



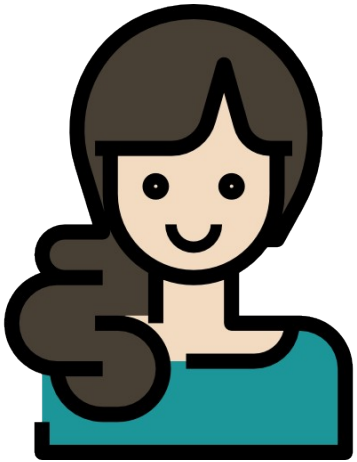
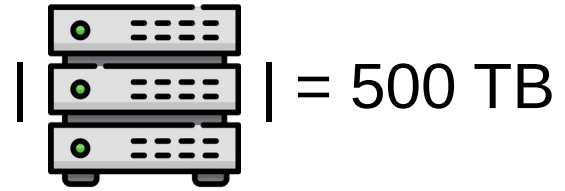
CISPA

HELMHOLTZ CENTER FOR
INFORMATION SECURITY

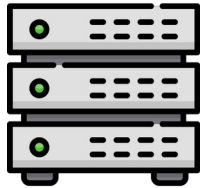
Rate-1 Incompressible Encryptions from Standard Assumptions

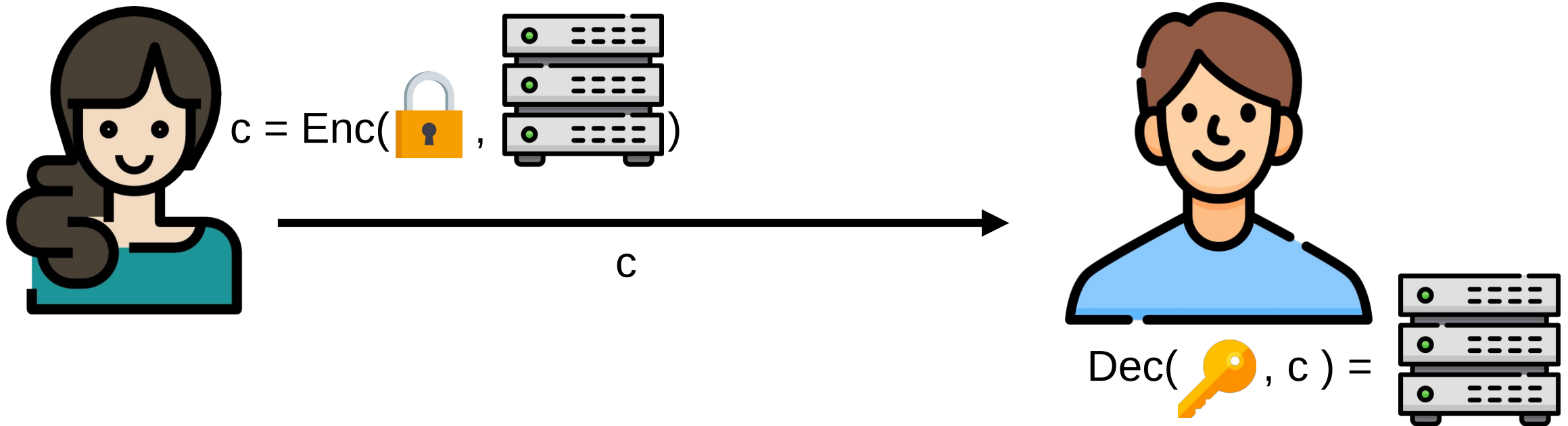
Pedro Branco (Johns Hopkins University), Nico Döttling (CISPA), Jesko Dujmovic (CISPA)

