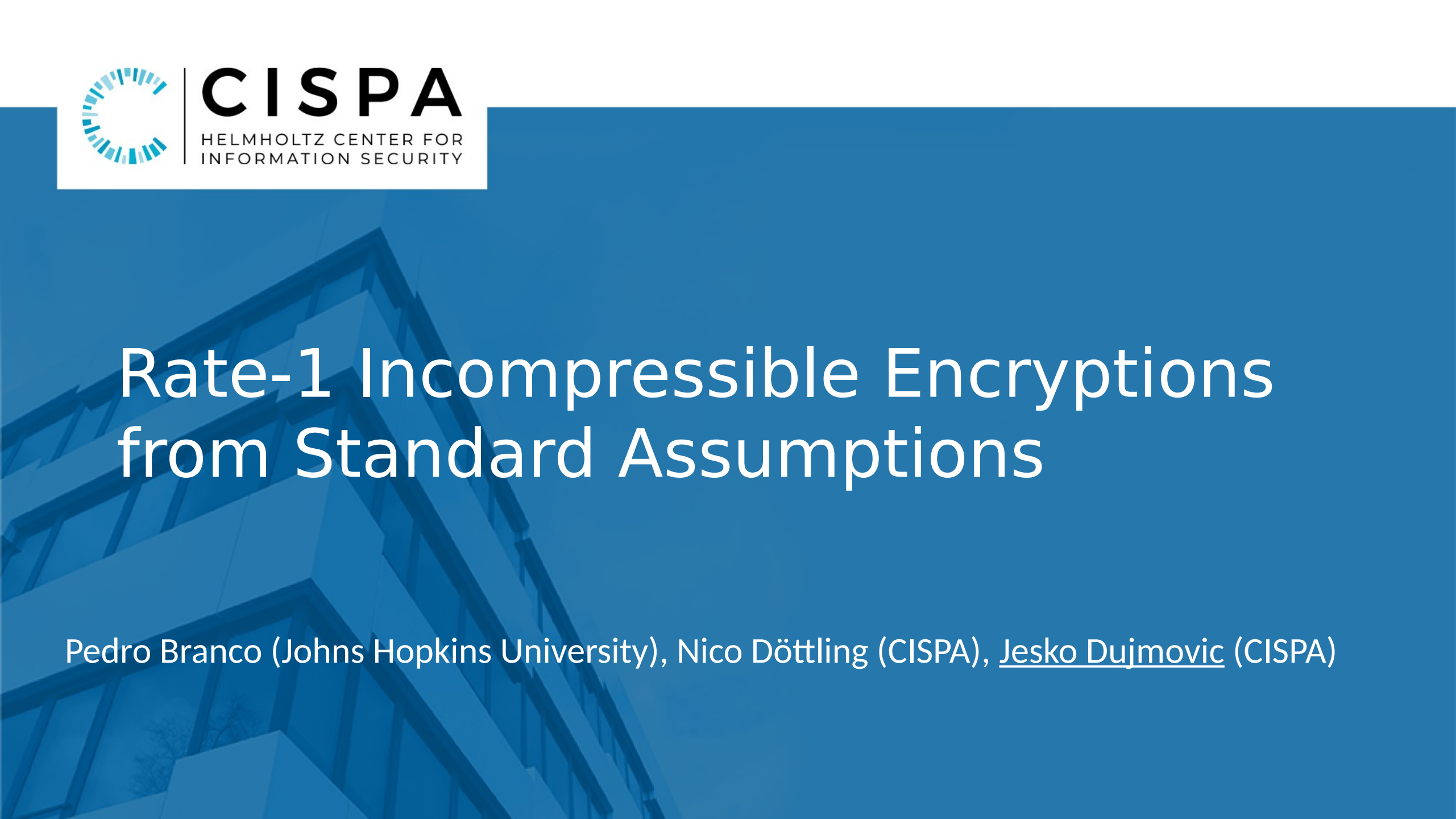
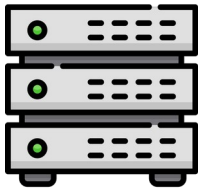
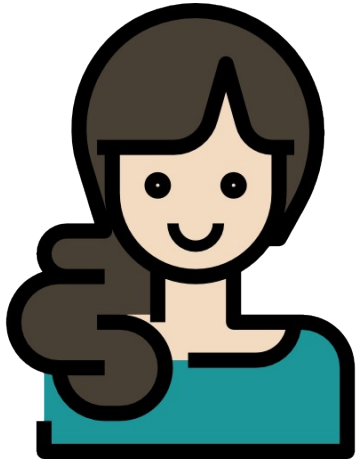


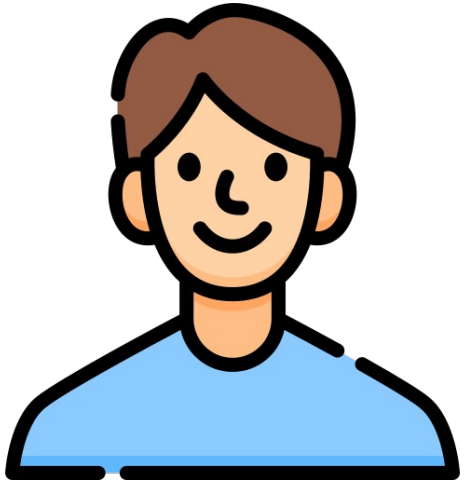
Rate-1 Incompressible Encryptions from Standard Assumptions

