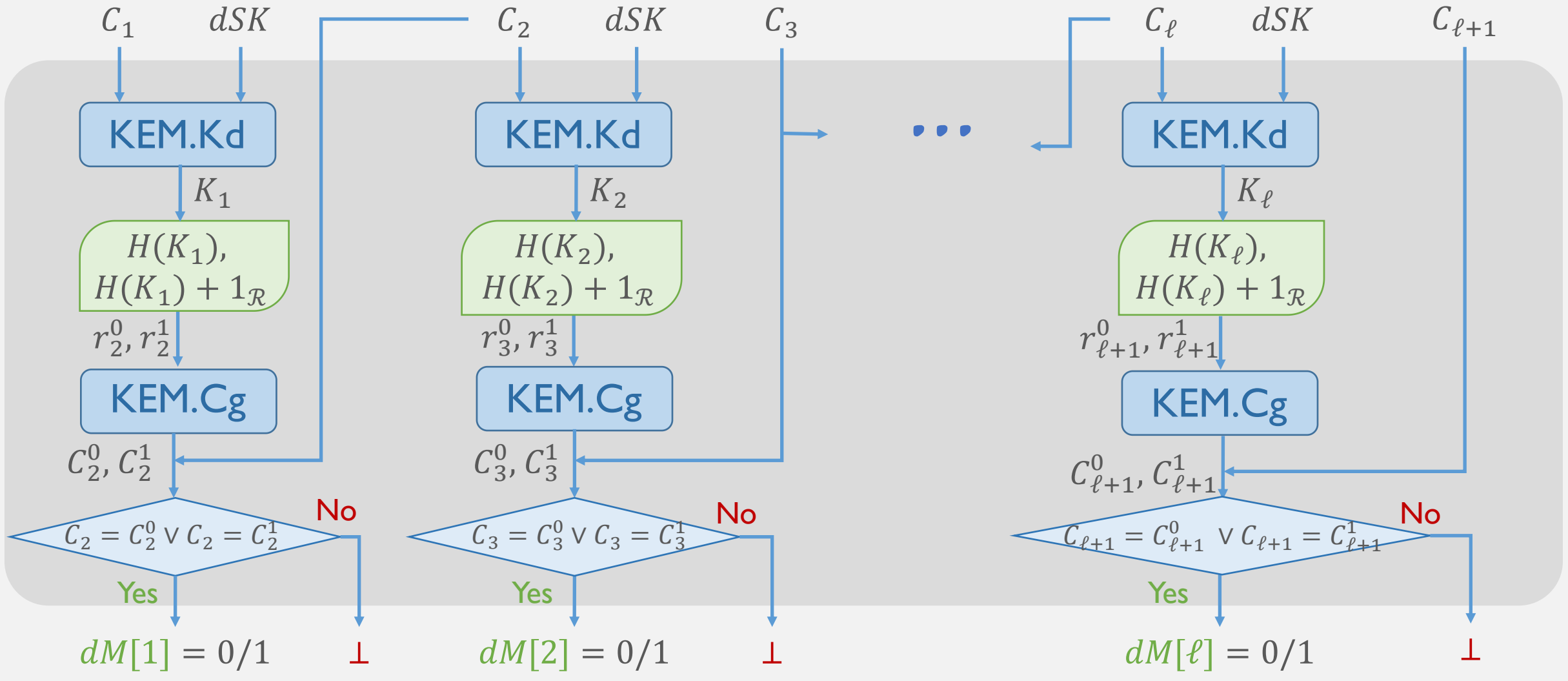
Construction II : Hybrid PKE with Special KEM