Incompressible Encryption

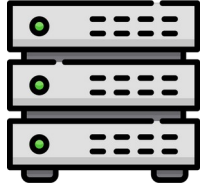


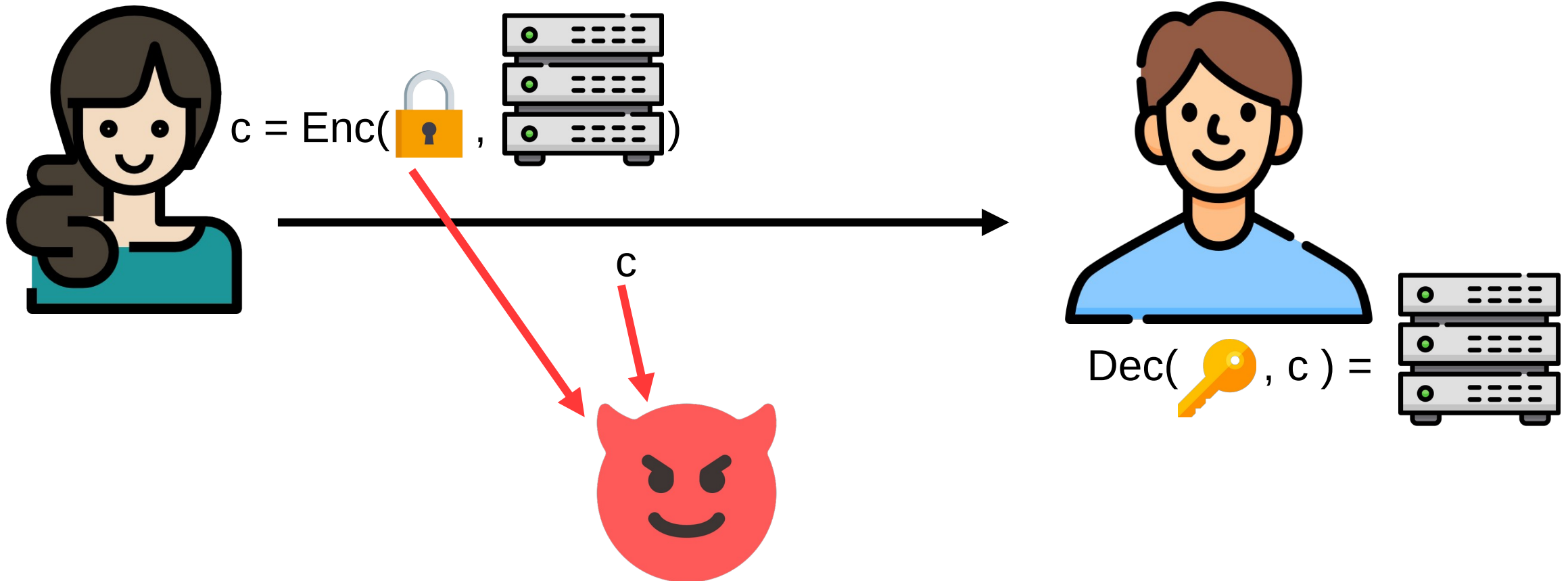
Incompressible Encryption

 = 500 TB

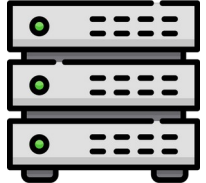


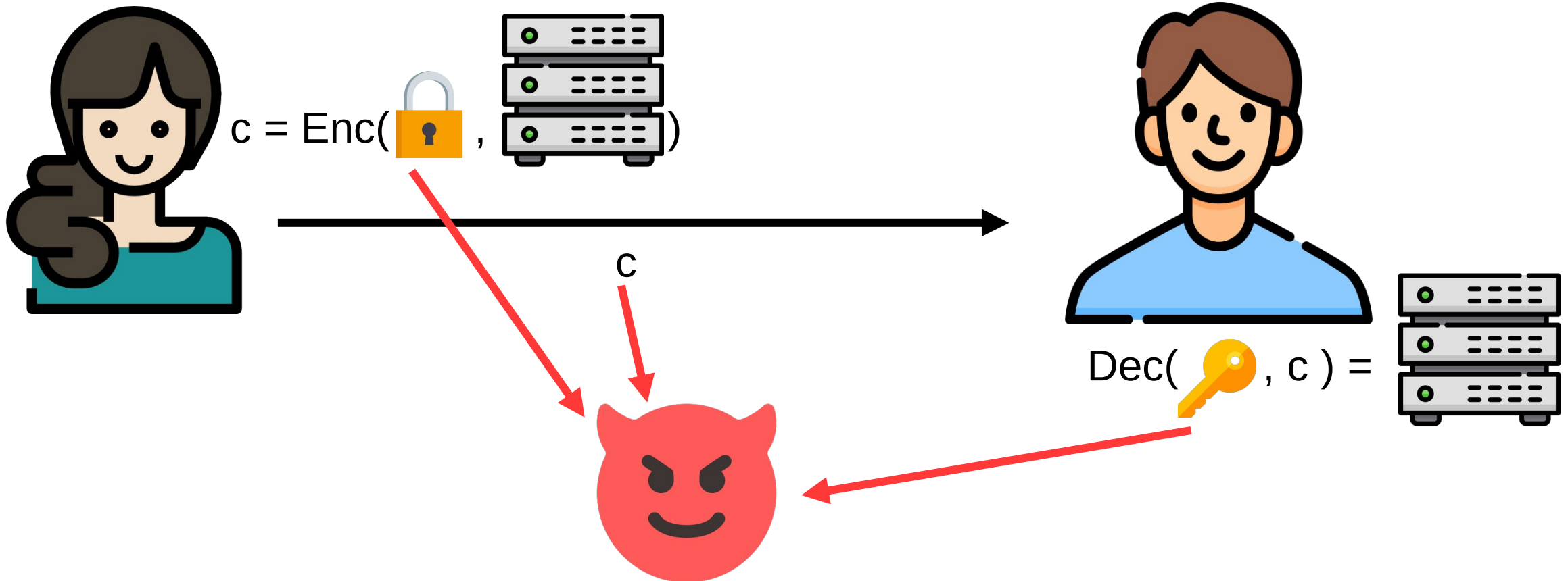
