Updatable Public Key Encryption

From Lattices

and efficient btw

Calvin Abou Haidar - Journées C2

Updatable Public Key Encryption

Plan

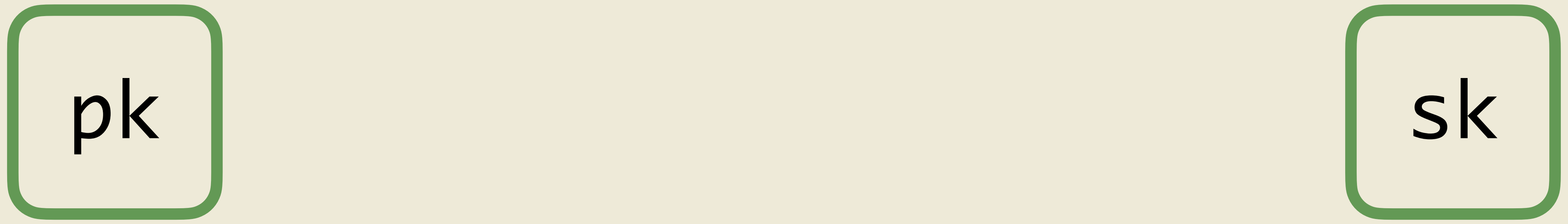
Definitions & Secure Messaging

Construction

A new assumption

Public Key Encryption

Definition

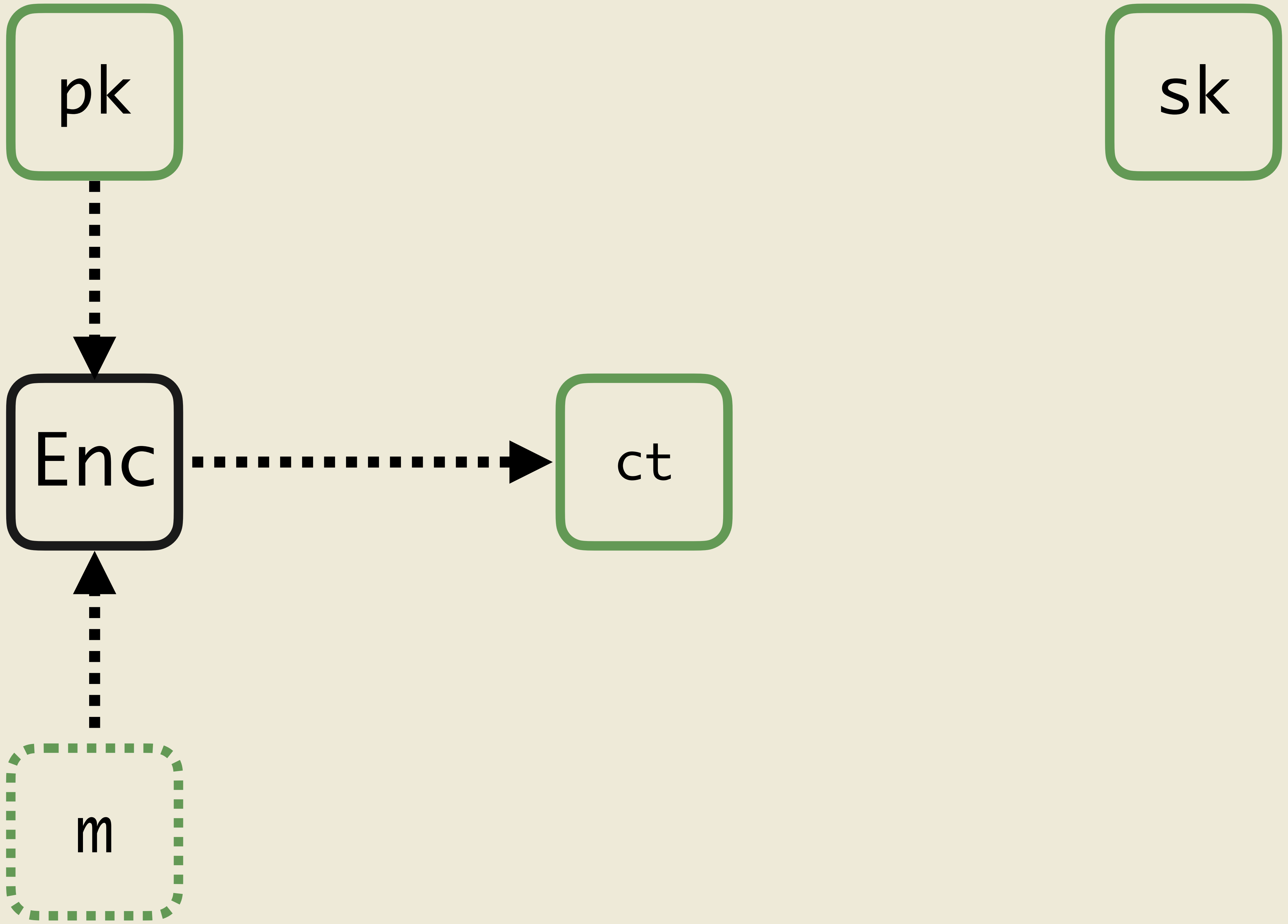


pk

sk

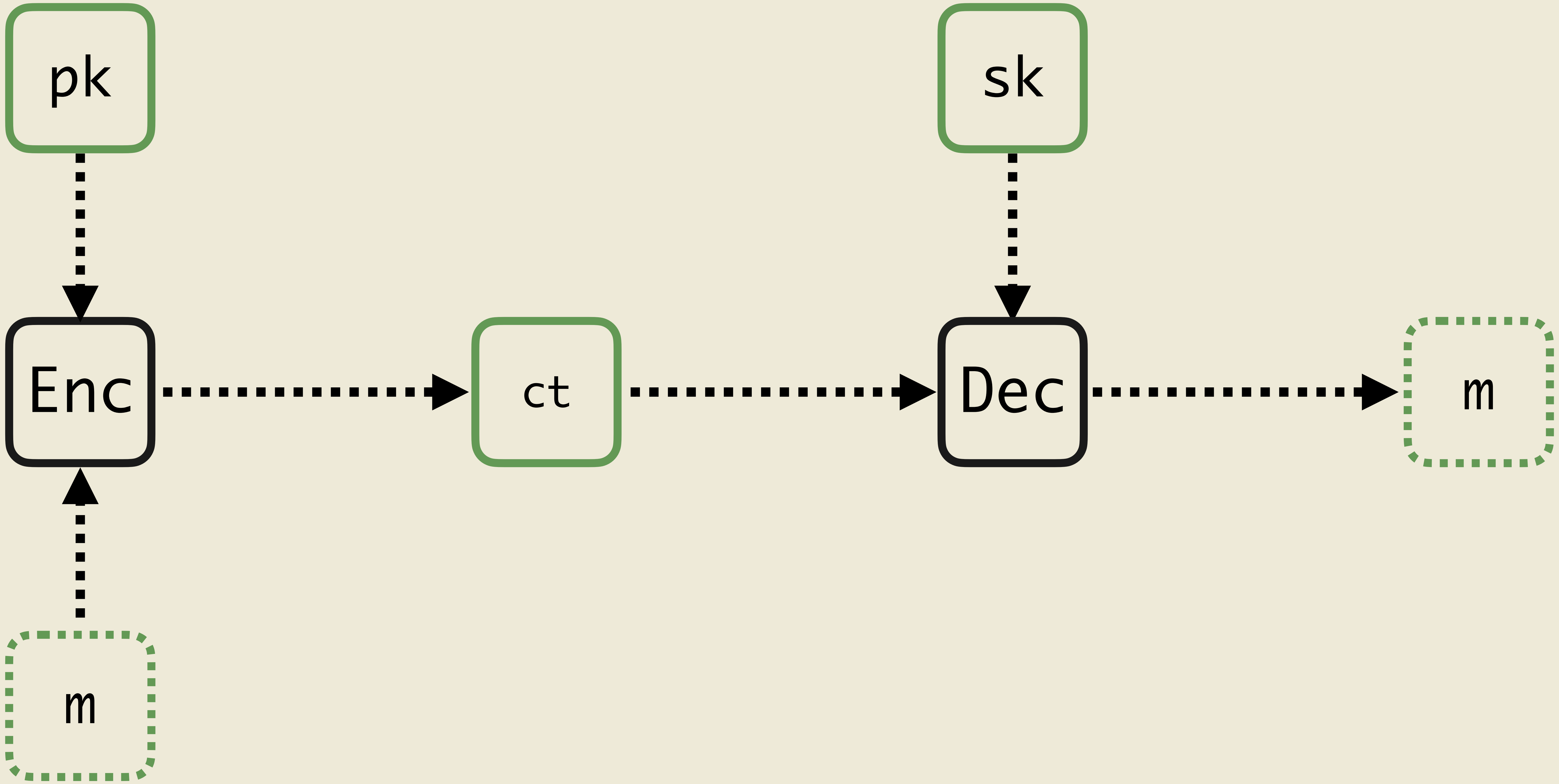
Public Key Encryption

Definition



Public Key Encryption

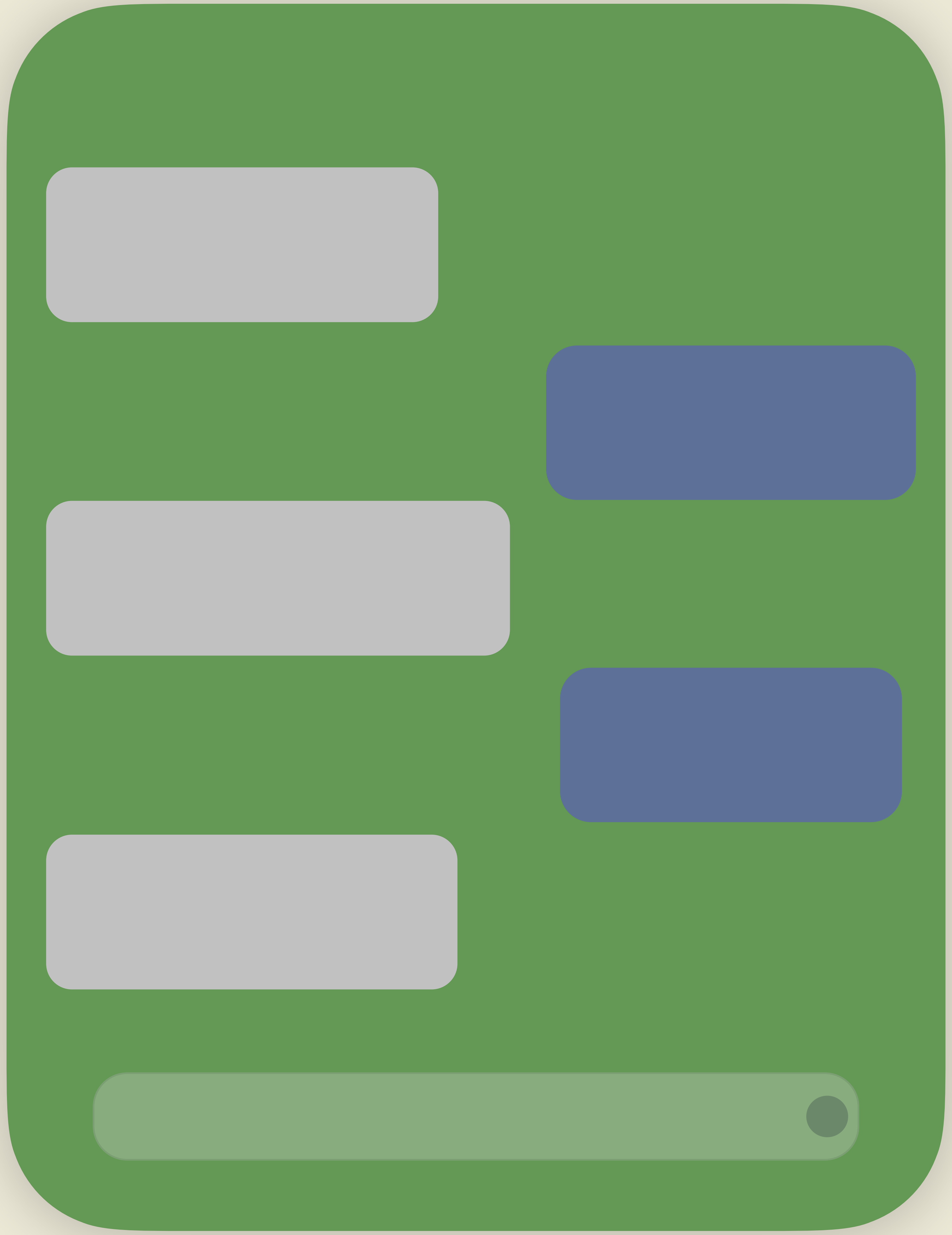
Definition



Secure Messaging

A quick introduction

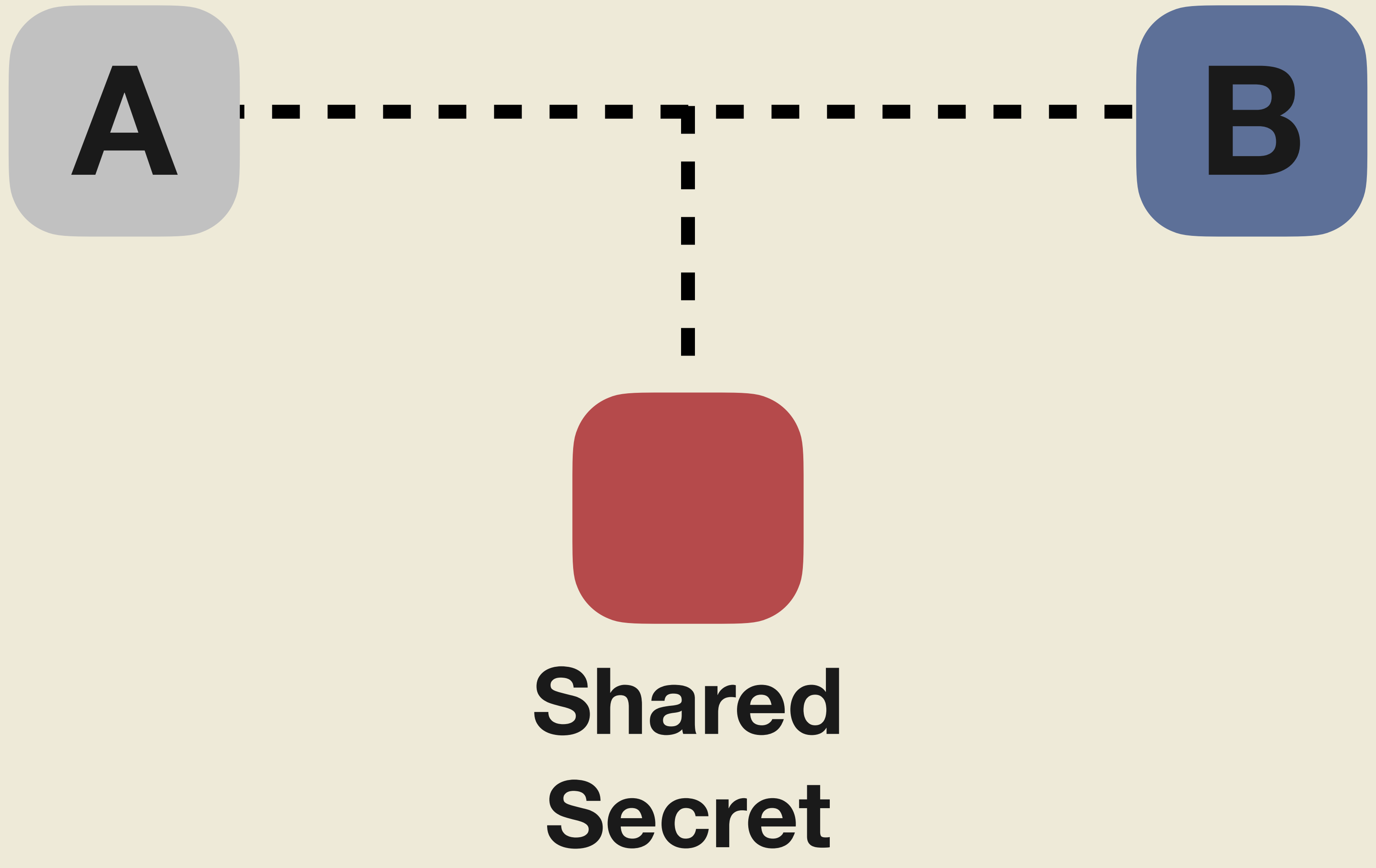
- Signal
- WhatsApp
- Et al.

