Dual System Encryption via Doubly Selective Security:

Framework, Fully-secure Functional Encryption for Regular Languages, and More

Nuttapong Attrapadung (Nuts)
AIST, Japan
@Eurocrypt 2014, Copenhagen

Our Results in One Slide

Framework
for fully-secure FE
(with tighter reduction)

Instantiations:

The first fully secure

- FE for regular languages
- ABE with short ciphertext
- unbounded ABE

and more

Our Results in One Slide

Framework
for fully-secure FE
(with tighter reduction)

focus in this talk

Instantiations:

The first fully secure

- FE for regular languages
- ABE with short ciphertext
- unbounded ABE

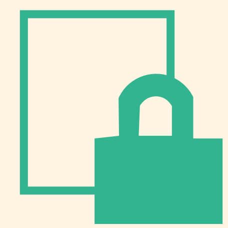
and more

1 Introduction

Functional Encryption Syntax

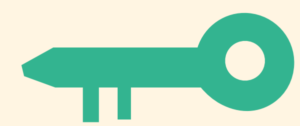
FE for predicate $R{:}A \times B \to \{0,1\}$ or family $\{R_k\}_k$

- Setup($k, 1^\lambda$) $\longrightarrow$ PK, MSK
- Encrypt(Y, M, PK) $\longrightarrow$ CT



for ciphertext
attribute Y

- KeyGen(X, MSK, PK) $\longrightarrow$ SK

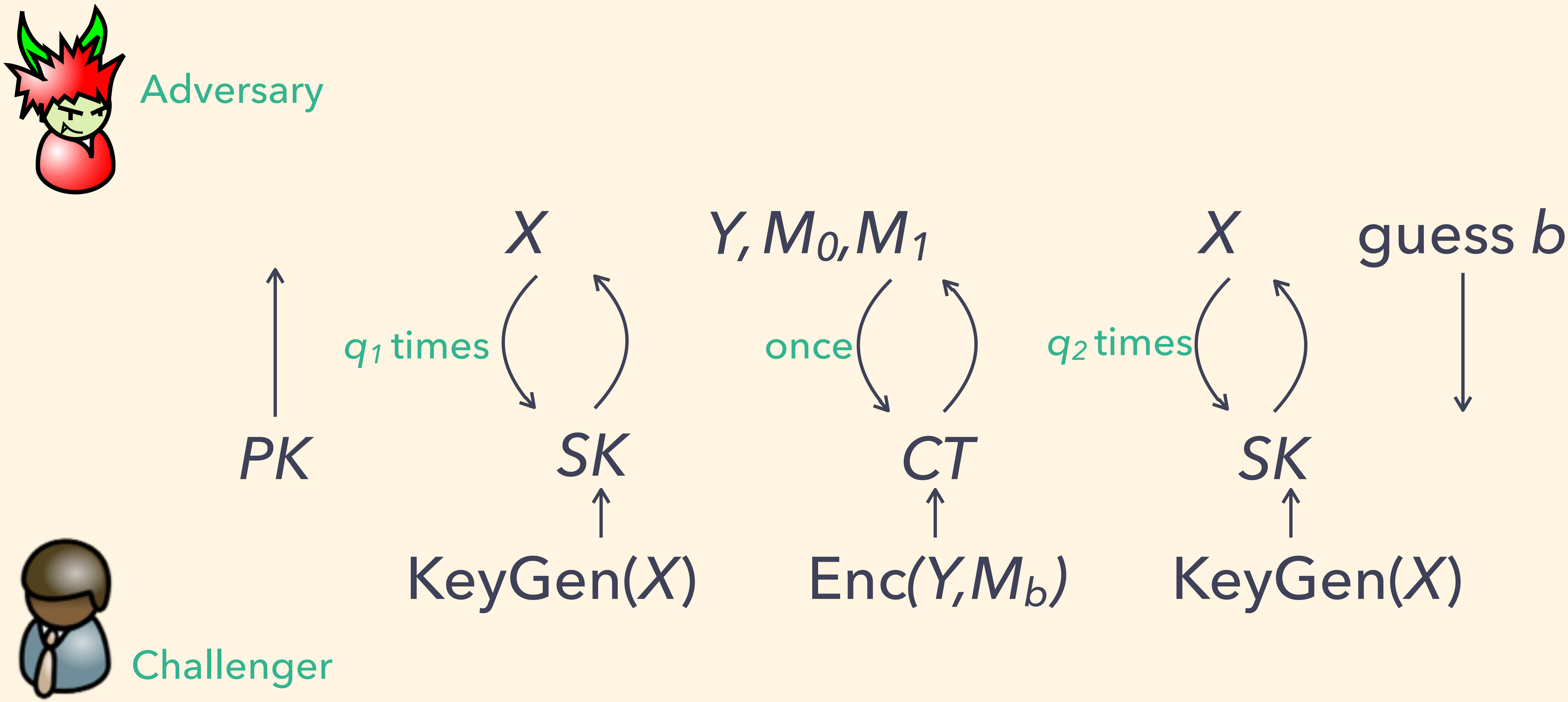


for key
attribute X

- Decrypt(CT, SK) $\longrightarrow$ M if $R(X,Y)=1$

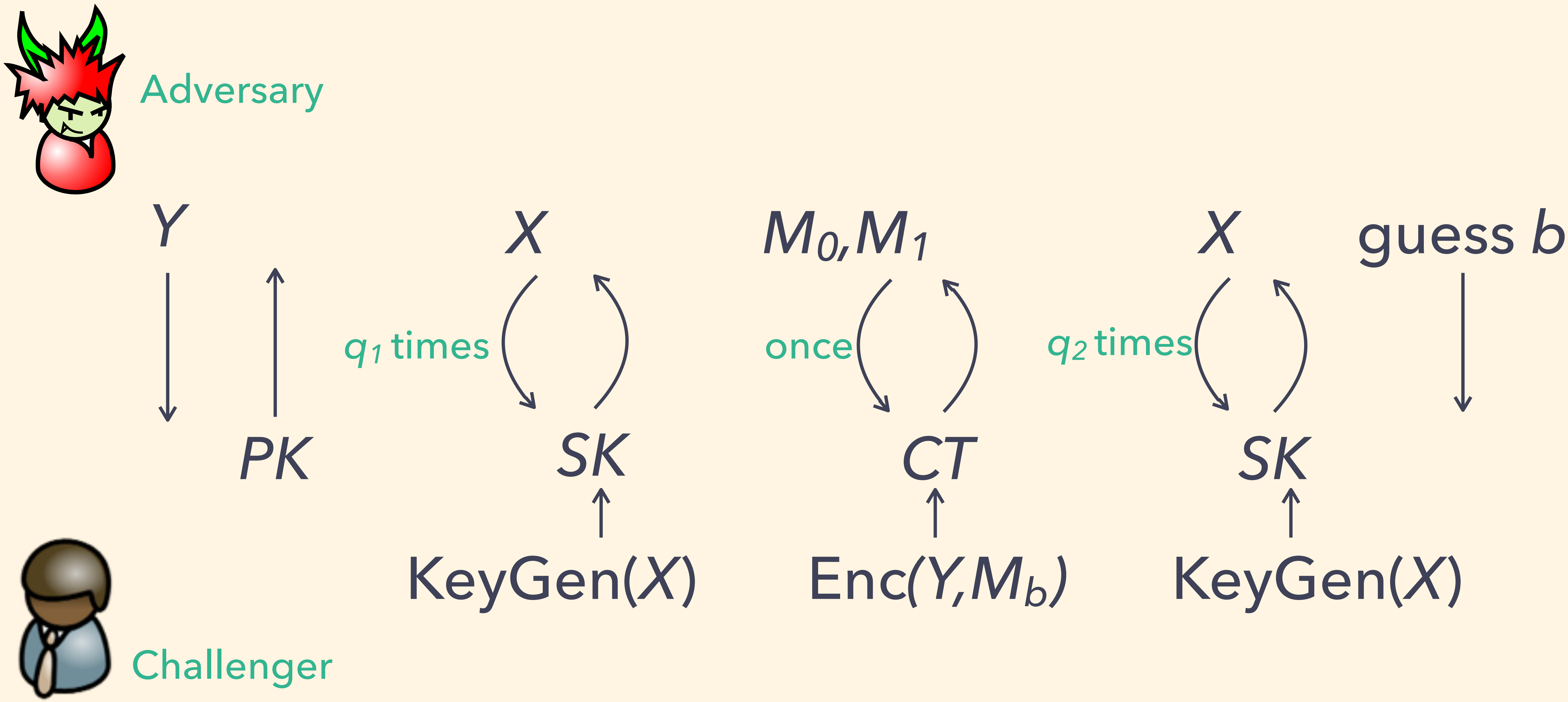
FE here means the class
"Public-index Predicate Encryption" of FE [BSW11].

Definition of Full Security for FE



Non-triviality condition: $R(X,Y)=0$

Definition of Selective Security for FE

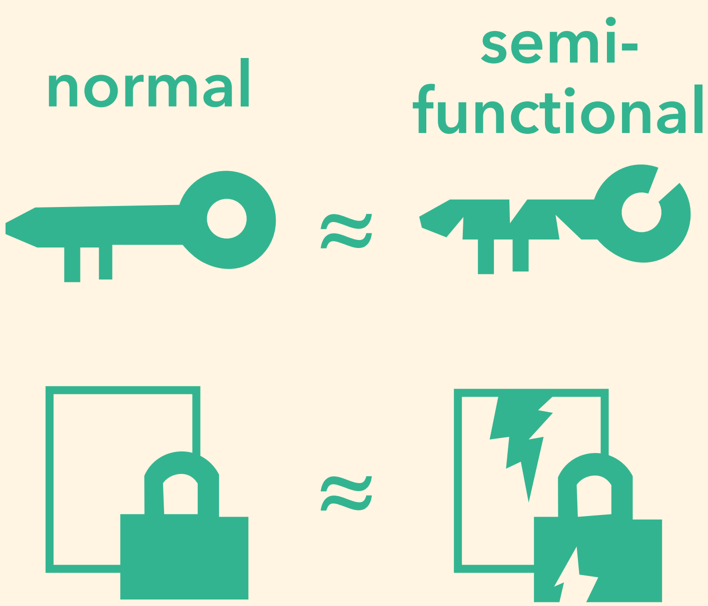


Non-triviality condition: $R(X,Y)=0$

Approaches for Full Security

Partitioning

- IBE [BB04b, Waters05]
- Seem not to work with richer FE



Dual-System Encryption [Waters09]

- Work also with richer FE:
  - ABE [LOSTW10,OT10,LW12,…]
  - Inner-product enc [OT12,…]
  - Spatial encryption [AL10,…]

Dual System Also Offers Simplicity.

An original FE scheme

Selectively-secure

Similar scheme but in composite-order bilinear group

A candidate for fully-secure scheme

Boneh-Boyen IBE

(selectively secure)

$CT=(g^s, g^{s(h_1+h_2 ID)}, e(g,g)^{as}M)$

$SK=(g^{a+r(h_1+h_2 ID')}, g^r)$

Lewko-Waters IBE

(fully secure)

$CT=(g_1^s, g_1^{s(h_1+h_2 ID)}, e(g_1,g_1)^{as}M)$

$SK=(g_1^{a+r(h_1+h_2 ID')} g_3^{w_1}, g_1^r g_3^{w_2})$

Boneh-Boyen IBE

(selectively secure)

$CT=(g^s, g^{s(h_1+h_2ID)}, e(g,g)^{as}M)$

$SK=(g^{a+r(h_1+h_2ID')}, g^r)$

Lewko-Waters IBE

(fully secure)

$CT=(g_1^s, g_1^{s(h_1+h_2ID)}, e(g_1,g_1)^{as}M)$

$SK=(g_1^{a+r(h_1+h_2ID')}g_3^{w_1}, g_1^r g_3^{w_2})$

Abstract Selective Secure FE

$CT=(g_1^{\mathbf{c}(\mathbf{s},\mathbf{h})}, e(g_1,g_1)^{as}M)$

$SK=g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})}$

Abstract Fully Secure FE ?

$CT=(g_1^{\mathbf{c}(\mathbf{s},\mathbf{h})}, e(g_1,g_1)^{as}M)$

$SK=g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_3^{\mathbf{w}}$

Apply to any scheme?

Successful Applications

	Selective	Full
IBE	BB04	LW10
ABE	GPSW06	LOSTW10
Spatial Encryption	BH08	AL10

Unsuccessful Applications

	Selective	Full
FE for regular languages	Waters12	?
ABE w/ short ciphertexts	ALP11	?
Fully-unbounded ABE	RW13	?

Open problem!

We ask:

Why did “traditional” dual systems fail for some schemes?

How to overcome that barrier?

To systematically answer, we provide a generic framework.

Our Framework Result

New primitive: Pair Encoding → **Generic** → **FE Scheme**

Perfectly secure pair encoding

Computationally secure encoding

"Doubly selective security"

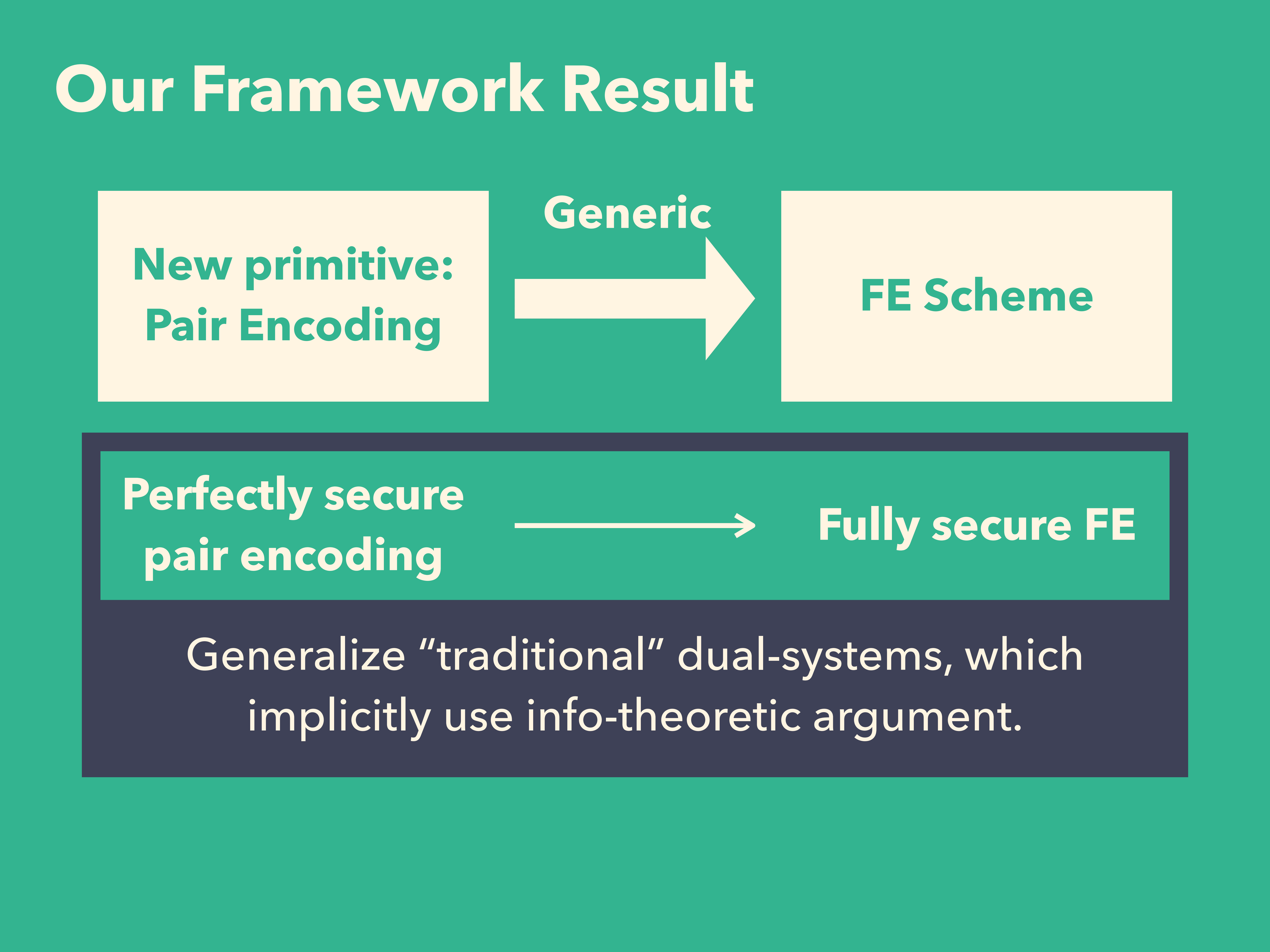
Our Framework Result

New primitive: Pair Encoding → (Generic) → FE Scheme

Perfectly secure pair encoding → Fully secure FE

Computationally secure encoding → Fully secure FE + tighter reduction

"Doubly selective security"


Our Framework Result
New primitive:
Pair Encoding
Generic
FE Scheme
Perfectly secure
pair encoding
Fully secure FE
Generalize “traditional” dual-systems, which
implicitly use info-theoretic argument.