Incompressible Encryption

 = 500 TB



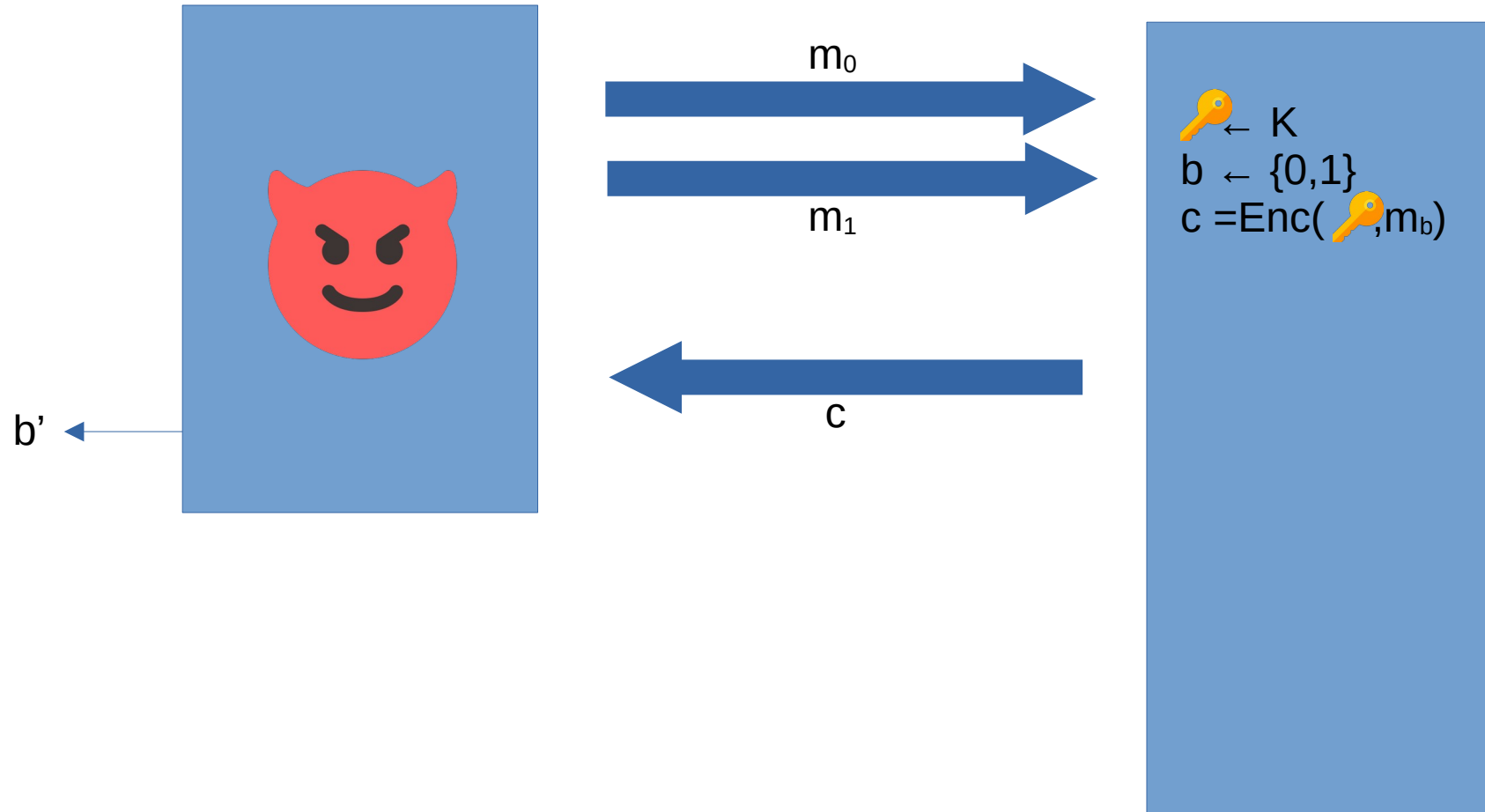
Incompressible Encryption

 = 500 TB



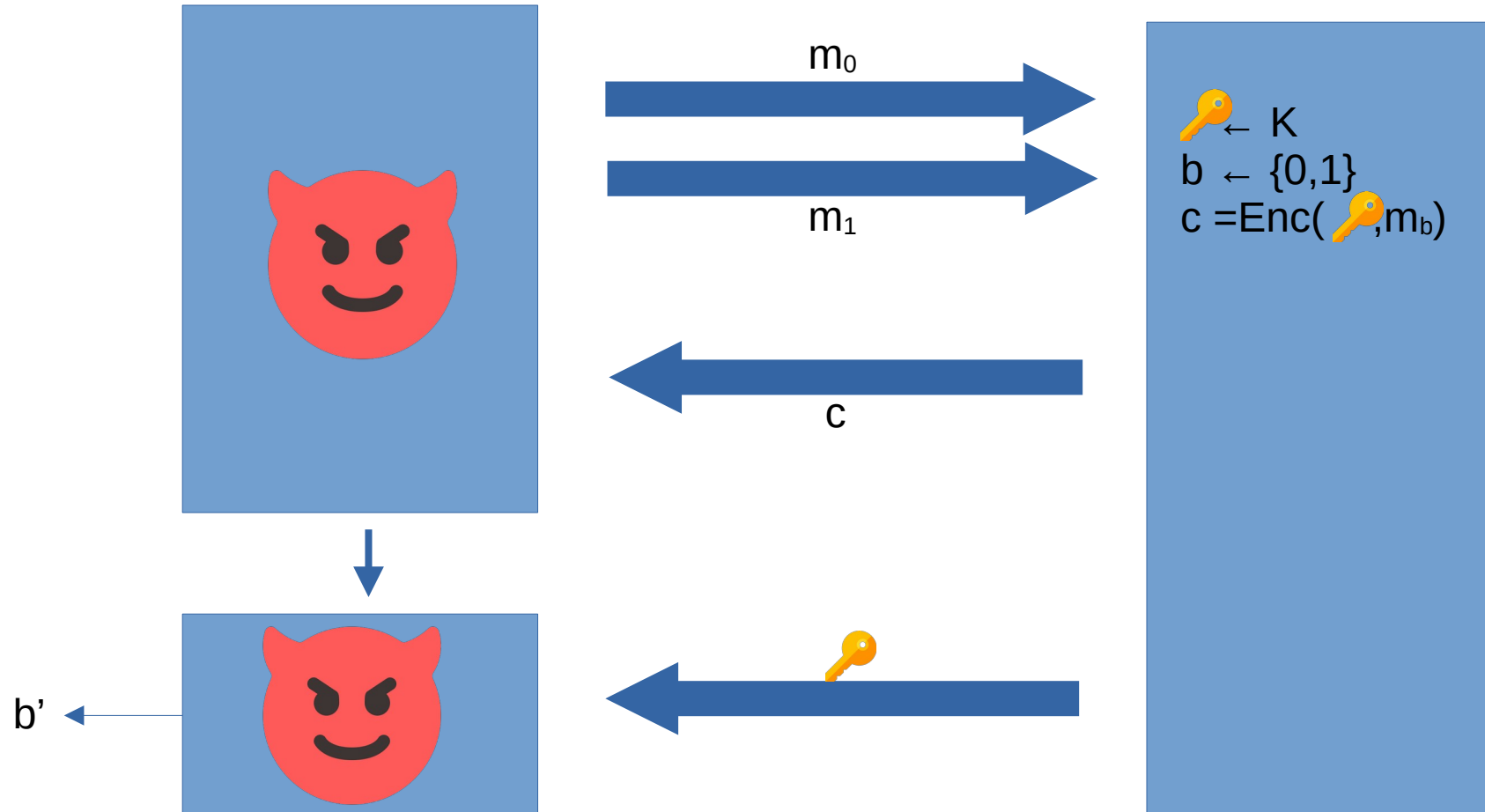
Incompressible Encryption [Dzi06,GWZ22]

EAV - Style



Incompressible Encryption [Dzi06,GWZ22]