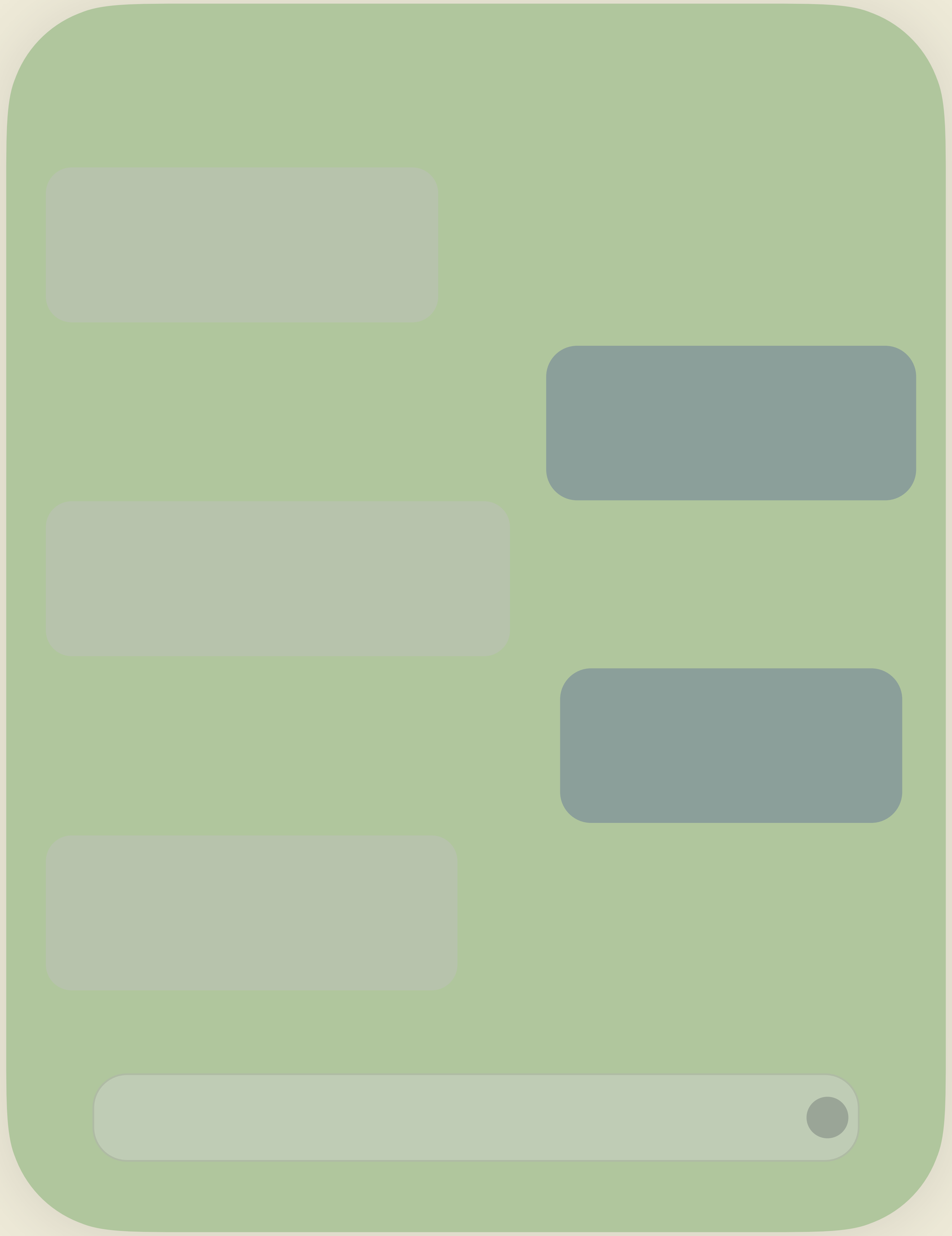


Secure Messaging

A quick introduction

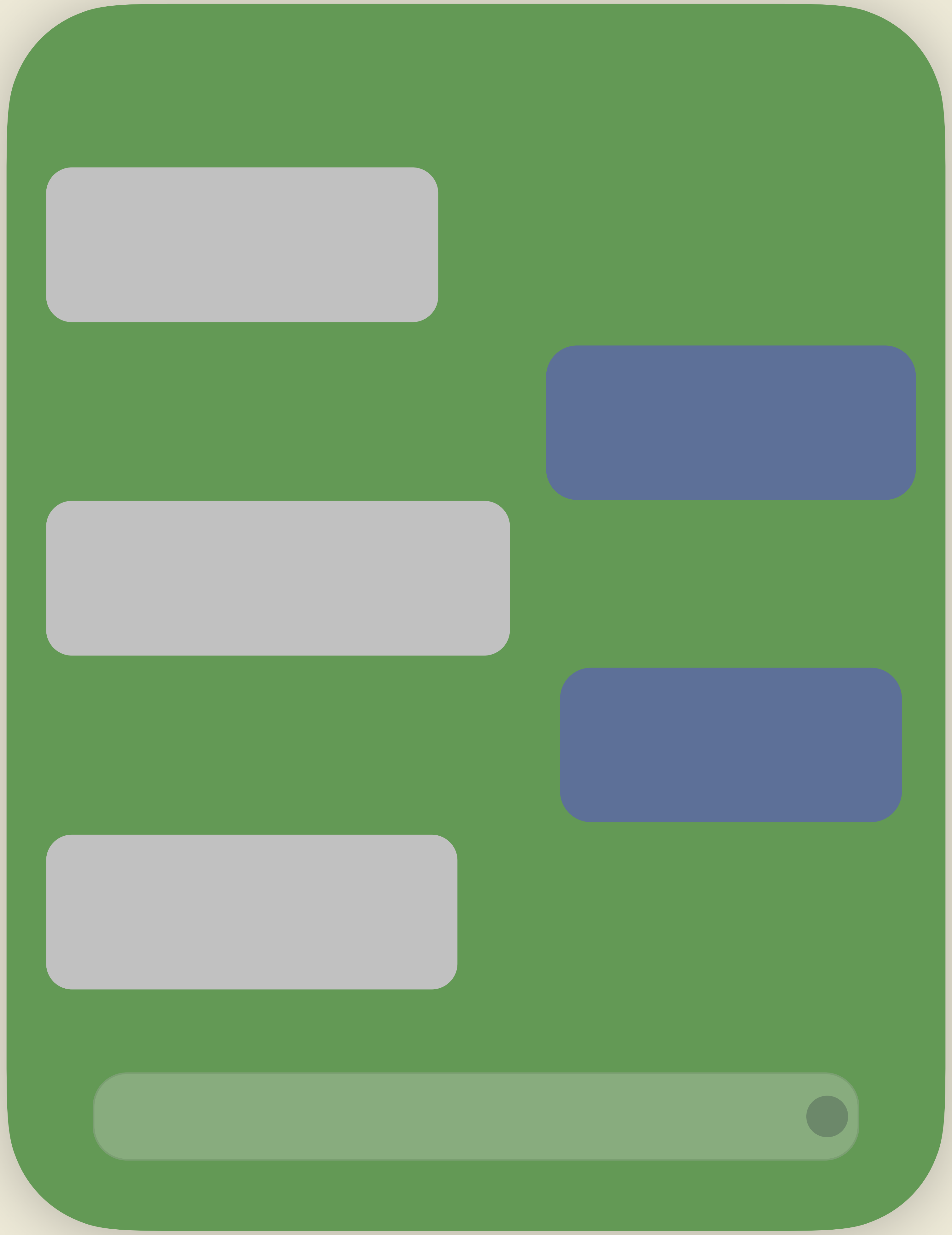
Key Exchange Phase





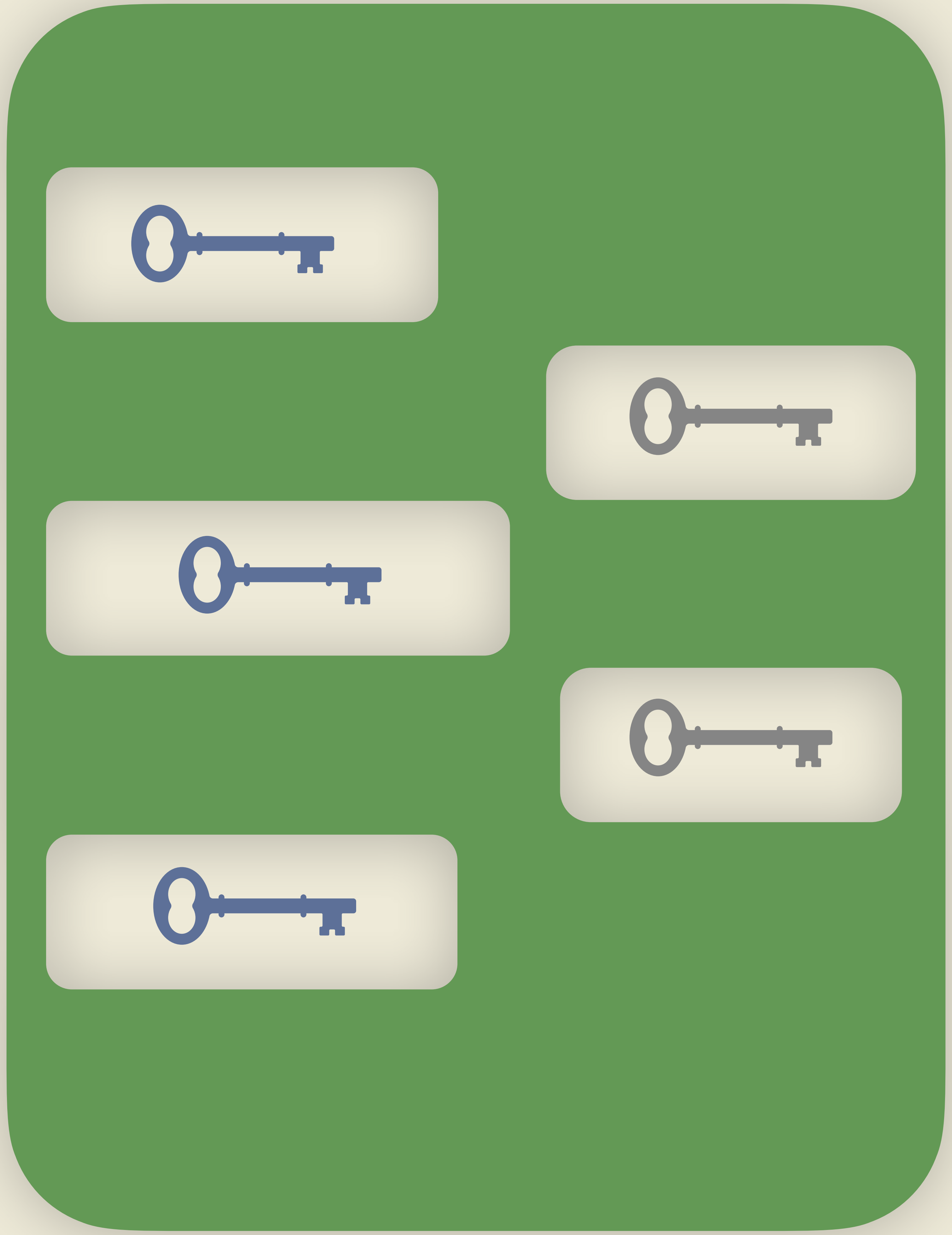
Secure Messaging

A quick introduction



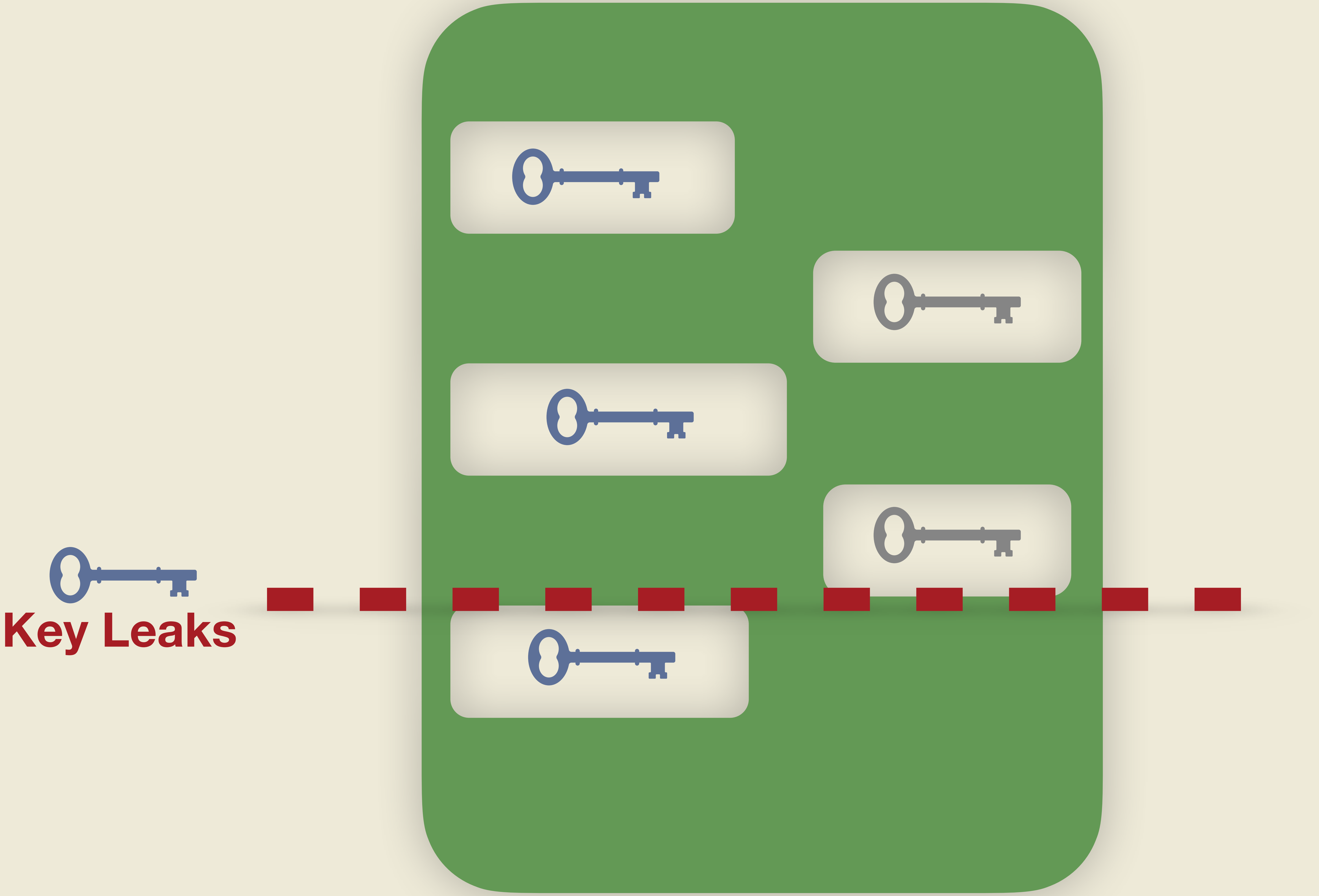
Secure Messaging

A quick introduction



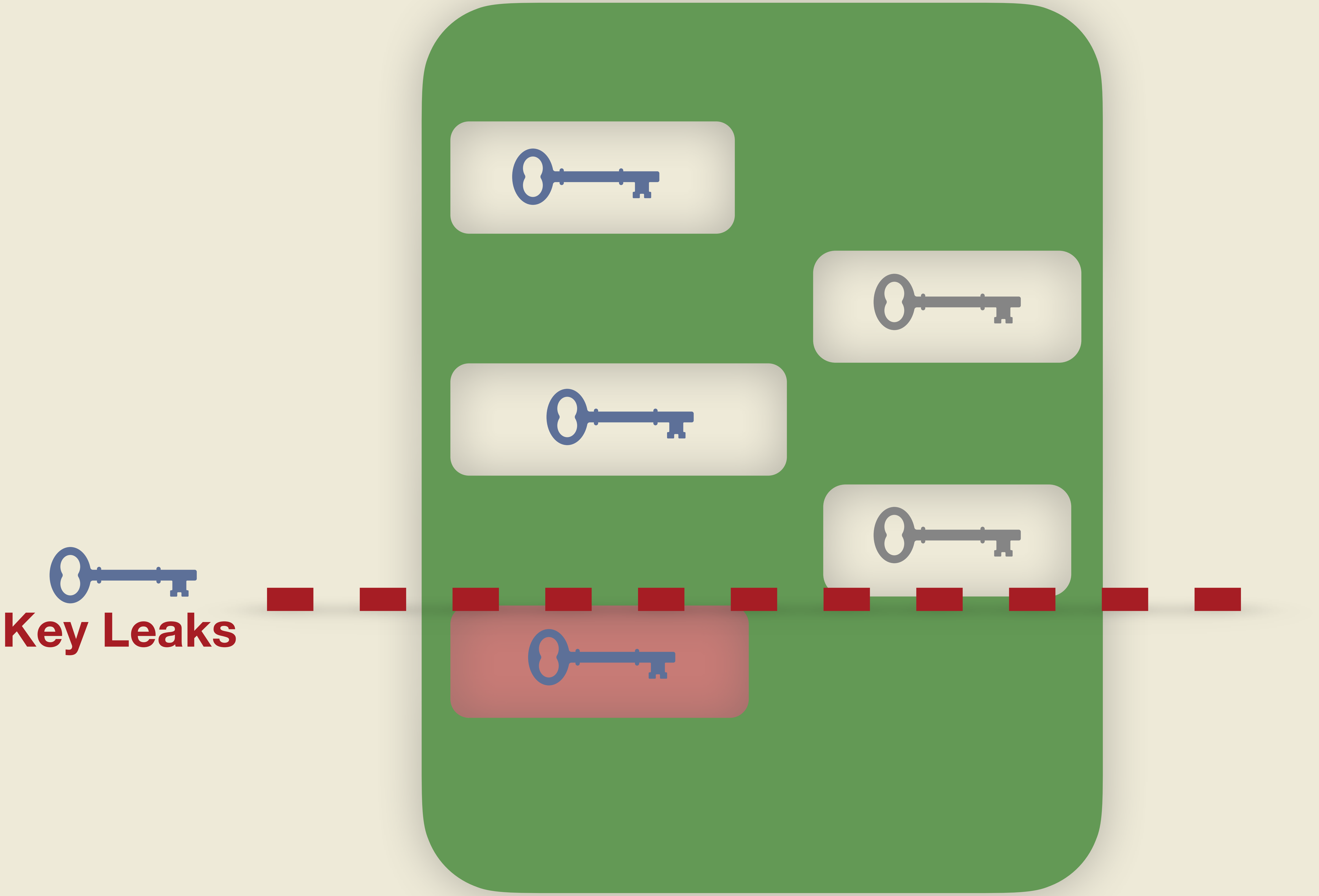
Secure Messaging

A quick introduction



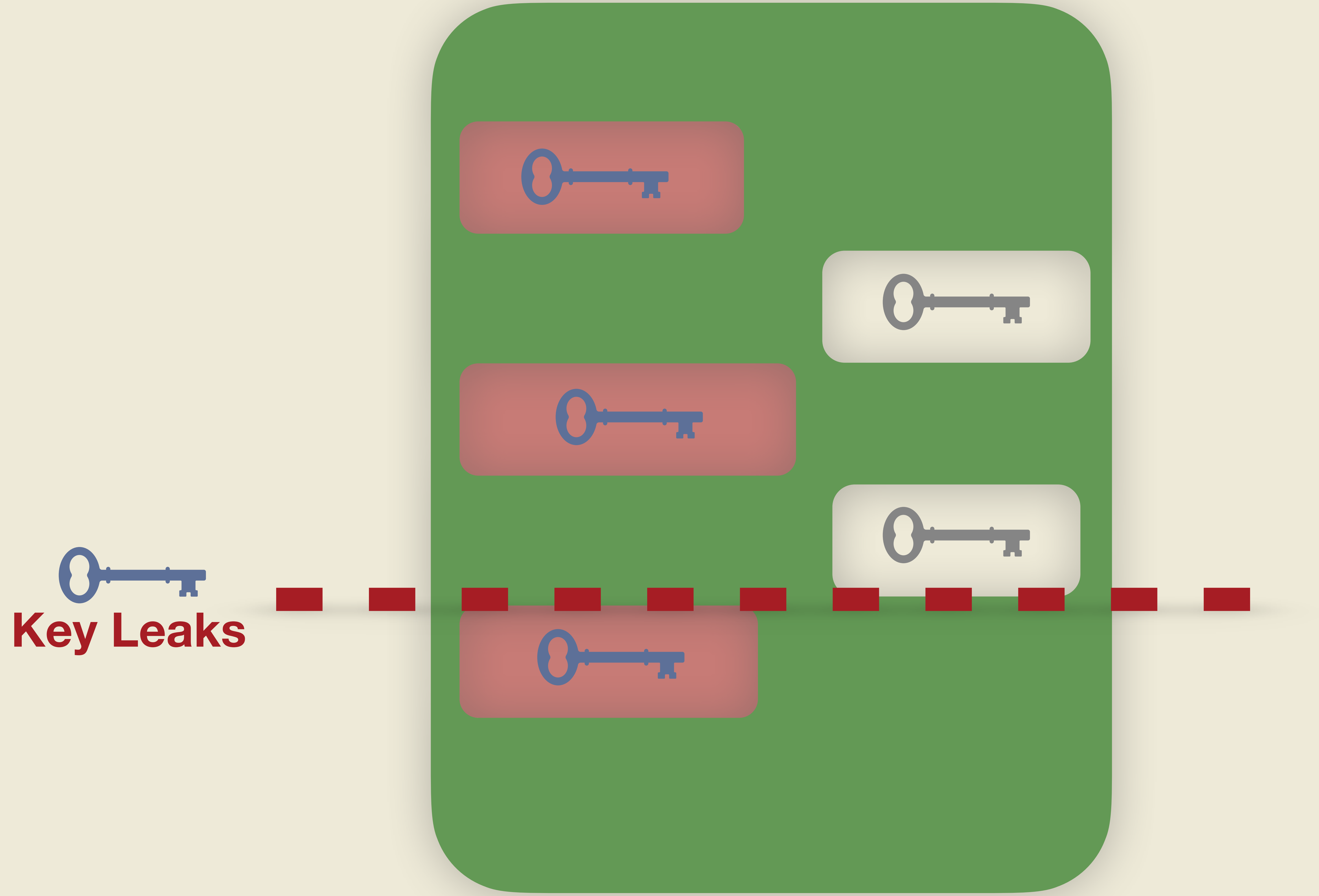
Secure Messaging

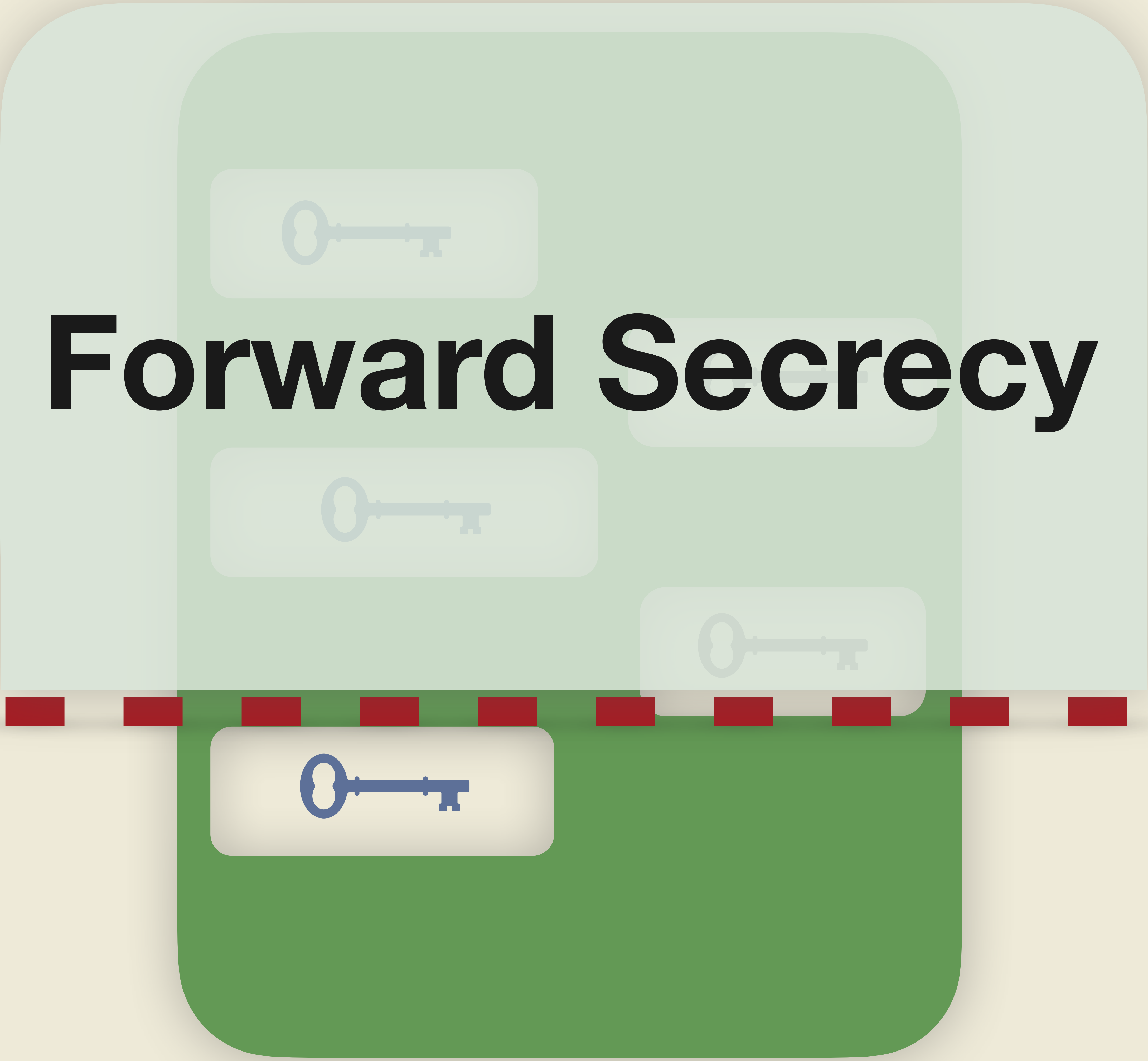
A quick introduction



Secure Messaging

A quick introduction

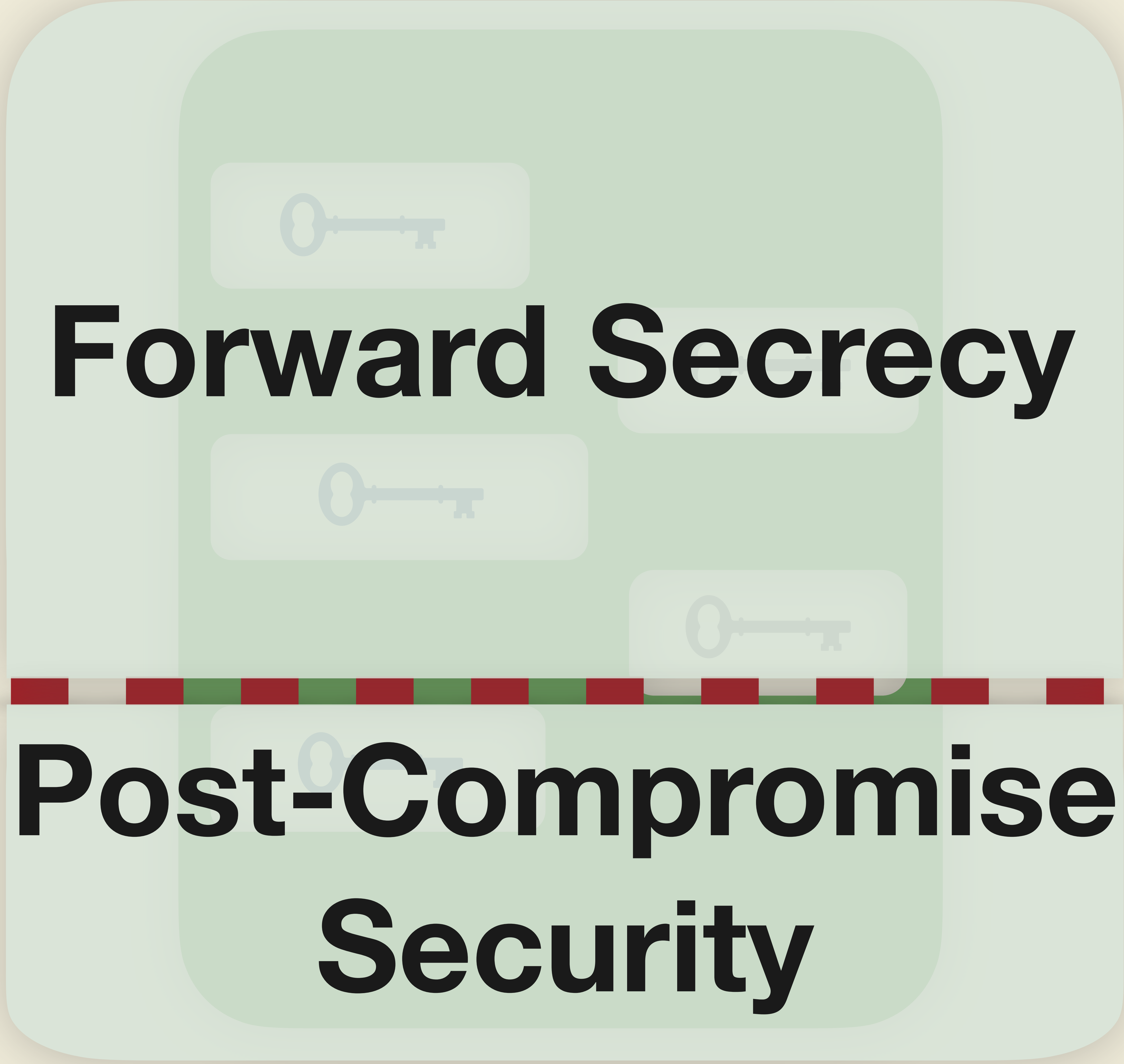




Forward Secrecy