- fRandom algorithm

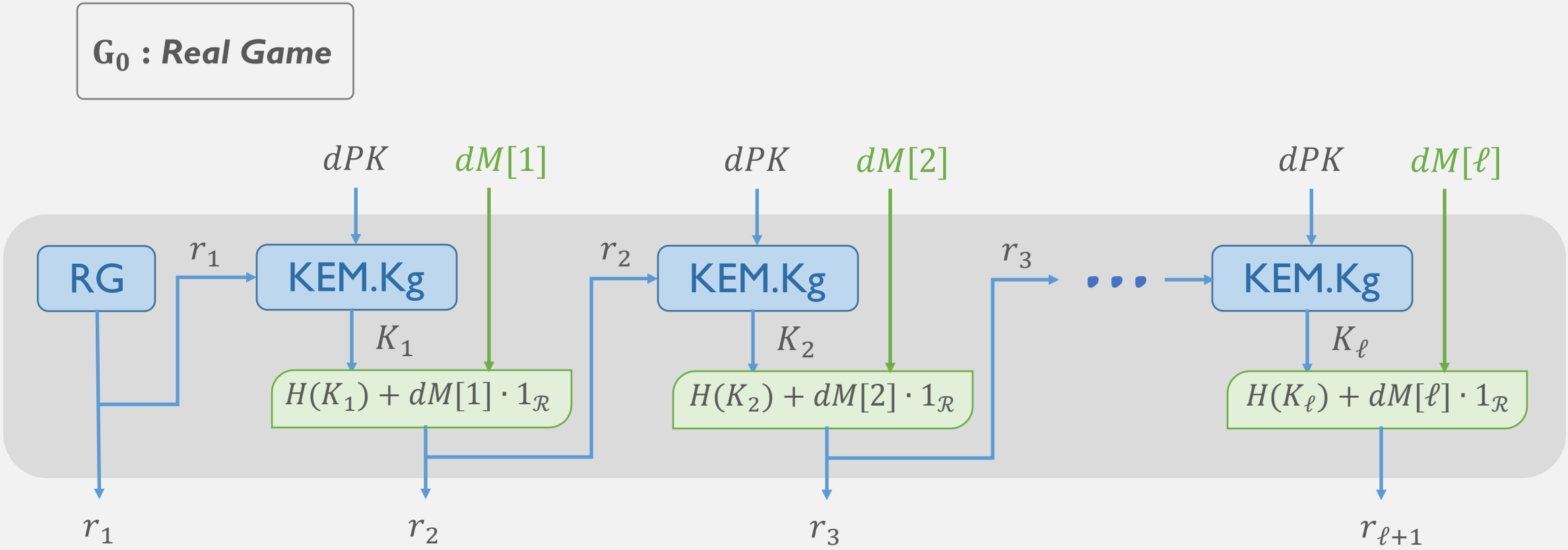


Construction II : Robustness

- dDec algorithm



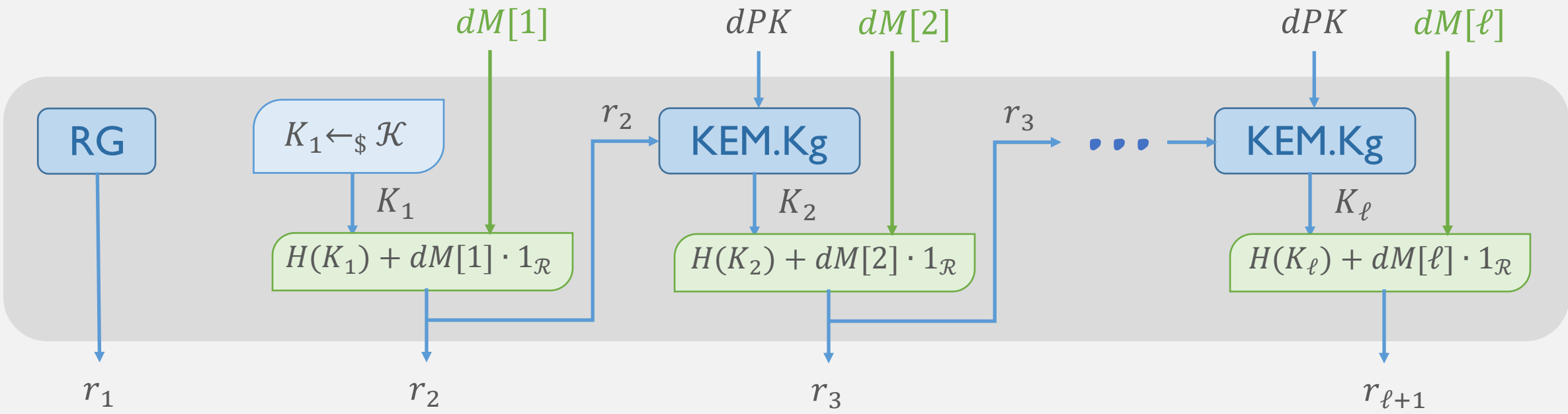
Construction II : Security



Construction II : Security

G_1 : *Replace K_1 with random key*

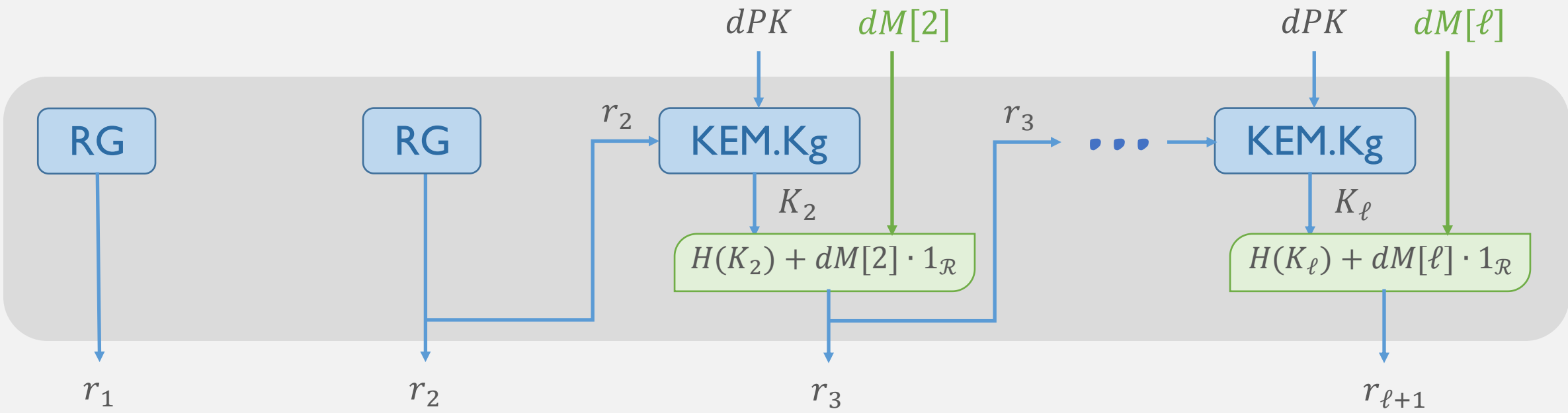
Key Pseudorandomness of KEM



Construction II : Security

G_2 : *Generate* r_2 *using RG*

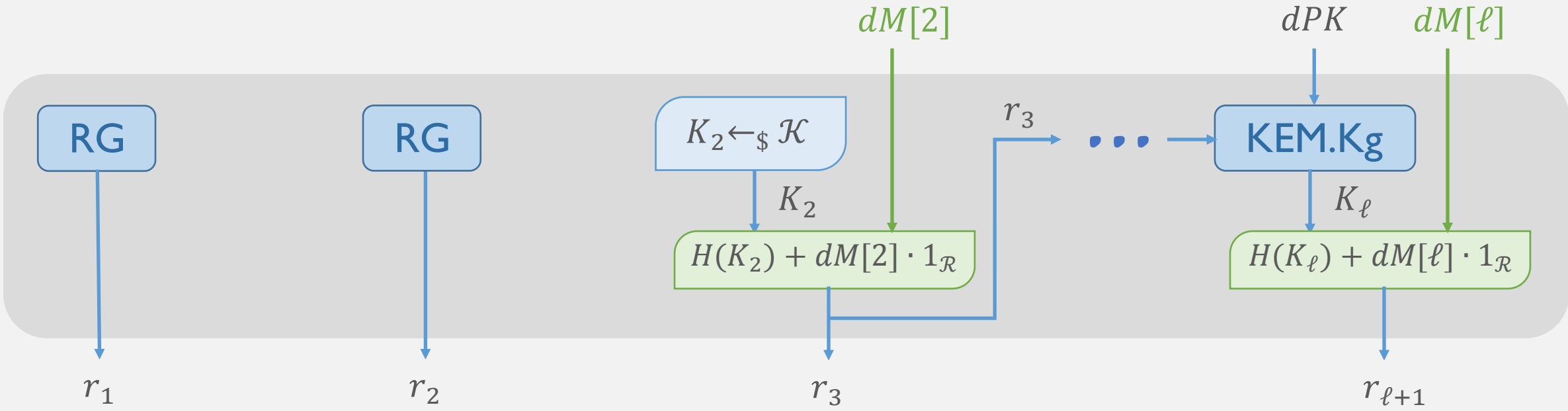
Entropy Smoothness of Hash Function Family