EAV - Style



Naive Attempt #1

$G(\text{key})$

\oplus

m

$=$

c

Naive Attempt #1

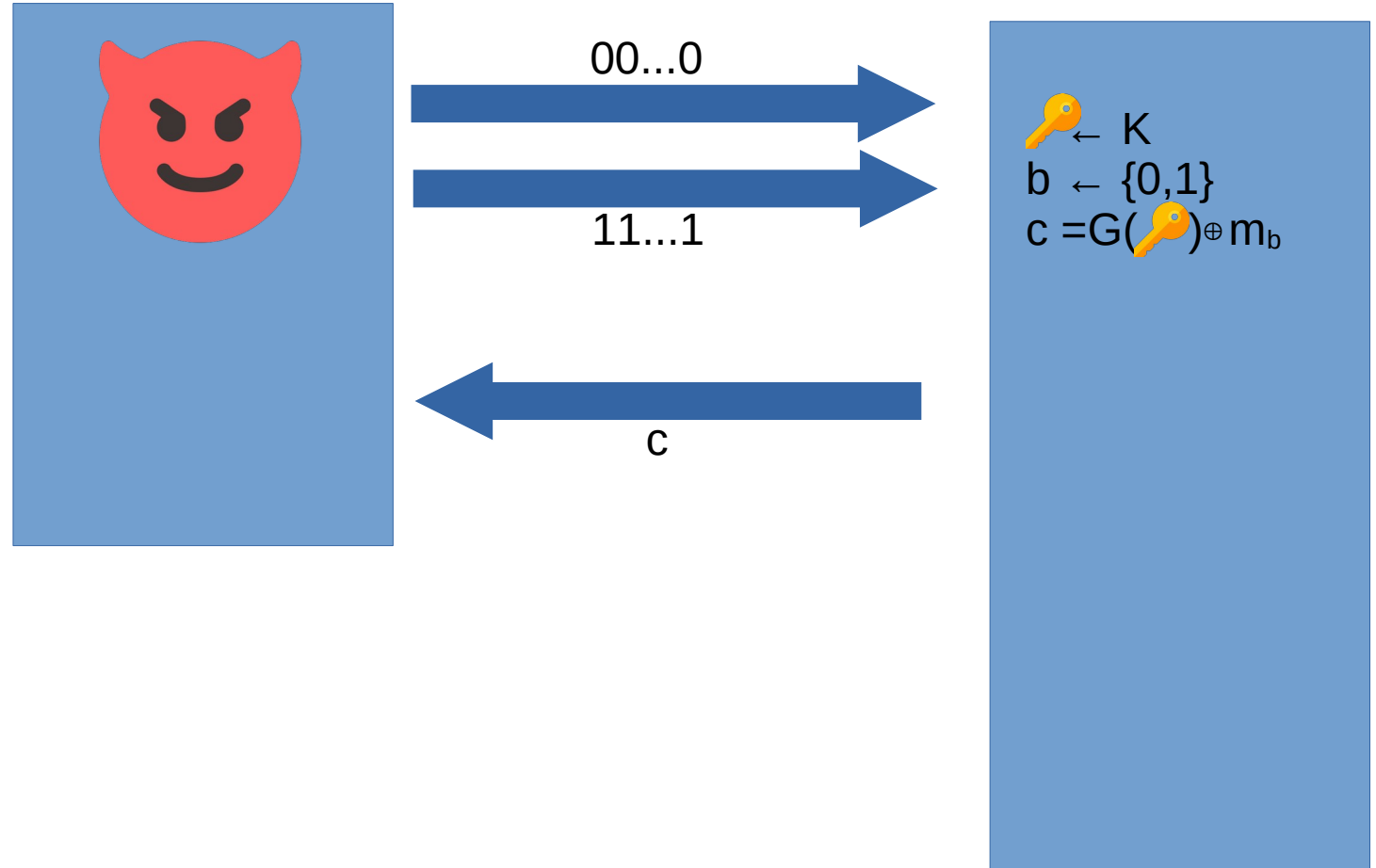
$G(\text{key})$

\oplus

m

$=$

c



Naive Attempt #1

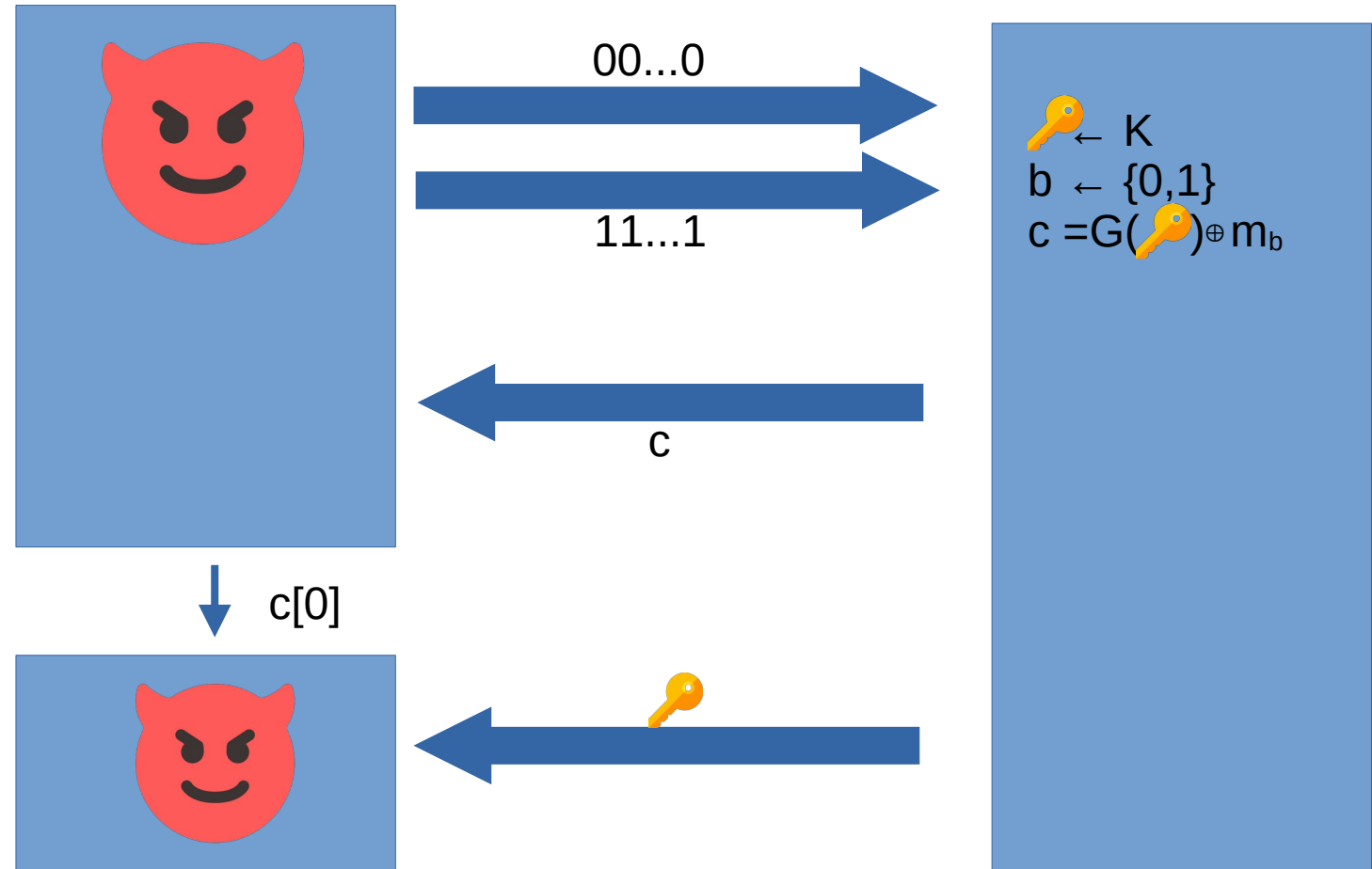
$G(\text{key})$

\oplus

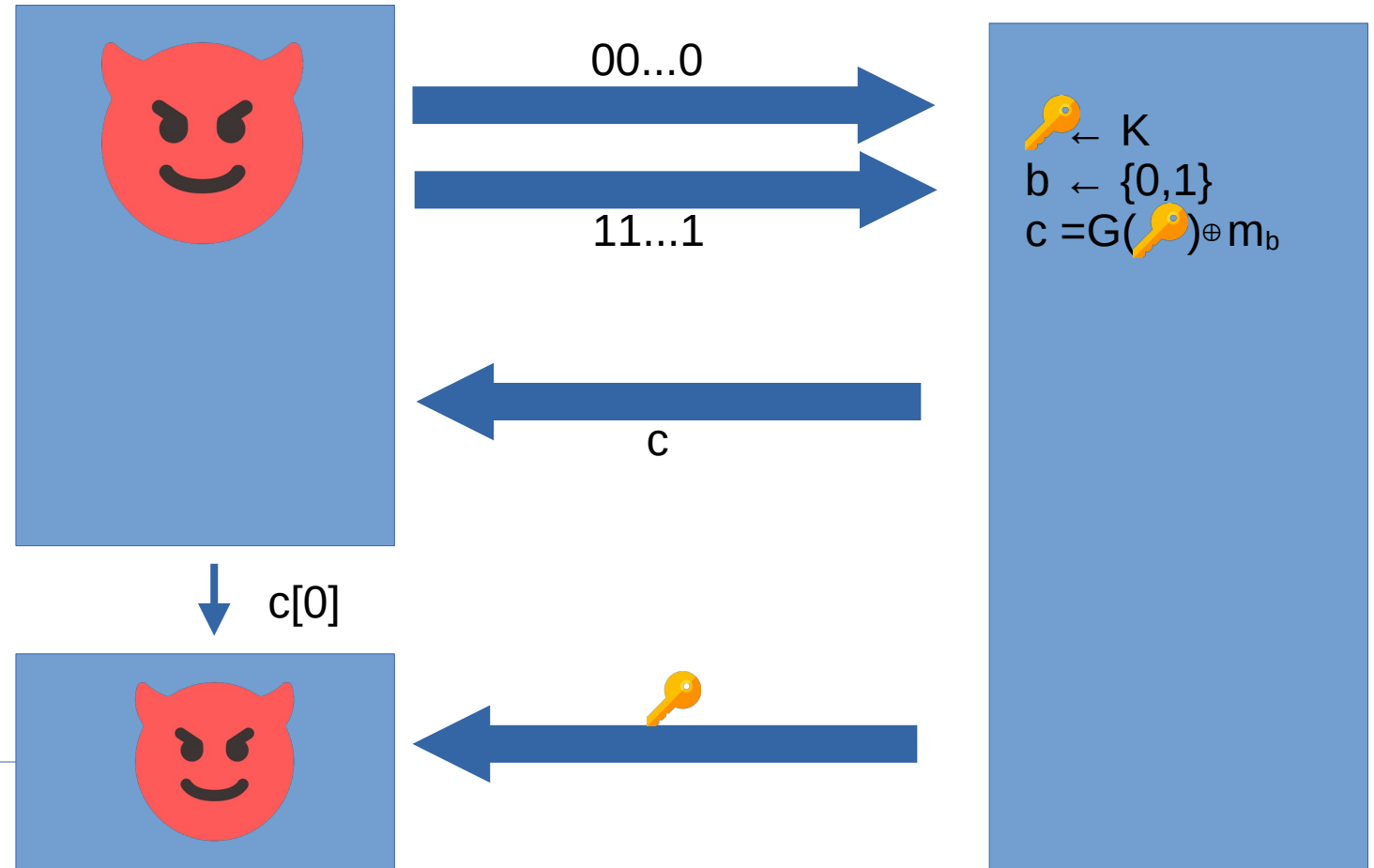
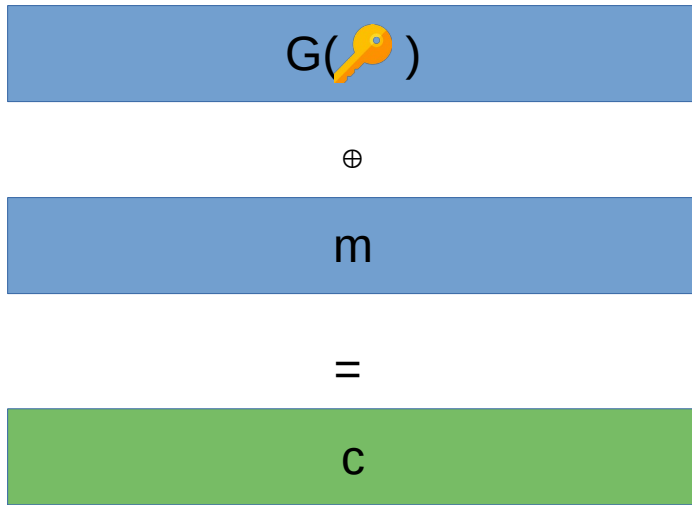
m

