Exotic & Powerful !!

ADVANCED CRYPTOGRAPHIC PRIMITIVES

PART 1: INTRO TO FUNCTIONAL ENCRYPTION

ACM INDIA SUMMER SCHOOL (12 – 06 – 2024)

Venkata Koppula (IIT Delhi)
kvenkata@iitd.ac.in

THE JOURNEY SO FAR . . .

- Secret Key Encryption [… B.C - today]
  - Data Encryption Standard
  - Advanced Encryption Standard

- Public Key Encryption [1976 - today]
  - Diffie-Hellman: Key exchange [1976]
  - Rivest-Shamir-Adleman: First candidate [1977]
  - Goldwasser-Micali: Theoretical foundations [1984]
  - …

THE JOURNEY SO FAR . . .

Art of secure communication

New directions and formalizations

Engineering and technology translation

Pre-1970

1970s - 1980s

Post-2000

21st Century Crypto: Newer directions and formalizations

*borrowed from Sikhar's slides

PLAN FOR TODAY'S SESSIONS

Functional Encryption

Code Obfuscation

PLAN FOR TODAY'S SESSIONS

Functional Encryption

Code Obfuscation

Cryptographic Solution

Formal Security Model

Define an adversarial model

Application

** borrowed from Sikhar's slides*

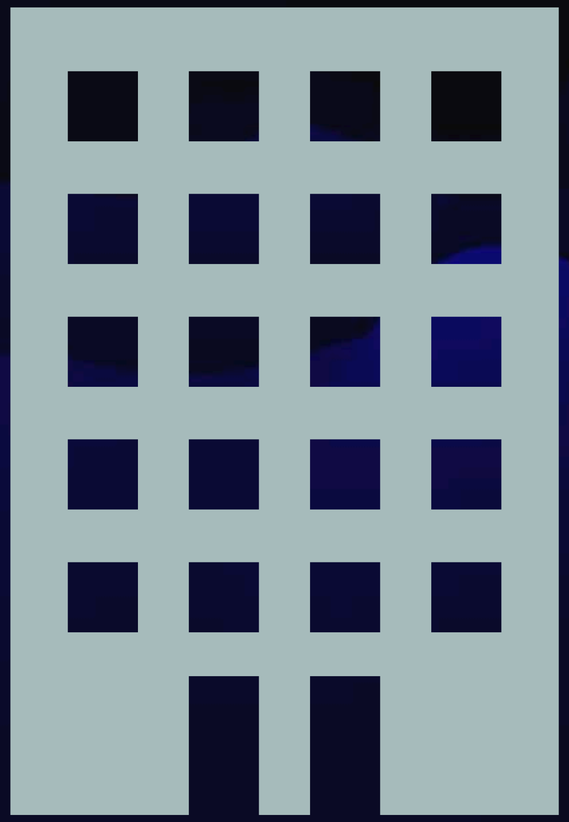
PART 1: FUNCTIONAL ENCRYPTION

(i) Identity based encryption

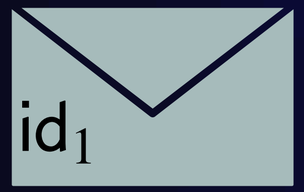
(ii) Attribute based encryption

(iii) Functional encryption

IDENTITY BASED ENCRYPTION



Anyone can encrypt using just identity and mpk



id_1

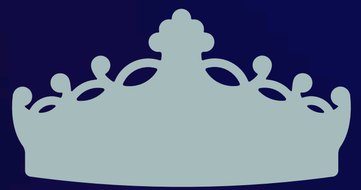
id_2

id_3

sk_1

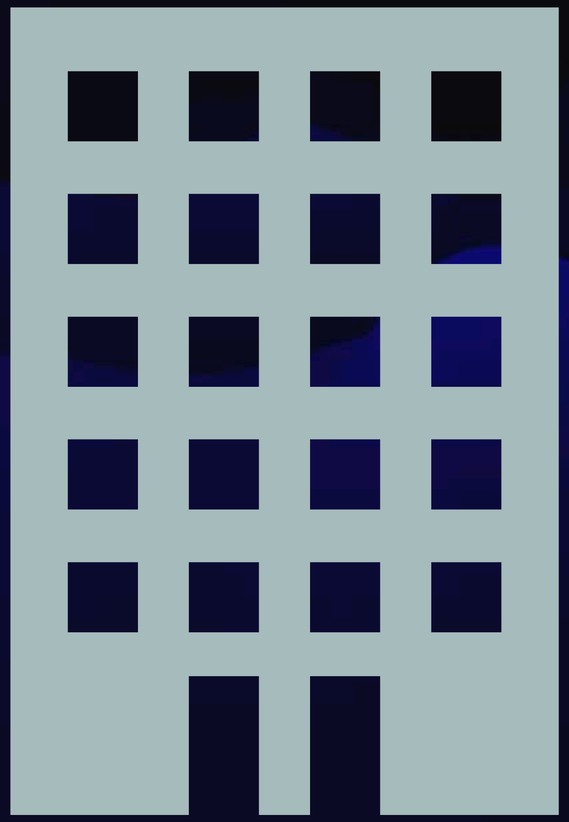
sk_2

sk_3



mpk
msk

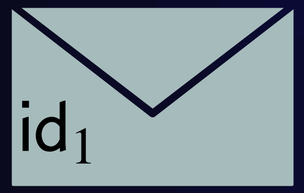
IDENTITY BASED ENCRYPTION

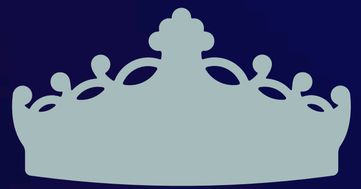


id_1 id_2 id_3

Anyone can encrypt using just identity and mpk

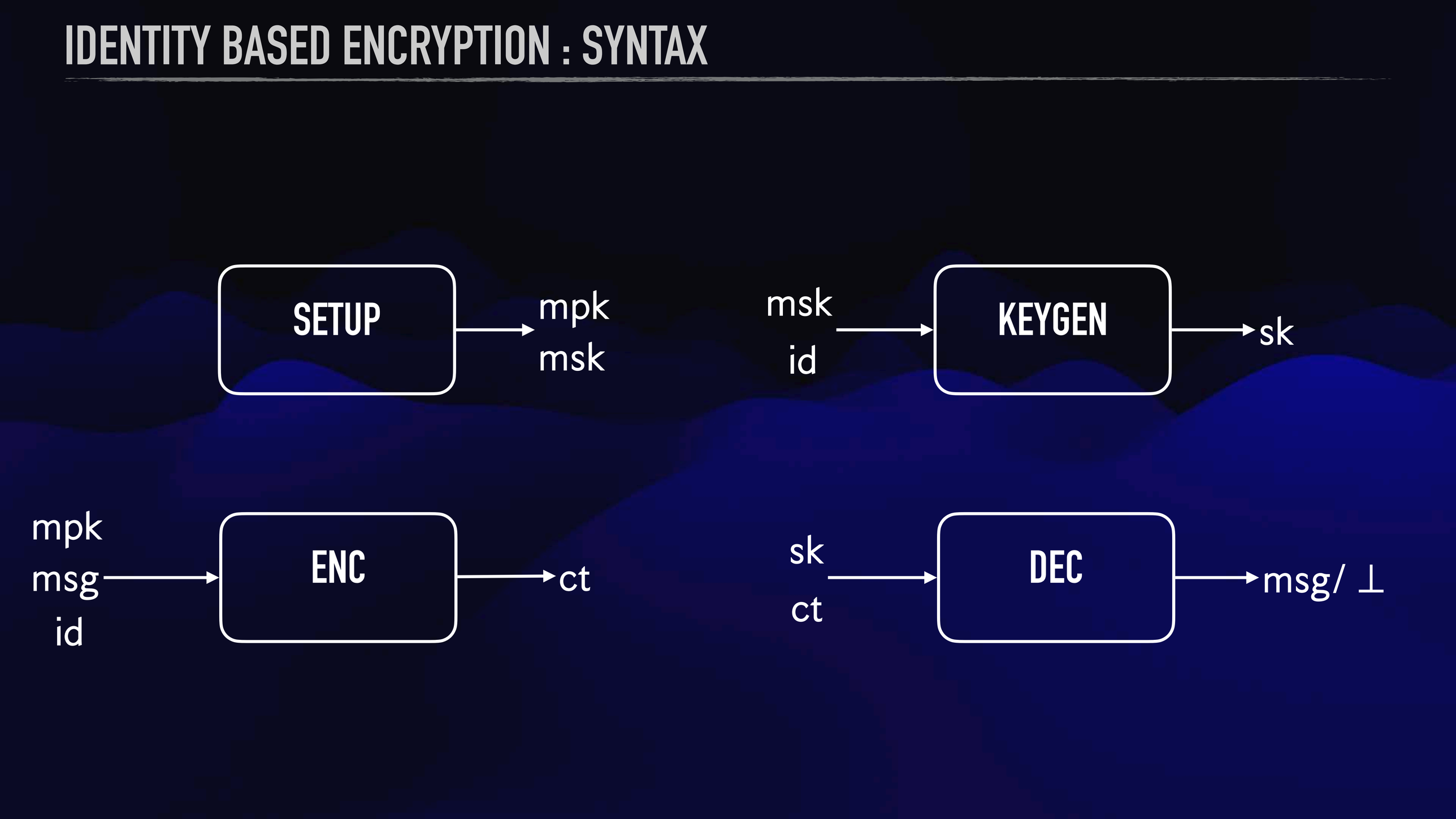
sk_1 sk_2 sk_3



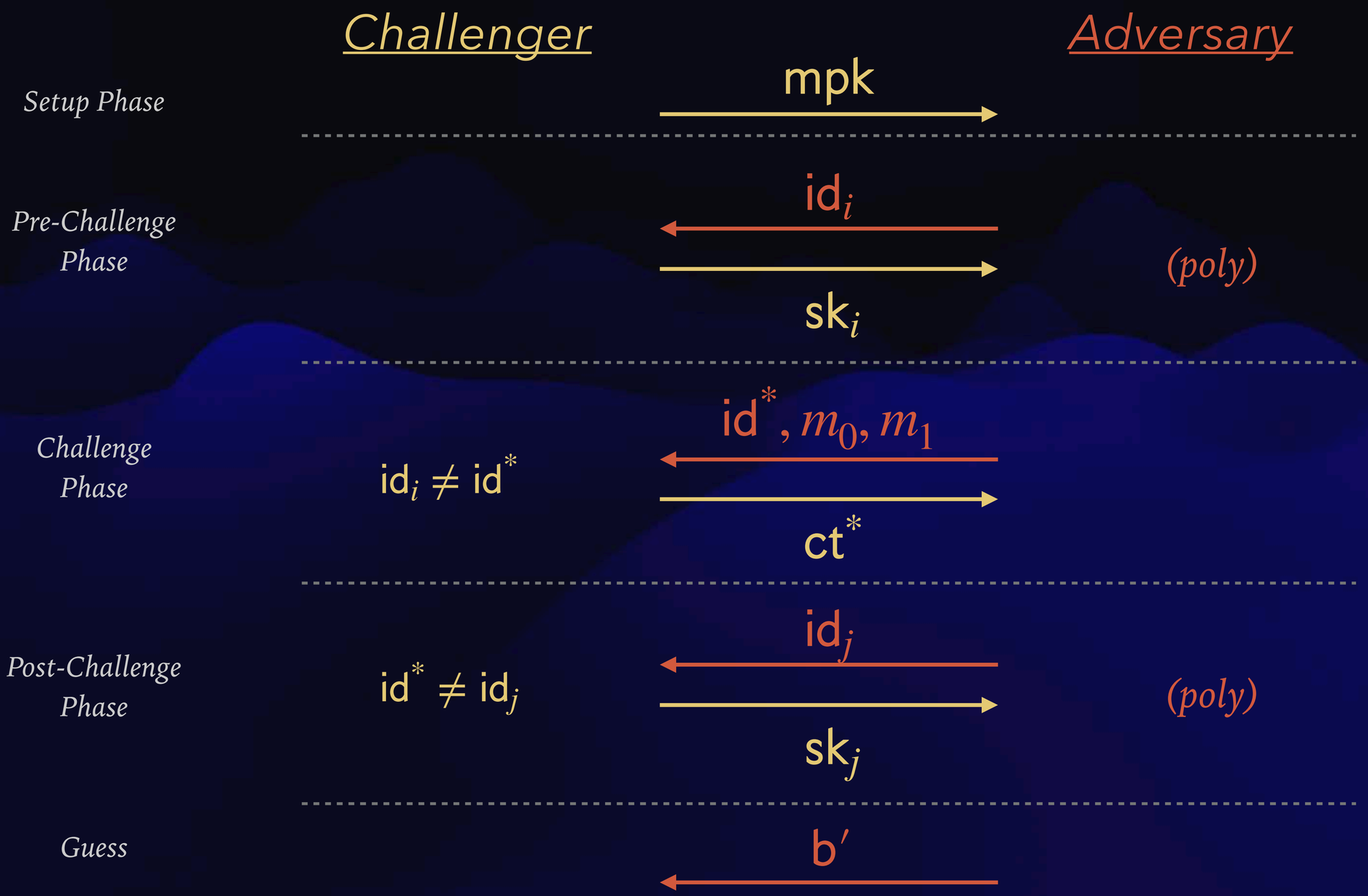


mpk
msk

IDENTITY BASED ENCRYPTION : SYNTAX



IDENTITY BASED ENCRYPTION : SECURITY



IDENTITY BASED ENCRYPTION : A 'TRIVIAL' CONSTRUCTION

$\mathcal{ID} = \{\mathsf{id}_1, \mathsf{id}_2, \ldots, \mathsf{id}_t\}$

Efficiency:

