Updatable Public Key Encryption

From Lattices

Calvin Abou Haidar, Alain Passelègue & Damien Stehlé

Asiacrypt 2023 - 广州

Updatable Public Key Encryption

Plan

Definitions & Secure Messaging

Construction

A new assumption

Introduction

Public Key Encryption

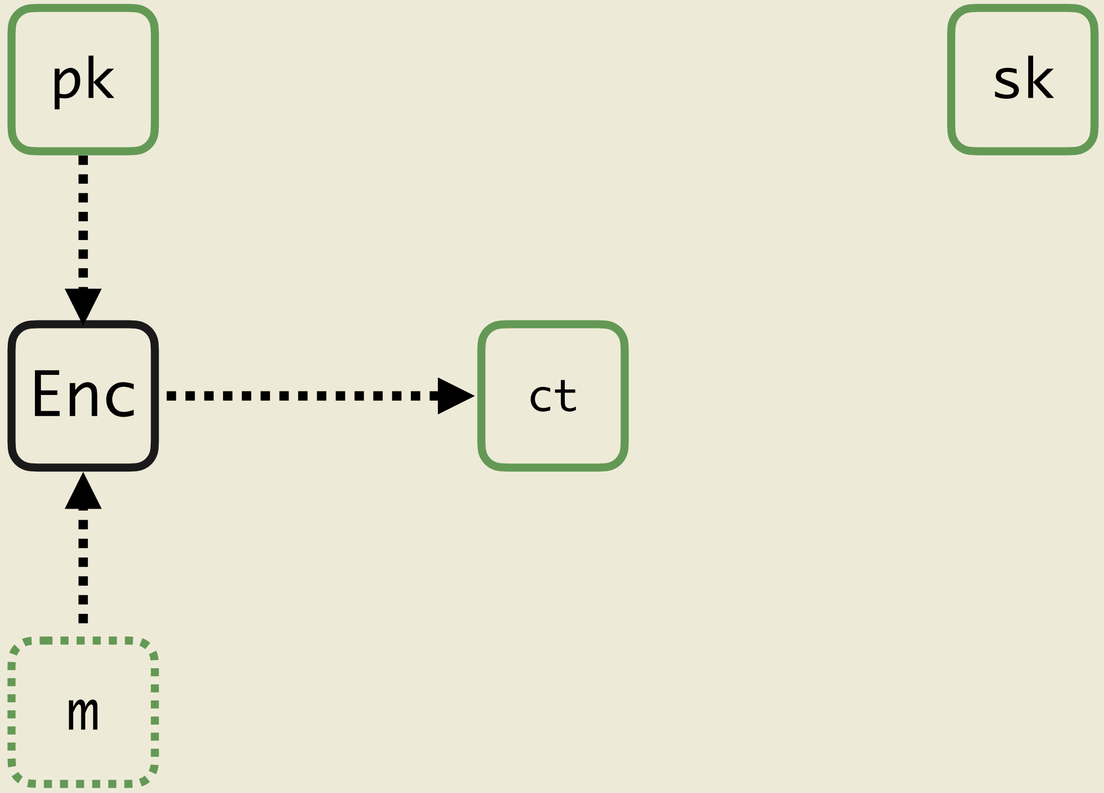
Definition

pk

sk

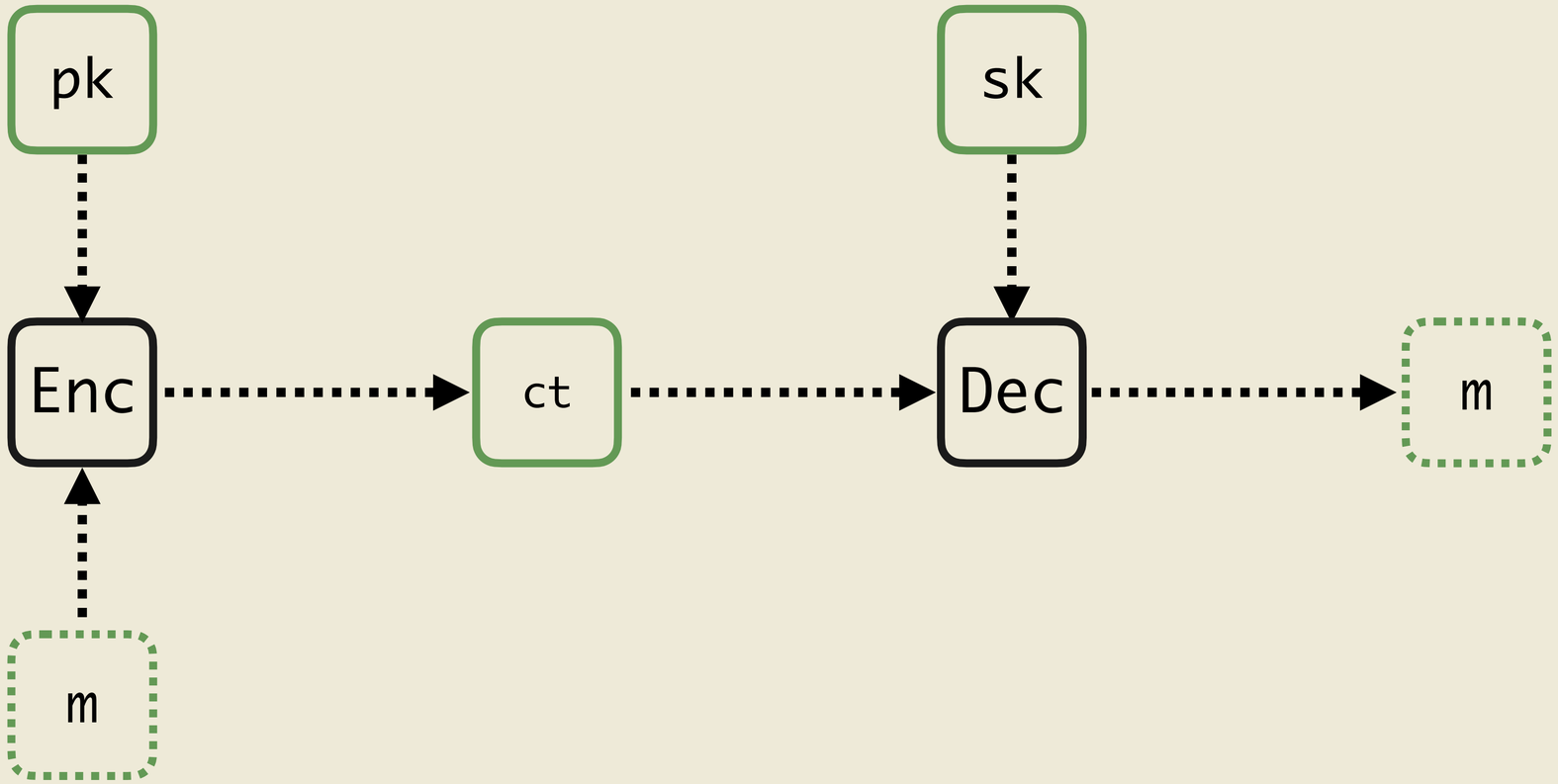
Public Key Encryption

Definition



Public Key Encryption

Definition



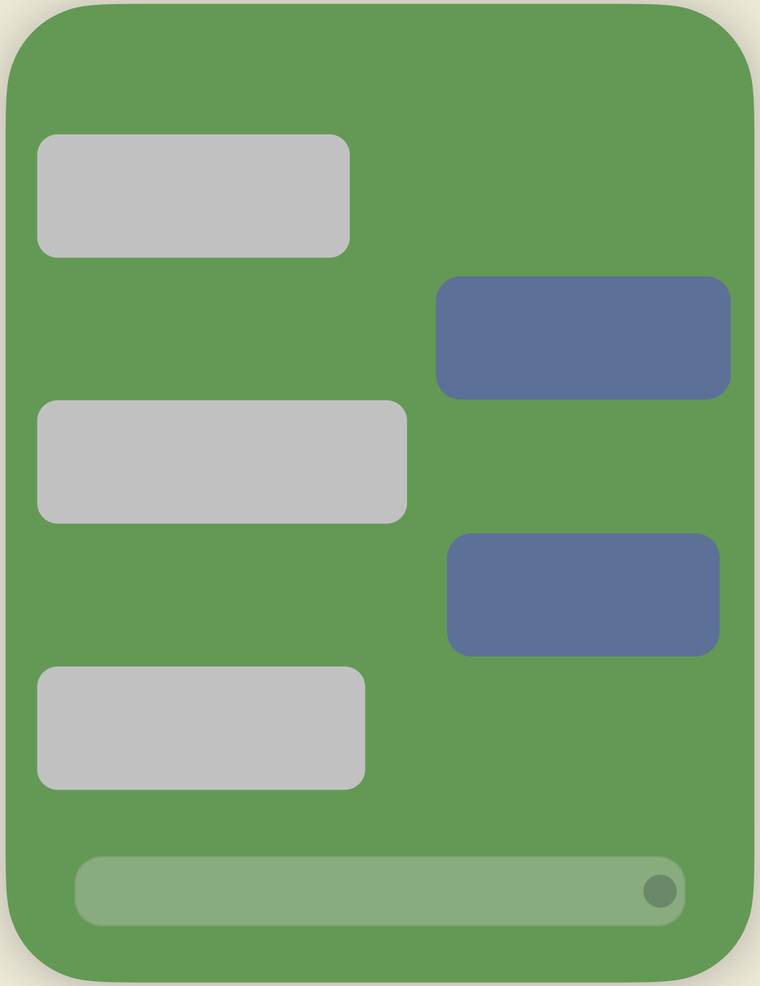
Secure Messaging

A quick introduction

Signal

WhatsApp

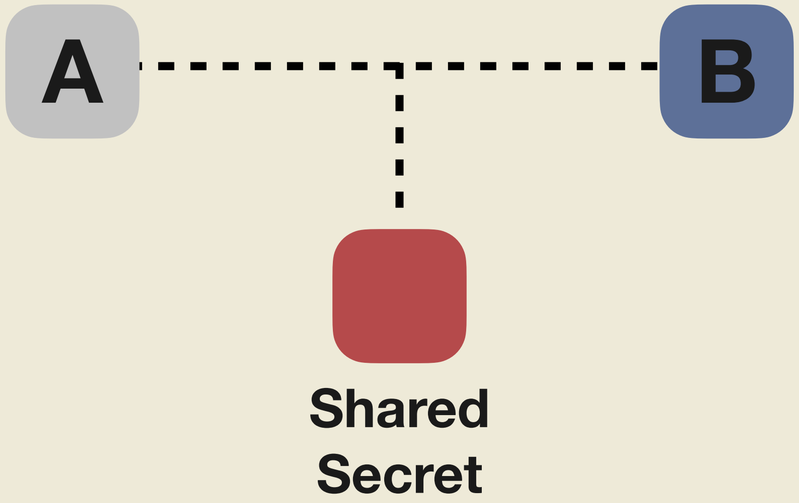
Et al.