$=$

c



Naive Attempt #1



Naive Attempt #2

Enc(, m)

G(s)

\oplus

m

=

Ext(,

C₁)

\oplus

S

=

C₂

Naive Attempt #2

Enc(🔑 ,m)

G(s)

⊕

m

=

Ext(🔑 ,

C₁)

⊕

S

=

C₂

Dec(🔑 ,m)

Ext(🔑 ,

C₁)

⊕

C₂

=

S

G(s)

=

m

Naive Attempt #2

Enc(, m)

G(s)

\oplus

m

=

Ext(,

C₁)

\oplus

S

=

C₂

Perfectly
hidden

Dec(, m)

Ext(,

C₁)

\oplus

C₂

=

S

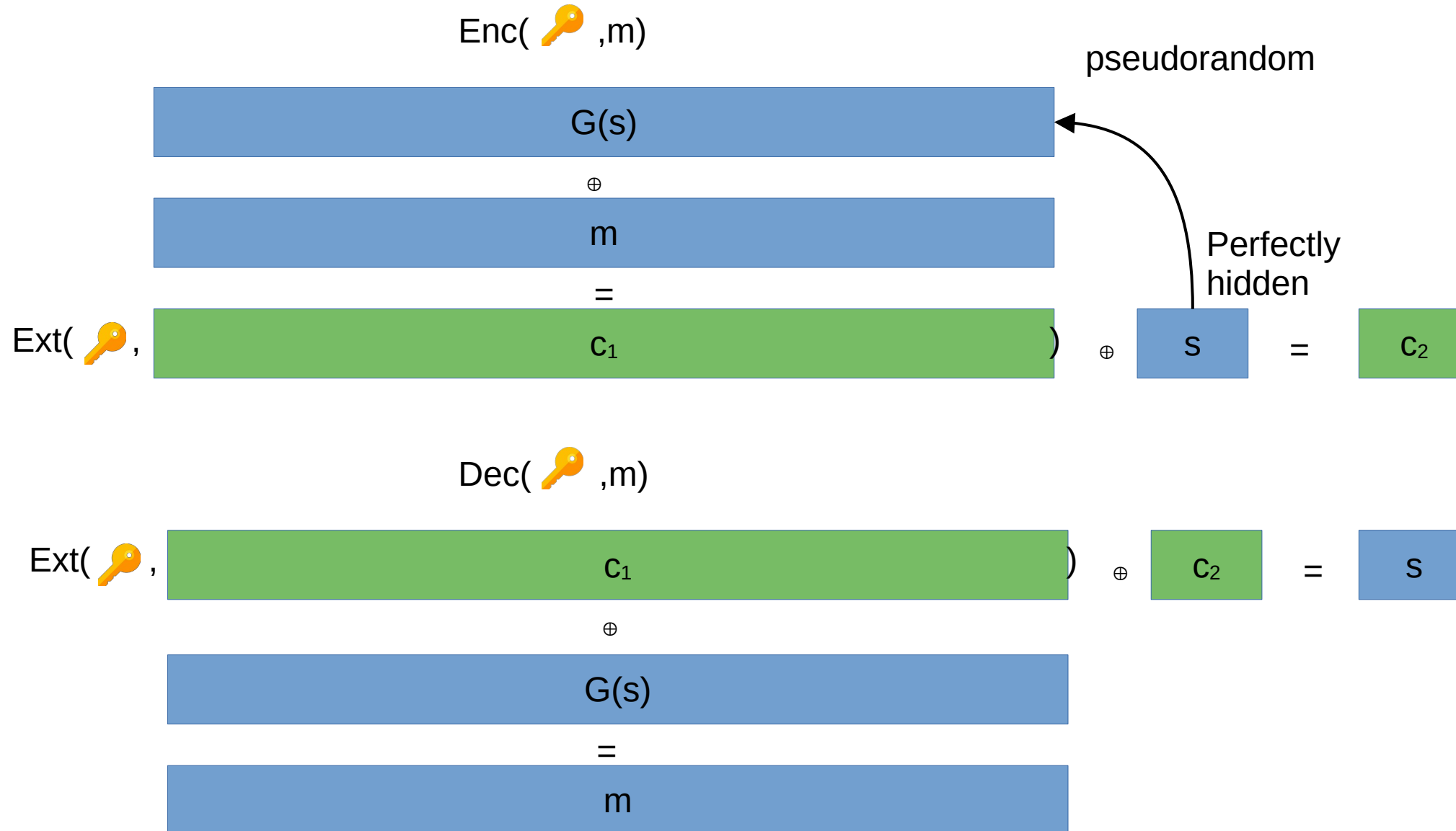
\oplus

G(s)