$|\mathsf{mpk}, \mathsf{msk}| \ll$ **no. of identities**

$\mathsf{Setup}\ () : \textit{Sample}\ (\mathsf{pk}_1, \mathsf{sk}_1), \ldots, (\mathsf{pk}_t, \mathsf{sk}_t)$

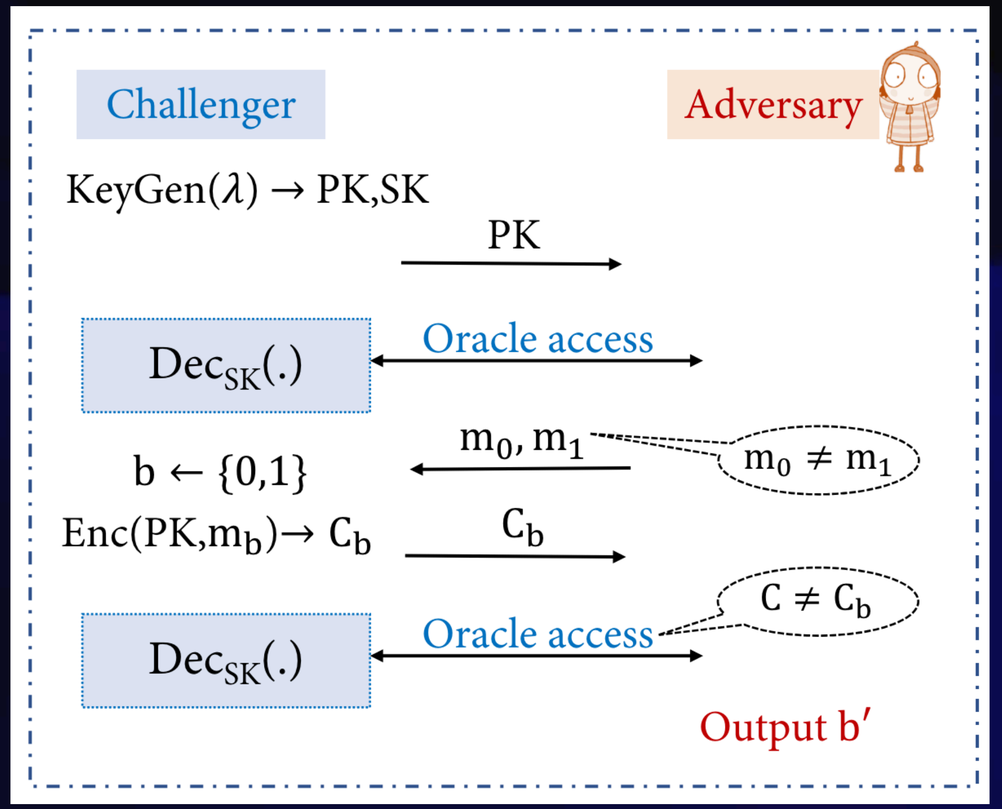
$\mathsf{mpk} = (\mathsf{pk}_1, \ldots, \mathsf{pk}), \quad \mathsf{msk} = (\mathsf{sk}_1, \ldots, \mathsf{sk}_t)$

$\mathsf{Enc}\ (\mathsf{mpk}, m, \mathsf{id}_i) : \mathsf{PKE}.\mathsf{Enc}\ (\mathsf{pk}_i, m)$

$\mathsf{KeyGen}\ (\mathsf{msk}, \mathsf{id}_i) : \textit{Output}\ \mathsf{sk}_i$

IDENTITY BASED ENCRYPTION : AN APPLICATION

CCA secure PKE using IBE



CCA Security Game

*If only pre-challenge decryption queries, then **CCA-1 security***

**borrowed from Sruthi's slides*

IDENTITY BASED ENCRYPTION : AN APPLICATION

Warm-up: CCA-1 secure PKE using IBE

Setup() : pk = ibe . mpk, sk = ibe . msk

Enc(ibe . mpk, m) : *Sample random* id

ibe . ct $\leftarrow$ IBE . Enc(ibe . mpk, id, m)

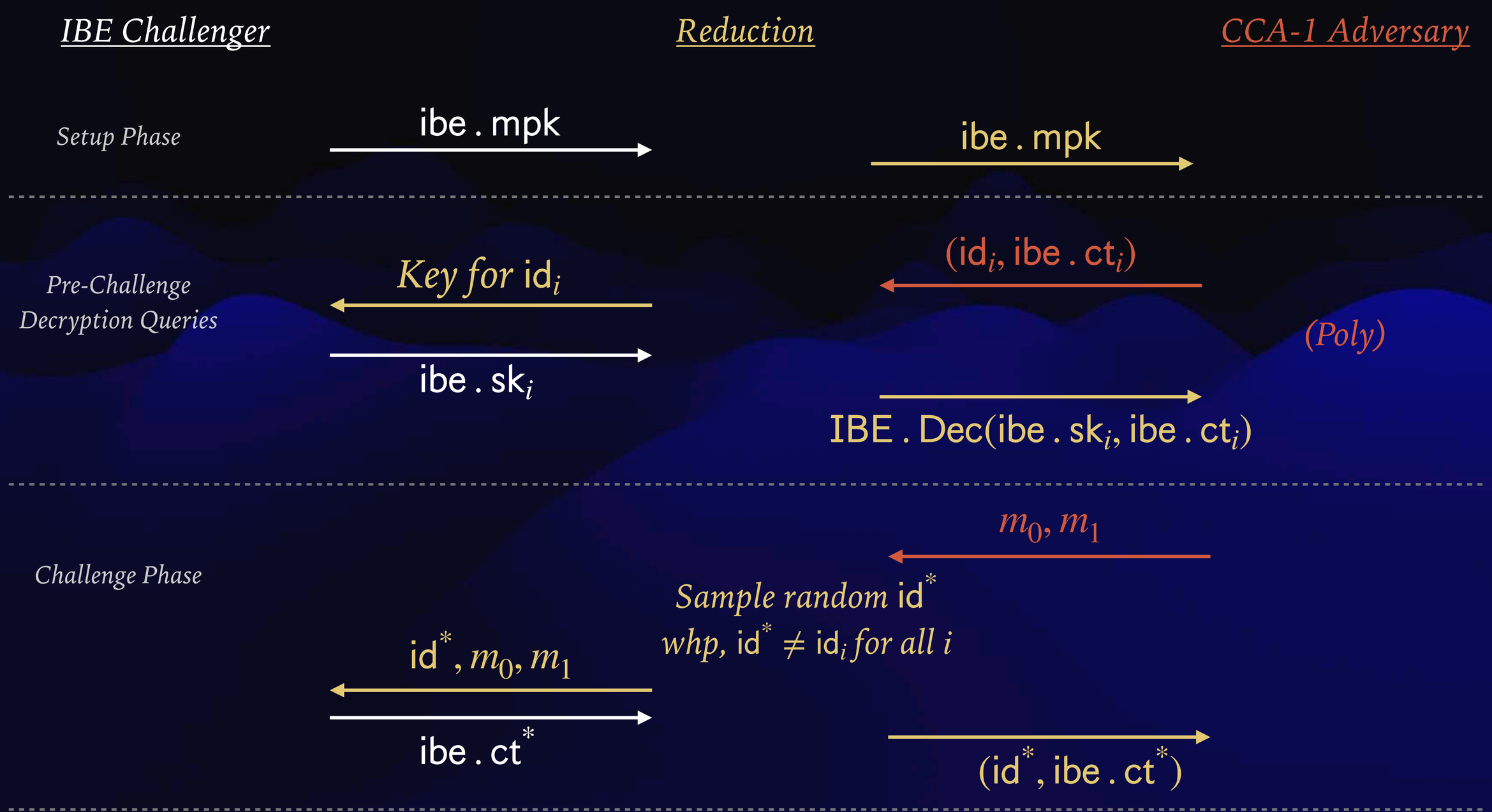
Output (id, ibe . ct)