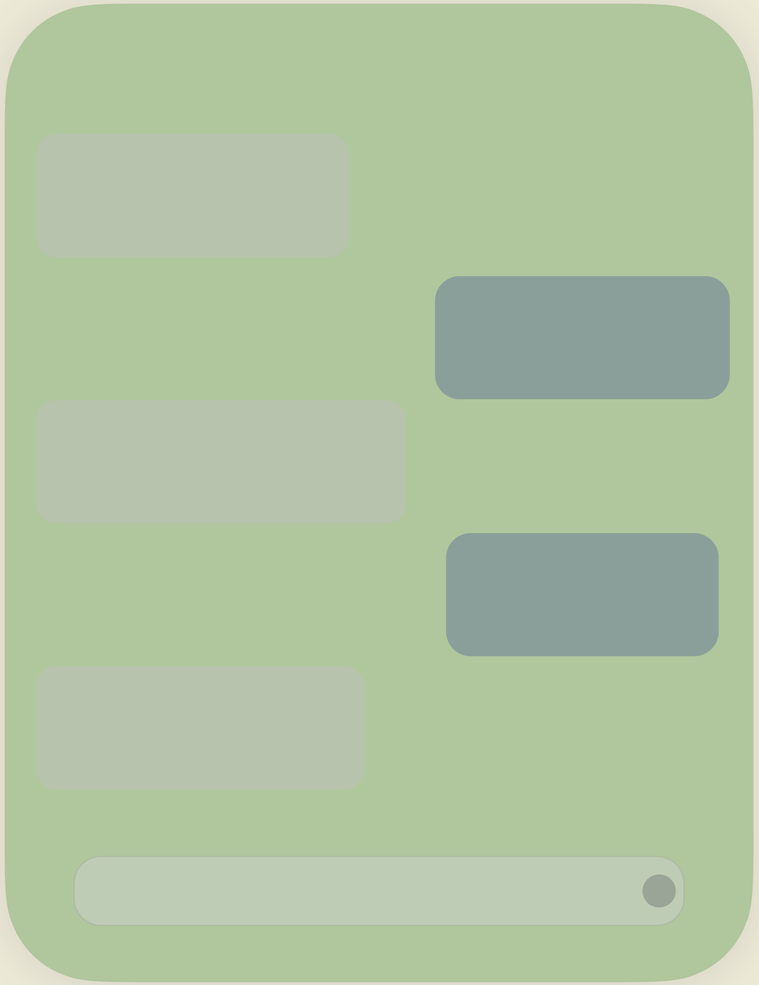


Secure Messaging

A quick introduction

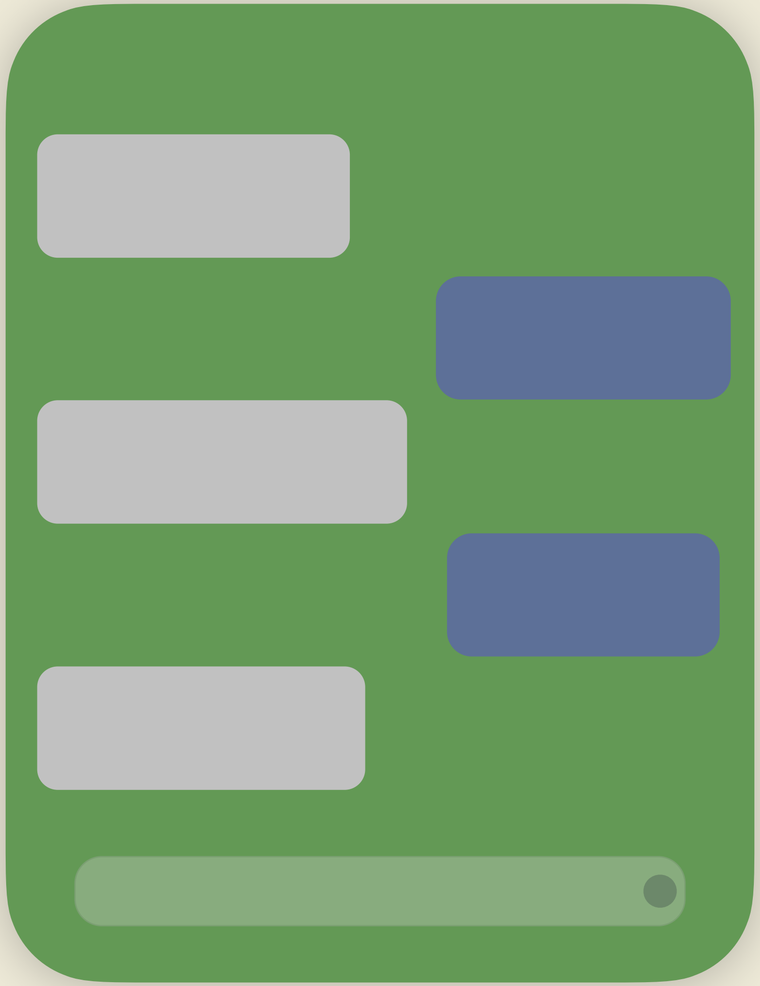
Key Exchange Phase





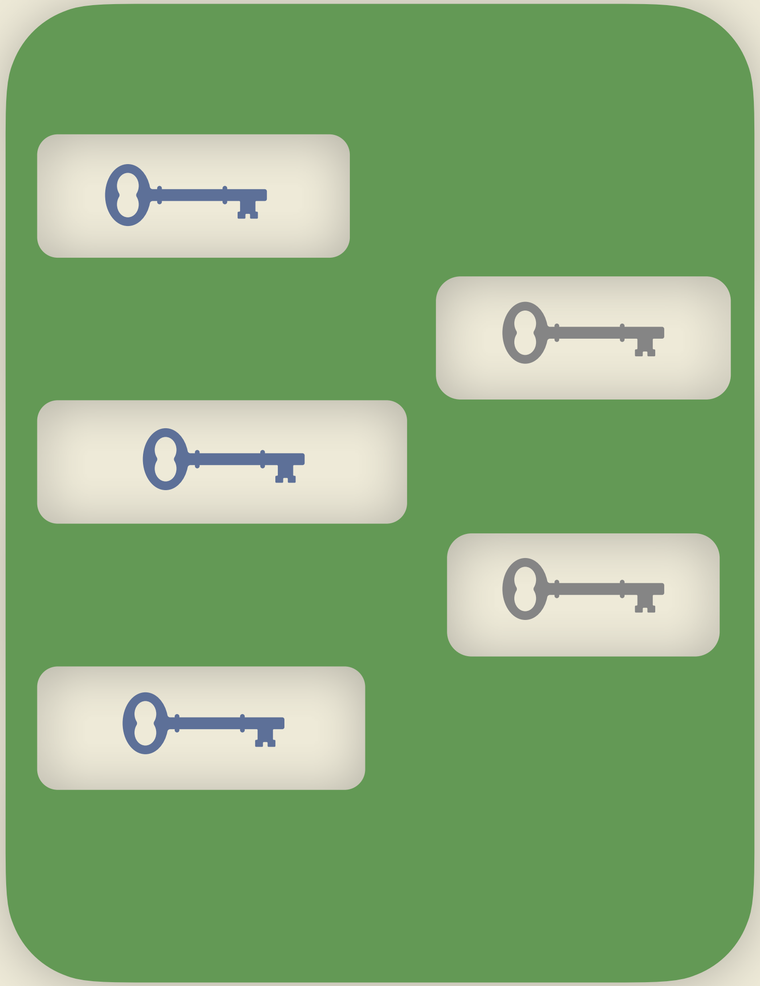
Secure Messaging

A quick introduction



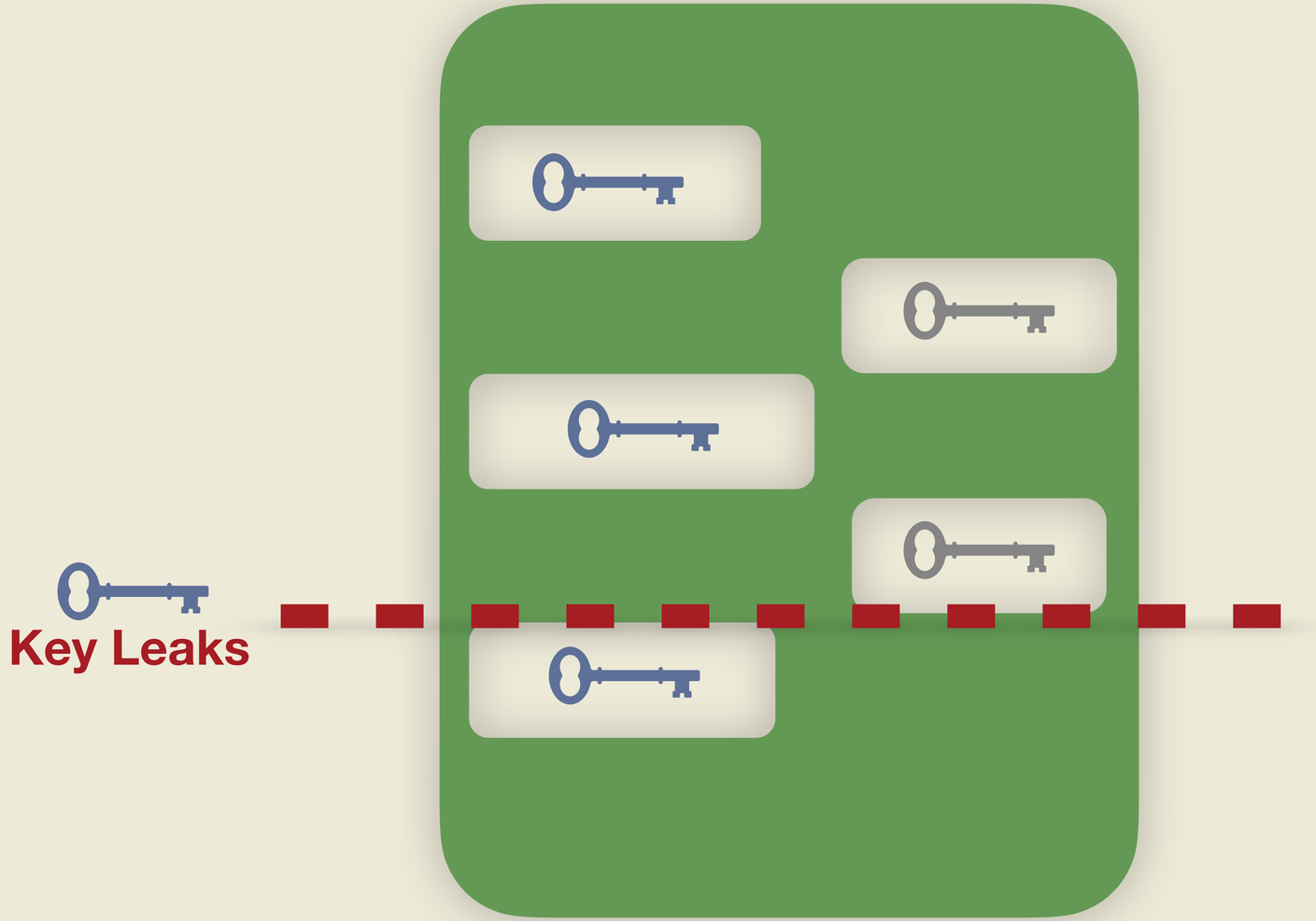
Secure Messaging

A quick introduction



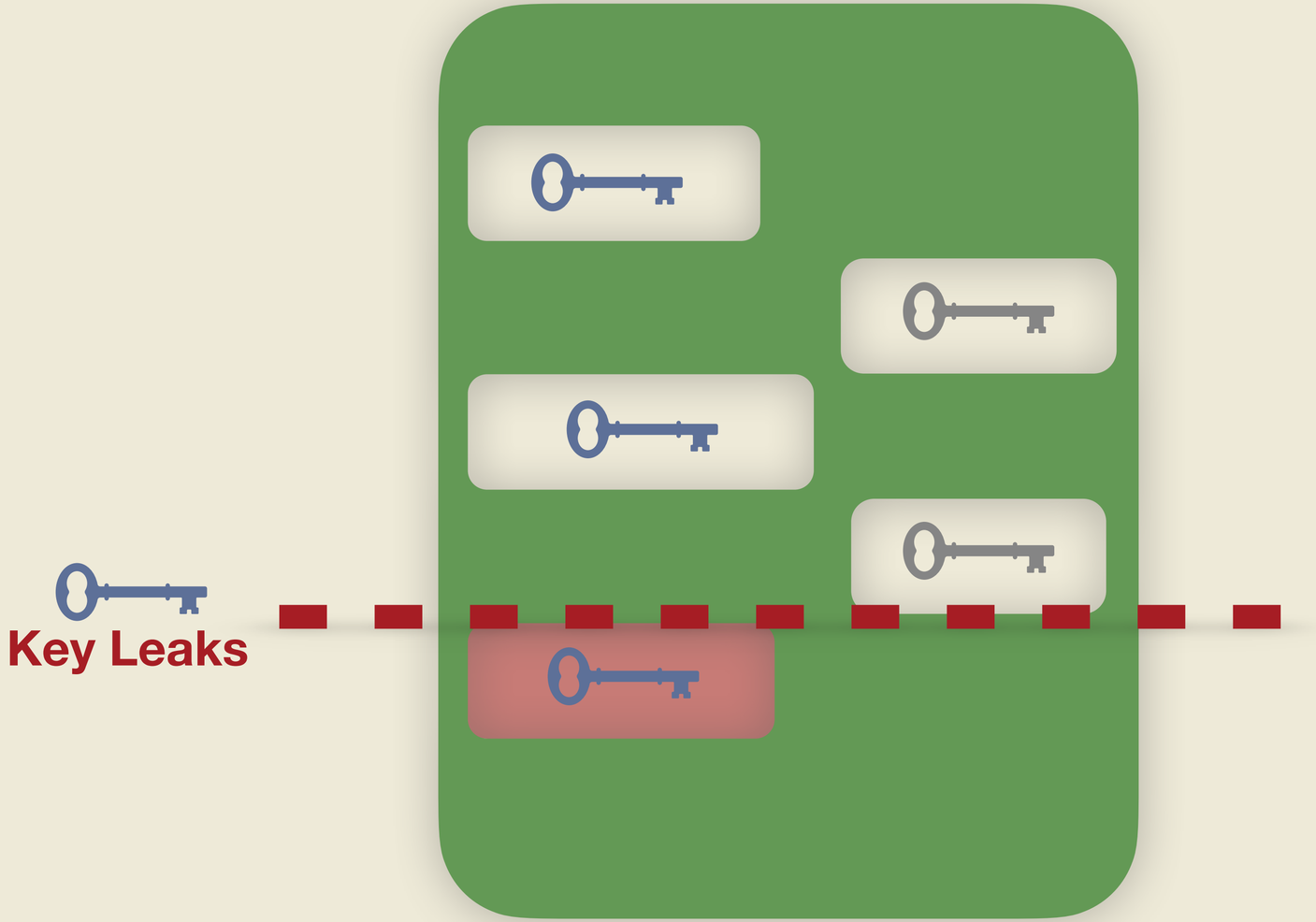
Secure Messaging

A quick introduction



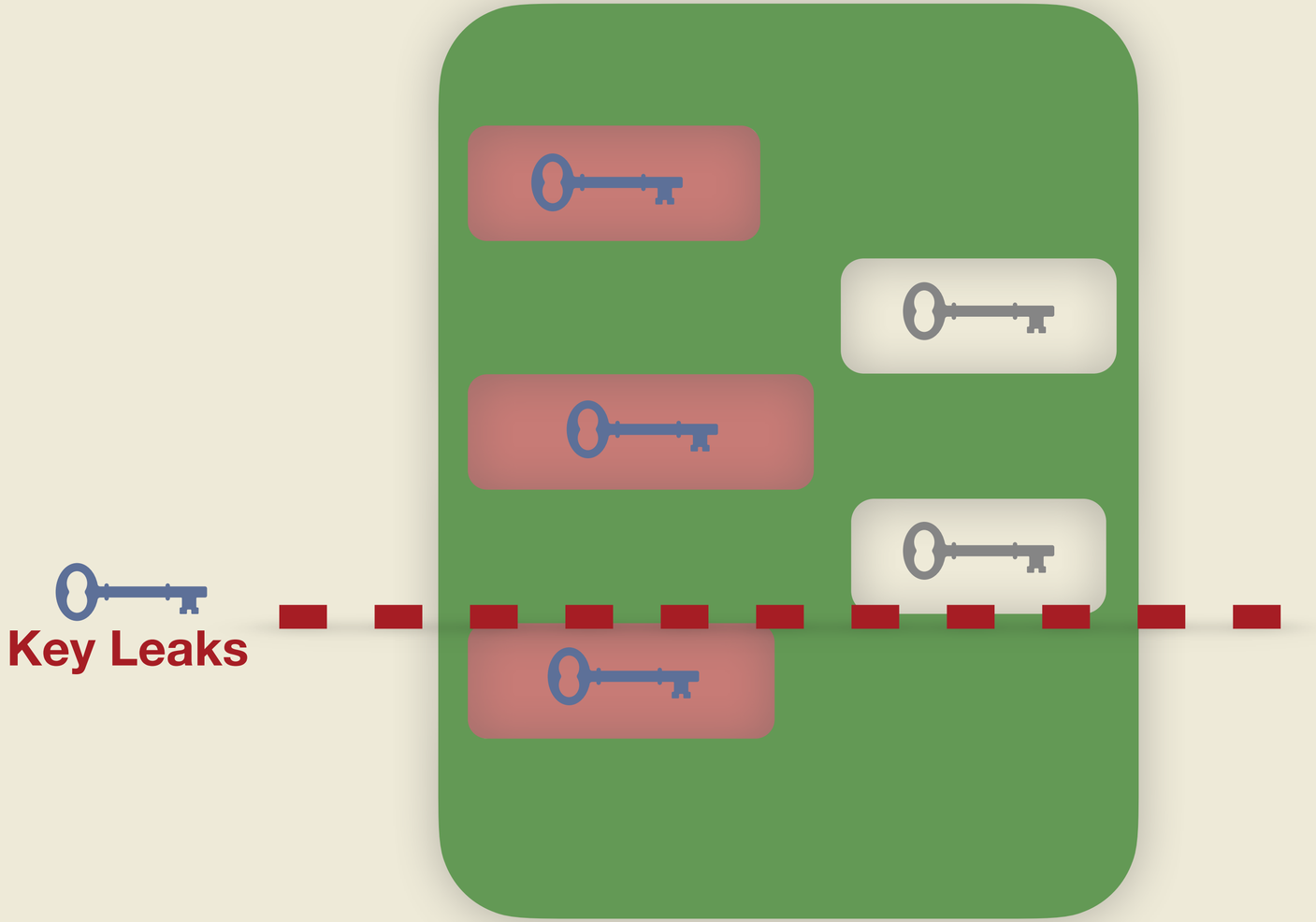
Secure Messaging

A quick introduction



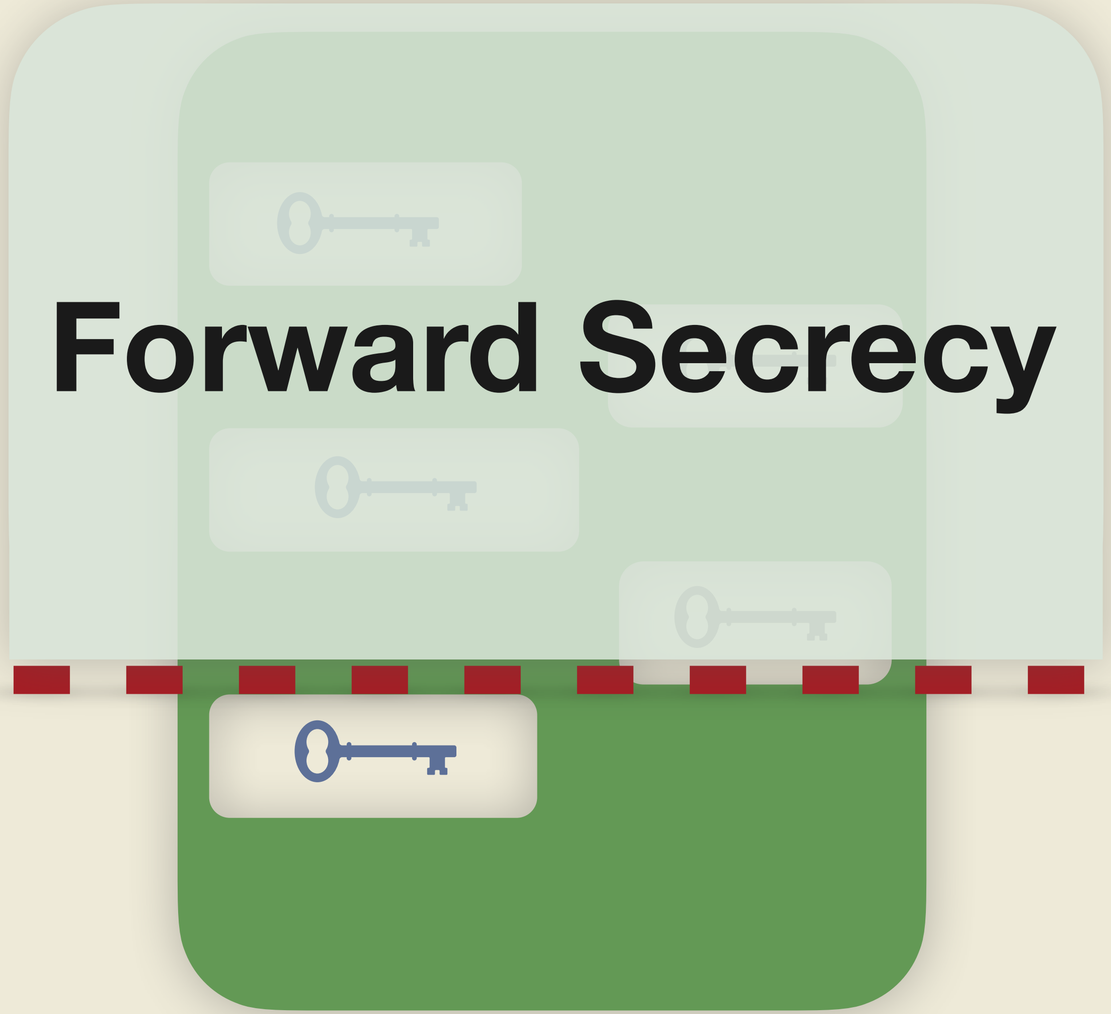
Secure Messaging

A quick introduction



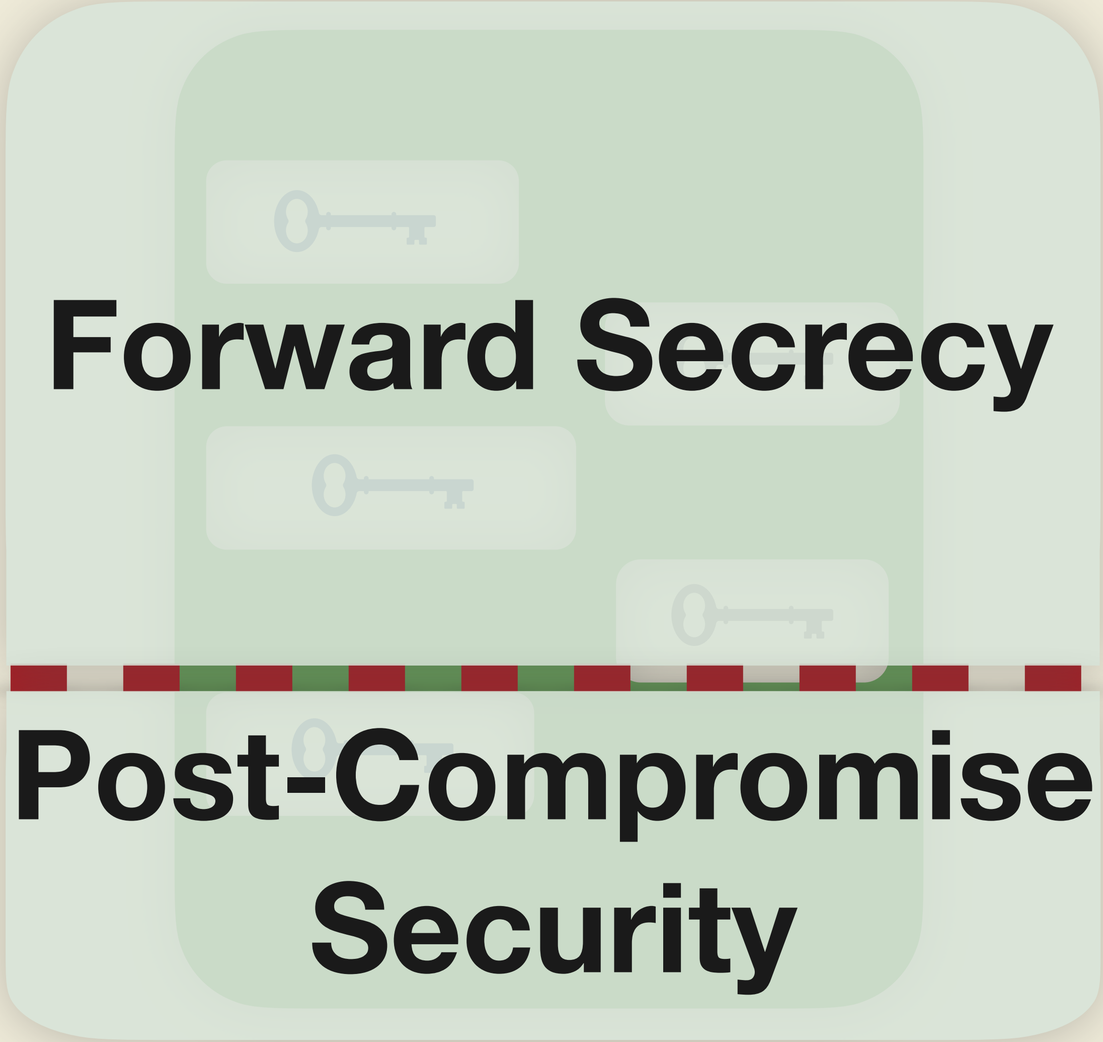
Secure Messaging

A quick introduction



Secure Messaging

A quick introduction

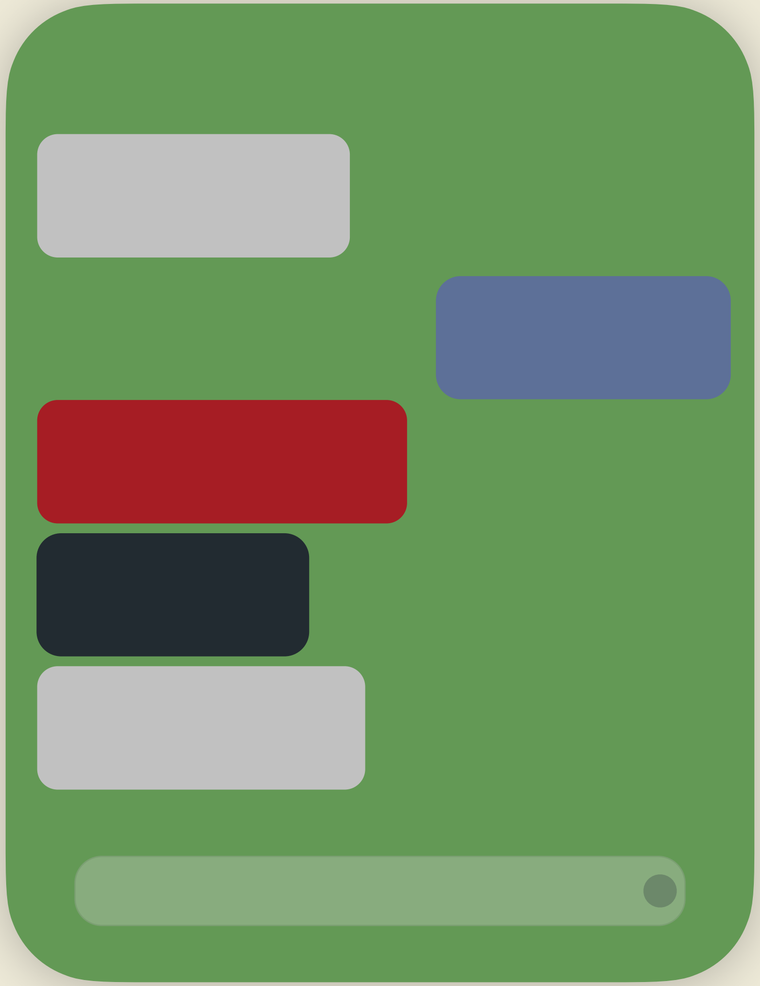


Secure Messaging

A quick introduction

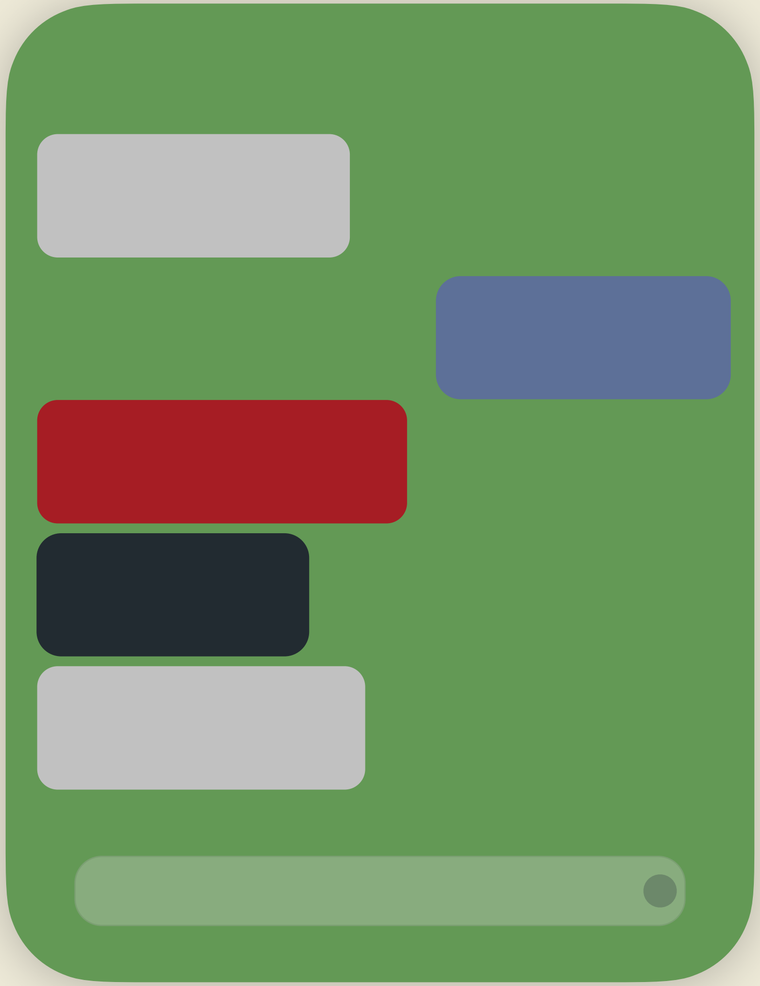
Group Messaging

Here comes trouble



Group Messaging

Here comes trouble

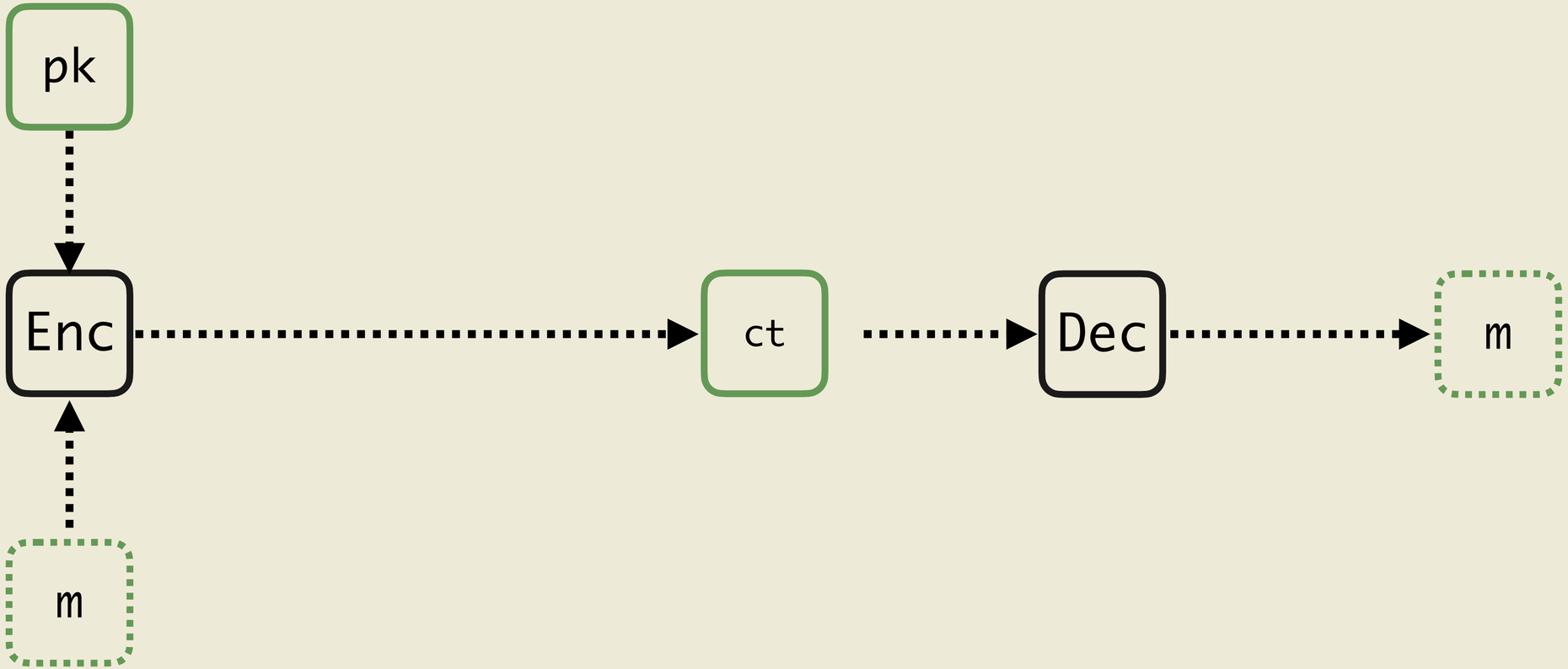


Need to update other user's key to ensure forward secrecy

Definition

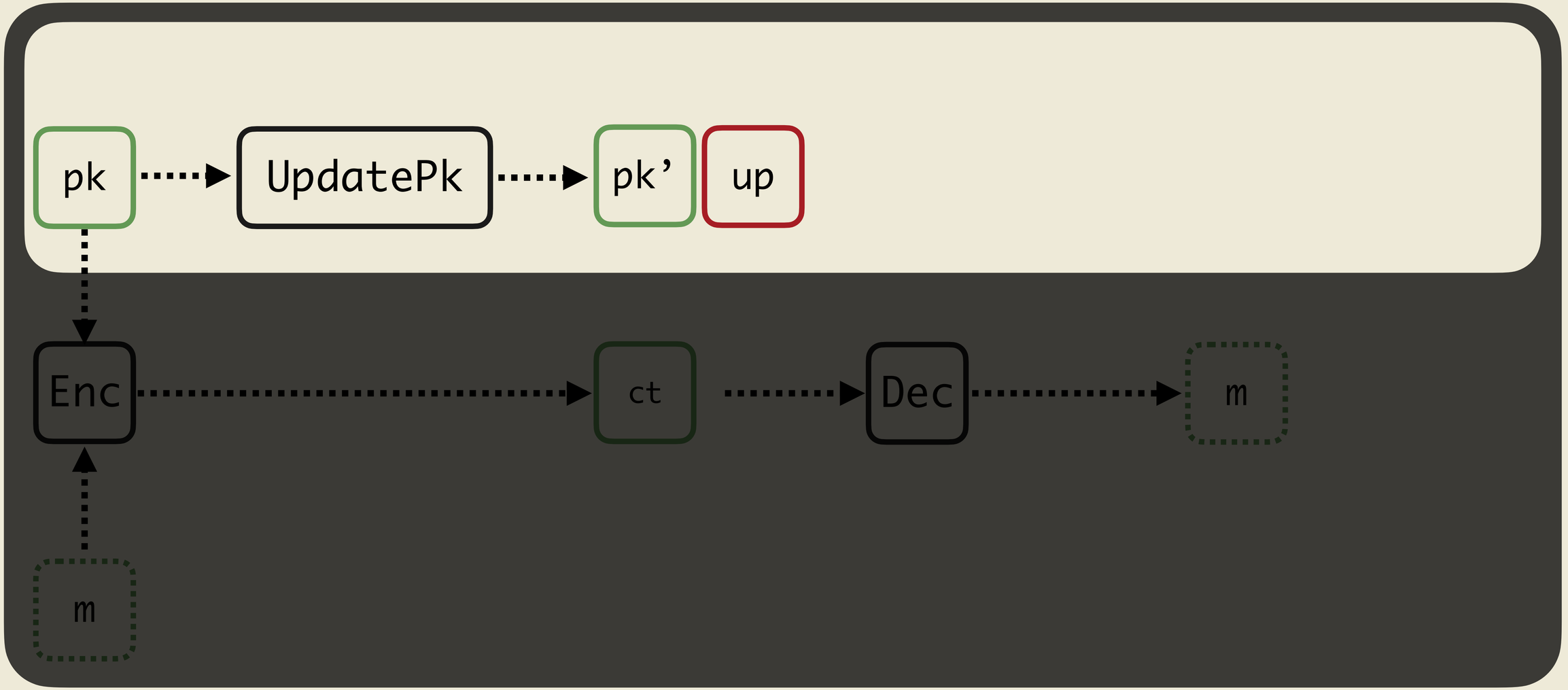
Updatable Public Key Encryption

Definition



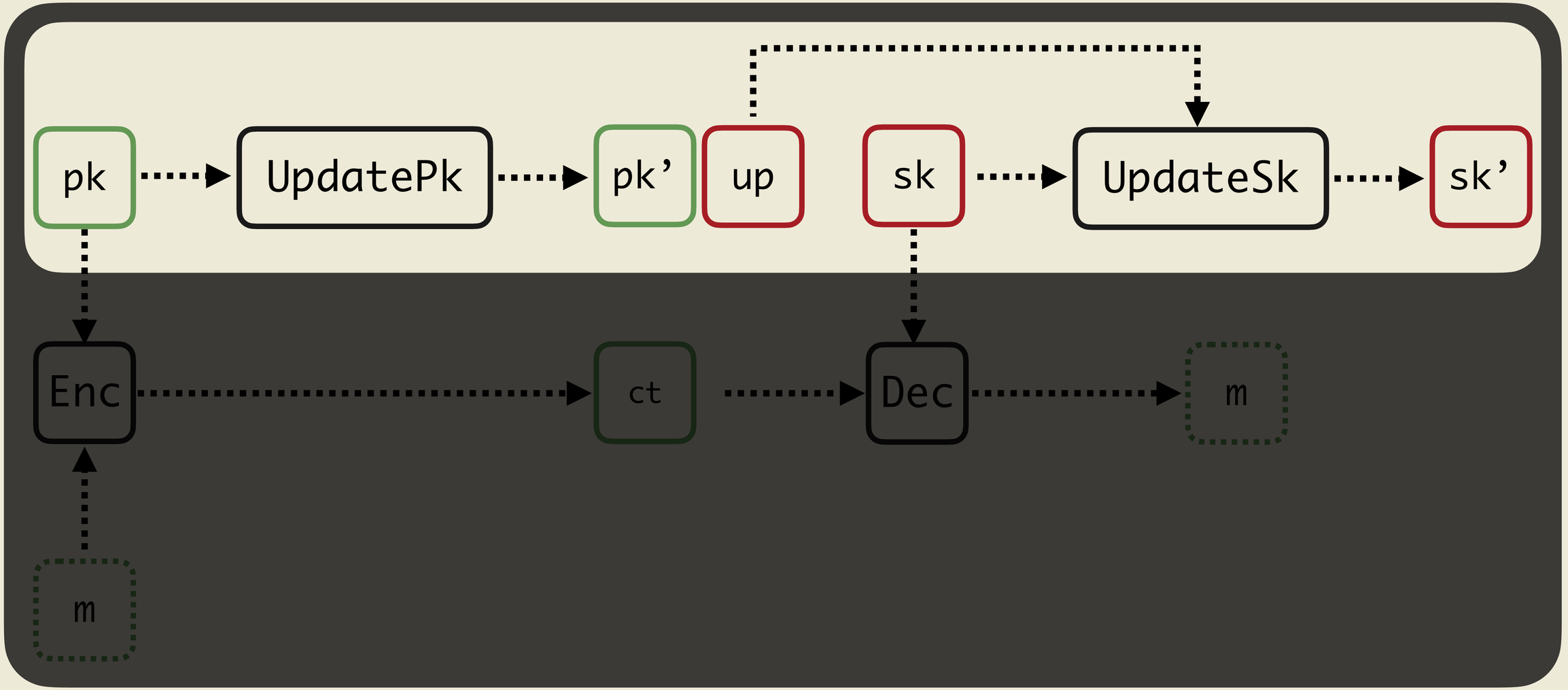
Updatable Public Key Encryption