Our Framework Result

New primitive: Pair Encoding → **Generic** → **FE Scheme**

Generalize Lewko-Waters12 ABE
+ New techniques for tighter reduction.

Computationally secure encoding → **Fully secure FE + tighter reduction**

A Glance at Pair Encoding

Recall the abstract scheme

$CT=(g_1^{\mathbf{c(s,h)}},\ e(g_1,g_1)^{as}M)$

$SK=g_1^{\mathbf{k(a,r,h)}}\cdot g_3^{\mathbf{w}}$

Pair encoding consists of *c*( ) and *k*( ).

Our Answer to Instantiations

	Selective	Fully-secure
FE for regular languages	Waters12	
ABE w/ short ciphertexts	ALP11	
Fully-unbounded ABE	RW13	

Our Answer to Instantiations

	Selective	Fully-secure
FE for regular languages	Waters12	
ABE w/ short ciphertexts	ALP11	
Fully-unbounded ABE	RW13	

↓

Why traditional dual systems failed:
(Implicit) encodings were not perfect.

Our Answer to Instantiations

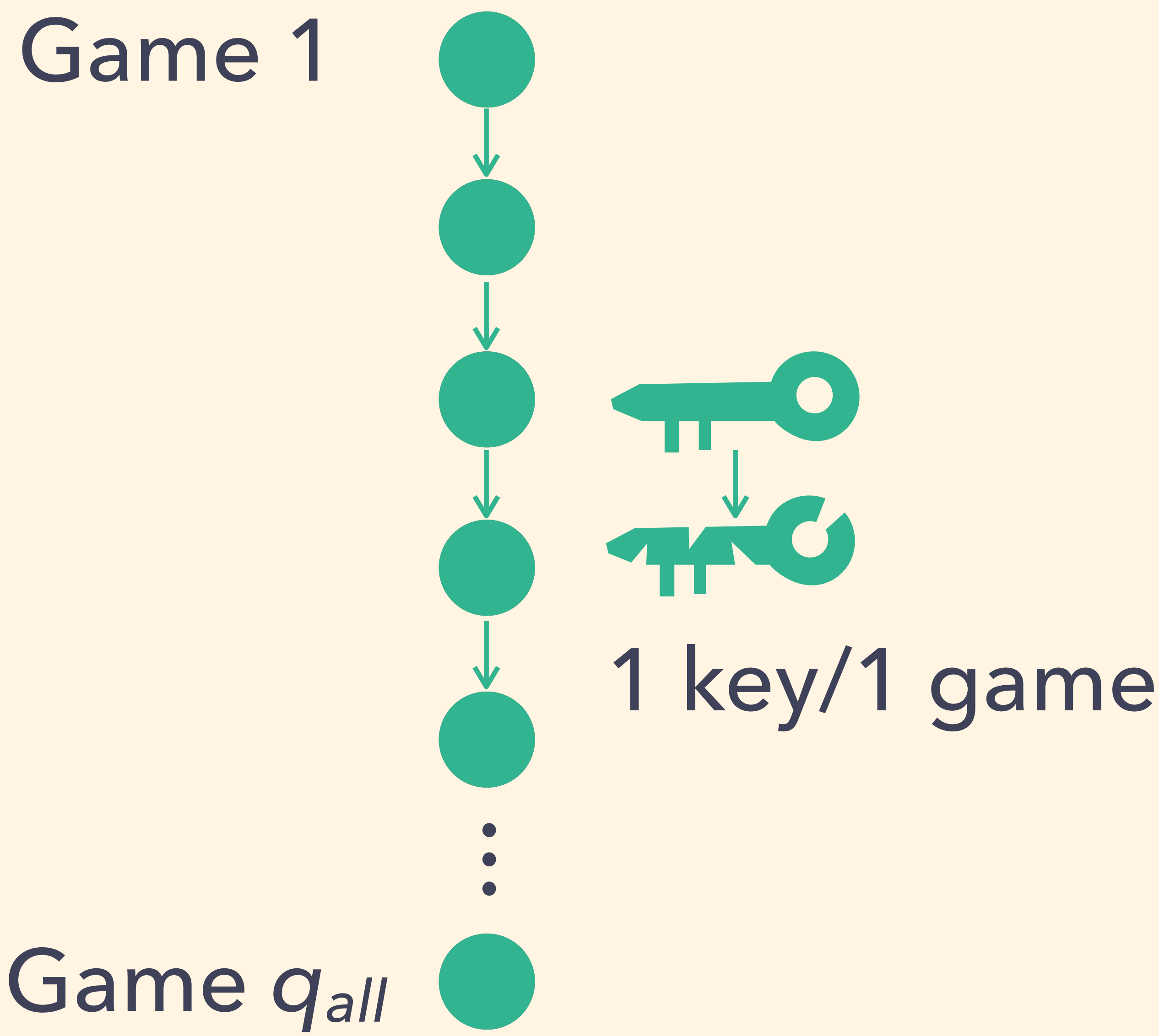
	Selective	Fully-secure
FE for regular languages	Waters12	**New!**
ABE w/ short ciphertexts	ALP11	**New!**
Fully-unbounded ABE	RW13	**New!**

Why traditional dual systems failed: (Implicit) encodings were not perfect.

How to overcome: Use computationally secure encodings

A Glance at Tighter Reduction

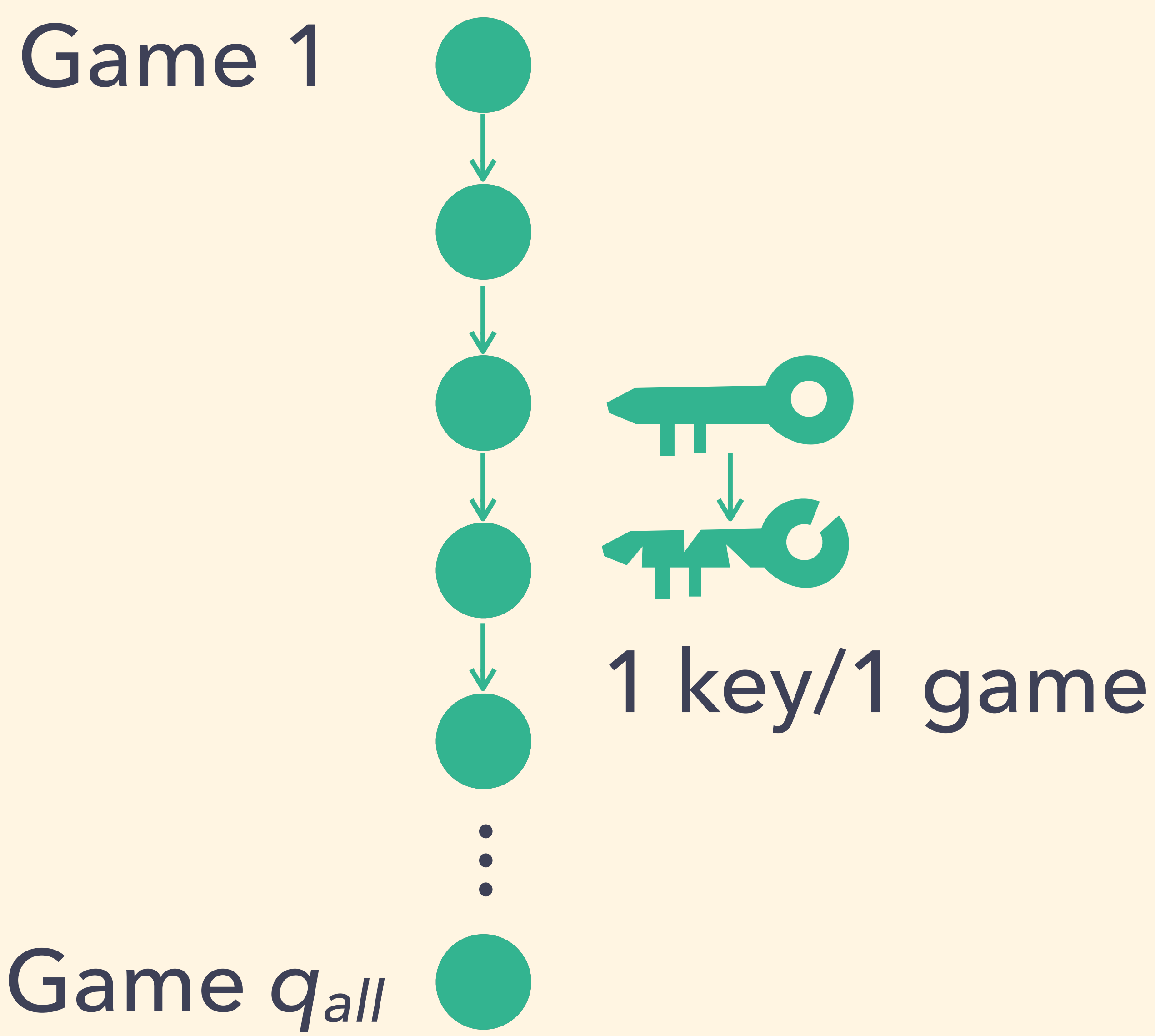
All prior dual-system proofs
(except [Chen-Wee Crypto13])



Reduction=$O(q_{all})$, $q_{all} = q_1 + q_2$

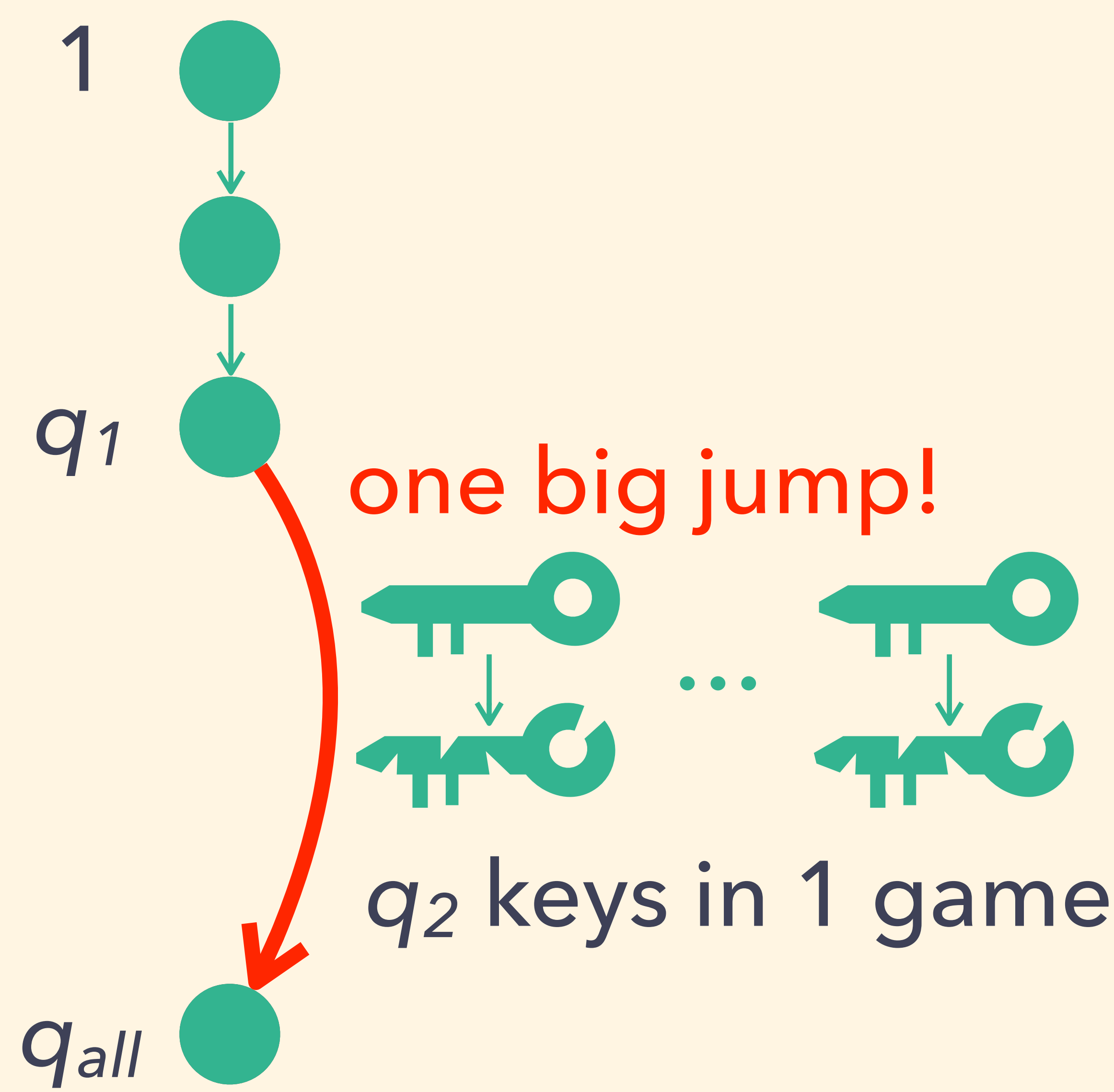
A Glance at Tighter Reduction

All prior dual-system proofs
(except [Chen-Wee Crypto13])



Reduction=$O(q_{all})$, $q_{all}= q_1+q_2$

Our new approach



Reduction=$O(q_1)$

Related work on Dual-System Framework

- [Chen-Wee Crypto13]: Dual-system groups
  - Unify prime- and composite-order groups but only to specific predicates (HIBE).
  - Ours unifies for any predicate (but specific to composite-order).
- [Wee TCC14]: Predicate Encoding
  - Independently abstracting perfectly secure encoding.