Dec(ibe . msk, (id, ibe . ct)) :

ibe . sk $\leftarrow$ IBE . KeyGen(ibe . msk, id)

Output IBE . Dec(ibe . sk, ibe . ct)

IDENTITY BASED ENCRYPTION : AN APPLICATION



IDENTITY BASED ENCRYPTION : AN APPLICATION

CCA secure PKE using IBE + One-time Signatures

Setup() : pk = ibe . mpk, sk = ibe . msk

Enc(ibe . mpk, m) : *Sample* (s . sk, s . vk)

ibe . ct $\leftarrow$ IBE . Enc(ibe . mpk, s . vk, m)

s . $\sigma \leftarrow$ S . Sign (s . sk, ibe . ct)

Output (s . vk, ibe . ct, s . σ)

Qn: Prove security.

Dec(ibe . msk, (s . vk, ibe . ct, s . σ)) :

Check S . Verify(s . vk, s . σ, ibe . ct) = 1

ibe . sk $\leftarrow$ IBE . KeyGen(ibe . msk, s . vk)

Output IBE . Dec(ibe . sk, ibe . ct)

IDENTITY BASED ENCRYPTION : AN APPLICATION

CCA Challenger *CCA Adversary*

Setup Phase

ibe . mpk →

Challenge Phase

m_0, m_1 ←

(s . vk , ibe . ct*, s . σ) →

Post-Challenge Decryption Queries

(s . vk$_i$, ibe . ct$_i$, s . σ_i) ←

Check S . Verify(s . vk$_i$, ibe . ct$_i$, s . σ) = 1

ibe . sk$_i$ ← KeyGen(ibe . msk, s . vk$_i$)

(Poly)