Definition



Updatable Public Key Encryption

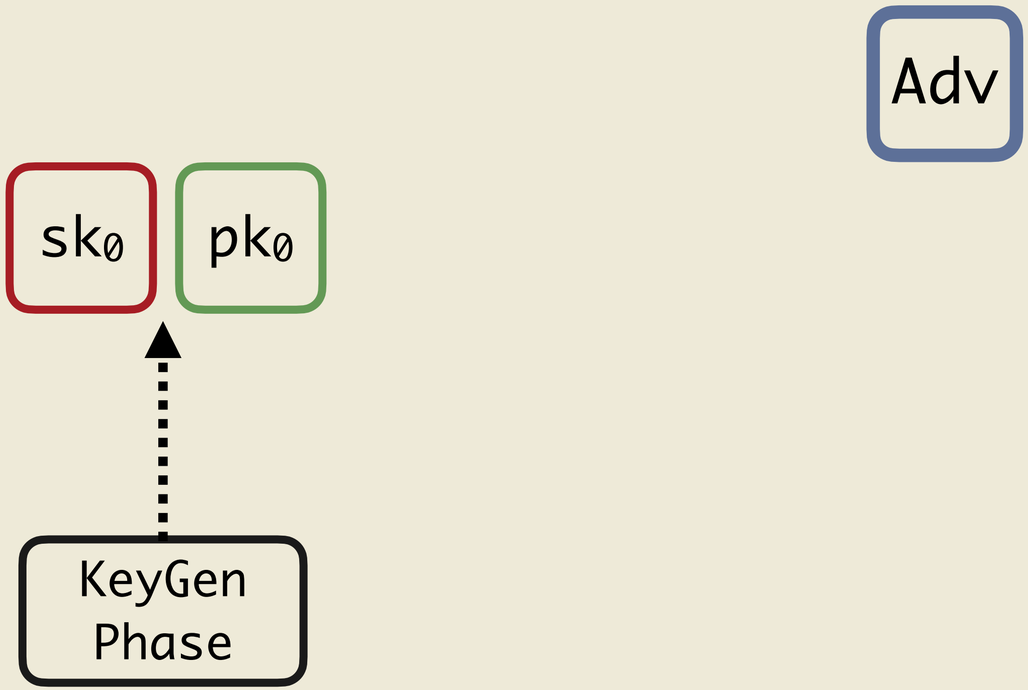
Definition



Security

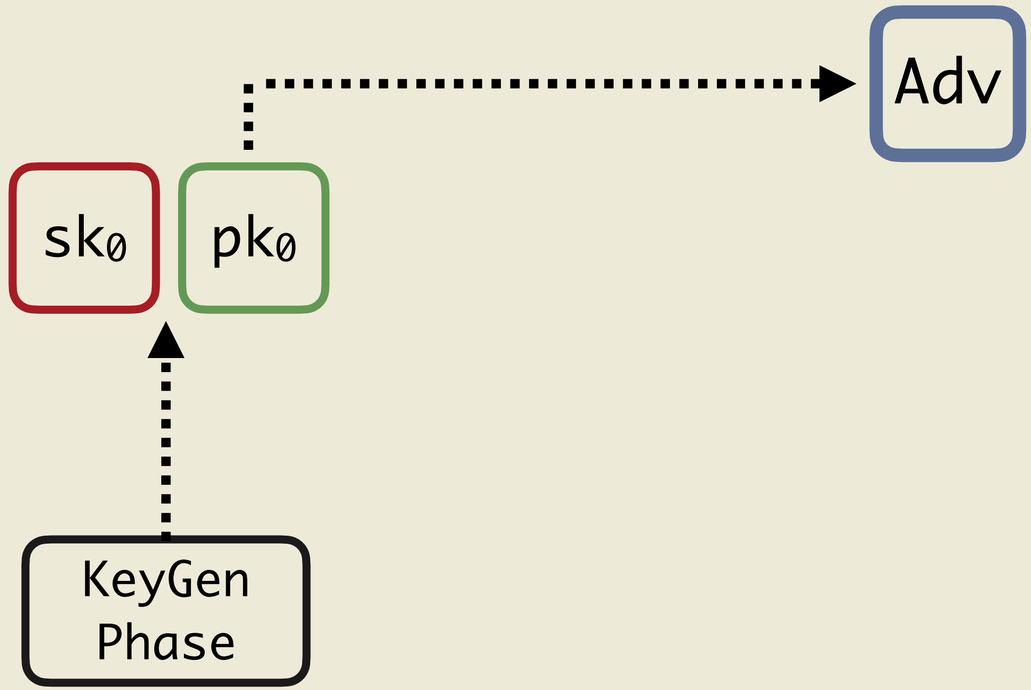
Updatable Public Key Encryption

Definition - Security



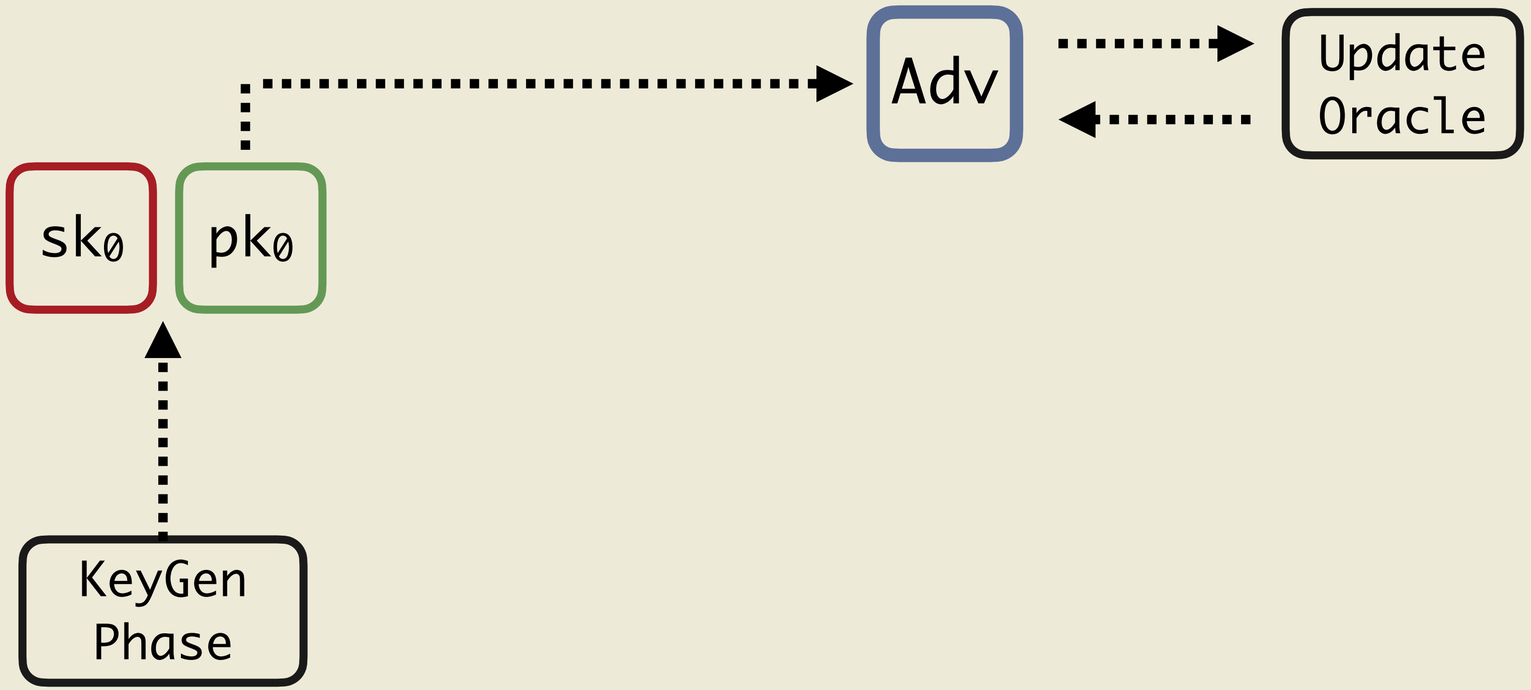
Updatable Public Key Encryption

Definition - Security



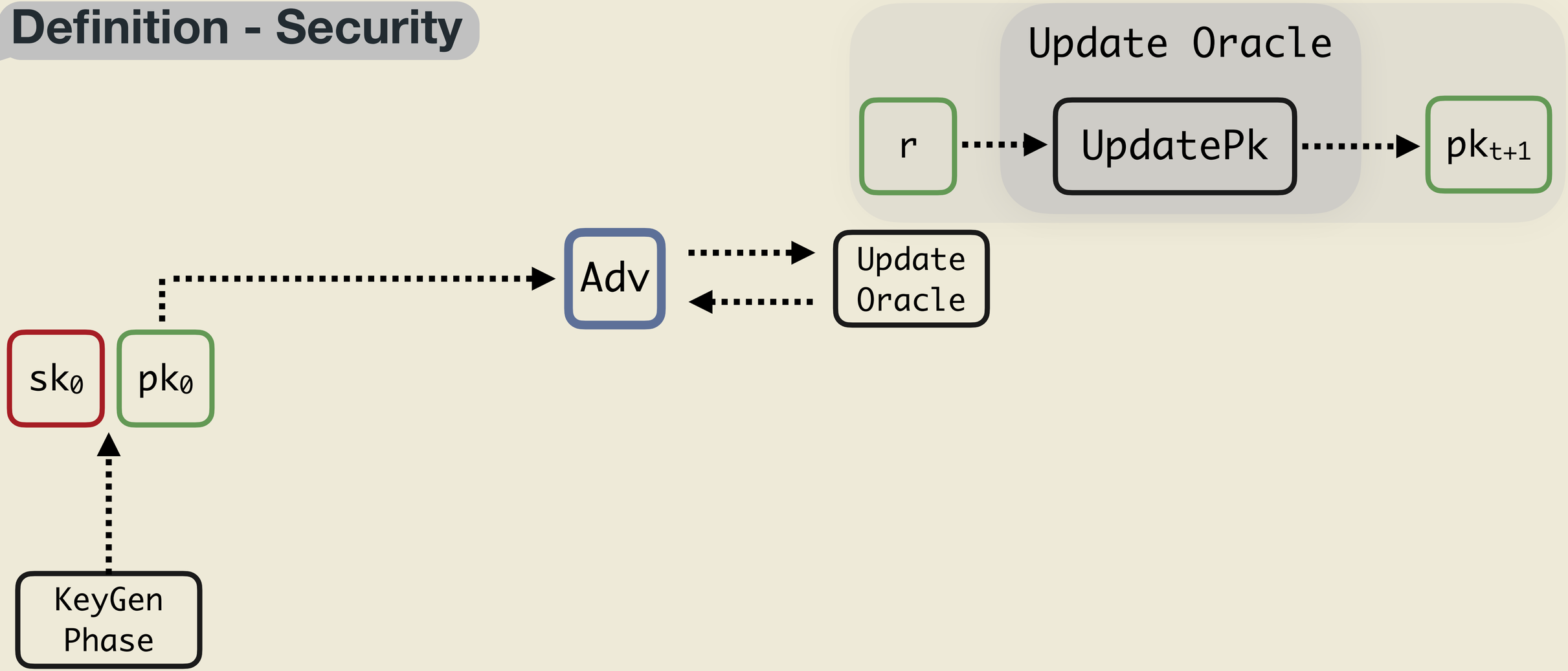
Updatable Public Key Encryption

Definition - Security



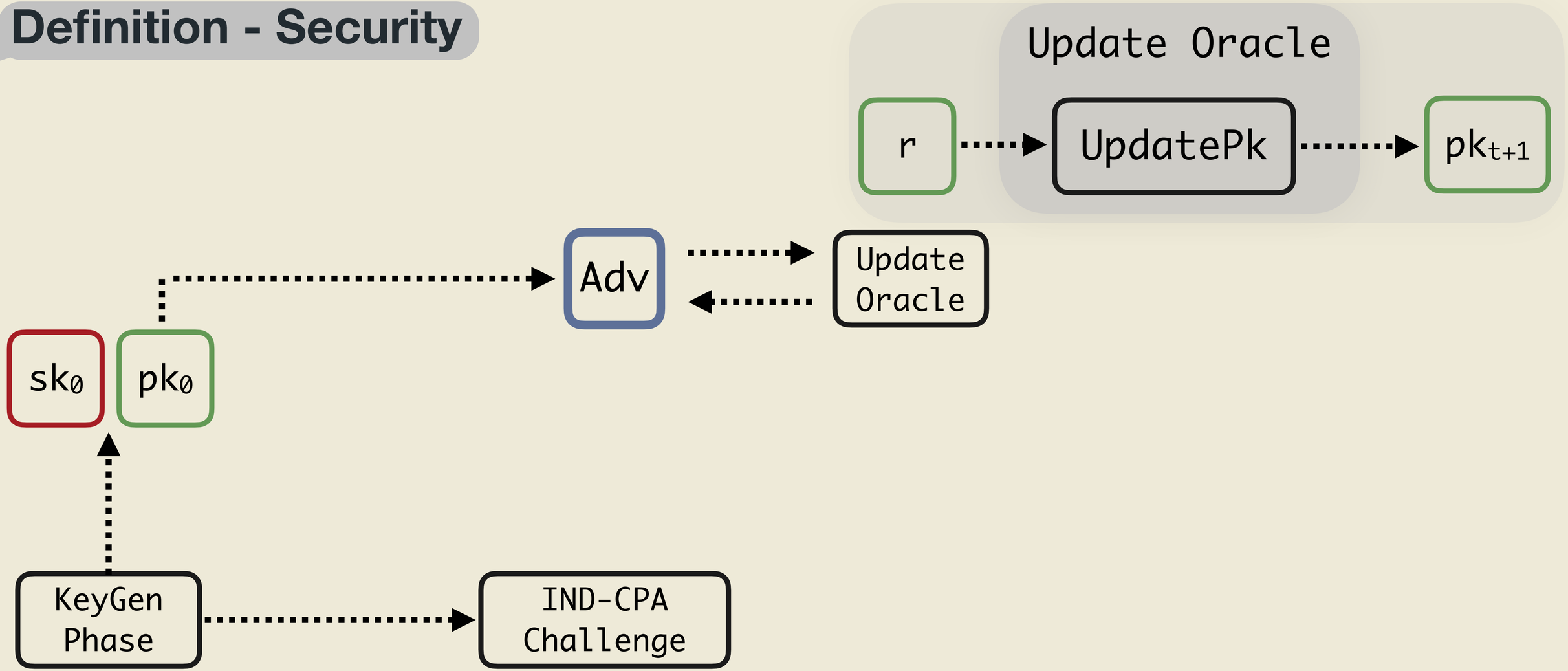
Updatable Public Key Encryption

Definition - Security



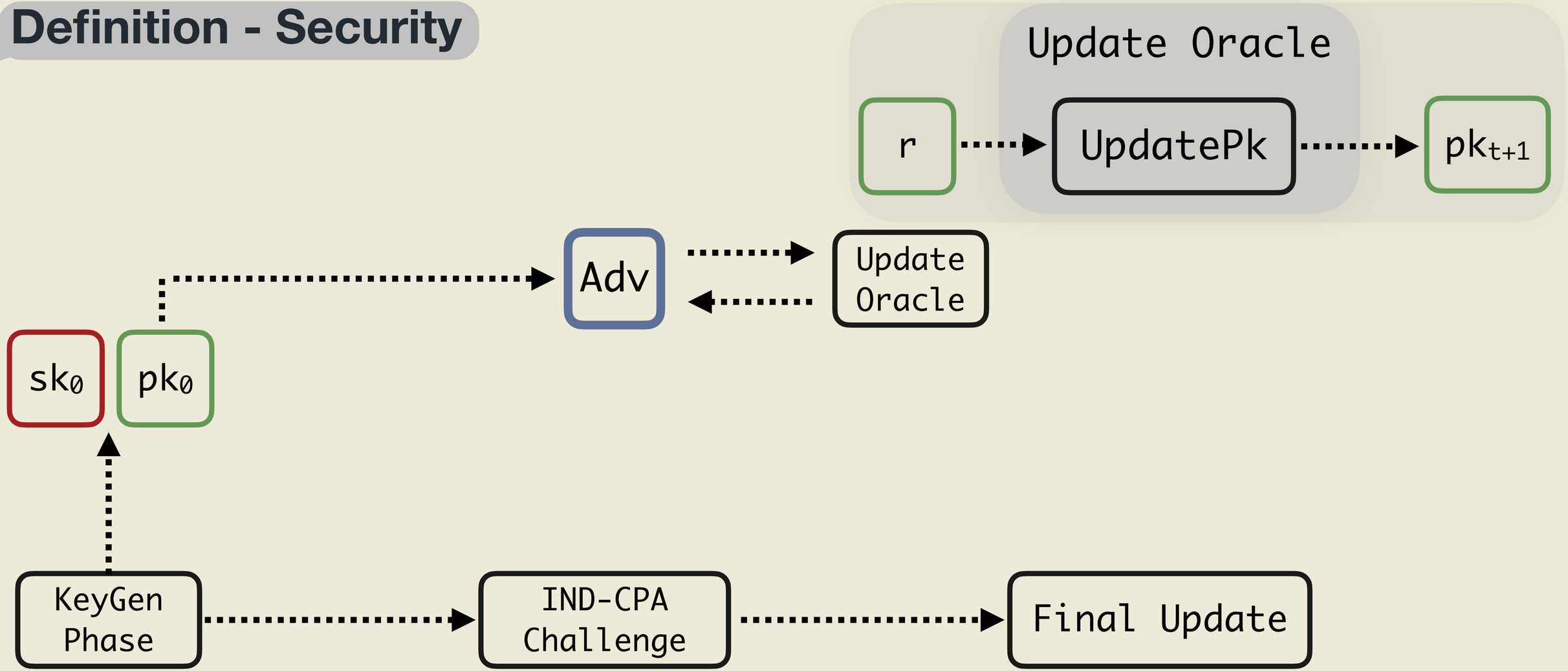
Updatable Public Key Encryption

Definition - Security



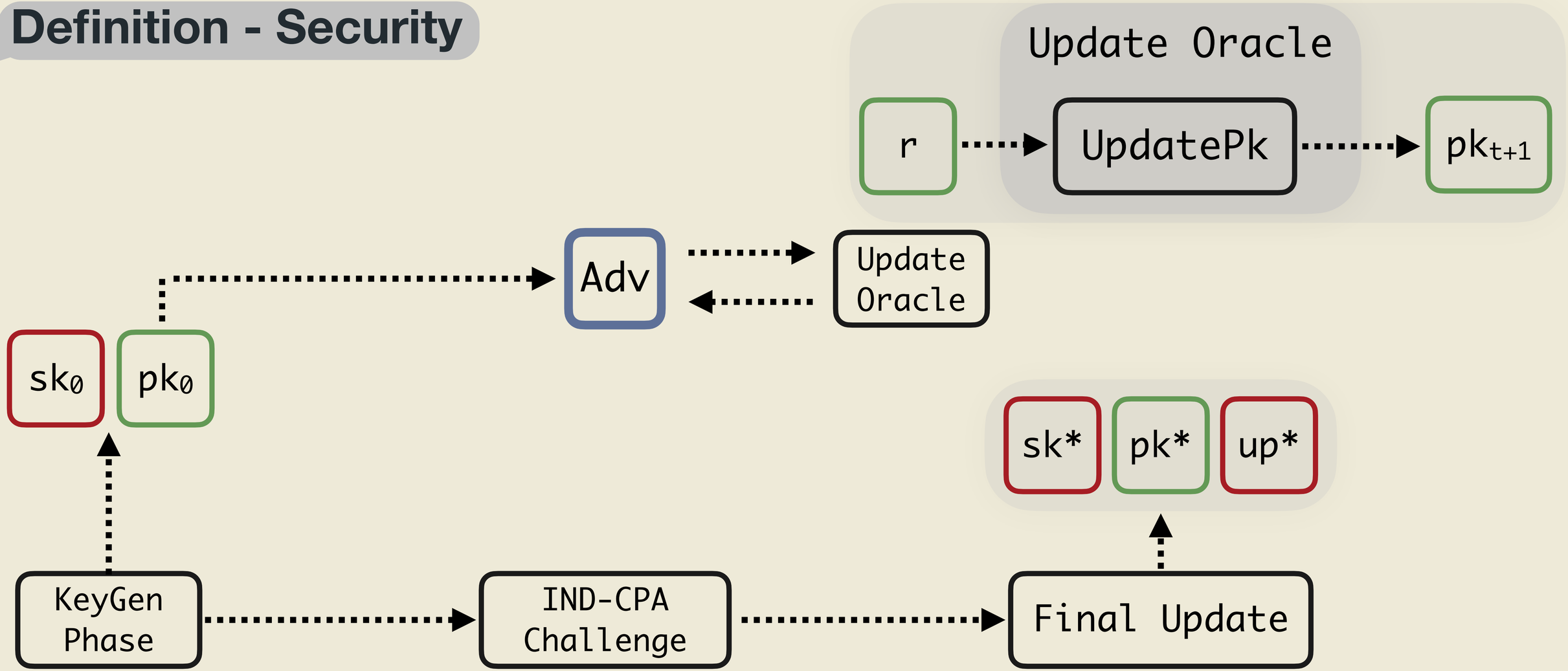
Updatable Public Key Encryption

Definition - Security



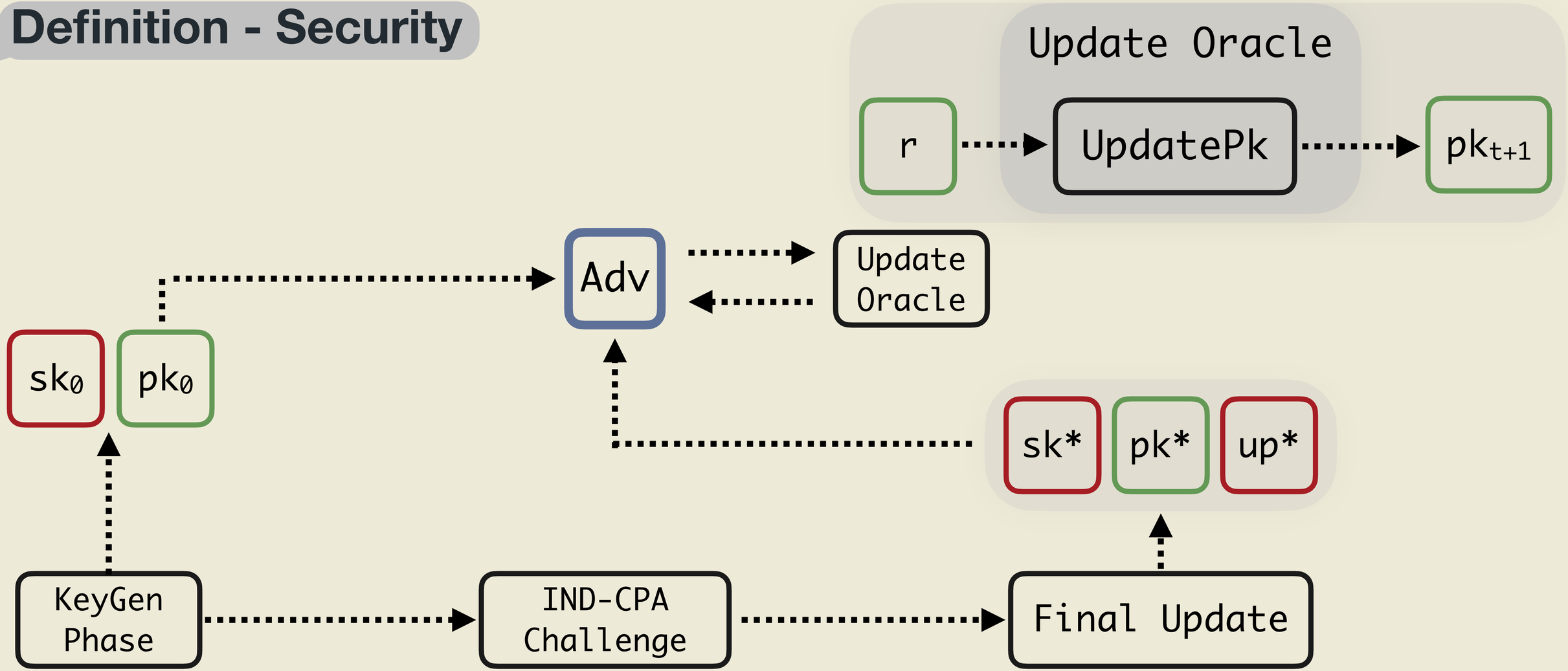
Updatable Public Key Encryption

Definition - Security



Updatable Public Key Encryption

Definition - Security



Construction

UPKE

Construction time

LWE Assumption

UPKE

Construction time

LWE Assumption

UPKE

Construction time

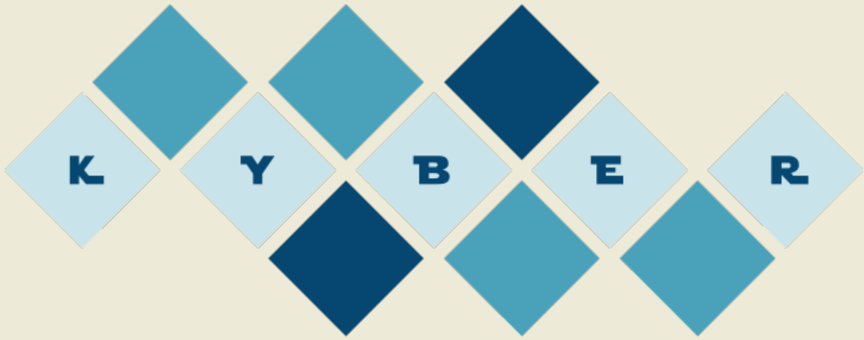
A , LWE Sample

LWE Assumption

LWE Sample = A s + e or U

UPKE

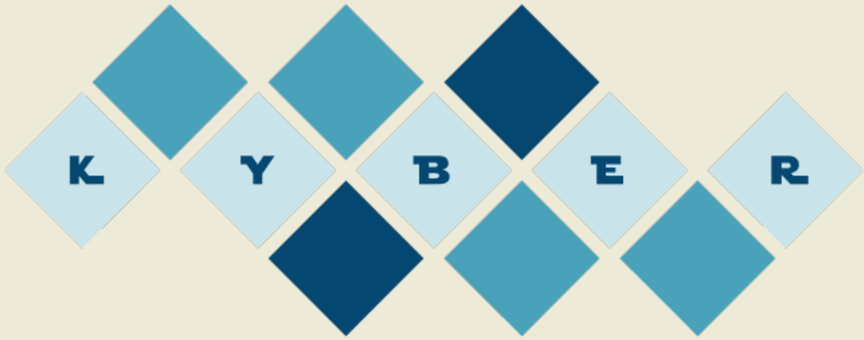
Construction time