Secure Messaging

A quick introduction



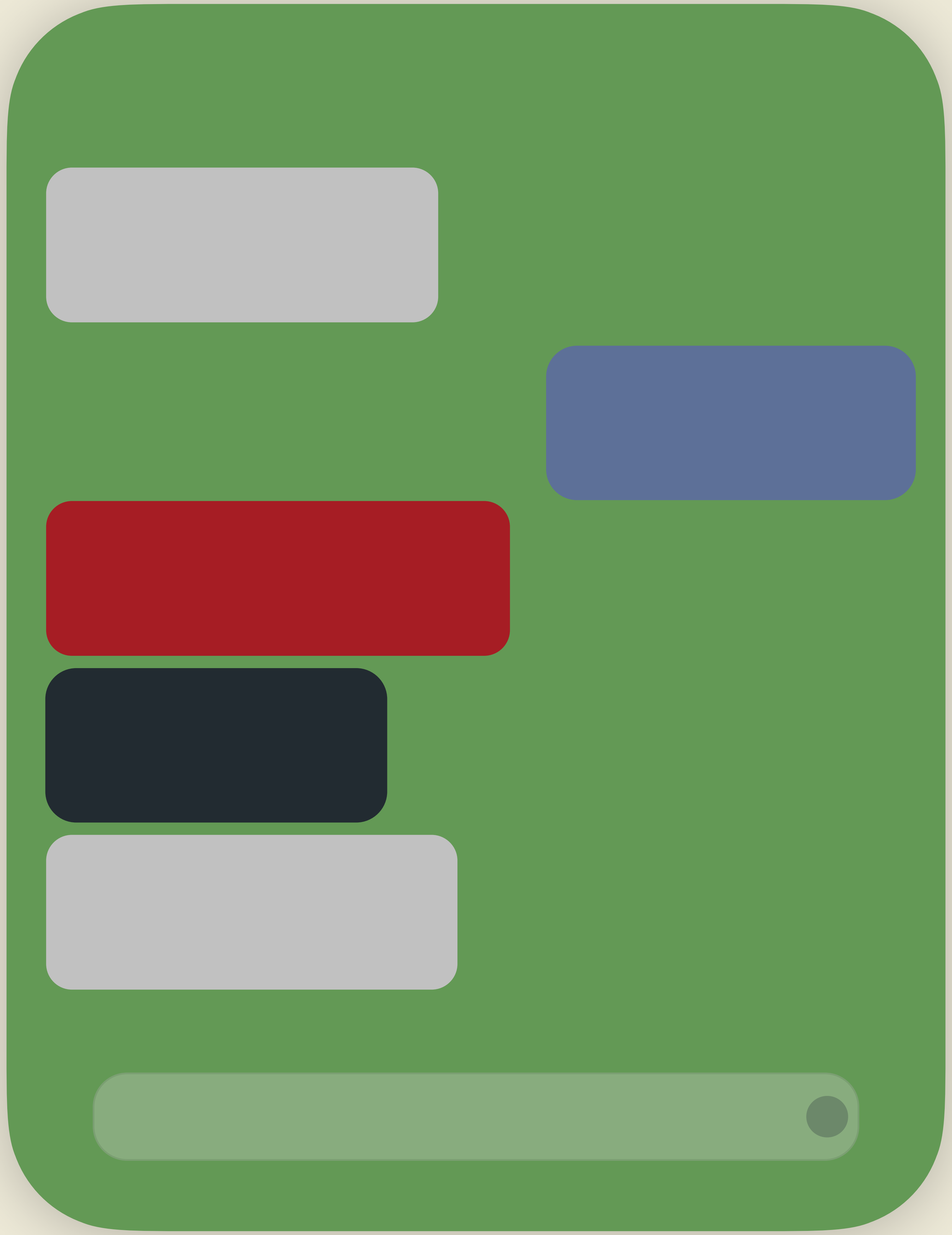
Forward Secrecy

Post-Compromise Security

Forward Secrecy

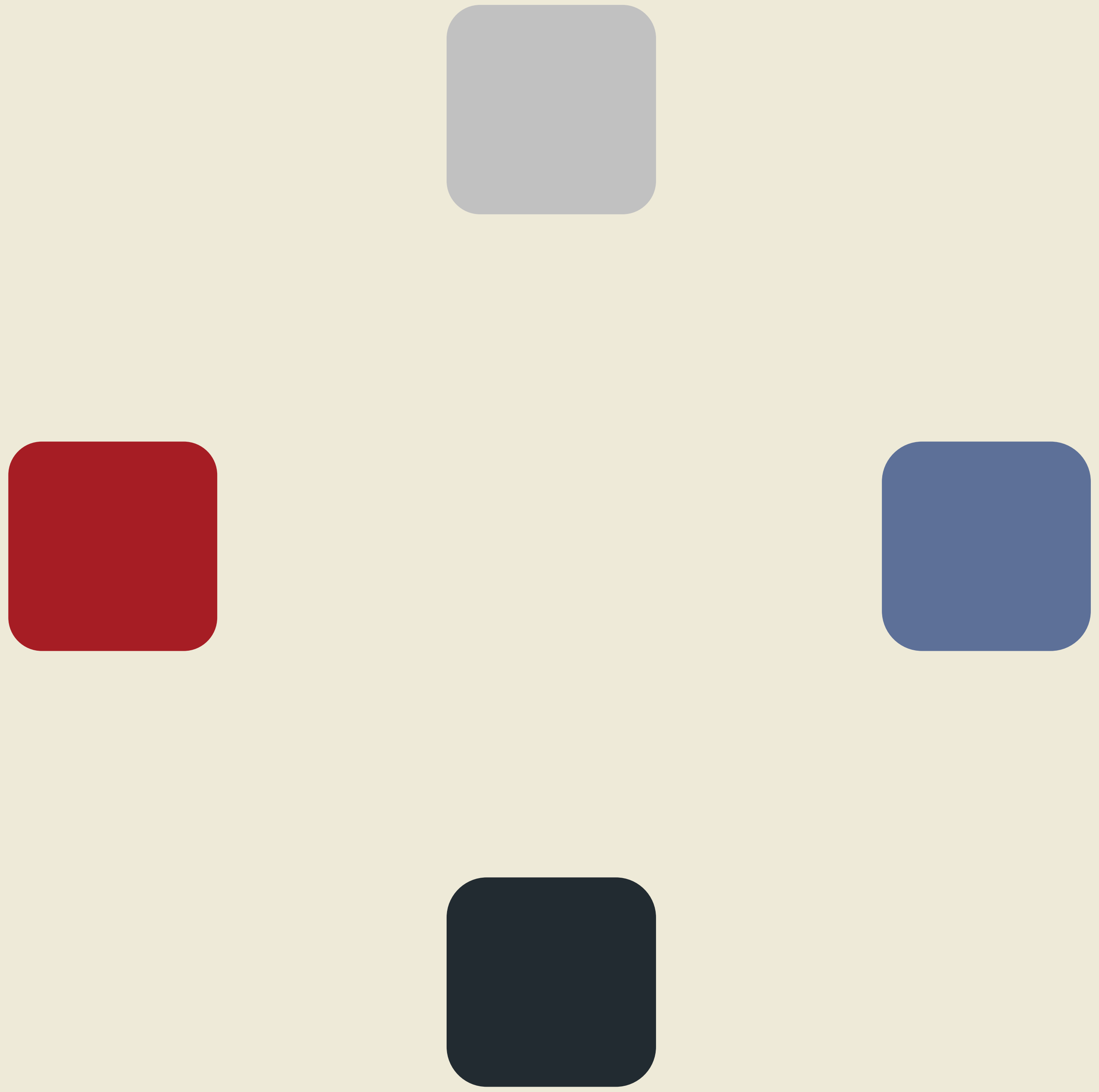
Group Messaging

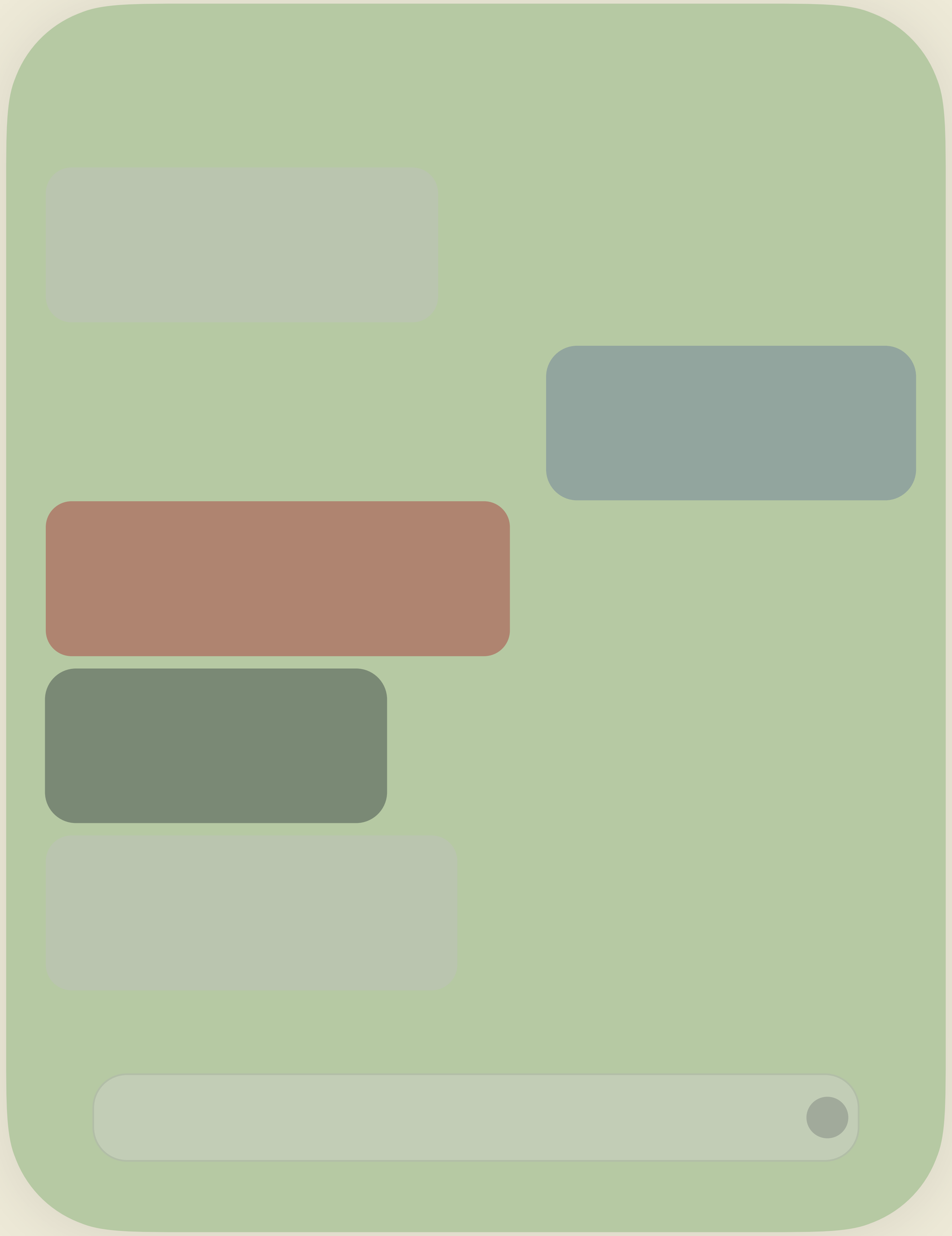
Here comes trouble



Group Messaging

Here comes trouble

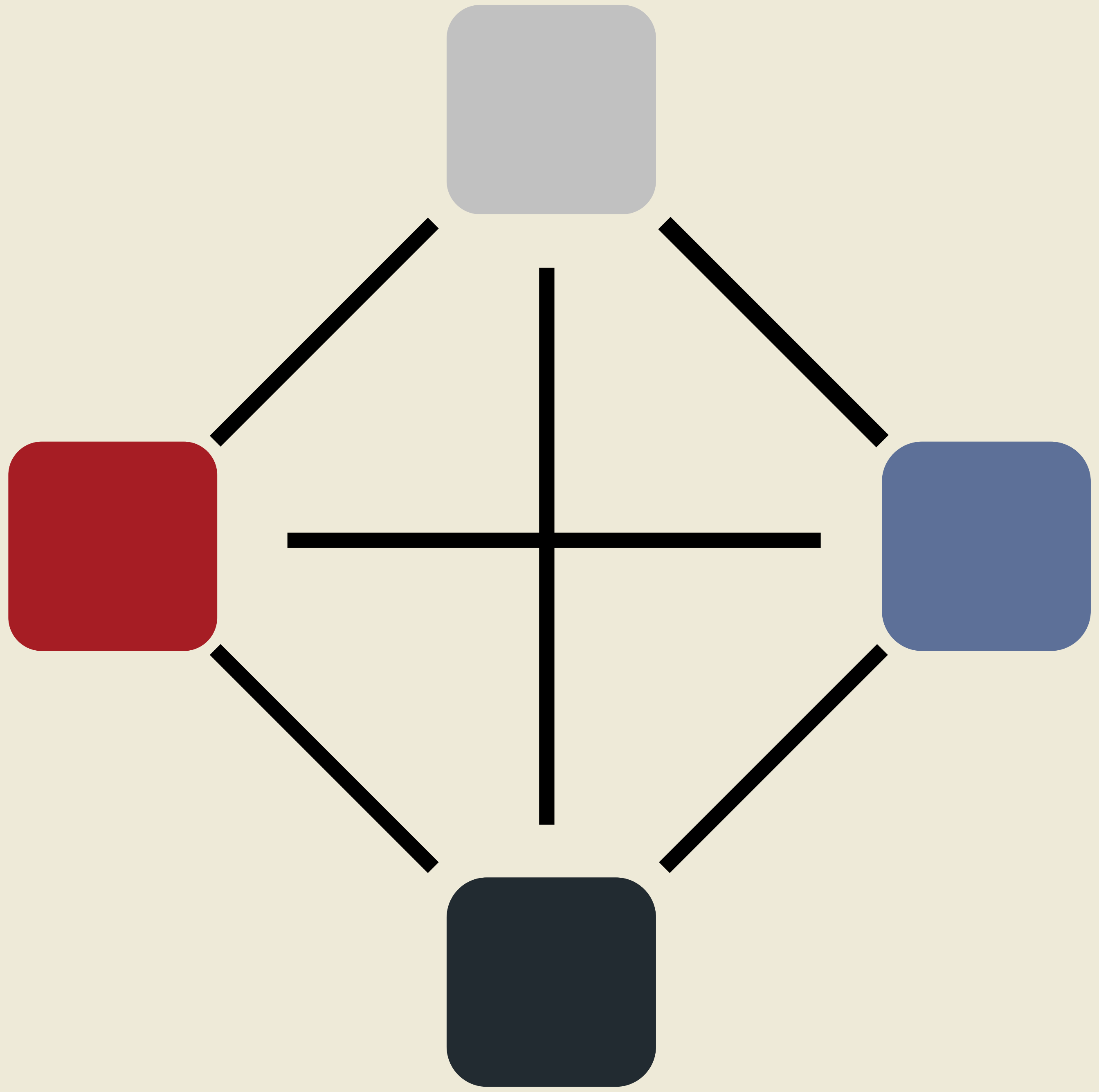




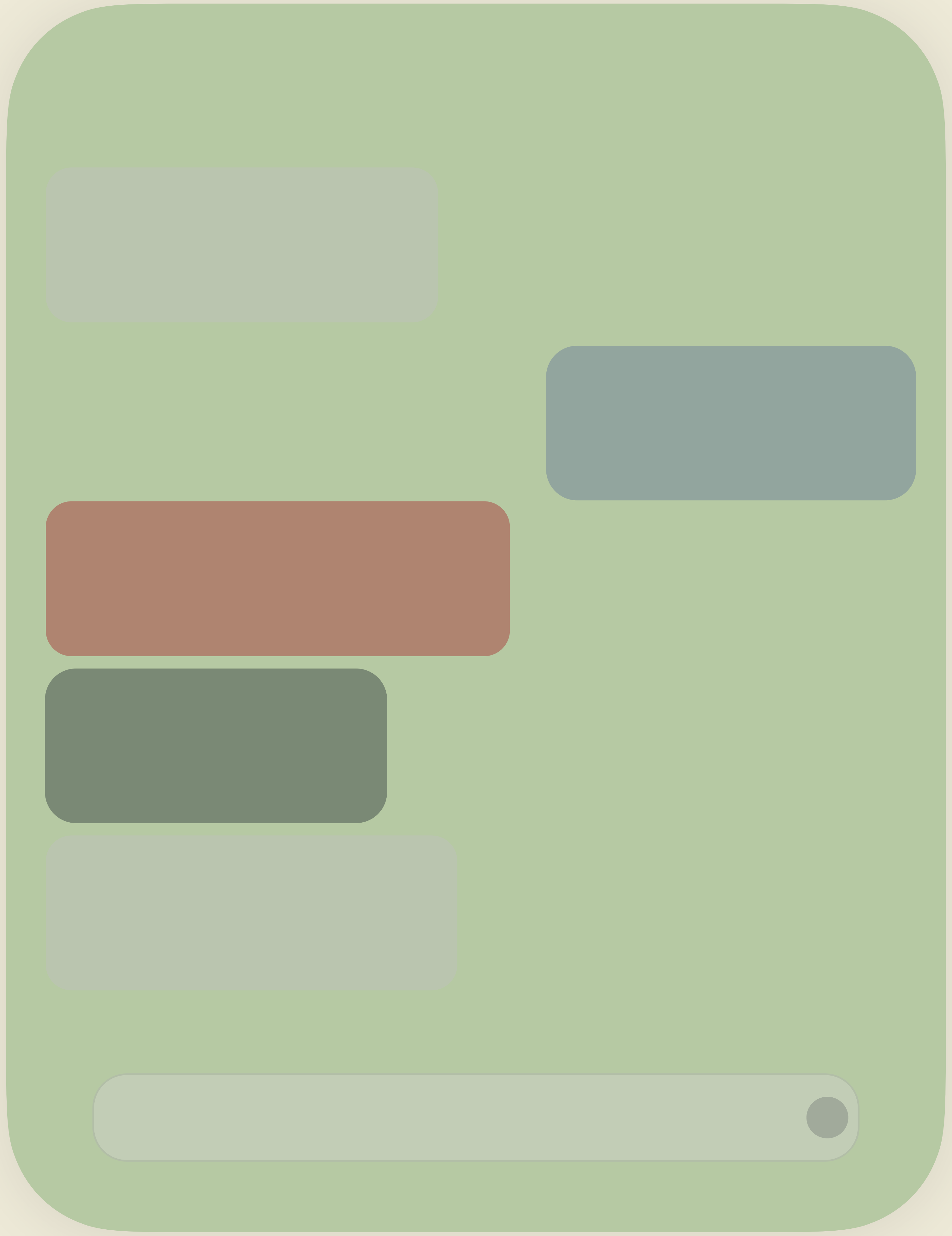
Signal

Group Messaging

Here comes trouble

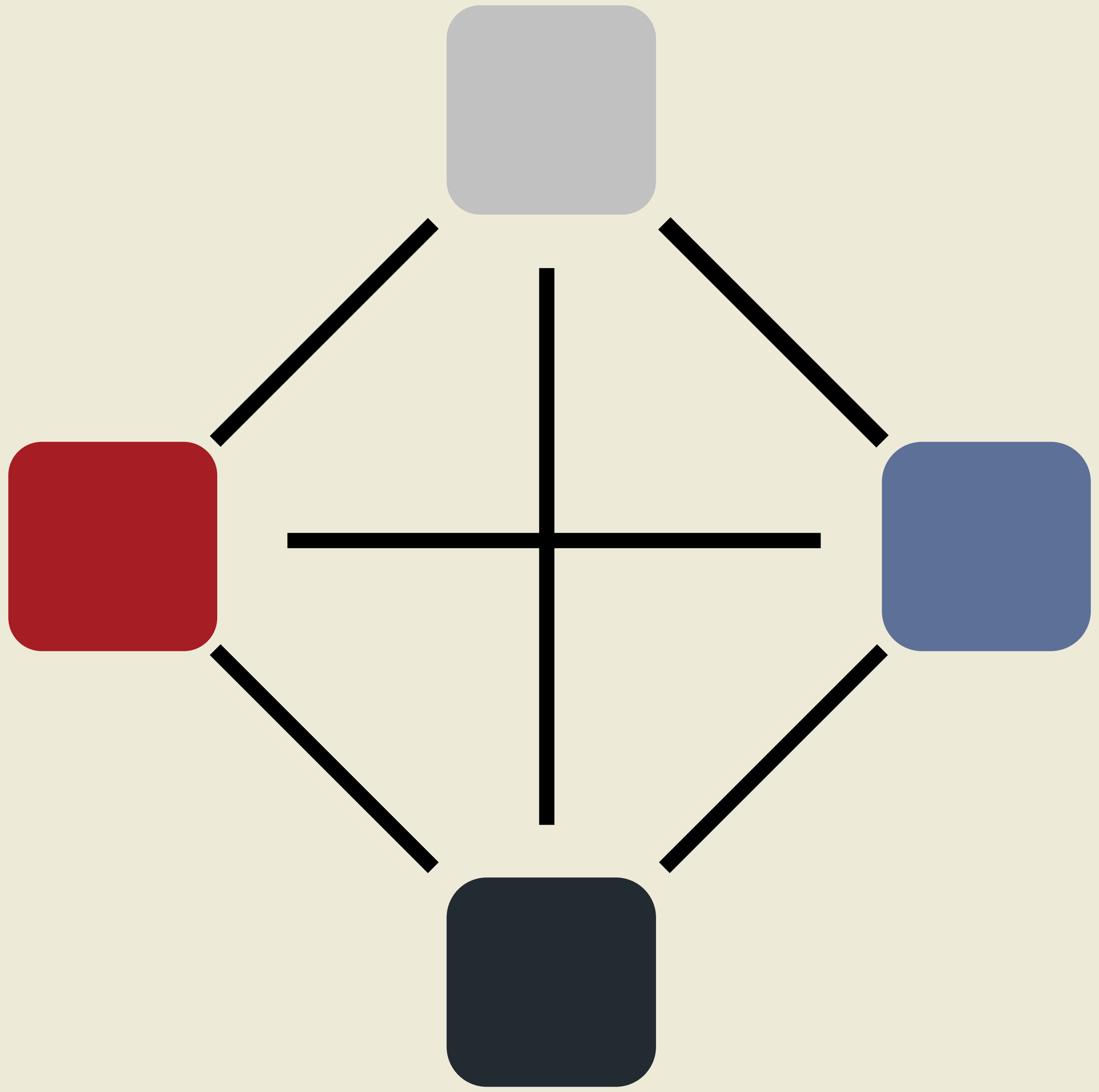


Signal

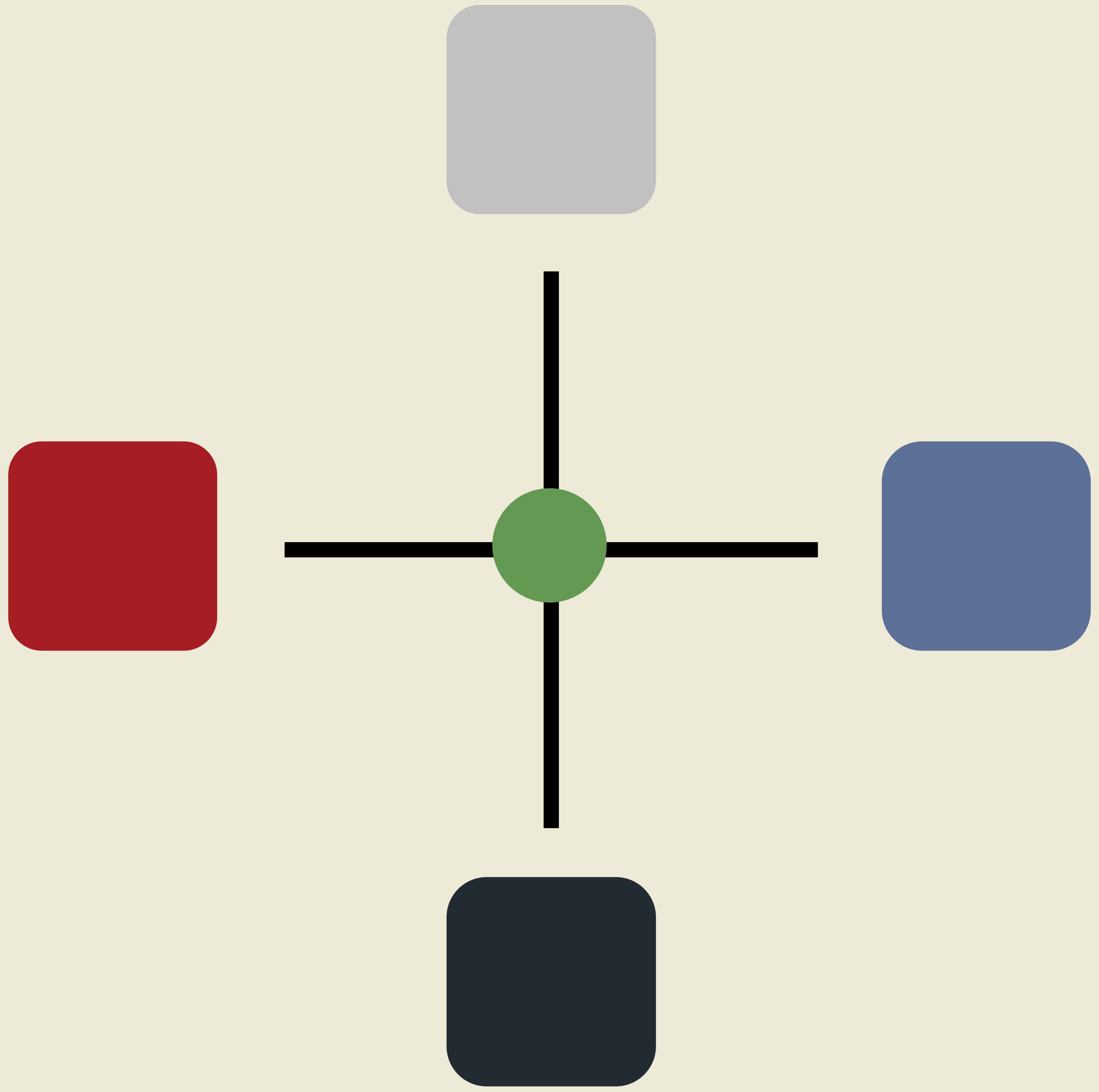


Group Messaging

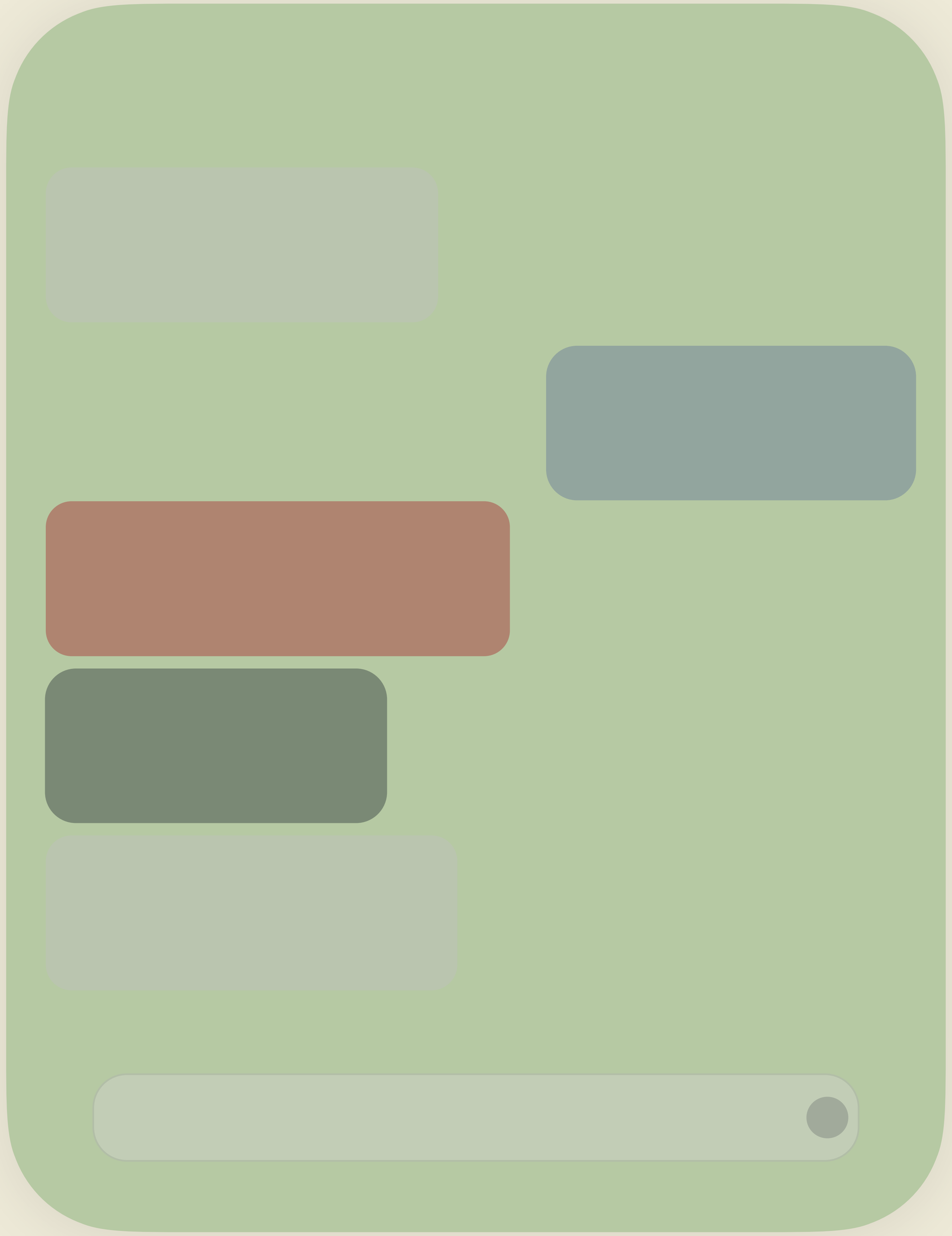
Here comes trouble



Signal

