Simpler Analysis for Predicate Encryption

Shashank Agrawal

VISA Research

Melissa Chase

Microsoft Research

Predicate Encryption

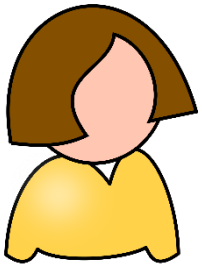
(with public index)

[BSW11]

Predicate Encryption

(with public index)

[BSW11]

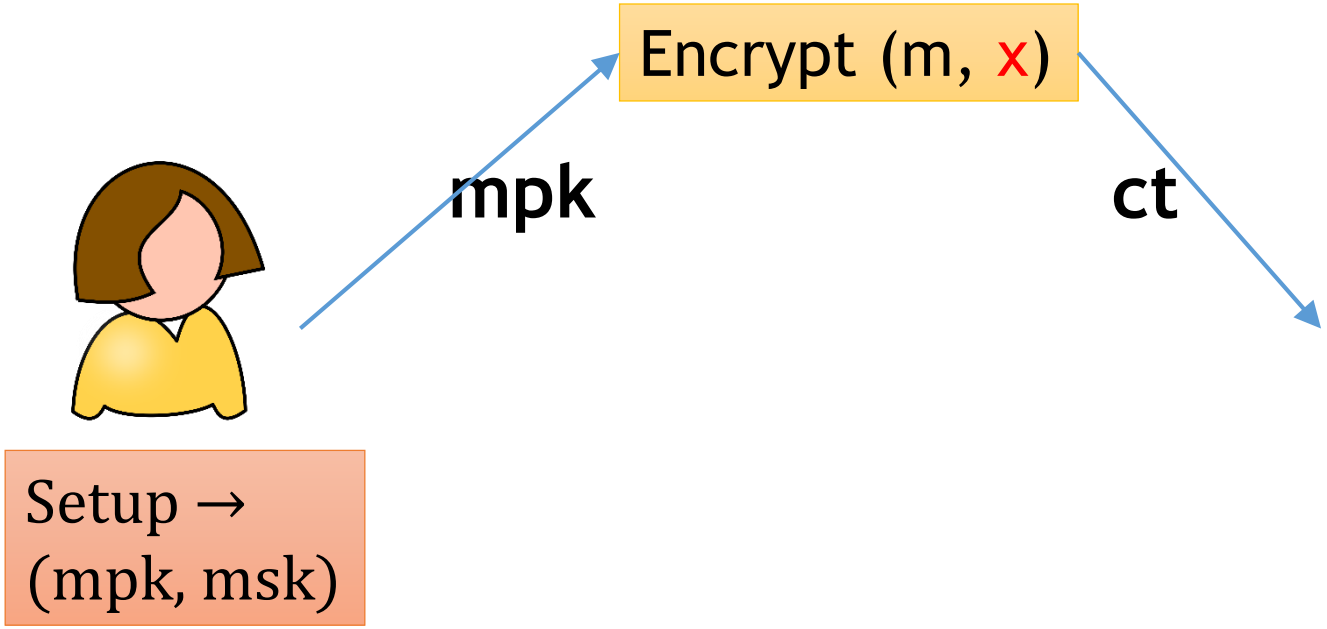


Setup → (mpk, msk)

Predicate Encryption

(with public index)

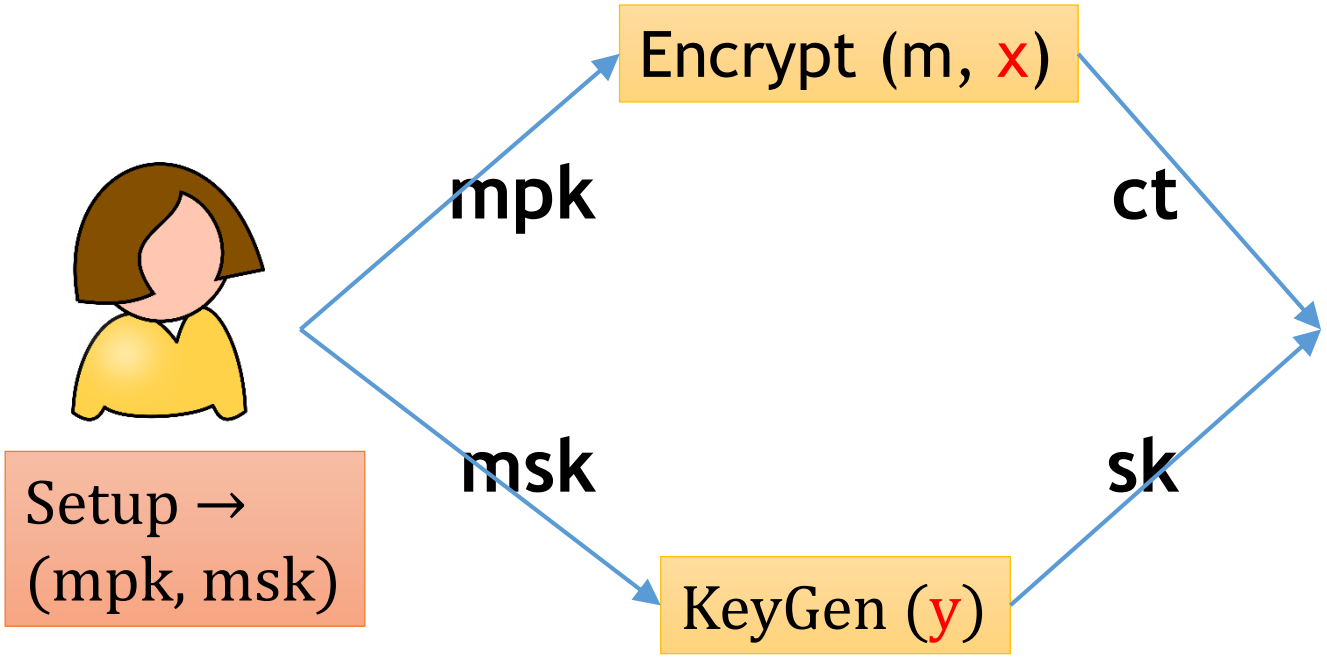
[BSW11]



Predicate Encryption

(with public index)

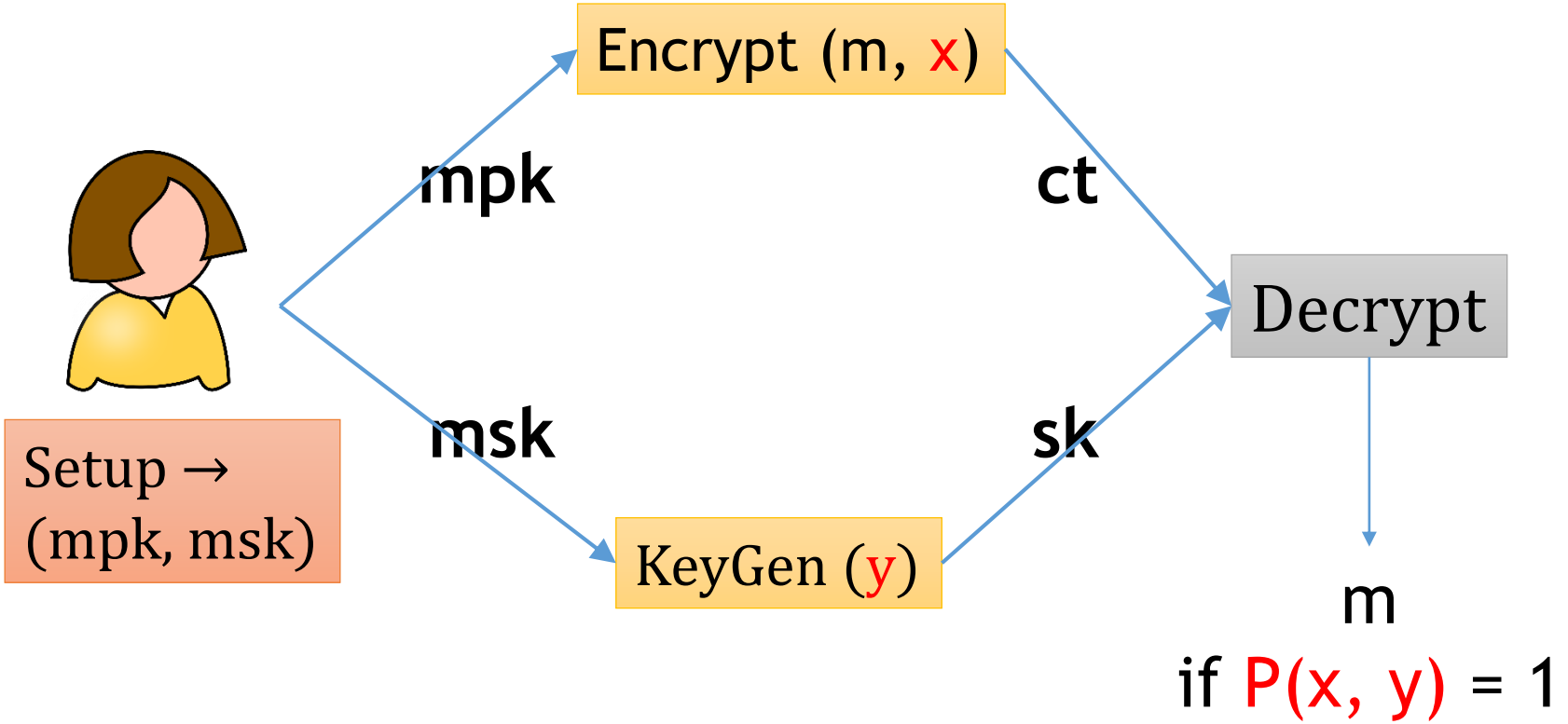
[BSW11]



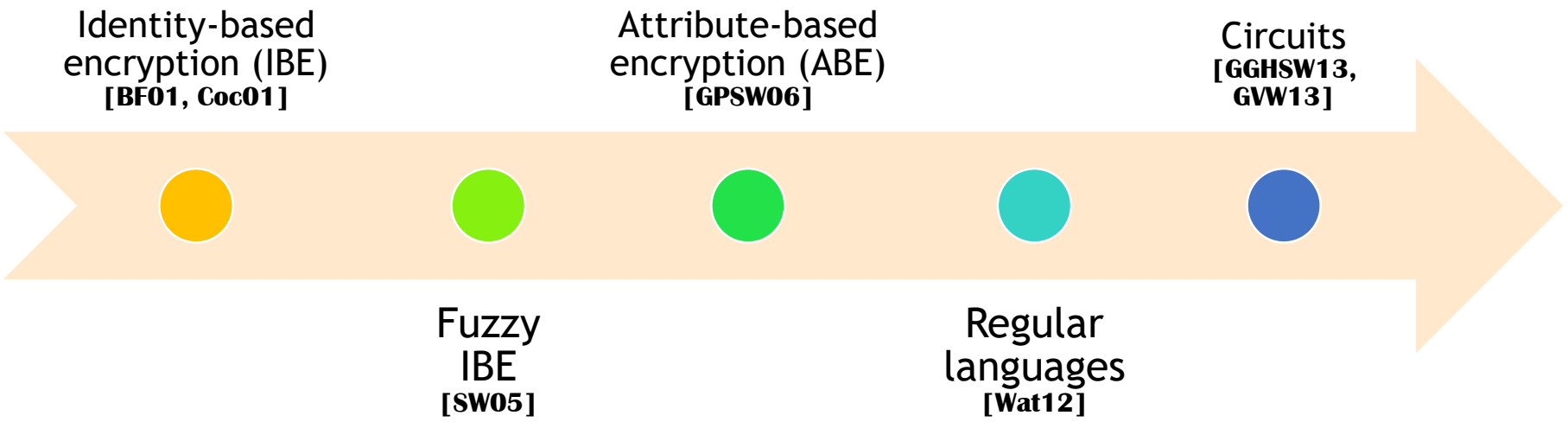
Predicate Encryption

(with public index)

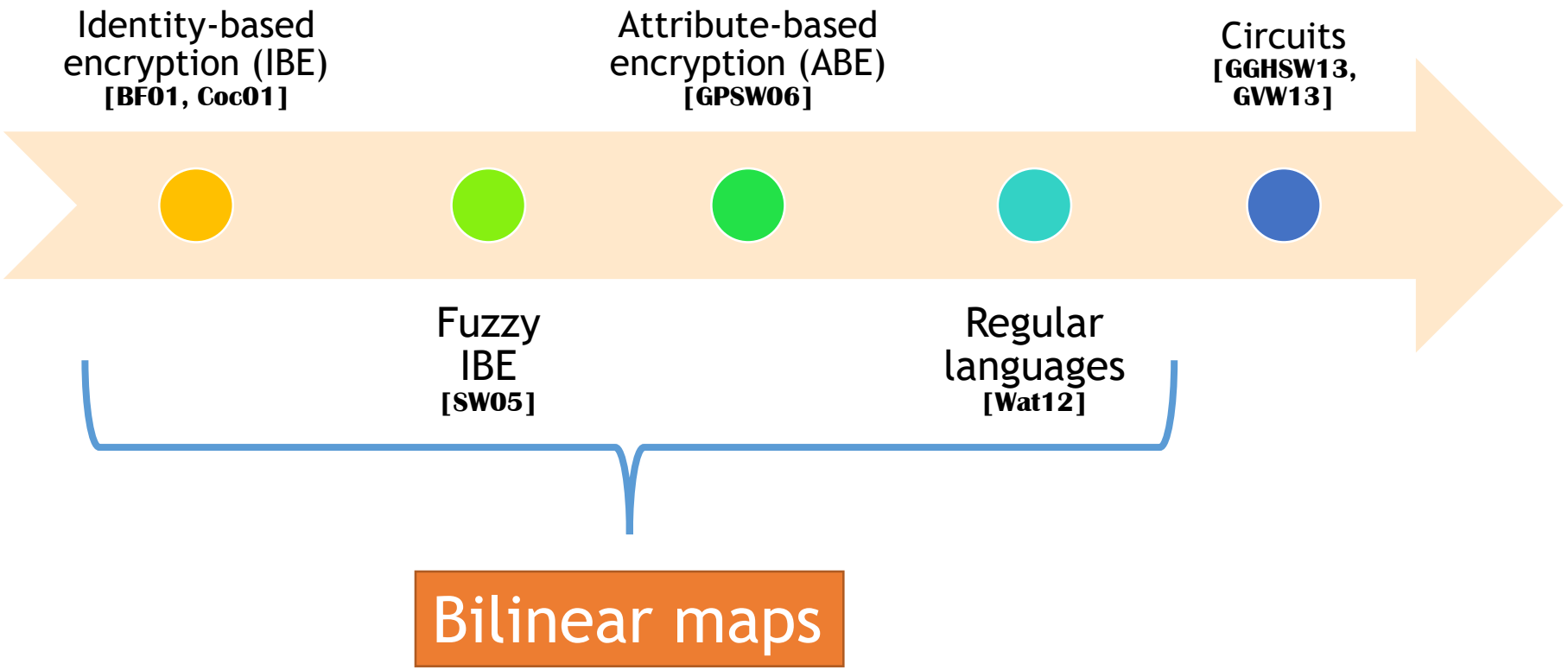
[BSW11]



A long way…


Identity-based encryption (IBE)
[BF01, Coc01]
Fuzzy IBE
[SW05]
Attribute-based encryption (ABE)
[GPSW06]
Regular languages
[Wat12]
Circuits
[GGHSW13, GVW13]

A long way…


Identity-based encryption (IBE)
[BF01, Coc01]
Attribute-based encryption (ABE)
[GPSW06]
Circuits
[GGHSW13, GVW13]
Fuzzy IBE
[SW05]
Regular languages
[Wat12]
Bilinear maps

Difficult task

Composite

Symmetric

Asymmetric

DBDH

DLIN

Subgroup decision

SXDH

DBDHI

q-BDHE

q-parallel BDHE

Projection

Canceling

Parameter-hiding

Dual system encryption

Pick a map

Pick an assumption

Many techniques

Central question:

Can we simplify design & analysis by identifying key properties?