UPKE

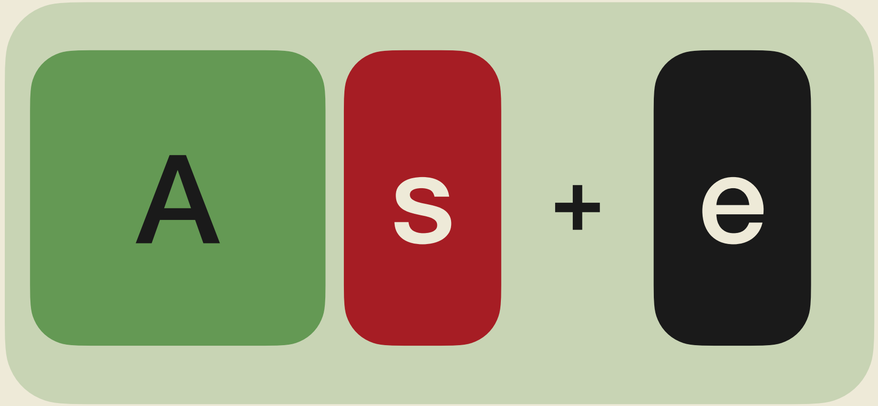
Construction time

sk



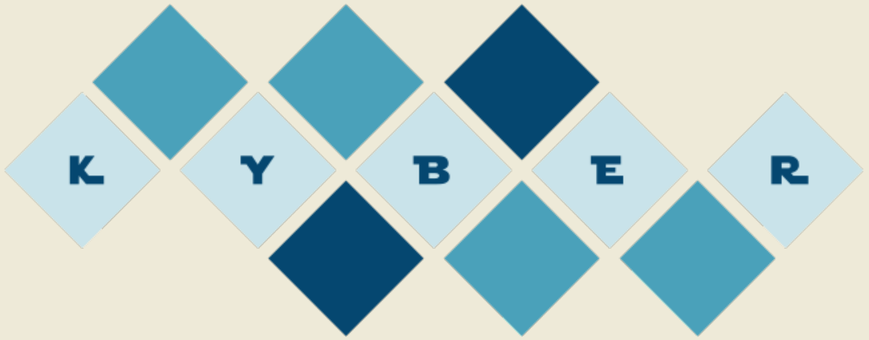
UPKE

Construction time



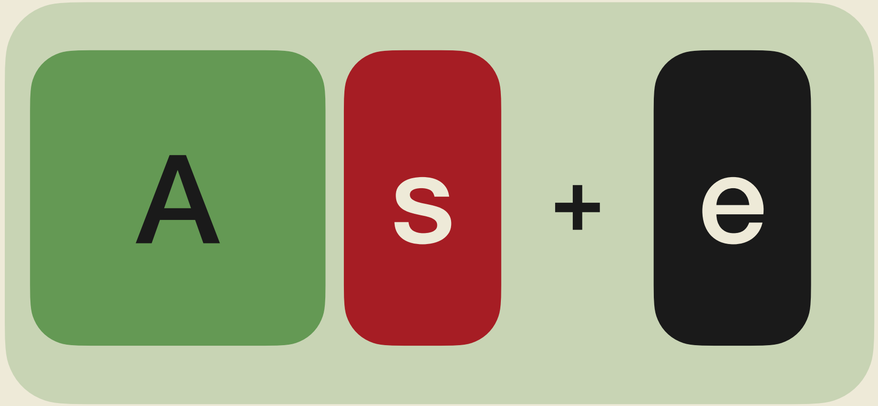
pk

sk



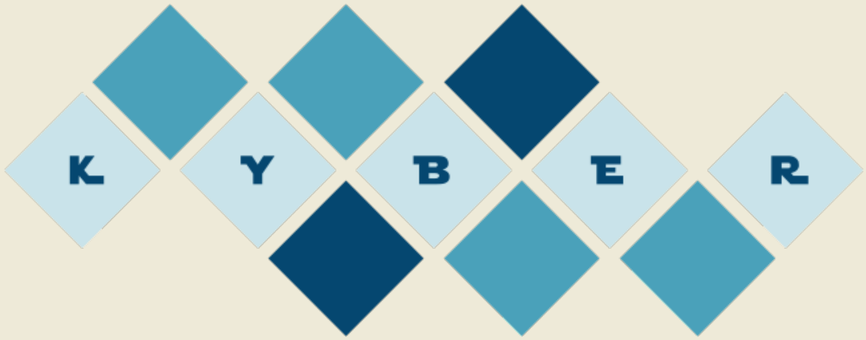
UPKE

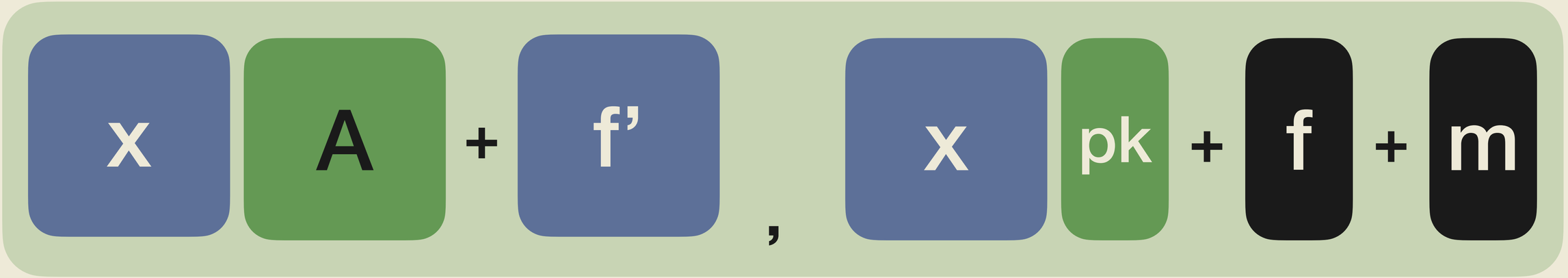
Construction time



pk

sk





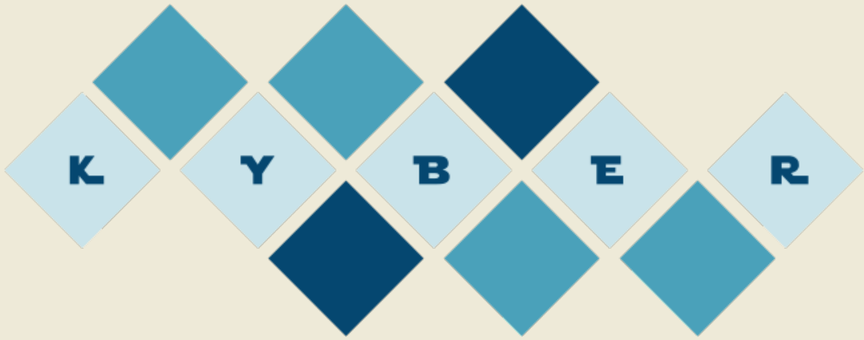
Enc(pk, m)

UPKE

Construction time

LWE Sample

S



pk

sk

x A + f’ , x pk + f + m

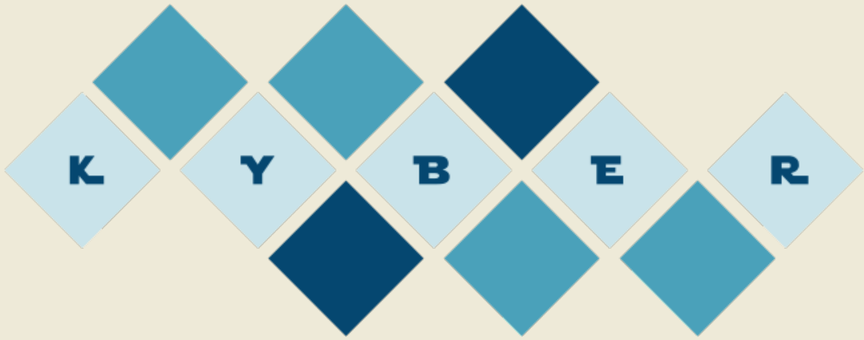
Enc(pk, m)

UPKE

Construction time

LWE Sample

S



pk

sk

x A + f’ , x pk + f

Enc(pk, m)

UPKE

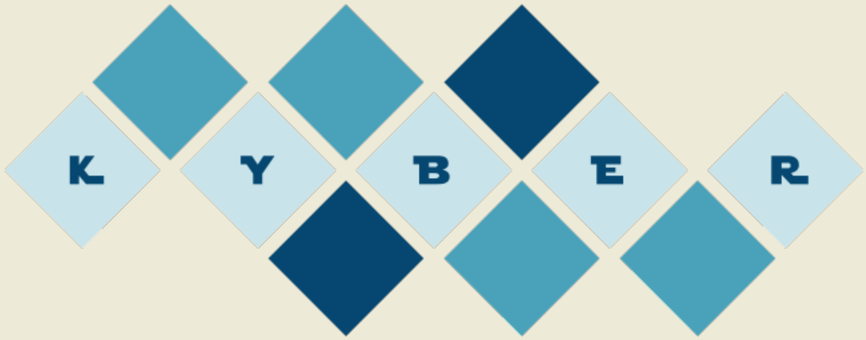
Construction time

LWE Sample

pk

s

sk



x A pk + f' f

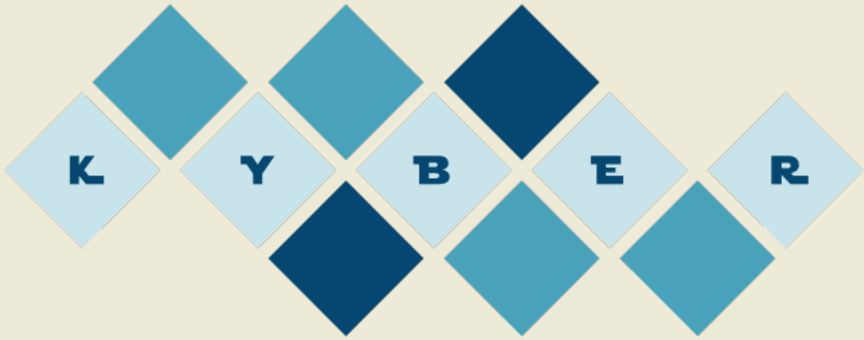
Enc(pk, m)

UPKE

Construction time

LWE Sample

S



pk

sk

LWE Sample

Enc(pk, m)

UPKE

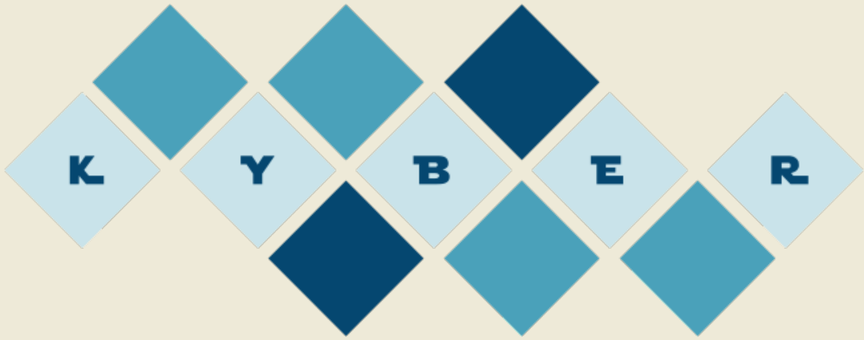
Construction time

A s + e

pk

s

sk

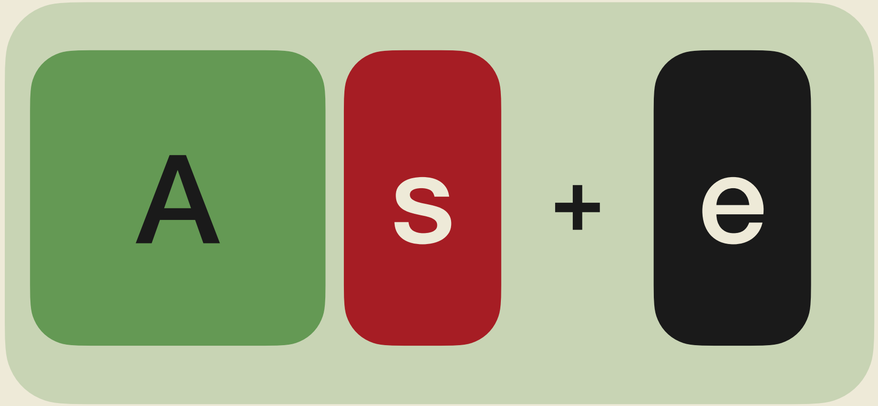


x A + f’ , x pk + f + m

Enc(pk, m)

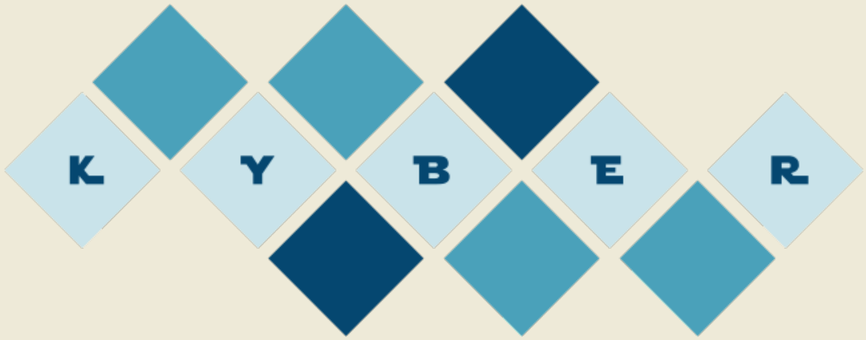
UPKE

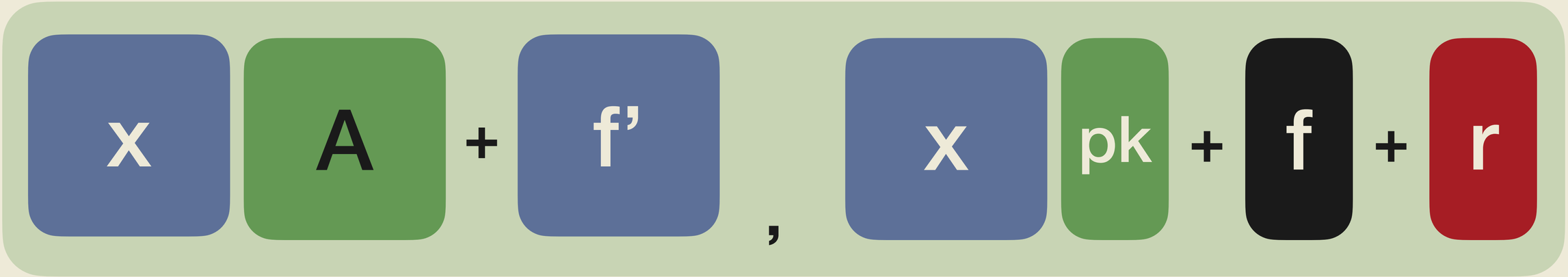
Construction time



pk

sk

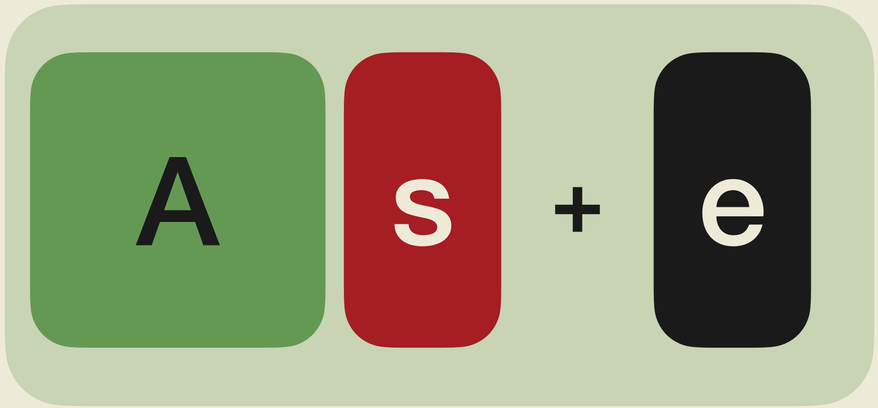




Enc(pk, r)