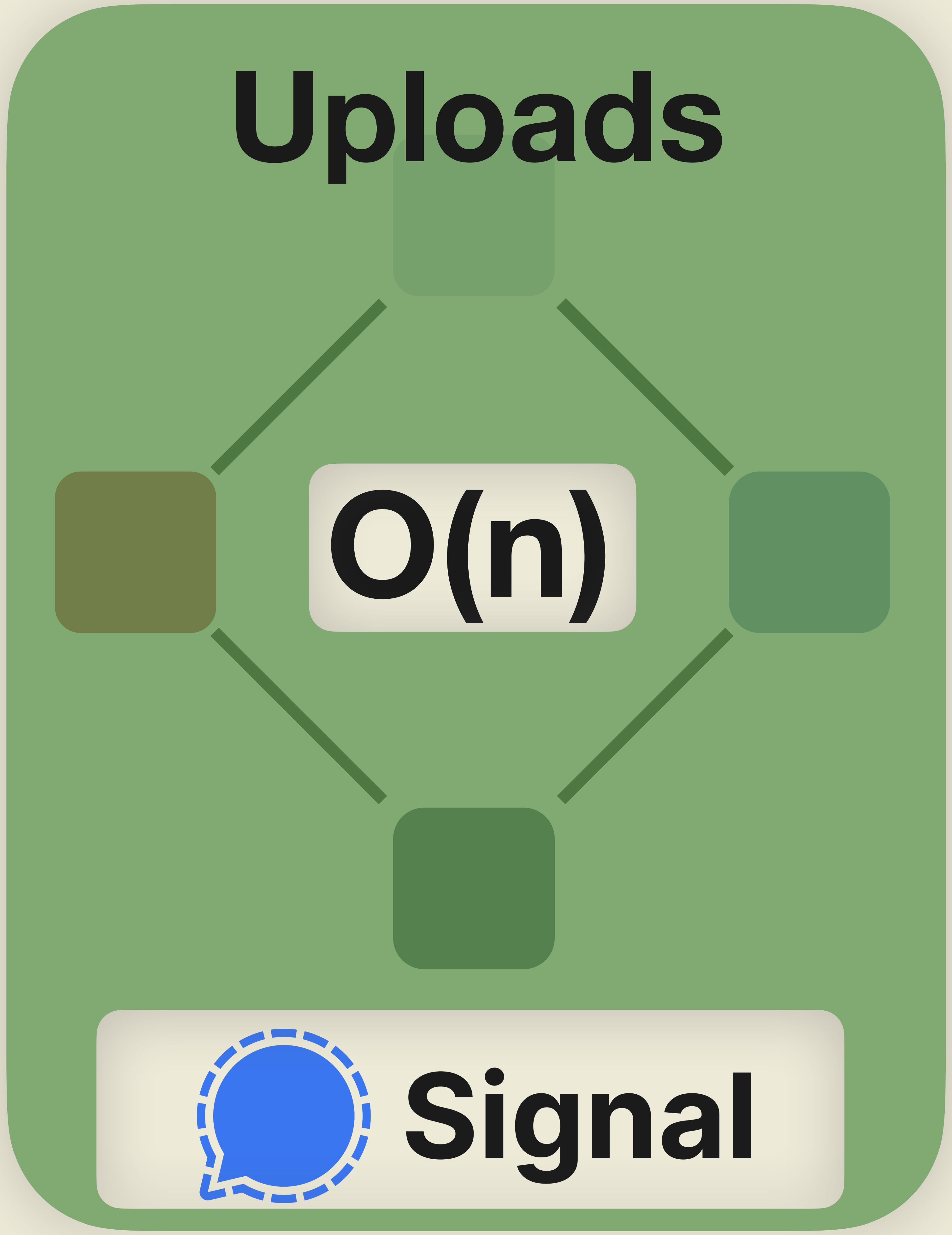


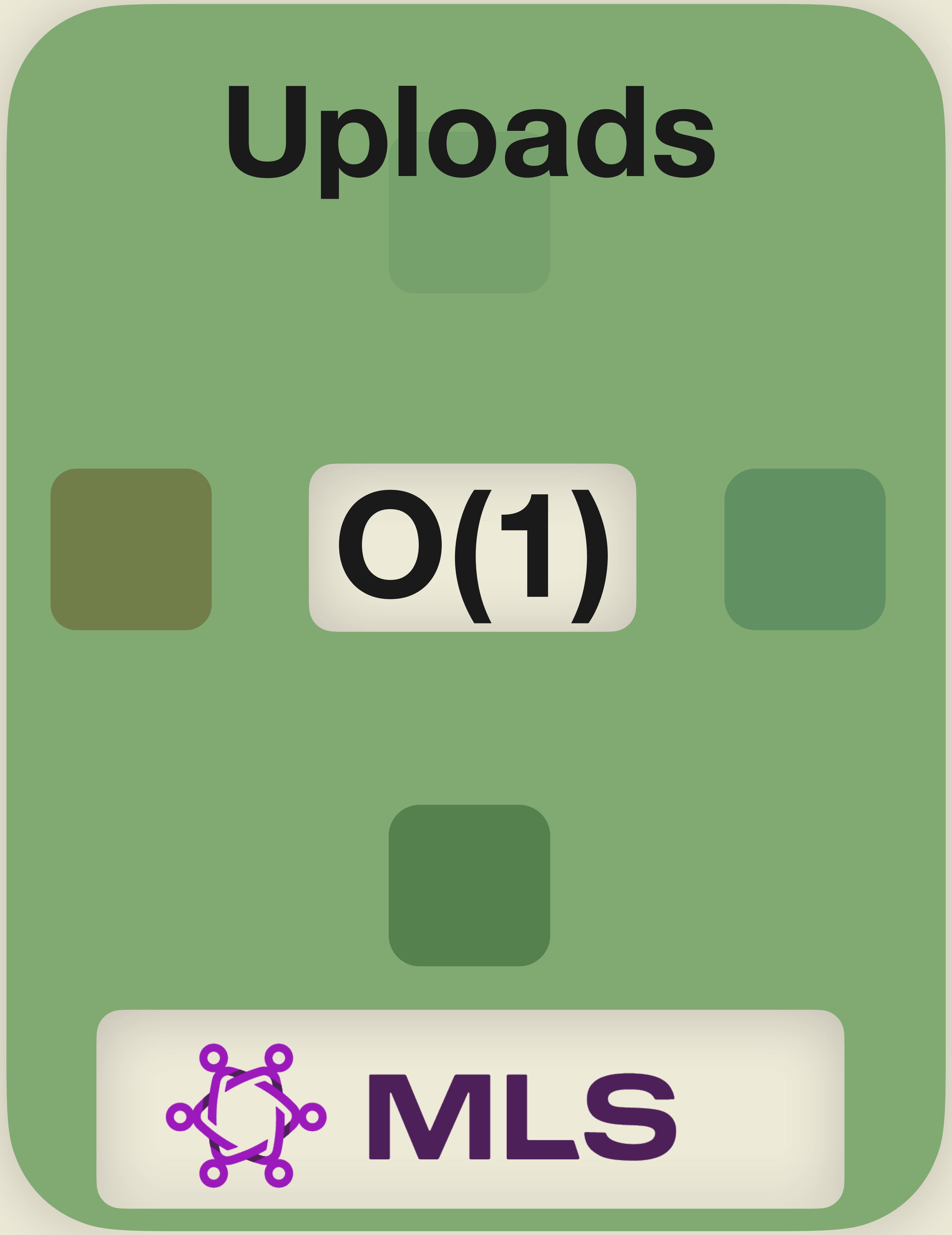
MLS

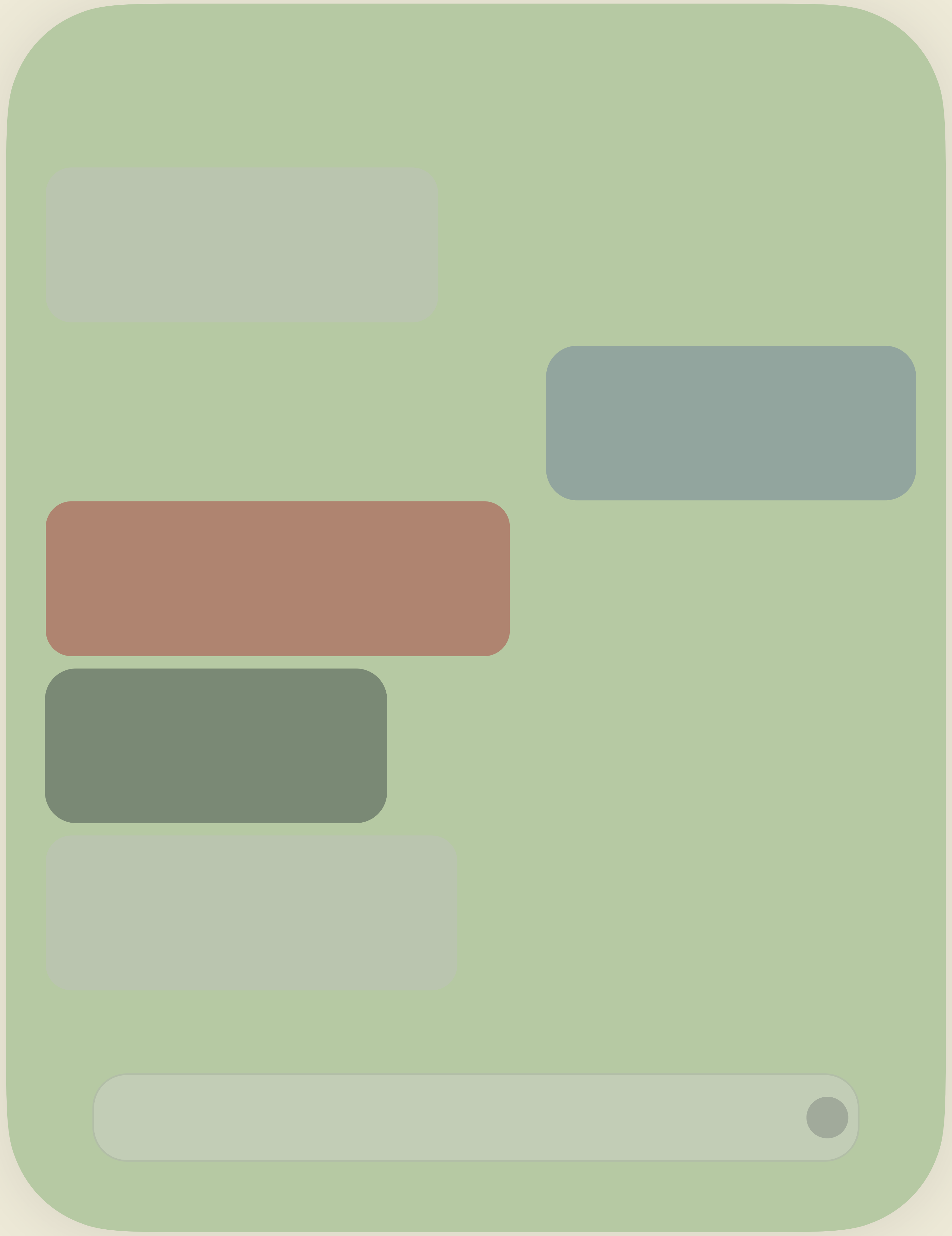


Group Messaging

Here comes trouble



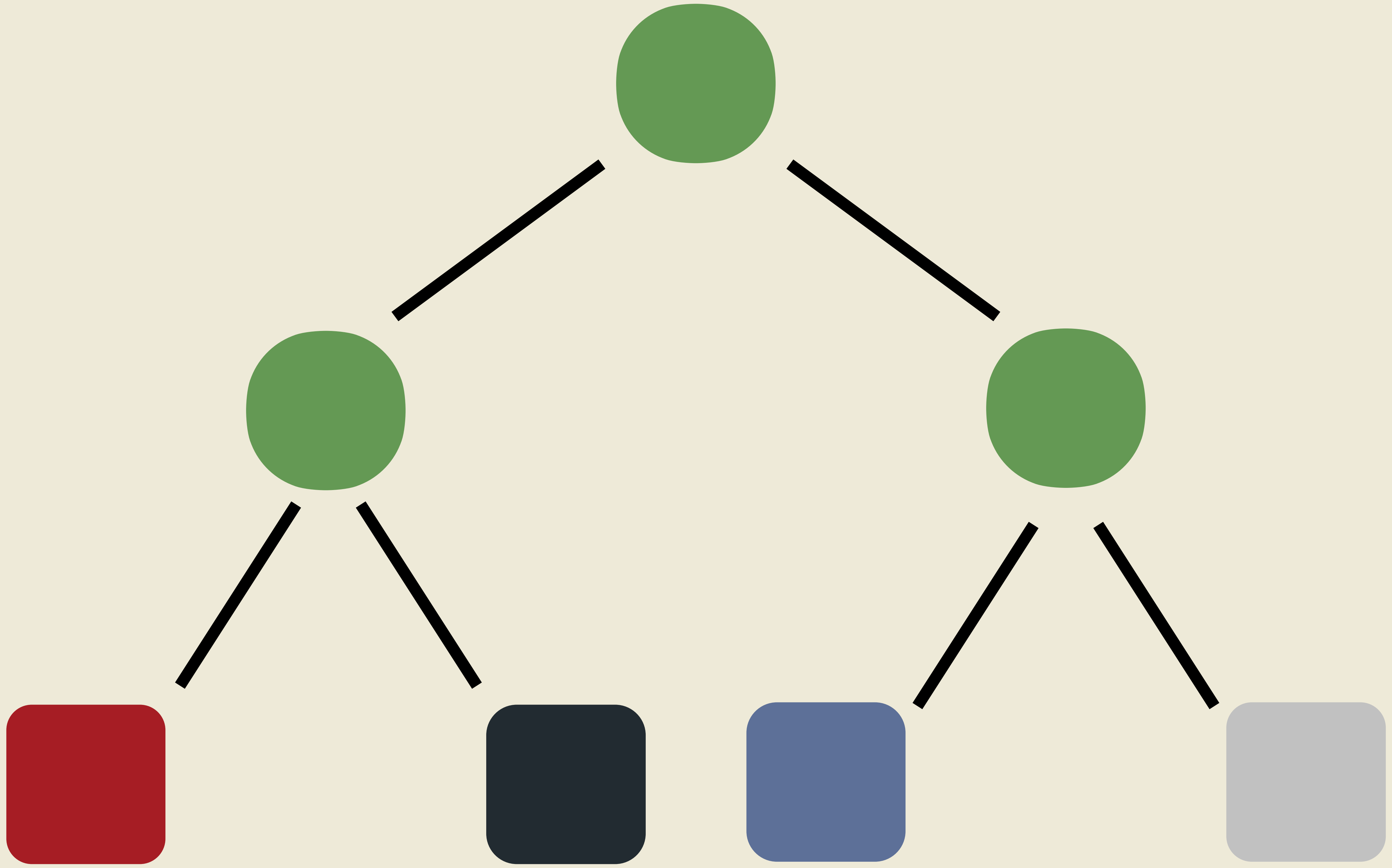




Group Messaging

Continuous Group Key Agreement

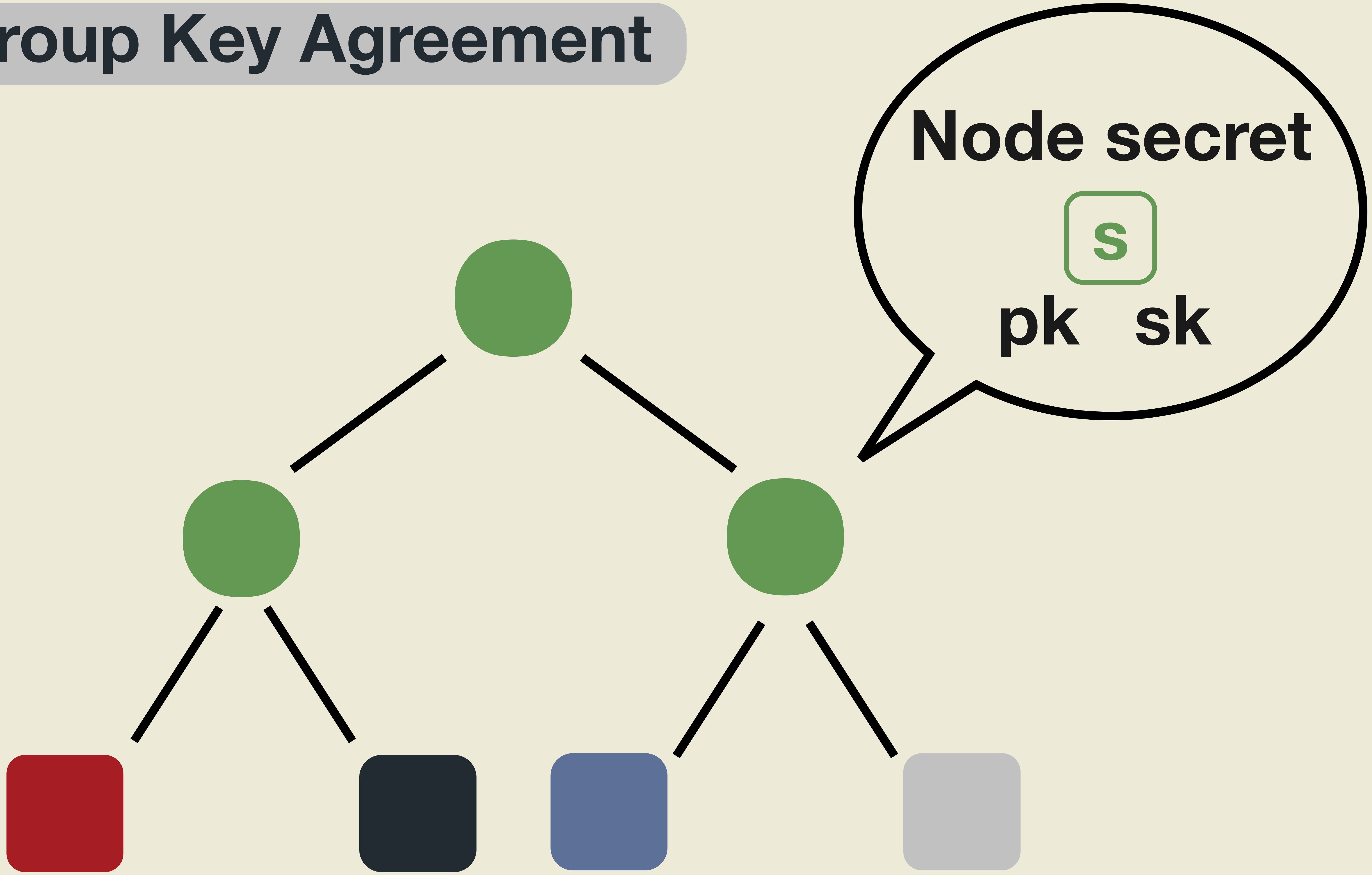
TreeKEM



Group Messaging

Continuous Group Key Agreement

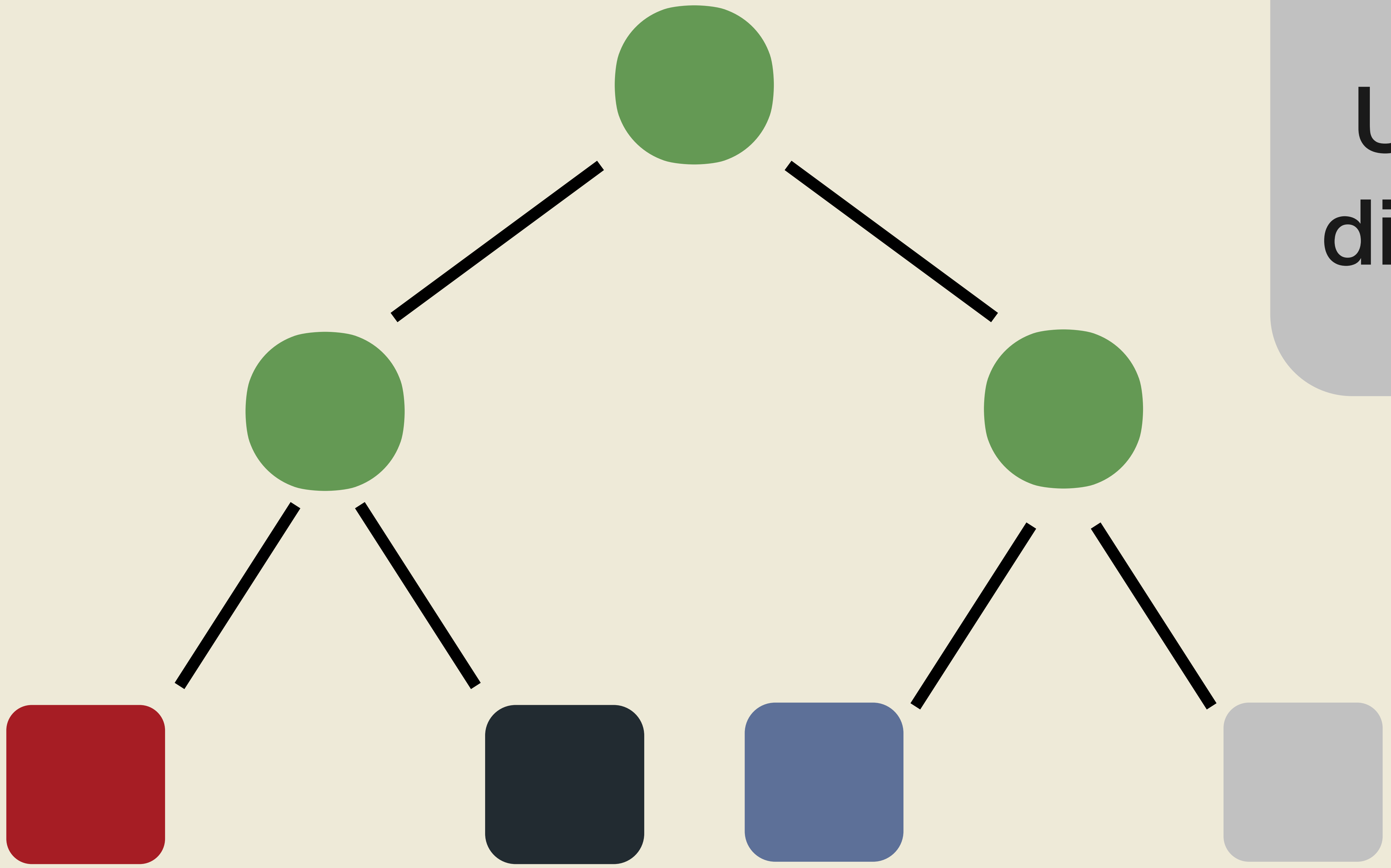
TreeKEM



Group Messaging

Continuous Group Key Agreement

TreeKEM



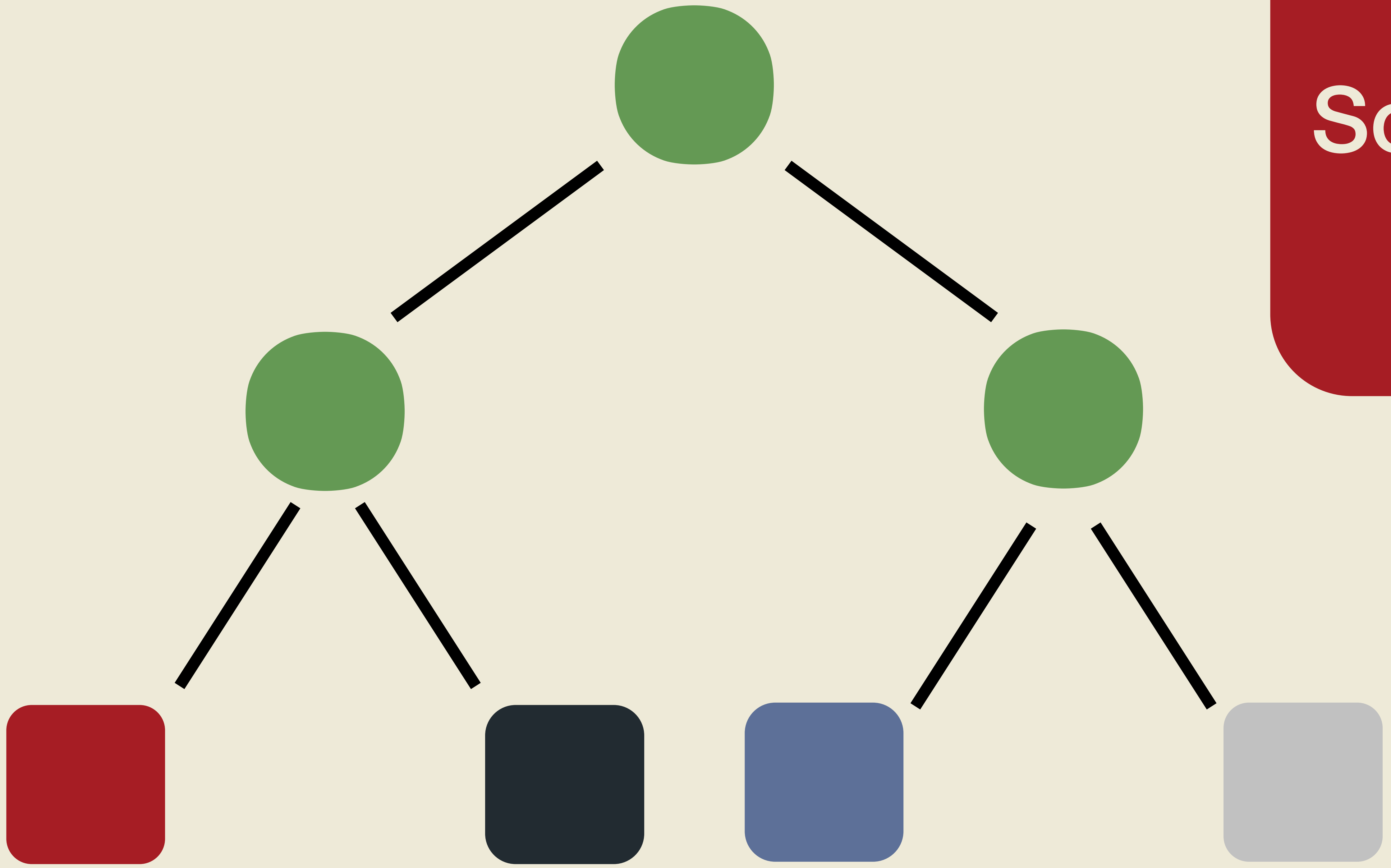
Tree invariant

User knows only direct path to root

Group Messaging

Continuous Group Key Agreement

TreeKEM