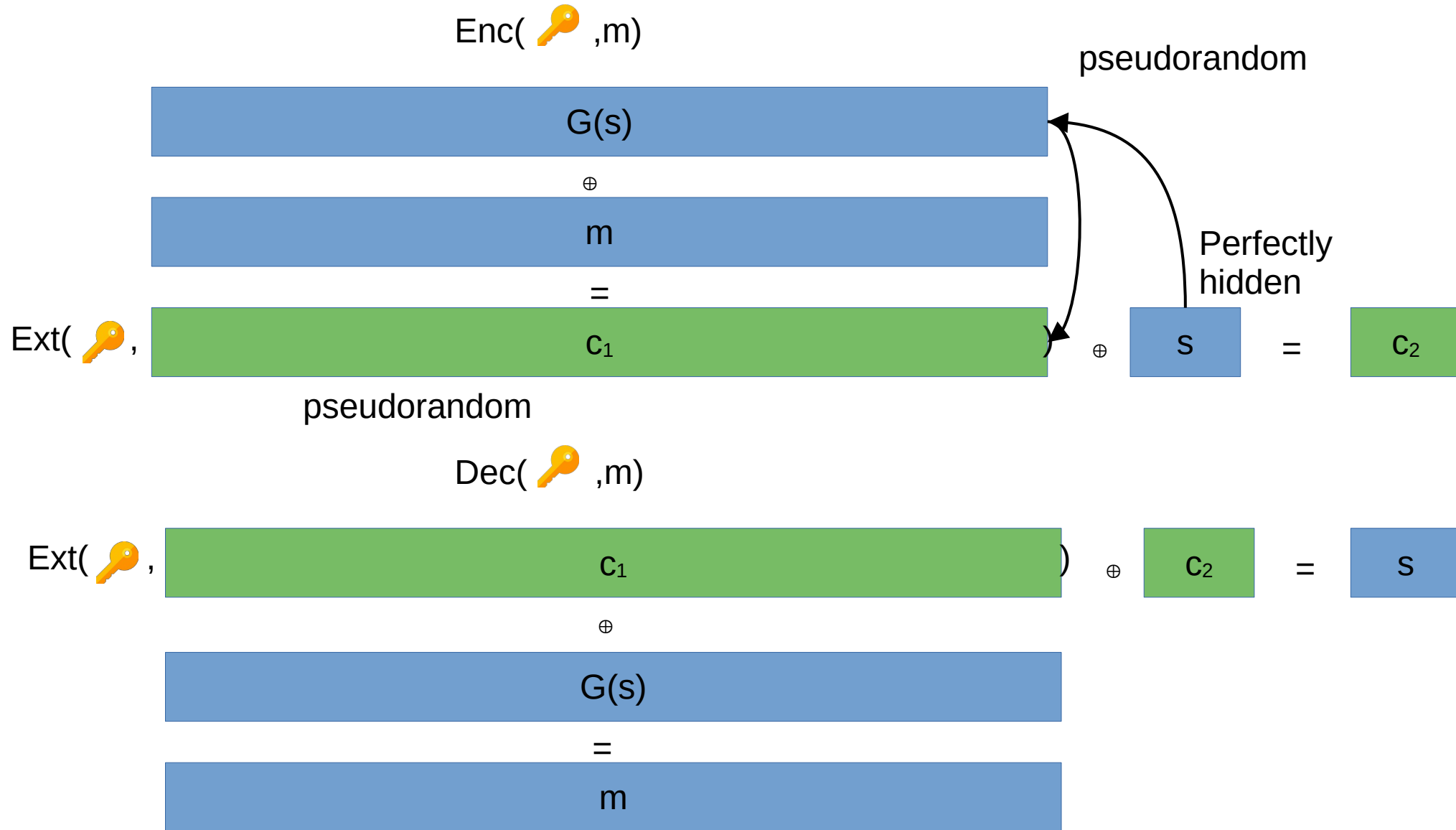
=

m

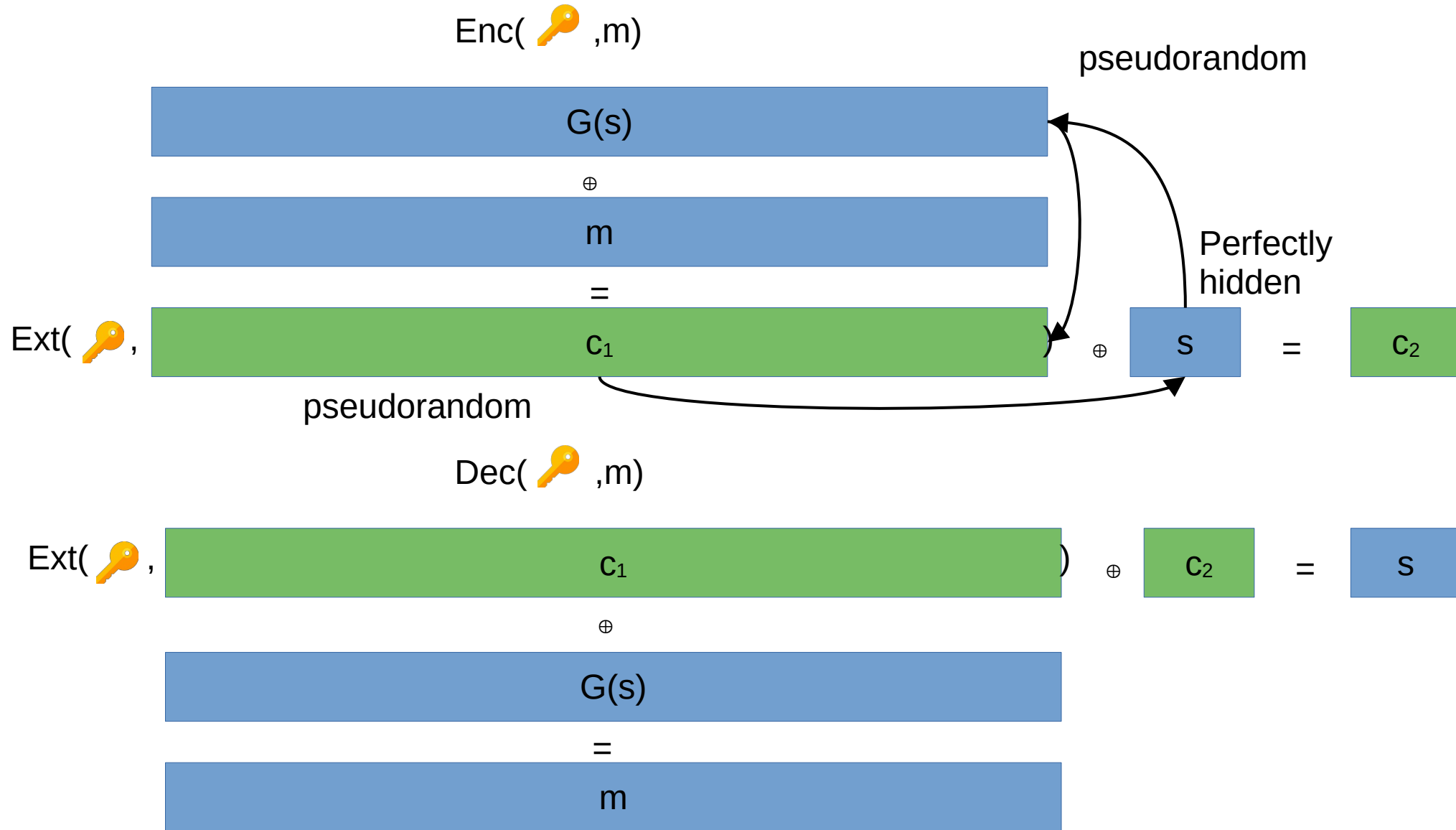
Naive Attempt #2



Naive Attempt #2



Naive Attempt #2



Entropic Encodings [DGO19, GLW20, MW20]

$$\text{Enc}_{\text{crs}}(\text{m}) = \text{c}$$

Entropic Encodings [DGO19, GLW20, MW20]

$$\text{Enc}_{\text{crs}}(\text{m}) = \text{c}$$

$$\text{Dec}_{\text{crs}}(\text{c}) = \text{m}$$

Entropic Encodings [DGO19, GLW20, MW20]

$$\text{Enc}_{\text{crs}}(\text{m}) = \text{c}$$

$$\text{Dec}_{\text{crs}}(\text{c}) = \text{m}$$

$$\text{SimEnc}(\text{m}) = \text{c}', \text{crs}'$$

$$\text{c}, \text{crs} \approx \text{c}', \text{crs}'$$

Entropic Encodings [DGO19, GLW20, MW20]

$$\text{En}_{\text{crs}}(\text{m}) = \text{c}$$

$$\text{De}_{\text{crs}}(\text{c}) = \text{m}$$

$$\text{SimEn}(\text{m}) = \text{c}', \text{crs}'$$

$$\text{c}, \text{crs} \approx \text{c}', \text{crs}'$$

$$H_{\infty}(\text{c}' \mid \text{crs}') \text{ is big for all m}$$

Entropic Encodings [DGO19, GLW20, MW20]