Progress so far…

- Wee [W14] and Attrapadung [A14]
  - Chen et al. [CGW15], Attrapadung and Yamada [AY15] Agrawal and Chase [AC16], Attrapadung [A16]

Progress so far…

- Wee [W14] and Attrapadung [A14]
  - Chen et al. [CGW15], Attrapadung and Yamada [AY15] Agrawal and Chase [AC16], Attrapadung [A16]

Encode predicate P into simple polynomials

Progress so far…

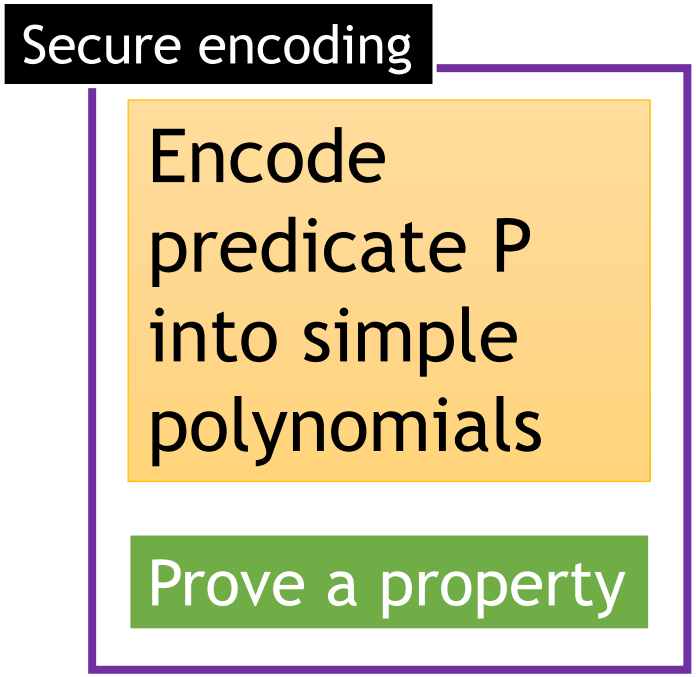
- Wee [W14] and Attrapadung [A14]
  - Chen et al. [CGW15], Attrapadung and Yamada [AY15] Agrawal and Chase [AC16], Attrapadung [A16]

Encode predicate P into simple polynomials

Prove a property

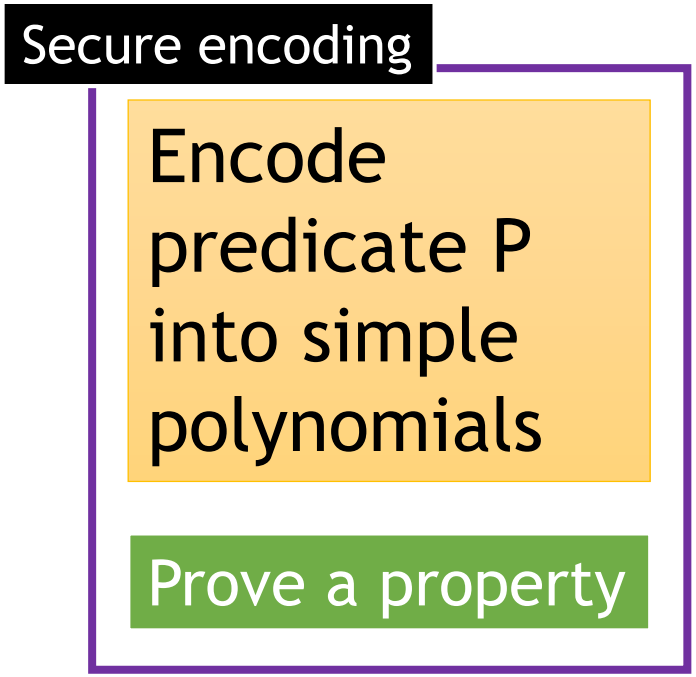
Progress so far…

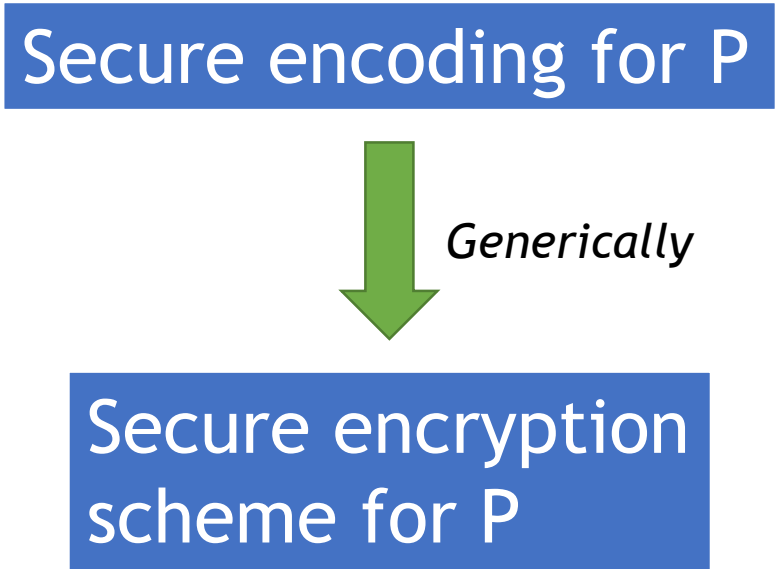
- Wee [W14] and Attrapadung [A14]
  - Chen et al. [CGW15], Attrapadung and Yamada [AY15] Agrawal and Chase [AC16], Attrapadung [A16]

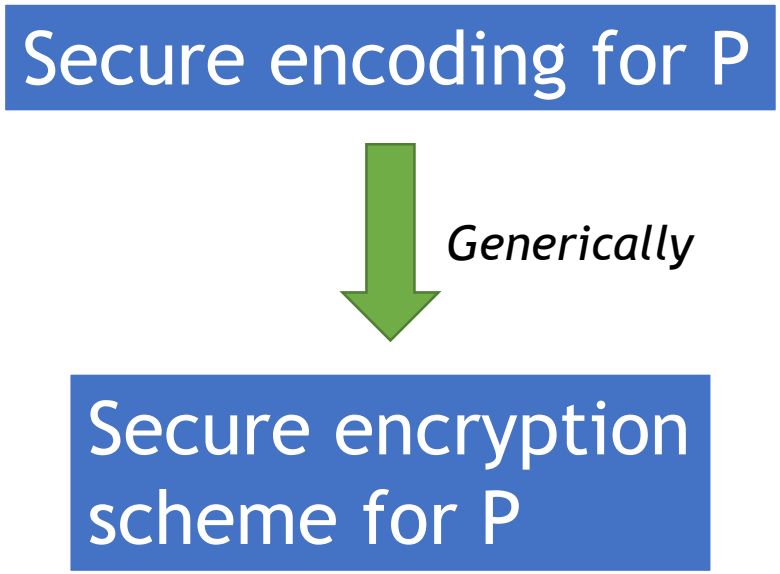


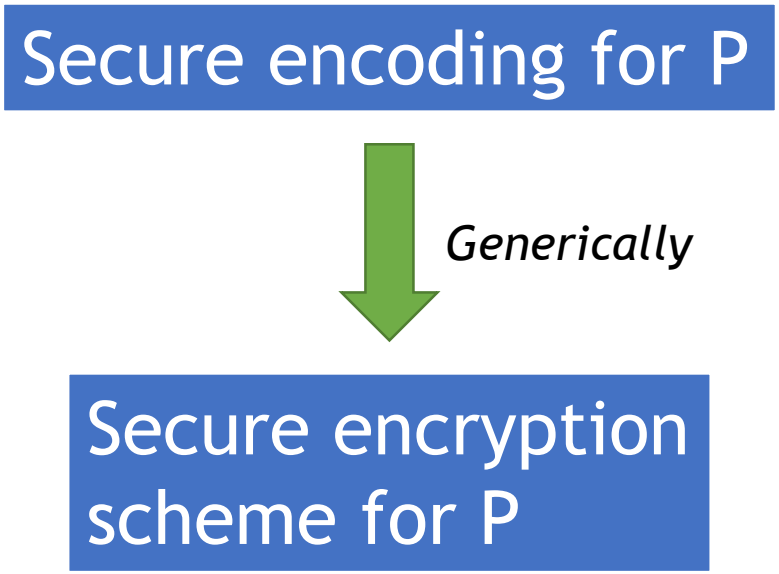
Progress so far…

- Wee [W14] and Attrapadung [A14]
  - Chen et al. [CGW15], Attrapadung and Yamada [AY15] Agrawal and Chase [AC16], Attrapadung [A16]