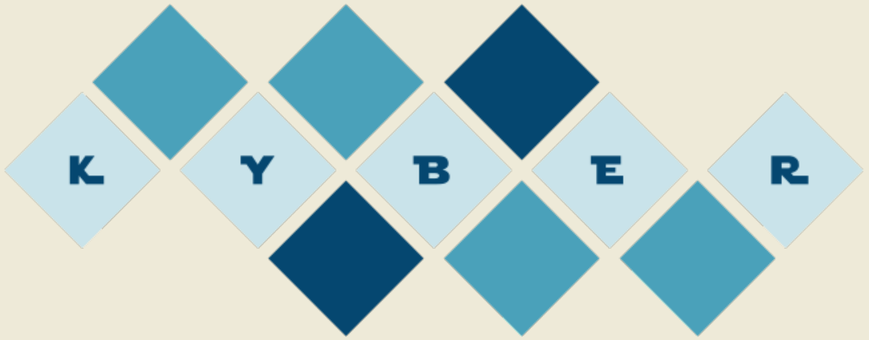
UPKE

Construction time



pk

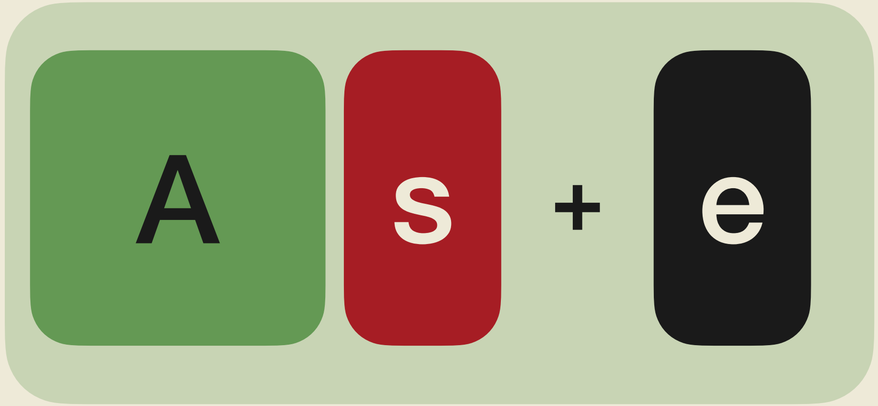
sk



Enc(pk, r)

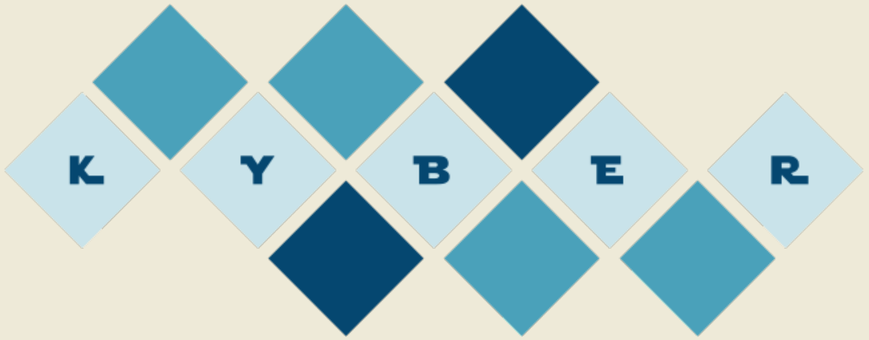
UPKE

Construction time

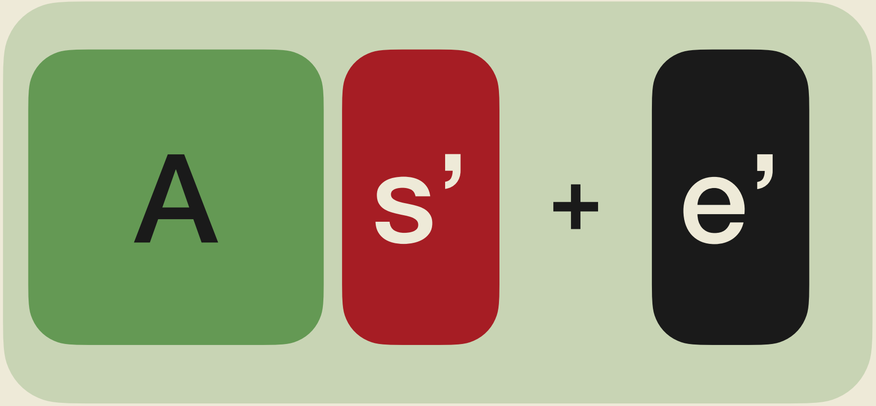


pk

sk



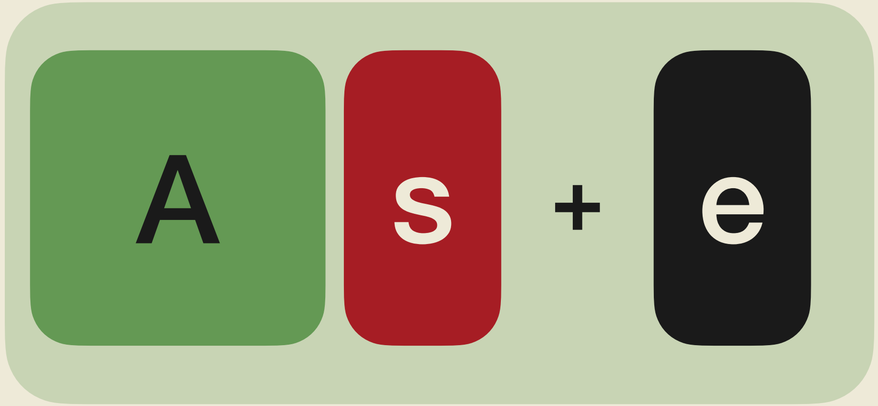
Enc(pk, r)



pk’

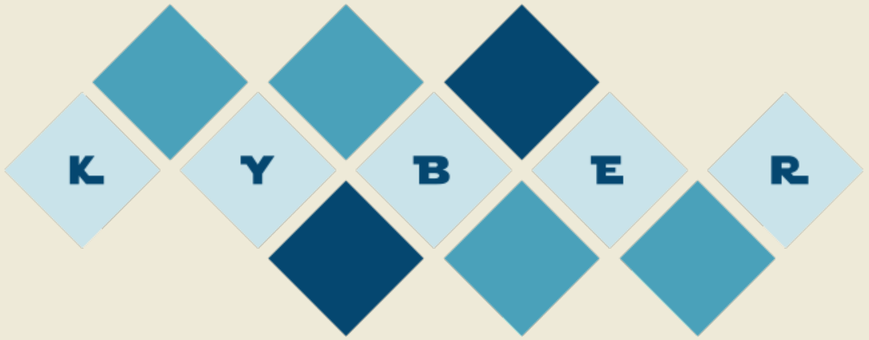
UPKE

Construction time

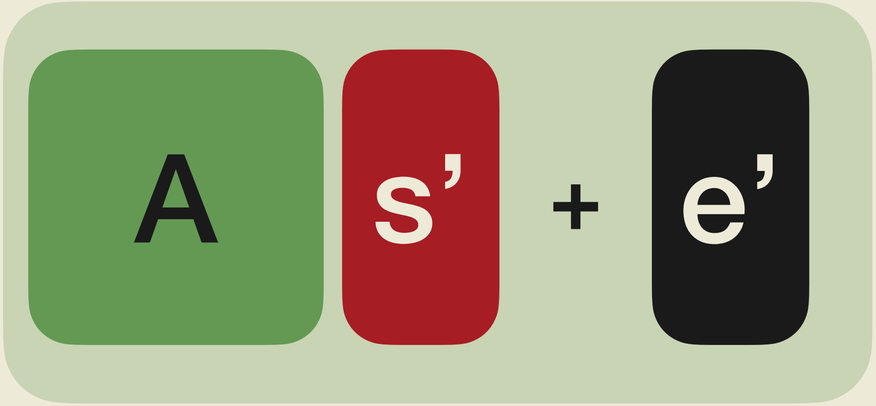


pk

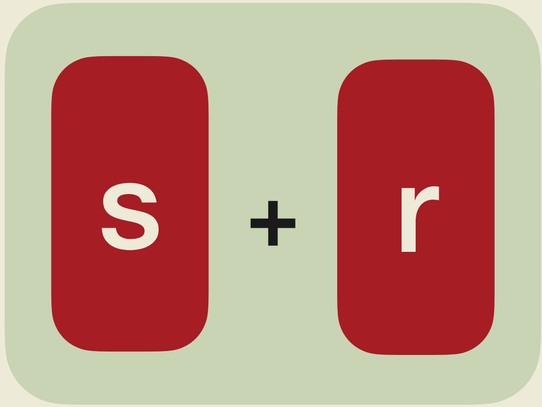
sk



Enc(pk, r)



pk’



sk’

UPKE

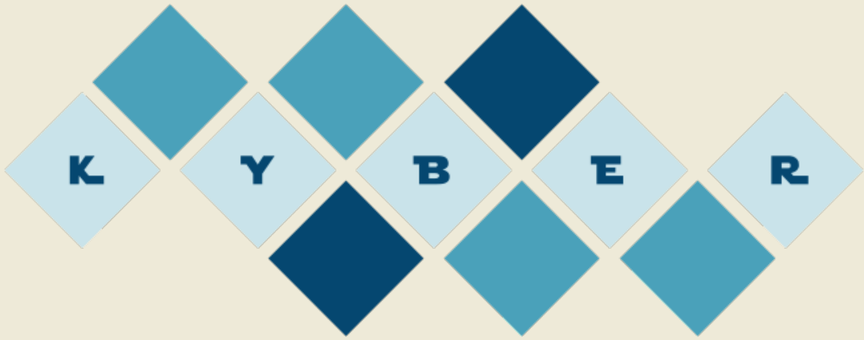
Construction time

A s + e

pk

s

sk



up

A s’ + e’

pk’

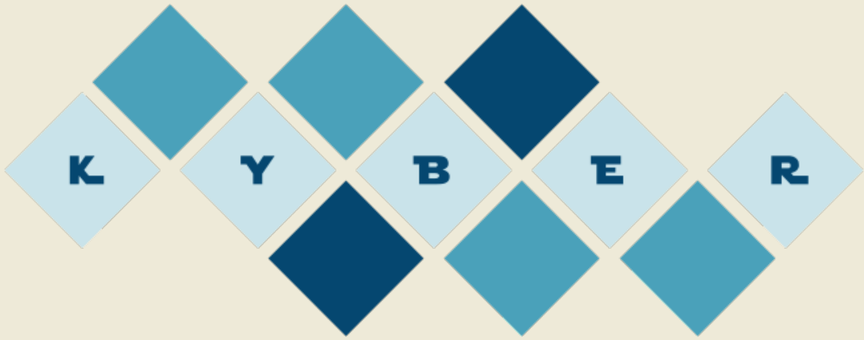
s + r

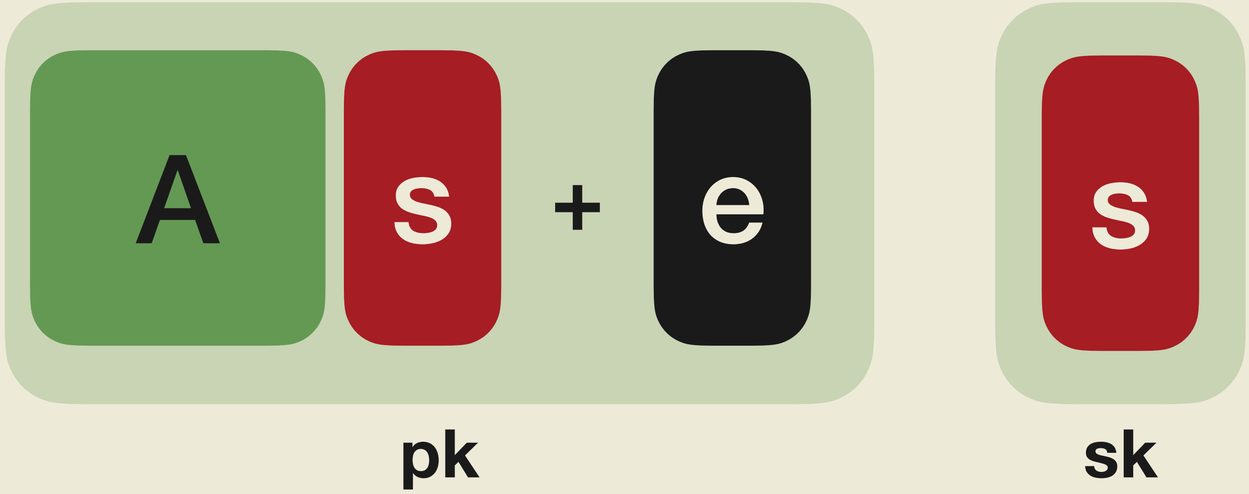
sk’

UPKE

Construction time

Done !

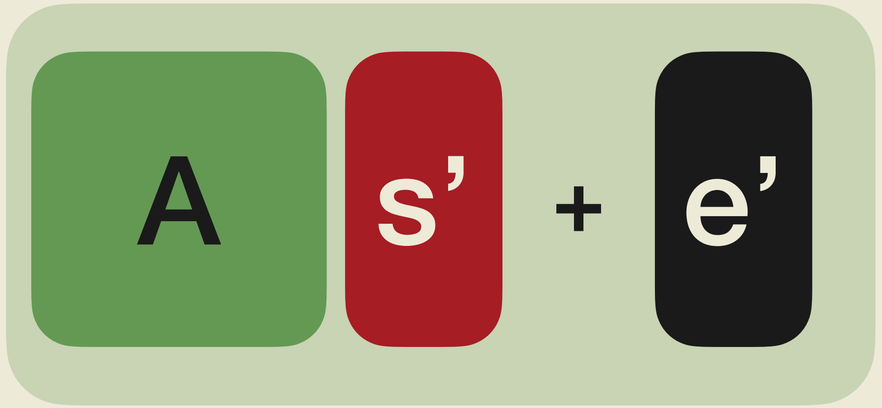




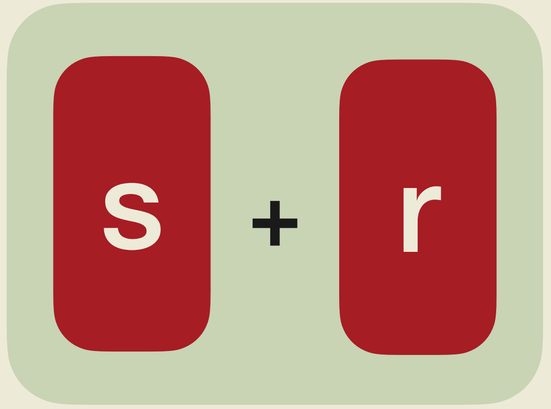
pk

sk

up



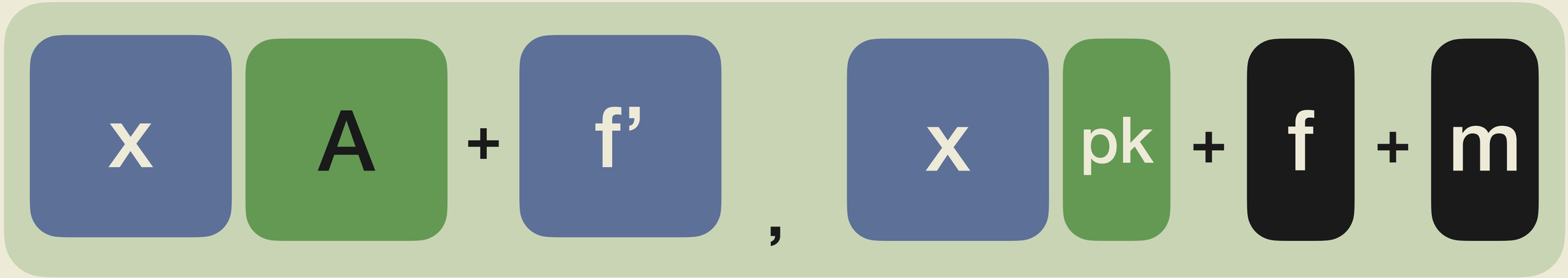
pk’



sk’