2 Framework

Pair Encoding: Definition

Pair Encoding for predicate $R=\{R_k\}_k$

$\text{Enc1}(X) \longrightarrow \boldsymbol{k}(a, \boldsymbol{r}, \boldsymbol{h})$ where $\boldsymbol{r}=(r_1,\ldots,r_m)$

$\text{Enc2}(Y) \longrightarrow \boldsymbol{c}(\boldsymbol{s}, \boldsymbol{h})$ where $\boldsymbol{s}=(s, s_1,\ldots,s_w)$

Pair Encoding: Definition

Pair Encoding for predicate $R=\{R_k\}_k$

$$\mathrm{Param}(k) \longrightarrow |\boldsymbol{h}| \qquad \text{where } \boldsymbol{h}=(h_1,\ldots,h_m)$$

$$\mathrm{Enc1}(X) \longrightarrow \boldsymbol{k}(a,\boldsymbol{r},\boldsymbol{h}) \qquad \text{where } \boldsymbol{r}=(r_1,\ldots,r_m)$$

$$\mathrm{Enc2}(Y) \longrightarrow \boldsymbol{c}(\boldsymbol{s},\boldsymbol{h}) \qquad \text{where } \boldsymbol{s}=(s,s_1,\ldots,s_w)$$

Pair Encoding: Definition

Pair Encoding for predicate $R=\{R_k\}_k$

Param(k)	$\longrightarrow$	$\lvert \boldsymbol{h} \rvert$	where $\boldsymbol{h}=(h_1,\ldots,h_m)$
Enc1(X)	$\longrightarrow$	$\boldsymbol{k}(a,\boldsymbol{r},\boldsymbol{h})$	where $\boldsymbol{r}=(r_1,\ldots,r_m)$
Enc2(Y)	$\longrightarrow$	$\boldsymbol{c}(\boldsymbol{s},\boldsymbol{h})$	where $\boldsymbol{s}=(s,s_1,\ldots,s_w)$
Pair(X,Y)	$\longrightarrow$	$\boldsymbol{E}$	

- Correctness : If $R(X,Y)=1$, $\boldsymbol{k}(a,\boldsymbol{r},\boldsymbol{h})\,\boldsymbol{E}\,\boldsymbol{c}(\boldsymbol{s},\boldsymbol{h})^{\top}=as$

Pair Encoding: Definition

Pair Encoding for predicate $R=\{R_k\}_k$

Param(k) $\longrightarrow$ $|\boldsymbol{h}|$ where $\boldsymbol{h}=(h_1,\ldots,h_m)$

Enc1(X) $\longrightarrow$ $\boldsymbol{k}(a,\boldsymbol{r},\boldsymbol{h})$ where $\boldsymbol{r}=(r_1,\ldots,r_m)$

Enc2(Y) $\longrightarrow$ $\boldsymbol{c}(\boldsymbol{s},\boldsymbol{h})$ where $\boldsymbol{s}=(s,s_1,\ldots,s_w)$

Pair(X,Y) $\longrightarrow$ $\boldsymbol{E}$

- Correctness : If $R(X,Y)=1$, $\boldsymbol{k}(a,\boldsymbol{r},\boldsymbol{h})\,\boldsymbol{E}\,\boldsymbol{c}(\boldsymbol{s},\boldsymbol{h})^{\top}=as$
- Security: If $R(X,Y)=0$, …to be defined.

Additional Requirements

Parameter-vanishing $\boldsymbol{k}(a,\mathbf{0},\boldsymbol{h}) = \boldsymbol{k}(a,\mathbf{0},\mathbf{0})$

Linearity for $\boldsymbol{k}$ $\boldsymbol{k}(a_1,\boldsymbol{r}_1,\boldsymbol{h})+\boldsymbol{k}(a_2,\boldsymbol{r}_2,\boldsymbol{h}) = \boldsymbol{k}(a_1+a_2,\boldsymbol{r}_1+\boldsymbol{r}_2,\mathbf{0})$

Linearity for $\boldsymbol{c}$ $\boldsymbol{c}(\boldsymbol{s}_1+\boldsymbol{s}_2,\boldsymbol{h}) = \boldsymbol{c}(\boldsymbol{s}_1,\boldsymbol{h})+\boldsymbol{c}(\boldsymbol{s}_2,\boldsymbol{h})$

Linearity implies homogeneity: $\boldsymbol{k}(0,\mathbf{0},\mathbf{0})=0$, $\boldsymbol{c}(\mathbf{0},\mathbf{0})=0$

Pair Encoding: Example for IBE

Param $\longrightarrow$ 2 That is, $\boldsymbol{h}=(h_1,h_2)$

Enc1(ID) $\longrightarrow$ $\boldsymbol{k}(a,r,\boldsymbol{h}) = (\ a+r(h_1+h_2 ID)\ ,\ \ r)$

Enc2(ID') $\longrightarrow$ $\boldsymbol{c}(s,\boldsymbol{h}) = (\ s\ ,\ \ s(h_1+h_2 ID')\ )$

Pair(ID,ID') $\longrightarrow$ $\boldsymbol{E} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- Correctness If $ID=ID'$

$$(a+r(h_1+h_2 ID), r)\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} s \\ s(h_1+h_2 ID') \end{pmatrix} = as$$

Composite-order Bilinear Groups

G, G_T of order $N=p_1p_2p_3$

with bilinear map e: $G \times G \rightarrow G_T$

have prime-order subgroups G_1, G_2, G_3

Orthogonality: $e(g_i, g_j)=1$ iff $i \neq j$

Subgroup Decision: Decide if $T \in G_1$ or $T \in G_{12}$

Constructing FE from Pair Encoding

FE for predicate *R* from Pair encoding for *R*

Setup $\longrightarrow$ $PK=(g_1, g_1^{\mathbf{h}}, e(g_1,g_1)^{a}, g_3)$, $MSK=a$

Encrypt(*Y*,*M*,*PK*) $\longrightarrow$ $CT=(g_1^{\mathbf{c}(\mathbf{s},\mathbf{h})}, e(g_1,g_1)^{as}M)$

Enc2(*Y*)=**c**(**s**,**h**)

KeyGen(*X*,*MSK*) $\longrightarrow$ $SK=g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot \mathbf{R}_3$

Enc1(*X*)=**k**(*a*,**r**,**h**)

Decrypt(*CT*,*SK*) $\longrightarrow$ $\mathbf{e}(g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})\mathbf{E}}, g_1^{\mathbf{c}(\mathbf{s},\mathbf{h})} \cdot \mathbf{R}_3)$

$= e(g_1,g_1)^{as}$

$\mathbf{k}(a,\mathbf{r},\mathbf{h})\ \mathbf{E}\ \mathbf{c}(\mathbf{s},\mathbf{h})^{\mathsf{T}} = as$

Security Proof of Our Framework

Semi-functional Ciphertexts/Keys

Can Be Defined in Terms of Pair Encoding Scheme

$g_1^{\mathbf{c}(\mathbf{s},\mathbf{h})} \cdot g_2^{\mathbf{c}(0,0)=0}$

$g_1^{\mathbf{c}(\mathbf{s},\mathbf{h})} \cdot g_2^{\mathbf{c}(\hat{\mathbf{s}},\hat{\mathbf{h}})}$

$e(g_1,g_1)^{as}$ unmodified

$g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(0,\mathbf{0},\mathbf{0})=0}$

$g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(0,\hat{\mathbf{r}},\hat{\mathbf{h}})}$

$g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(\hat{a},\hat{\mathbf{r}},\hat{\mathbf{h}})}$

$g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(\hat{a},\mathbf{0},\mathbf{0})}$

Each randomness except “semi-param” $\hat{\mathbf{h}}$ is fresh for each.

Semi-functional Ciphertexts/Keys

Can Be Defined in Terms of Pair Encoding Scheme

C $g_1^{\mathbf{c}(\mathbf{s},\mathbf{h})} \cdot g_2^{\mathbf{c}(0,0)=0}$

C $g_1^{\mathbf{c}(\mathbf{s},\mathbf{h})} \cdot g_2^{\mathbf{c}(\hat{\mathbf{s}},\hat{\mathbf{h}})}$

$e(g_1,g_1)^{as}$ unmodified

K $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(0,\mathbf{0},\mathbf{0})=0}$

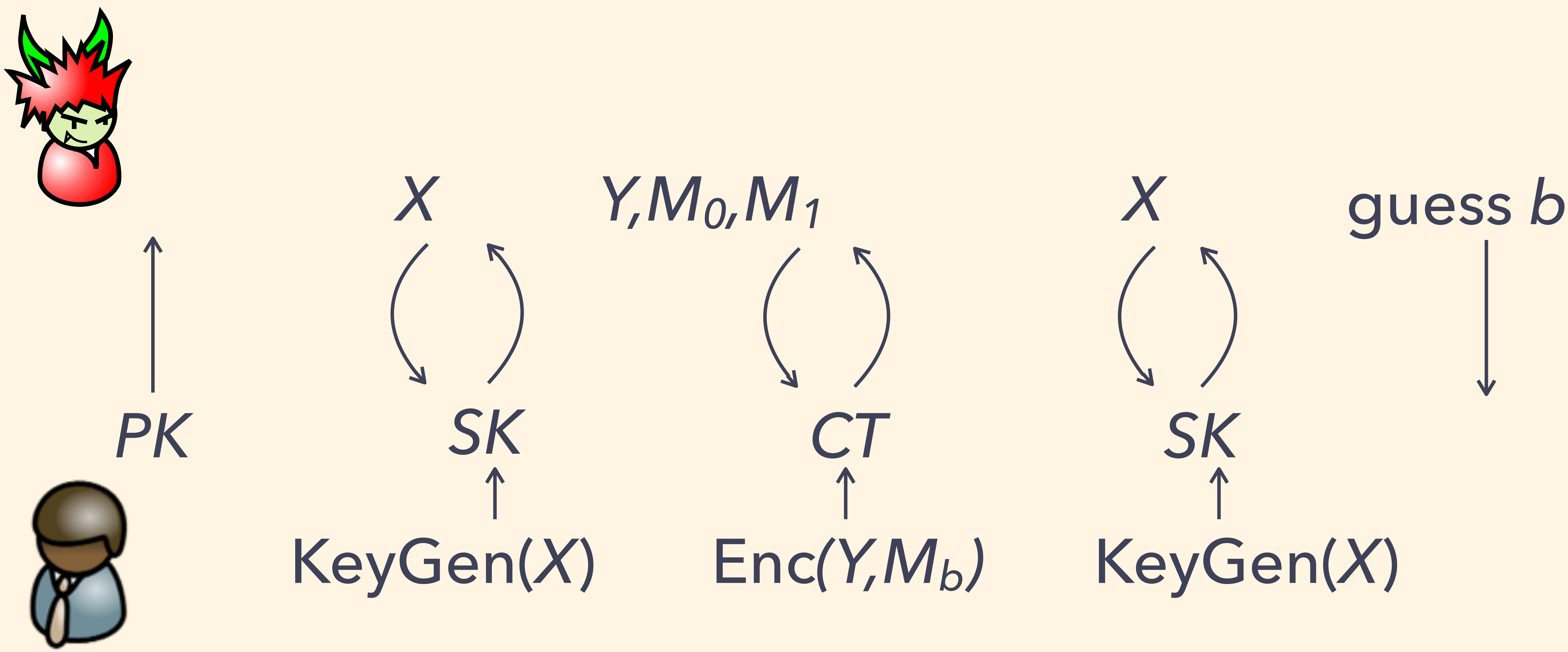
K1 $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(0,\hat{\mathbf{r}},\hat{\mathbf{h}})}$

K2 $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(\hat{a},\hat{\mathbf{r}},\hat{\mathbf{h}})}$

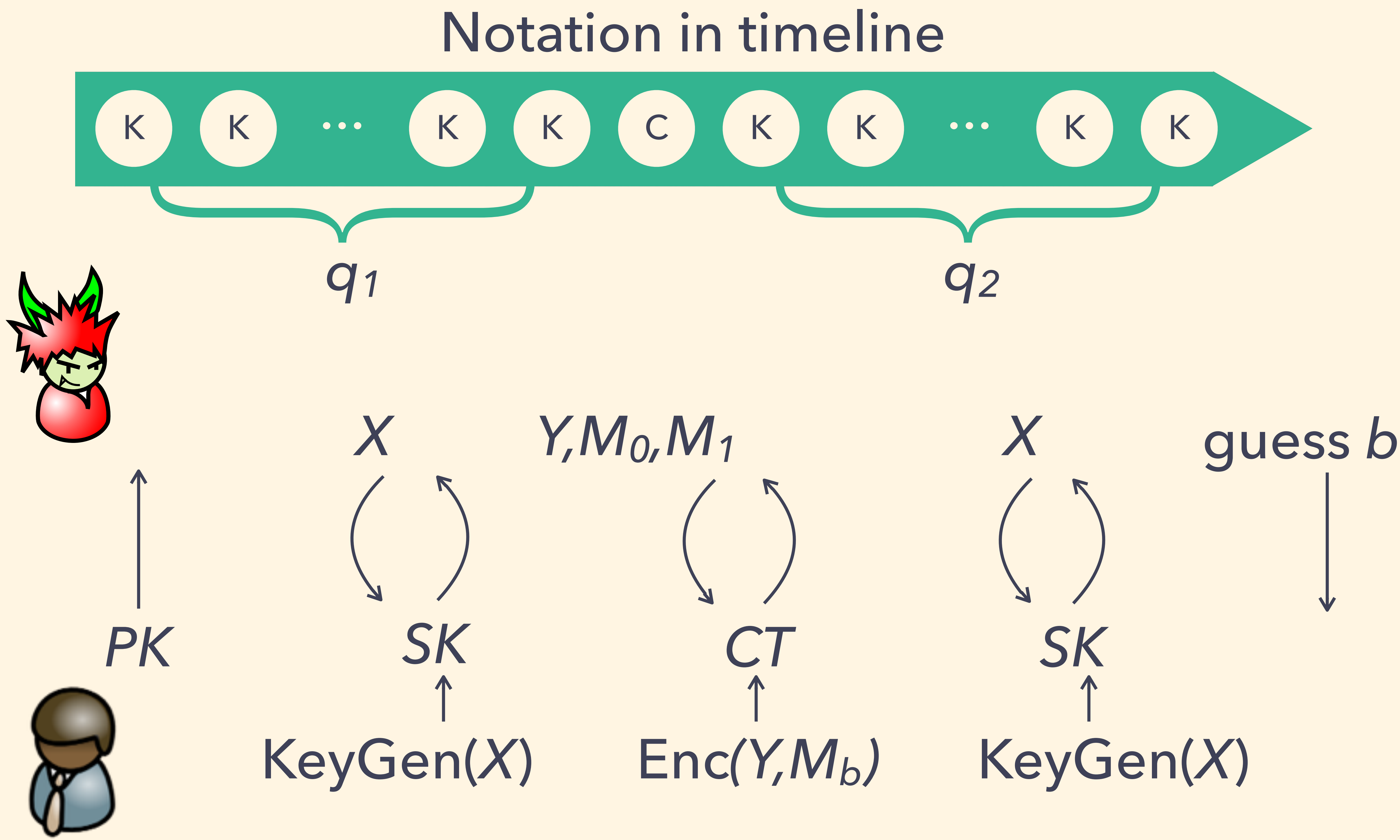
K3 $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(\hat{a},\mathbf{0},\mathbf{0})}$

Each randomness except "semi-param" $\hat{\mathbf{h}}$ is fresh for each.