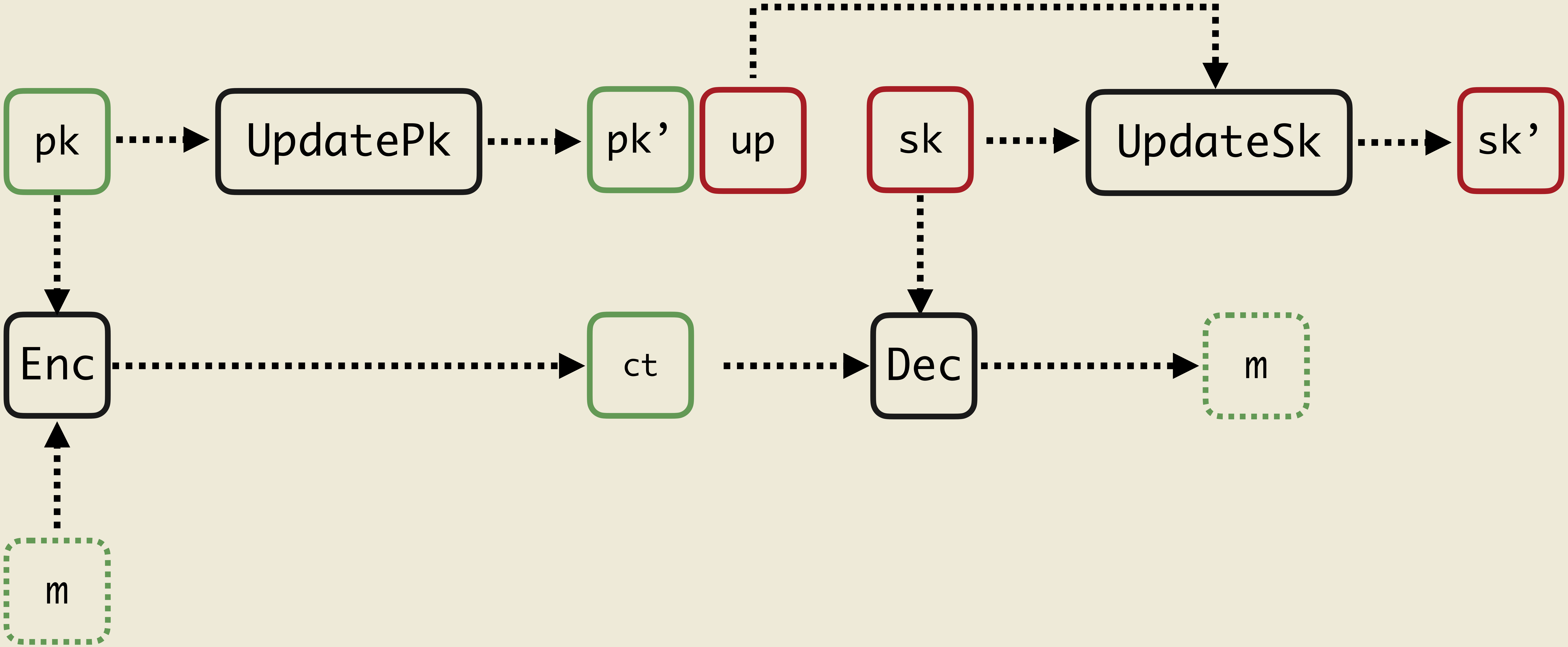


Problem

Some keys cannot be updated

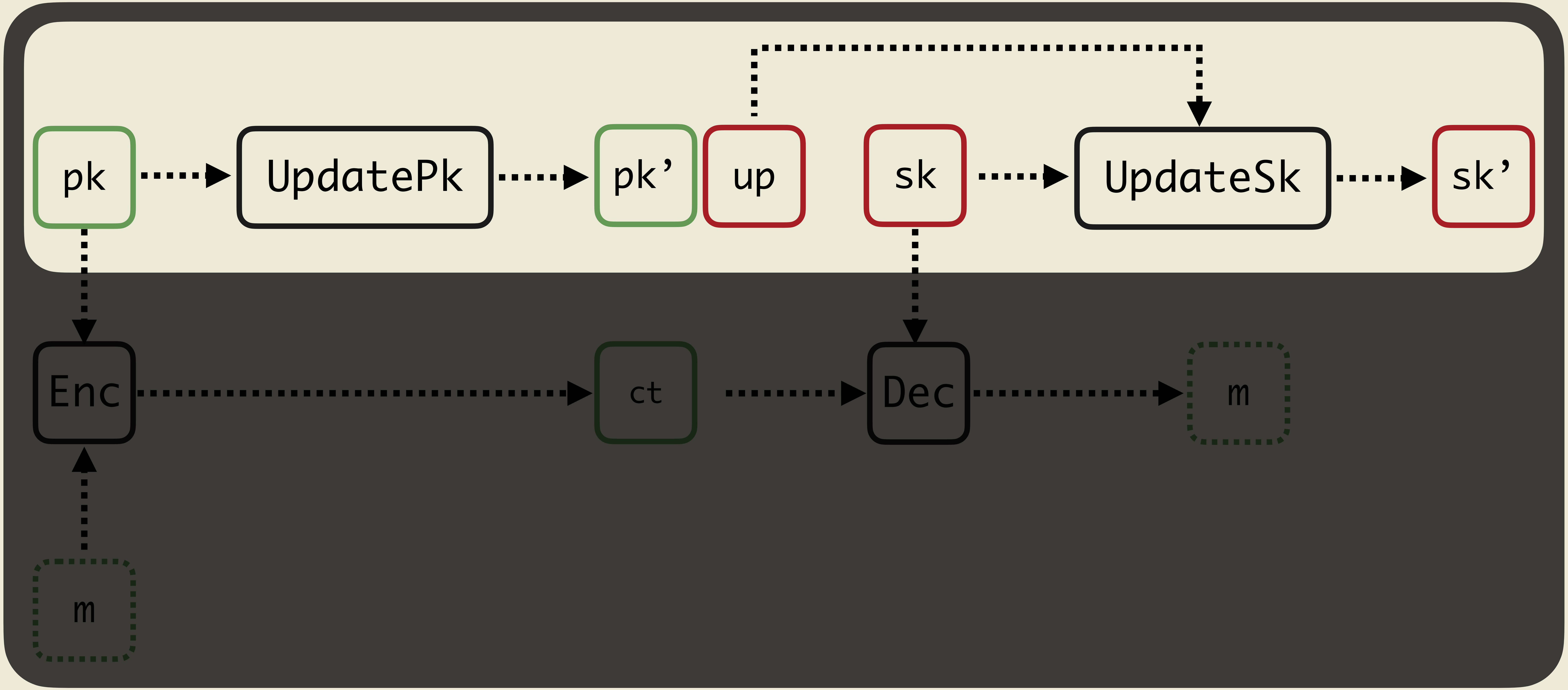
Updatable Public Key Encryption

Definition



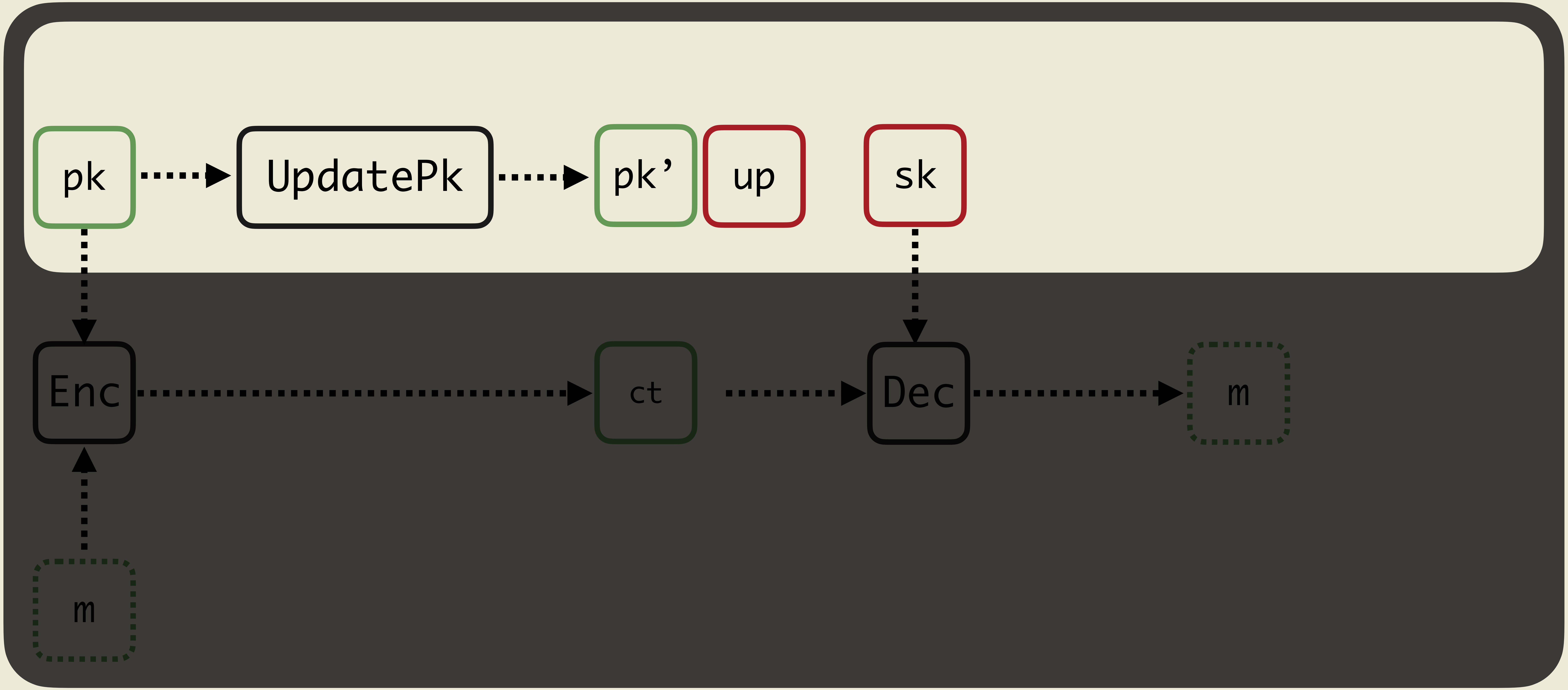
Updatable Public Key Encryption

Definition



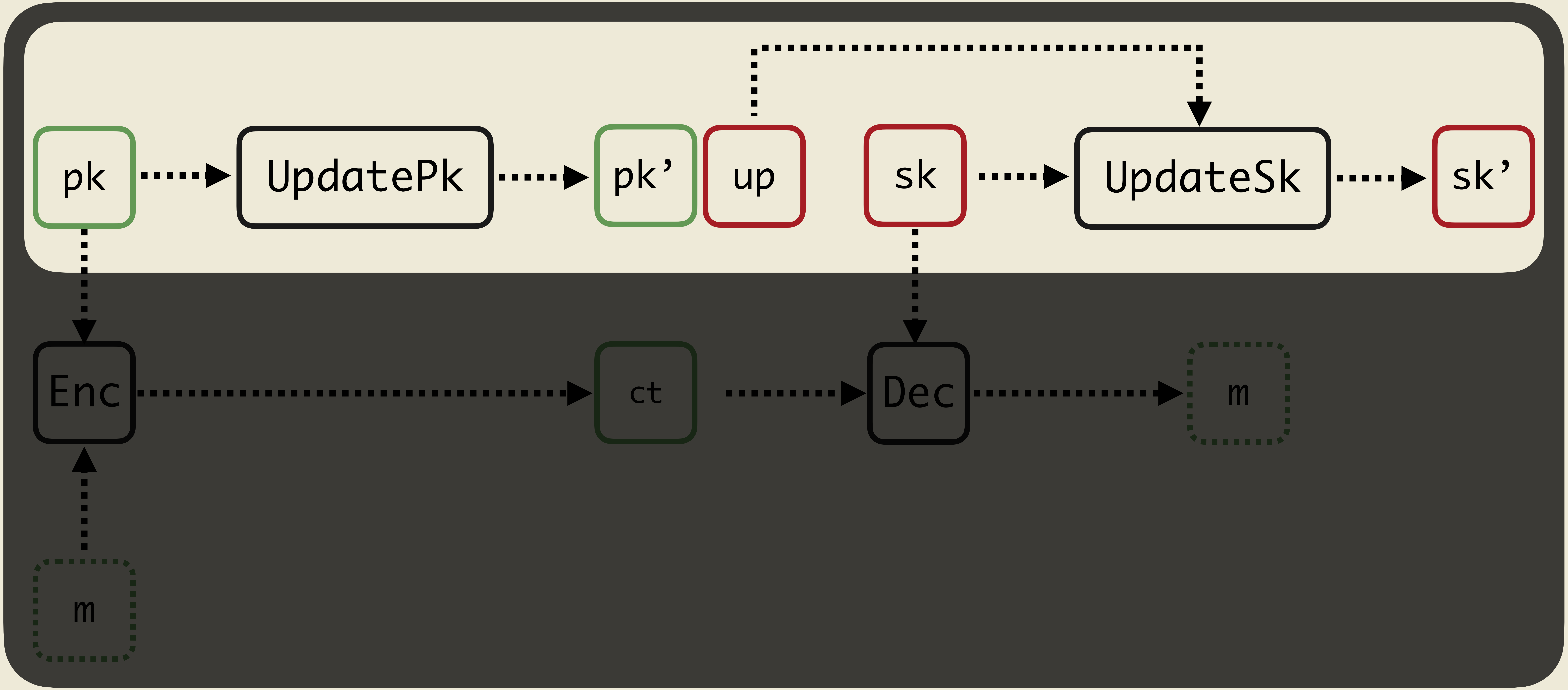
Updatable Public Key Encryption

Definition



Updatable Public Key Encryption

Definition



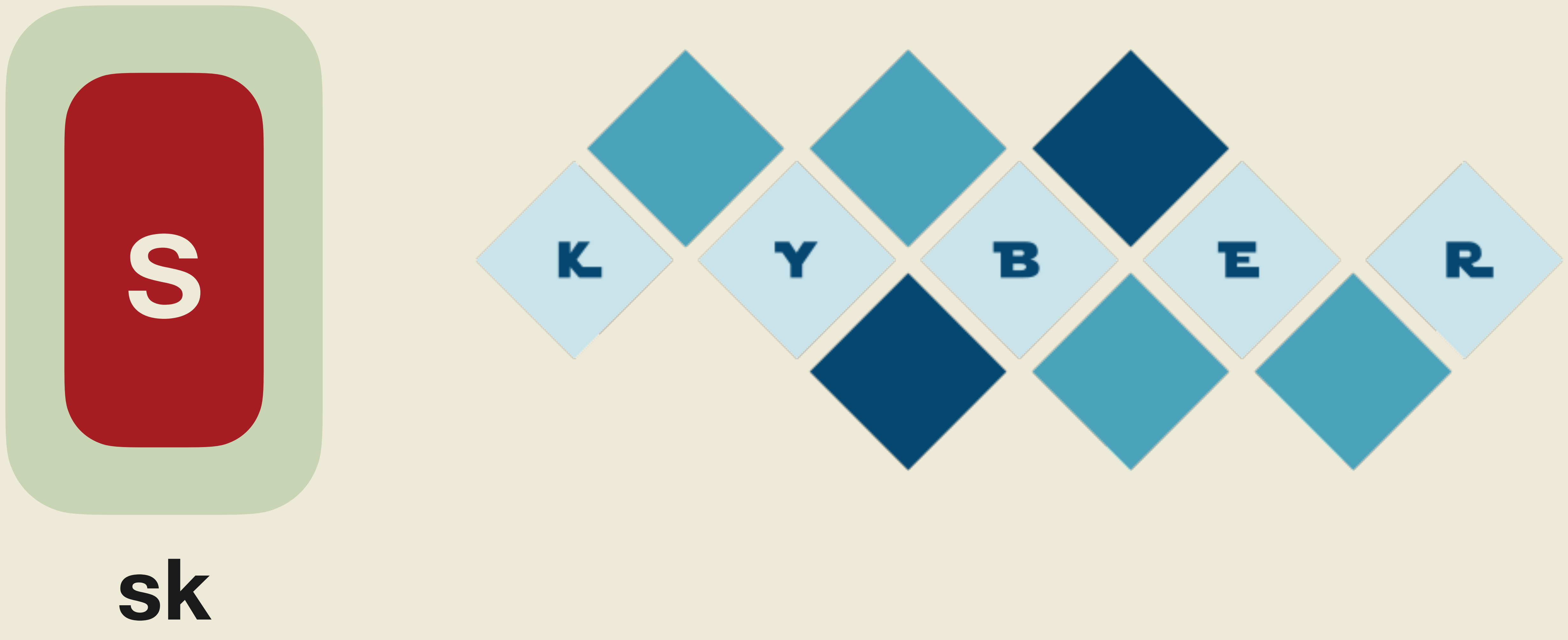
UPKE

Construction time

KYBER

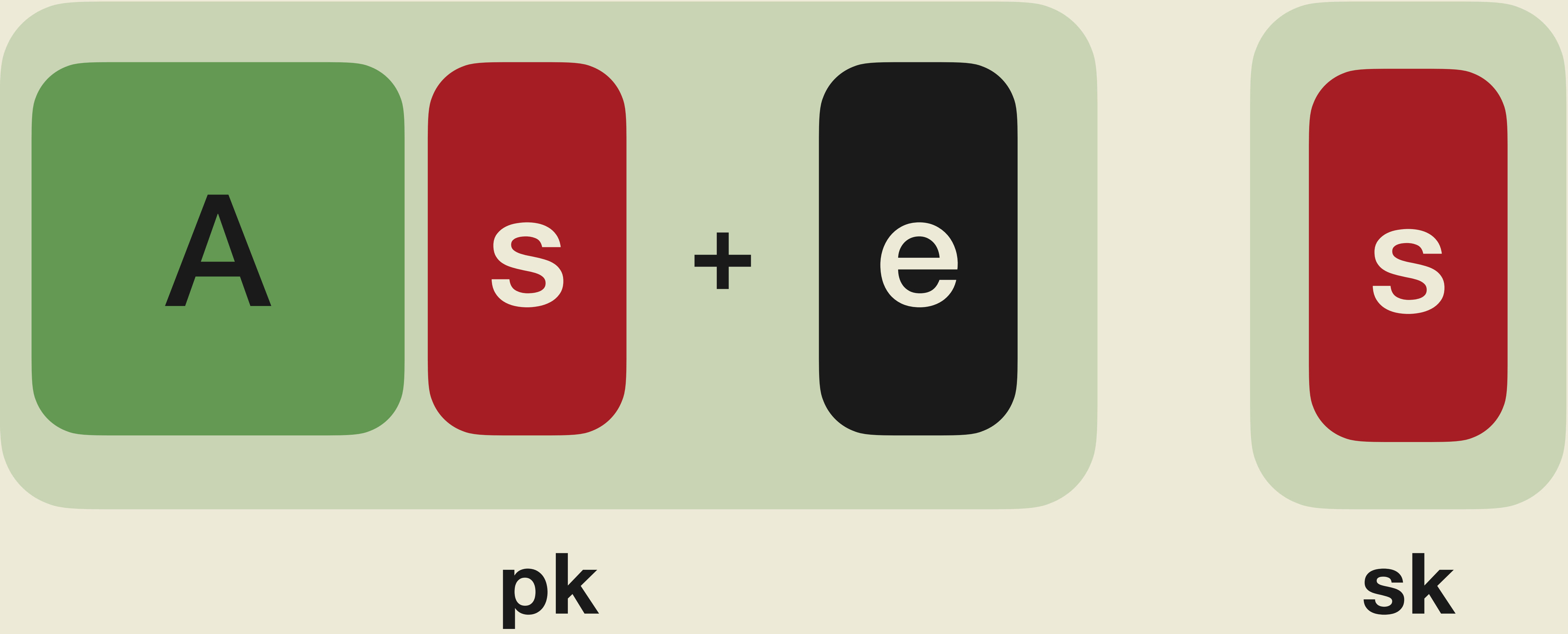
UPKE

Construction time



UPKE

Construction time



UPKE

Construction time

$$A\,s + e$$

pk

$$s$$

sk