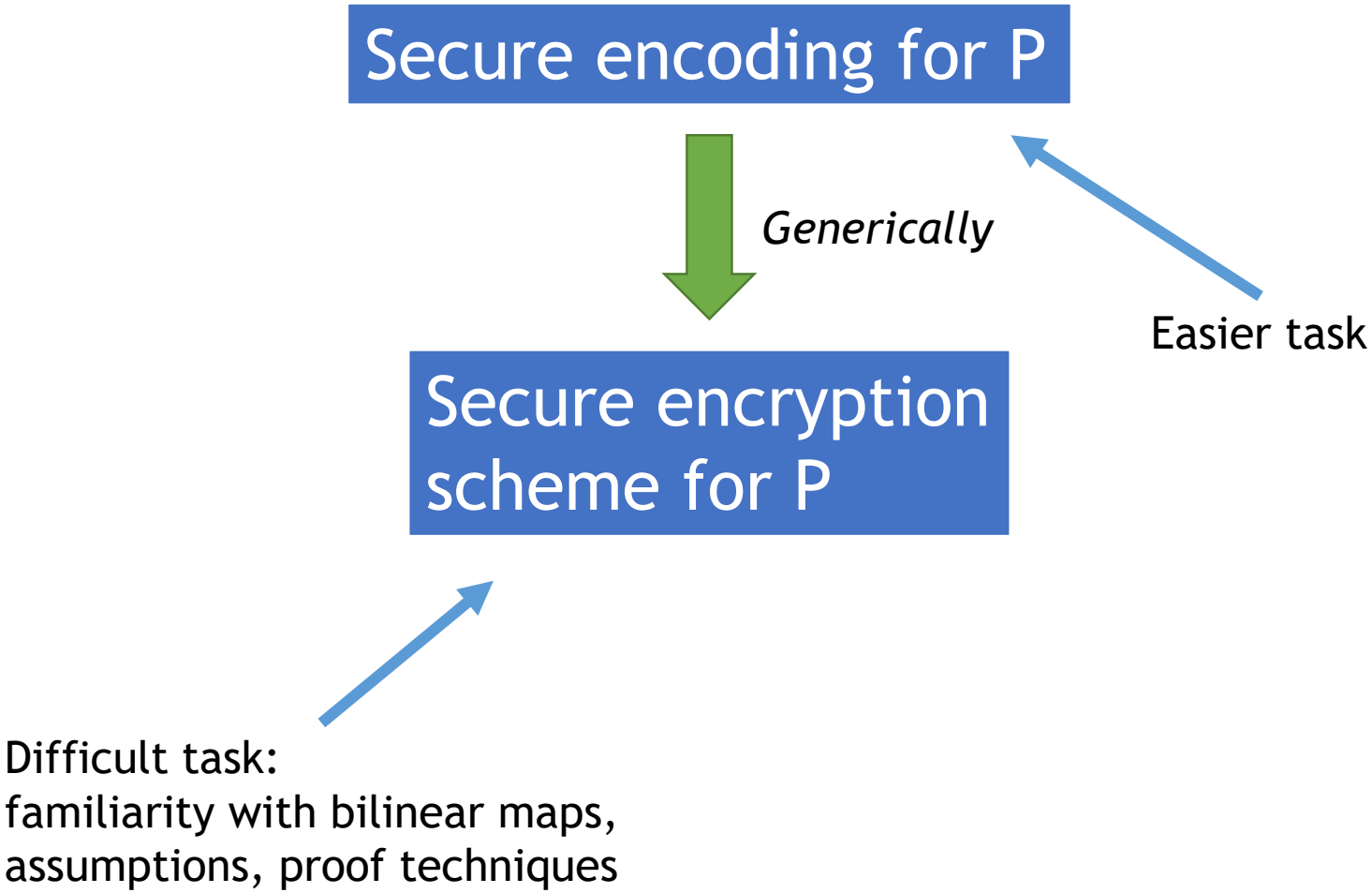


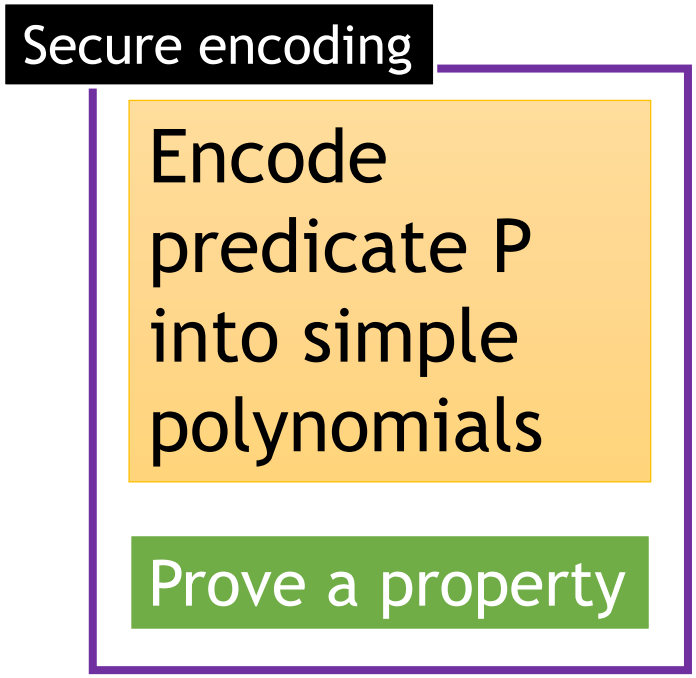


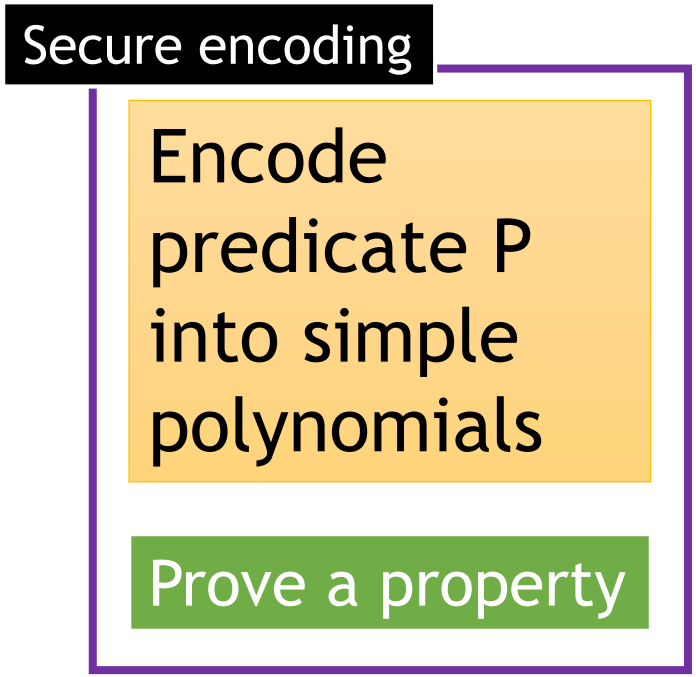

Secure encoding for P
Generically
Secure encryption scheme for P



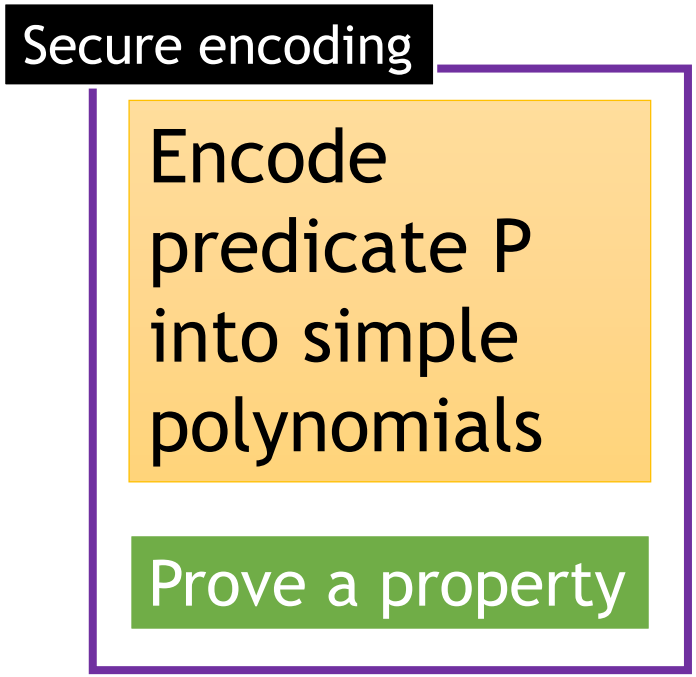
Difficult task:
familiarity with bilinear maps, assumptions, proof techniques


Secure encoding for P
Generically
Easier task
Secure encryption scheme for P
Difficult task:
familiarity with bilinear maps,
assumptions, proof techniques


Secure encoding
Encode predicate P into simple polynomials
Prove a property

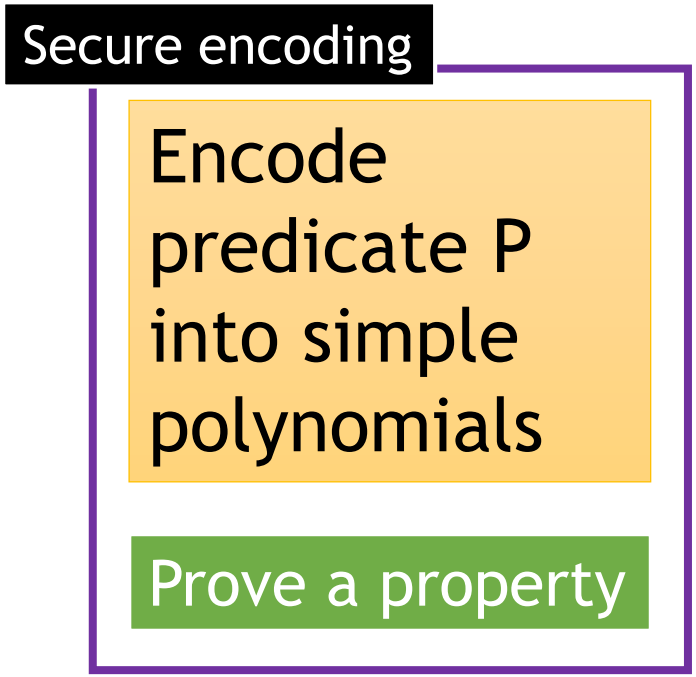


Design secure encoding:



Design secure encoding:

- Encoding exists?



Design secure encoding:

- Encoding exists?
- Proving property easy?

Design secure encoding:

- Encoding exists?
- Proving property easy?

Information-theoretic

[W14, A14, CGW15, AC16]

Computational

[A14, AY15, A16]

Design secure encoding:
- Encoding exists?
- Proving property easy?

Information-theoretic

[W14, A14, CGW15, AC16]

Good: Easy to use

Bad: No encoding known for many predicates

Computational

[A14, AY15, A16]

Design secure encoding:
- Encoding exists?
- Proving property easy?

Information-theoretic

[W14, A14, CGW15, AC16]

Good: Easy to use

Bad: No encoding known for many predicates

Computational

[A14, AY15, A16]

Good: Captures many predicates

Bad: Proofs are hard

Design secure encoding:
- Encoding exists?
- Proving property easy?

Information-theoretic

[W14, A14, CGW15, AC16]

Good: Easy to use

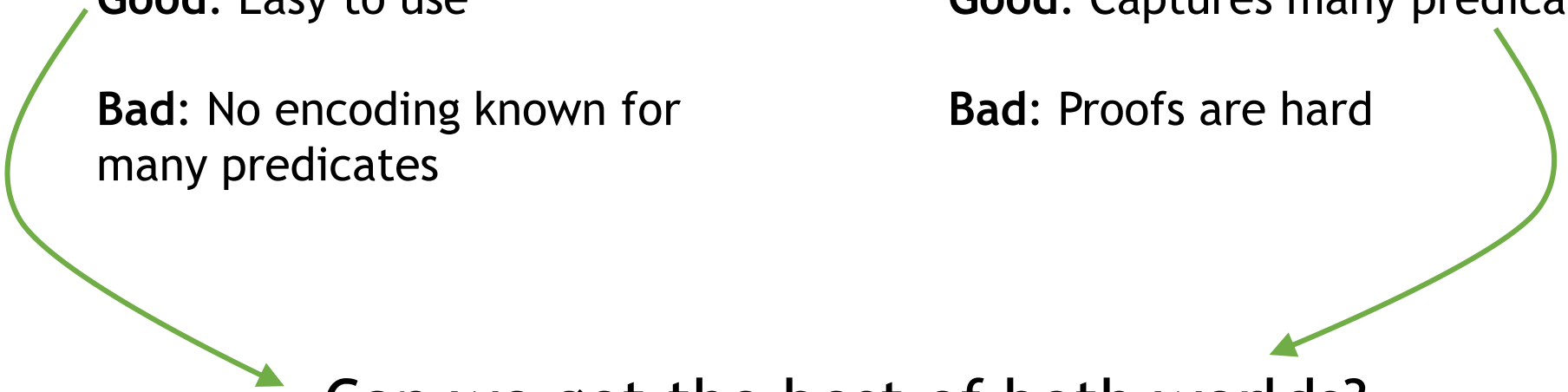
Bad: No encoding known for many predicates

Computational

[A14, AY15, A16]

Good: Captures many predicates

Bad: Proofs are hard



Can we get the best of both worlds?

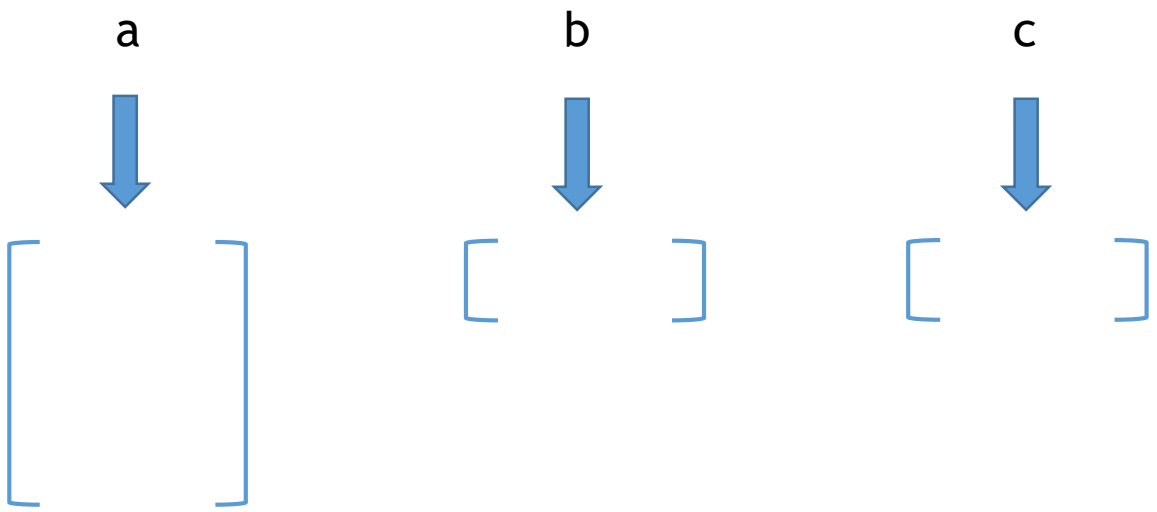
Symbolic property

Symbolic property

Variables in the encoding: a b c

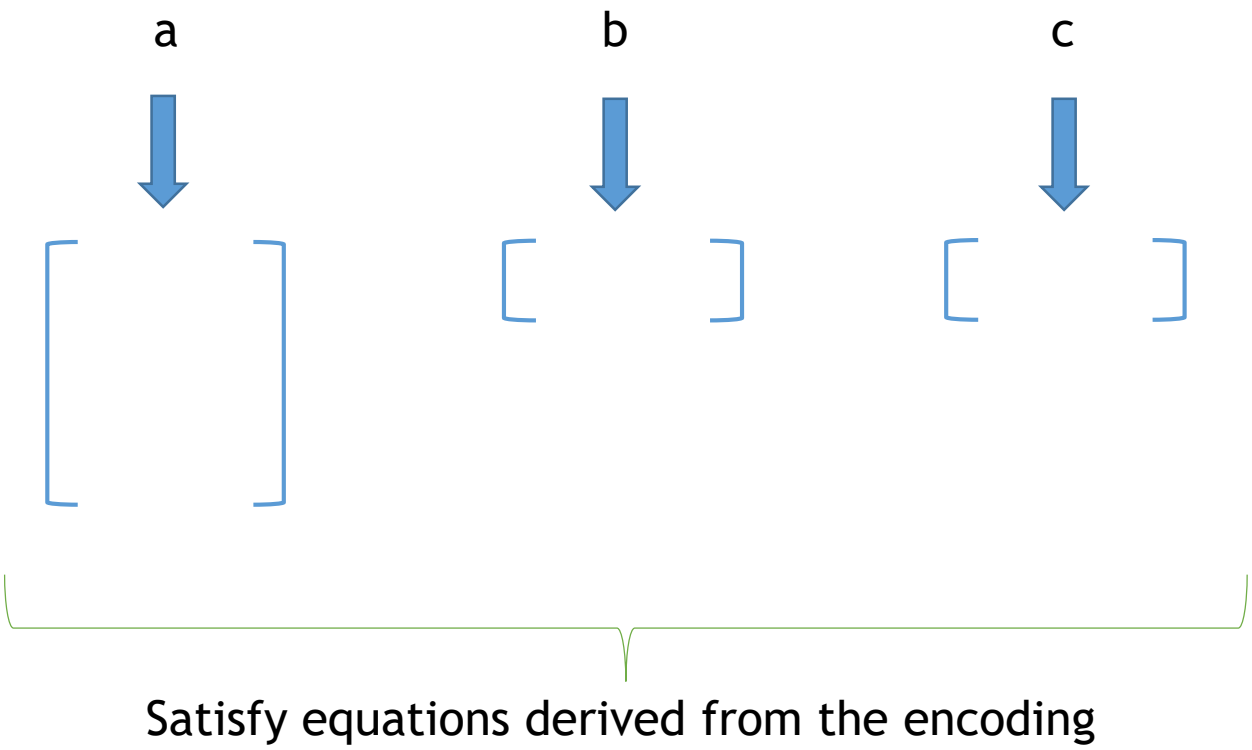
Symbolic property

Variables in the encoding:



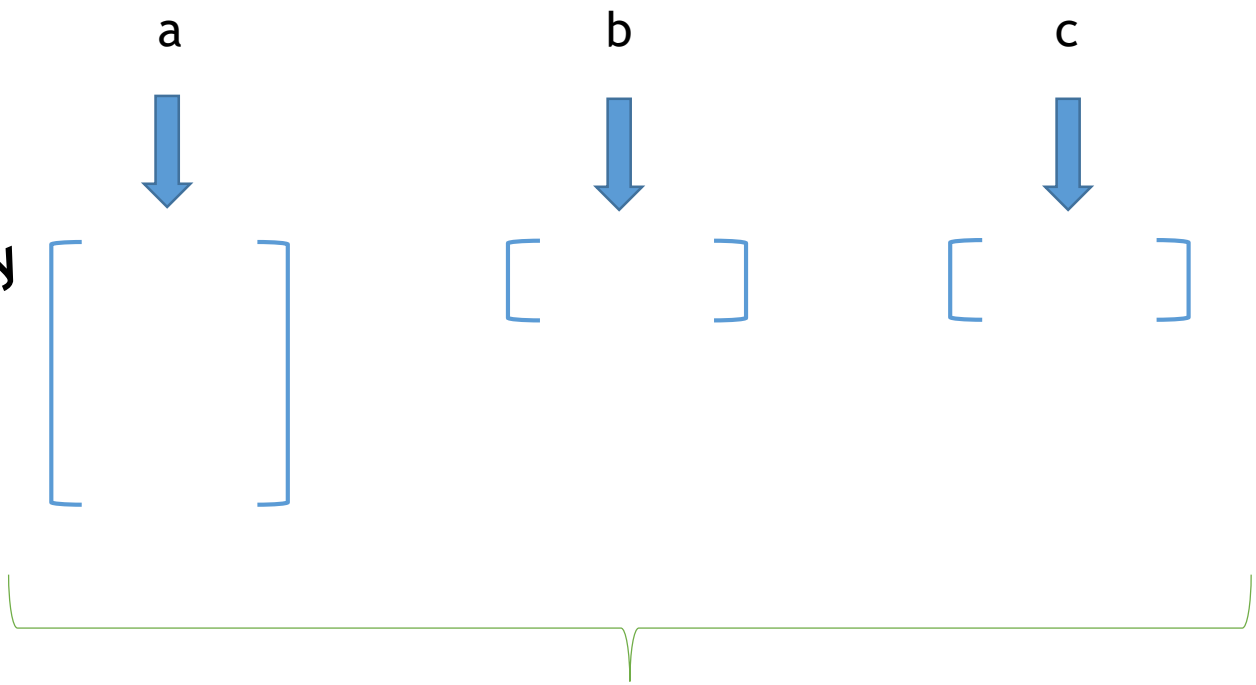
Symbolic property

Variables in the encoding:



Symbolic property

Variables in the encoding:

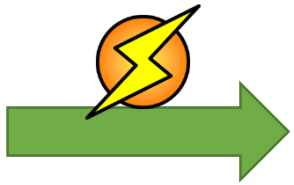


No indistinguishability of distributions!