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

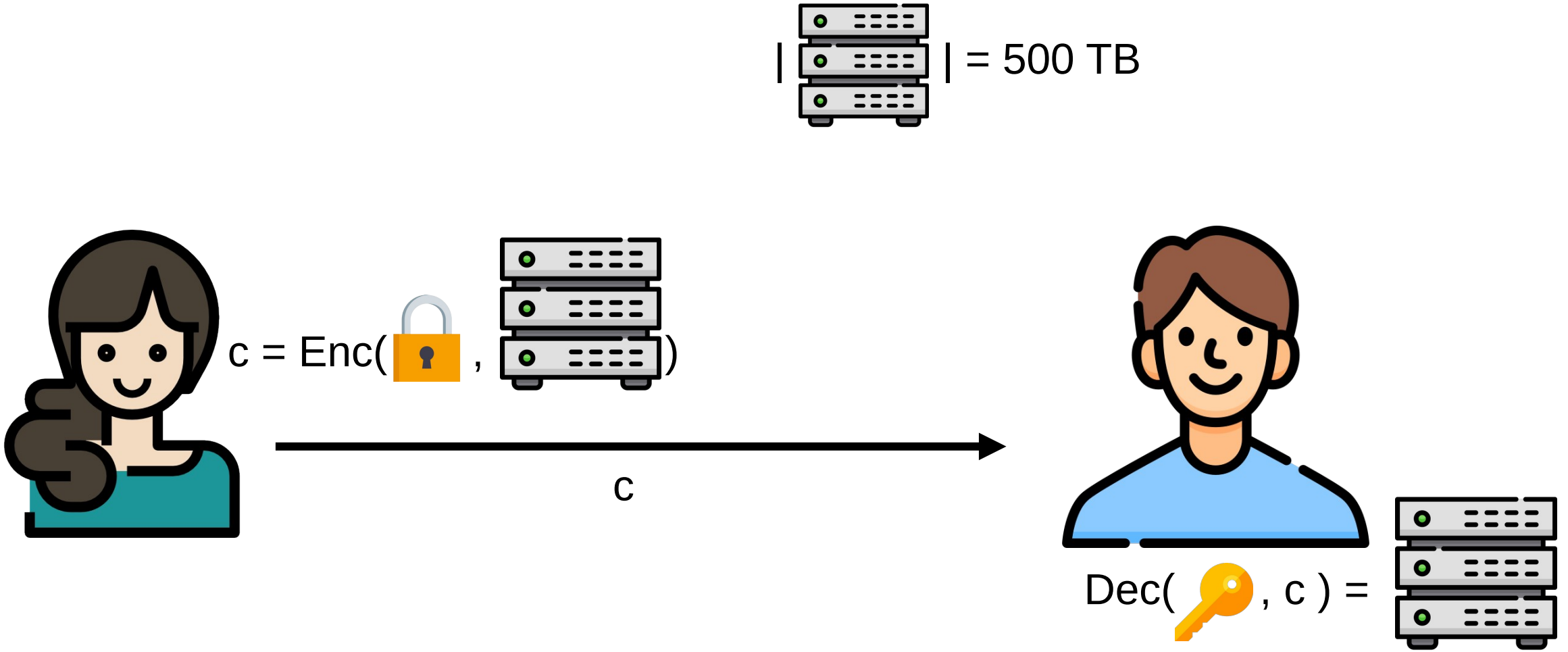
Incompressible Encryption

|  | = 500 TB

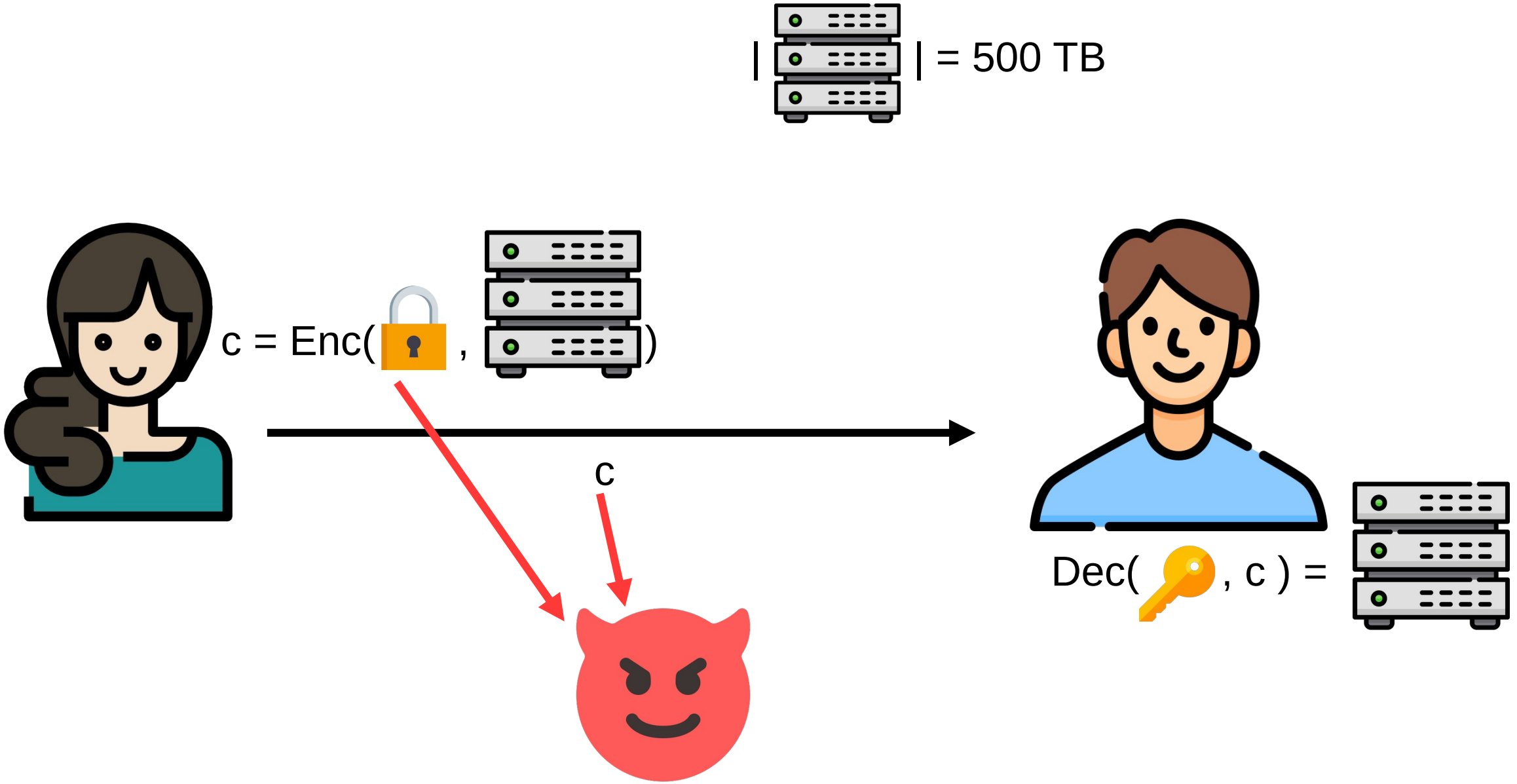




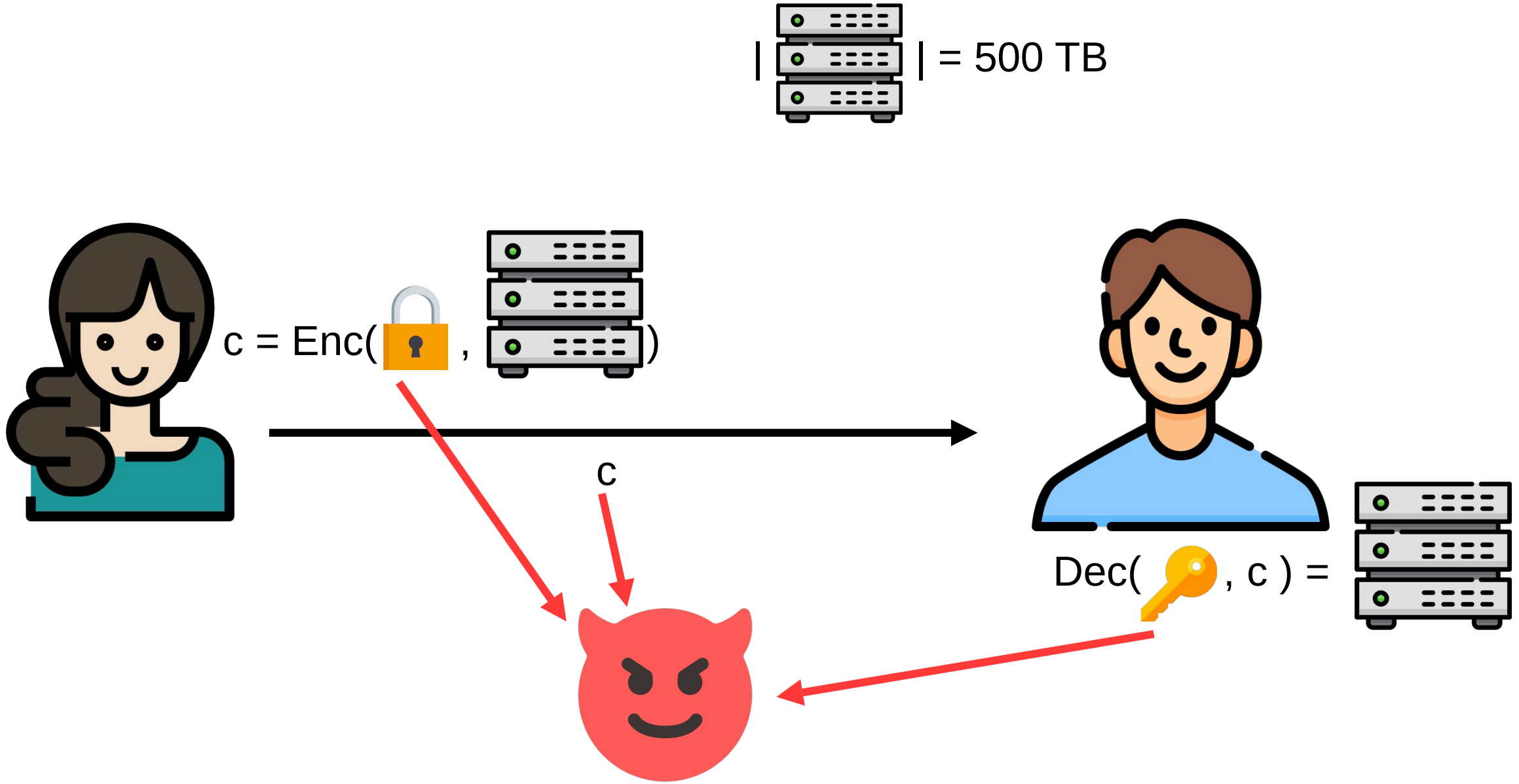
Incompressible Encryption



Incompressible Encryption

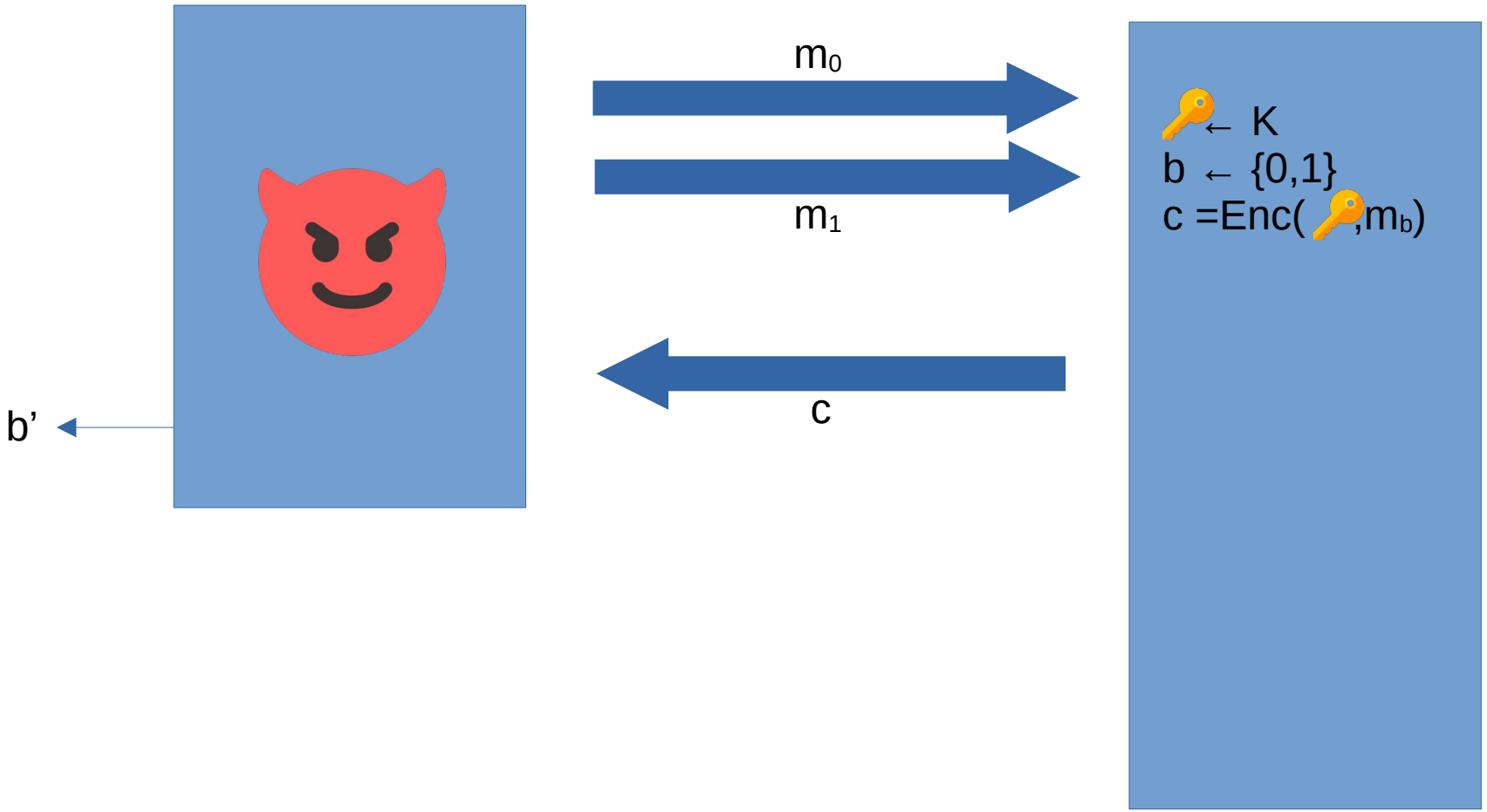


Incompressible Encryption



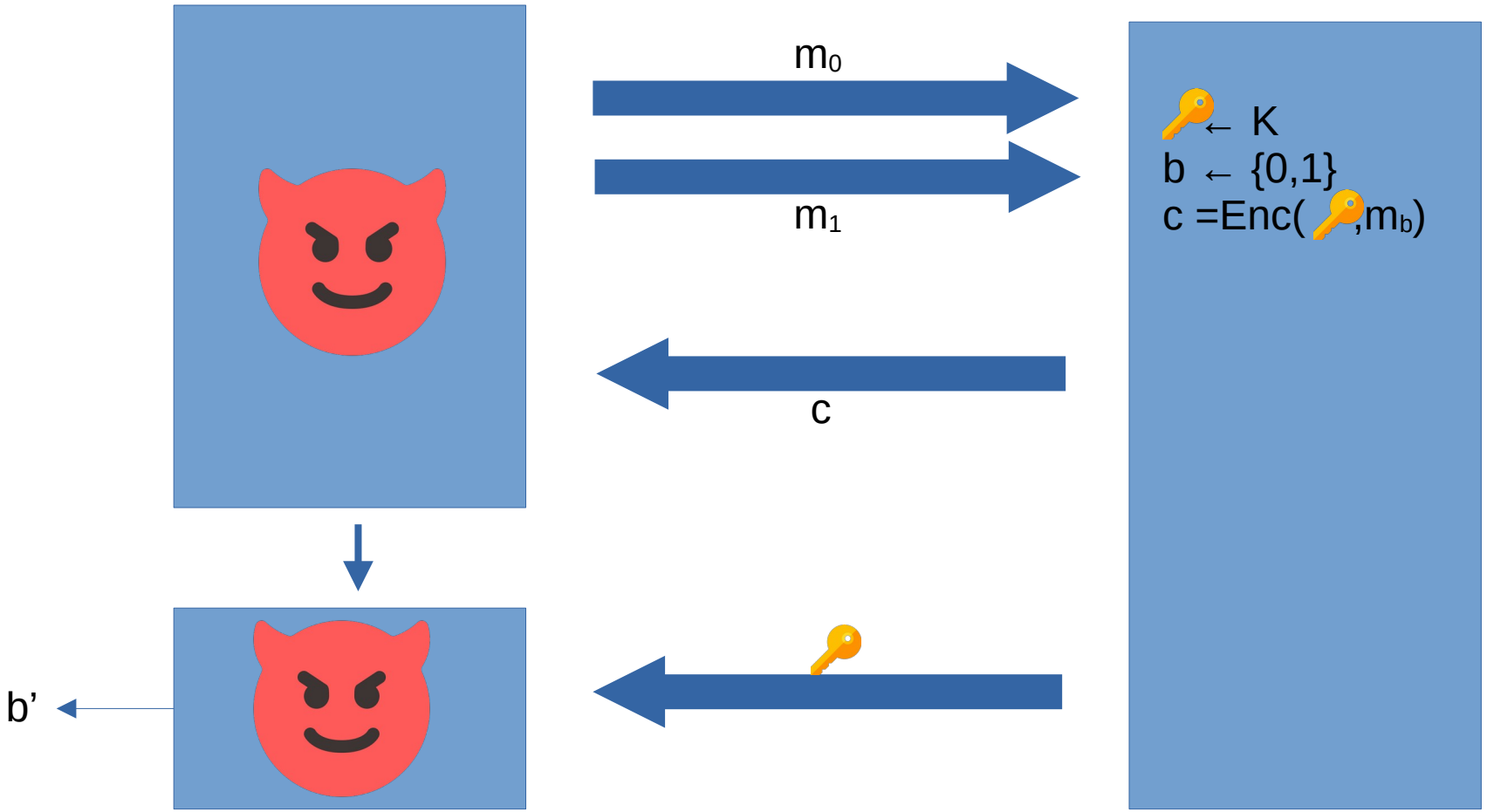
Incompressible Encryption [Dzi06,GWZ22]