$$\text{Enc}_{\text{crs}}(\text{m}) = \text{c}$$

$$\text{Dec}_{\text{crs}}(\text{c}) = \text{m}$$

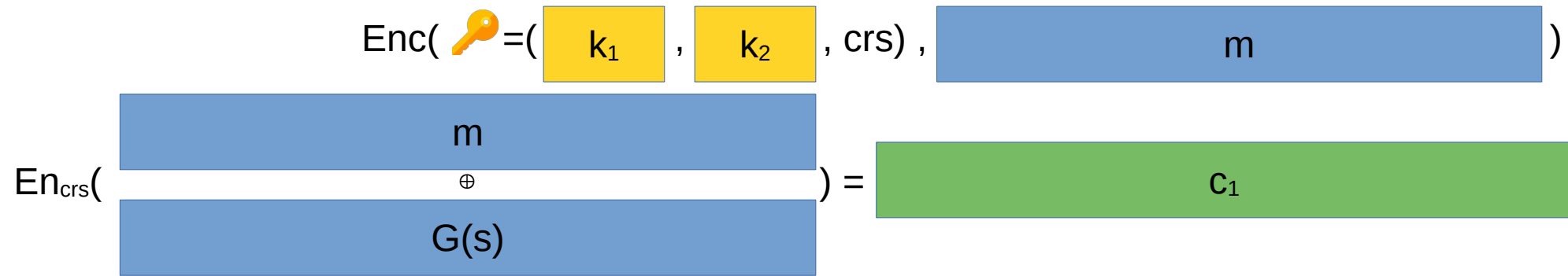
$$\text{SimEnc}(\text{m}) = \text{c}', \text{crs}'$$

$$\text{c}, \text{crs} \approx \text{c}', \text{crs}'$$

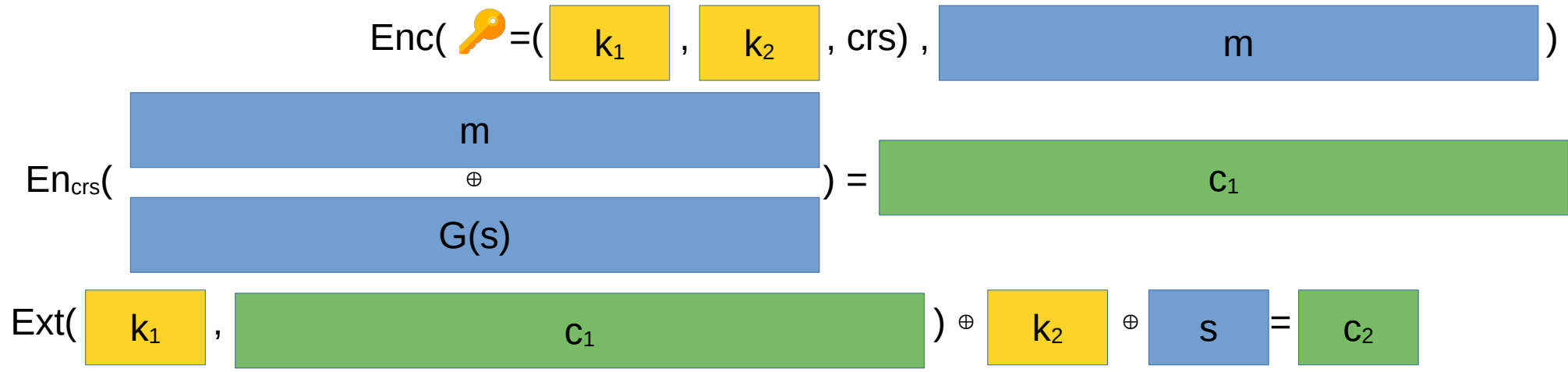
$$H_{\infty}(\text{c}' \mid \text{crs}') \text{ is big for all m}$$

LWE or DCR

Construction



Construction



Construction

$$\text{Enc}(\text{key} = (k_1, k_2, \text{crs}), m)$$

$$\text{Enc}_{\text{crs}}(m \oplus G(s)) = C_1$$

$$\text{Ext}(k_1, C_1) \oplus k_2 \oplus s = C_2$$

$$\text{Dec}(\text{key} = (k_1, k_2, \text{crs}), C_1, C_2)$$

$$\text{Ext}(k_1, C_1) \oplus C_2 \oplus k_2 = s$$

$$\text{Dec}_{\text{crs}}(C_1) \oplus G(s)$$

$$= m$$

Construction

$$\text{Enc}(\text{key} = (k_1, k_2, \text{crs}), m)$$

$$\text{Enc}_{\text{crs}}(m \oplus G(s)) = C_1 \text{ pseudoentropy}$$

$$\text{Ext}(k_1, C_1) \oplus k_2 \oplus s = C_2$$

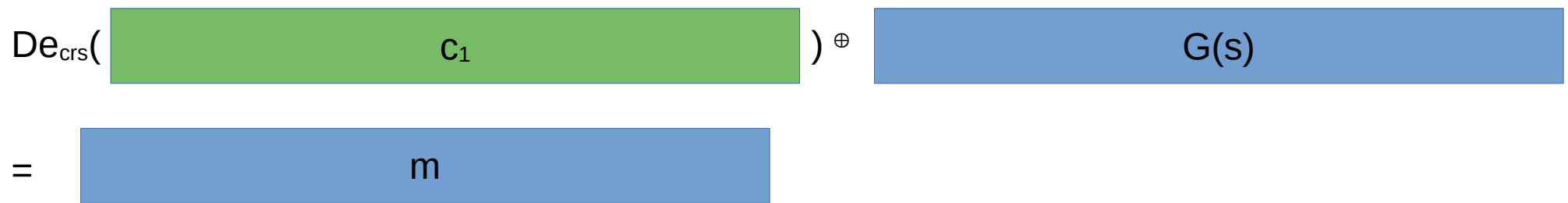
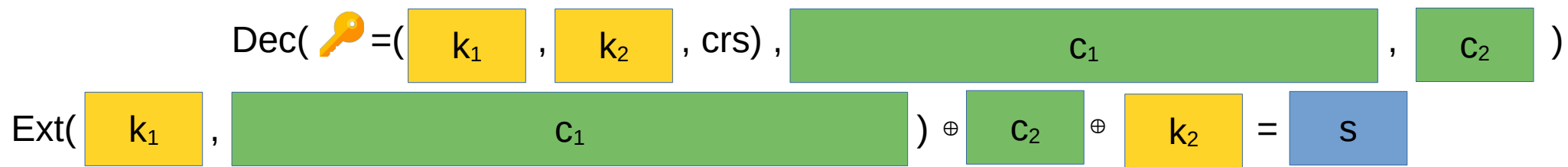
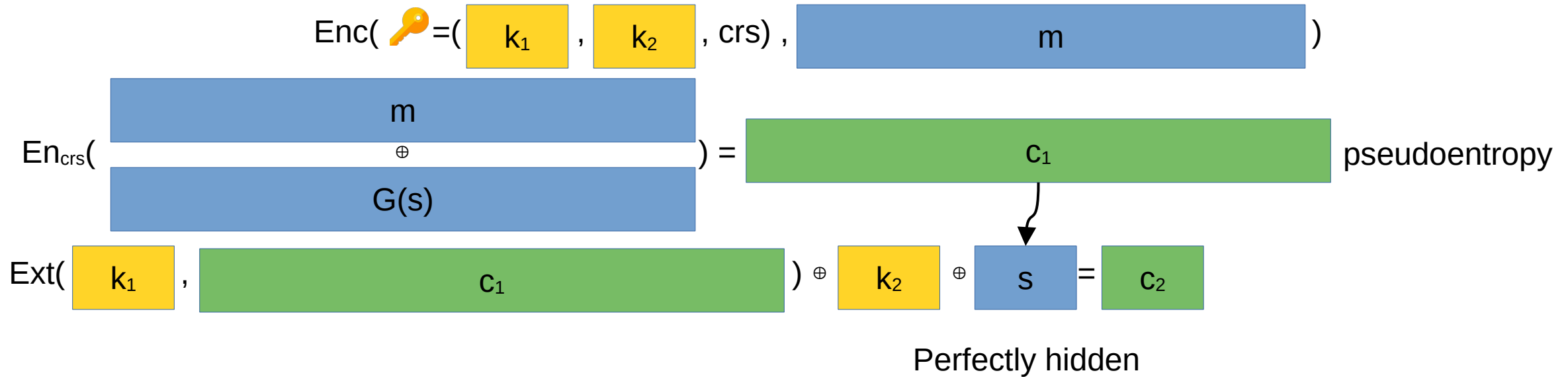
$$\text{Dec}(\text{key} = (k_1, k_2, \text{crs}), C_1, C_2)$$