Recall Definition for Full Security

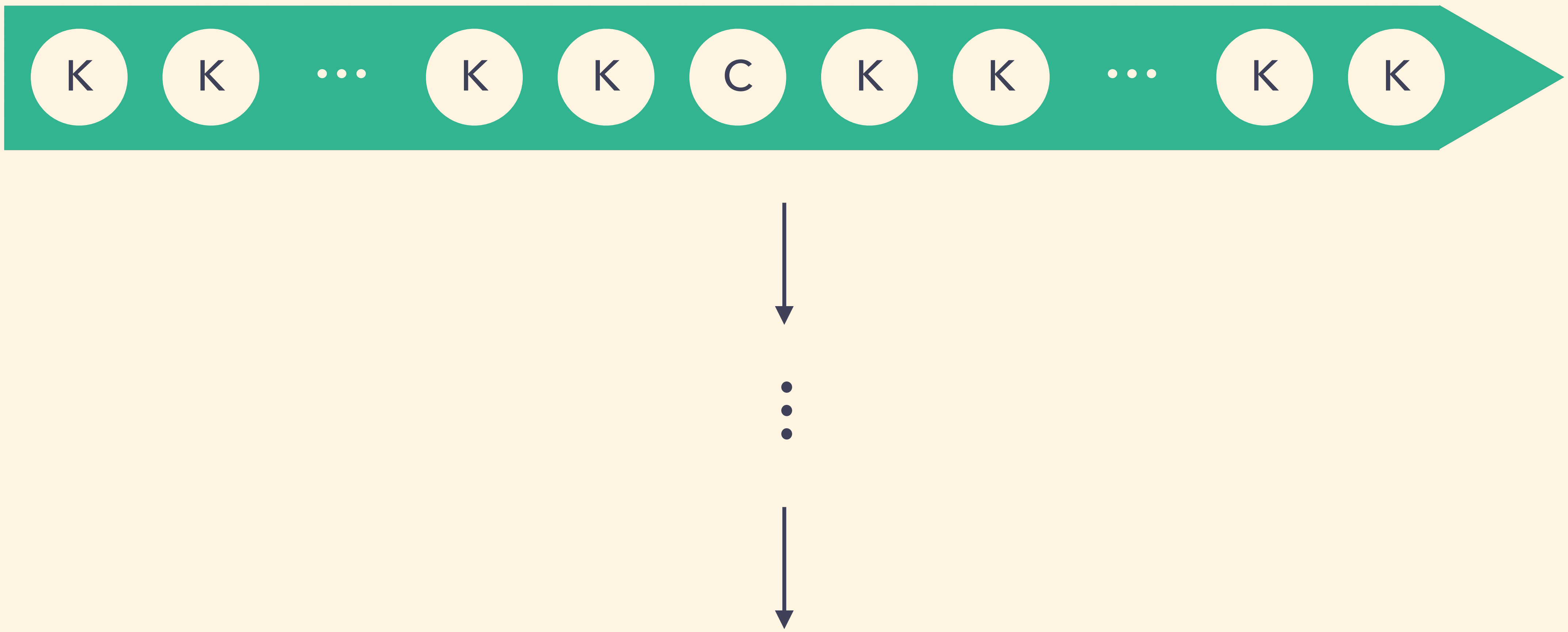


Recall Definition for Full Security

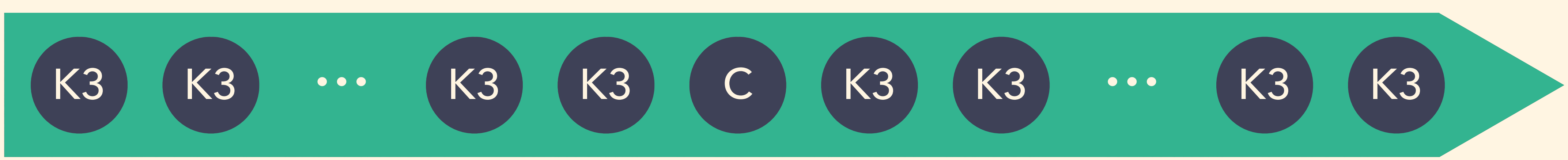


Aim of the Proof

Real game: all normal



Final game: all semi-functional

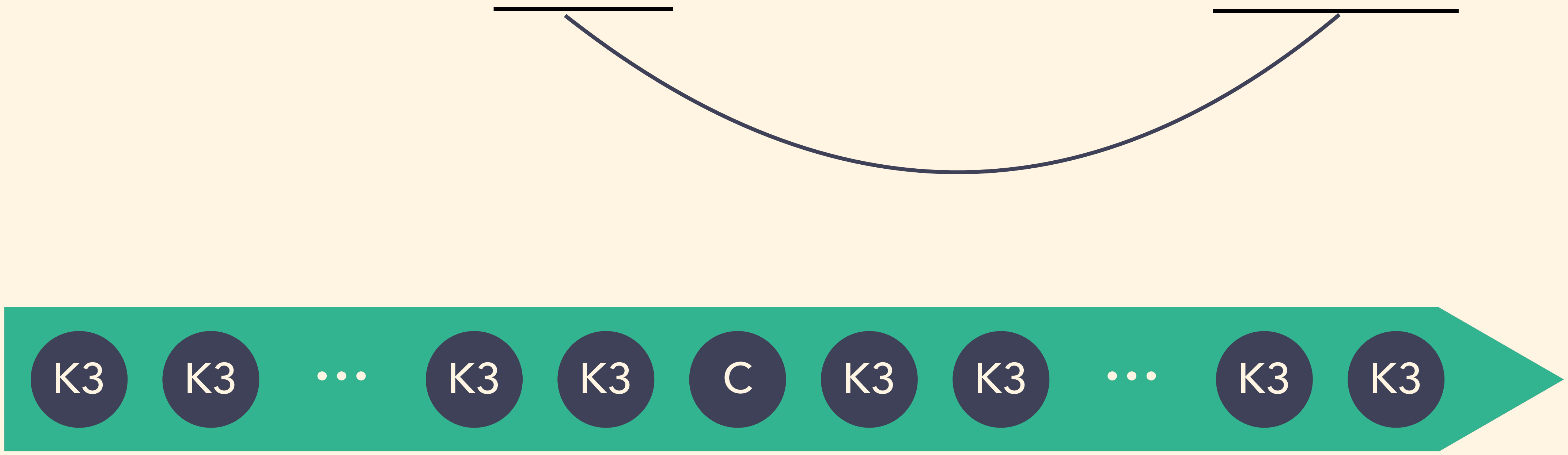


Final Game

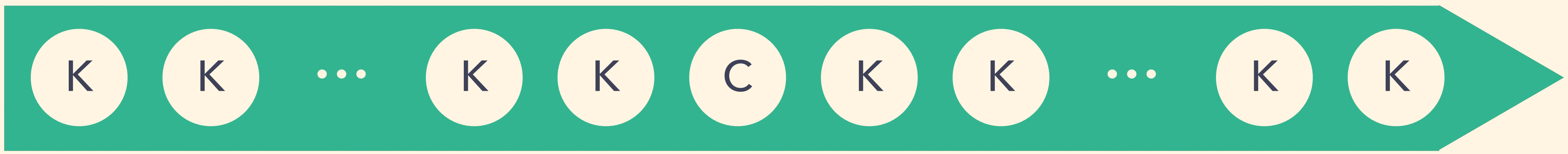
Adversary will have no advantage.

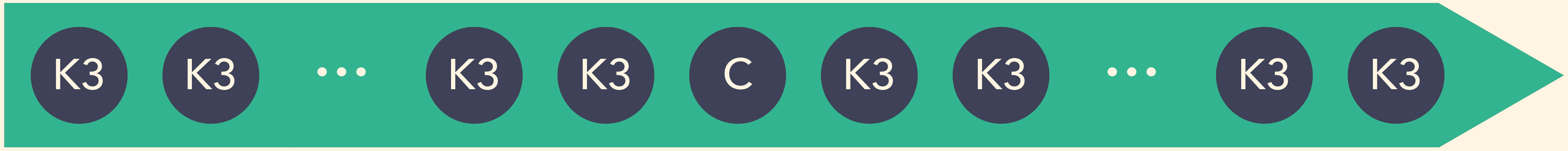
Intuition: decryption contains random $e(g_2,g_2)^{\hat{a}\hat{s}}$

C $g_1^{\mathbf{c}(\mathbf{s},\mathbf{h})} \cdot \underline{g_2^{\mathbf{c}(\hat{\mathbf{s}},\hat{\mathbf{h}})}}$ K3 $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot \underline{g_2^{\mathbf{k}(\hat{a},\mathbf{0},\mathbf{0})}}$