EAV - Style

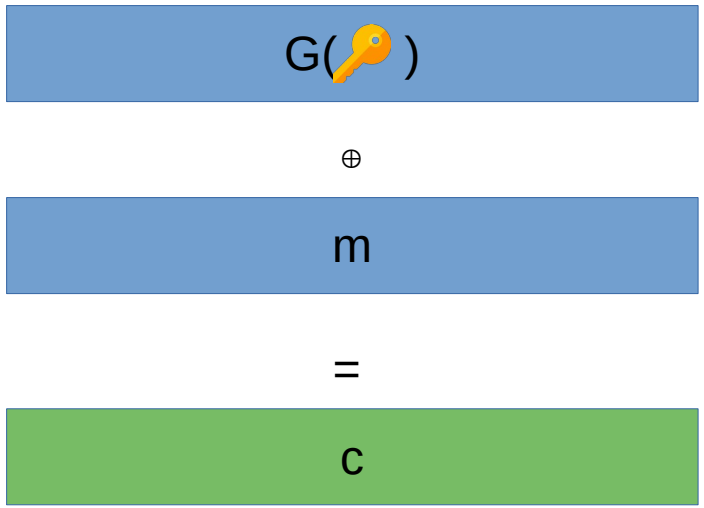


Incompressible Encryption [Dzi06,GWZ22]