$$\text{Ext}(k_1, C_1) \oplus C_2 \oplus k_2 = s$$

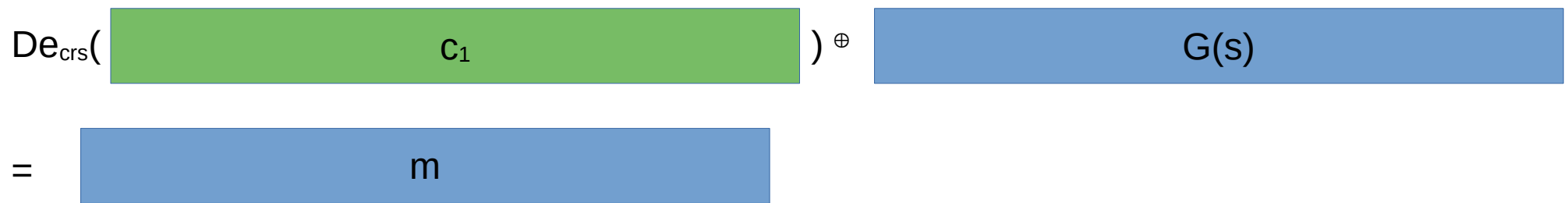
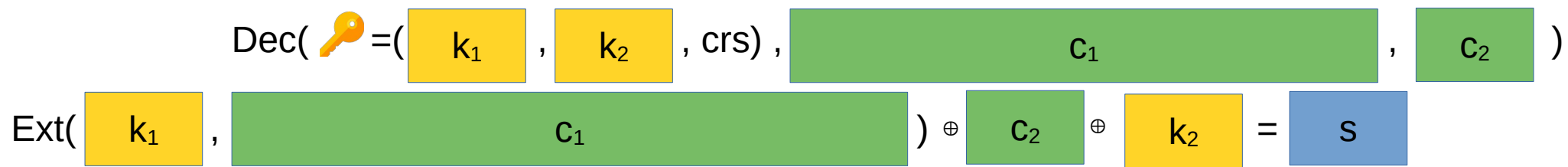
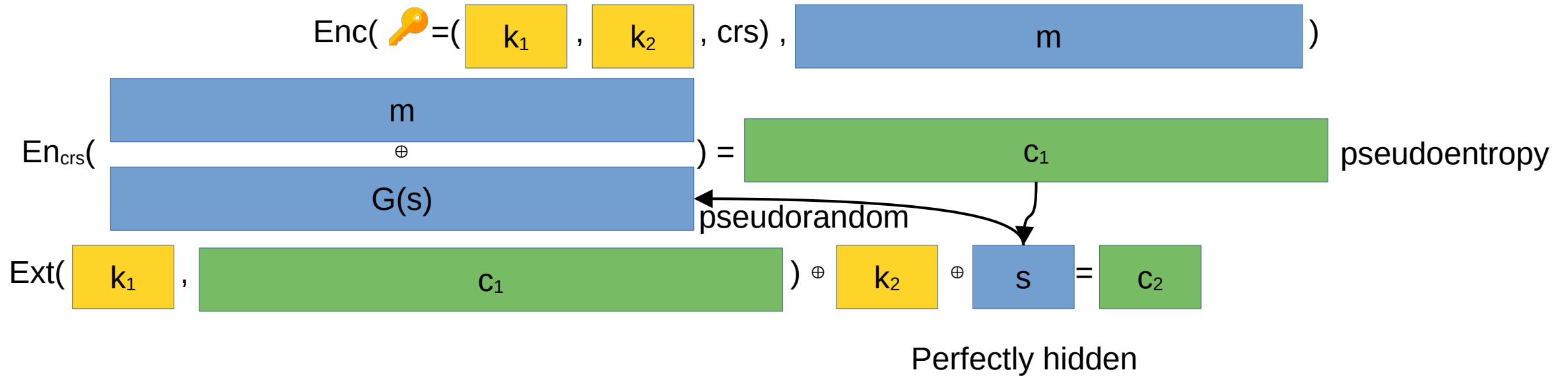
$$\text{De}_{\text{crs}}(C_1) \oplus G(s)$$

$$= m$$

Construction



Construction



Theorem 1 (informal). Assuming the hardness of (LWE or DCR) there exists a Incompressible (EAV-style) Symmetric-Key Encryption with

- Message length n
- Ciphertext length $n + \text{poly}(\lambda)$
- Key length $n + \text{poly}(\lambda)$ (dominated by crs)

Theorem 1 (informal). Assuming the hardness of (LWE or DCR) there exists a Incompressible (EAV-style) Symmetric-Key Encryption with

- Message length n
- Ciphertext length $n + \text{poly}(\lambda)$
- Key length $n + \text{poly}(\lambda)$ (dominated by crs)

Are Public-Key assumptions necessary to achieve Incompressible (EAV-style) Symmetric-Key Encryption?

We extend this to Incompressible Public-Key Encryption using a form of Hash Proof Systems

We extend this to Incompressible Public-Key Encryption using a form of Hash Proof Systems

Theorem 2 (informal). Assuming Incompressible Symmetric-Key Encryption and DDH there exists a Incompressible CCA public-key encryption with

- Message length n
- Public-key length $n^{2/3}\text{poly}(\lambda)$
- Ciphertext length $(n+n^{2/3})\text{poly}(\lambda)$
- Secret-key length $n \text{ poly}(\lambda)$

We extend this to Incompressible Public-Key Encryption using a form of Hash Proof Systems

Theorem 2 (informal). Assuming Incompressible Symmetric-Key Encryption and DDH there exists a Incompressible CCA public-key encryption with

- Message length n
- Public-key length $n^{2/3}\text{poly}(\lambda)$
- Ciphertext length $(n+n^{2/3})\text{poly}(\lambda)$
- Secret-key length $n \text{ poly}(\lambda)$

Is it possible to achieve best possible parameters without assuming iO?

Summary



- Entropic Encodings (LWE or DCR) → Incompressible EAV SKE
 - A) Extension to Incompressible CCA PKE
 - B) DDH, LWE or Group Actions → Programmable HPS
 - C) Simple Uninstatiability ROM

eprint.iacr.org/2022/697

Dzi06 – Forward-Secure Storage
GWZ22 – Incompressible Cryptography
DGO19 – Proofs of Replicated Storage Without Timing Assumptions
GLW20 – New Techniques in Replica Encodings with Client Setup
MW20 – Incompressible Encodings