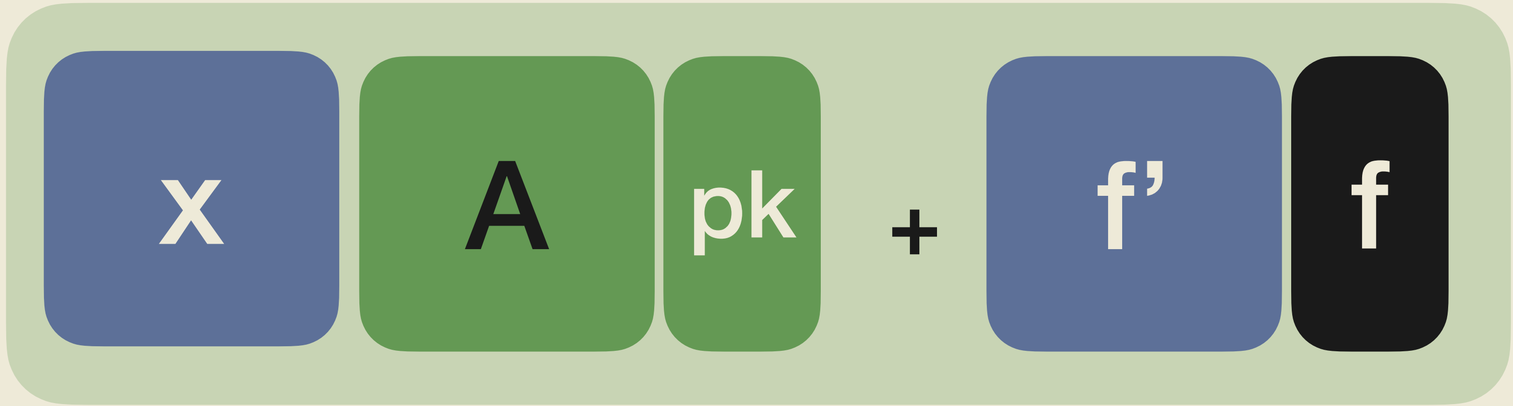
UPKE

Construction time



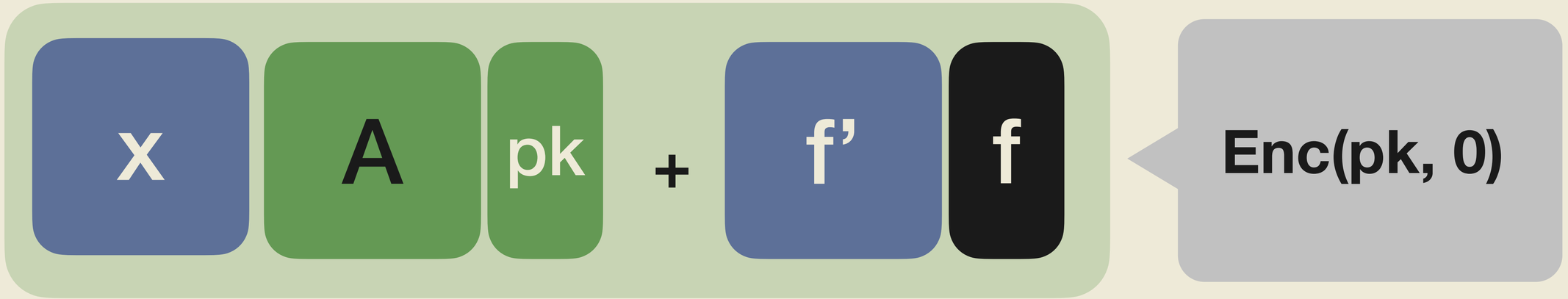
UPKE

Construction time



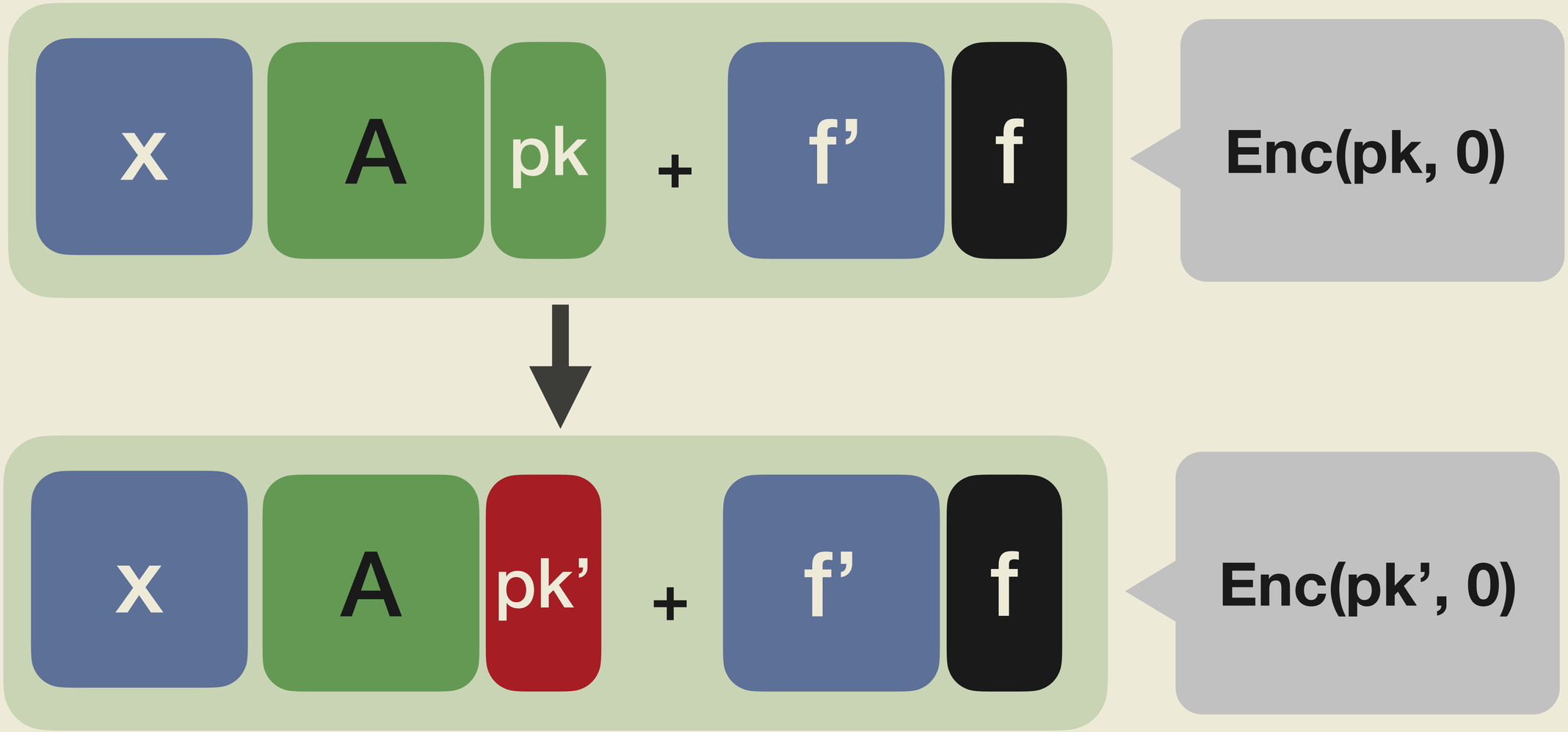
UPKE

Construction time



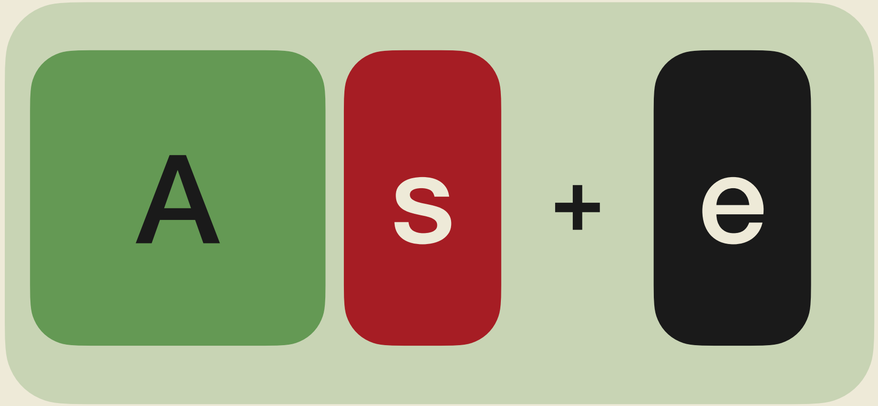
UPKE

Construction time



UPKE

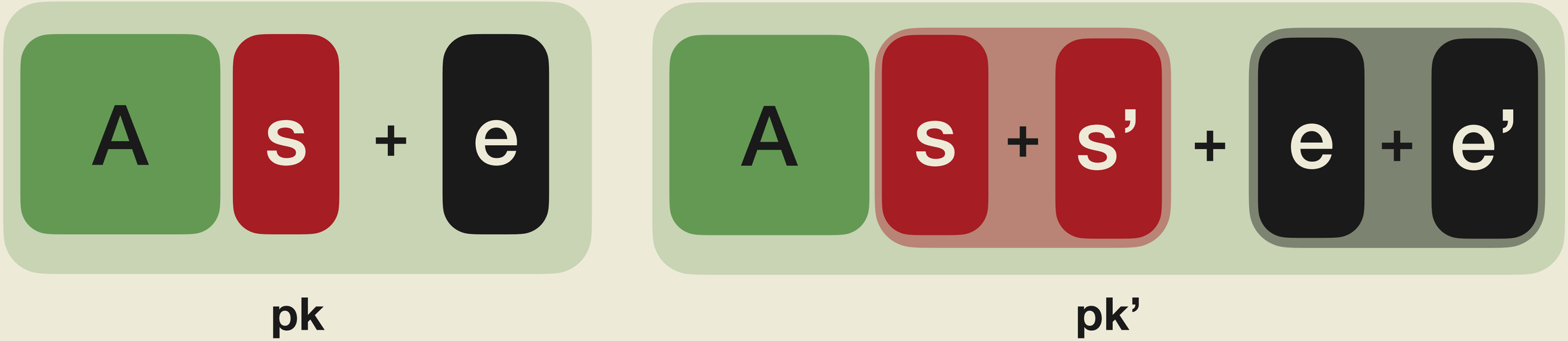
Assumption time



pk

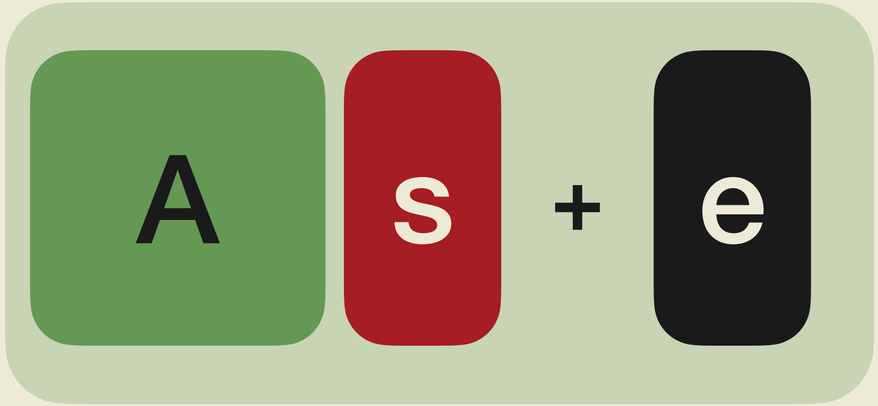
UPKE

Assumption time

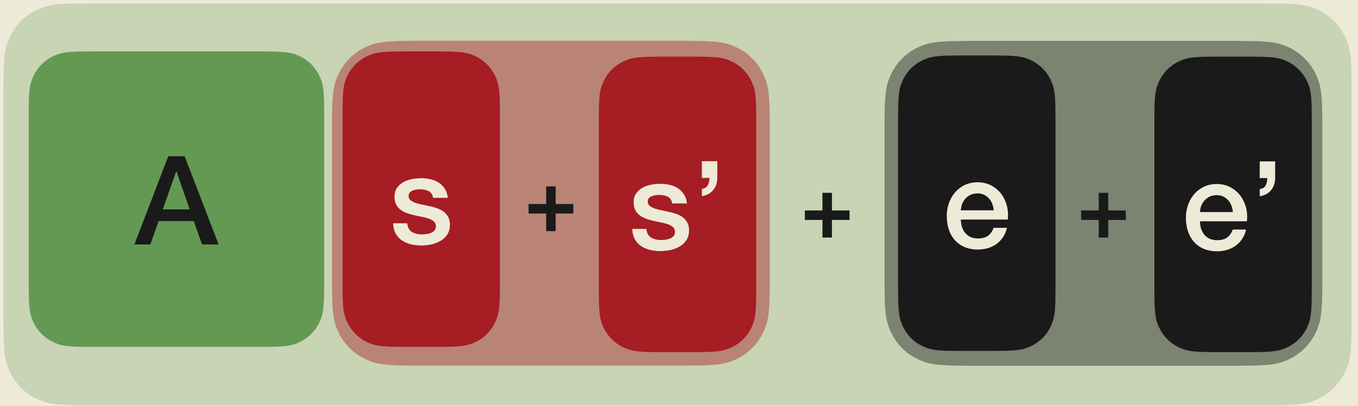


UPKE

Assumption time



pk

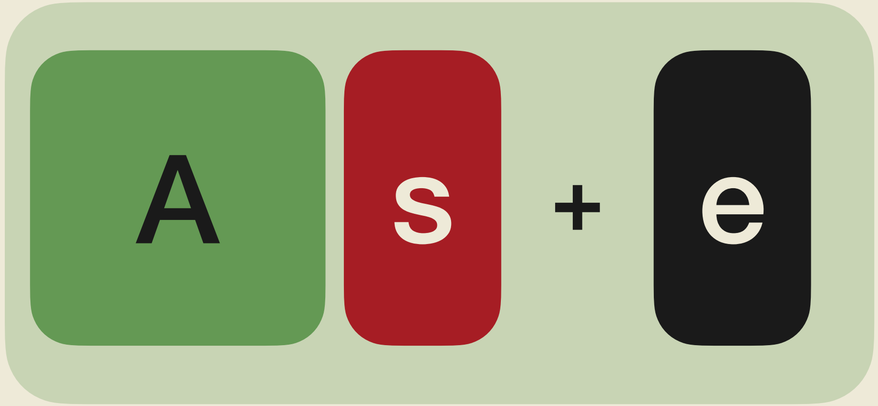


pk’