For any predicate P

For any predicate P

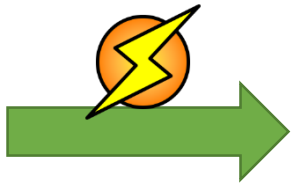
Encoding satisfies Symbolic property



Secure encryption scheme for P

For any predicate P

Encoding satisfies Symbolic property

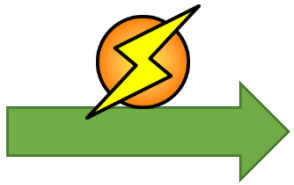


Secure encryption scheme for P

Under a fixed q-type assumption on Type-III pairings

For any predicate P

Encoding satisfies Symbolic property



Secure encryption scheme for P

Under a fixed q-type assumption on Type-III pairings

* Ciphertext-policy & key-policy ABE
  multi-use / short ciphertext / large universe

* Regular languages

Transformations

Transformations

Encoding  Compact encoding

Transformations

Encoding

Compact encoding

Encryption schemes with constant size ciphertexts/keys

Transformations

Encoding → Compact encoding

Encryption schemes with constant size ciphertexts/keys

Encoding for P → Encoding for dual P

Inherent property

Inherent property

Encoding not trivially broken

Encoding satisfies
Symbolic property!

Coming up:

- Encodings
- Symbolic property
- Why inherent?
- Open questions

Running example

Running example

- Lewko-Waters' IBE **[LW10]**
  - Ciphertexts & keys associated with identities
  - Decryption succeeds if identities match

Running example

- Lewko-Waters' IBE [LW10]
  - Ciphertexts & keys associated with identities
  - Decryption succeeds if identities match

- If IBE only concern
  - Use information-theoretic properties [W14, A14, CGW15, AC16]
  - Simple analysis, standard assumption

Running example

- Lewko-Waters' IBE [LW10]
  - Ciphertexts & keys associated with identities
  - Decryption succeeds if identities match

- If IBE only concern
  - Use information-theoretic properties [W14, A14, CGW15, AC16]
  - Simple analysis, standard assumption

- Symbolic property: much more, easily
  * Ciphertext-policy & key-policy ABE
    multi-use / short ciphertext / large universe
  * Regular languages

Encodings

Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha}\left(u^{ID'} h\right)^{r}$

Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha} \left(u^{ID'} h\right)^{r}$

g b 1 gg g b 1 b 1 bb b 1 1 b 1 g b 1 , g b 2 gg g b 2 b 2 bb b 2 2 b 2 g b 2 , ee g,g α g,g gg,gg g,g g,g α αα g,g α

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\, b_1 s + b_2 s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha} \left(u^{ID'} h\right)^{r}$

g b 1 gg g b 1 b 1 bb b 1 1 b 1 g b 1 , g b 2 gg g b 2 b 2 bb b 2 2 b 2 g b 2 , ee g,g α g,g gg,gg g,g g,g α αα g,g α

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\, b_1 s + b_2 s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha} \left(u^{ID'} h\right)^{r}$

$g\ \ b\ 1\ \ g g\ g\ \ b\ 1\ \ \ b\ 1\ b b\ b\ 1\ 1\ b\ 1\ g\ \ b\ 1\ ,$
$g\ \ b\ 2\ g g\ g\ \ b\ 2\ \ \ b\ 2\ b b\ b\ 2\ 2\ b\ 2\ g\ \ b\ 2\ , e e$
$g,g\ \ \alpha\ \ g,g\ g g,g g\ g,g\ \ \ g,g\ \ \alpha\ \alpha\alpha\ \ g,g\ \ \alpha$

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\ b_1 s + b_2 s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha} (u^{ID'} h)^{r}$

C 1 = g ID b 1 s + b 2 s gg g ID b 1 s + b 2 s IIDD b 1 bb b 1 1 b 1 ss + b 2 bb b 2 2 b 2 ss g ID b 1 s + b 2 s , C 2 CC C 2 2 C 2 = g s gg g s ss g s

C 0 =MM· e g,g α s e g,g α ee g,g α g,g gg,g g g,g g,g α αα g,g α e g,g α e g,g α s ss e g,g α s

g b 1 gg g b 1 b 1 bb b 1 1 b 1 g b 1 , g b 2 gg g b 2 b 2 bb b 2 2 b 2 g b 2 , ee g,g α g,g gg,gg g,g g,g α αα g,g α

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C\ 1\ 1\ 1 = g^{ID\ b_1 s + b_2 s}$, $C_2 = g^{s}$

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\ b_1 s + b_2 s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha} \left(u^{ID'} h\right)^{r}$

C 1 = g ID b 1 s + b 2 s gg g ID b 1 s + b 2 s IIDD b 1 bb b 1 1 b 1 ss + b 2 bb b 2 2 b 2 ss g ID b 1 s + b 2 s , C 2 CC C 2 2 C 2 = g s gg g s ss g s

C 0 =MM· e g,g α s e g,g α ee g,g α g,g gg,g g g,g g,g α αα g,g α e g,g α e g,g α s ss e g,g α s

g b 1 gg g b 1 b 1 bb b 1 1 b 1 g b 1 , g b 2 gg g b 2 b 2 bb b 2 2 b 2 g b 2 , ee g,g α g,g gg,gg g,g g,g α αα g,g α

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C\ 1\ 1\ 1 = g^{ID\ b_1 s + b_2 s}$, $C_2 = g^{s}$

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\ b_1 s + b_2 s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha} \left(u^{ID'} h\right)^{r}$

K 1 = g r gg g r rr g r , K 2 KK K 2 2 K 2 = g α + I D ′ b 1 r+ b 2 r gg g α + I D ′ b 1 r+ b 2 r αα + II D ′ DD D ′′ D ′ b 1 bb b 1 1 b 1 rr+ b 2 bb b 2 2 b 2 rr g α + I D ′ b 1 r+ b 2 r
C 1 = g ID b 1 s + b 2 s gg g ID b 1 s + b 2 s IIDD b 1 bb b 1 1 b 1 ss + b 2 bb b 2 2 b 2 ss g ID b 1 s + b 2 s , C 2 CC C 2 2 C 2 = g s gg g s ss g s
C 0 =MM· e g,g α s e g,g α ee g,g α g,g gg,gg g,g g, g α αα g,g α e g,g α e g,g α s ss e g,g α s
g b 1 gg g b 1 b 1 bb b 1 1 b 1 g b 1 , g b 2 gg g b 2 b 2 bb b 2 2 b 2 g b 2 , ee g,g α g,g gg,gg g,g g,g α αα g,g α

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C 1 1 1 = g^{ID\, b_1 s + b_2 s}$, $C_2 = g^{s}$

Secret key

$K 1 1 1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

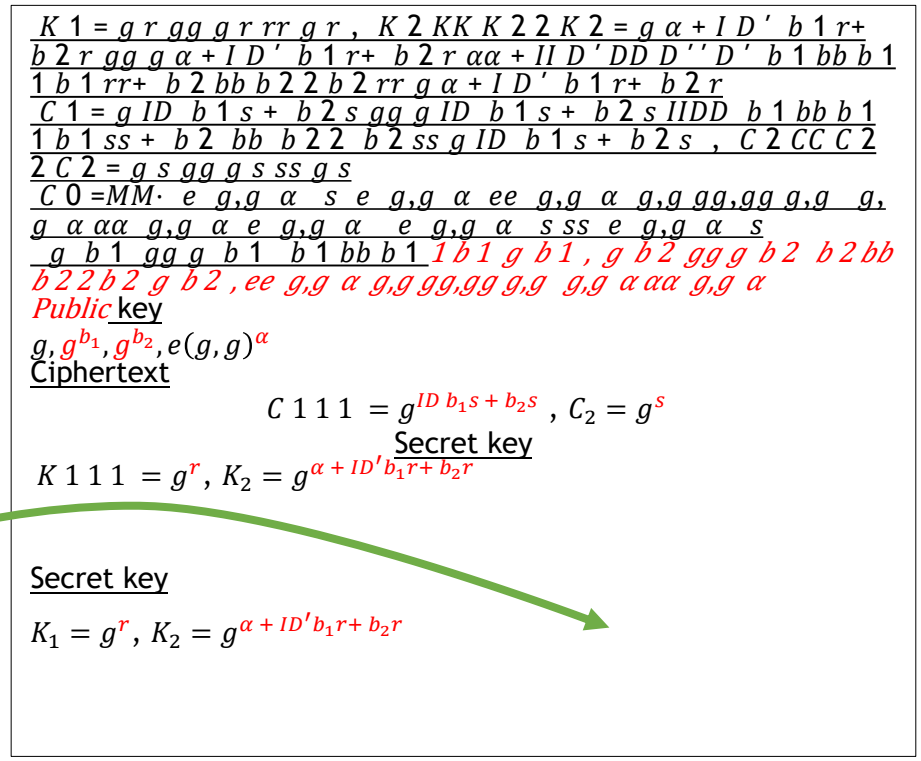
Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha} \left(u^{ID'} h\right)^{r}$



Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

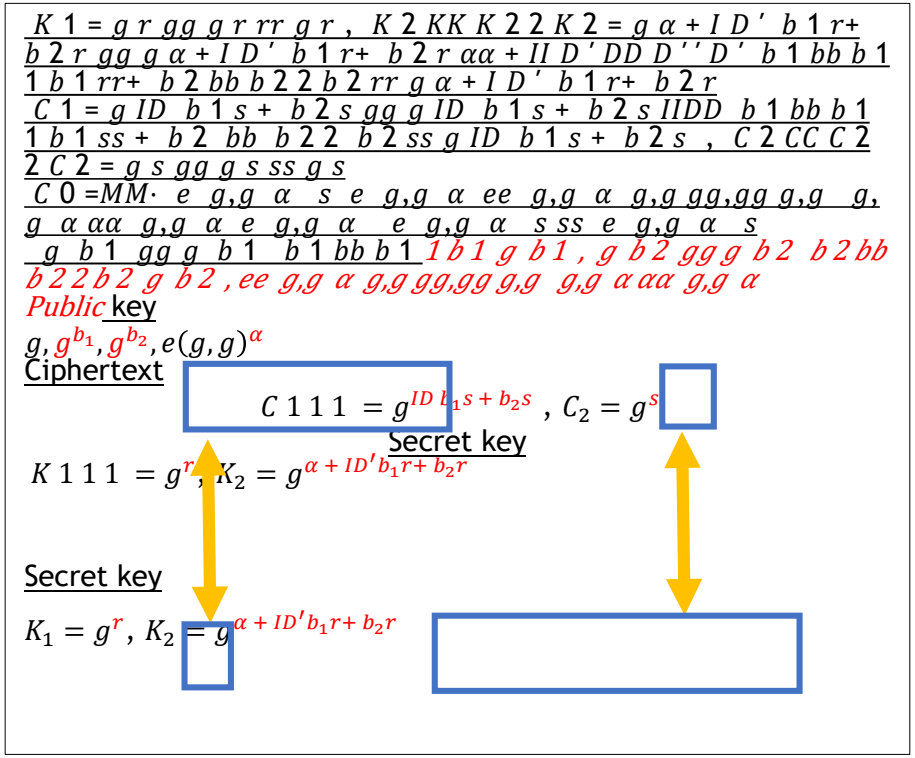
Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha} \left(u^{ID'} h\right)^{r}$



Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

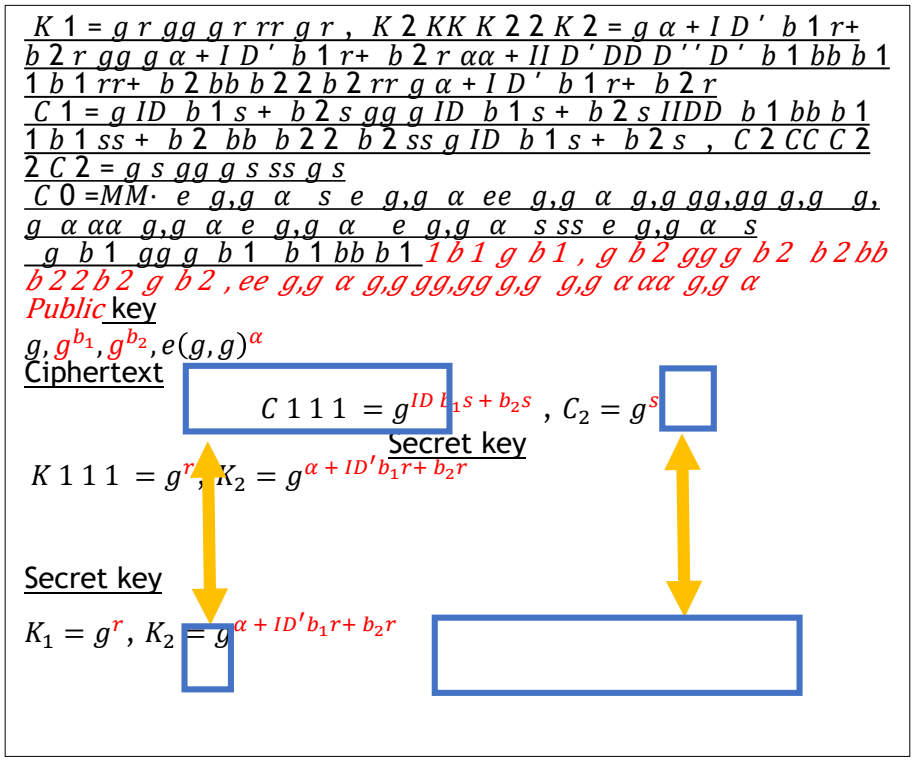
Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha} \left(u^{ID'} h\right)^{r}$



$$\alpha s + (ID' - ID)(b_2 - b_1) sr$$

Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

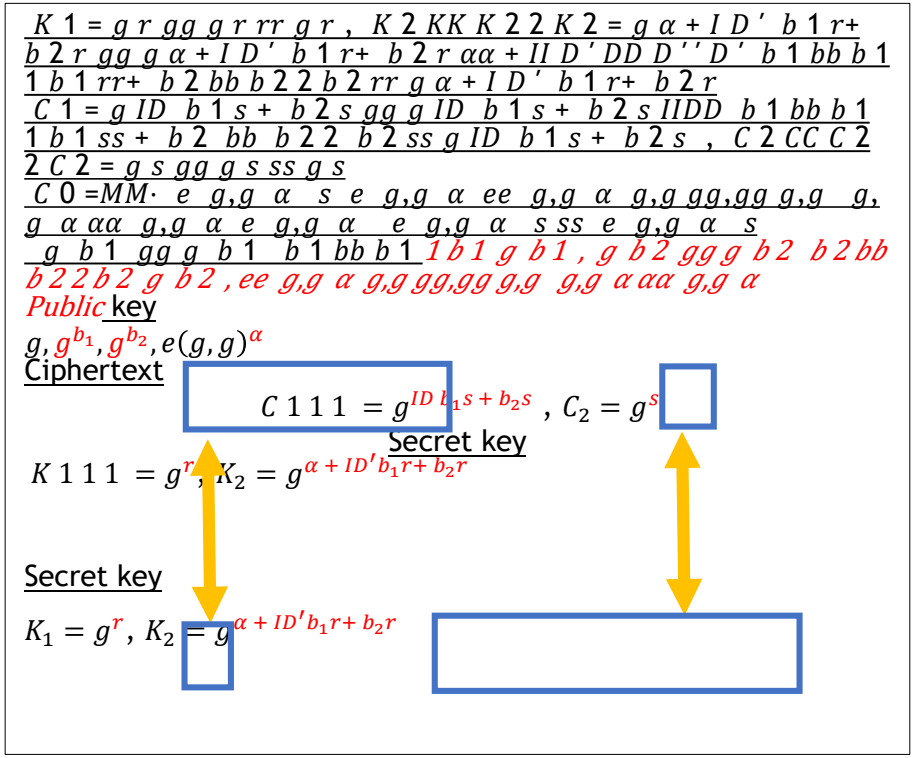
Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha} \left(u^{ID'} h\right)^{r}$