Construction II : Security

G_3 : *Replace* K_2 *with random key*

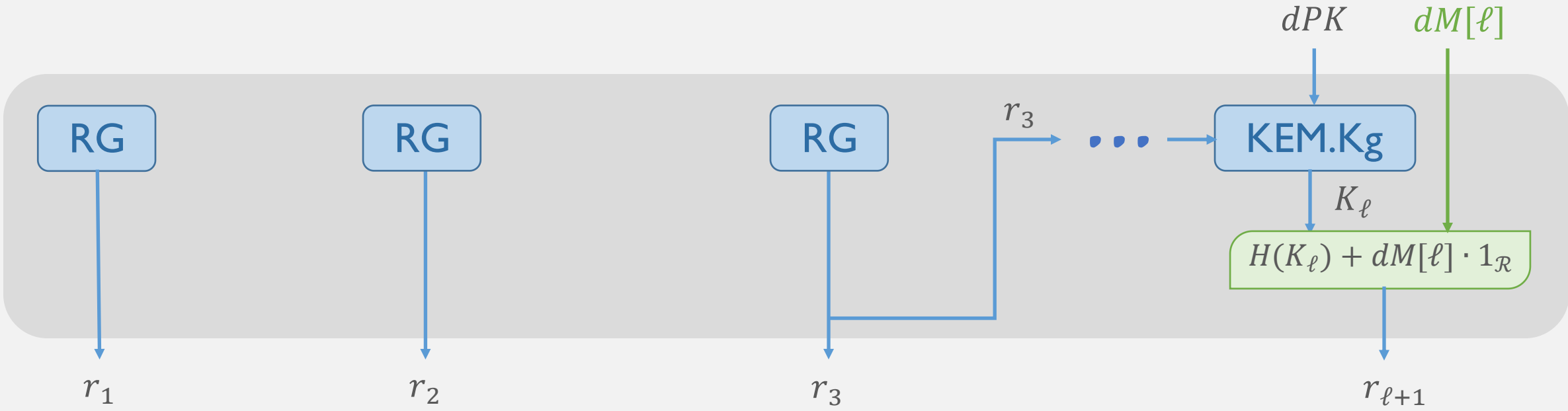
Key Pseudorandomness of KEM



Construction II : Security

$\mathbf{G_4}$: *Generate* r_3 *using RG*

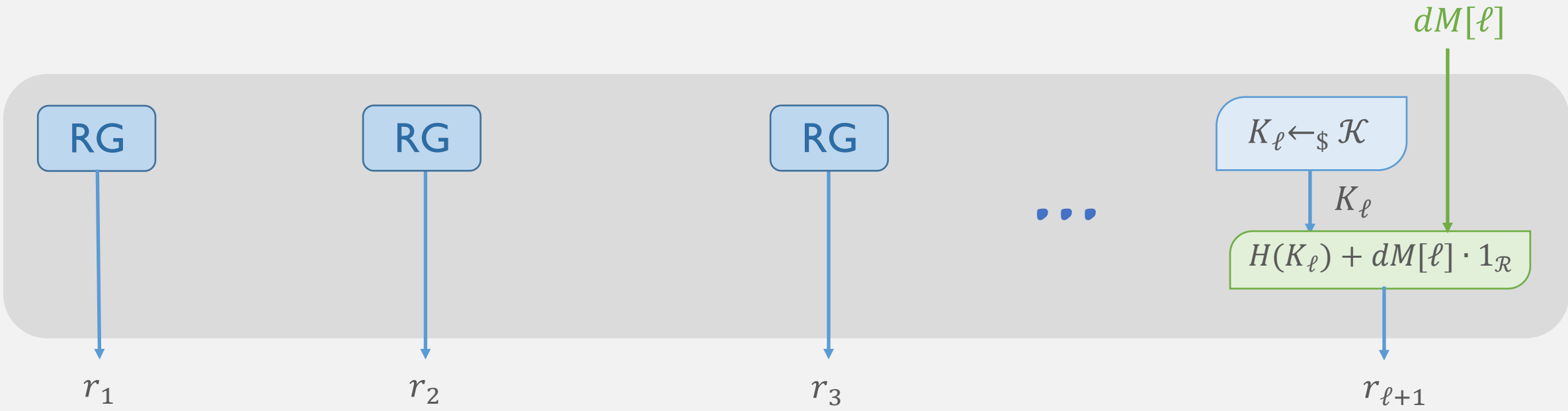
Entropy Smoothness of Hash Function Family