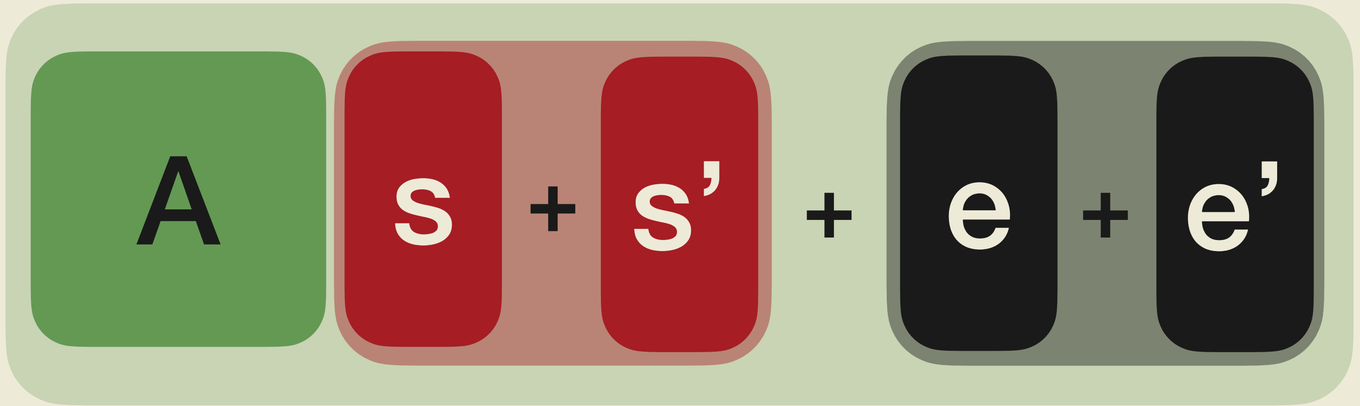
LWE Sample

UPKE

Assumption time



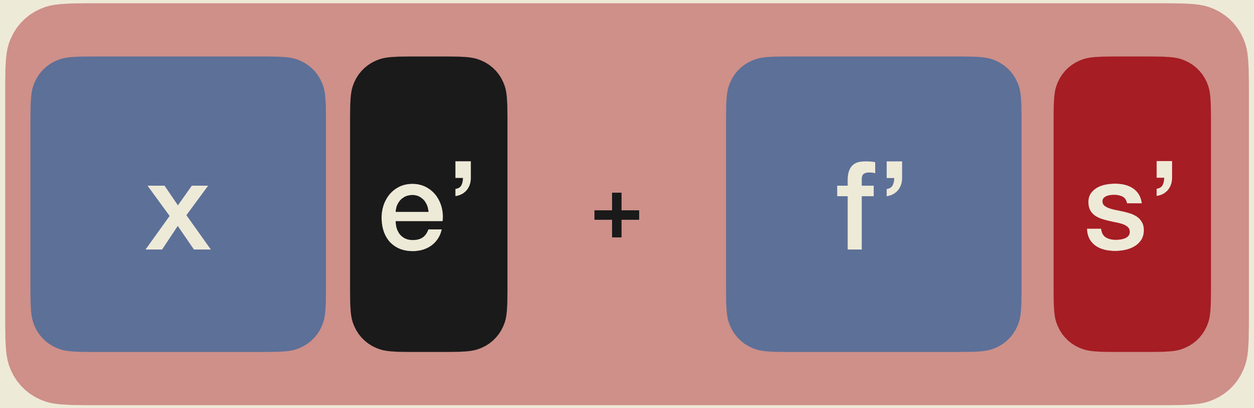
pk



LWE Sample

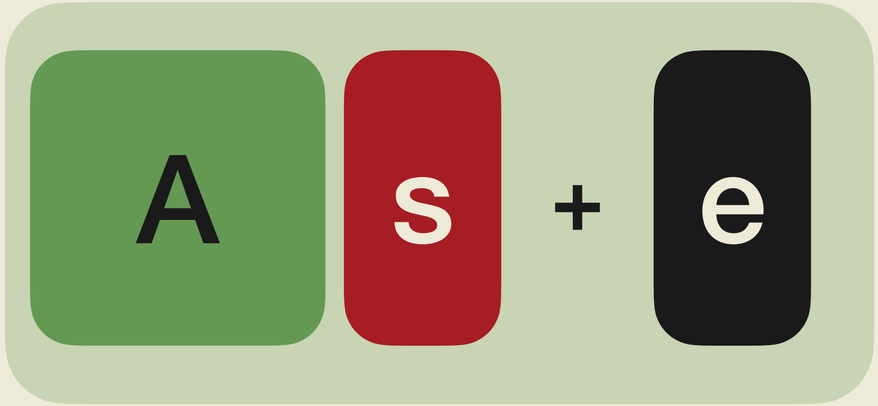
+

Cross terms



UPKE

Assumption time



pk

Cross terms - with flooding
Dodis et al. TCC 21

LWE Sample + **Very small**

UPKE

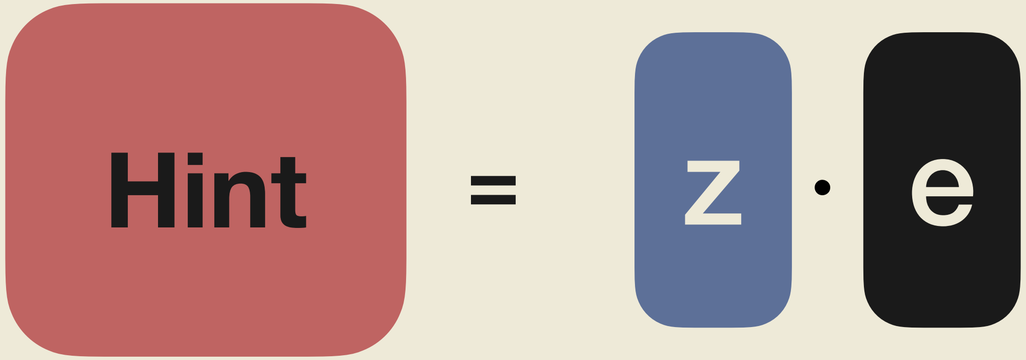
Assumption time

LWE + Hint variant

UPKE

Assumption time

LWE + Hint variant



Extended LWE

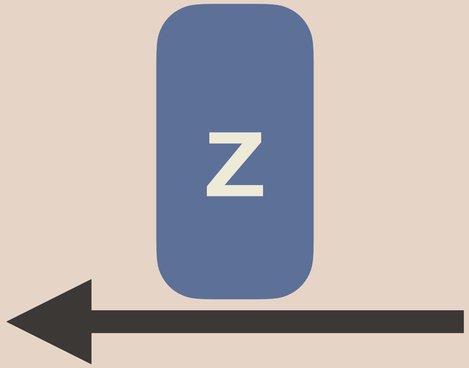
UPKE

Assumption time

Extended LWE

UPKE

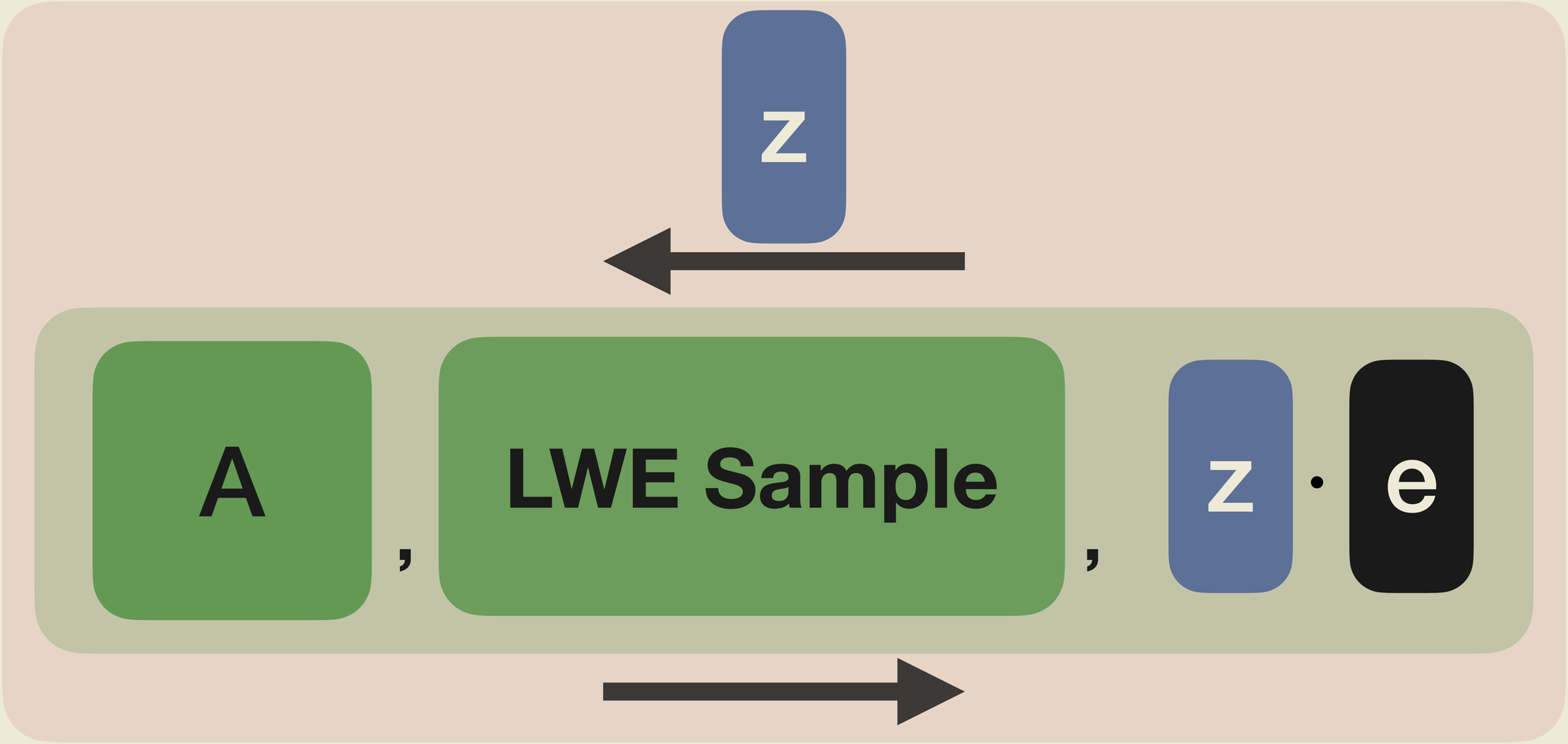
Assumption time



Extended LWE

UPKE

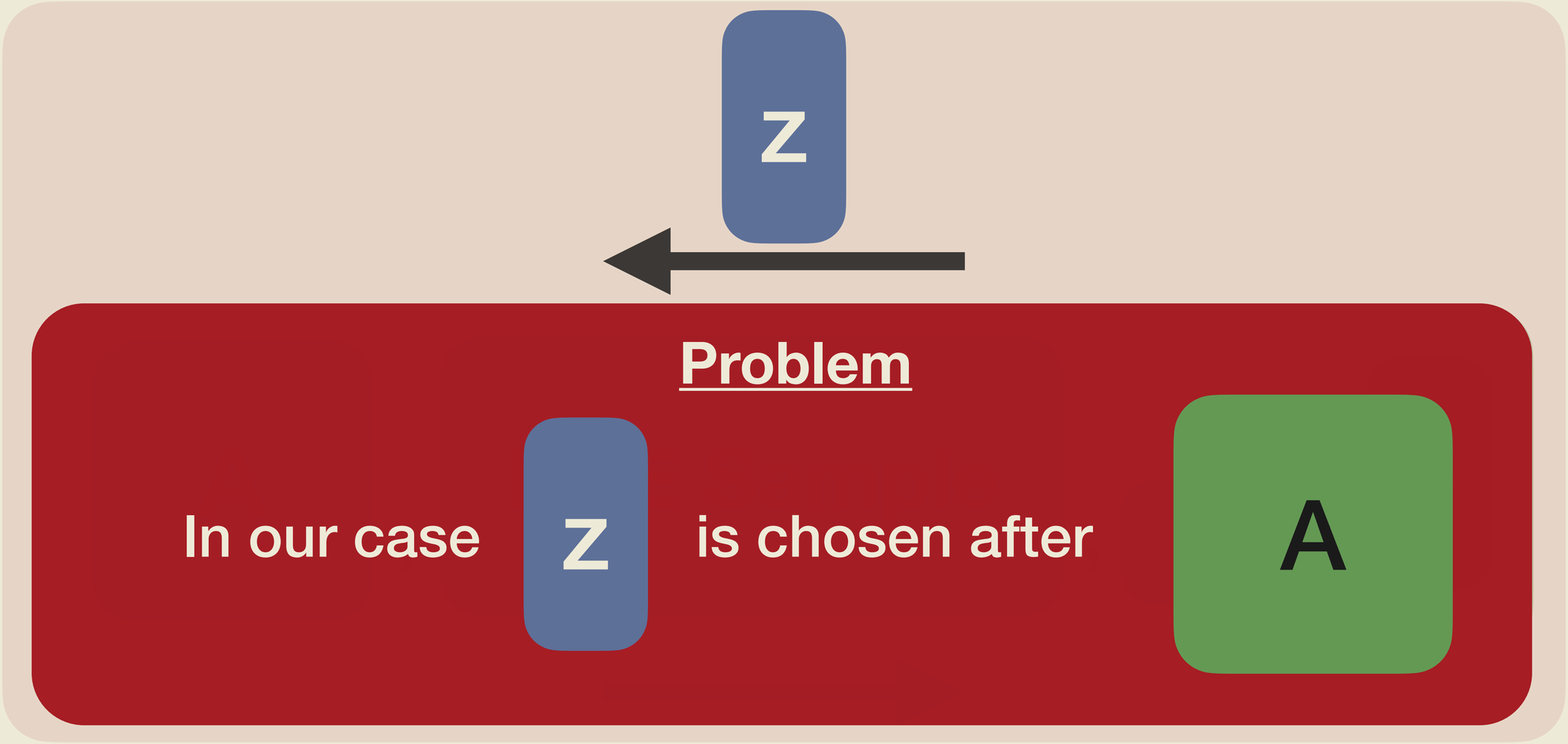
Assumption time



Extended LWE

UPKE

Assumption time



Extended LWE

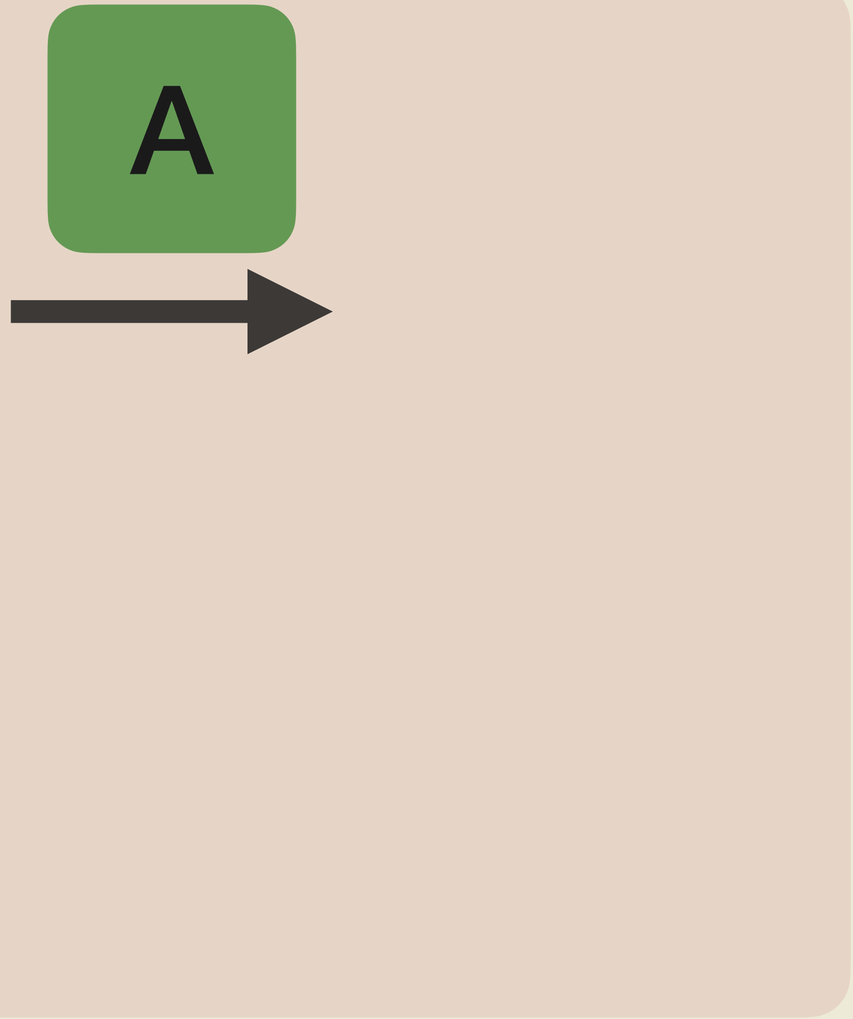
UPKE

Assumption time

What we need

UPKE

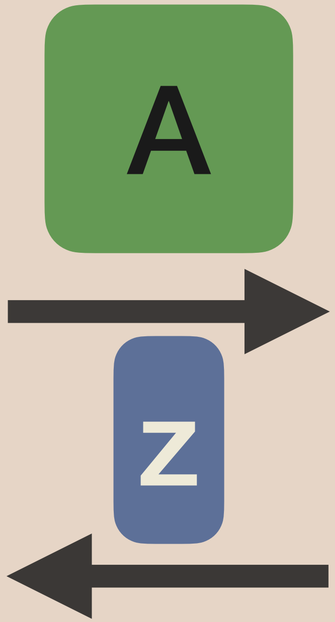
Assumption time



What we need

UPKE

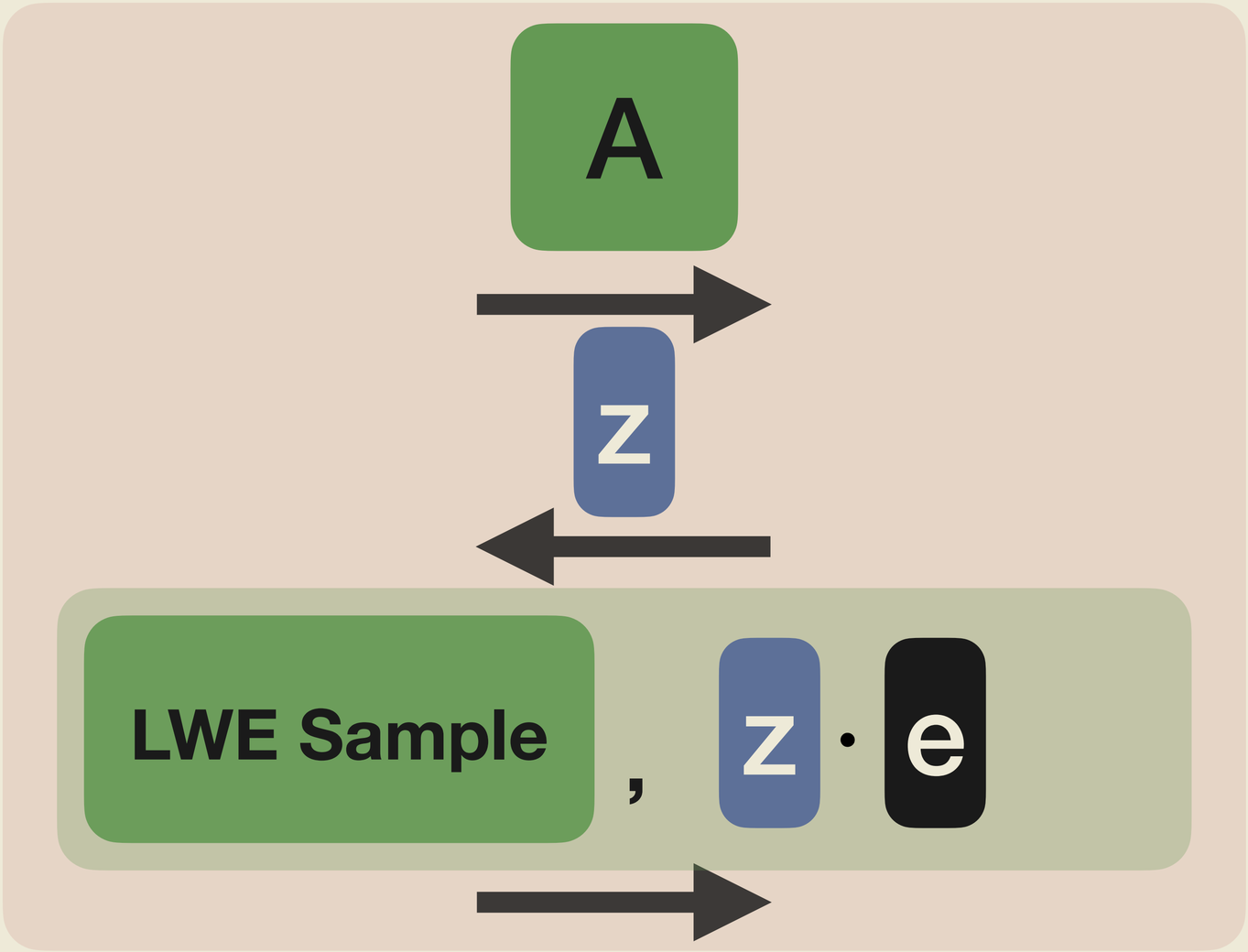
Assumption time



What we need

UPKE

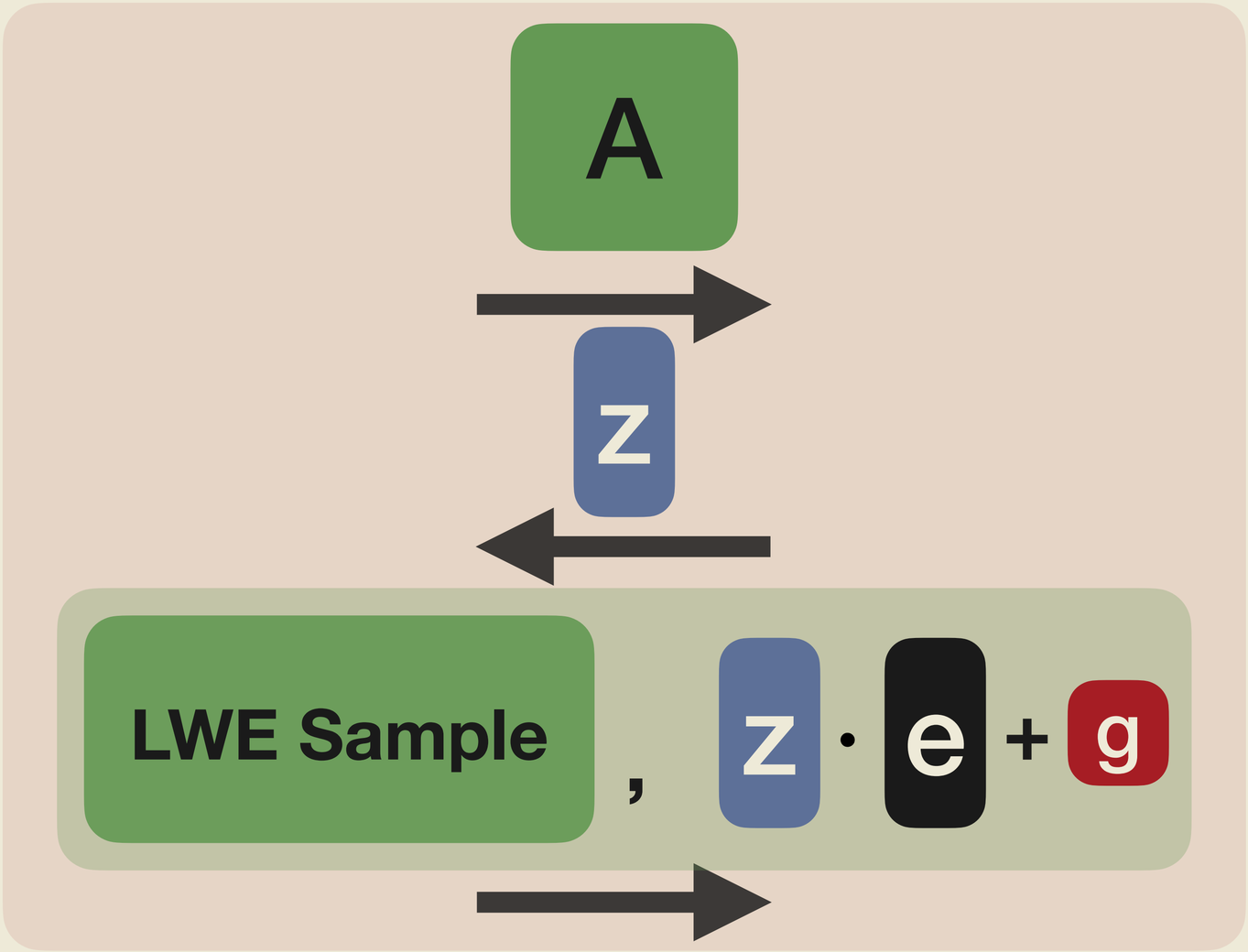
Assumption time



What we need

UPKE

Assumption time

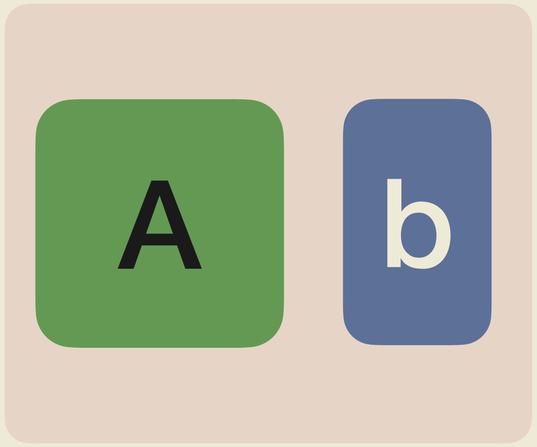


Adaptive extended LWE

Reduction

UPKE

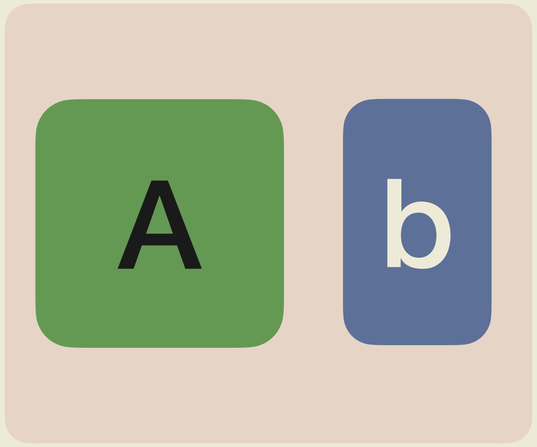
Assumption time - Reduction



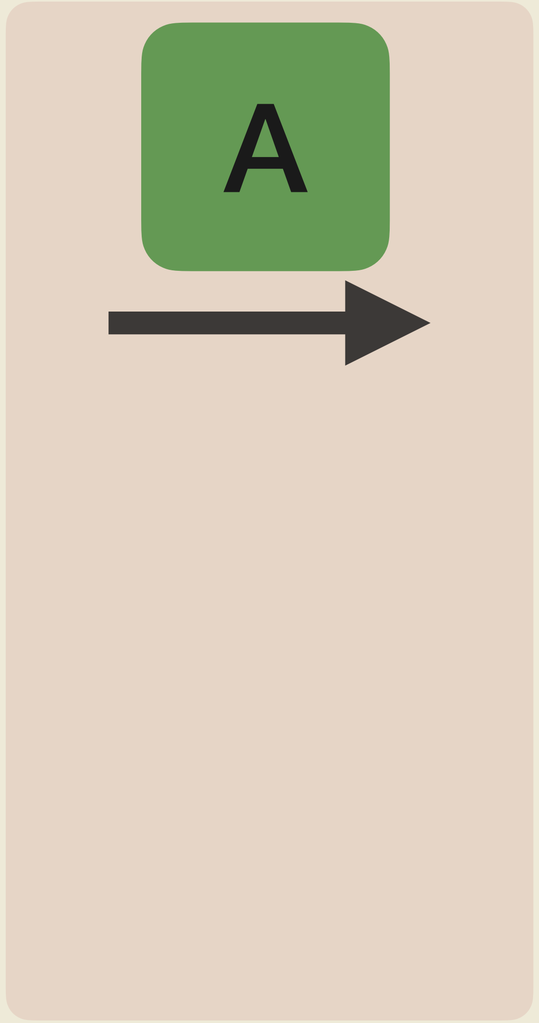
LWE

UPKE

Assumption time - Reduction



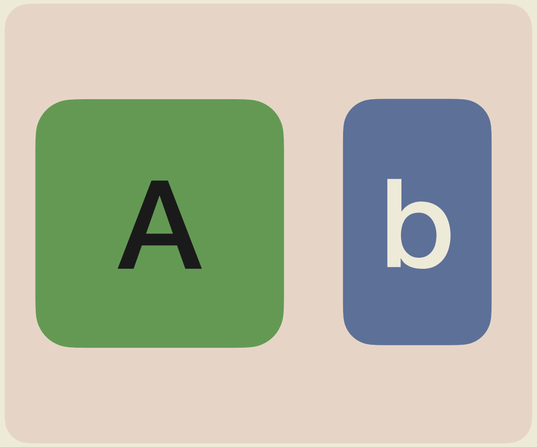
LWE



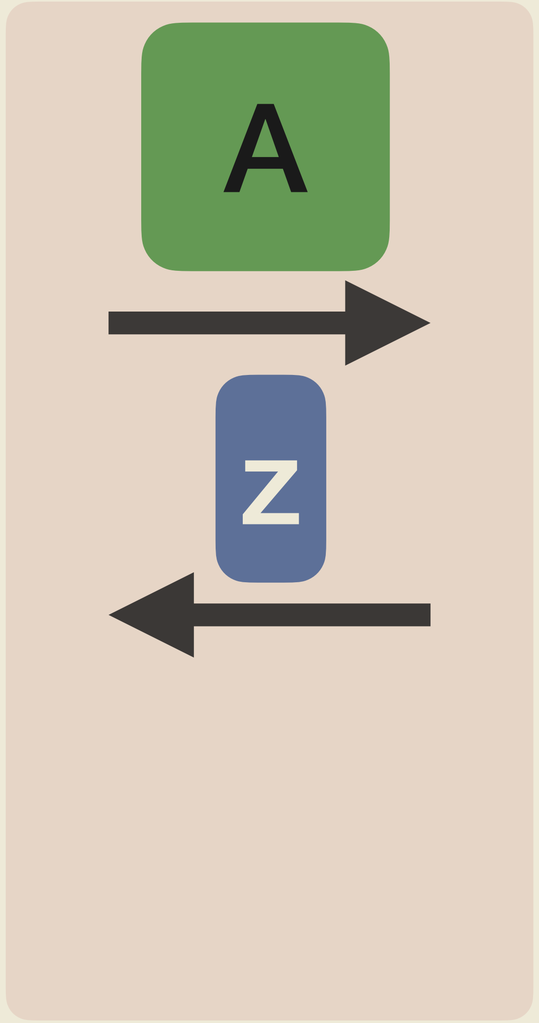
AextLWE

UPKE

Assumption time - Reduction



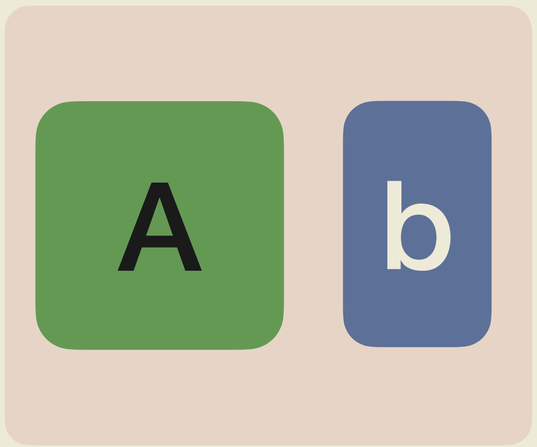
LWE

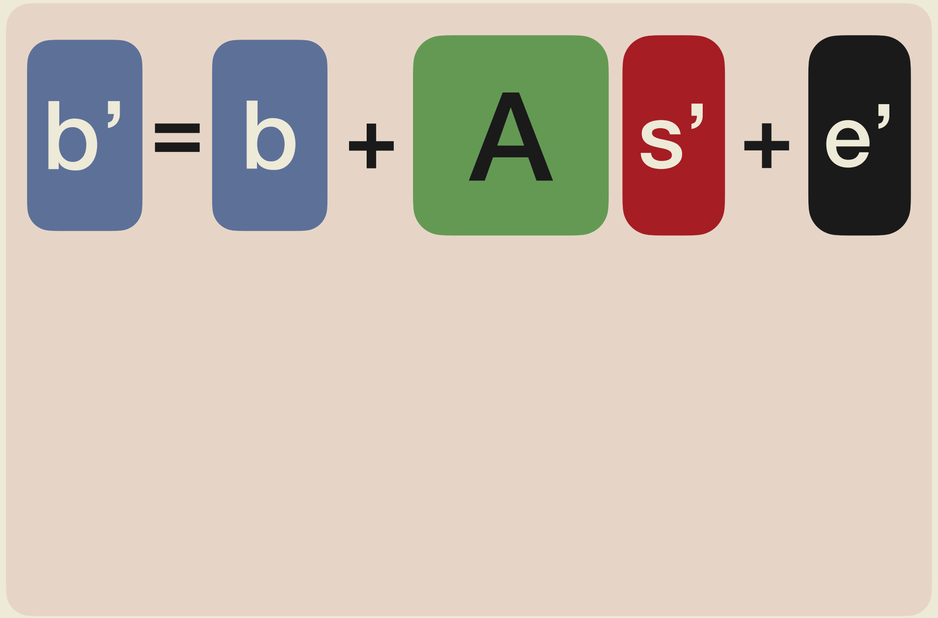


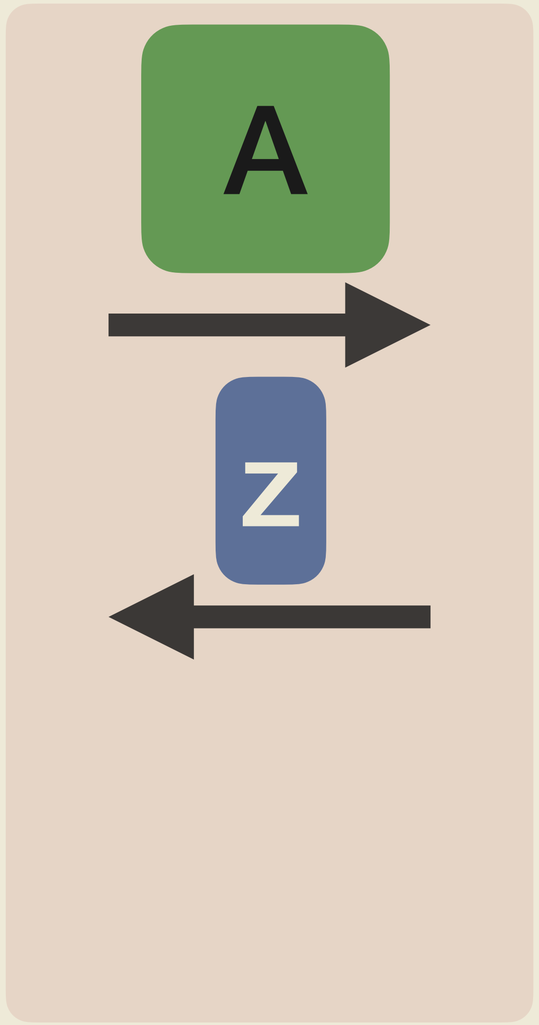
AextLWE

UPKE

Assumption time - Reduction





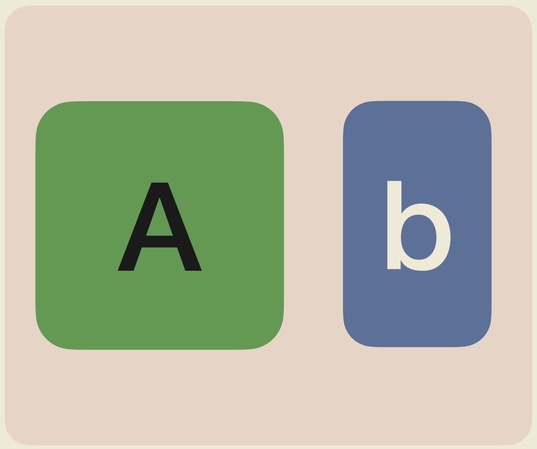


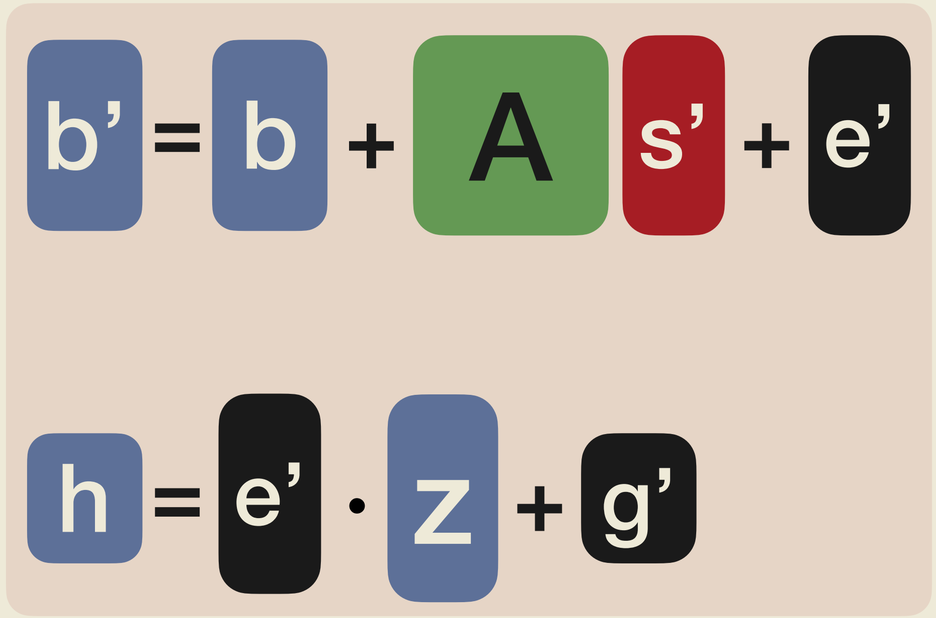
LWE

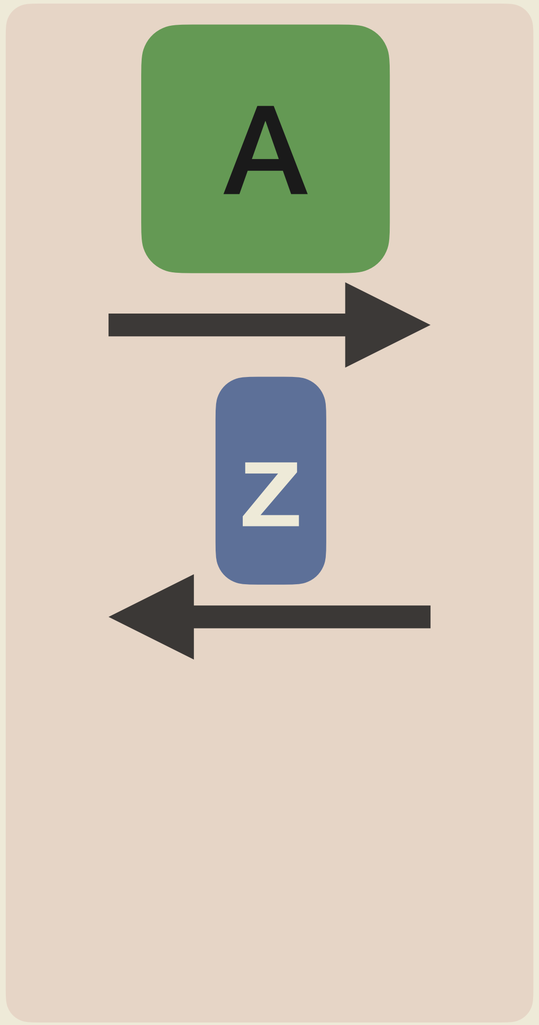
AextLWE

UPKE

Assumption time - Reduction





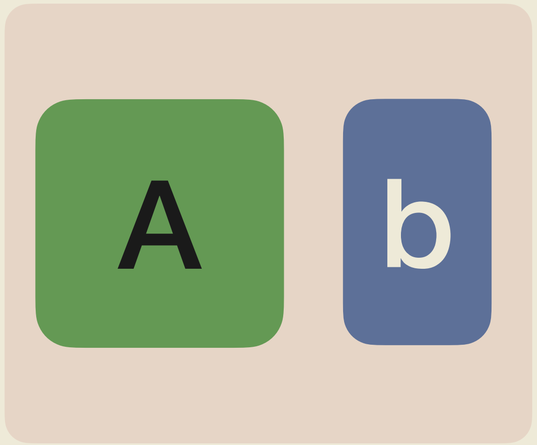


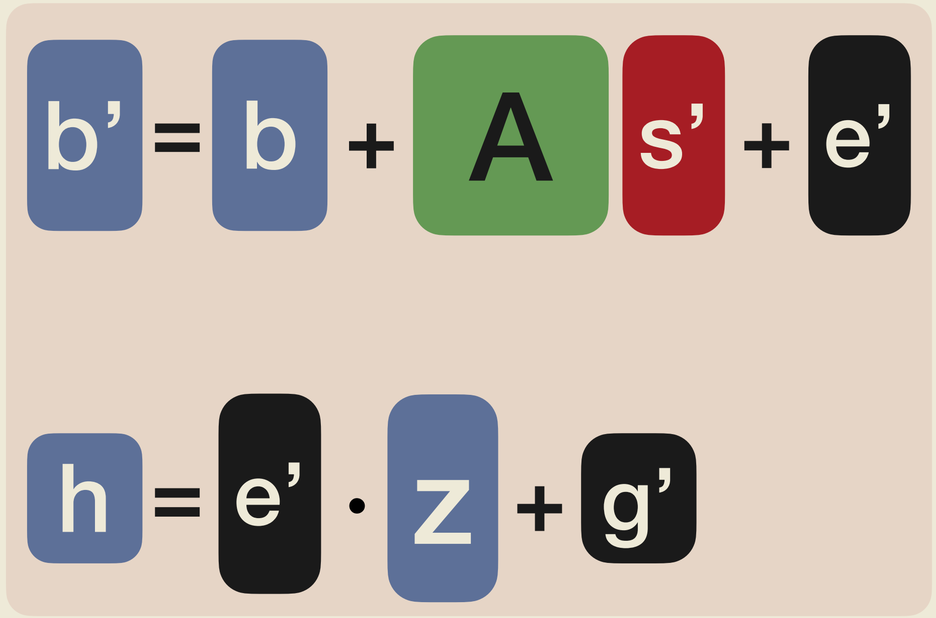
LWE