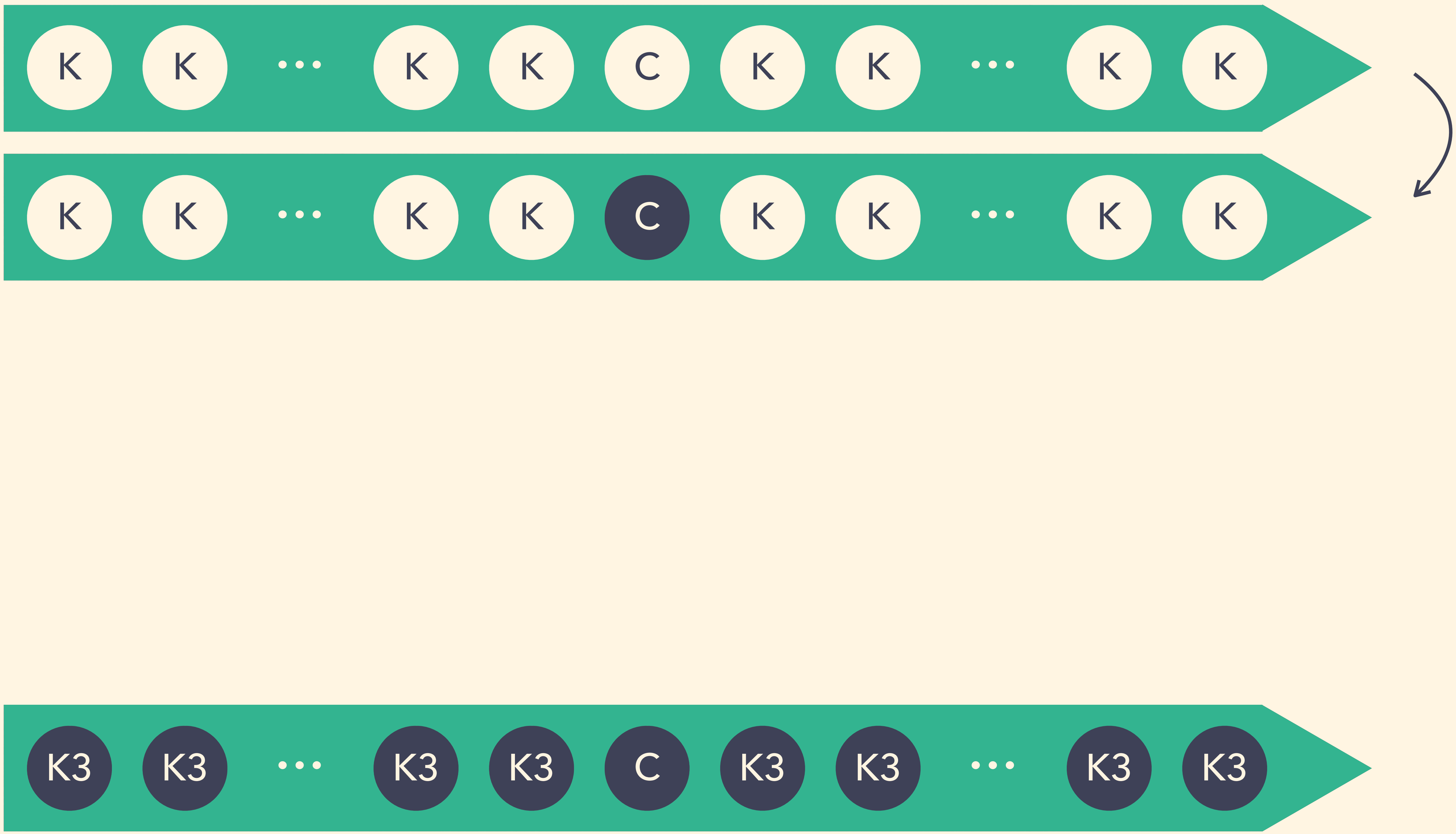


Game Sequence in the Proof

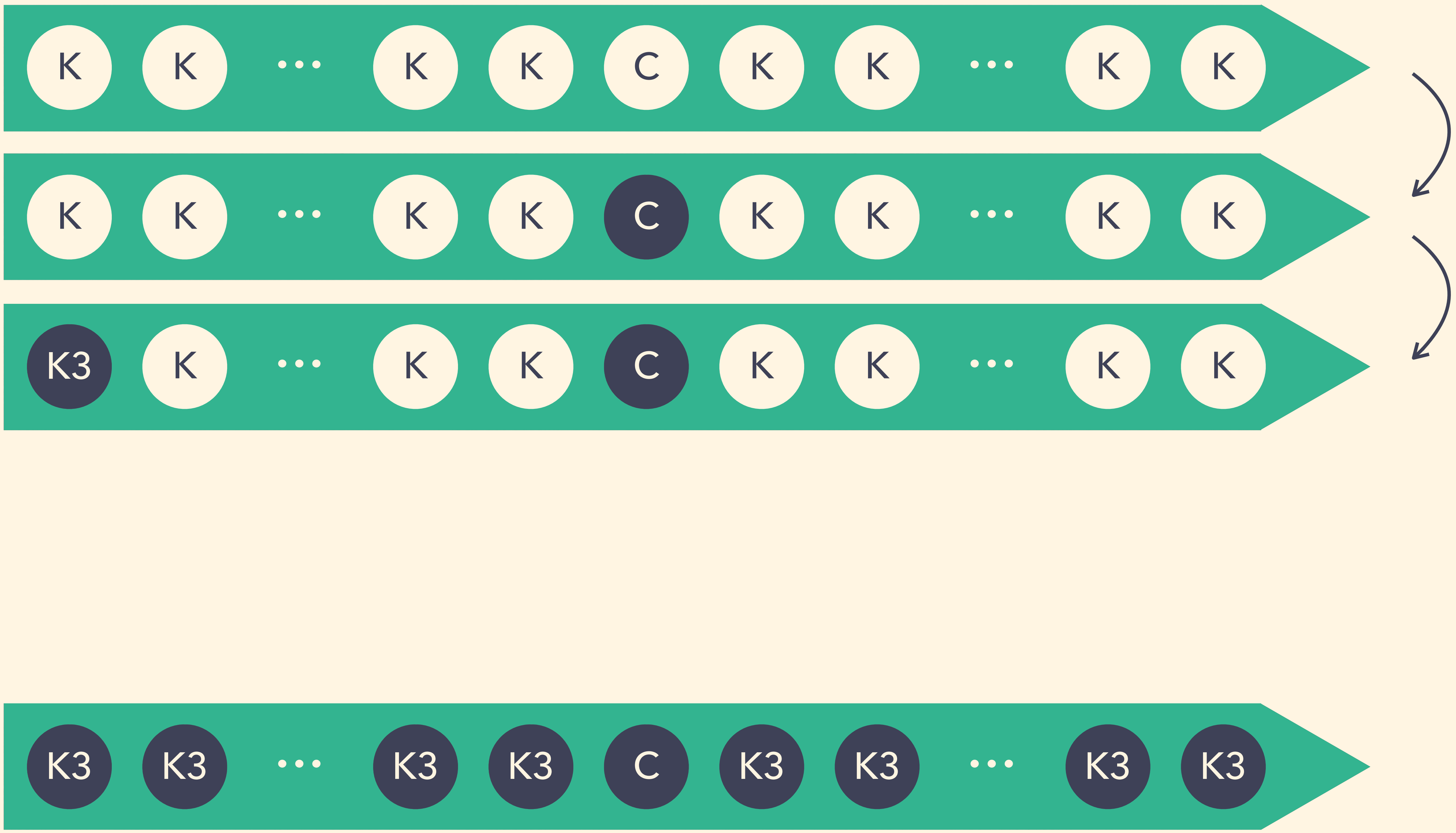




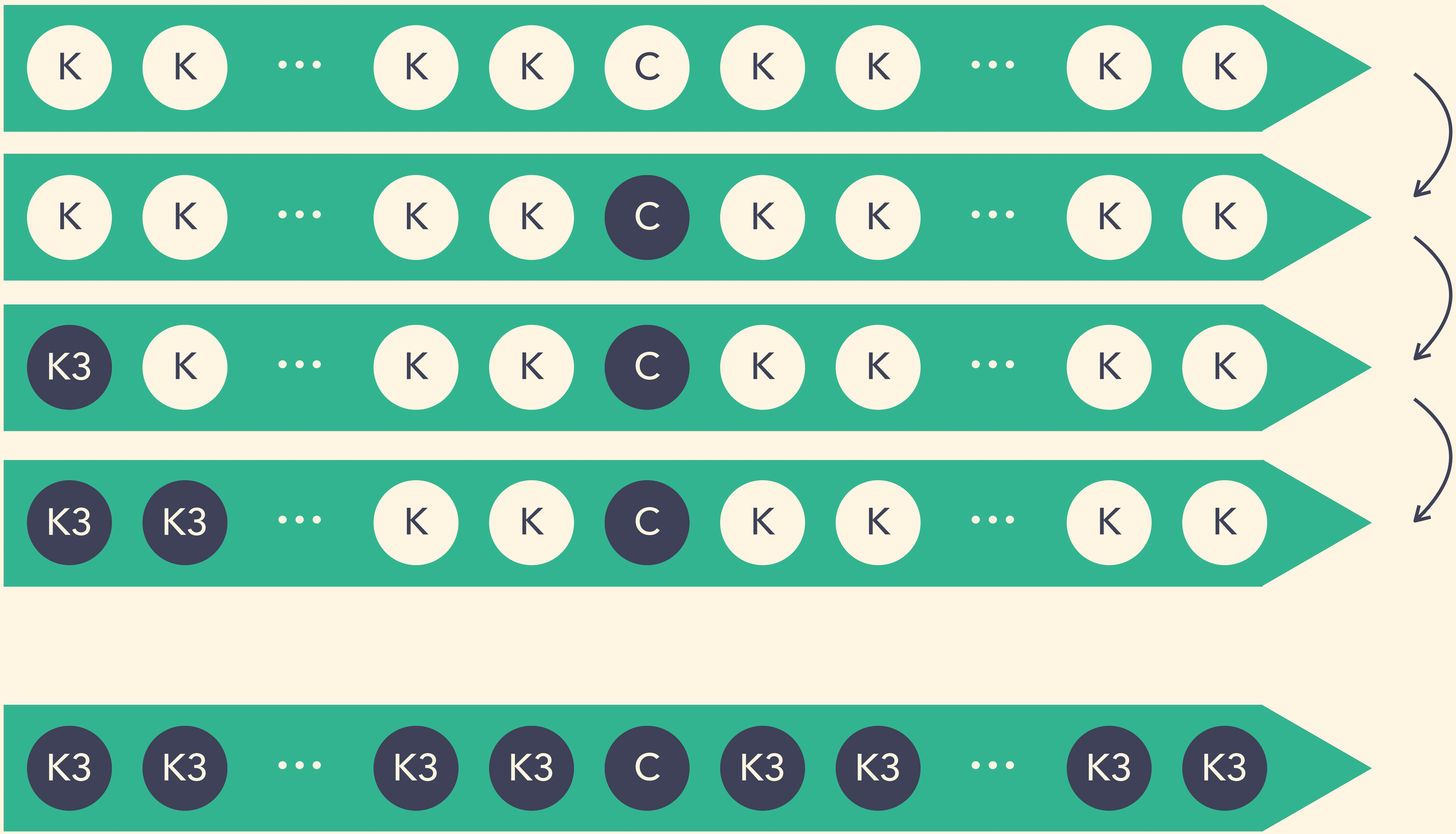
Game Sequence in the Proof



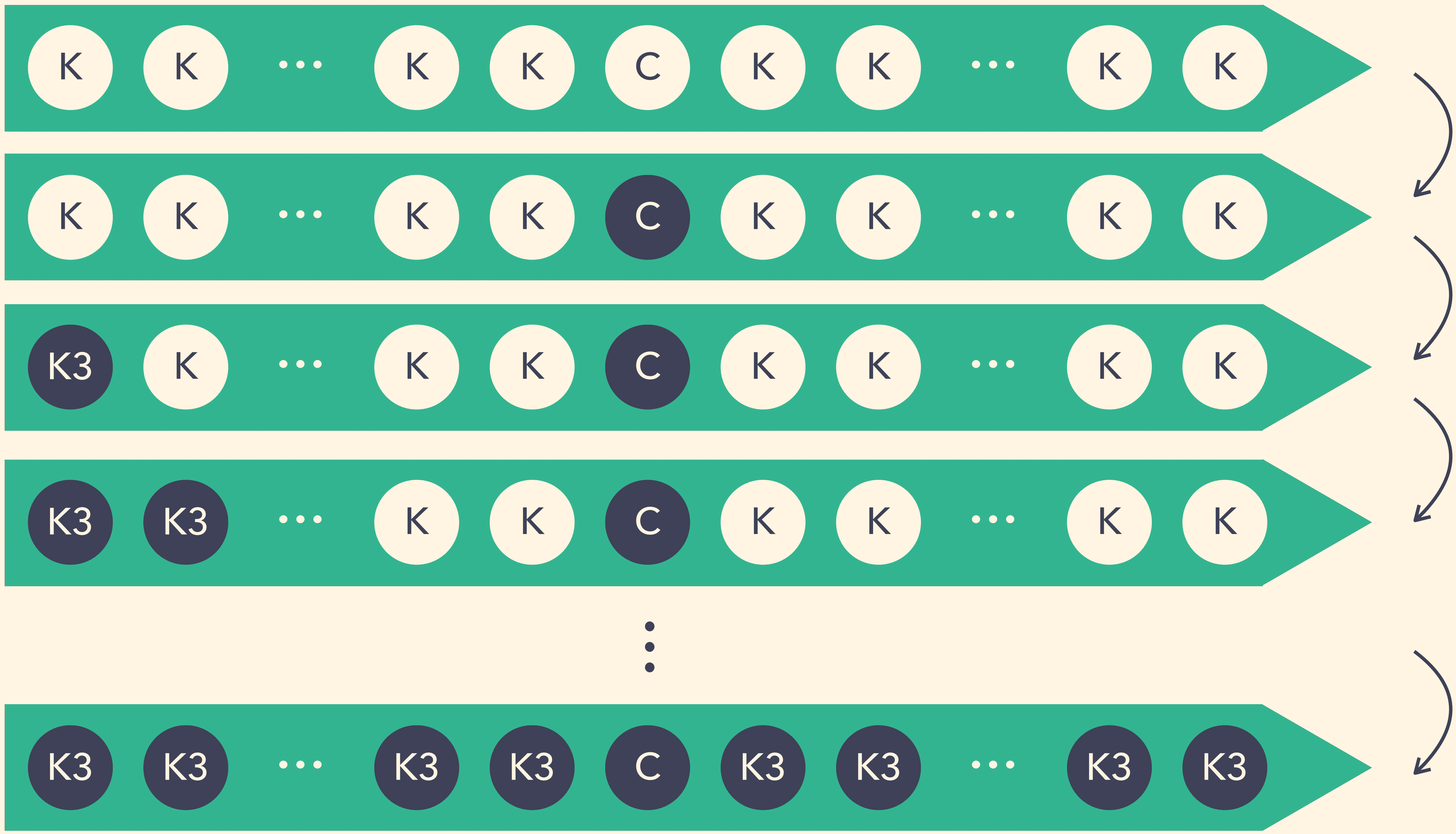
Game Sequence in the Proof



Game Sequence in the Proof

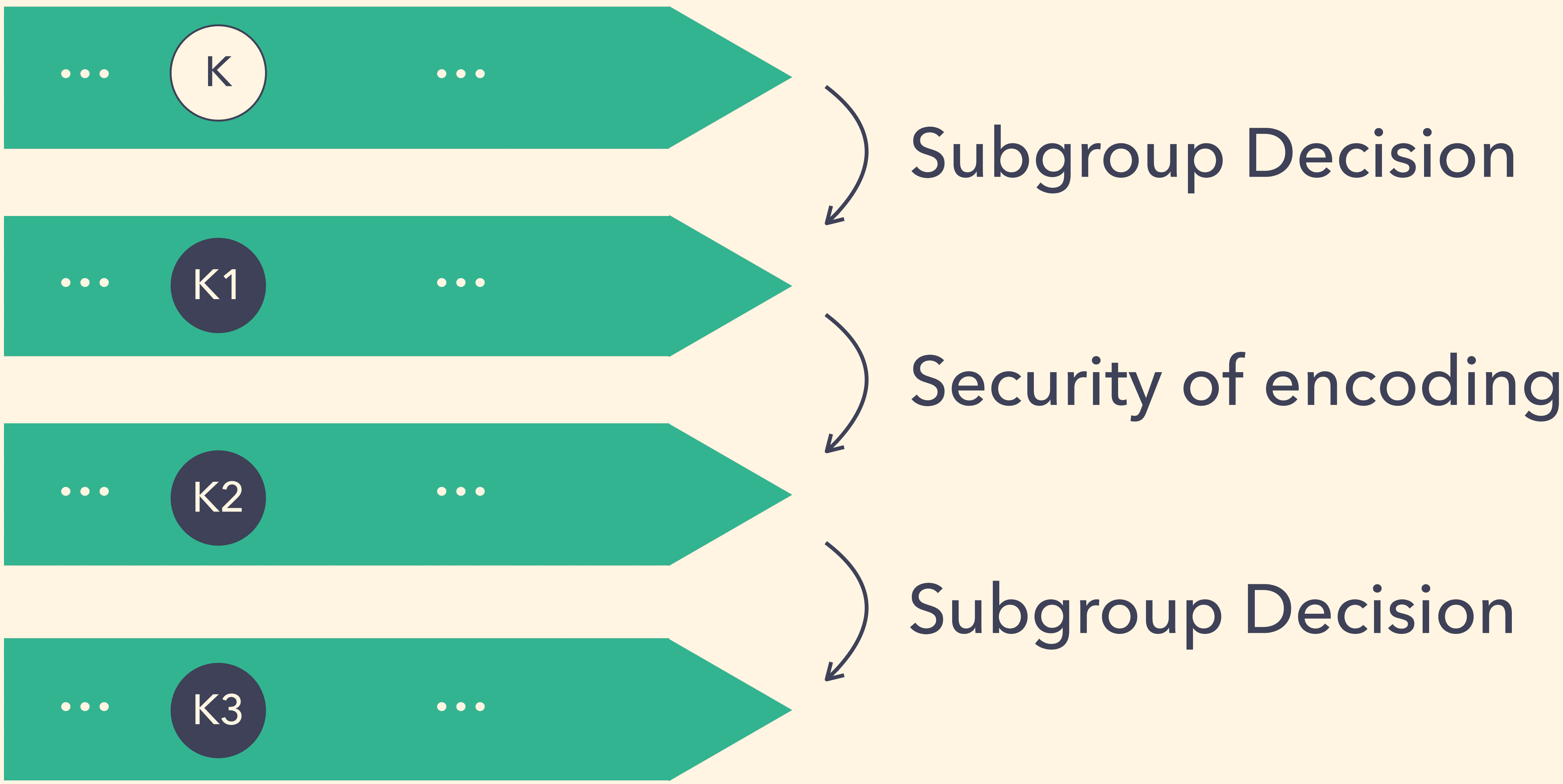


Game Sequence in the Proof

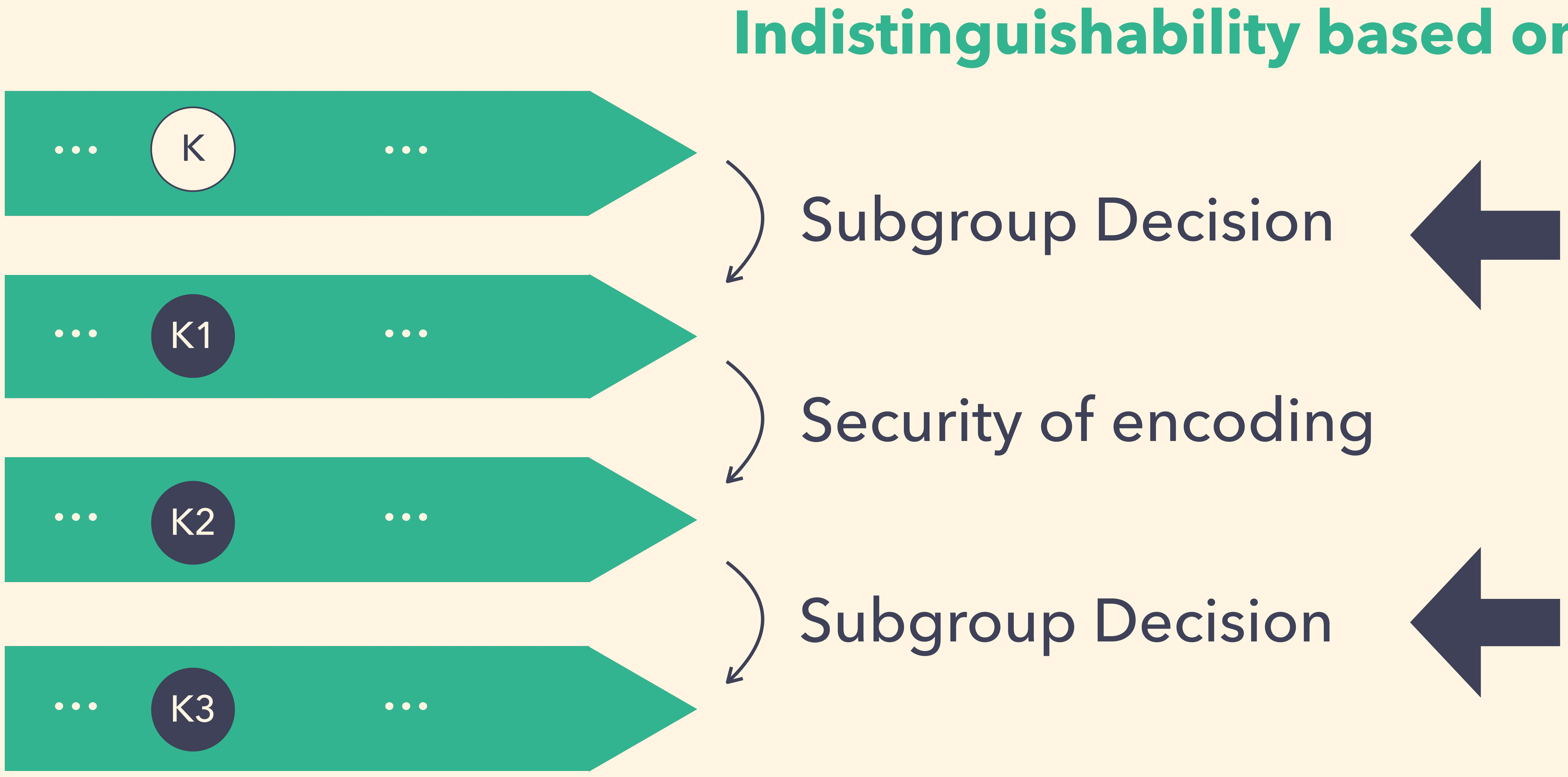


Game Subsequence

Indistinguishability based on



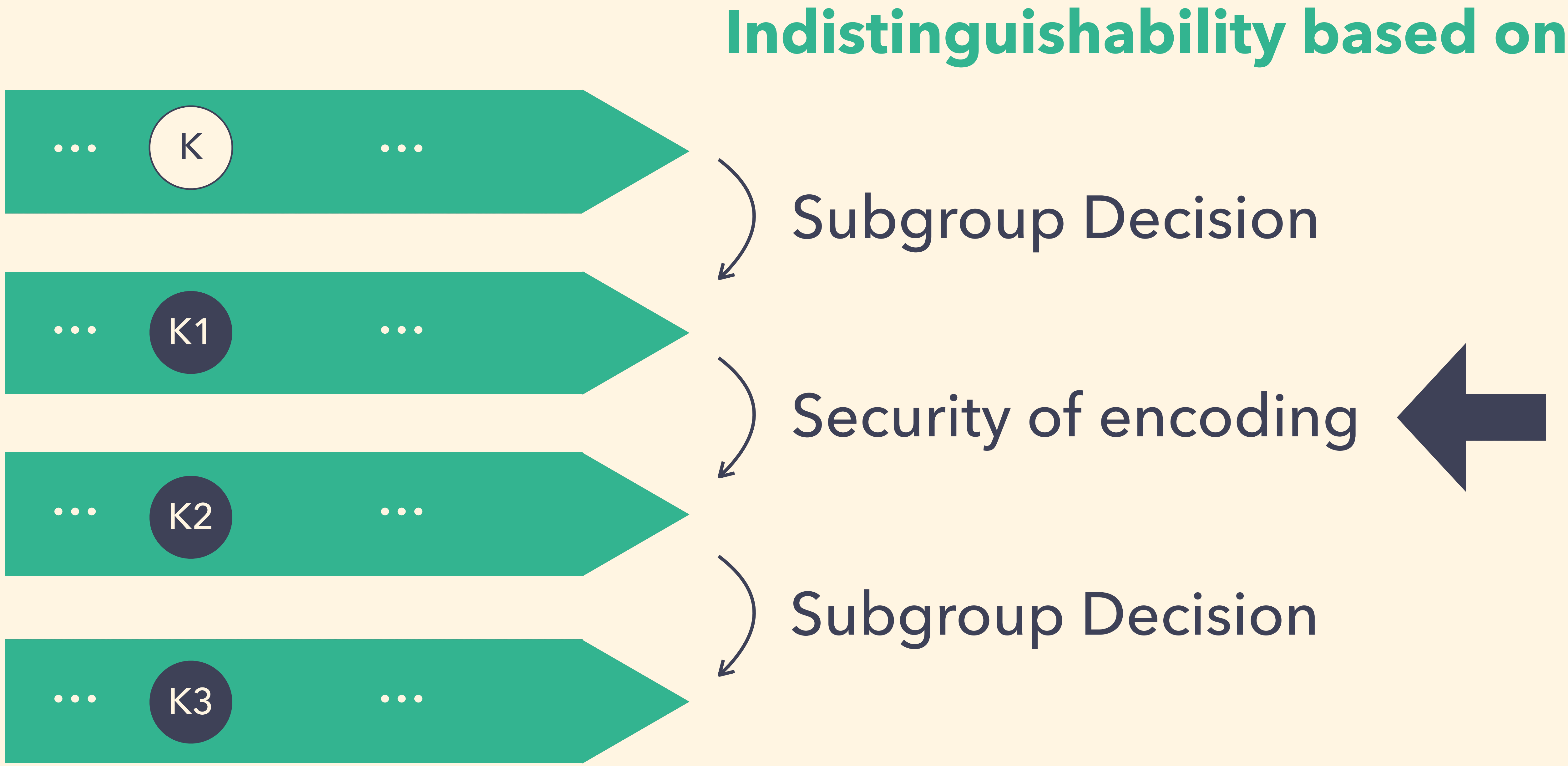
Game Subsequence



Intuition: These two do not depend on encoding.

Use linearity, param-vanishing of ***k*** and orthogonality of *G*.

Game Subsequence



The 2nd Transition

K1 $g_1^{\boldsymbol{k}(a,\boldsymbol{r},\boldsymbol{h})} \cdot g_2^{\boldsymbol{k}(0,\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$

K2 $g_1^{\boldsymbol{k}(a,\boldsymbol{r},\boldsymbol{h})} \cdot g_2^{\boldsymbol{k}(\hat{a},\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$

Security of encoding

(to be defined)

The 2nd Transition

K1 $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(0,\hat{\mathbf{r}},\hat{\mathbf{h}})}$

K2 $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(\hat{a},\hat{\mathbf{r}},\hat{\mathbf{h}})}$

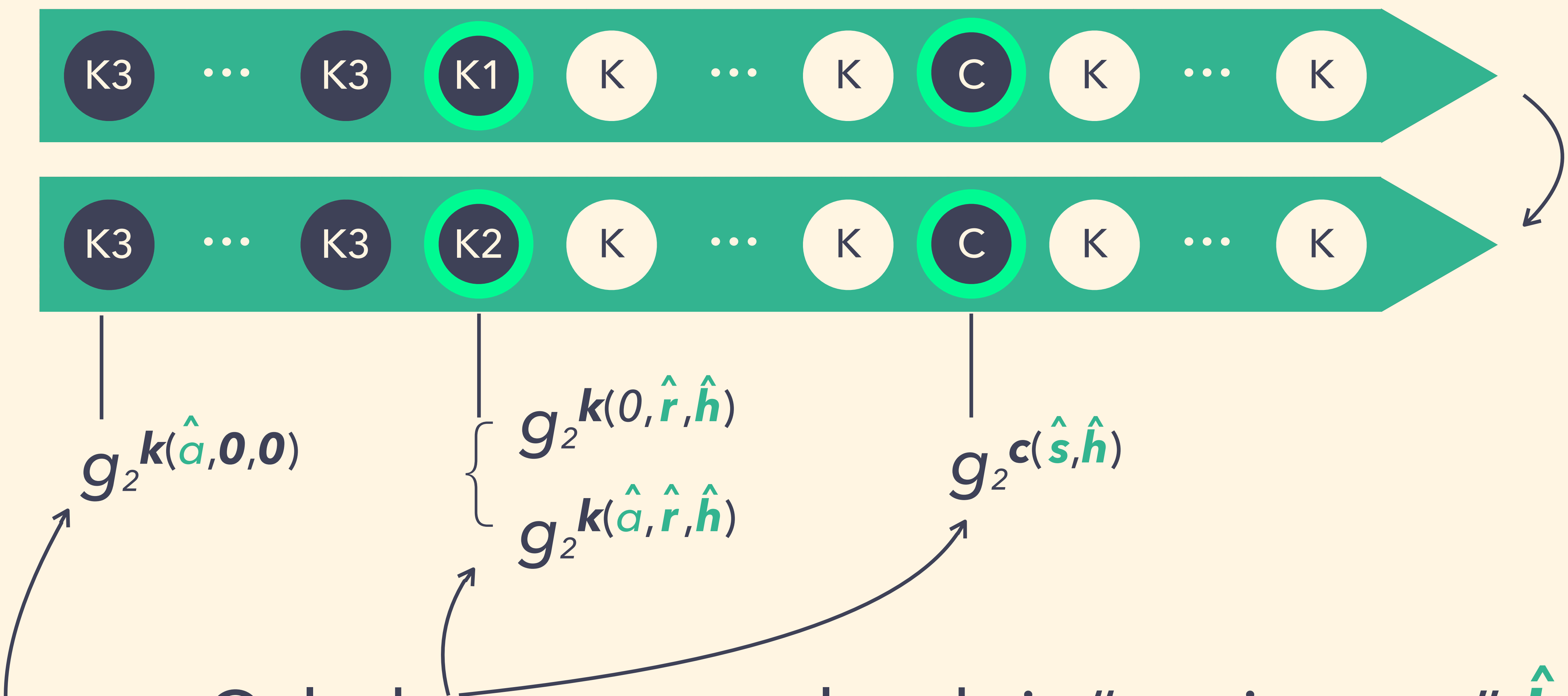
Security of encoding

(to be defined)

Idea: just define security of encoding to be exactly the indistinguishability of these two games!

The 2nd Transition

In More Details



- Only these are correlated via "semi-param" $\hat{h}$.
- "Isolating" all other keys.

Defining Security of Encoding