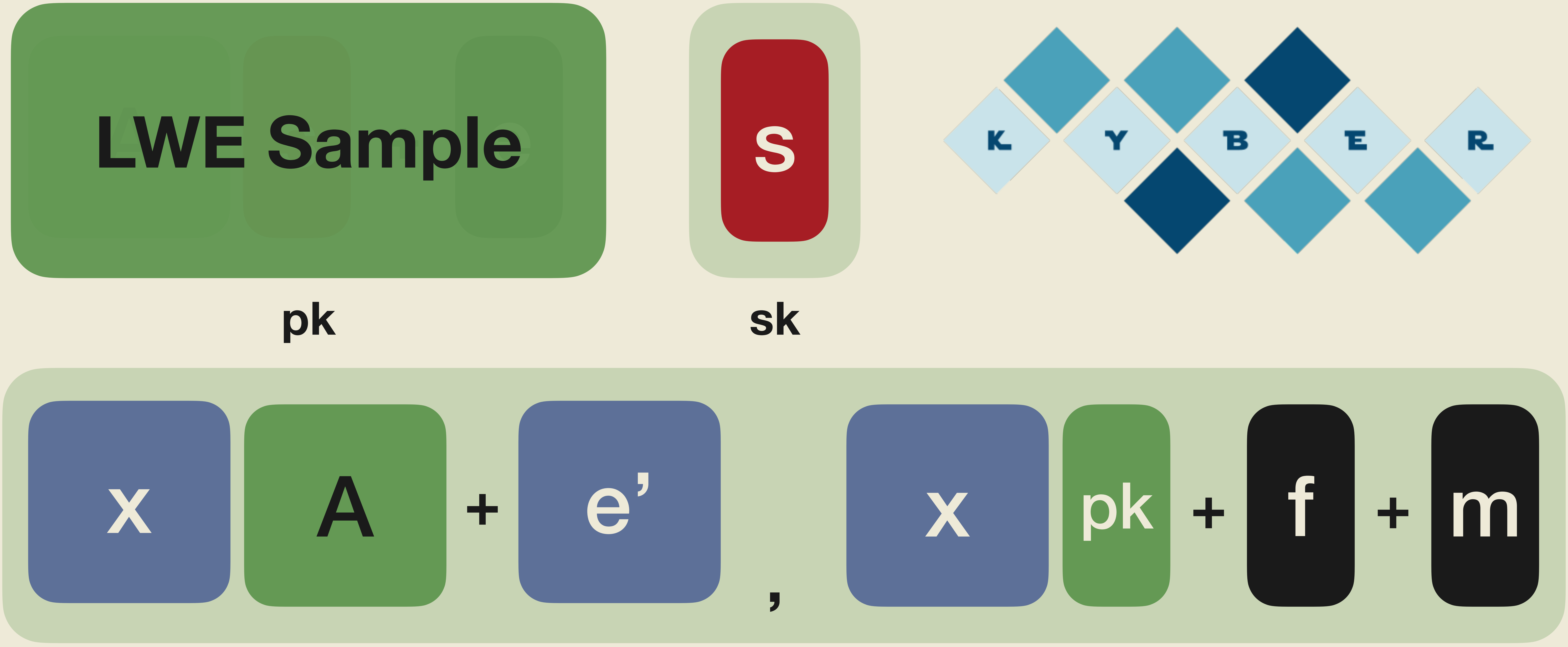
KYBER

$$x\,A + e' \quad , \quad x\,pk + f + m$$

Enc(pk, m)

UPKE

Construction time



LWE Sample

pk

s

sk

x A + e' , x pk + f + m

Enc(pk, m)

UPKE

Construction time

LWE Sample

pk

s

sk

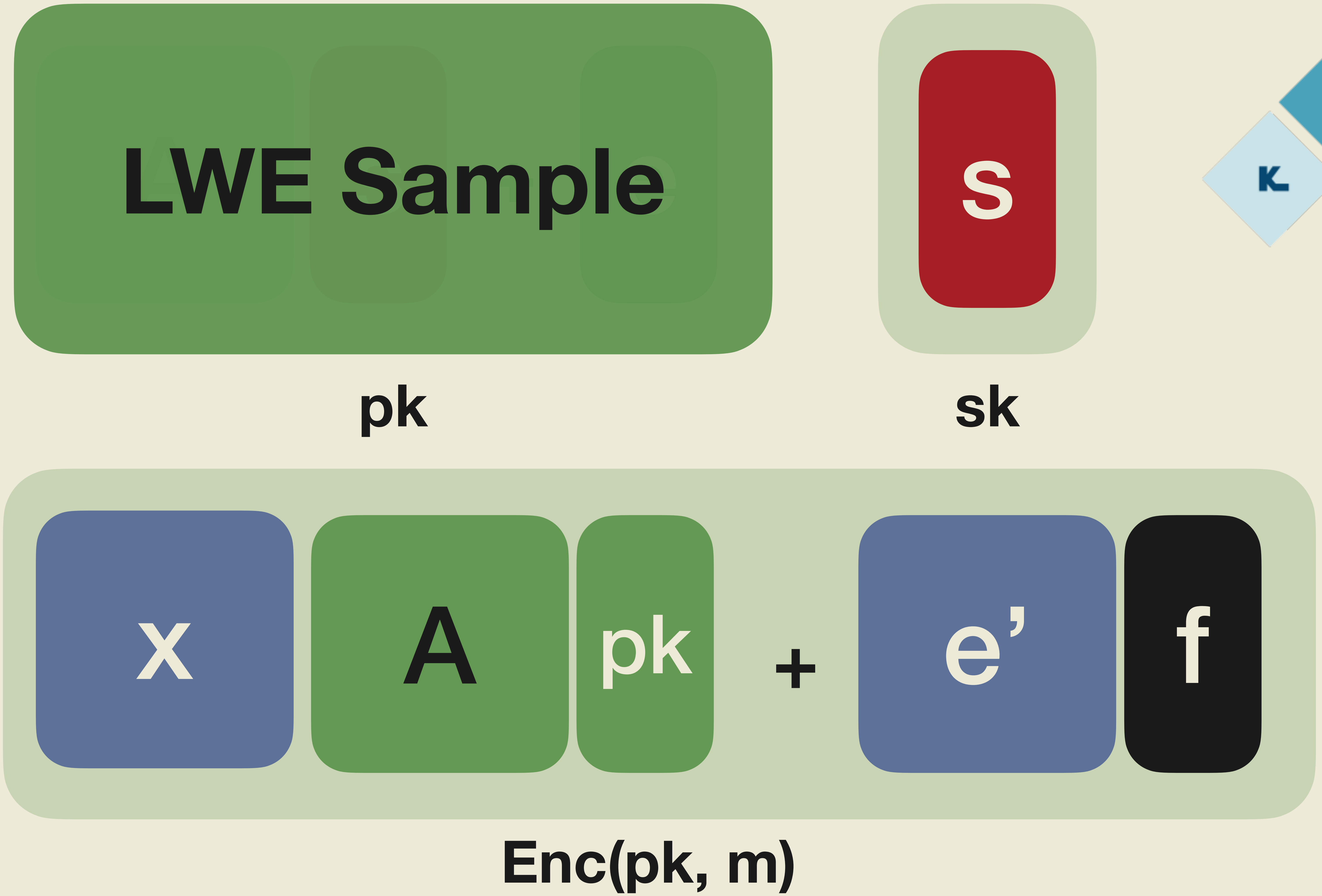
KYBER

x A + e’ , x pk + f

Enc(pk, m)

UPKE

Construction time



LWE Sample

s

pk

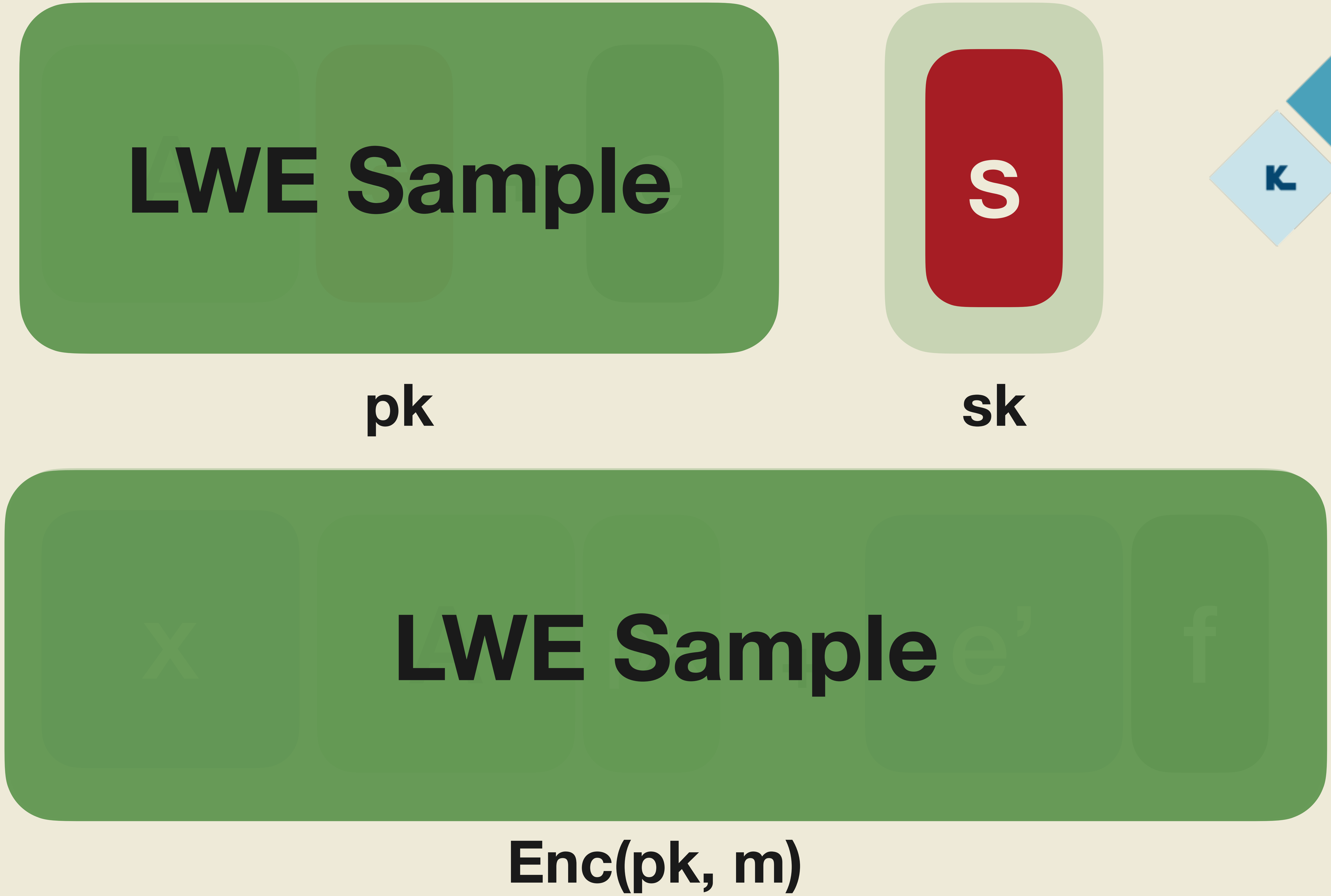
sk

x A pk + e’ f

Enc(pk, m)

UPKE

Construction time



pk

sk

Enc(pk, m)

UPKE

Construction time

$A \, s + e$

pk

s

sk

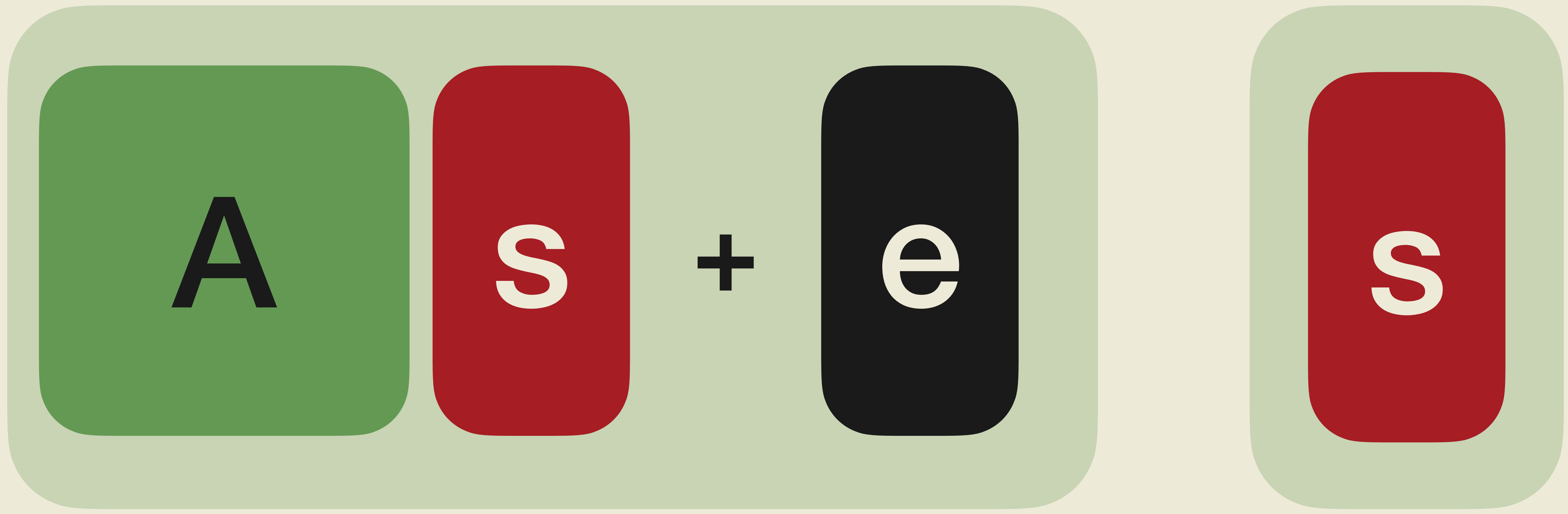
KYBER

$x \, A + e'$, $x \, pk + f + m$

Enc(pk, m)