Construction II : Security

$\mathbf{G}_{2\ell-1}$: *Replace* K_ℓ *with random key*

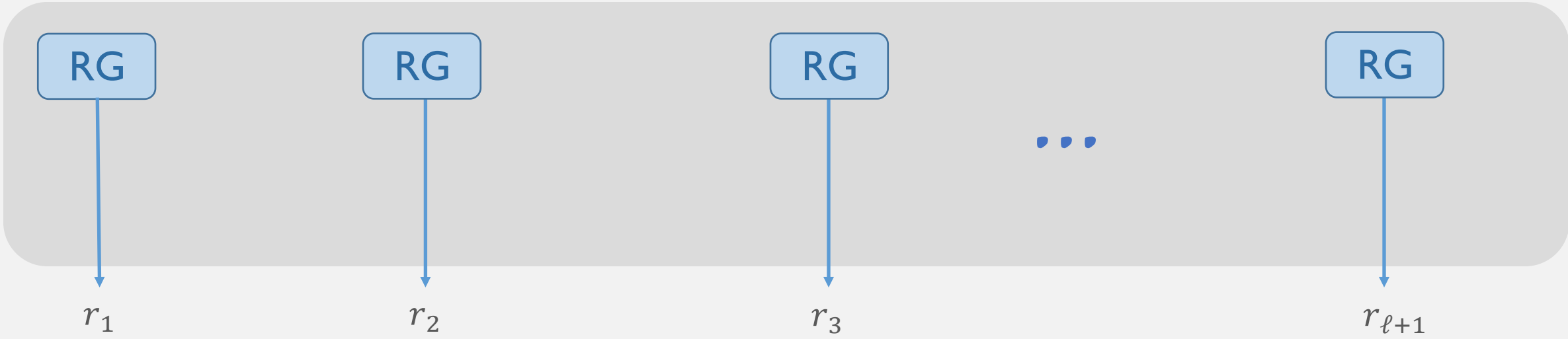
Key Pseudorandomness of KEM



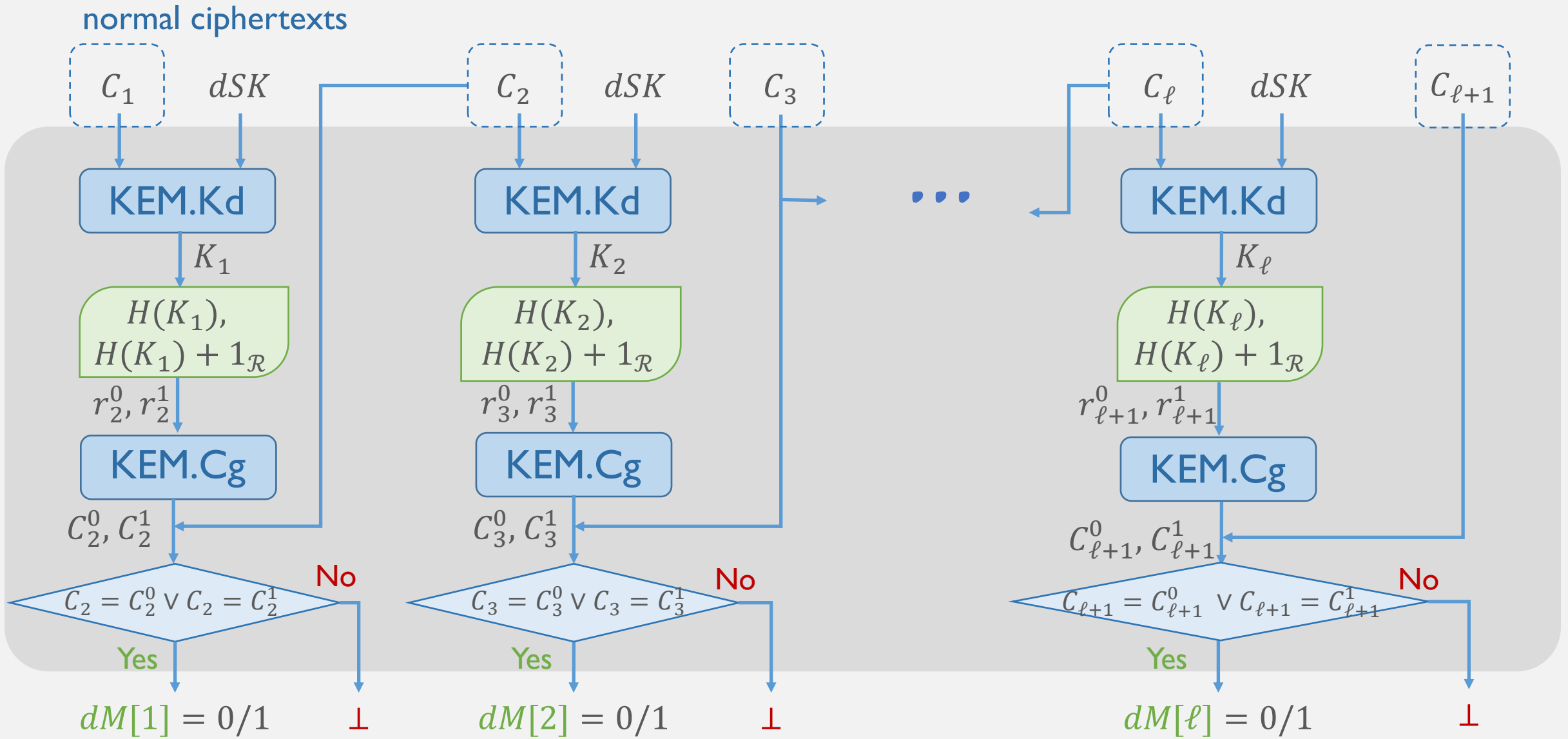
Construction II : Security

$\mathbf{G}_{2\ell}$: *Generate* $r_{\ell+1}$ *using RG (Ideal Game)*

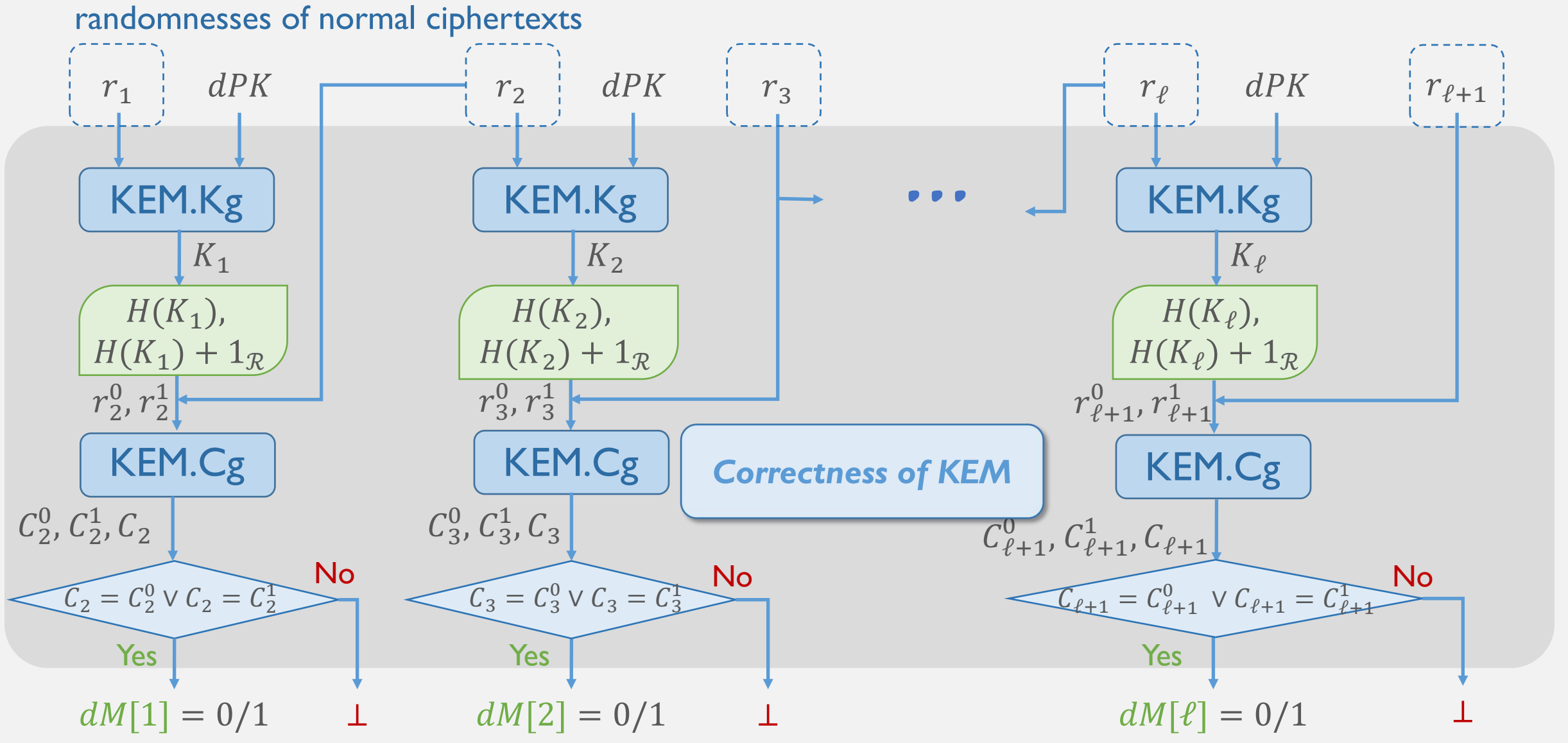
Entropy Smoothness of Hash Function Family