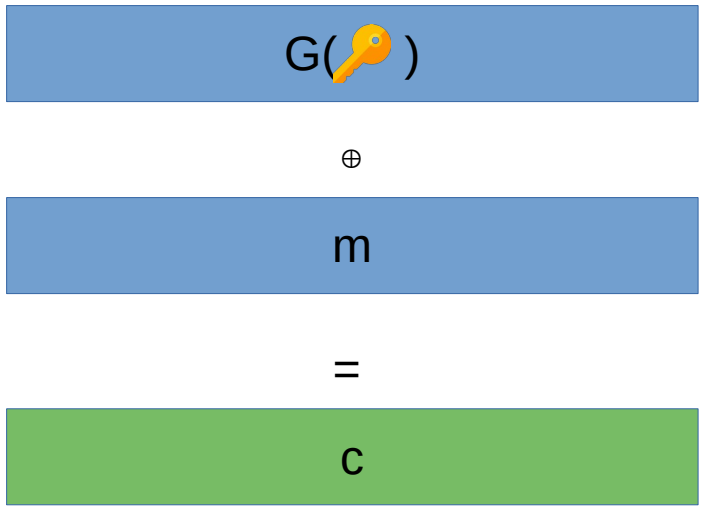
EAV - Style

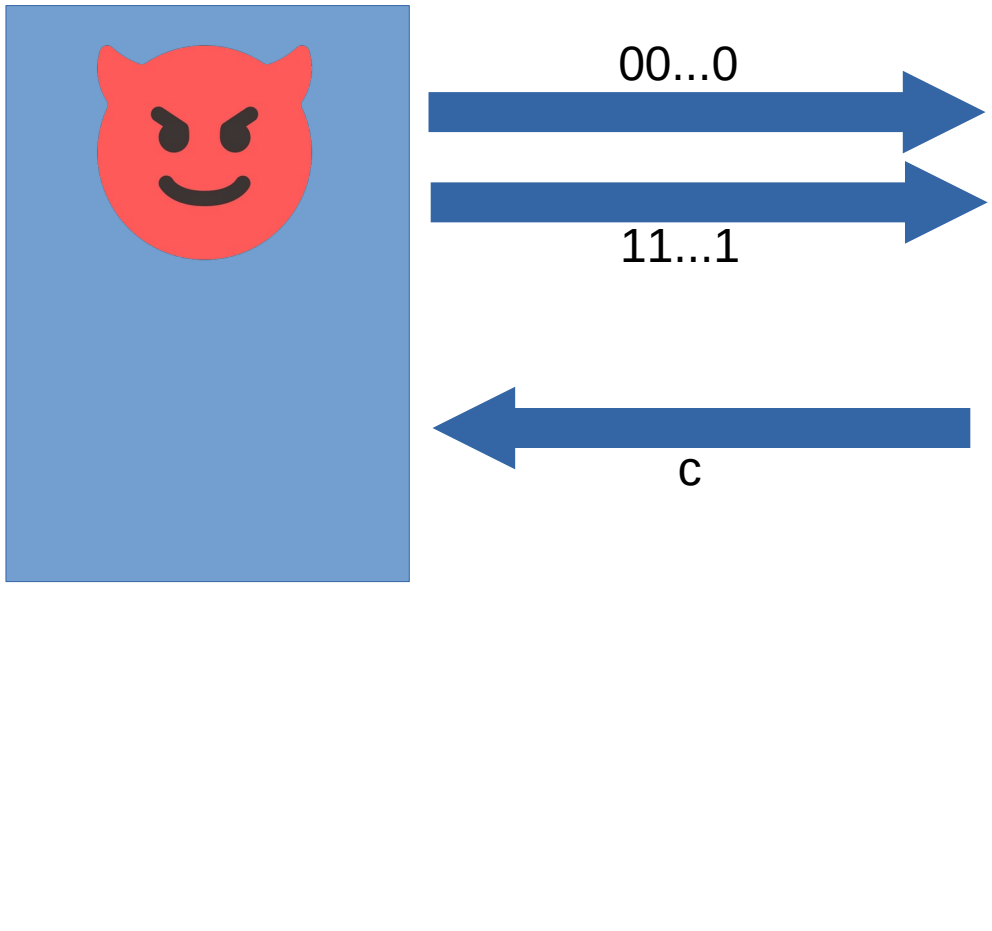


Naive Attempt #1

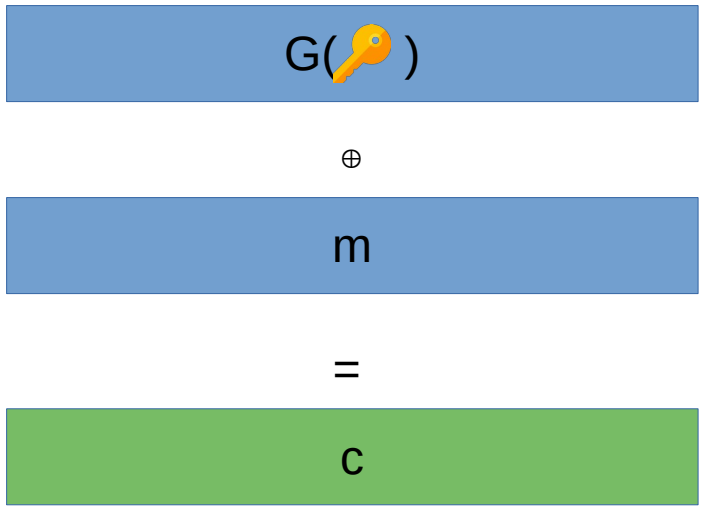


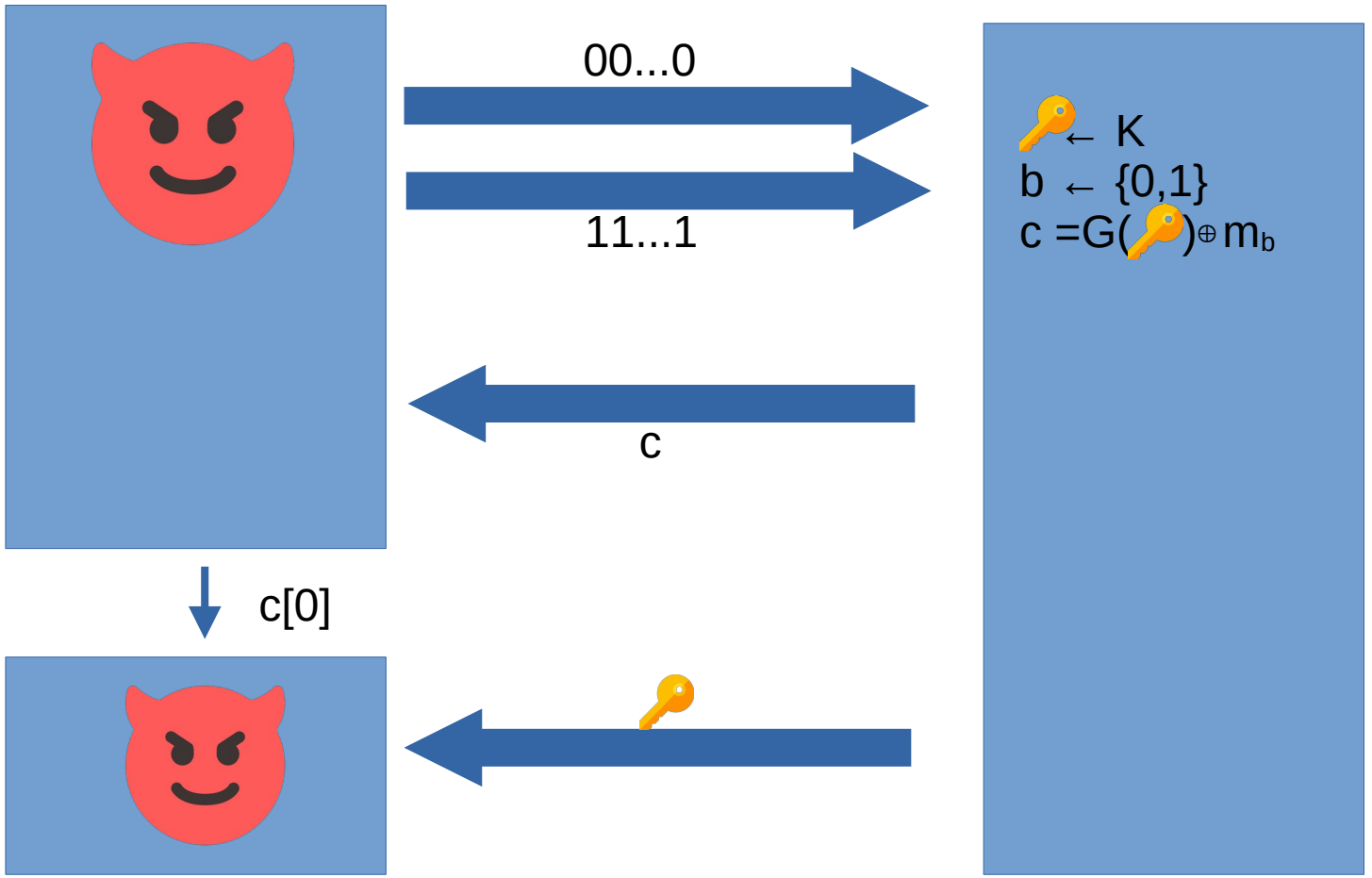
Naive Attempt #1



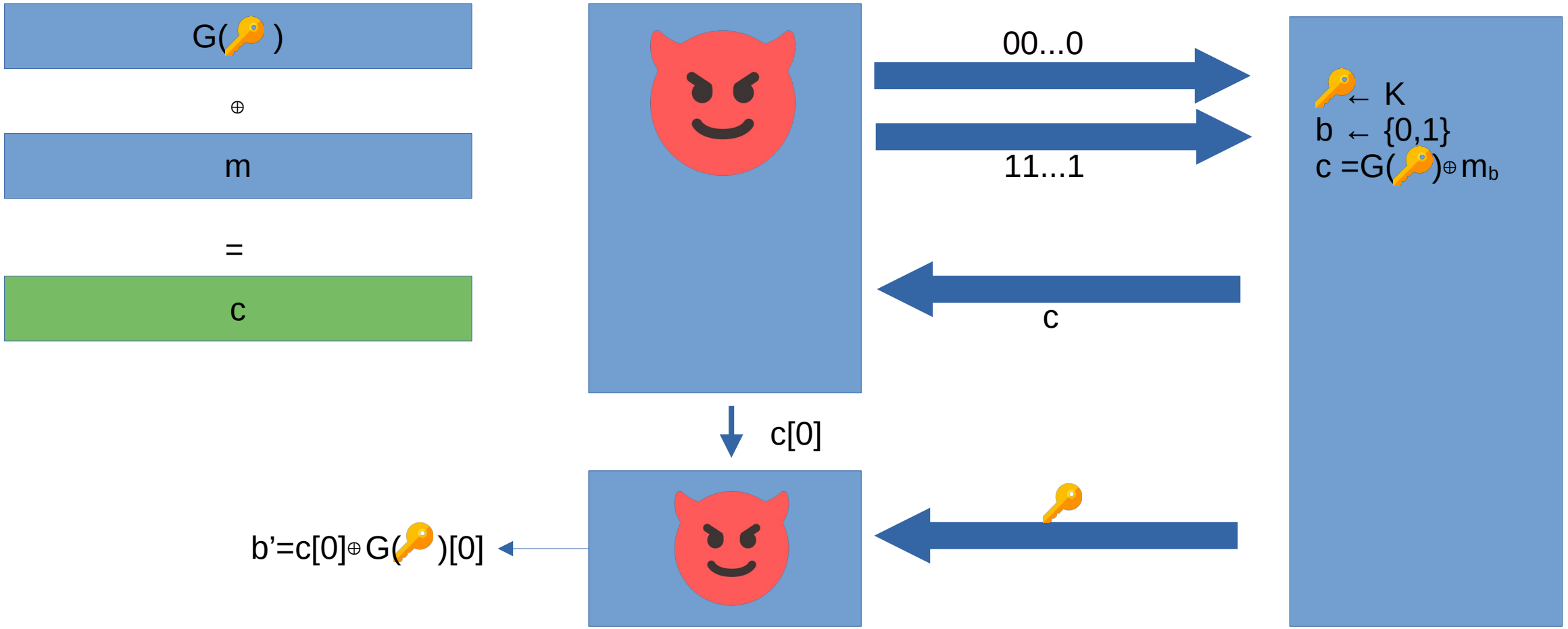


Naive Attempt #1

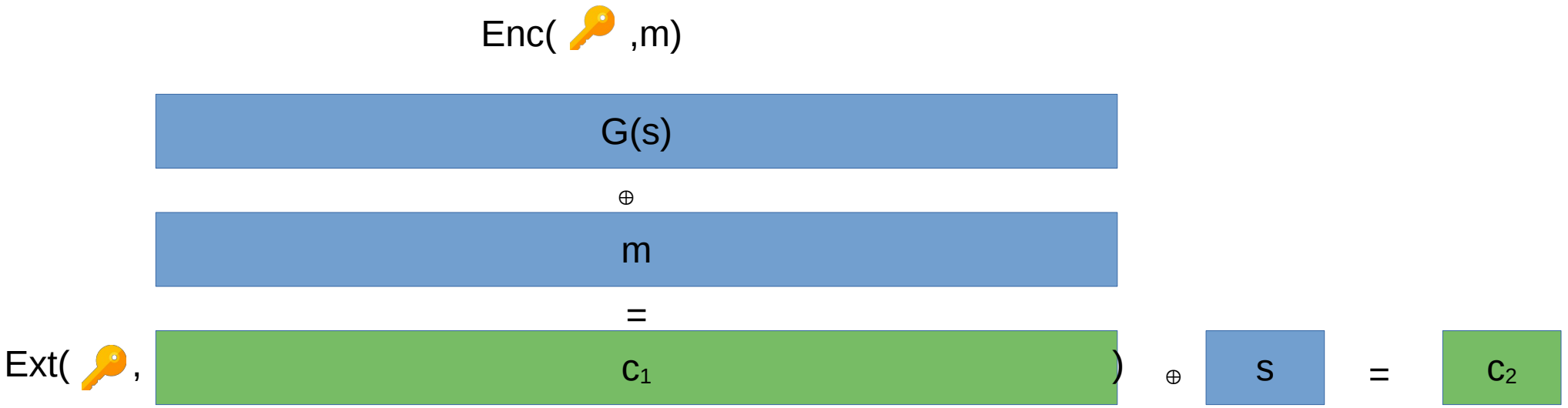




