An Overview of Identity Based Encryption

Dan Boneh

Stanford University

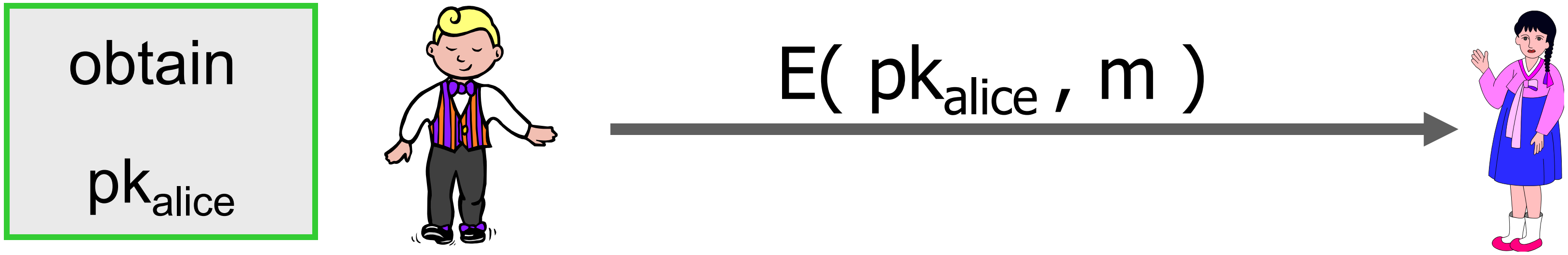
Recall: Pub-Key Encryption (PKE)

PKE Three algorithms : (G, E, D)

$G(1^\lambda) \rightarrow (pk,sk)$ outputs pub-key and secret-key

$E(pk, m) \rightarrow c$ encrypt m using pub-key pk

$D(sk, c) \rightarrow m$ decrypt c using sk

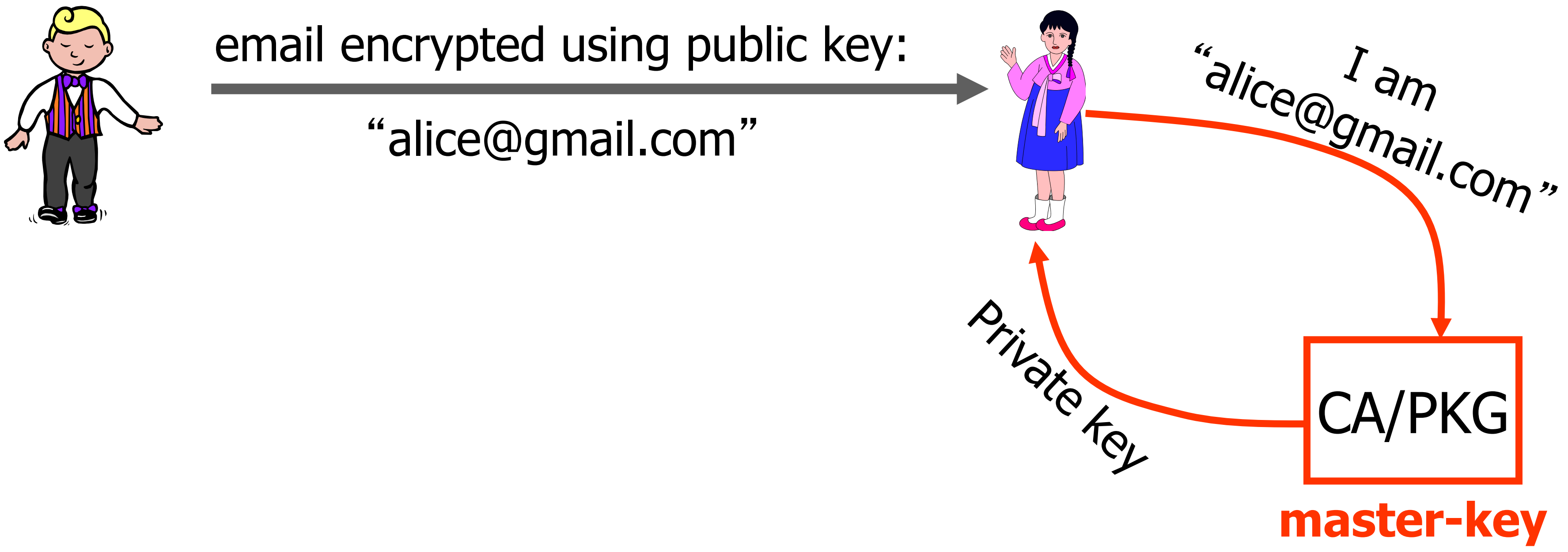


obtain pk_{alice}

$E(pk_{alice} , m)$

Identity Based Encryption [Sha '84]