Construction II : Robustness

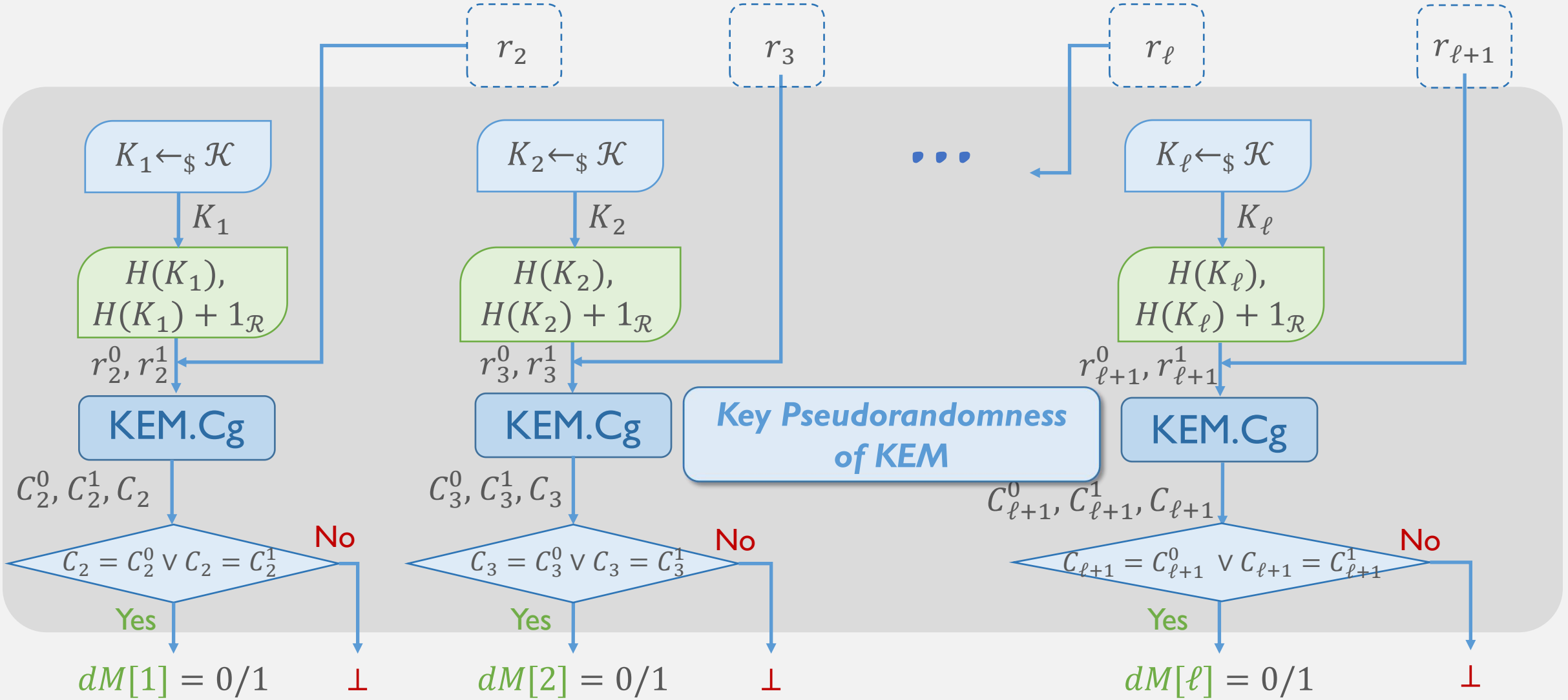


Construction II : Robustness



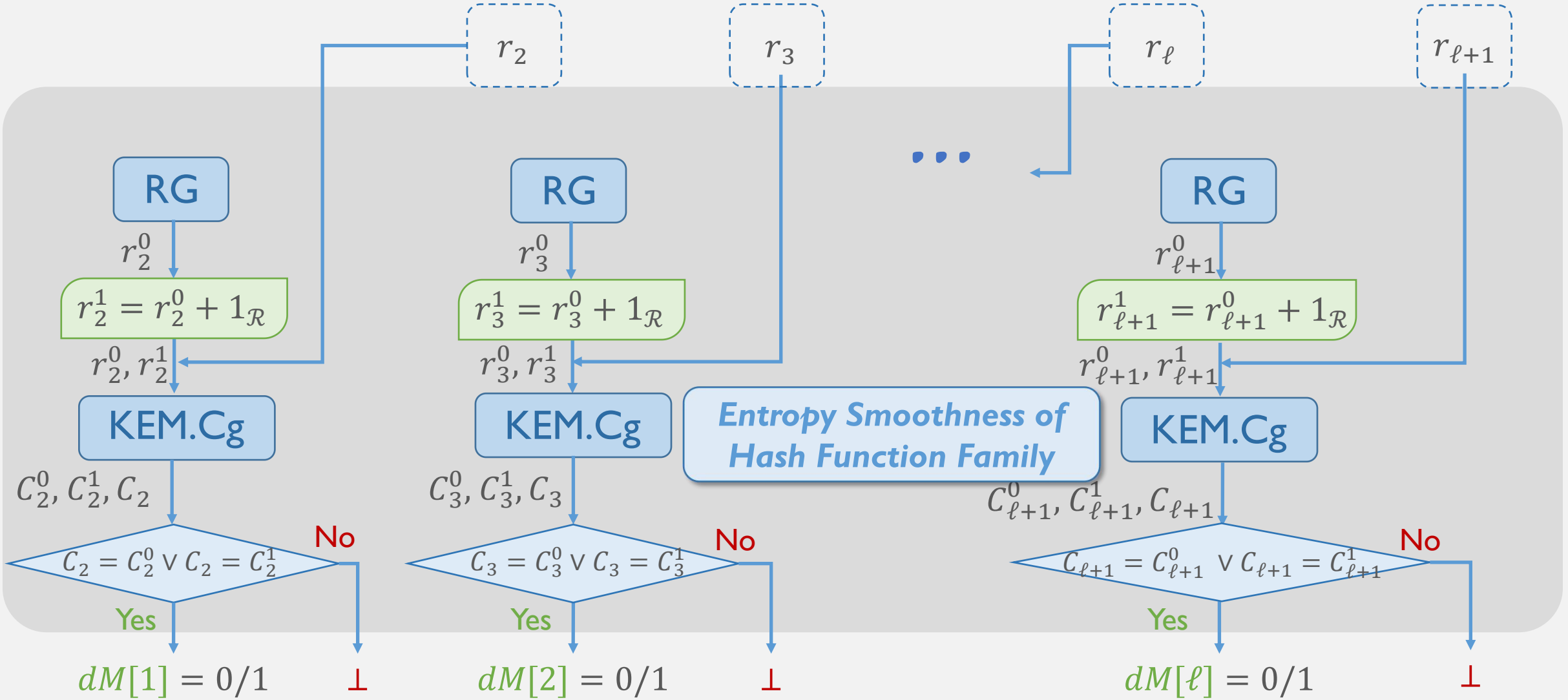
Construction II : Robustness

randomnesses of normal ciphertexts

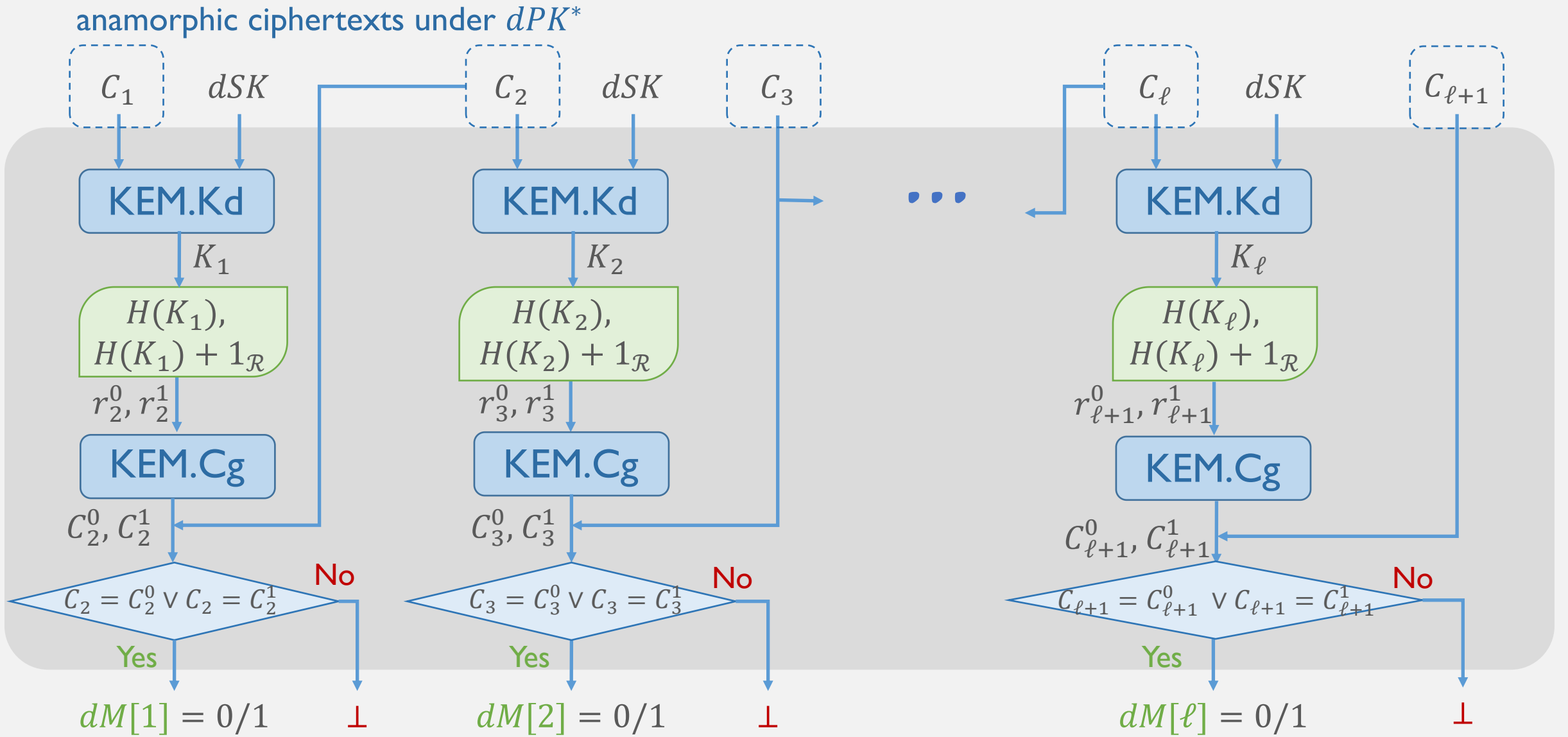


Construction II : Robustness