$$\alpha s + (ID' - ID)(b_2 - b_1)sr$$

$$ID' = ID: \quad \alpha s$$

Lewko-Waters' IBE

Public key

$g, u, h, e(g,g)^{\alpha}$

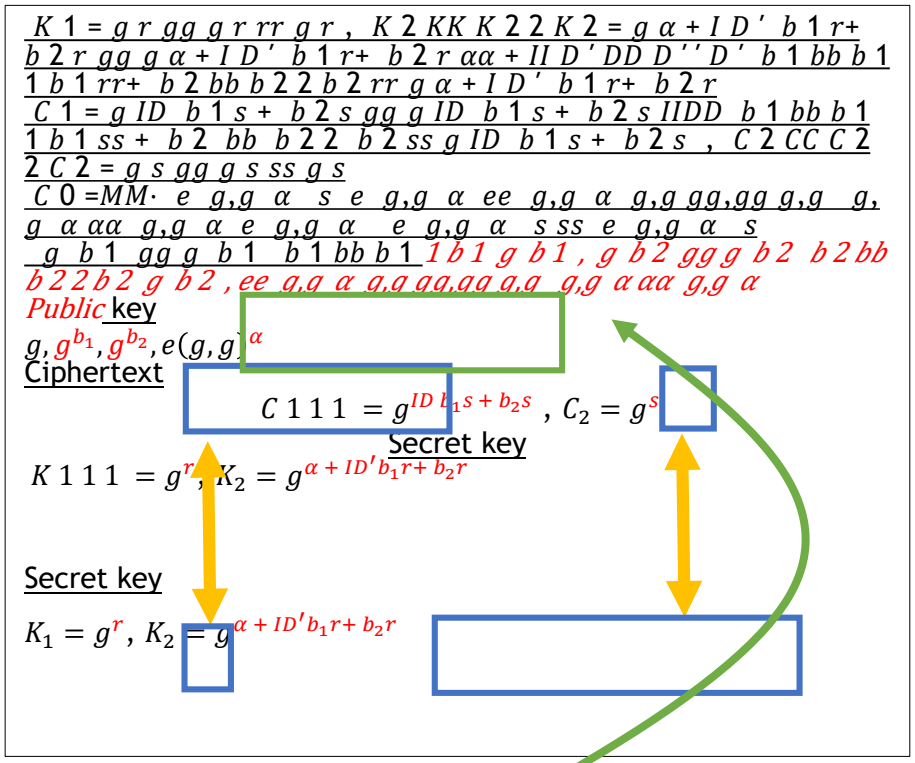
Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = (u^{ID} h)^{s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha} \left(u^{ID'} h\right)^{r}$



$\alpha s + (ID' - ID)(b_2 - b_1) sr$

$ID' = ID$: αs

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\ b_1 s + b_2 s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

[W14, Att14]

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\ b_1 s + b_2 s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Param

b_1, b_2

Enc-CT

$ID\ b_1 s + b_2 s, \quad s$

Enc-Key

$r, \quad \alpha + ID' b_1 r + b_2 r$

[W14, Att14]

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\ b_1 s + b_2 s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Param

b_1, b_2

Enc-CT

$ID\ b_1 s + b_2 s, \quad s$

Enc-Key

$r, \quad \alpha + ID' b_1 r + b_2 r$

Variables: b_1, b_2 s α, r

[W14, Att14]

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\ b_1 s + b_2 s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Param

b_1, b_2

Enc-CT

$ID\ b_1 s + b_2 s, \quad s$

Enc-Key

$r, \quad \alpha + ID' b_1 r + b_2 r$

Variables: b_1, b_2 s α, r

Common

[W14, Att14]

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\ b_1 s + b_2 s}$, $C_2 = g^{s}$

Secret key

$K_1 = g^{r}$, $K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Param

b_1, b_2

Enc-CT

$ID\ b_1 s + b_2 s, \quad s$

Enc-Key

$r, \quad \alpha + ID' b_1 r + b_2 r$

Variables: b_1, b_2 s α, r

Polynomials: $ID\ b_1 s + b_2 s,$ $\alpha + ID' b_1 r + b_2 r$

[W14, Att14]

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\ b_1 s + b_2 s}\ ,\ C_2 = g^{s}$

Secret key

$K_1 = g^{r},\ K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Param

b_1, b_2

Enc-CT

$ID\ b_1 s + b_2 s, \qquad s$

Enc-Key

$r, \quad \alpha + ID' b_1 r + b_2 r$

Variables: b_1, b_2 s α, r

Polynomials: $ID\ b_1 s + b_2 s,$ $\alpha + ID' b_1 r + b_2 r$

Correctness: P(x, y) = 1 ⇒ Recover αs

[W14, Att14]

Public key

$g, g^{b_1}, g^{b_2}, e(g,g)^{\alpha}$

Ciphertext

$C_0 = M \cdot (e(g,g)^{\alpha})^{s}$

$C_1 = g^{ID\ b_1 s + b_2 s}\ ,\ C_2 = g^{s}$

Secret key

$K_1 = g^{r}\ ,\ K_2 = g^{\alpha + ID' b_1 r + b_2 r}$

Param

b_1, b_2

Enc-CT

$ID\ b_1 s + b_2 s, \quad s$

Enc-Key

$r, \quad \alpha + ID' b_1 r + b_2 r$

Variables: b_1, b_2 s α, r

Polynomials: $ID\ b_1 s + b_2 s,$ $\alpha + ID' b_1 r + b_2 r$

Correctness: P(x, y) = 1 ⇒ Recover αs α, s special variables

Security

Security

Param

b_1, b_2

Enc-CT

$ID\ b_1 s + b_2 s,\ \ s$

Enc-Key

$r,\ \alpha + ID' b_1 r + b_2 r$

- Correct encoding scheme

Security

Param

b_1, b_2

Enc-CT

$ID\ b_1 s + b_2 s,\ \ s$

Enc-Key

$r,\ \alpha + ID' b_1 r + b_2 r$

- Correct encoding scheme
- Doesn't matter where it came from

Security

Param

b_1, b_2

Enc-CT

$ID\ b_1 s + b_2 s,\ \ s$

Enc-Key

$r,\ \alpha + ID' b_1 r + b_2 r$

- Co⇒ Fully secure encryption
- Doesn't matter where it came from
- Some property when P(x, y) = 0