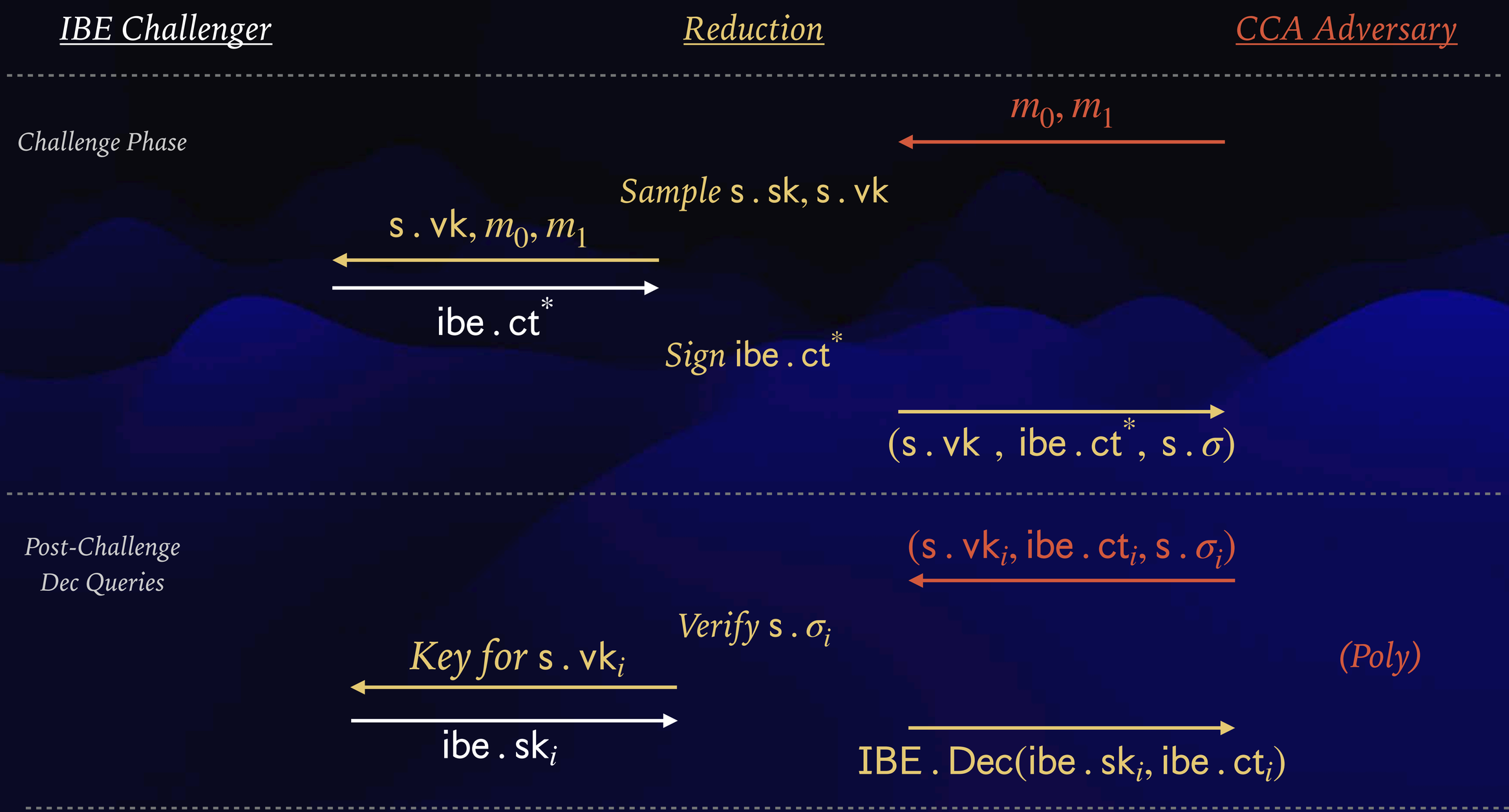
IBE . Dec(ibe . sk$_i$, ibe . ct$_i$) →

Security of signature scheme ensures s . vk ≠ s . vk$_i$ for all i

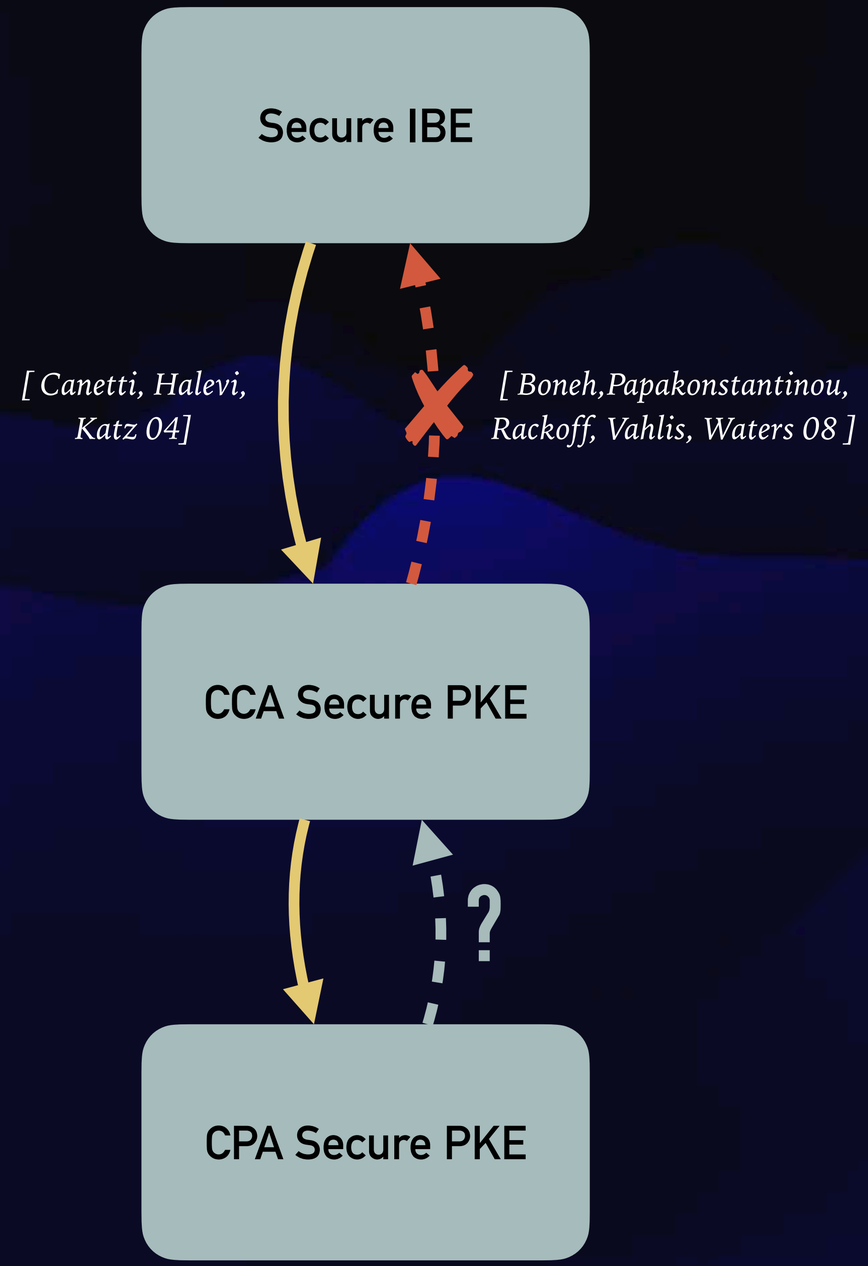
Guess

b' ←

IDENTITY BASED ENCRYPTION : AN APPLICATION



IDENTITY BASED ENCRYPTION : SUMMARY AND BRIEF HISTORY



- [Shamir 84] : Proposed the notion of IBE

- [Boneh-Franklin 01] : First IBE scheme in random oracle mode, using 'bilinear maps'. Awarded Godel Prize in 2013.

Dan Boneh

Matthew Franklin

- [Boneh-Boyen 04] : IBE without random oracle model, using bilinear maps

- [Gentry-Peikert-Vaikuntanathan 08, Cash-Hofheinz-Kiltz-Peikert 10, Agrawal-Boneh-Boyen 10] : IBE from lattices

IDENTITY BASED ENCRYPTION : QUESTIONS

Qn: You are given an IBE scheme with identity space $\{0,1\}^n$.
Construct an IBE scheme with identity space $\{0,1\}^*$.
You can use any other crypto primitive.

Qn: You are given an IBE scheme with identity space $\{0,1\}^*$.
Construct a secure signature scheme using this IBE scheme
(no other crypto primitives are allowed).

PART 1: FUNCTIONAL ENCRYPTION

(i) Identity based encryption

(ii) Attribute based encryption

(iii) Functional encryption

ATTRIBUTE BASED ENCRYPTION

Encrypt messages with ‘access policy’