Computationally secure encoding

Cannot distinguish

$$\left\{\begin{array}{l} g_2^{\mathbf{k}(0,\hat{r},\hat{h})} \\ g_2^{\mathbf{k}(\hat{a},\hat{r},\hat{h})} \end{array}\right.$$

$$g_2^{\mathbf{c}(\hat{s},\hat{h})}$$

Defining Security of Encoding

Perfectly secure encoding

Identical (info-theoretic) $\left\{ \begin{array}{l} \boldsymbol{k}(0, \hat{\boldsymbol{r}}, \hat{\boldsymbol{h}}) \\ \boldsymbol{k}(a, \hat{\boldsymbol{r}}, \hat{\boldsymbol{h}}) \end{array} \right.$

$$\boldsymbol{c}(\hat{\boldsymbol{s}}, \hat{\boldsymbol{h}})$$

Computationally secure encoding

Cannot distinguish ← $\left\{ \begin{array}{l} g_2^{\boldsymbol{k}(0, \hat{\boldsymbol{r}}, \hat{\boldsymbol{h}})} \\ g_2^{\boldsymbol{k}(\hat{a}, \hat{\boldsymbol{r}}, \hat{\boldsymbol{h}})} \end{array} \right.$

$$g_2^{\boldsymbol{c}(\hat{\boldsymbol{s}}, \hat{\boldsymbol{h}})}$$

Defining Security of Encoding

Perfectly secure encoding

Identical (info-theoretic)

$$\left\{ \begin{array}{l} \boldsymbol{k}(0, \hat{\boldsymbol{r}}, \hat{\boldsymbol{h}}) \\ \boldsymbol{k}(a, \hat{\boldsymbol{r}}, \hat{\boldsymbol{h}}) \end{array} \right. \qquad \boldsymbol{c}(\hat{\boldsymbol{s}}, \hat{\boldsymbol{h}})$$

Computationally secure encoding

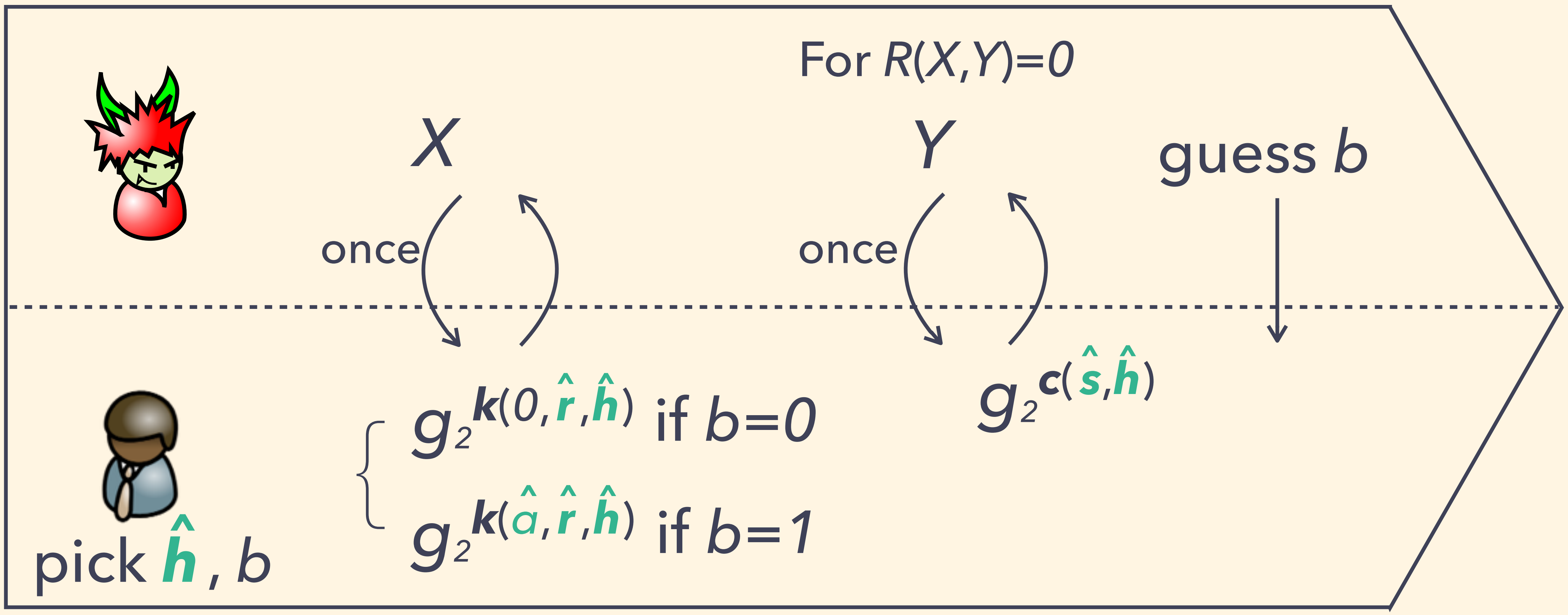
Cannot distinguish ←

$$\left\{ \begin{array}{l} g_2^{\boldsymbol{k}(0, \hat{\boldsymbol{r}}, \hat{\boldsymbol{h}})} \\ g_2^{\boldsymbol{k}(\hat{a}, \hat{\boldsymbol{r}}, \hat{\boldsymbol{h}})} \end{array} \right. \qquad g_2^{\boldsymbol{c}(\hat{\boldsymbol{s}}, \hat{\boldsymbol{h}})}$$