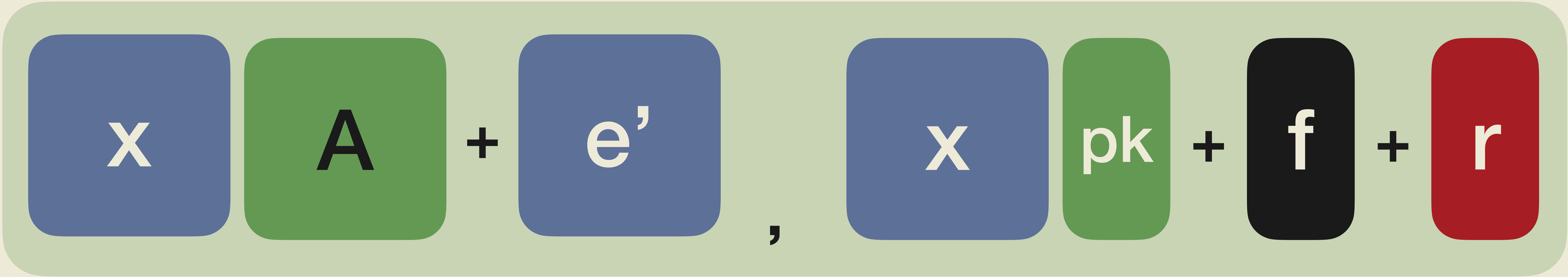
UPKE

Construction time



pk

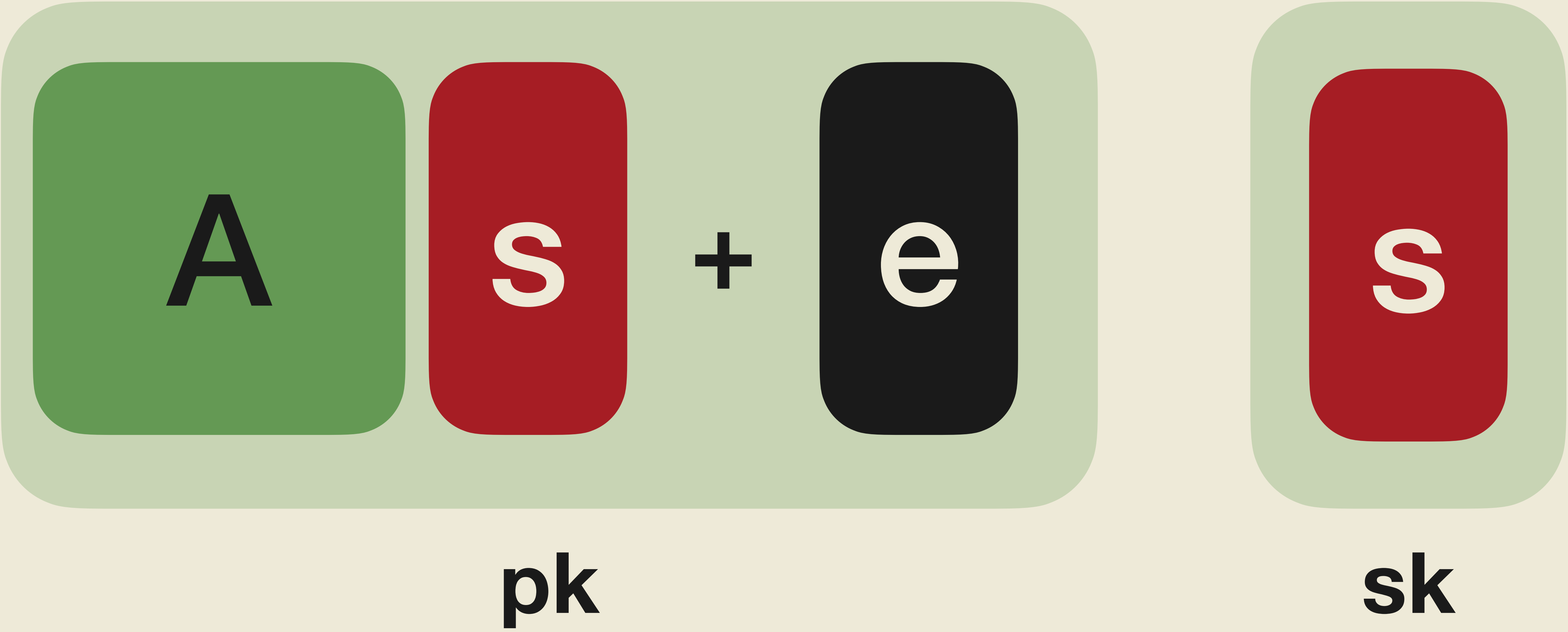
sk



Enc(pk, r)

UPKE

Construction time



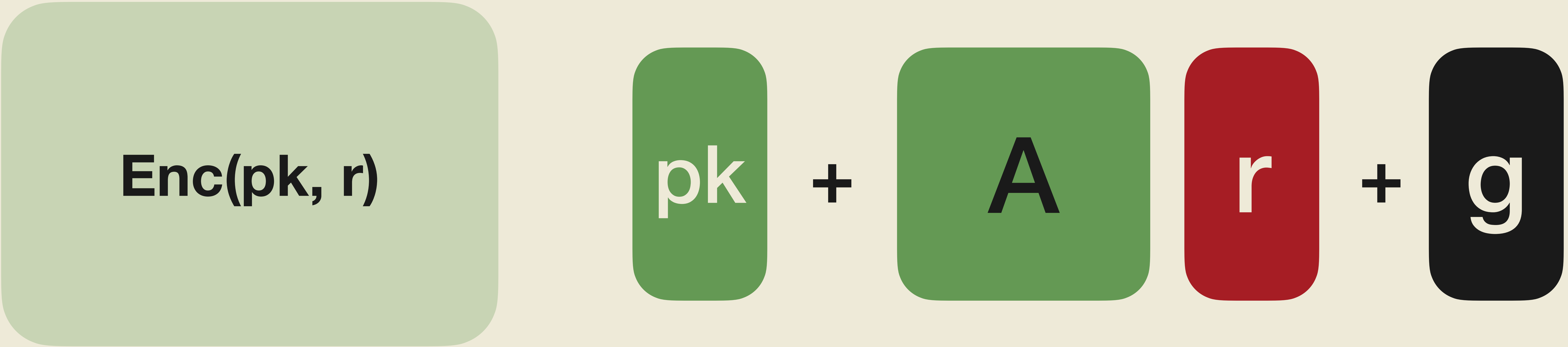
A s + e

s

pk

sk

KYBER



Enc(pk, r)

pk + A r + g

UPKE

Construction time

A s + e

pk

s

sk

KYBER

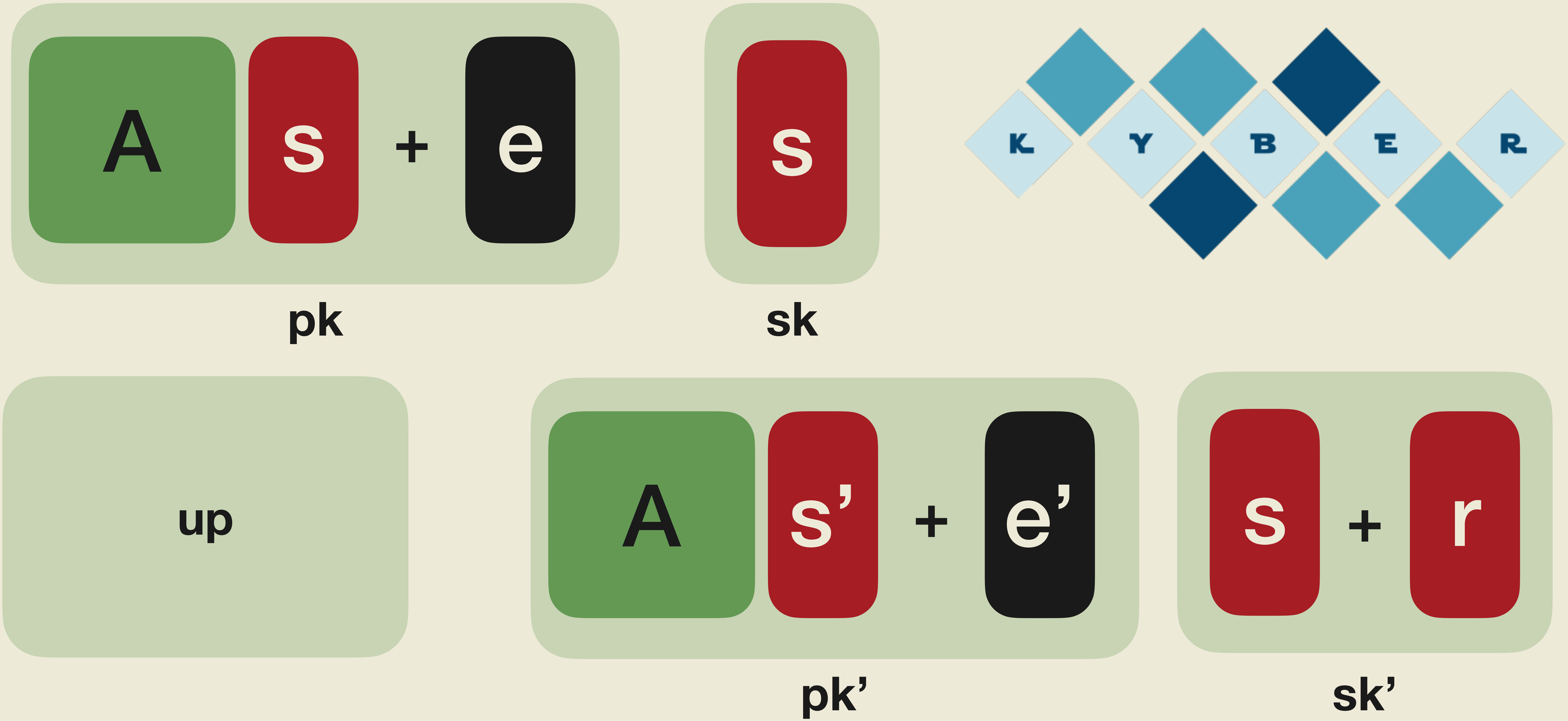
Enc(pk, r)

A s’ + e’

pk’

UPKE

Construction time



$A \; s + e$

pk

s

sk

up

$A \; s' + e'$

pk’

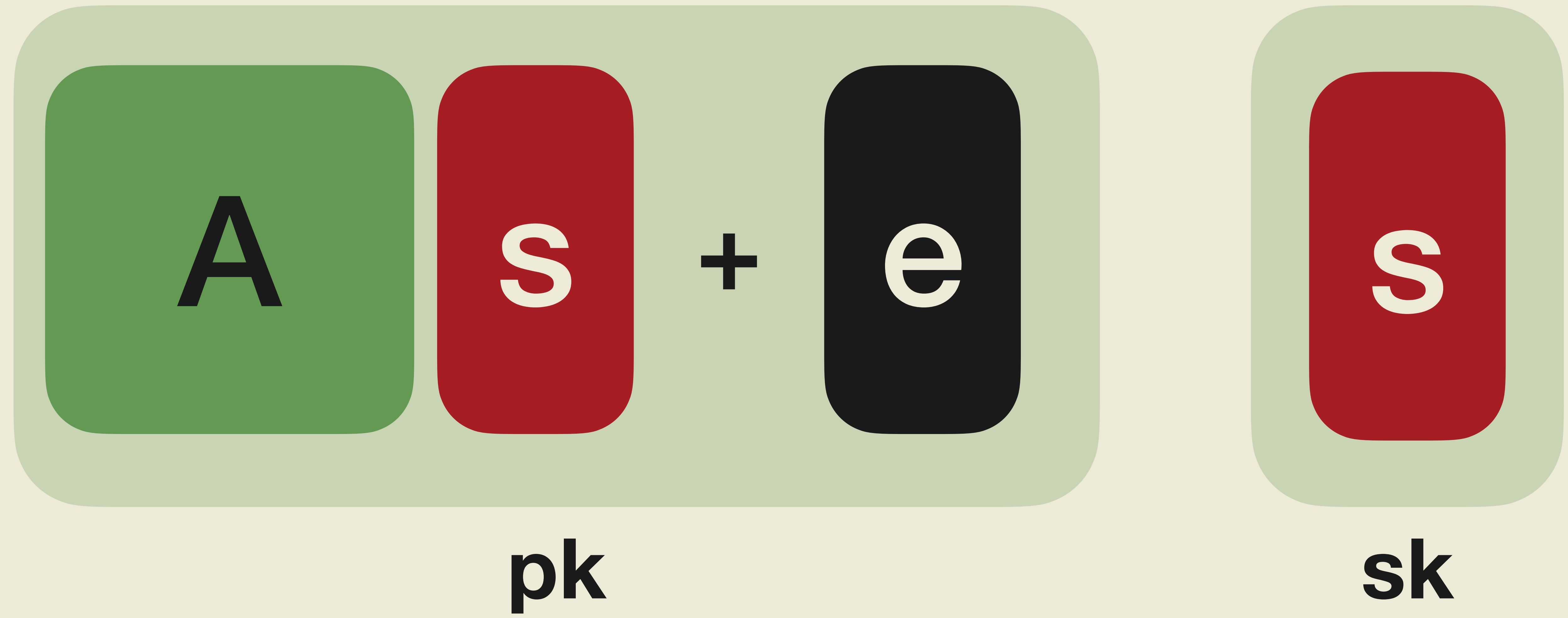
$s + r$

sk’

UPKE

Construction time

Done !

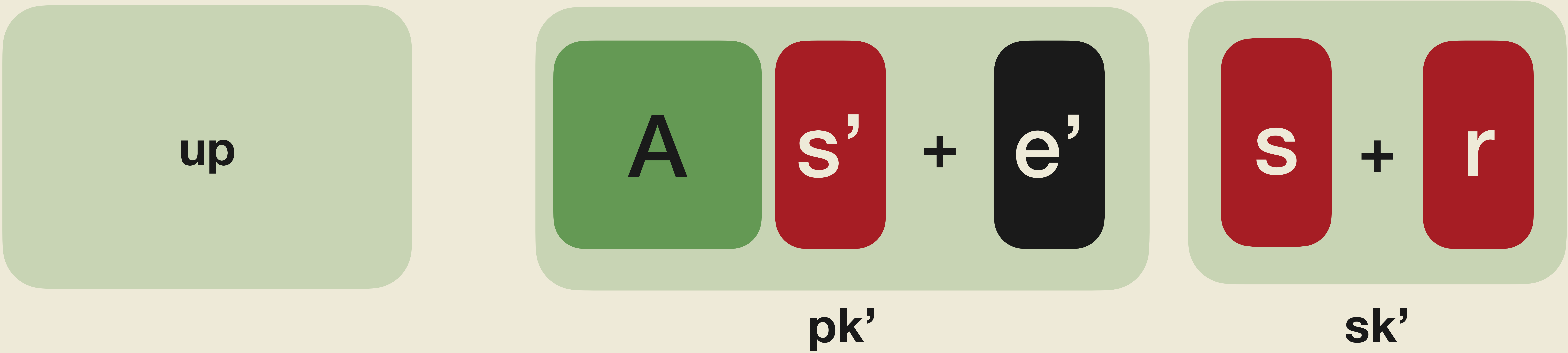


$A\ s + e$

pk

s

sk



up

$A\ s' + e'$

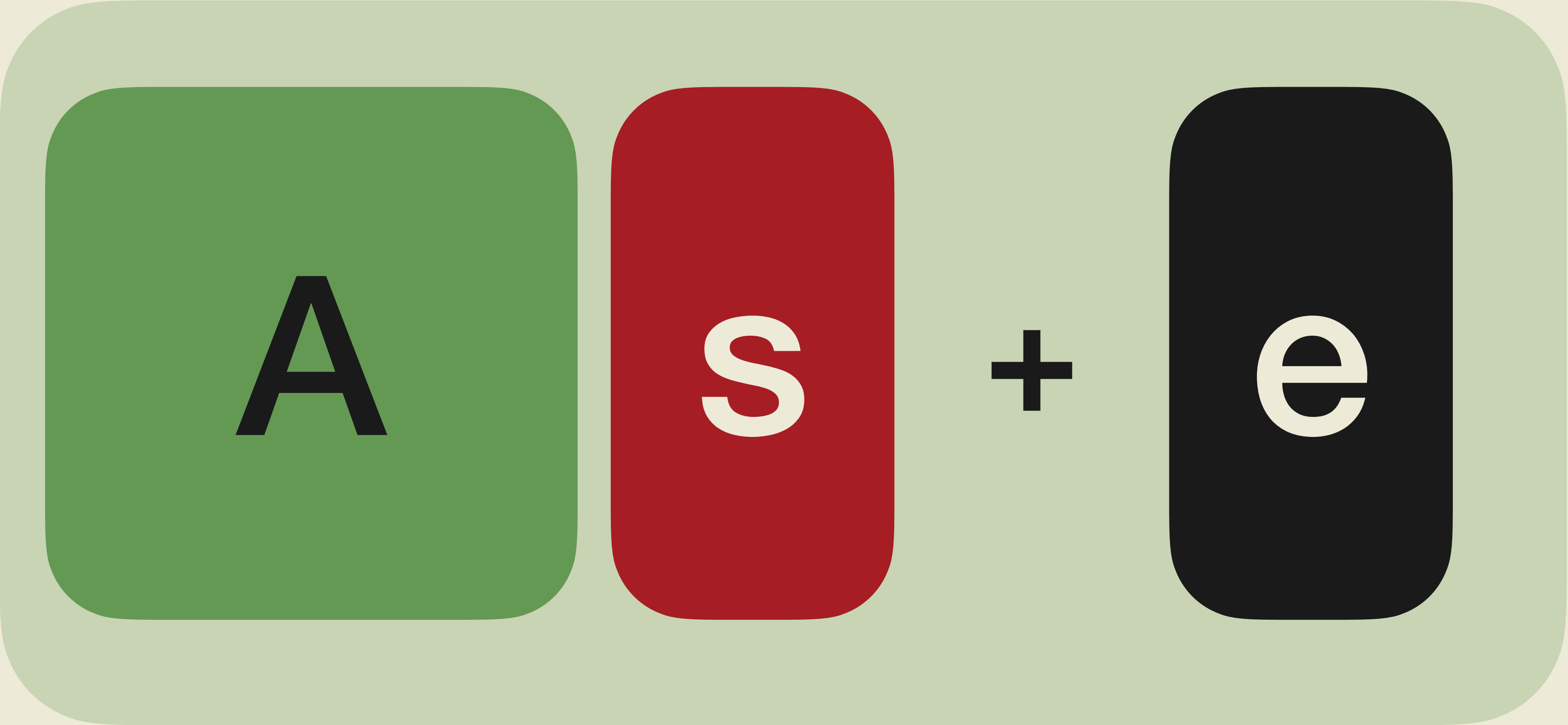
pk’

$s + r$

sk’