  Fully secure encryptio

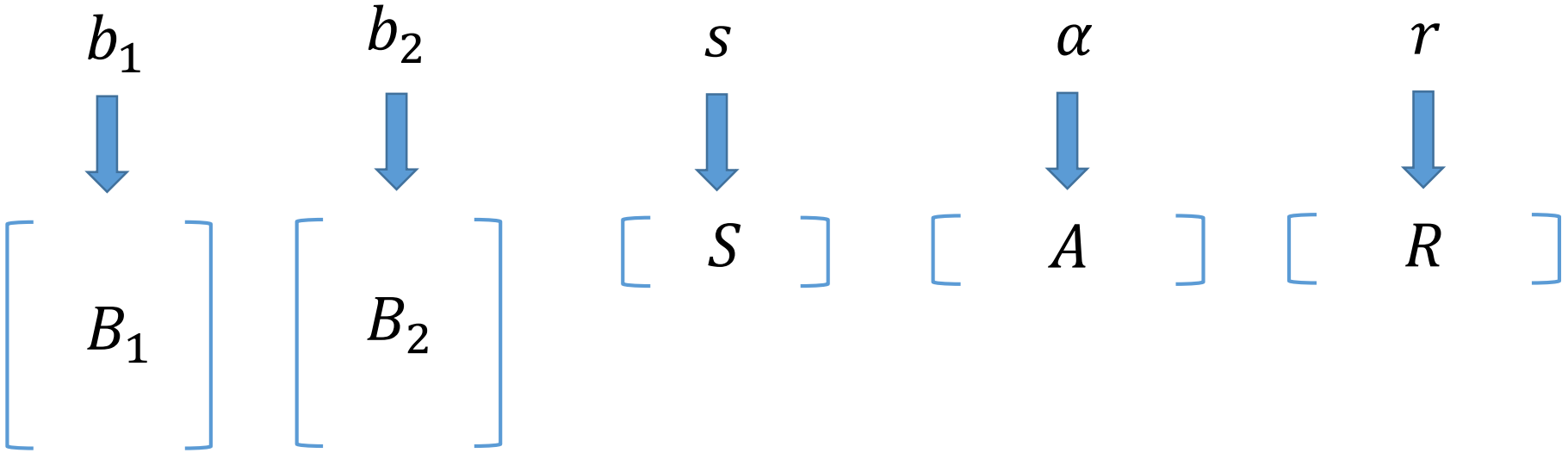
Symbolic property

Symbolic property

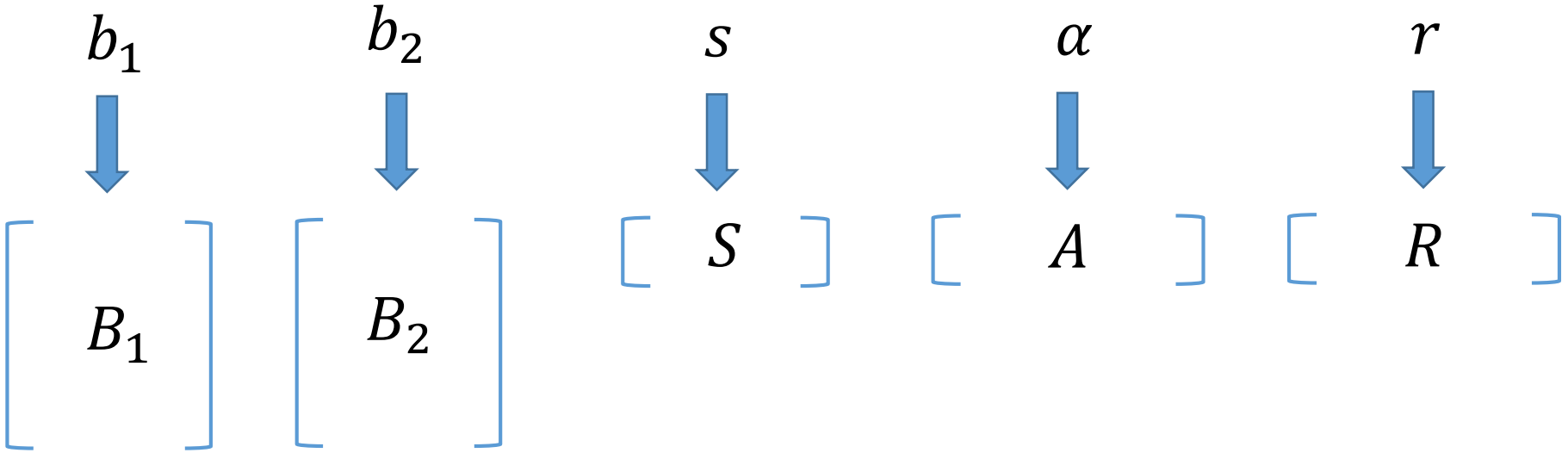
Symbolic property

b_1 b_2 s α r

Symbolic property

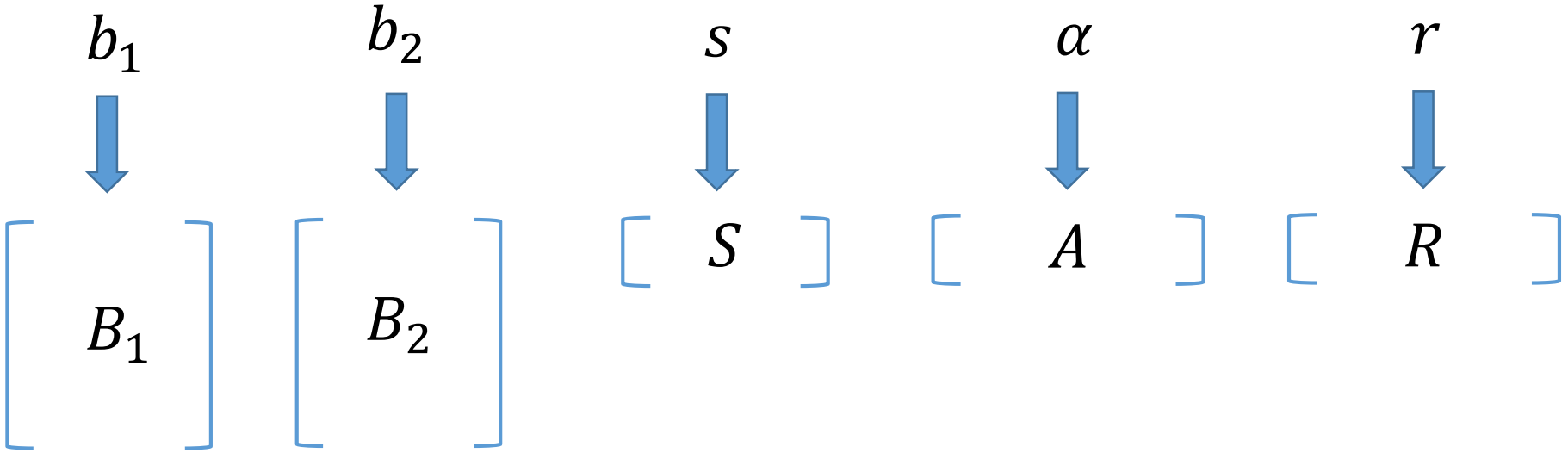


Symbolic property



Polynomials: $ID\ b_1 s + b_2 s,$ $\alpha + ID' b_1 r + b_2 r$

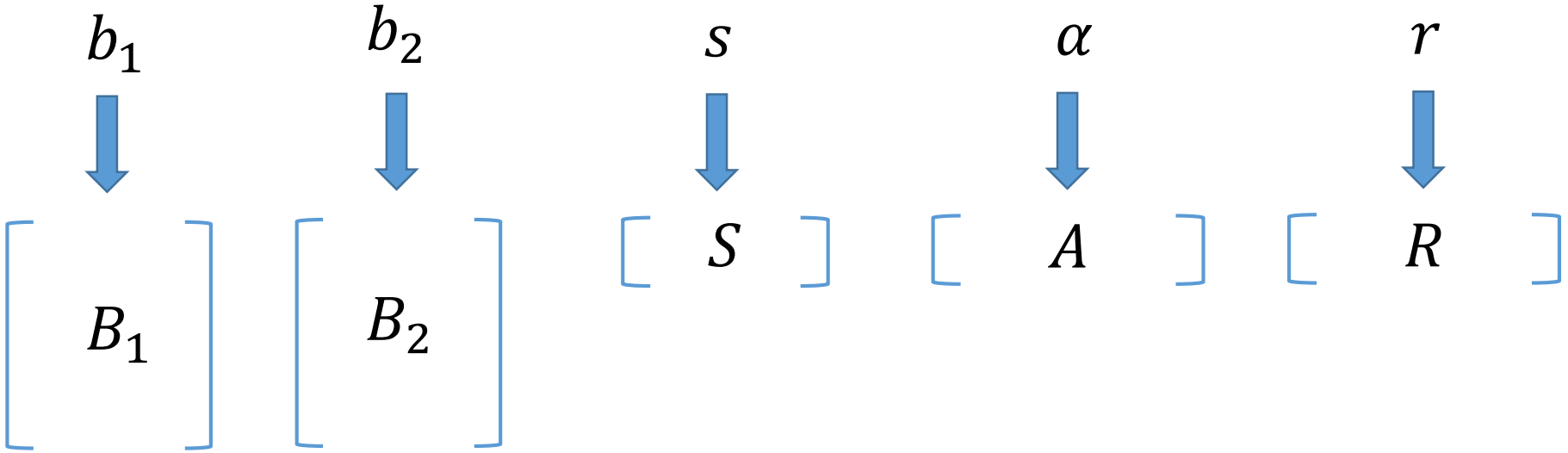
Symbolic property



Polynomials: $ID\ b_1 s + b_2 s,$ $\alpha + ID' b_1 r + b_2 r$

$ID\ B_1 S^T + B_2 S^T,$ $A + ID' R B_1 + R B_2$

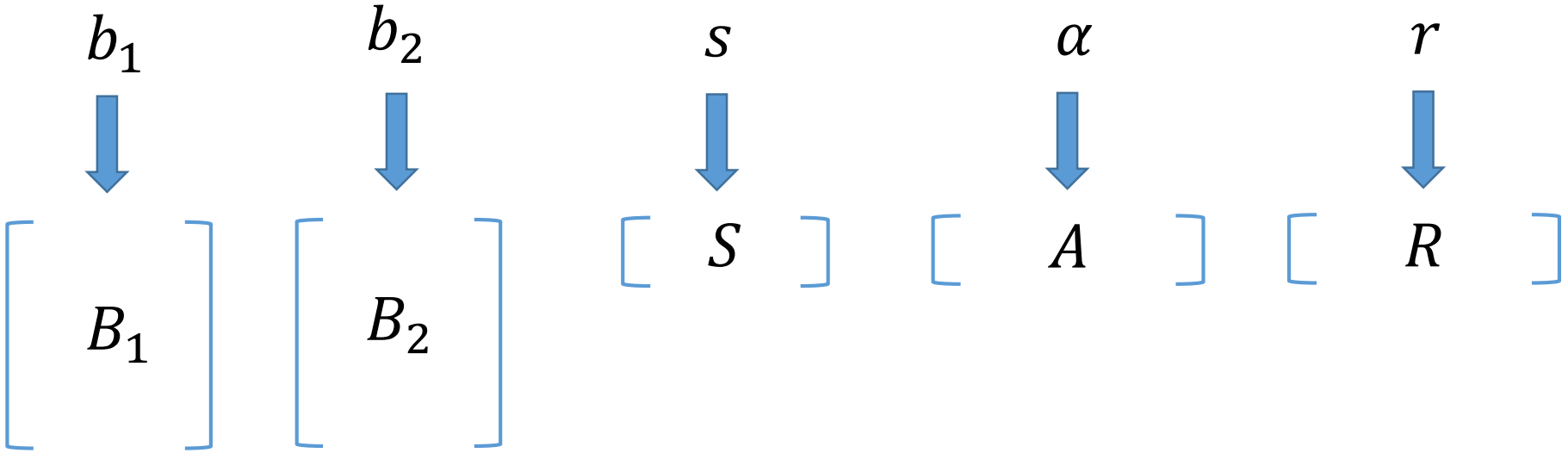
Symbolic property



Polynomials: $ID\ b_1 s + b_2 s,$ $\alpha + ID' b_1 r + b_2 r$

$ID\ B_1 S^T + B_2 S^T, = 0$ $A + ID' R B_1 + R B_2 = 0$

Symbolic property

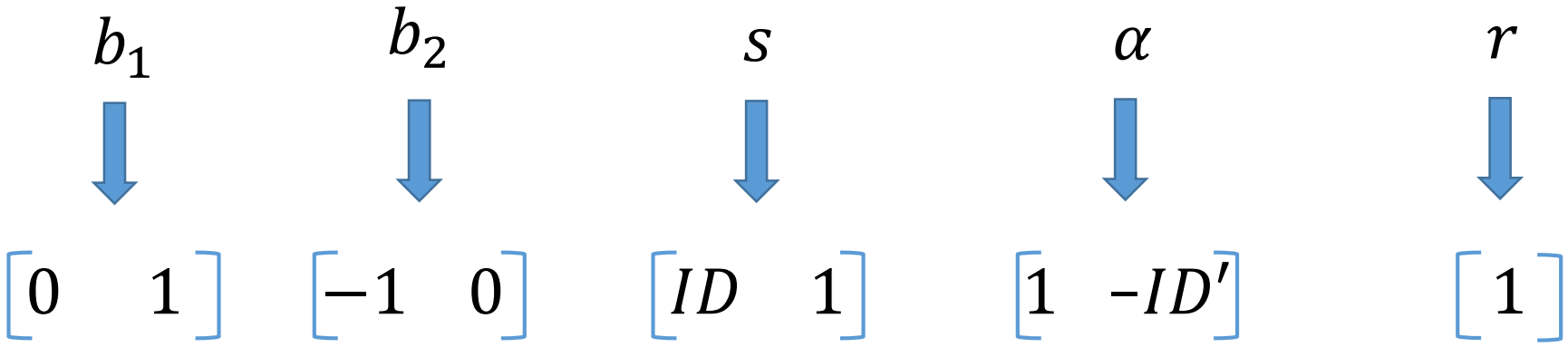


Polynomials: $ID\ b_1 s + b_2 s,$ $\alpha + ID' b_1 r + b_2 r$

$ID\ B_1 S^T + B_2 S^T, = 0$ $A + ID' R B_1 + R B_2 = 0$

$s \to S, \alpha \to A$ S not orthogonal to A

b_1 b_2 s α r


b_1
b_2
s
α
r
$\begin{bmatrix} 0 & 1 \end{bmatrix}$
$\begin{bmatrix} -1 & 0 \end{bmatrix}$
$\begin{bmatrix} ID & 1 \end{bmatrix}$
$\begin{bmatrix} 1 & -ID' \end{bmatrix}$
$\begin{bmatrix} 1 \end{bmatrix}$

b_1 b_2 s α r

$$\begin{bmatrix} 0 & 1 \end{bmatrix} \quad \begin{bmatrix} -1 & 0 \end{bmatrix} \quad \begin{bmatrix} ID & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & -ID' \end{bmatrix} \quad \begin{bmatrix} 1 \end{bmatrix}$$

$$ID\ b_1 s + b_2 s \longrightarrow ID \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} ID \\ 1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \end{bmatrix} \begin{bmatrix} ID \\ 1 \end{bmatrix}$$

$$= ID \begin{bmatrix} 1 \end{bmatrix} + \begin{bmatrix} -ID \end{bmatrix}$$

$$= \begin{bmatrix} 0 \end{bmatrix}$$

b_1 b_2 s α r

$\begin{bmatrix} 0 & 1 \end{bmatrix}$ $\begin{bmatrix} -1 & 0 \end{bmatrix}$ $\begin{bmatrix} ID & 1 \end{bmatrix}$ $\begin{bmatrix} 1 & -ID' \end{bmatrix}$ $\begin{bmatrix} 1 \end{bmatrix}$

$$ID\ b_1 s + b_2 s \longrightarrow ID \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} ID \\ 1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \end{bmatrix} \begin{bmatrix} ID \\ 1 \end{bmatrix}$$

$$= ID \begin{bmatrix} 1 \end{bmatrix} + \begin{bmatrix} -ID \end{bmatrix}$$

$$= \begin{bmatrix} 0 \end{bmatrix}$$

$\begin{bmatrix} ID & 1 \end{bmatrix}, \begin{bmatrix} 1 & -ID' \end{bmatrix}$ are not orthogonal if $ID \neq ID'$

b_1 b_2 s α r

$\begin{bmatrix} 0 & 1 \end{bmatrix}$ $\begin{bmatrix} -1 & 0 \end{bmatrix}$ $\begin{bmatrix} ID & 1 \end{bmatrix}$ $\begin{bmatrix} 1 & -ID' \end{bmatrix}$ $\begin{bmatrix} 1 \end{bmatrix}$

$ID\ b_1 s + b_2 s \longrightarrow ID \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} ID \\ 1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \end{bmatrix} \begin{bmatrix} ID \\ 1 \end{bmatrix}$

$= ID \begin{bmatrix} 1 \end{bmatrix} + \begin{bmatrix} -ID \end{bmatrix}$

$= \begin{bmatrix} 0 \end{bmatrix}$

Done!

$\begin{bmatrix} ID & 1 \end{bmatrix}, \begin{bmatrix} 1 & -ID' \end{bmatrix}$ are not orthogonal if $ID \neq ID'$

Symbolic property

Symbolic property

- Additional level of flexibility

Symbolic property

- Additional level of flexibility
- Two parts: selective & co-selective

Symbolic property

- Additional level of flexibility
- Two parts: selective & co-selective
- Selective property:

  vectors for key-encoding variables $(\alpha, r_1, r_2, \dots)$
  can depend on both x & y

Symbolic property

- Additional level of flexibility
- Two parts: selective & co-selective
- Selective property:

  vectors for key-encoding variables $(\alpha, r_1, r_2, \ldots)$
  can depend on both x & y

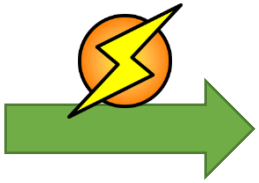
- Co-selective property

  vectors for ctxt-encoding variables $(s, s_1, s_2, \ldots)$
  can depend on both x & y

Generic transformation

For any predicate P

Encoding satisfies Symbolic property

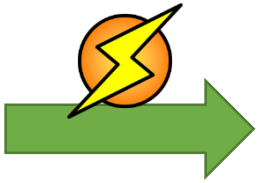


Fully secure encryption scheme

Generic transformation

For any predicate P

Encoding satisfies Symbolic property

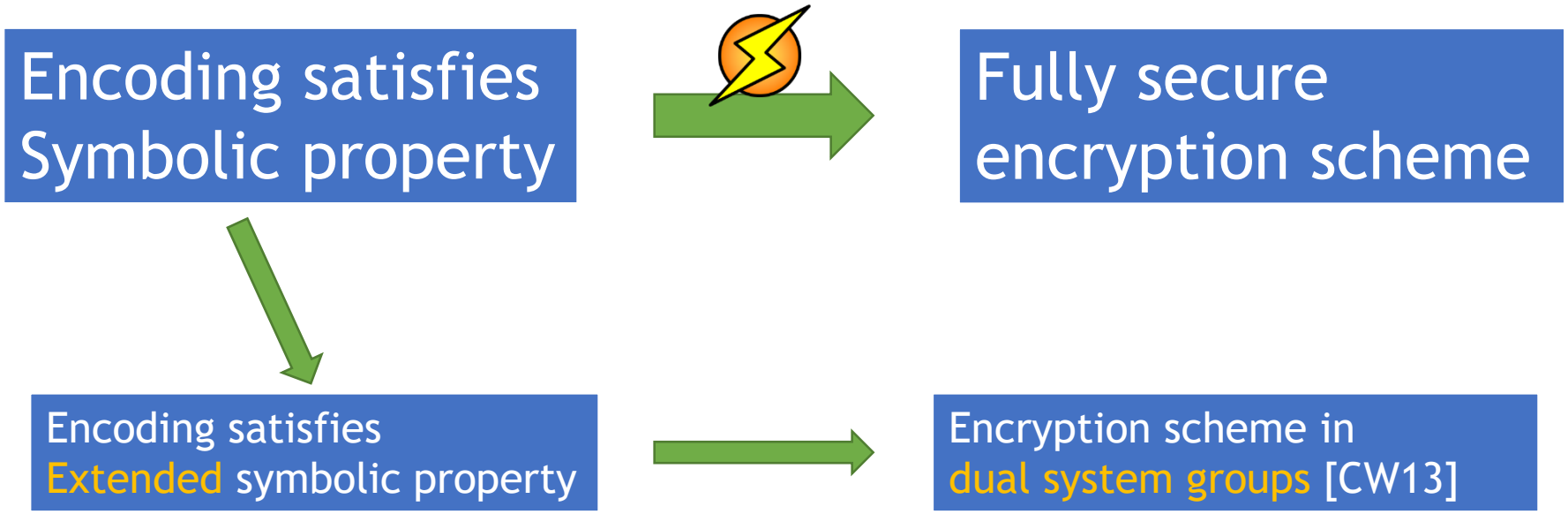


Fully secure encryption scheme

Encoding satisfies Extended symbolic property

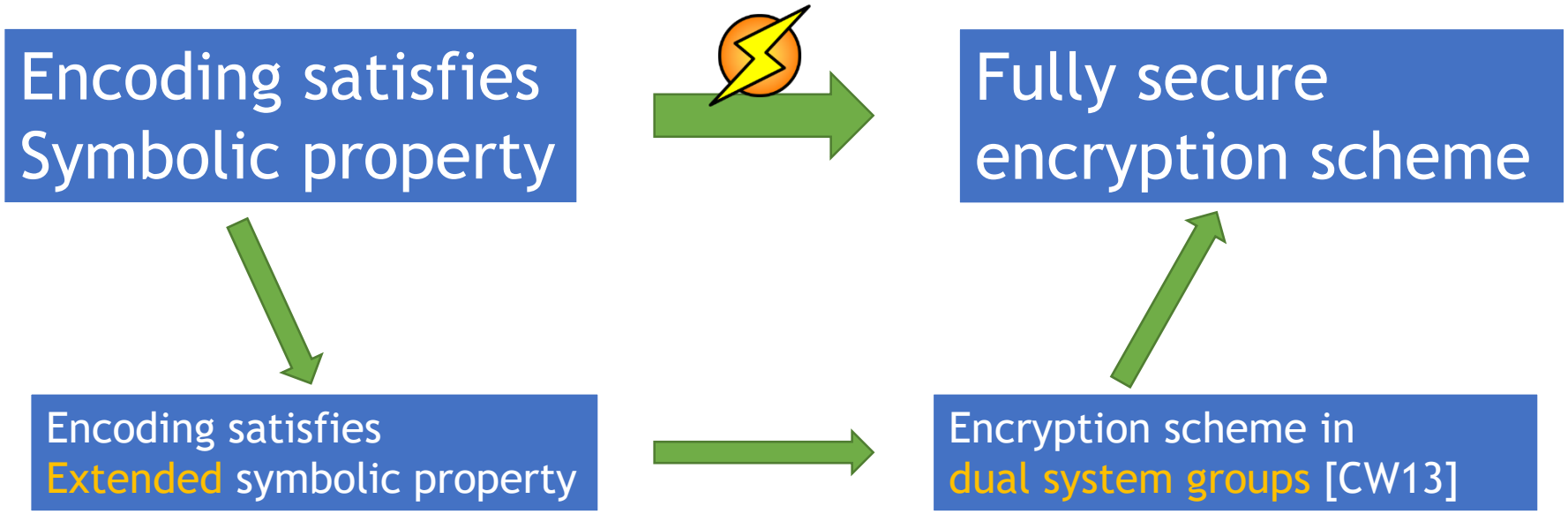
Generic transformation

For any predicate P



Generic transformation

For any predicate P



Inherent property

Inherent property

Inherent property

Correctness: When P(x, y) = 1, recover αs

Inherent property

Correctness: When P(x, y) = 1, recover αs

$$M \cdot e(g,g)^{\alpha s}$$

Inherent property

Correctness: When P(x, y) = 1, recover αs

$$M \cdot e(g,g)^{\alpha s}$$

When P(x, y) = 0, not recover αs

Inherent property

Correctness: When P(x, y) = 1, recover αs

$$M \cdot e(g,g)^{\alpha s}$$

When P(x, y) = 0, not recover αs

Trivially broken:

$\exists$x, y s.t. P(x, y) = 0, αs can be recovered

Inherent property

Inherent property

Not trivially broken a basic property

Inherent property

Not trivially broken a basic property

Not trivially broken ⇒ Satisfies symbolic property!