1st flavor: ***k*** before ***c***

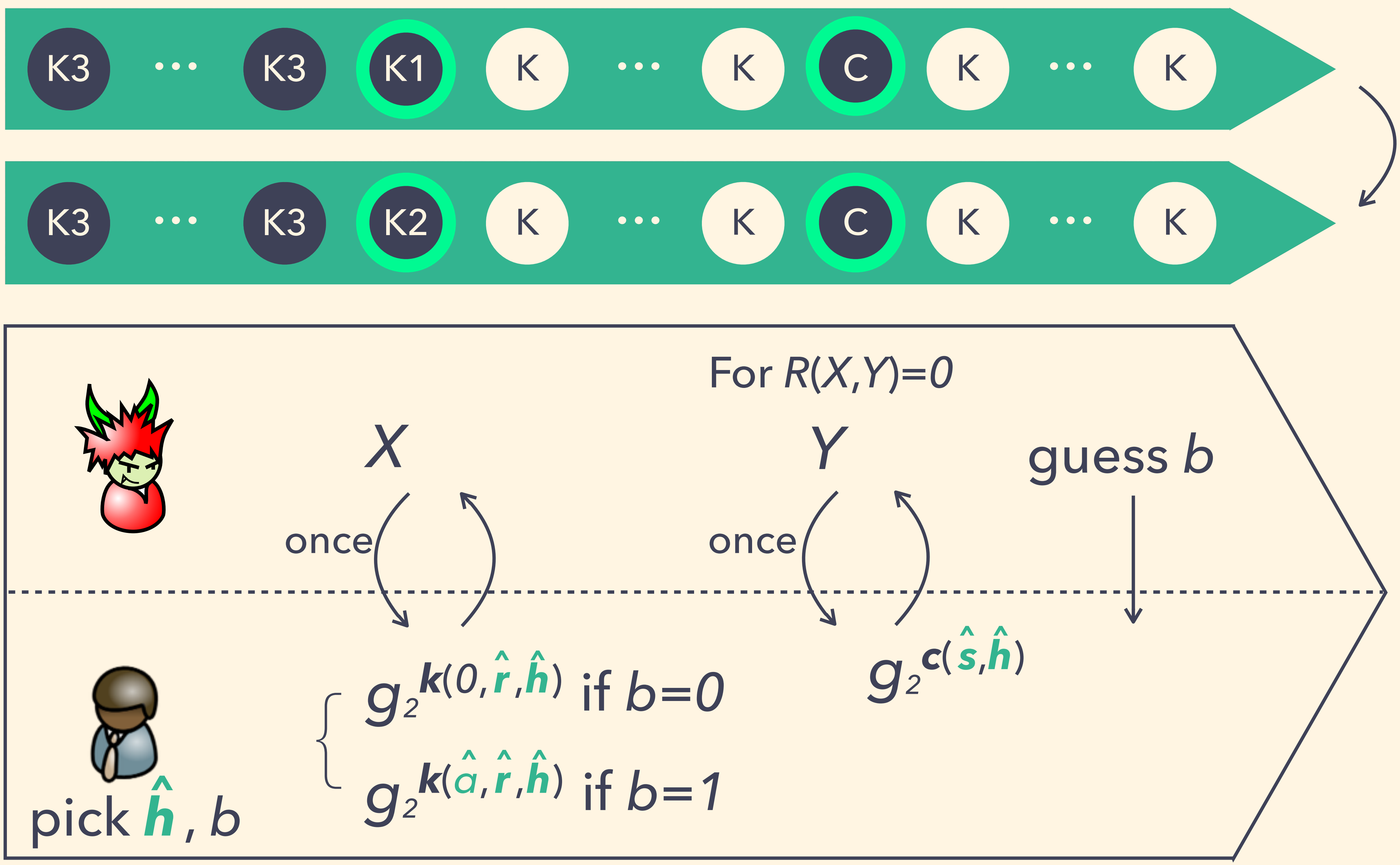
2nd flavor: ***c*** before ***k***

Computationally Security 1: *k* before *c*

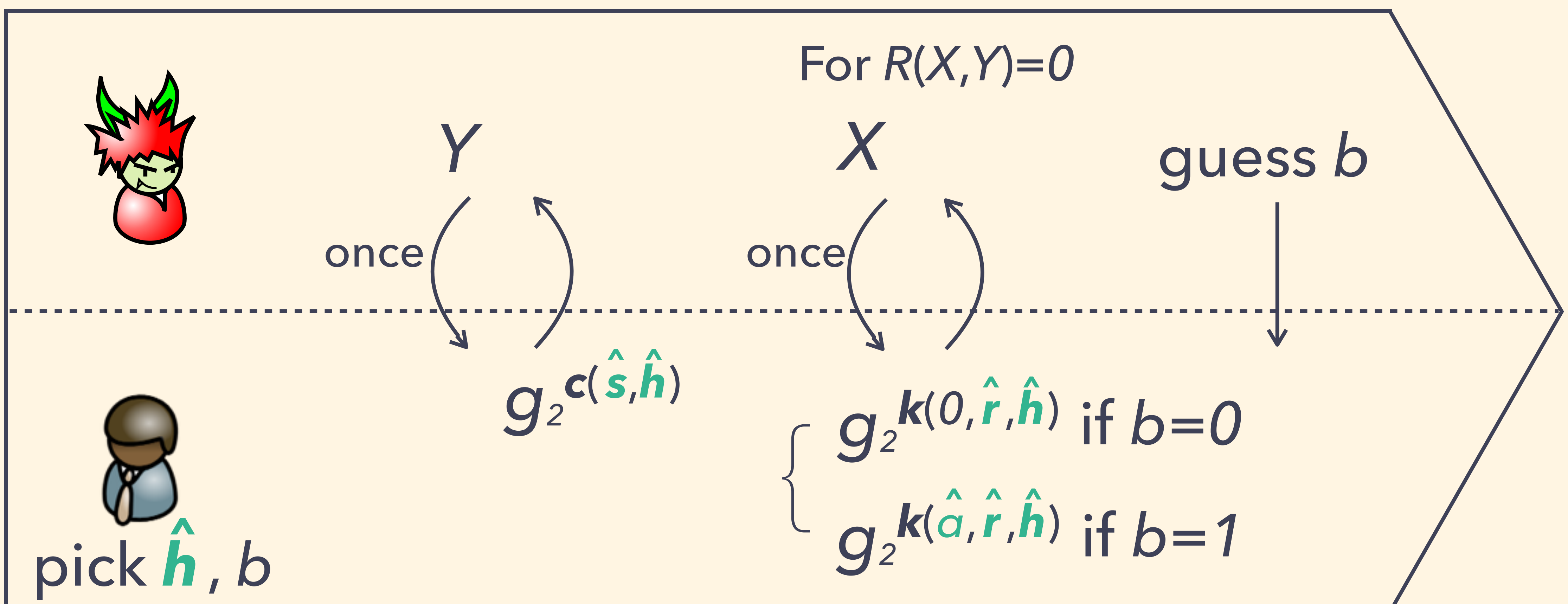


Computationally Security 1: *k* before *c*

For Transitions of *Pre-challenge Keys*

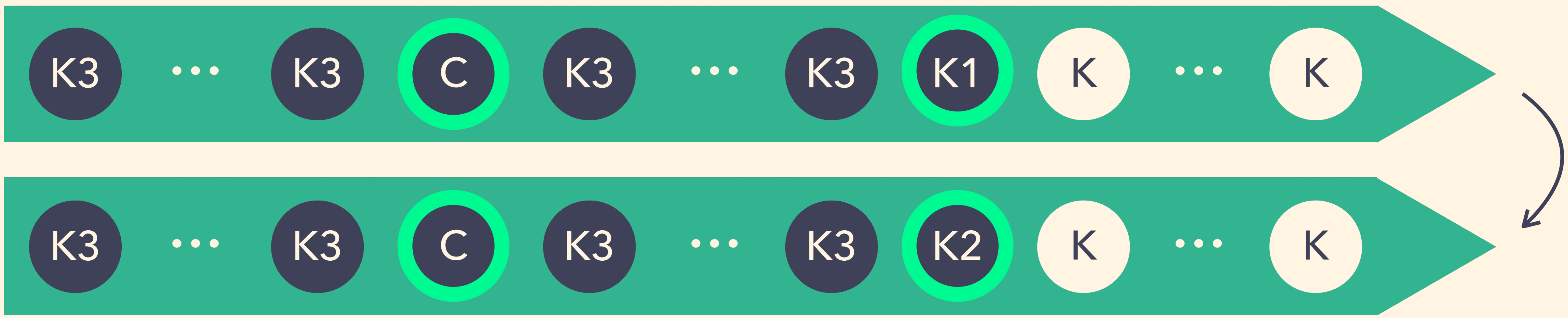


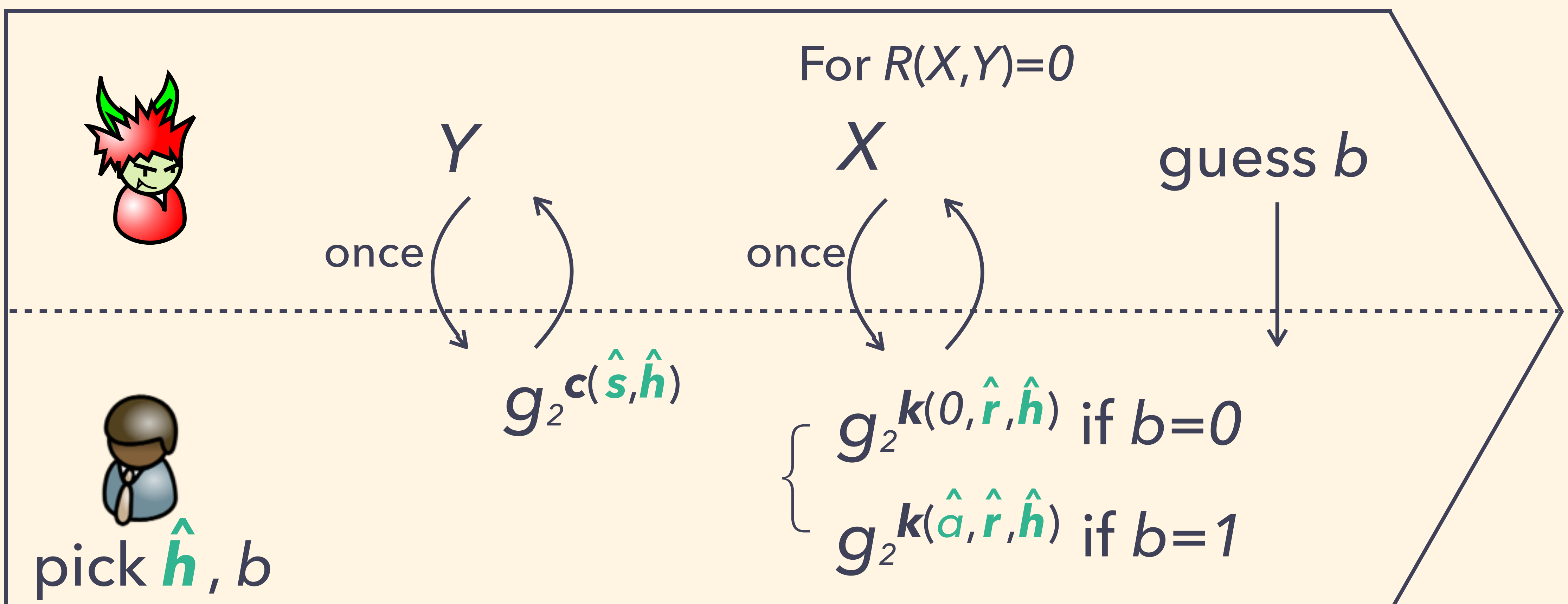
Computationally Security 2: c before *k*



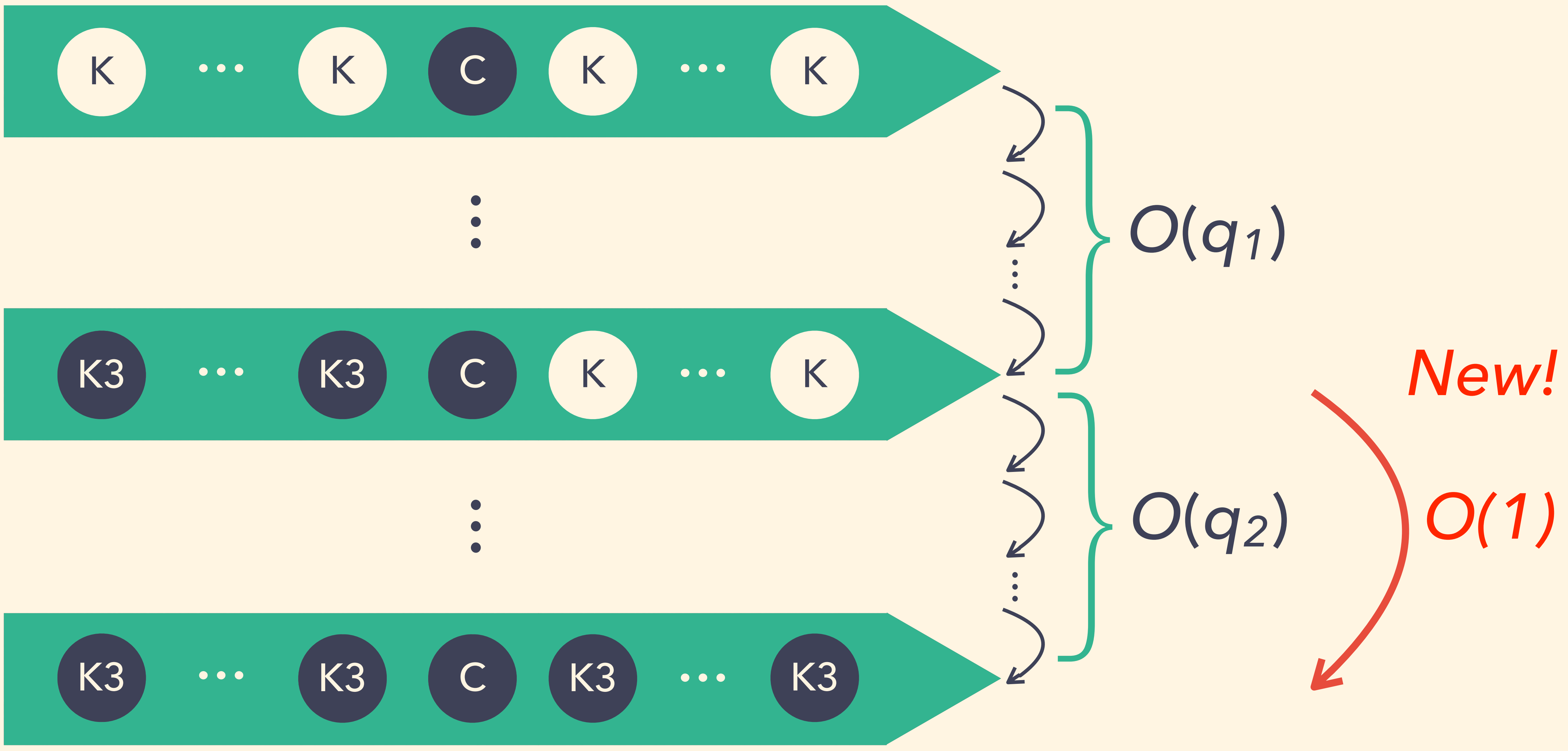
Computationally Security 2: c before *k*