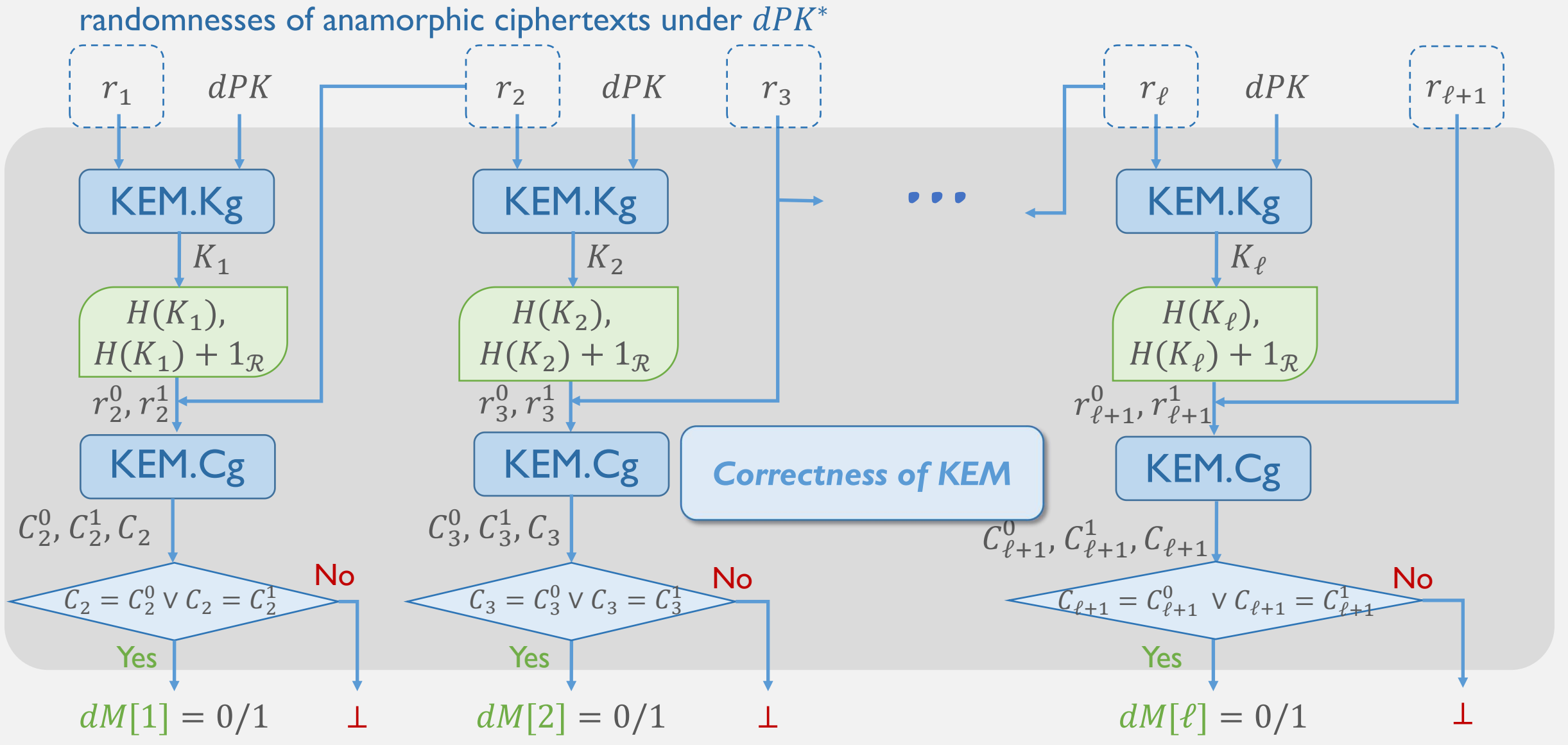
randomnesses of normal ciphertexts



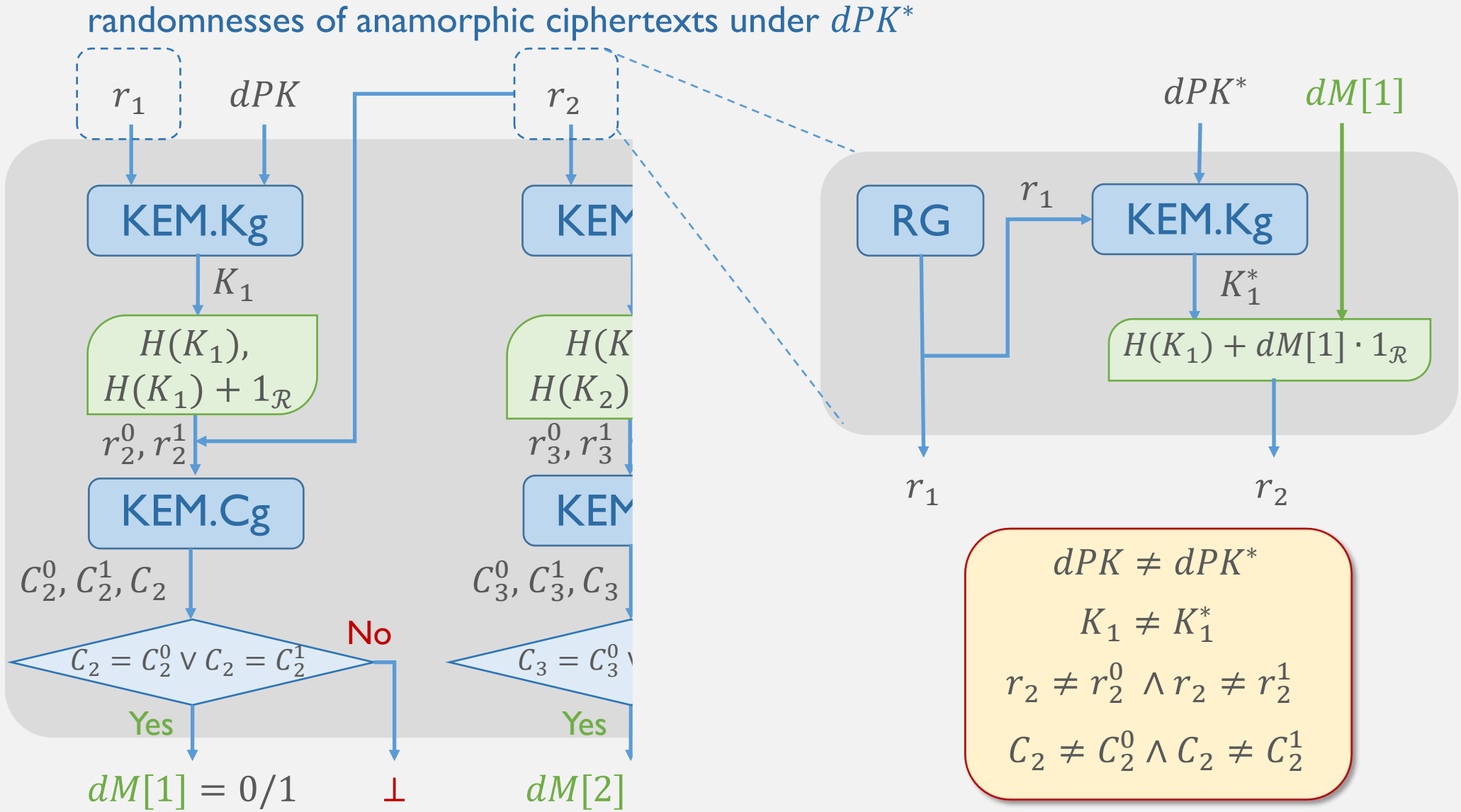
Construction II : Robustness



Construction II : Robustness

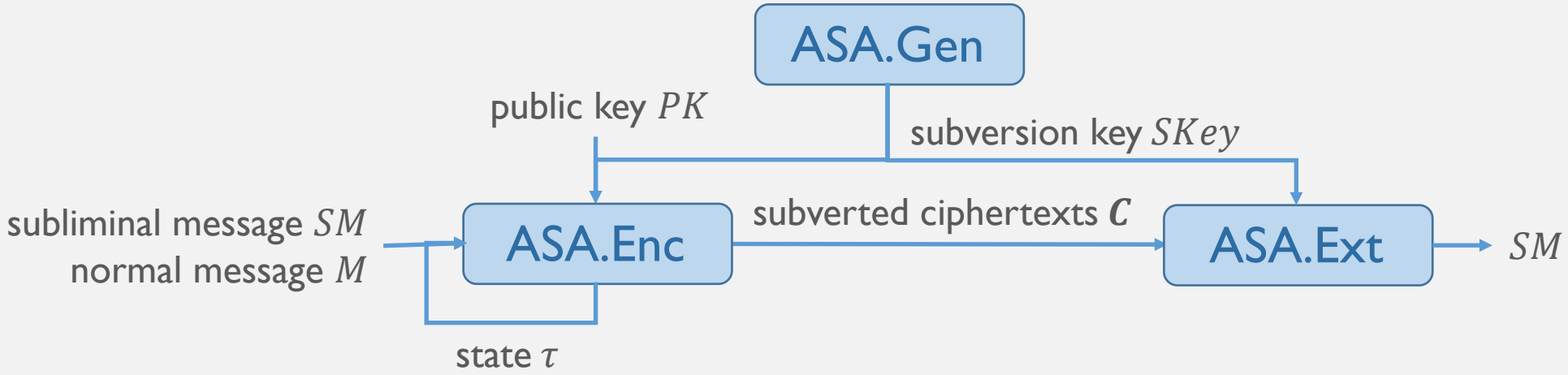


Construction II : Robustness



Construction II : Conclusion