Param

b_1, b_2

Enc-CT

$ID \; b_1 s + b_2 s, \qquad s$

Enc-Key

$r, \qquad \alpha + ID' b_1 r + b_2 r$

Param

b_1, b_2

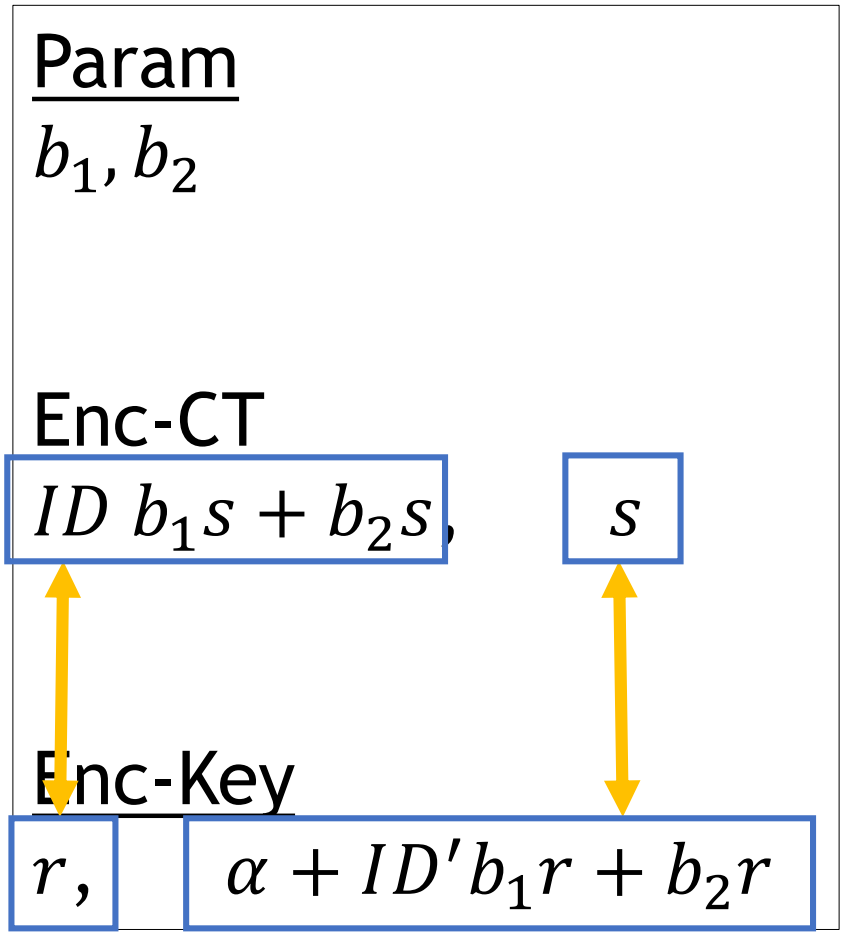
Enc-CT

$ID \; b_1 s + b_2 s, \qquad s$

Enc-Key

$r, \qquad \alpha + ID' b_1 r + b_2 r$

$ID' = ID: \quad \alpha s$



$ID' = ID: \quad \alpha s$

Param

b_1, b_2

Enc-CT

$ID\ b_1 s + b_2 s, \qquad s$

Enc-Key

$r, \qquad \alpha + ID' b_1 r + b_2 r$

$ID' = ID: \quad \alpha s$

$ID' \neq ID: \quad \alpha s$

General encodings

Predicate P

Param

$b_1, b_2, \ldots$

Enc-CT

$C_1, C_2, C_3, \ldots$ $\quad s, s_1, s_2, \ldots$

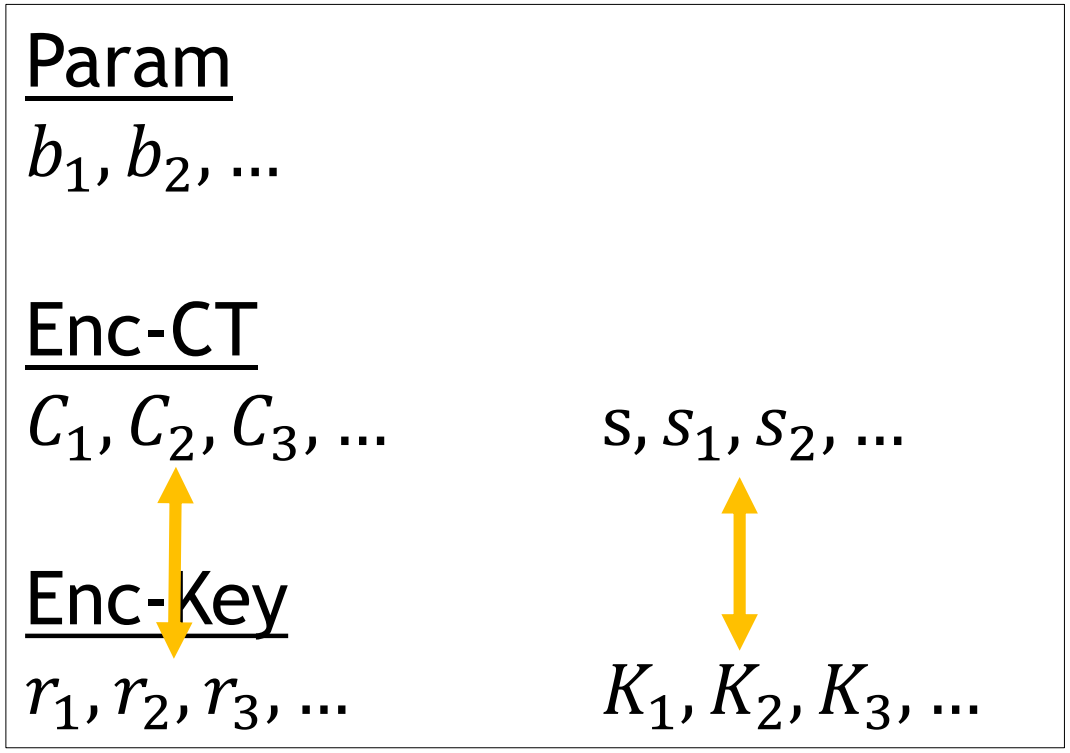
Enc-Key

$r_1, r_2, r_3, \ldots$ $\quad K_1, K_2, K_3, \ldots$

Many variables & polynomials

General encodings

Predicate P



Many variables & polynomials

When P(x, y) = 0, cannot be combined to get αs

General encodings

Predicate P

Param

$b_1, b_2, \ldots$

Enc-CT

$C_1, C_2, C_3, \ldots$

$s, s_1, s_2, \ldots$

Enc-Key

$r_1, r_2, r_3, \ldots$

$K_1, K_2, K_3, \ldots$

Many variables & polynomials

When P(x, y) = 0, cannot be combined to get αs

General encodings

Predicate P

Param

$b_1, b_2, \ldots$

Enc-CT

$C_1, C_2, C_3, \ldots$

$s, s_1, s_2, \ldots$

Enc-Key

$r_1, r_2, r_3, \ldots$

$K_1, K_2, K_3, \ldots$

Many variables & polynomials

When P(x, y) = 0, cannot be combined to get αs

Selective symbolic property

Predicate P

Param

$b_1, b_2, \ldots$

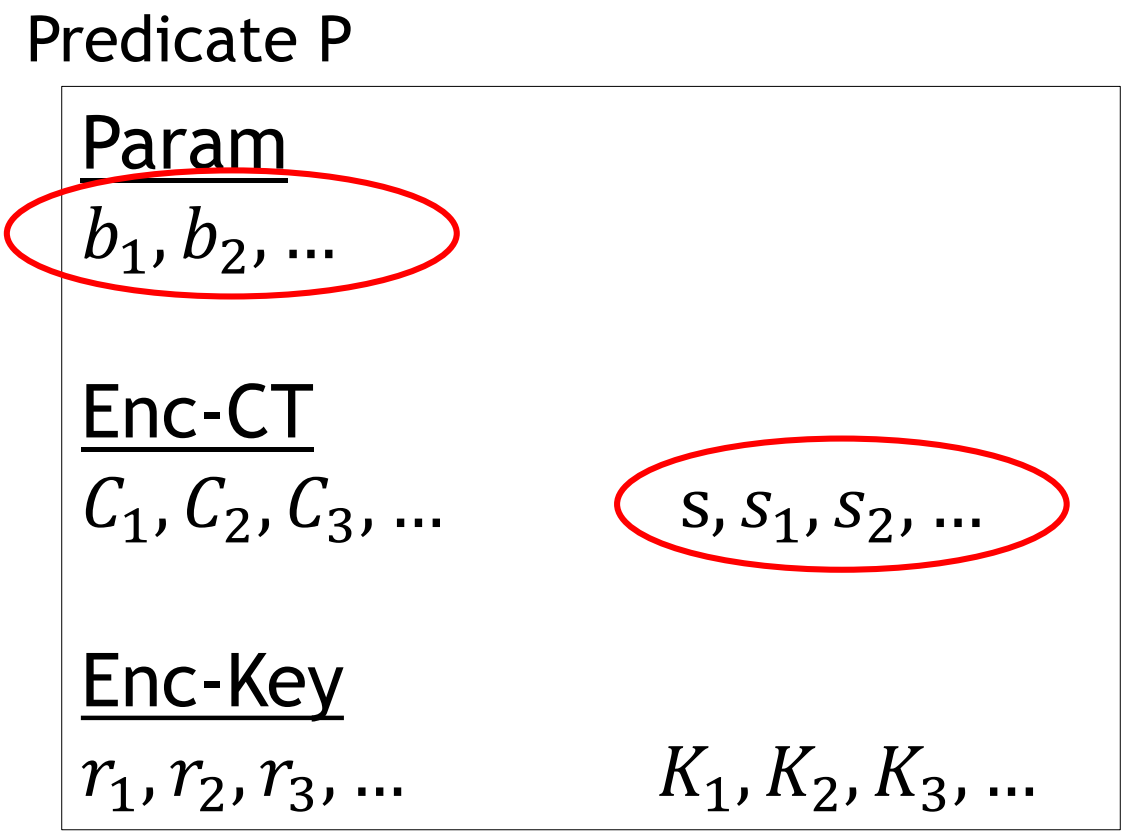
Enc-CT