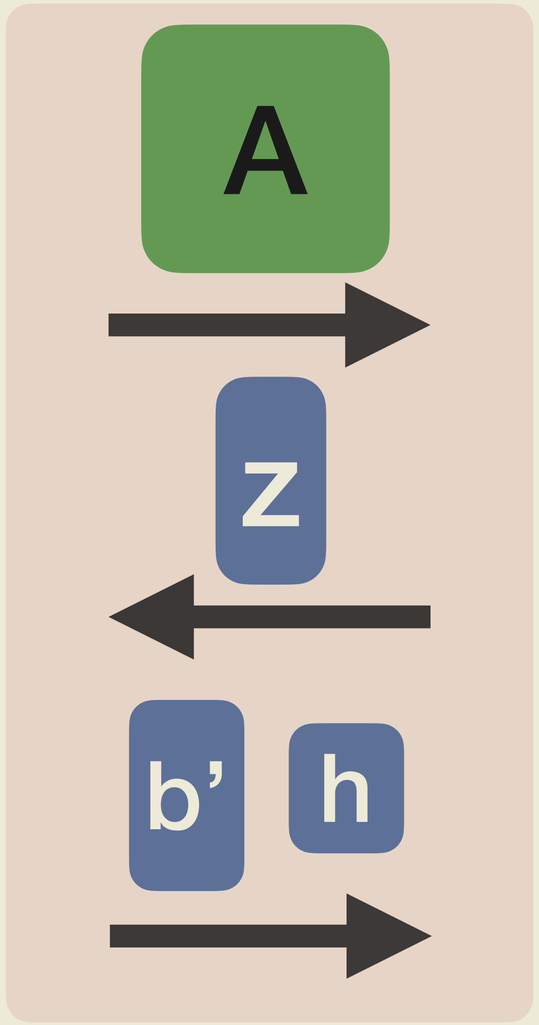
AextLWE

UPKE

Assumption time - Reduction







LWE

AextLWE

UPKE

Assumption time - Reduction

$$b' = b + A\,s' + e'$$

$$h = e' \cdot z + g'$$

UPKE

Assumption time - Reduction

$$b' = b + A\,s' + e'$$

$$h = e' \cdot z + g'$$

h is a hint on e'

should be of $e + e'$

UPKE

Assumption time - Reduction

$$b' = b + A\,s' + e'$$

$$h = e + e' \cdot z - e \cdot z + g'$$

h is a hint on e'

should be of $e + e'$

UPKE

Assumption time - Reduction

$$b' = b + A\,s' + e'$$

$$h = e + e' \cdot z + g$$

$$g = -e \cdot z + g'$$

UPKE

Assumption time - Reduction

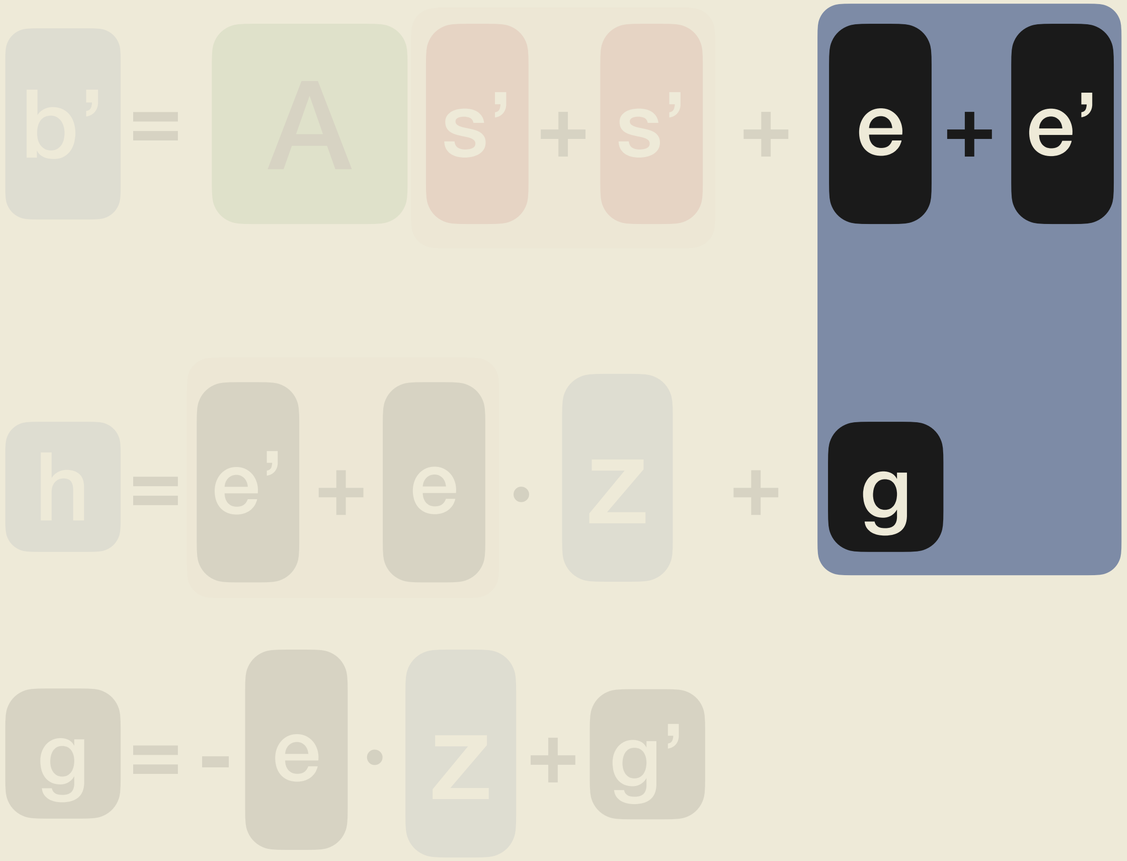
$$b' = A\,s + s' + e + e'$$

$$h = e + e' \cdot z + g$$

$$g = -e \cdot z + g'$$

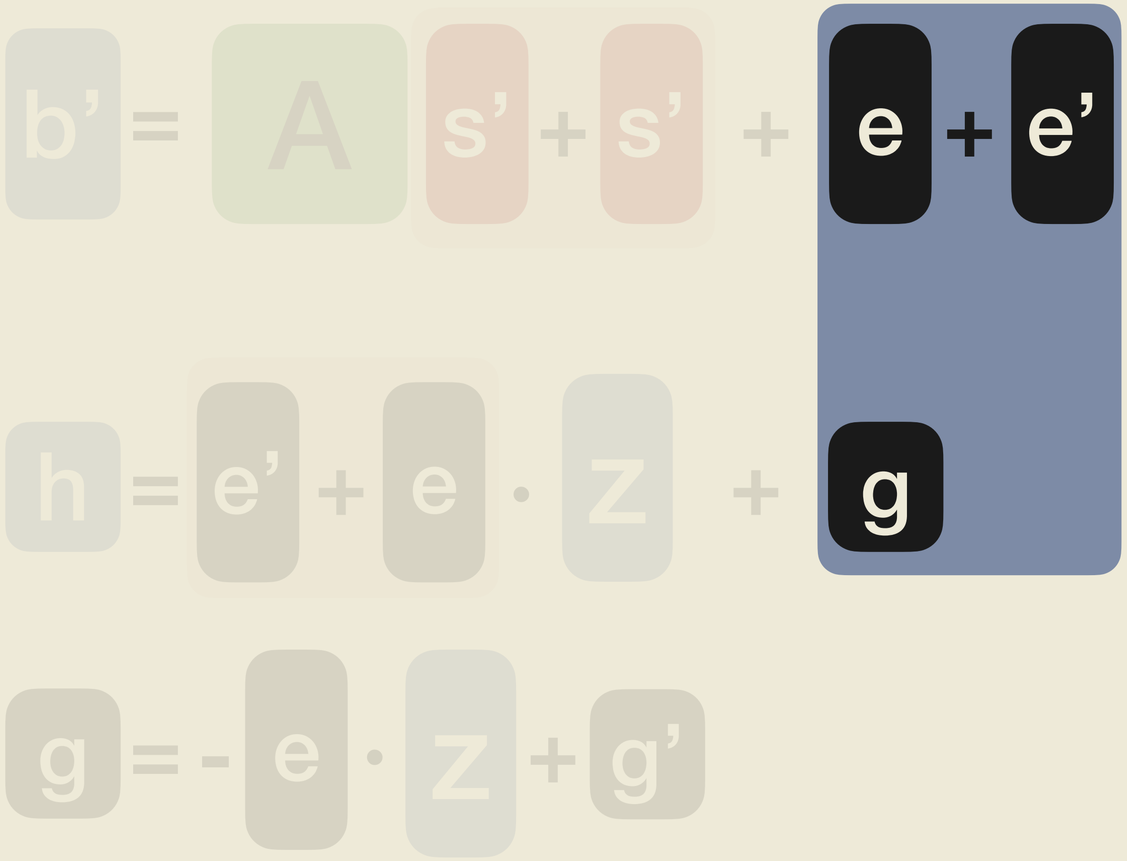
UPKE

Assumption time - Reduction



UPKE

Assumption time - Reduction



Needs to be a spherical Gaussian

UPKE

Assumption time - Reduction

$$b' = A\,s' + s' + e + e'$$

$$h = e' + e \cdot Z + g$$

$$g = -e \cdot Z + g'$$

$$\begin{bmatrix} Id \\ -z^T \end{bmatrix} e + \begin{bmatrix} e' \\ g' \end{bmatrix}$$

UPKE

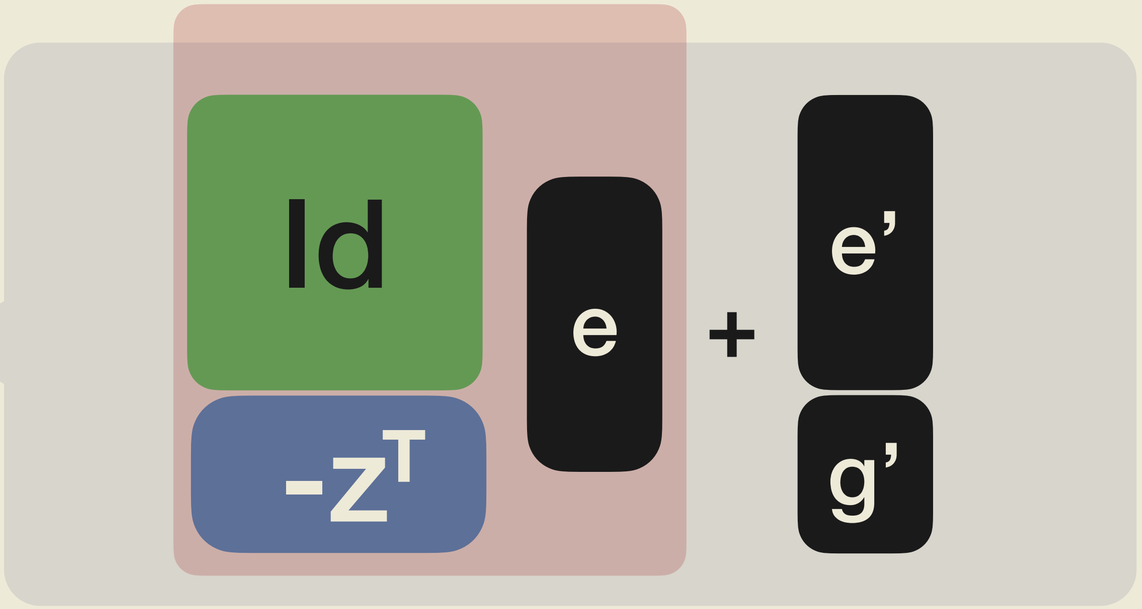
Assumption time - Reduction

$b' = A\,s' + s' + e + e'$

$h = e' + e \cdot Z + g$

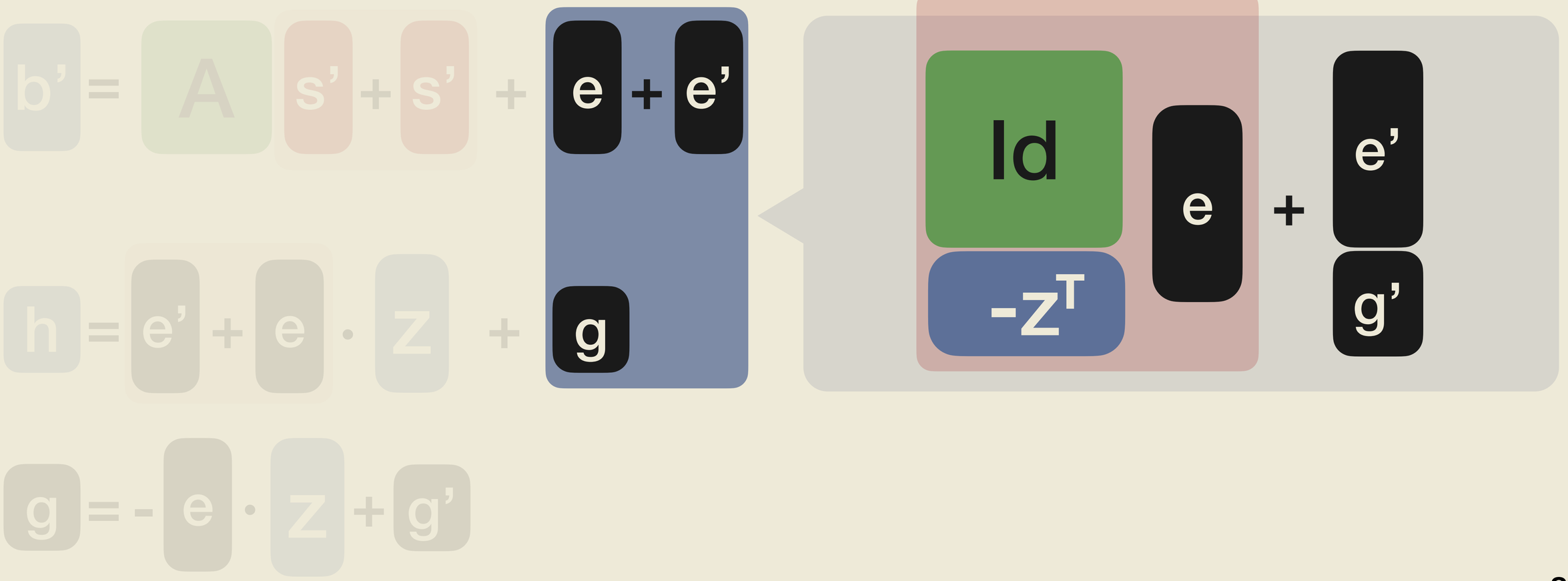
$g = -e \cdot Z + g'$

No control



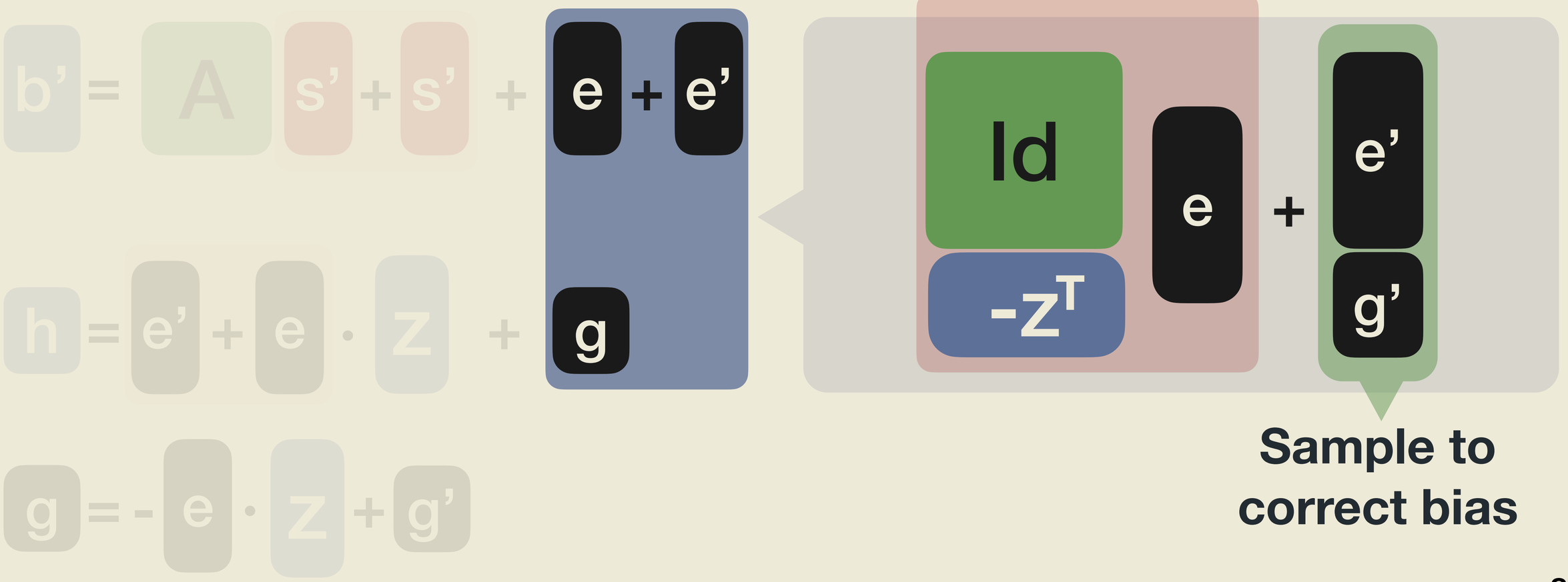
UPKE

Assumption time - Reduction



UPKE

Assumption time - Reduction

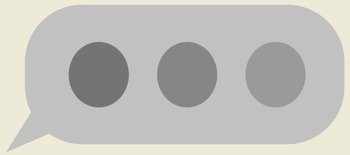


Sizes

Concrete Sizes

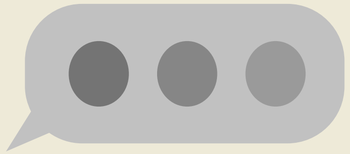
KYBER	ct	up
0 update	0.8 KB	
2^{10} updates	3.0 KB	12 KB
2^{15} updates	5.8 KB	12 KB

Other Contributions



Other Contributions

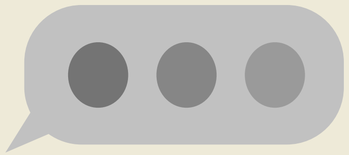
An FO transform for UPKE



Other Contributions

An FO transform for UPKE

CU transform



Other Contributions

An FO transform for UPKE

CU transform

Thanks ! See ia.cr/2023/1400 for more details