- Generalized Algorithm-Substitution Attack (ASA) on PKE

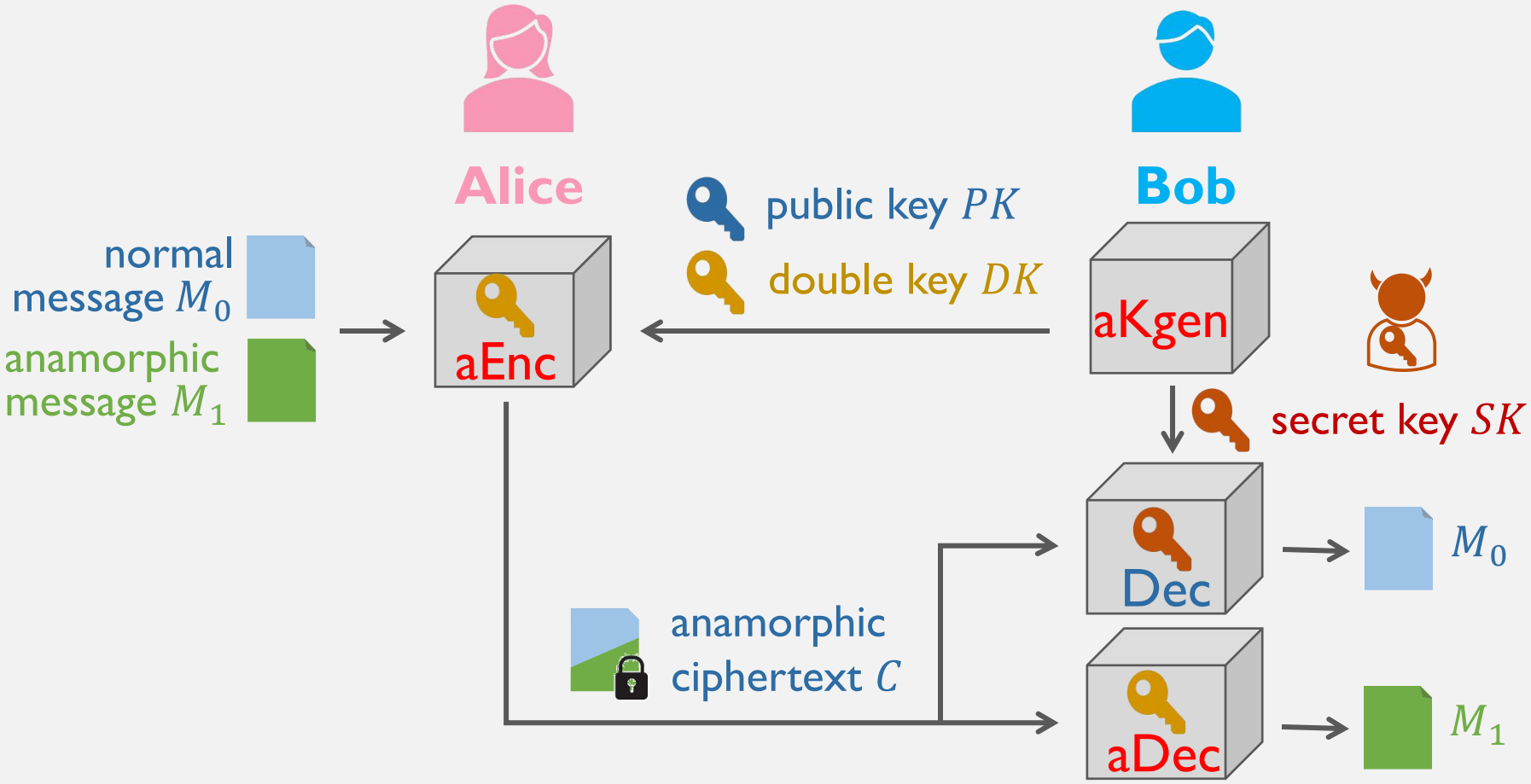


- Relation between ℓ-Sender-AME and generalized ASA on PKE
  - ℓ-Sender-AME $\Rightarrow$ generalized ASA on PKE (Theorem 8.2)
  - generalized ASA on PKE $\not\Rightarrow$ ℓ-Sender-AME