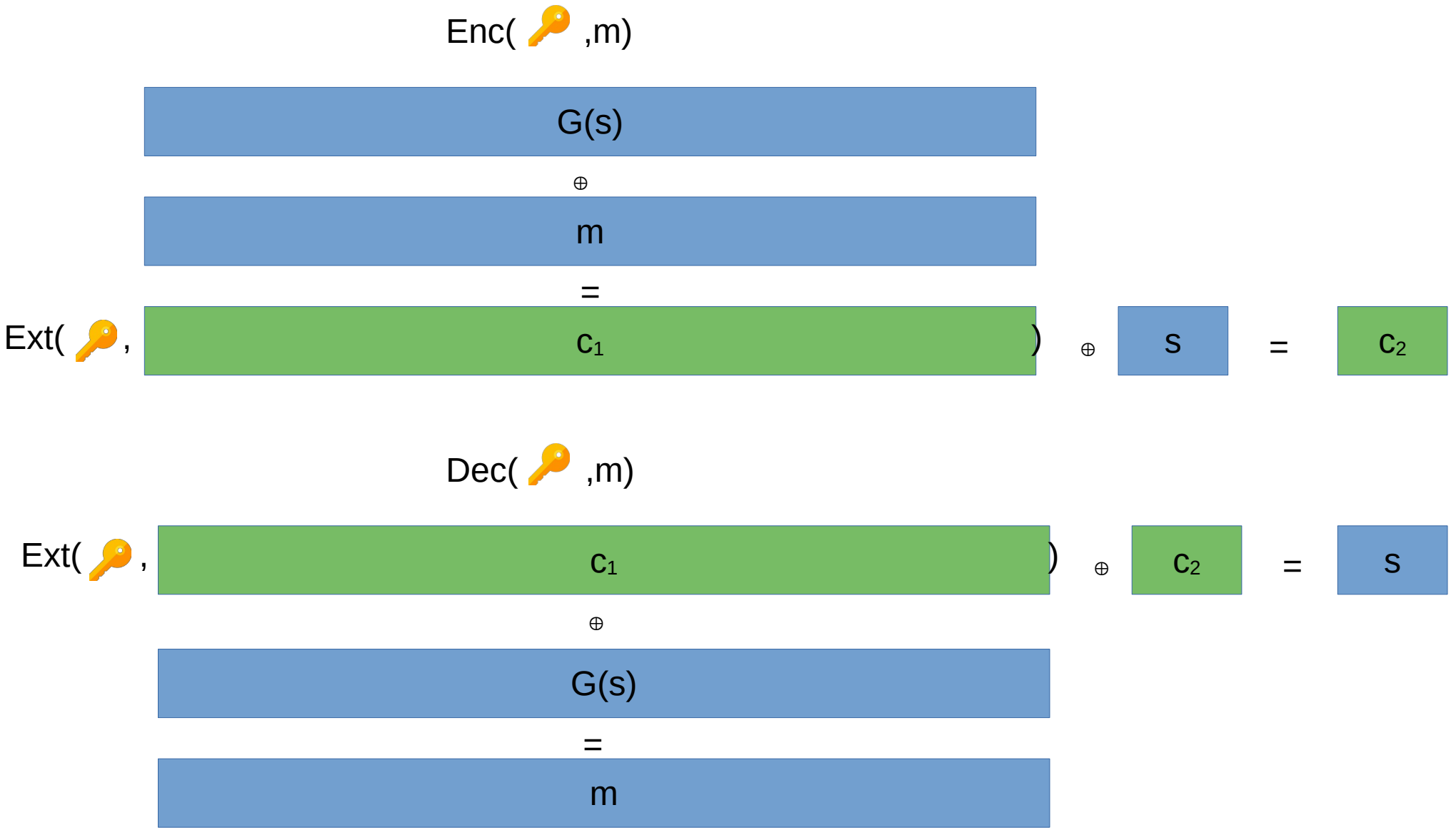
Naive Attempt #1



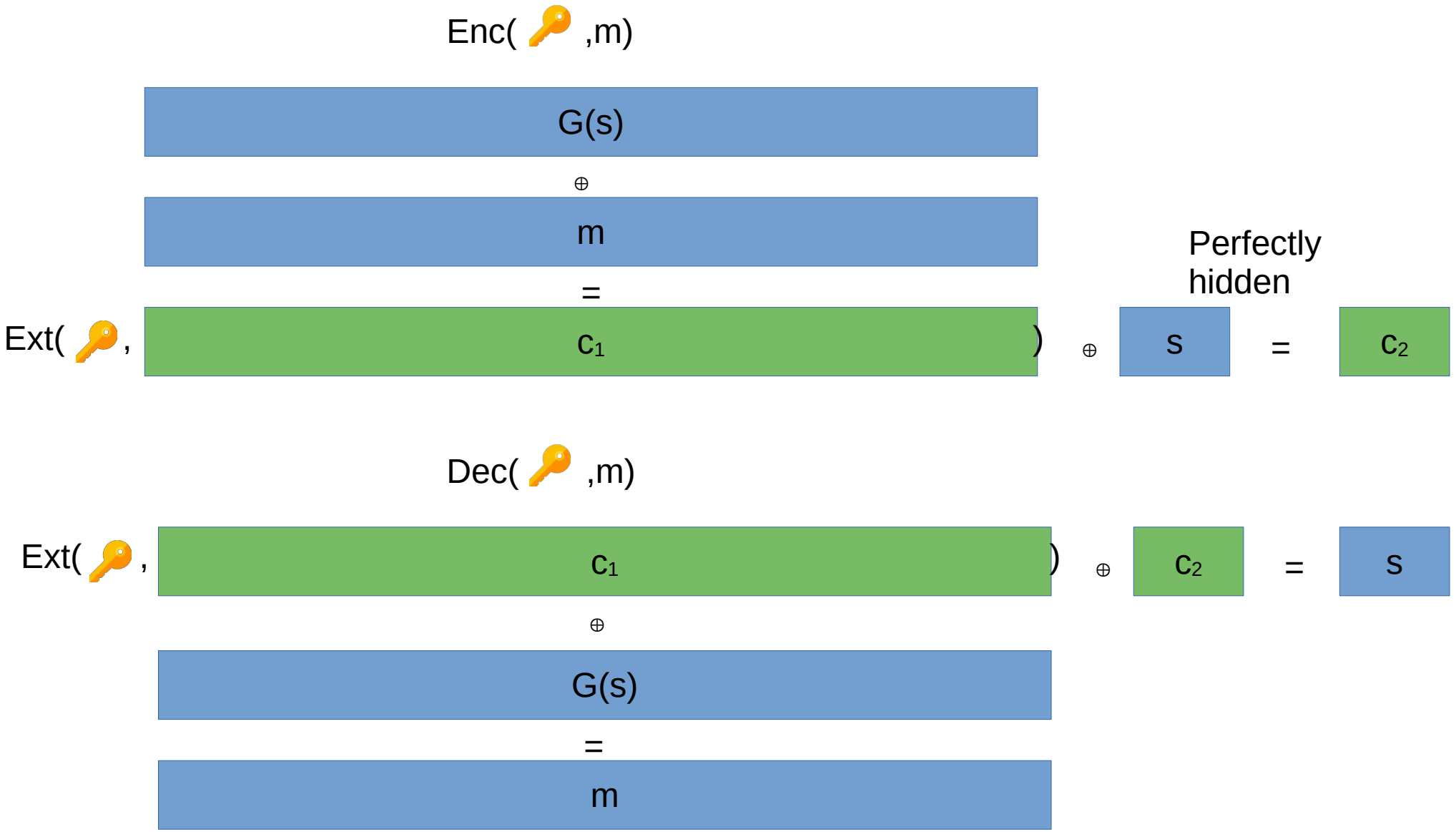
Naive Attempt #2



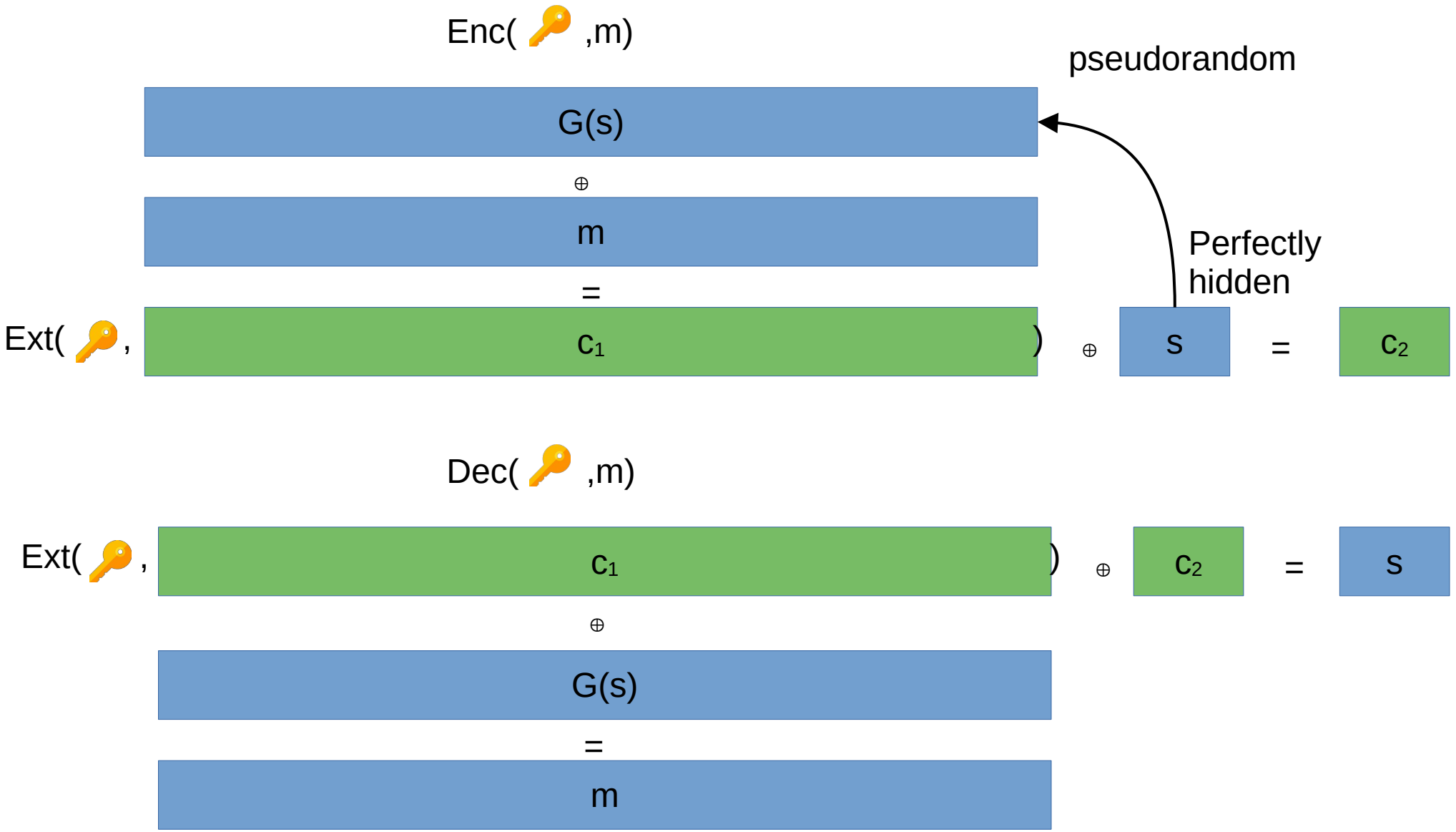
Naive Attempt #2



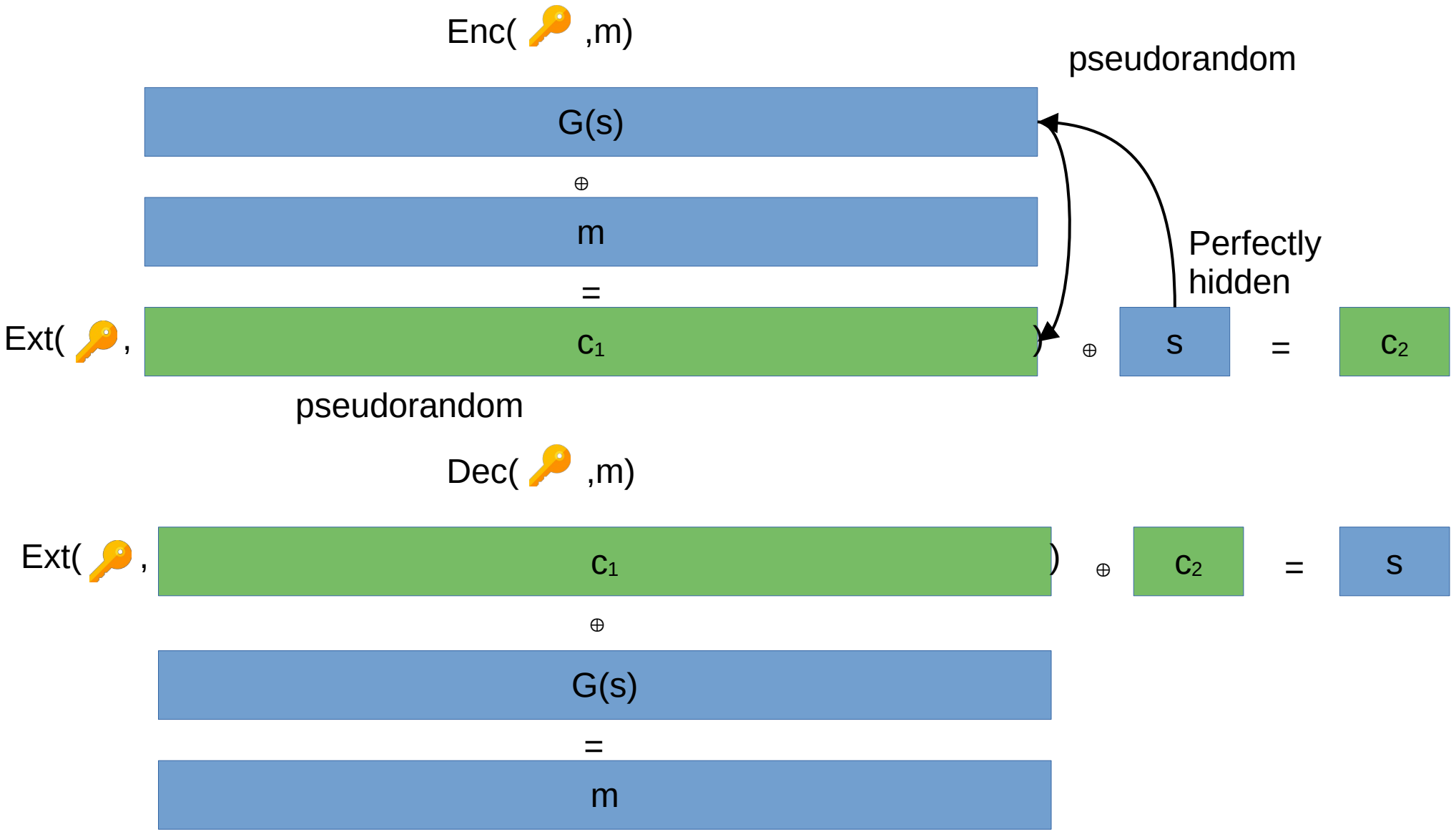
Naive Attempt #2



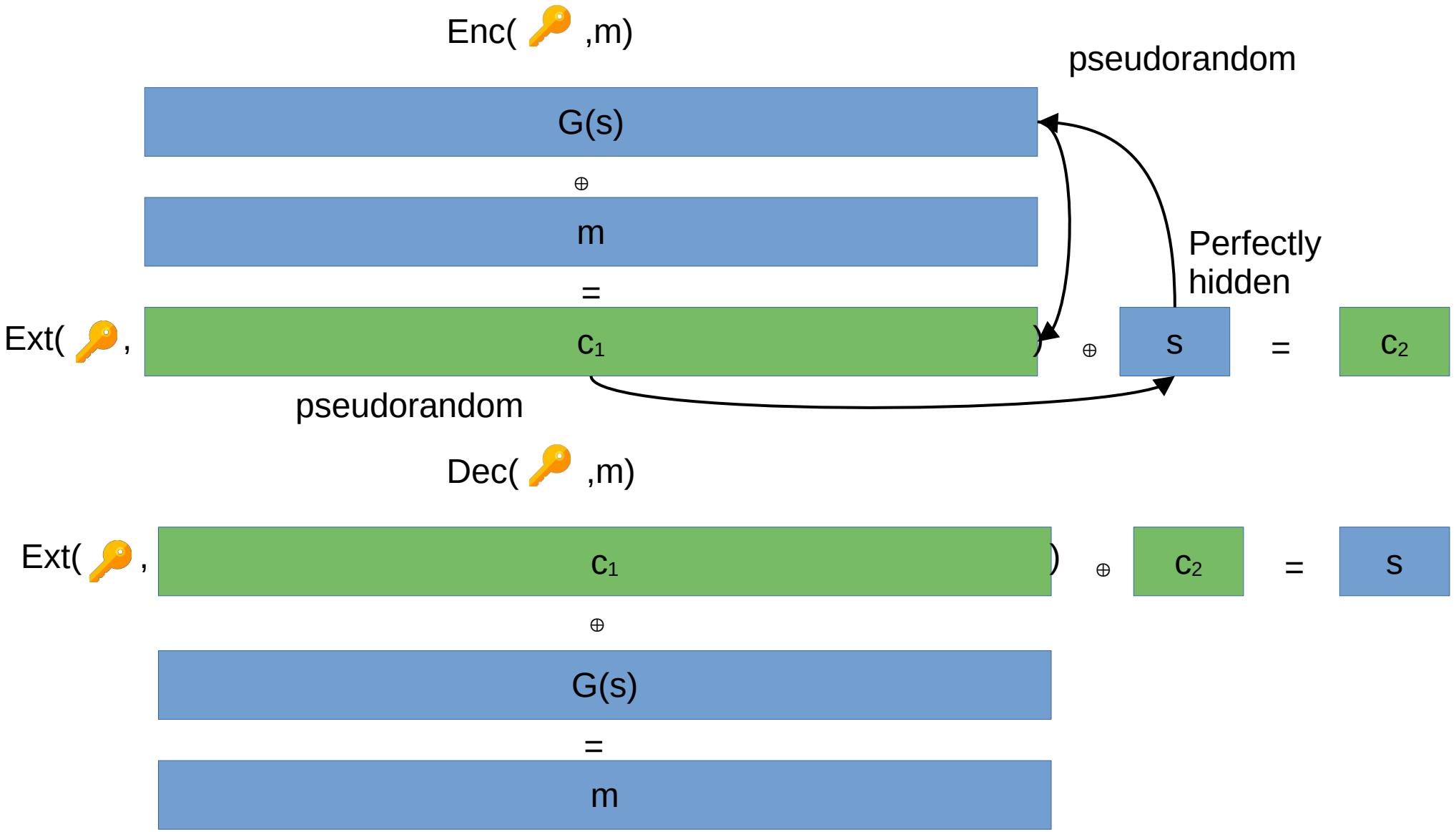