Only users having attribute satisfying access policy should learn message

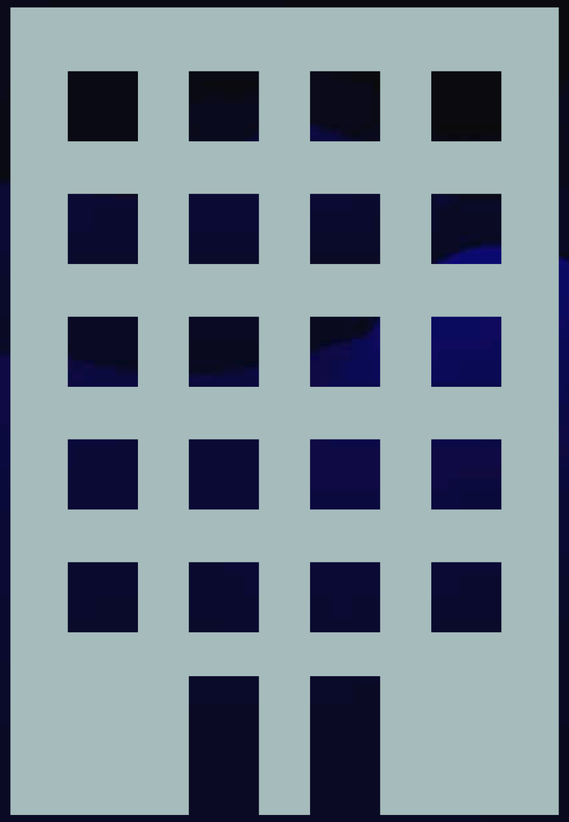
Attributes

College: IITB / non-IITB
Current degree: Bachelors/Masters/PhD
Department: CSE/non-CSE

Encrypt message for

(CSE ∧ Bachelors)
∨
(IITB ∧ non-CSE)