For Transitions of *Post*-challenge Keys



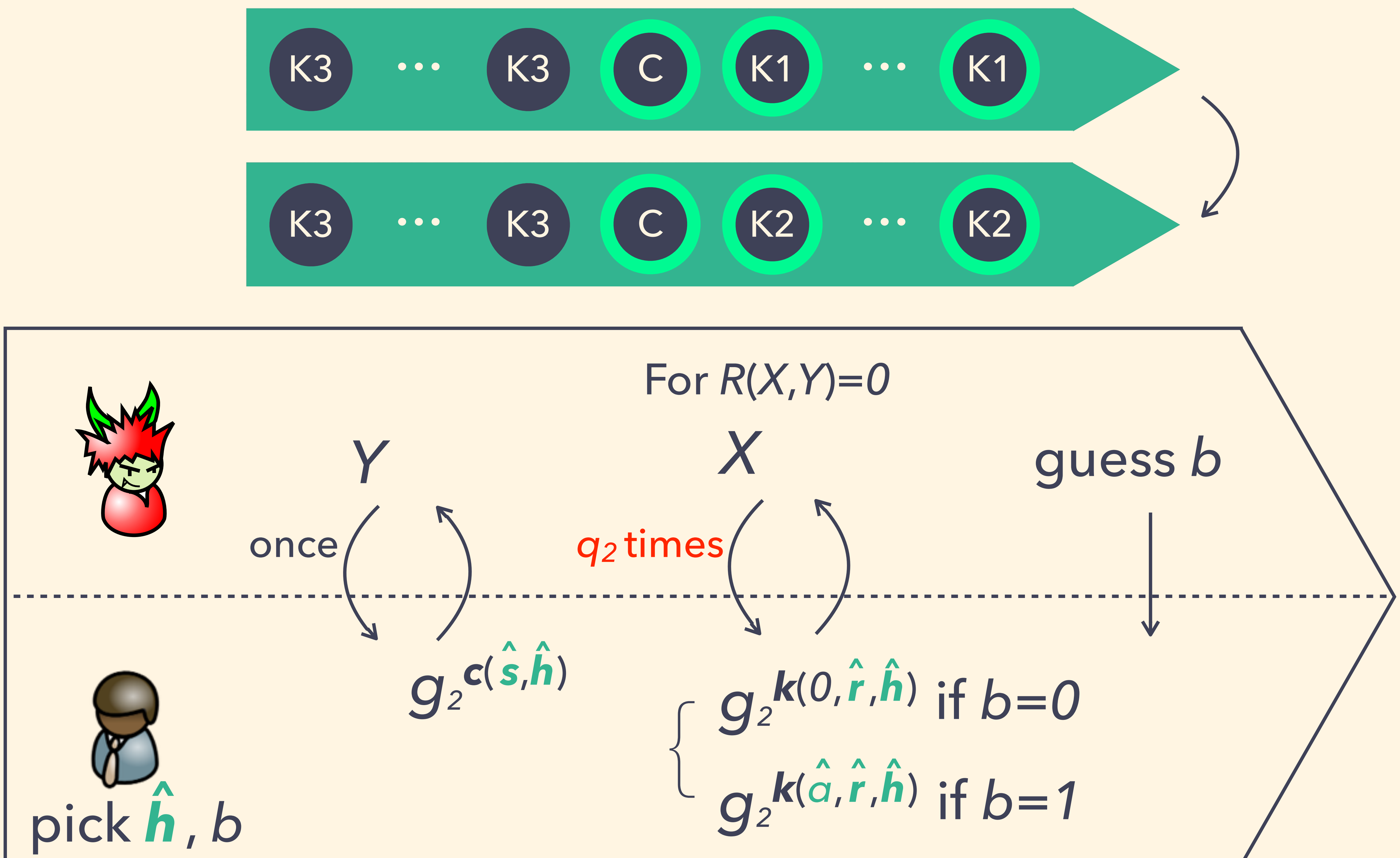


Tighter Security Proof

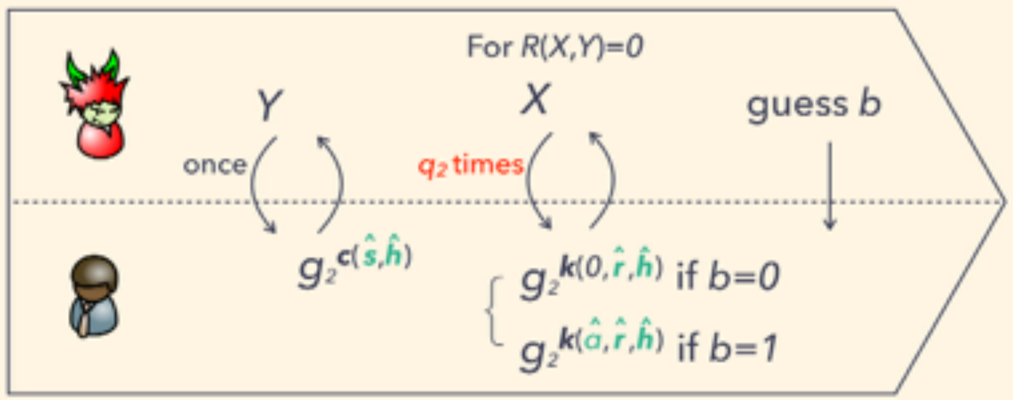


Refining Computationally Security 2

For Transitions of *Post*-challenge Keys

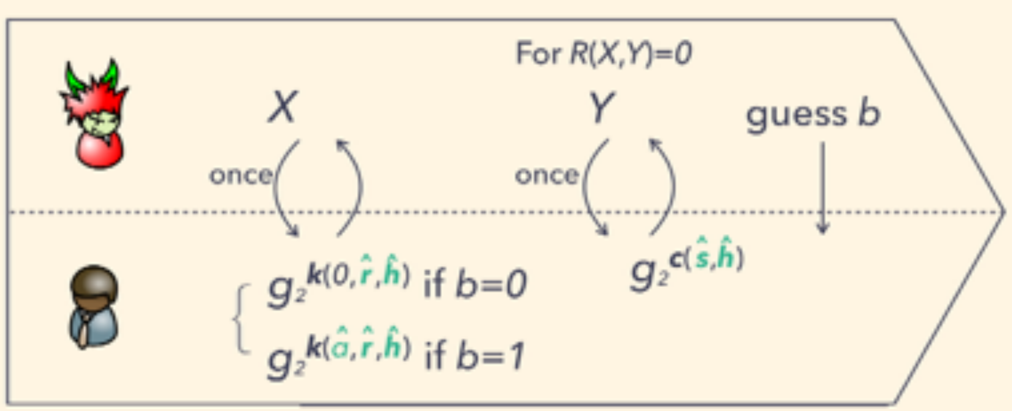


“Doubly Selective Security”



$Y \rightarrow$ program $\hat{h} \rightarrow X$

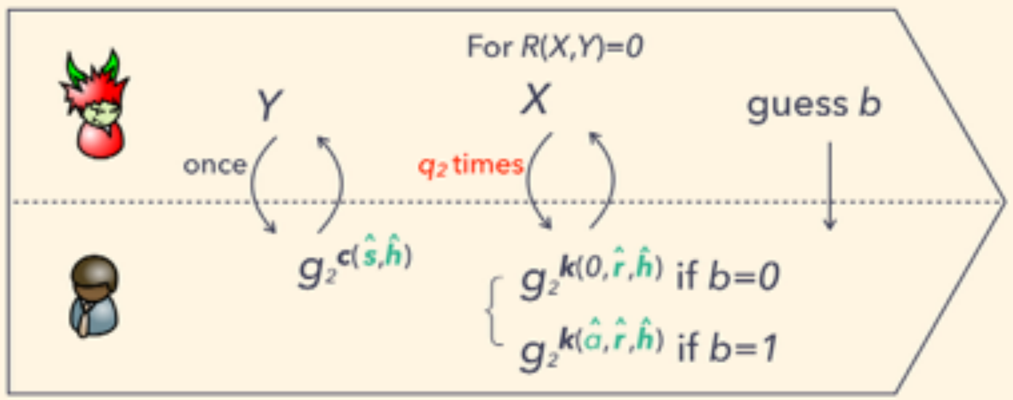
The 2nd notion is called **Selective** Master-key Hiding since the order of queries mimics selective security of FE but in semi-functional space.



$X \rightarrow$ program $\hat{h} \rightarrow Y$

The 1st notion is called **Co-Selective** Master-key Hiding since the order of queries mimics co-selective security of FE but in semi-functional space.

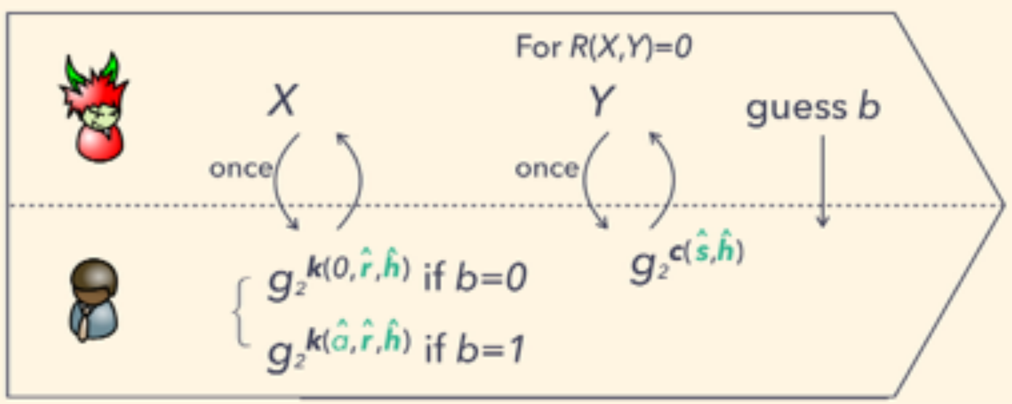
"Doubly Selective Security"



$Y \rightarrow$ program $\hat{h} \rightarrow X$

The 2nd notion is called **Selective** Master-key Hiding

Can borrow proof techniques for selective security of FE



$X \rightarrow$ program $\hat{h} \rightarrow Y$

The 1st notion is called **Co-Selective** Master-key Hiding

Can borrow proof techniques for co-selective security of FE or selective security of its dual!

3 Instantiations

Fully Secure IBE

Lewko-Waters IBE $\boldsymbol{h}=(h_1,h_2)$

$\boldsymbol{k}=(a+r(h_1+h_2ID), r)$

$\boldsymbol{c}=(s, s(h_1+h_2ID'))$

- Encoding is perfect.
  - $f(x)=h_1+h_2x$ is pair-wise independent
- Full security of IBE: $O(q_{all})$ to Subgroup Decision

Our new IBE $\boldsymbol{h}=(h_1,h_2,h_3)$

$\boldsymbol{k}=(a+r_1(h_1+h_2ID)+r_2h_3, r_1, r_2)$

$\boldsymbol{c}=(s, s(h_1+h_2ID'), sh_3)$

- Encoding is perfect.
- Encoding is also selective under 3-party DH.
- Full security of IBE: $O(q_1)$ to Subgroup Decision plus $O(1)$ to 3-party DH

Fully Secure IBE

	|Public key|	|Ciphertext|, |key|	Reduction	Assumption
Waters 05	$O(n)$	$O(1)$	$O(nq_{all})$	DBDH
Gentry 06	$O(1)$	$O(1)$	$O(1)$	q_{all}-ABDHE
Waters 09	$O(1)$	$O(1)$	$O(q_{all})$	DBDH,DLIN
Lewko-Waters 10	$O(1)$	$O(1)$	$O(q_{all})$	subgroup
Chen-Wee 13	$O(n)$	$O(1)$	$O(n)$	DLIN
Our IBE	$O(1)$	$O(1)$	$\mathbf{O(q_1)}$	3DH, subgroup

n = ID length

FE for Regular Languages

	Security	Reduction	Assumption
Waters 12	selective	$O(1)$	Q-type
Our FE for regular languages	**full**	$O(q_1)$	Q-type, subgroup

FE for Regular Languages

Selective security of our encoding

- Borrow techniques from selective security of Waters'.
- Hence, use a similar "Q-type" assumption to Waters'.
  - Q is ciphertext attribute size of *one query*.
  - Q is *not* the number of queries (q_1,q_2).

Co-selective security of our encoding

- New techniques, new Q-type assumption.

KP-ABE with Short Ciphertext

	Ciphertext size	Key size	Security	Reduction	Assumption
A.-Libert-Panafieu 11	$O(1)$	$O(tk)$	selective	$O(1)$	Q-type
Takashima 14	$O(1)$	$O(tk)$	selective	$O(q_{all})$	DLIN
Our ABE w/ short ciphertext	$O(1)$	$O(tk)$	**full**	$O(q_1)$	Q-type, subgroup

t = max attribute set in ciphertext,   k= policy size for key

Unbounded KP-ABE

	Large universe ?	Unbounded attribute repetition?	Security	Reduction	Assumption
Lewko-Waters 11	yes	yes	selective	$O(q_{all})$	subgroup
Lewko-Waters 12	no	yes	full	$O(q_{all})$	Q-type, subgroup
Okamoto-Takashima 12b	yes	no	full	$O(q_{all})$	DLIN
Rouselakis-Waters 13	yes	yes	selective	$O(1)$	Q-type
Our unbounded ABE	**yes**	**yes**	**full**	$O(q_1)$	Q-type, subgroup

More Results

- Generic dual scheme conversion for perfectly-secure encoding.
  - Convert key-policy to ciphertext-policy (& vice versa)
- Fully-secure dual (ciphertext-policy) FE for regular languages.
- Unification of schemes based on dual systems and some improvements.

Take-Home Ideas

- Our framework can be considered as a method for boosting doubly selectively security (of encoding) to fully security (of FE).
- Why does it matters? Proving double selective security of encoding can use techniques from proving classical selective security.

Thank you

Recall the Definitions of Semi-Keys

K $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(0,\mathbf{0},\mathbf{0})}$

↓ Subgroup Decision

K1 $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(0,\hat{\mathbf{r}},\hat{\mathbf{h}})}$

↓ Security of encoding

K2 $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(\hat{a},\hat{\mathbf{r}},\hat{\mathbf{h}})}$

↓ Subgroup Decision

K3 $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(\hat{a},\mathbf{0},\mathbf{0})}$

Proof for the 1st Transition

K $g_1^{\boldsymbol{k}(a,\boldsymbol{r},\boldsymbol{h})} \cdot g_2^{\boldsymbol{k}(0,\boldsymbol{0},\boldsymbol{0})}$

Subgroup Decision

K1 $g_1^{\boldsymbol{k}(a,\boldsymbol{r},\boldsymbol{h})} \cdot g_2^{\boldsymbol{k}(0,\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$

Subgroup Decision problem: Decide if $T \in G_1$ or $T \in G_{12}$

Proof for the 1st Transition

Simulated by

(K) $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(0,\mathbf{0},\mathbf{0})}$ $\qquad$ $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h}')} \cdot (g_1^{t_1})^{\mathbf{k}(0,\mathbf{r}',\mathbf{h}')}$

T

(K1) $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(0,\hat{\mathbf{r}},\hat{\mathbf{h}})}$ $\qquad$ $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h}')} \cdot (g_1^{t_1} g_2^{t_2})^{\mathbf{k}(0,\mathbf{r}',\mathbf{h}')}$

Subgroup Decision problem: Decide if $T \in G_1$ or $T \in G_{12}$

Proof for the 1st Transition

Simulated by

K: $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(0,\mathbf{0},\mathbf{0})}$ — simulated by $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h}')} \cdot (g_1^{t_1})^{\mathbf{k}(0,\mathbf{r}',\mathbf{h}')}$

T

K1: $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(0,\hat{\mathbf{r}},\hat{\mathbf{h}})}$ — simulated by $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h}')} \cdot (g_1^{t_1} g_2^{t_2})^{\mathbf{k}(0,\mathbf{r}',\mathbf{h}')}$

Subgroup Decision problem: Decide if $T \in G_1$ or $T \in G_{12}$

Simulation is OK due to linearity, param-vanishing of $\mathbf{k}$ and "parameter-hiding" of G:

$\mathbf{h} = \mathbf{h}' \bmod p_1$ and $\hat{\mathbf{h}} = \mathbf{h}' \bmod p_2$ are independent.

Proof for the 3rd Transition is similar

Simulated by

K2 $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(\hat{a},\hat{\mathbf{r}},\hat{\mathbf{h}})}$ $\qquad$ $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h}')} \cdot (g_1^{t_1} g_2^{t_2})^{\mathbf{k}(a',\mathbf{r}',\mathbf{h}')}$

T

K3 $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h})} \cdot g_2^{\mathbf{k}(\hat{a},\mathbf{0},\mathbf{0})}$ $\qquad$ $g_1^{\mathbf{k}(a,\mathbf{r},\mathbf{h}')} \cdot (g_1^{t_1})^{\mathbf{k}(a',\mathbf{r}',\mathbf{h}')}$