Naive Attempt #2



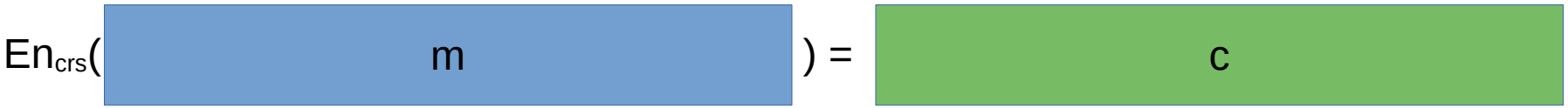
Naive Attempt #2



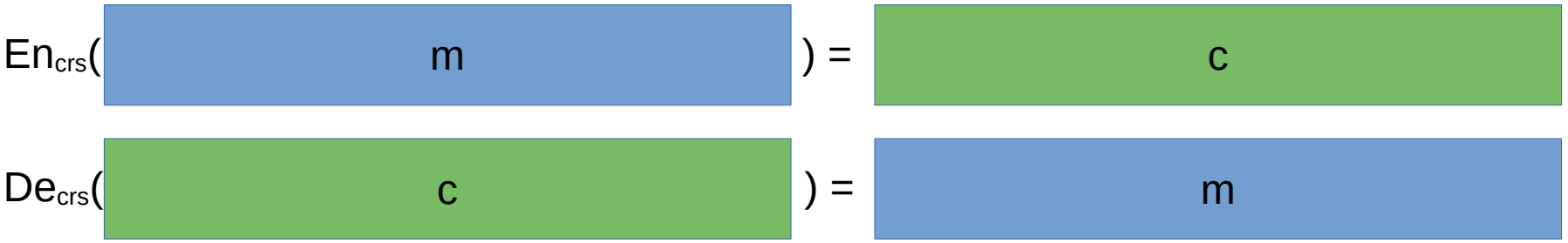
Naive Attempt #2



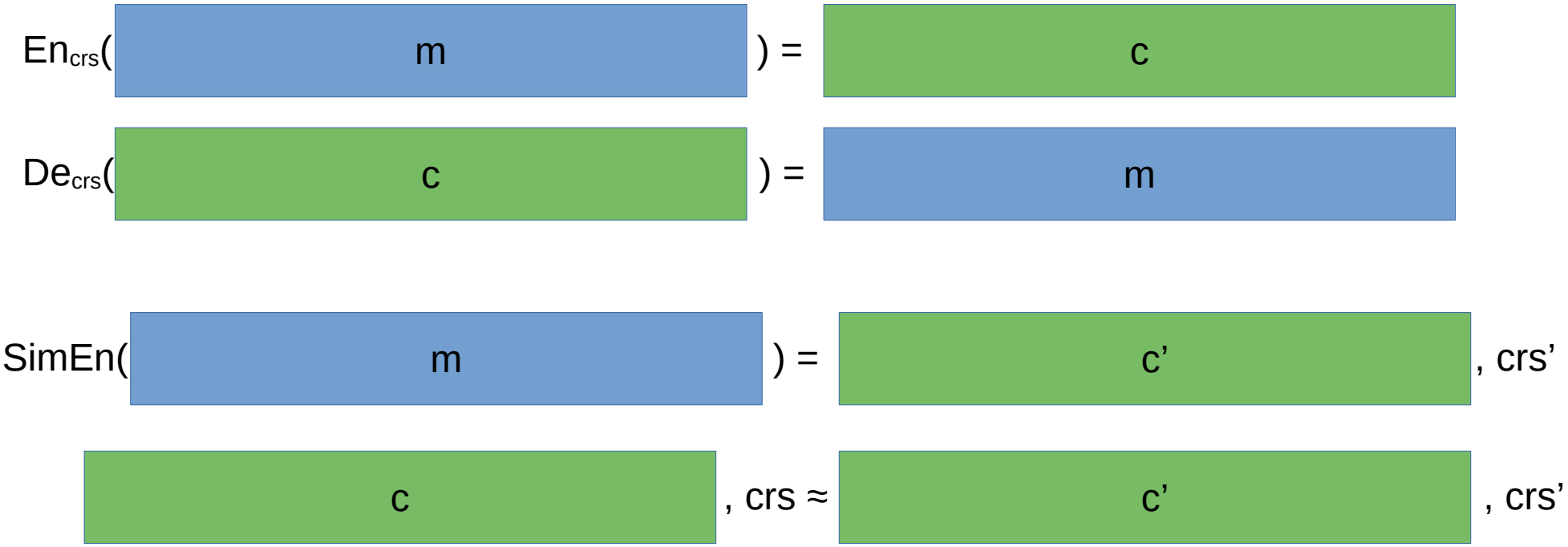
Entropic Encodings [DGO19,GLW20,MW20]



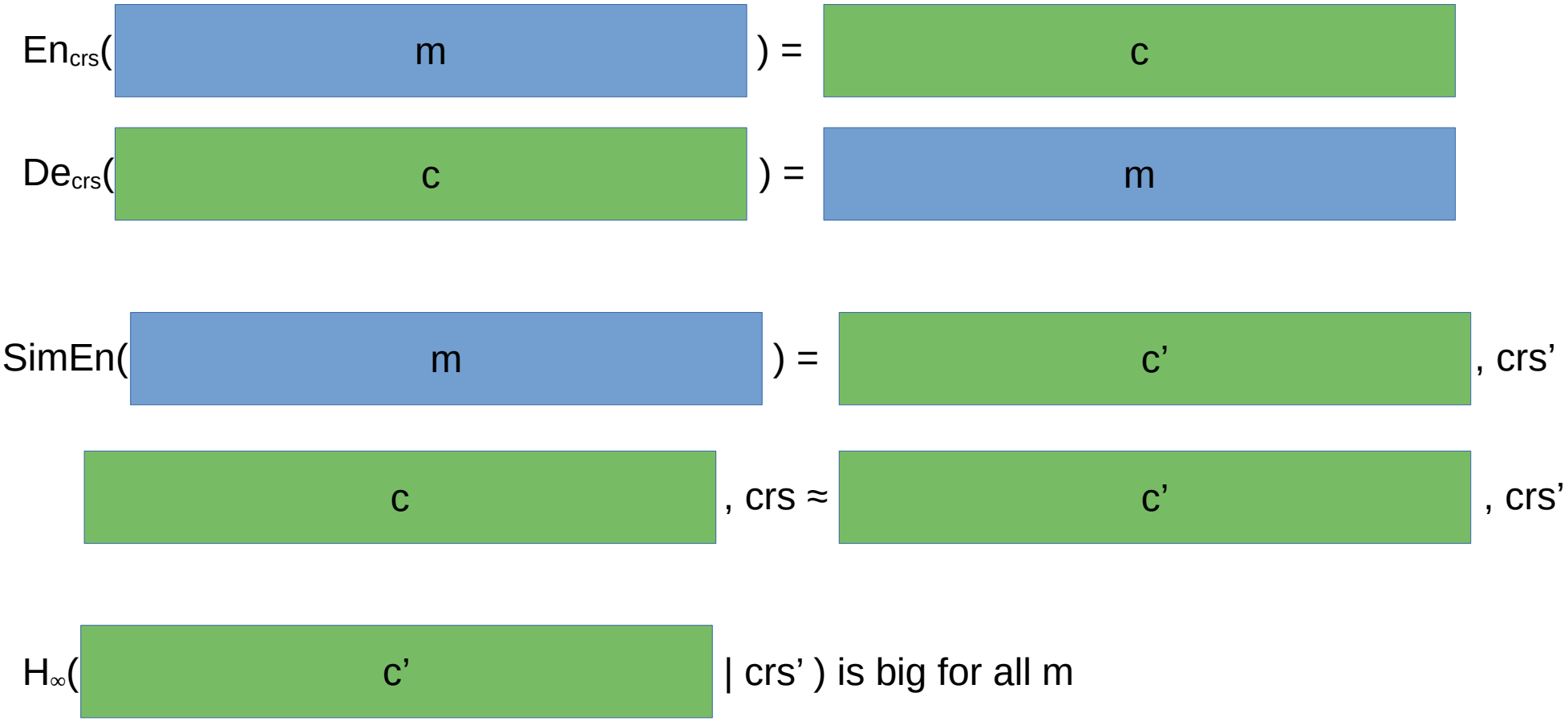
Entropic Encodings [DGO19,GLW20,MW20]