ATTRIBUTE BASED ENCRYPTION



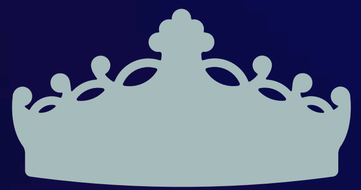
Anyone can encrypt using policy

att_1

att_2

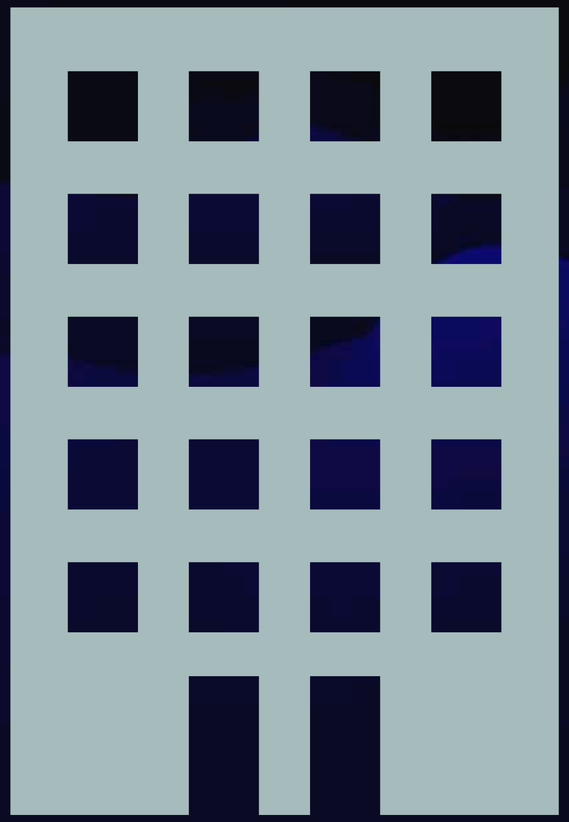
att_3

sk_1 sk_2 sk_3



mpk
msk

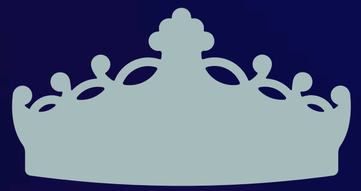
ATTRIBUTE BASED ENCRYPTION



Anyone can encrypt using policy and mpk

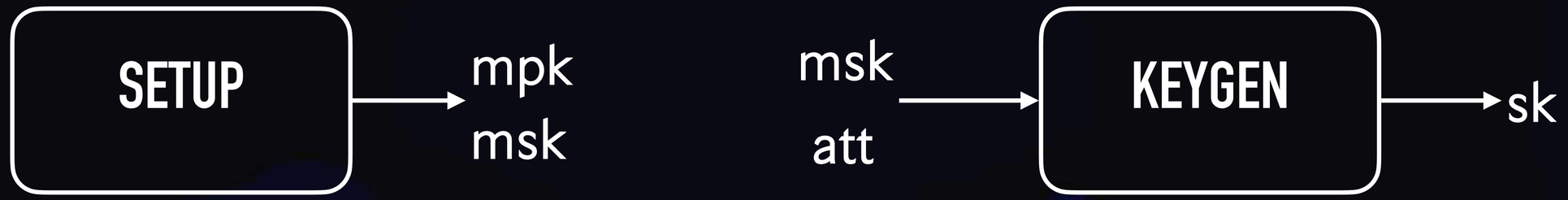
att_1 att_2 att_3

sk_1 sk_2 sk_3



mpk
msk

ATTRIBUTE BASED ENCRYPTION : SYNTAX

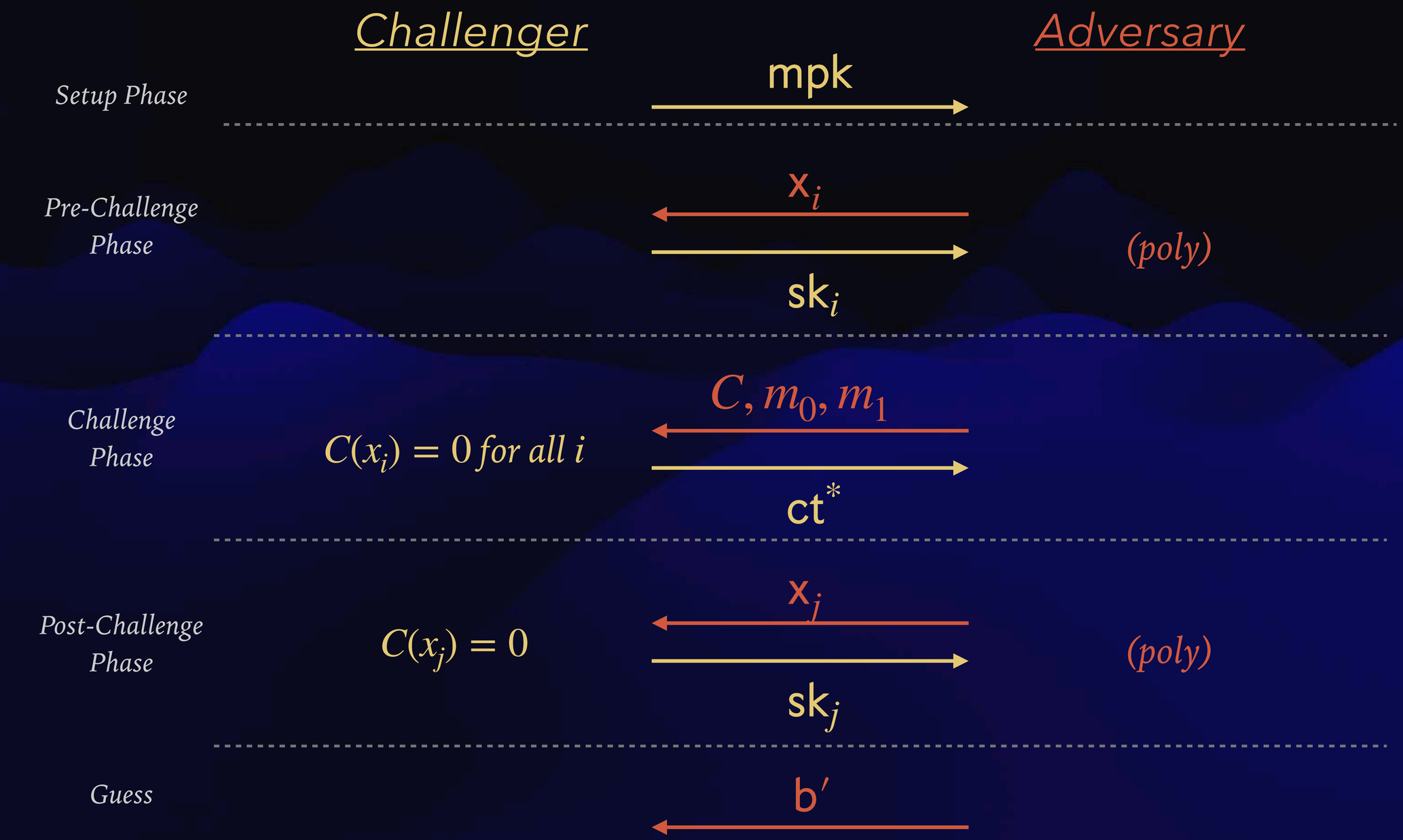


Default:

Policies will be described using circuit C, attributes using bit-vector x

Decryption outputs message if $C(x) = 1$

ATTRIBUTE BASED ENCRYPTION : SECURITY



EXAMPLE: ATTRIBUTE BASED ENCRYPTION FOR SUBSET RELATION

Universe $\mathcal{U}$

Policies and attributes: subsets of $\mathcal{U}$

Policy P accepts attribute A if $P \subseteq A$

Goal: ABE for subset relation, using IBE with identity space $\mathcal{U}$

EXAMPLE: ATTRIBUTE BASED ENCRYPTION FOR SUBSET RELATION

$$\text{Setup}() : \text{mpk} = \text{ibe}.\text{mpk}, \quad \text{msk} = \text{ibe}.\text{msk}$$

$\text{KeyGen}(\text{ibe}.\text{msk}, A) :$

$\forall a \in A, \text{ibe}.\text{sk}_a \leftarrow \text{IBE}.\text{KeyGen}(\text{ibe}.\text{msk}, a)$

$\text{sk}_A = \{\text{ibe}.\text{sk}_a\}_{a \in A}$

$\text{Enc}(\text{ibe}.\text{mpk}, P, m) :$

$z_0 = m . \quad \forall i \in [t], z_i \leftarrow \text{IBE}.\text{Enc}(\text{ibe}.\text{mpk}, p_i, z_{i-1})$

$\text{ct} = z_t$

Qn: Is this scheme secure?

ATTRIBUTE BASED ENCRYPTION: COLLUSION RESISTANCE

ct : *Challenge ciphertext for policy* P

A_1, A_2 : *sets such that* $P \nsubseteq A_1, P \nsubseteq A_2,$ *but* $P \subseteq A_1 \cup A_2$

sk_1 : *key for* A_1, sk_2 : *key for* A_2

sk_1 *and* sk_2 *can together decrypt* ct!

ATTRIBUTE BASED ENCRYPTION : SUMMARY AND BRIEF HISTORY

- IBE: special case of ABE
- Two kinds of ABE:
  - **Ciphertext Policy** ABE:
    $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{policy}, m),\ \mathsf{sk} \leftarrow \mathsf{KeyGen}(\mathsf{att})$
  - **Key Policy** ABE:
    $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{att}, m),\ \mathsf{sk} \leftarrow \mathsf{KeyGen}(\mathsf{policy})$
- Collusion resistance: key challenge in ABE security
- Many feasibility-related open questions!

- [Sahai- Waters 05] : Proposed the notion of ABE
- [Goyal-Pandey-Sahai-Waters 06]: KP-ABE for formulae, using bilinear maps
- [Gorbunov-Vaikuntanathan-Wee 13]: KP-ABE for circuits, using lattices
- [Bethencourt-Sahai-Waters 07]: CP-ABE for formulae, using bilinear maps
- [Wee 22]: CP-ABE for circuits, using lattices