UPKE

Assumption time



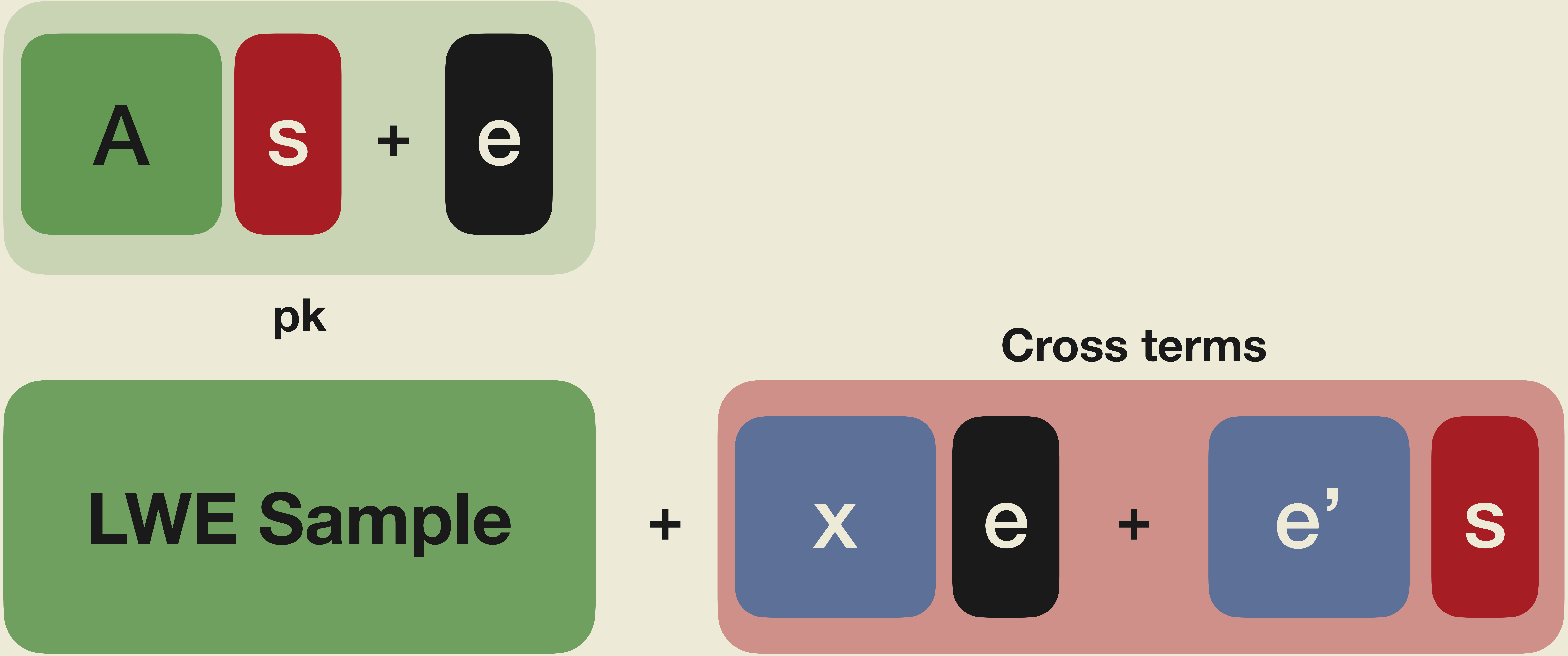
$A s + e$

pk

LWE Sample

UPKE

Assumption time



A s + e

pk

Cross terms

LWE Sample + x e + e’ s

UPKE

Assumption time

A s + e

pk

Cross terms - with flooding

LWE Sample + Very small

UPKE

Assumption time

A , LWE Sample , Hint

LWE + Hint variant

UPKE

Assumption time

A , LWE Sample , Hint

LWE + Hint variant

Hint = $z^T e$

Extended LWE

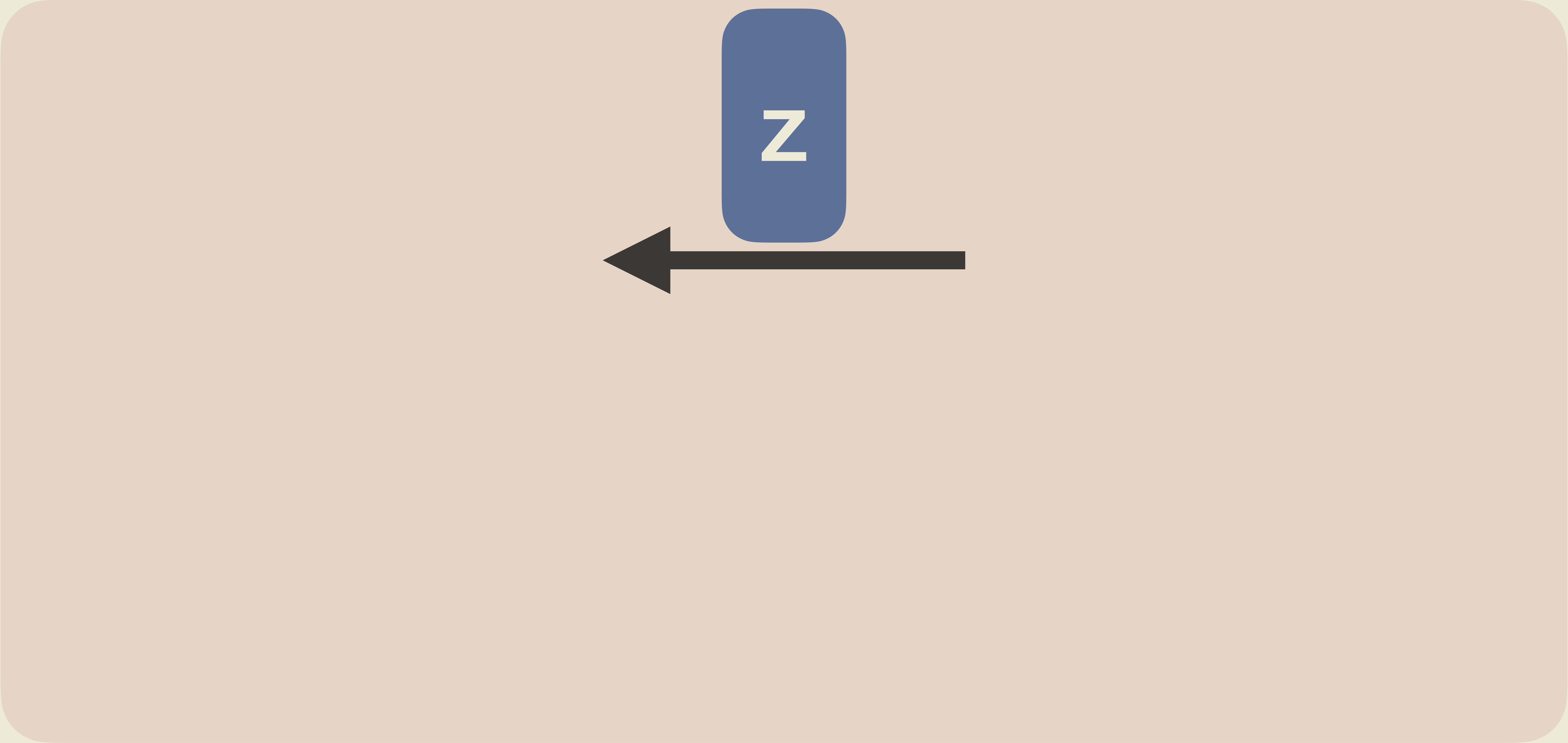
UPKE

Assumption time

Extended LWE

UPKE

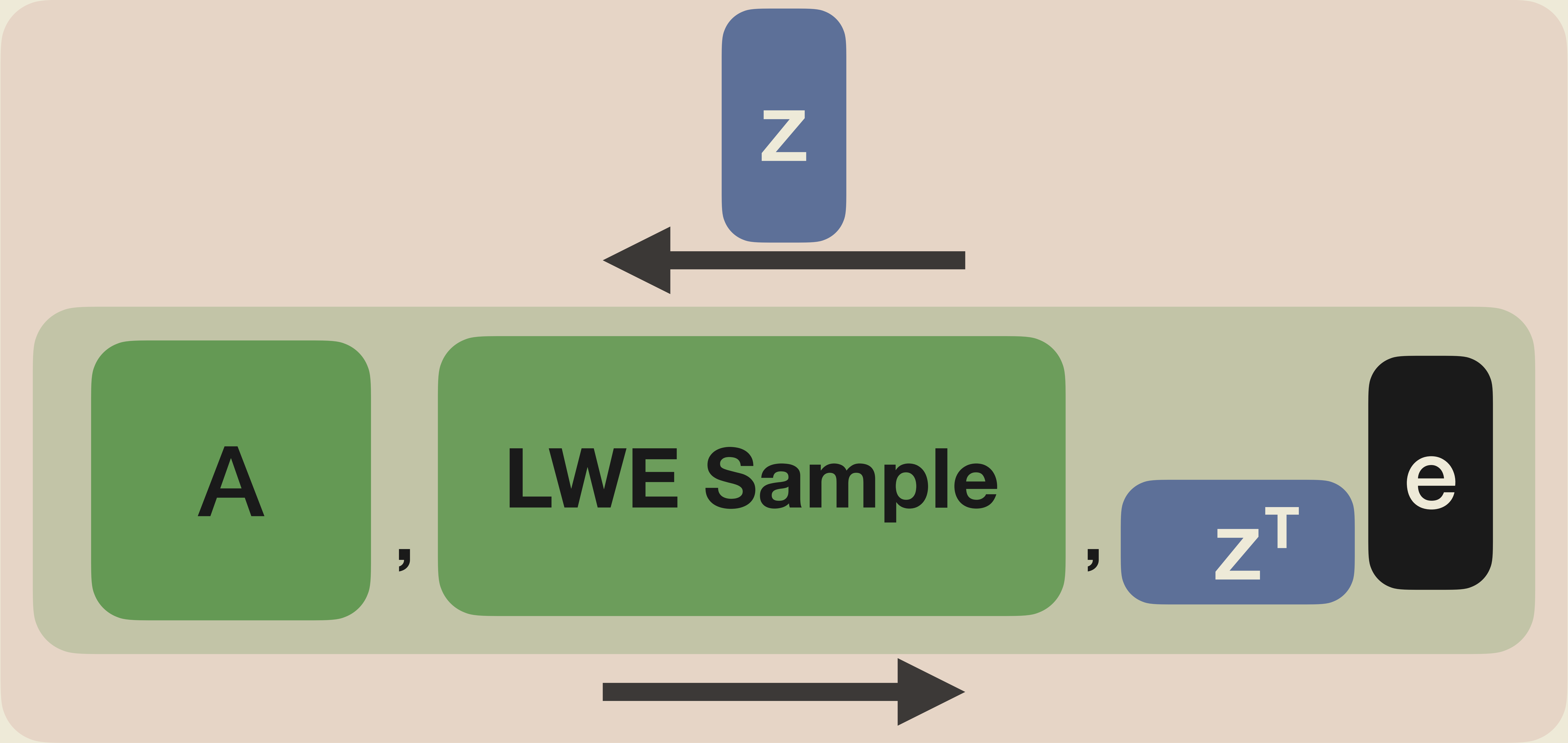
Assumption time



Extended LWE

UPKE

Assumption time



z

A , LWE Sample , $z^T e$

Extended LWE

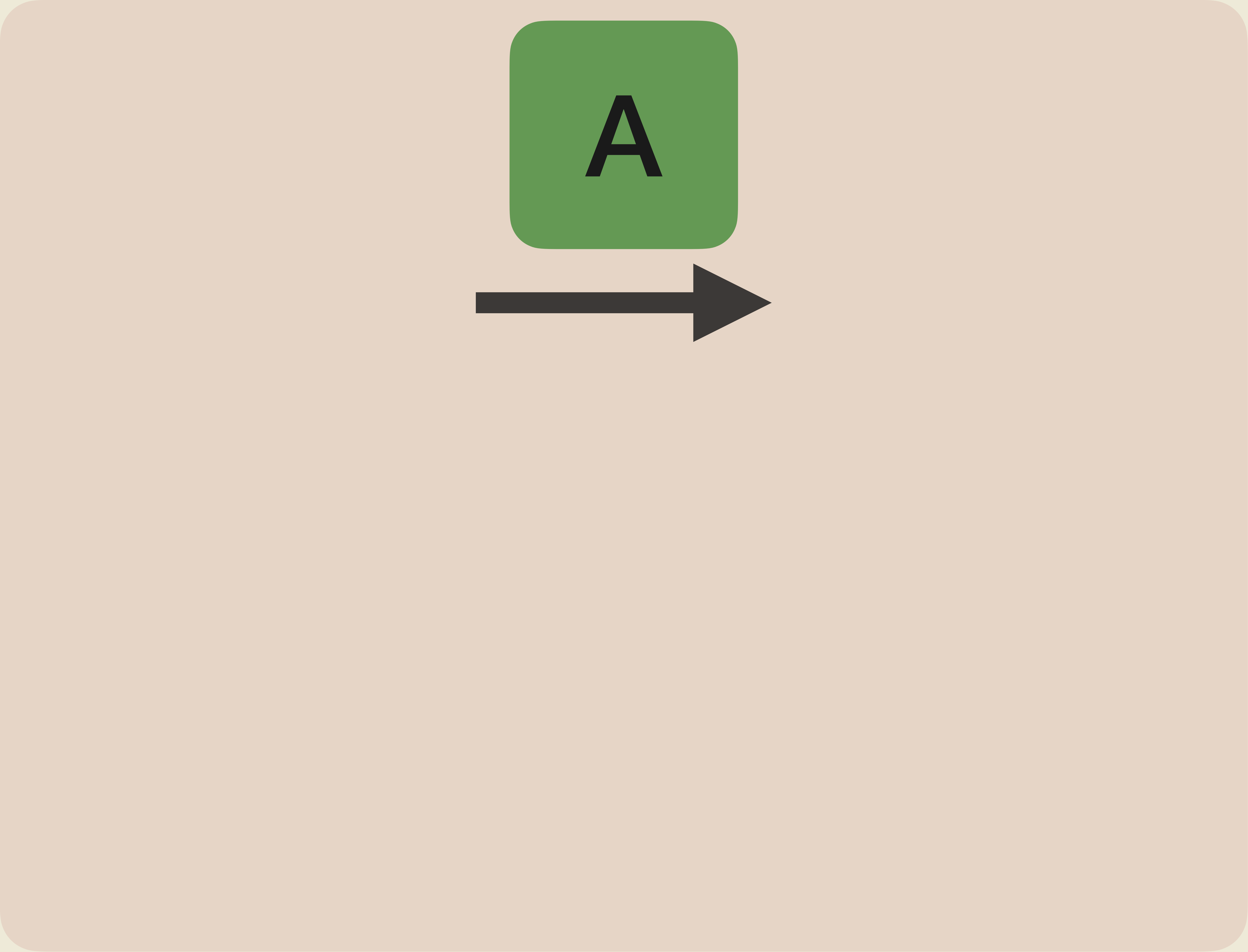
UPKE

Assumption time

What we need

UPKE

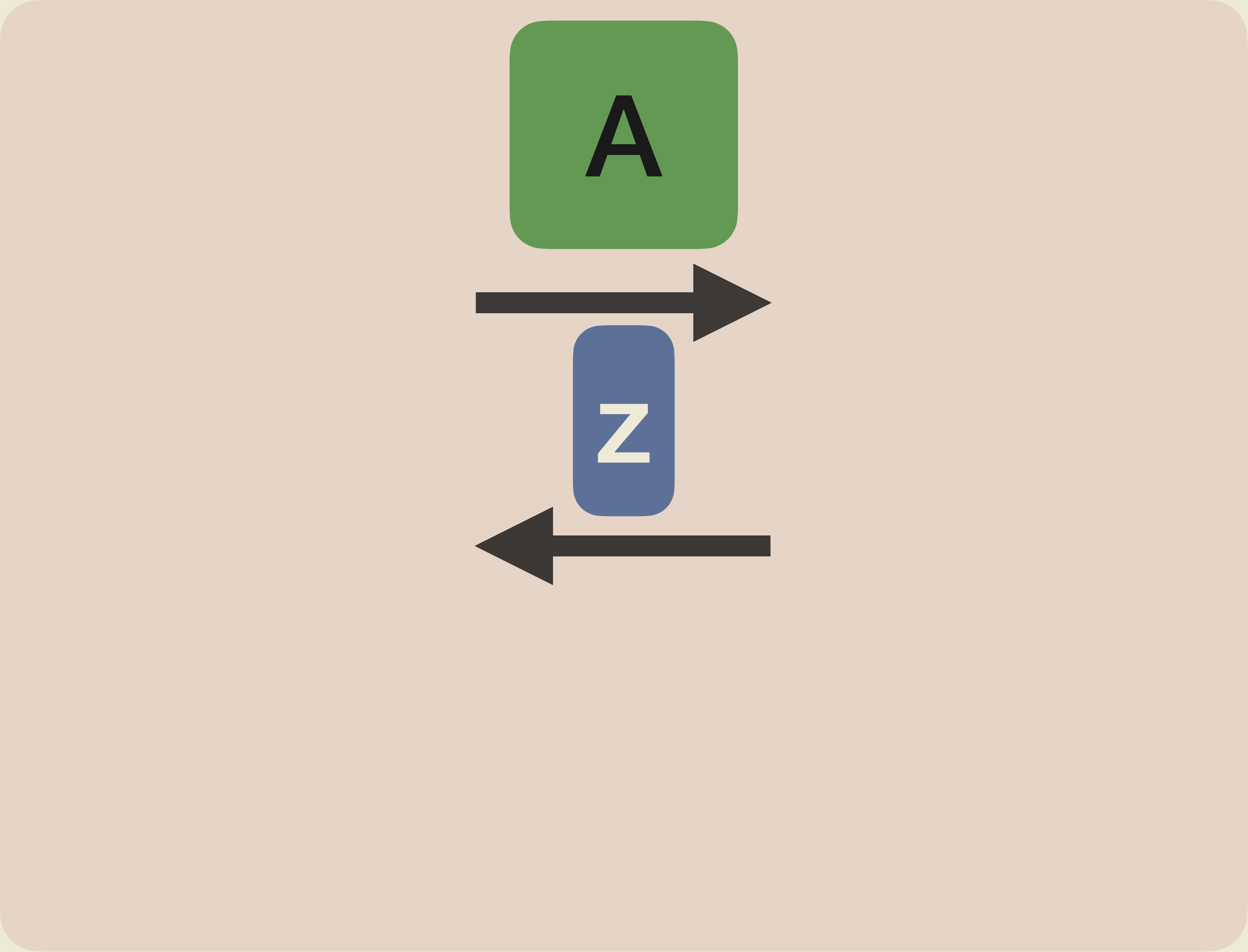
Assumption time



What we need

UPKE

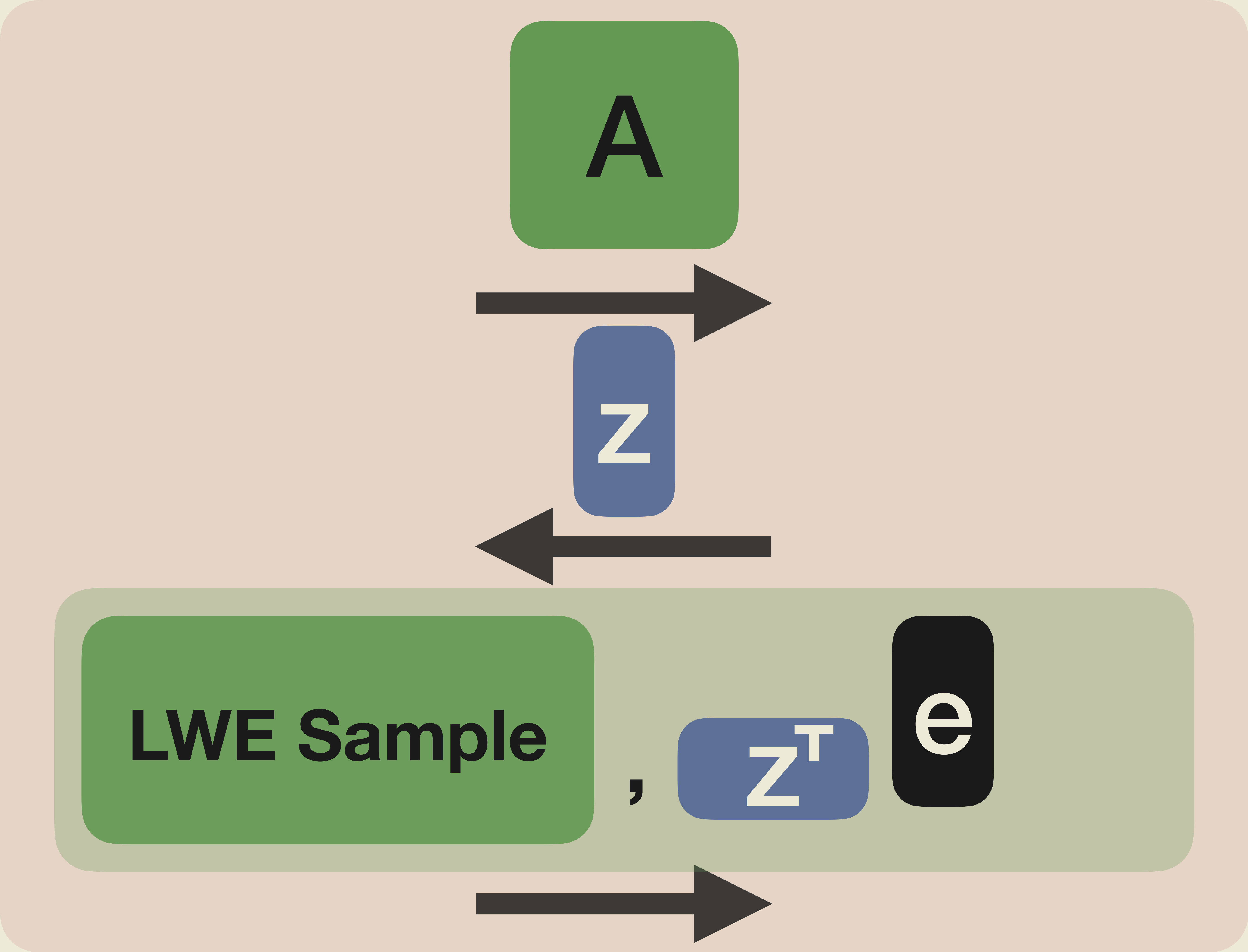
Assumption time



What we need

UPKE

Assumption time



A

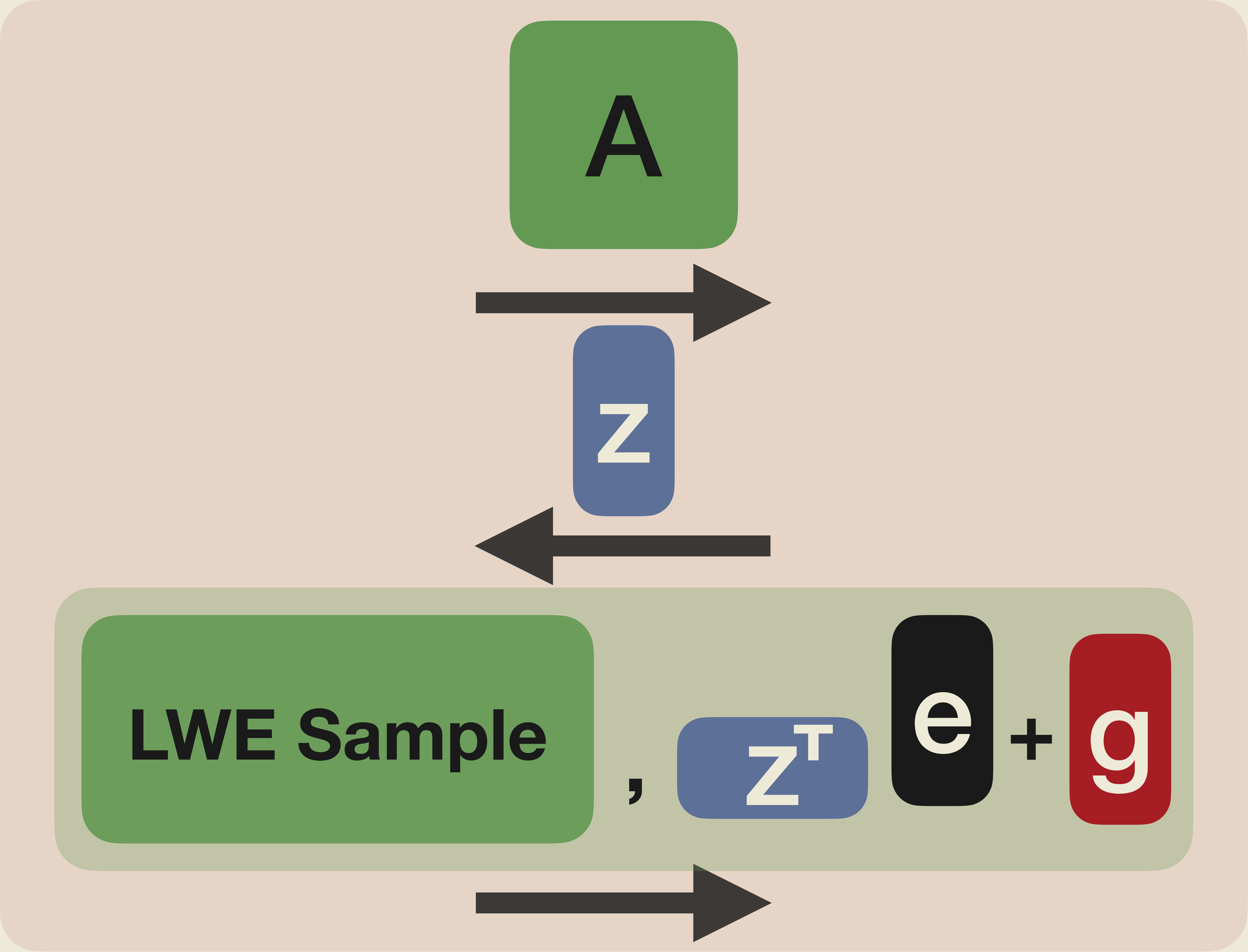
z

LWE Sample , $z^{T}e$

What we need

UPKE

Assumption time



Adaptive extended LWE

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

Other Contributions

An FO transform for UPKE

CU transform

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