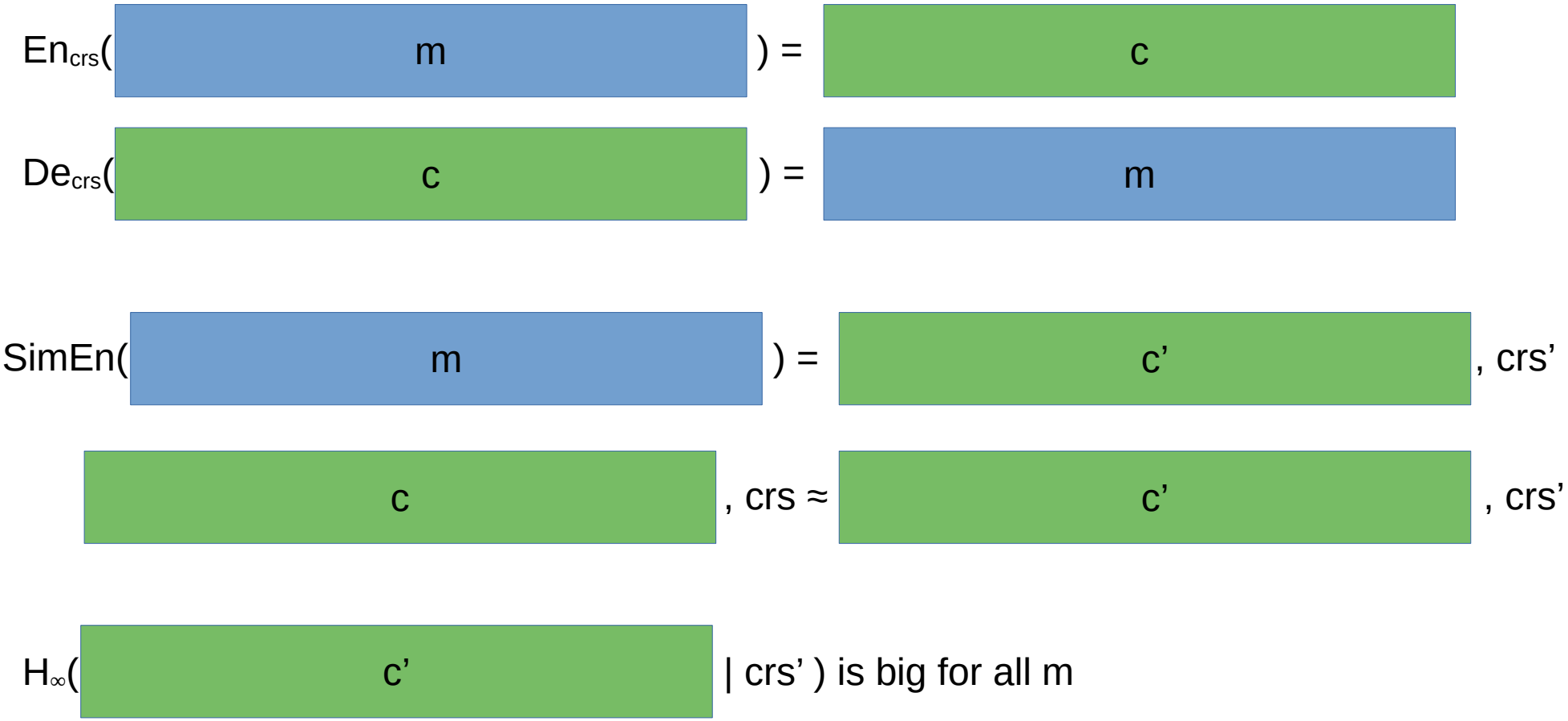
Entropic Encodings [DGO19,GLW20,MW20]



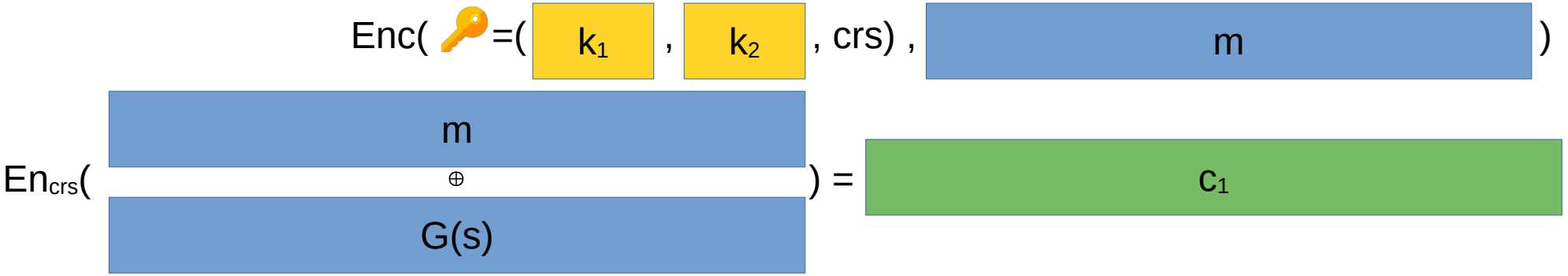
Entropic Encodings [DGO19,GLW20,MW20]



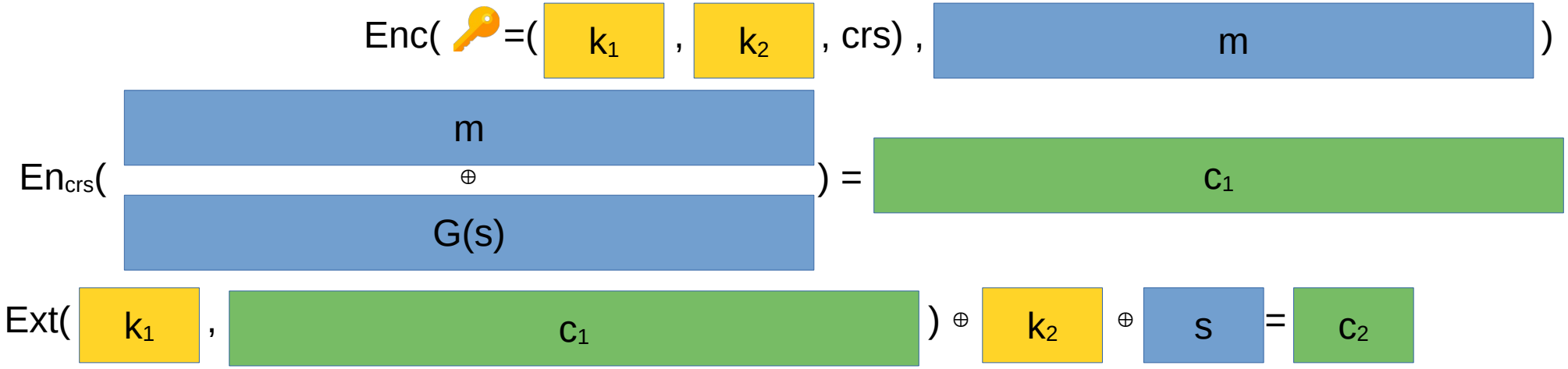
Entropic Encodings [DGO19,GLW20,MW20]