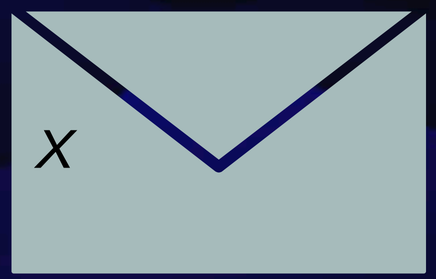
PART 1:
FUNCTIONAL ENCRYPTION

(i) Identity based encryption

(ii) Attribute based encryption

(iii) Functional encryption

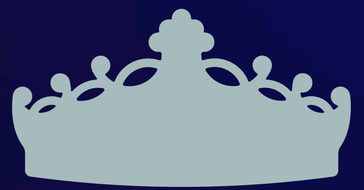
FUNCTIONAL ENCRYPTION



f_1 f_2 f_3

$f_1(x)$ $f_2(x)$ $f_3(x)$

sk_1 sk_2 sk_3

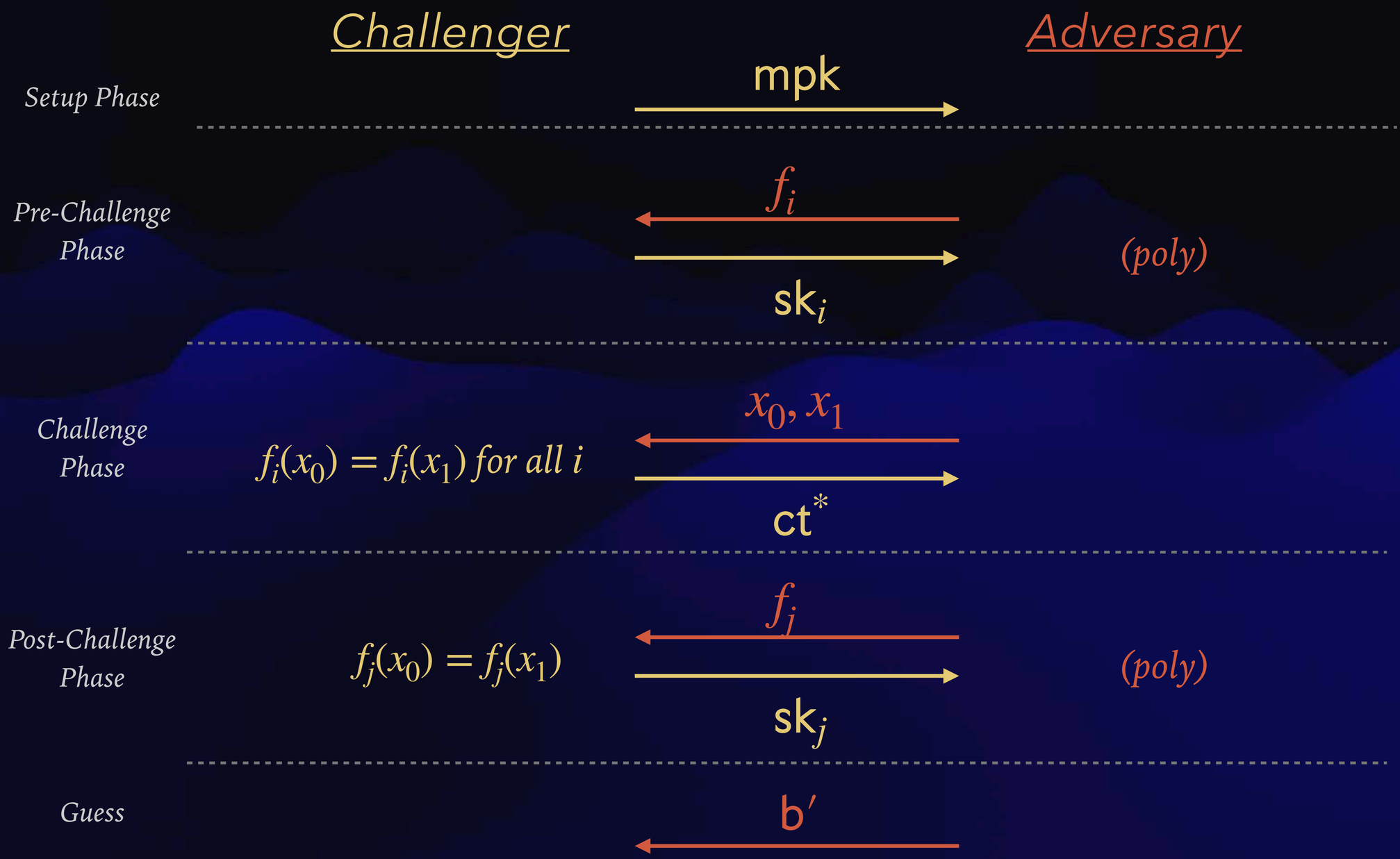


mpk
msk

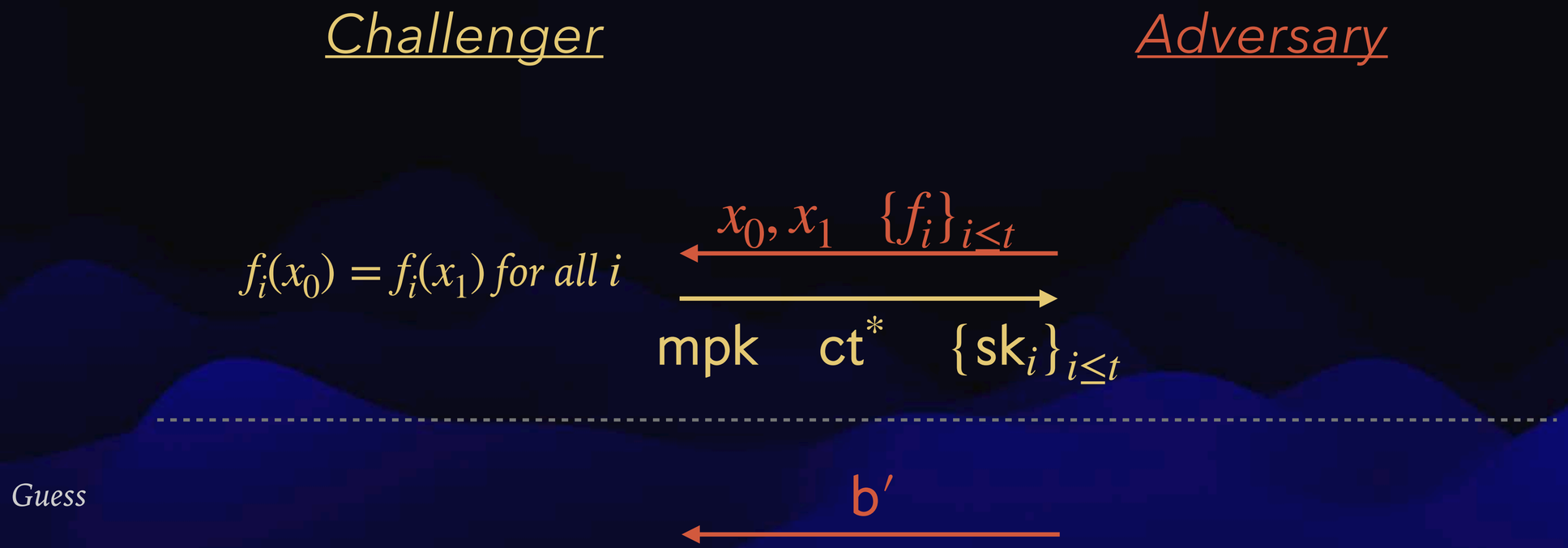
FUNCTIONAL ENCRYPTION : SYNTAX

Qn: FE $\Longrightarrow$ ABE ?

FUNCTIONAL ENCRYPTION : SECURITY



FUNCTIONAL ENCRYPTION : BOUNDED COLLUSION SECURITY



Theorem: Assuming PKE exists, there exists an FE scheme with t-bounded security.

Qn: PKE + Garbled ckts $\Longrightarrow$ 1-bounded secure FE ?

FUNCTIONAL ENCRYPTION : SUMMARY AND BRIEF HISTORY

- IBE, ABE: special cases of FE
- Bounded collusion FE can be built from PKE
- Many feasibility-related open questions!

- [Katz-Sahai- Waters 05] : FE for inner products, using bilinear maps
- [Boneh-Sahai-Waters 11, O'Neill 11]: Defined FE for general circuits
- [Garg-Gentry-Halevi-Raykova-Sahai-Waters 13]: First candidate construction using novel cryptographic assumptions
- [Jain-Lin-Sahai 20]: Construction based on standard assumptions (bilinear maps + LWE + low-depth PRGs)

THANK YOU !