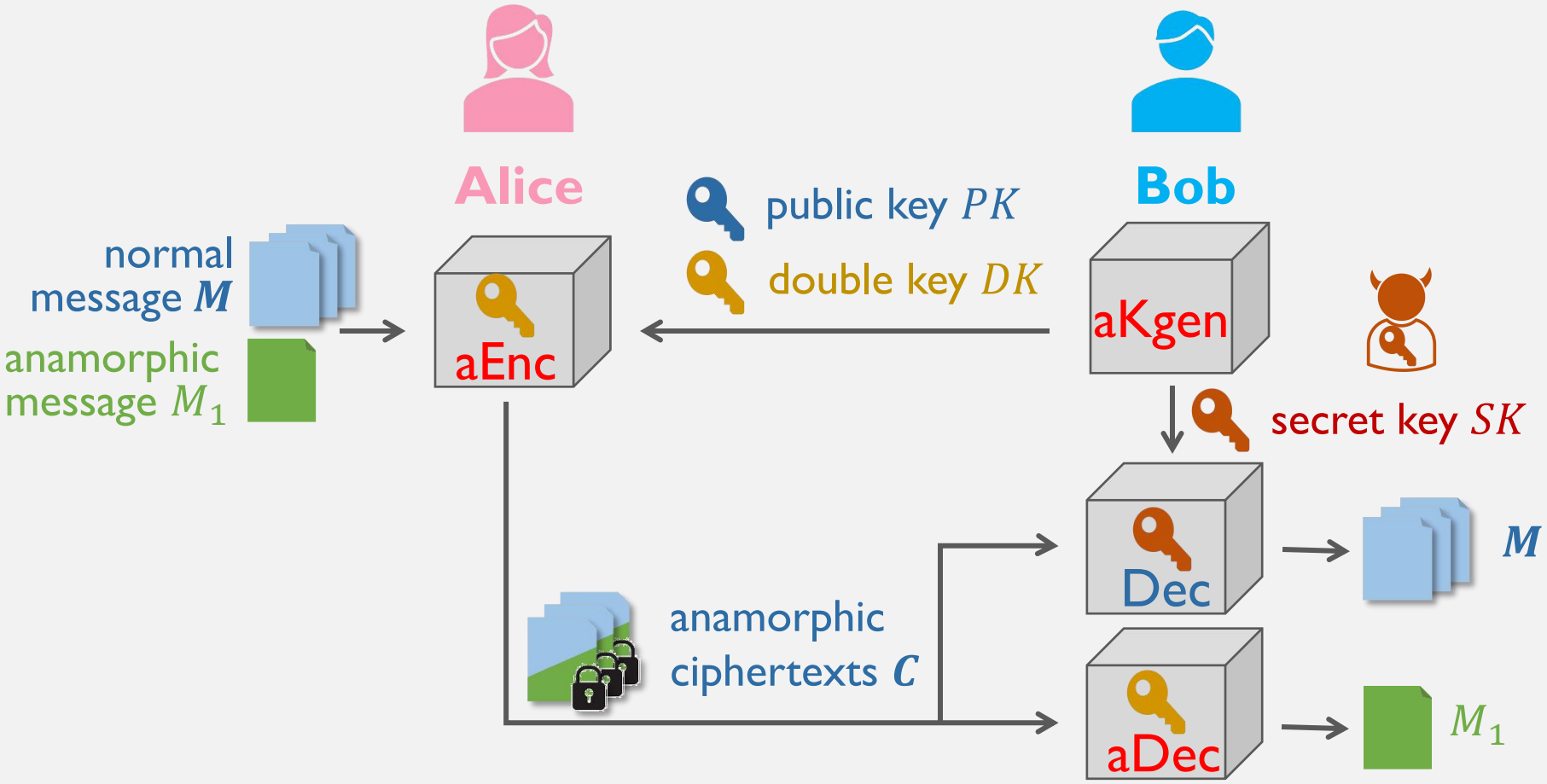
Our Work

- New Formalization
- Generic Constructions
- Relation Exploration

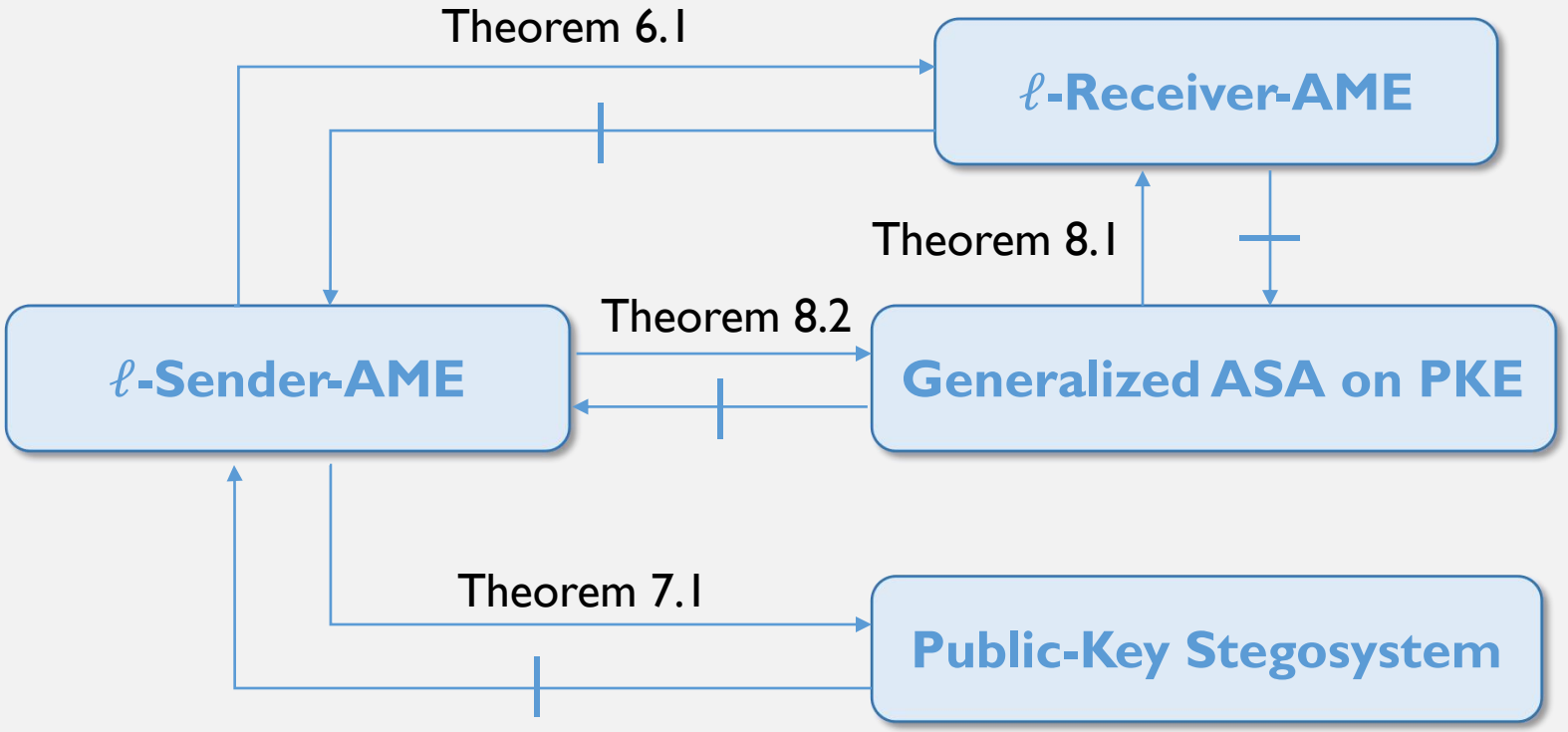
Receiver-Anamorphic Encryption [PPY22]



ℓ-Receiver-Anamorphic Encryption



Relations


Theorem 6.1
ℓ-Receiver-AME
Theorem 8.1
Theorem 8.2
ℓ-Sender-AME
Generalized ASA on PKE
Theorem 7.1
Public-Key Stegosystem

Thanks!

✍ wangyi14@nudt.edu.cn