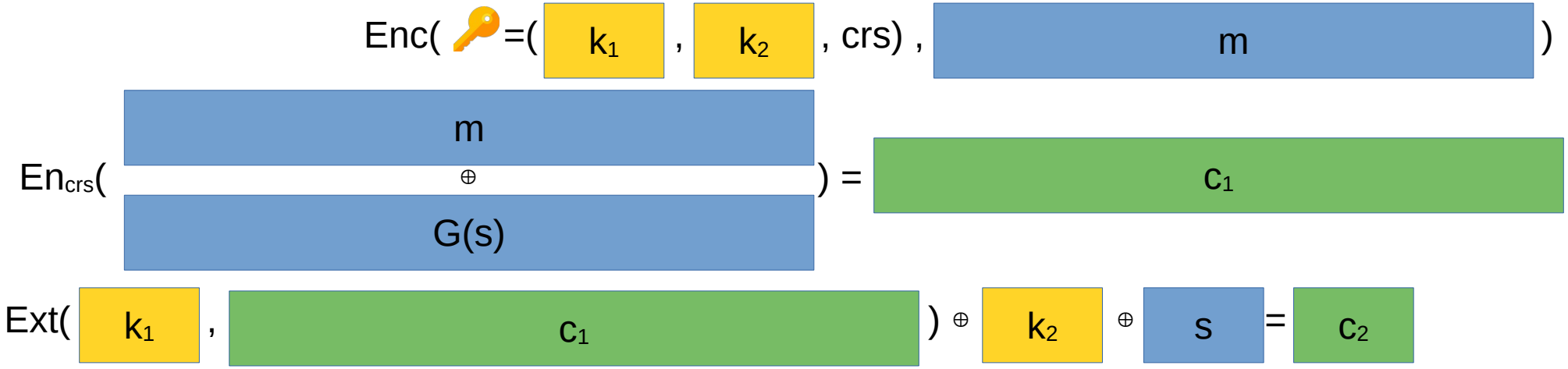
Construction

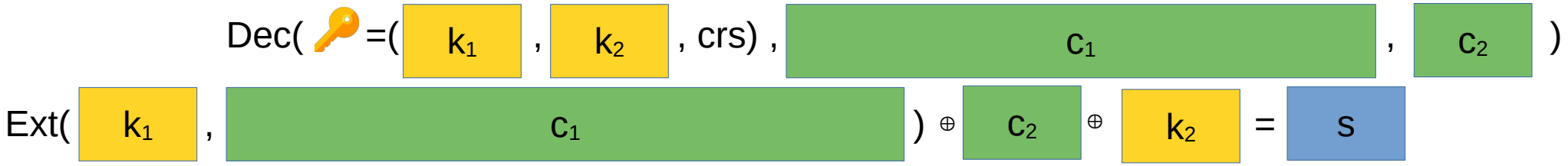


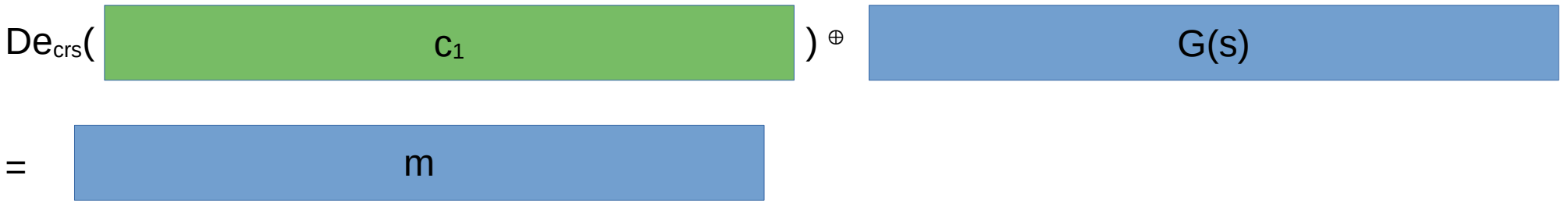
Construction



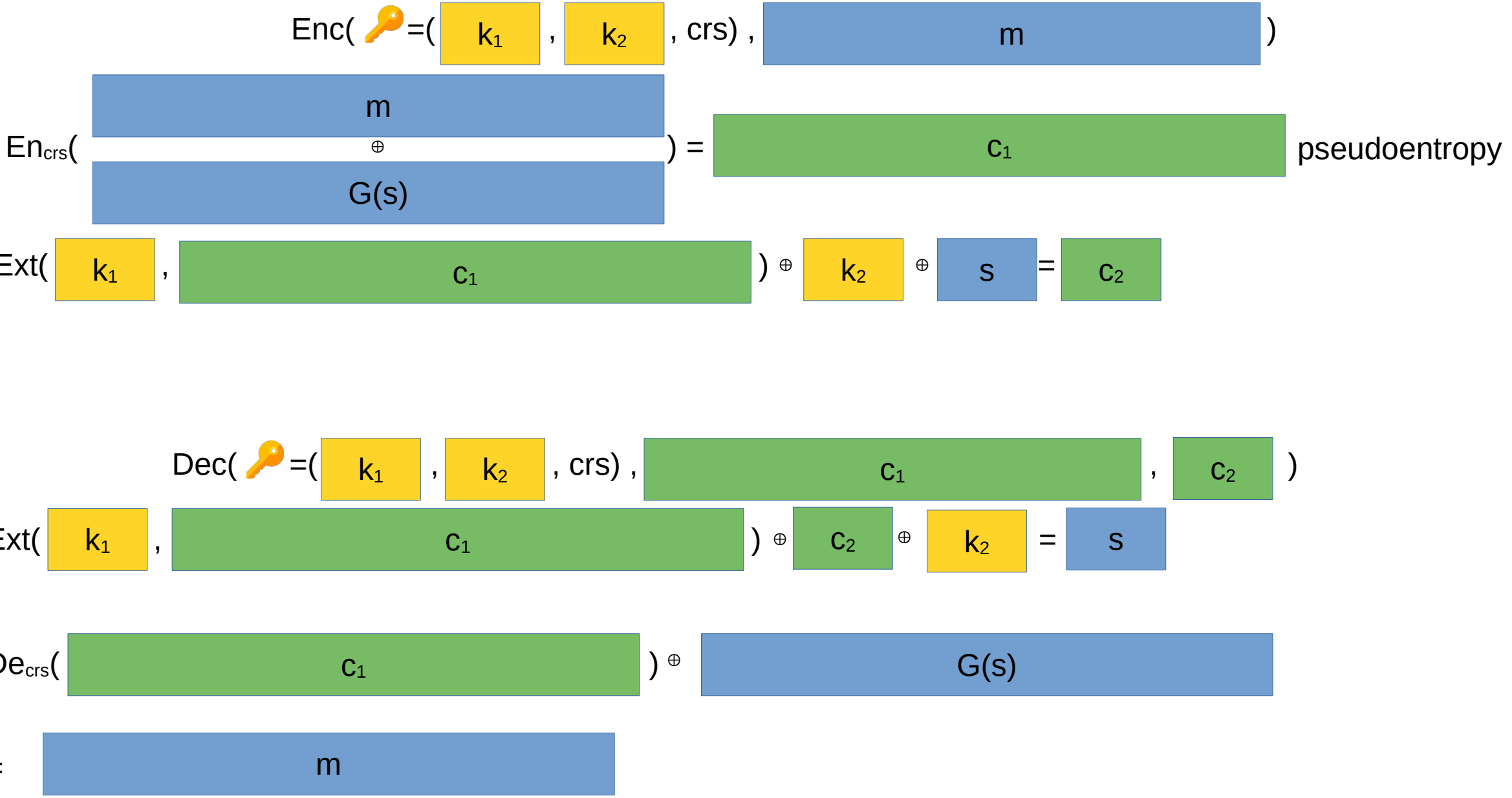
Construction



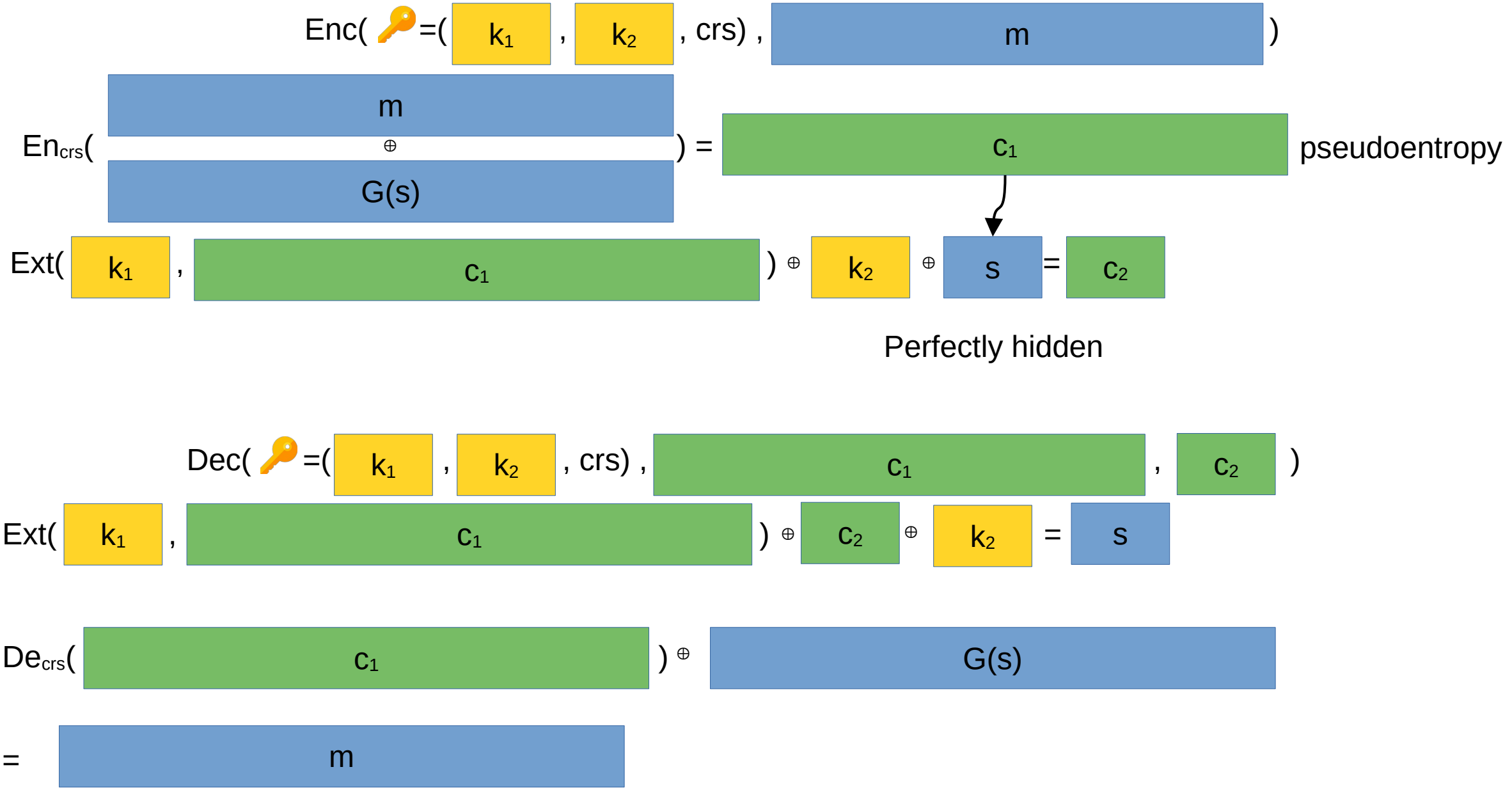




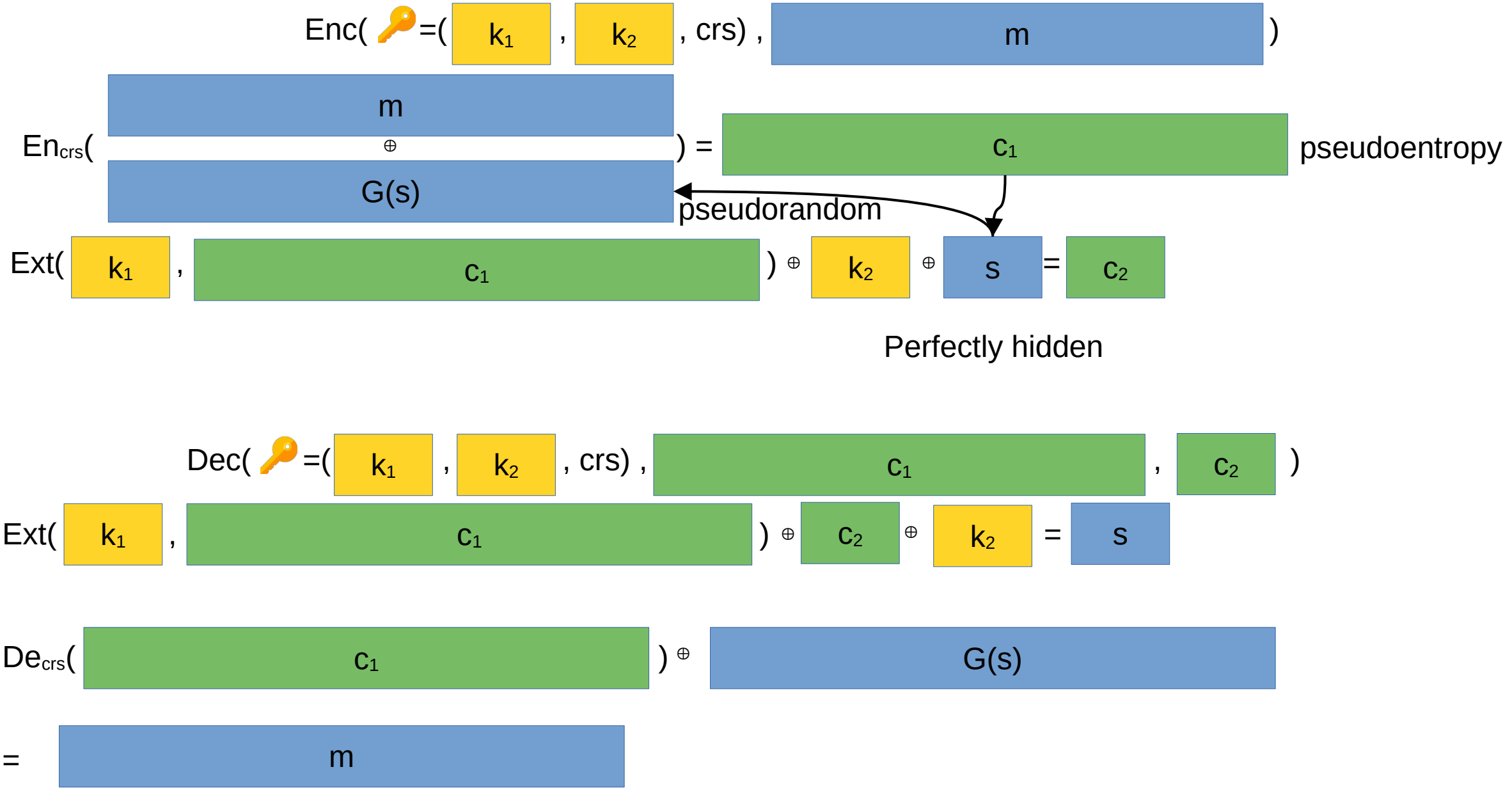
Construction



Construction



Construction



Main Result

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)

Main Result

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+poly(λ)
- Key length n+poly(λ) (dominated by crs)

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

Main Result

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

Main Result

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 $n\ \text{poly}(\lambda)$

Main Result

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