$C_1, C_2, C_3, \ldots$ $\quad$ $s, s_1, s_2, \ldots$

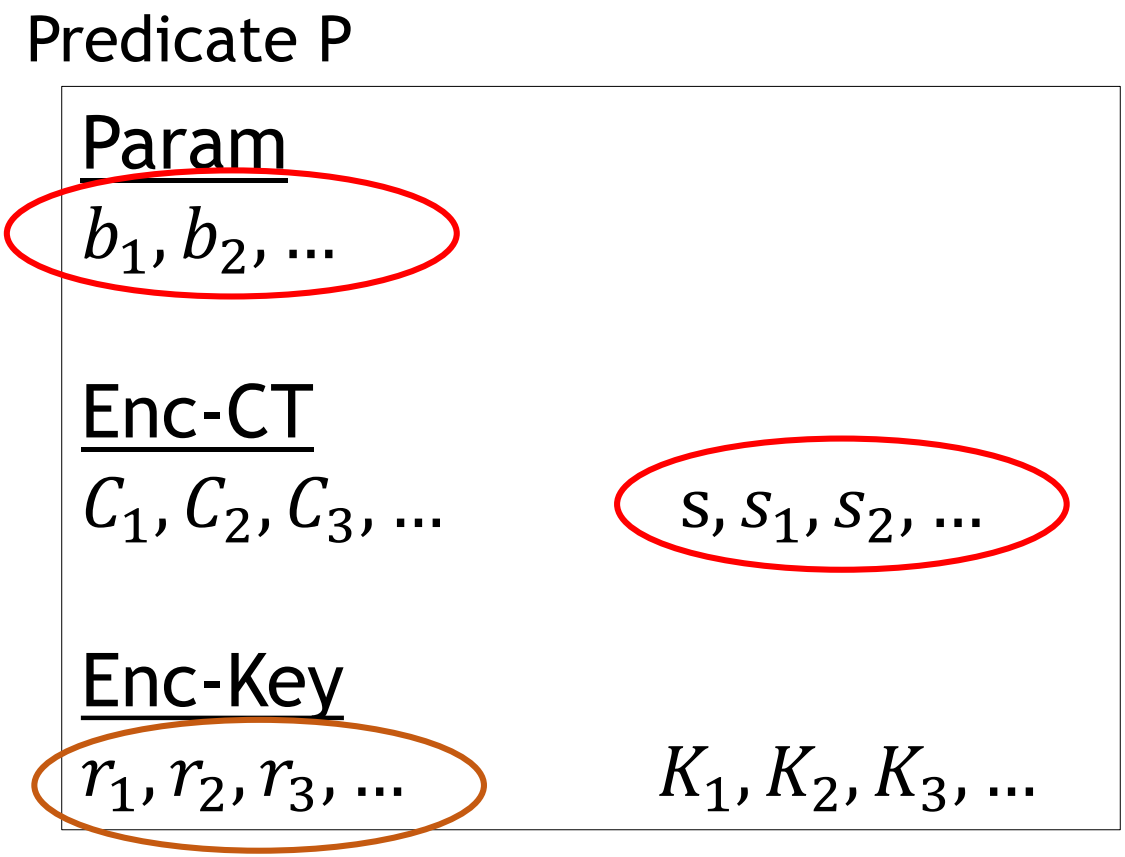
Enc-Key

$r_1, r_2, r_3, \ldots$ $\quad$ $K_1, K_2, K_3, \ldots$

Selective symbolic property



Selective symbolic property

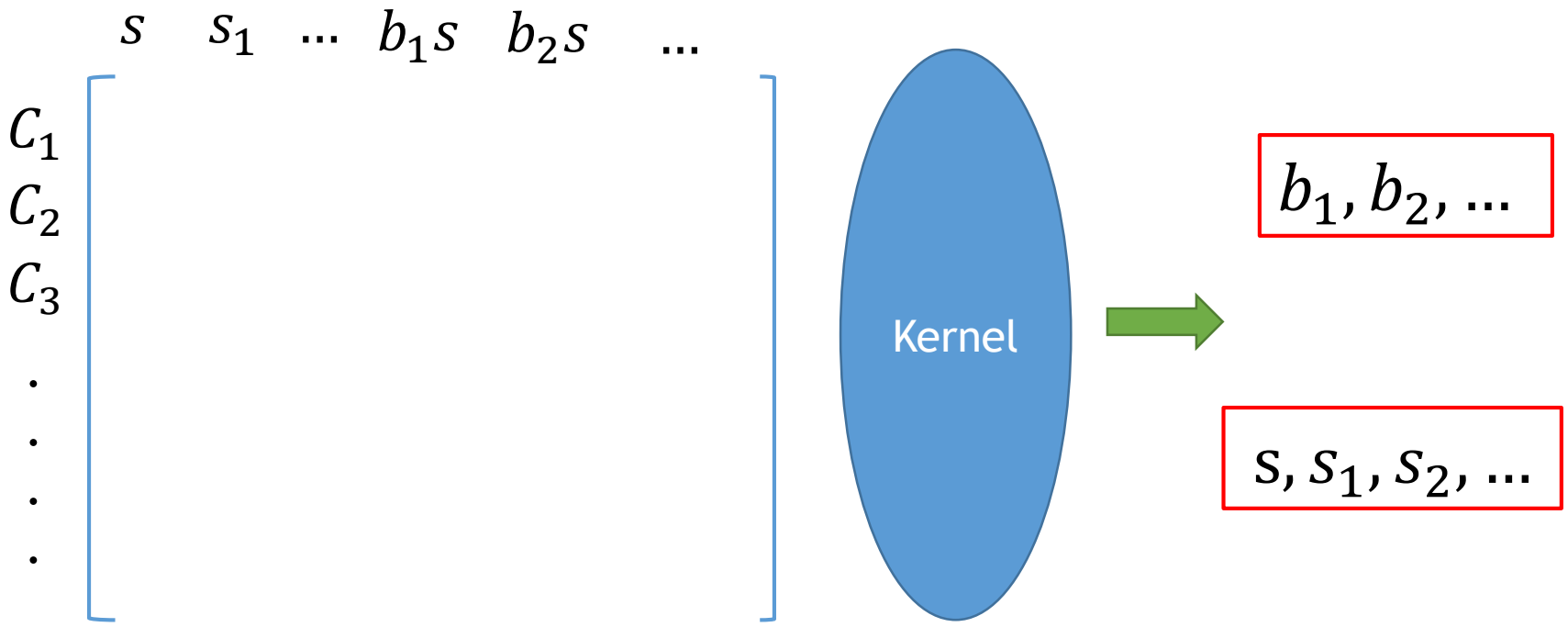


$C_1, C_2, C_3, \ldots$

$$C_1, C_2, C_3, \ldots$$

	s	s_1	…	$b_1 s$	$b_2 s$	…
C_1						
C_2						
C_3						
.						
.						
.						
.						

$C_1, C_2, C_3, \ldots$

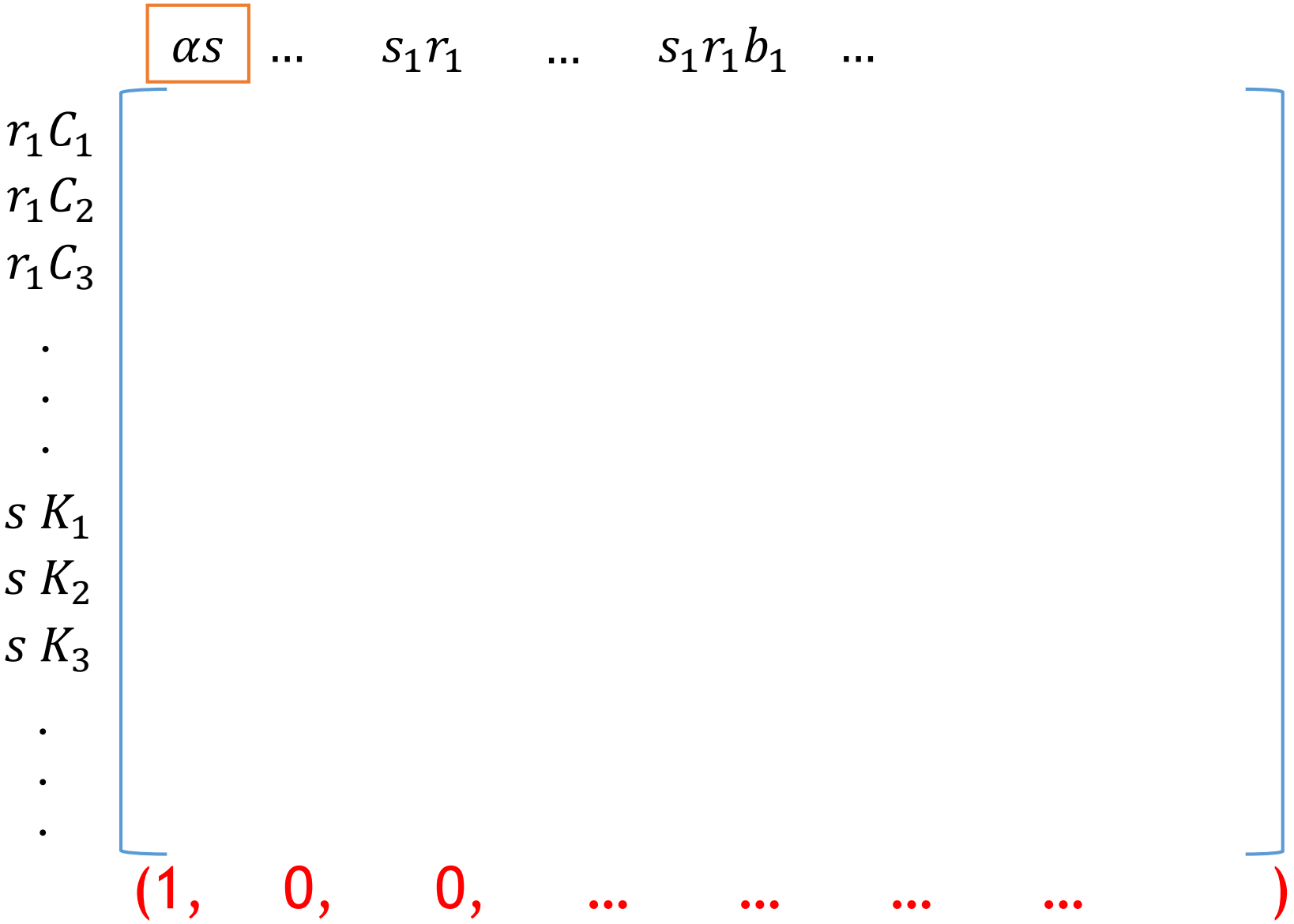


$K_1, K_2, K_3, \ldots$

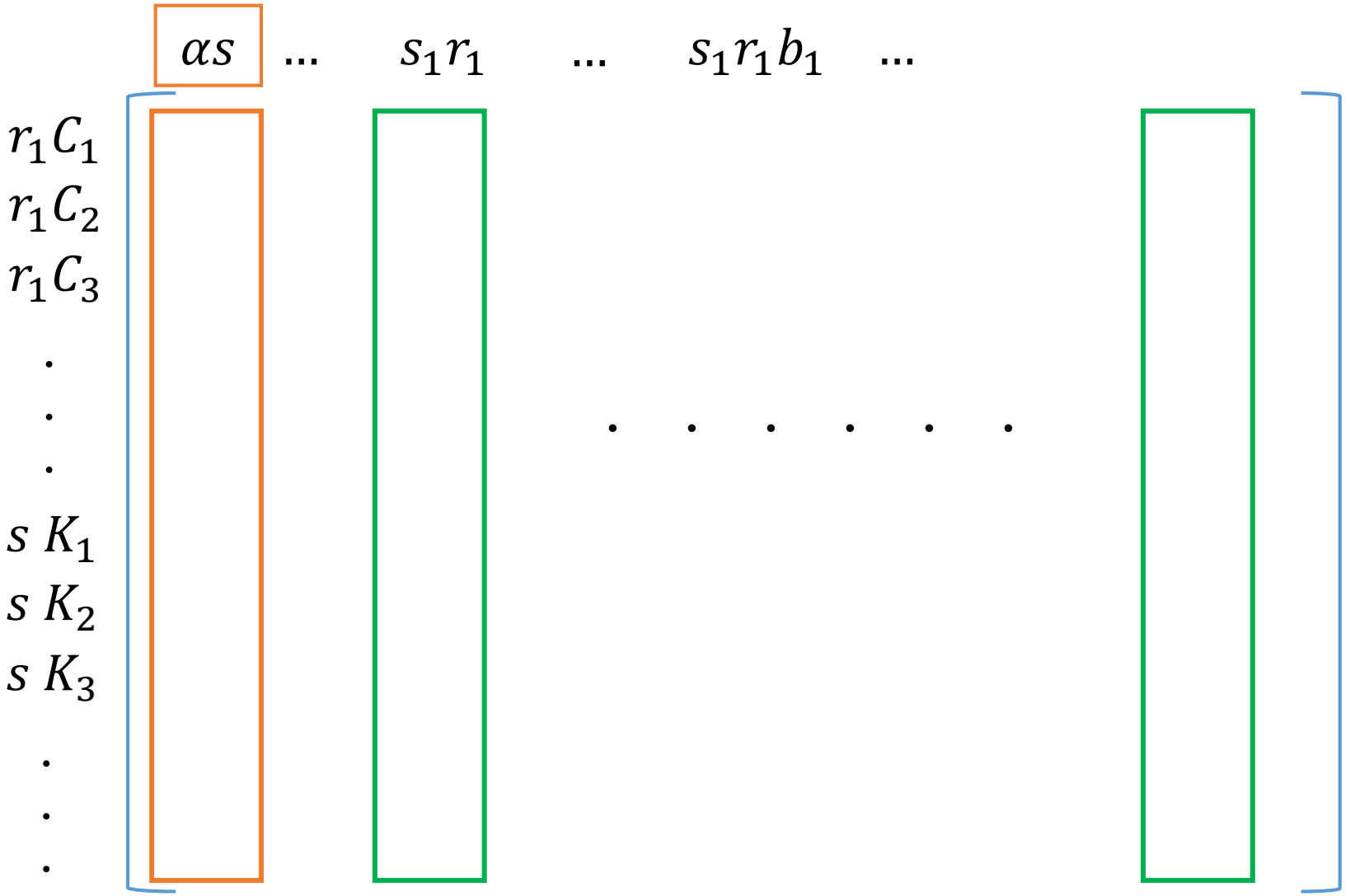
$K_1, K_2, K_3, \ldots$

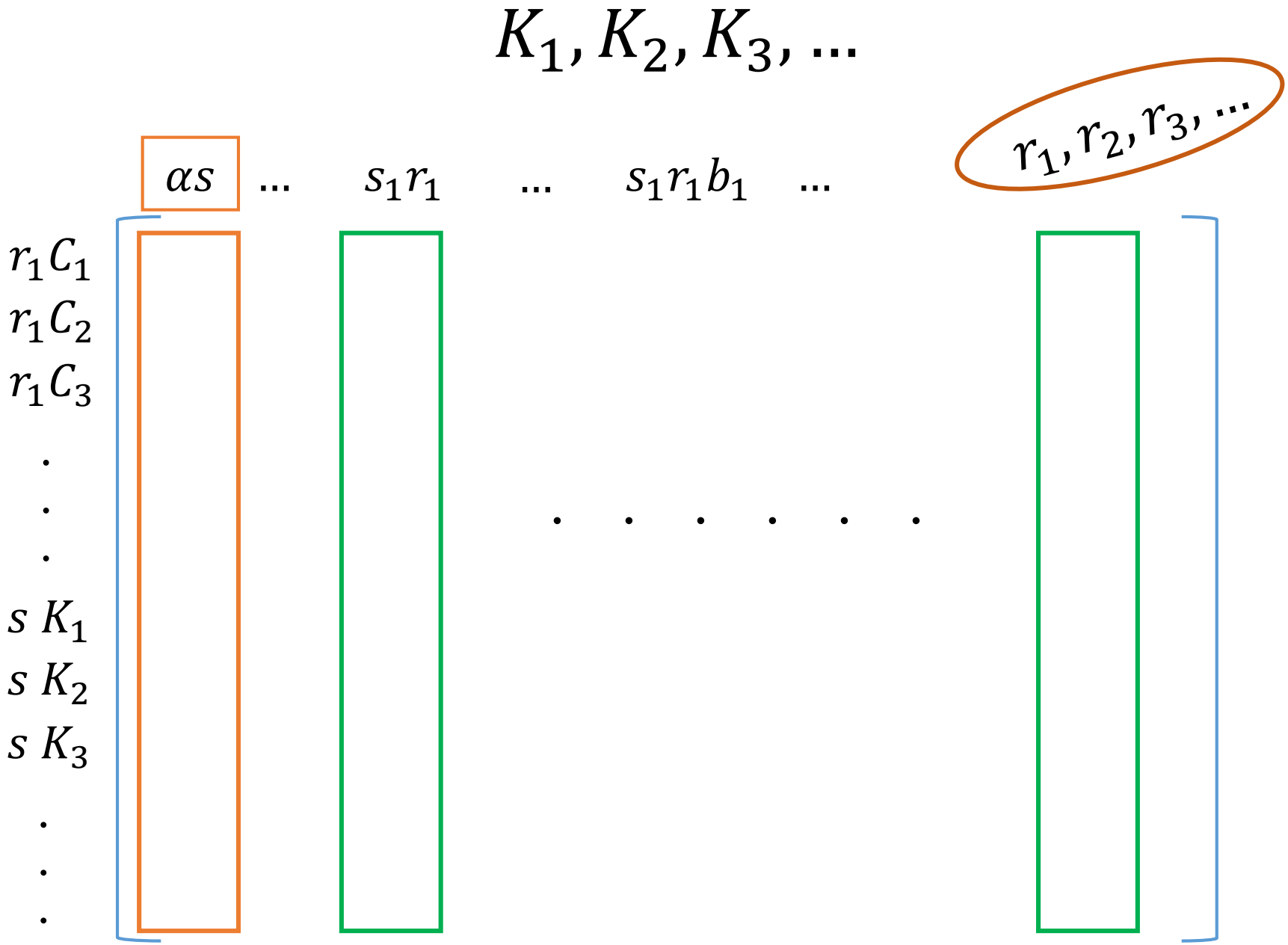
	αs	...	$s_1 r_1$	...	$s_1 r_1 b_1$	...
$r_1 C_1$						
$r_1 C_2$						
$r_1 C_3$						
.						
.						
.						
$s\ K_1$						
$s\ K_2$						
$s\ K_3$						
.						
.						
.						

$K_1, K_2, K_3, \ldots$



$K_1, K_2, K_3, \ldots$




$K_1, K_2, K_3, \ldots$
$r_1, r_2, r_3, \ldots$
αs
$s_1 r_1$
$s_1 r_1 b_1$
$r_1 C_1$
$r_1 C_2$
$r_1 C_3$
$s\ K_1$
$s\ K_2$
$s\ K_3$

Open questions

Open questions

Open questions

- Our new q-type assumption
  - Simple cases vis-à-vis standard assumptions

Open questions

- Our new q-type assumption
  - Simple cases vis-à-vis standard assumptions
- Automating proof generation
  - Generate mappings through a program

Open questions

- Our new q-type assumption
  - Simple cases vis-à-vis standard assumptions
- Automating proof generation
  - Generate mappings through a program
- Push boundaries
  - Go beyond NC1?

Thank you!