- IBE: PKE system where PK is an arbitrary string
  - e.g. e-mail address, phone number, IP addr…



email encrypted using public key:

"alice@gmail.com"

"I am alice@gmail.com"

Private key

CA/PKG

master-key

Identity Based Encryption

Four algorithms : (S,G,E,D)

$S(1^\lambda) \rightarrow (pp, mk)$ output params, pp,
and master-key, mk

$G(mk, ID) \rightarrow sk_{ID}$ outputs private key, sk_{ID} , for ID

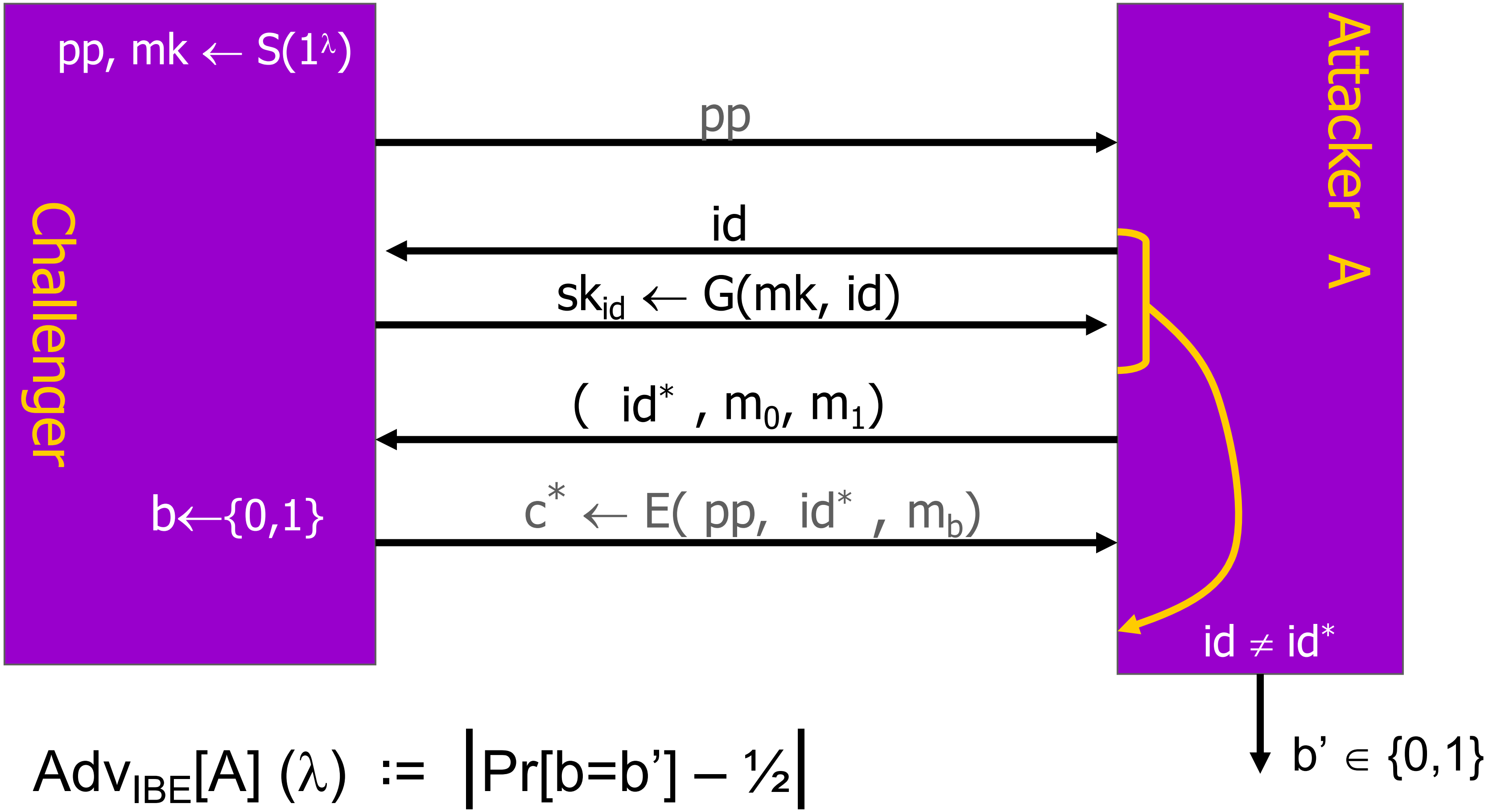
$E(pp, ID, m) \rightarrow c$ encrypt m using pub-key ID (and pp)

$D(sk_{ID}, c) \rightarrow m$ decrypt c using sk_{ID}

IBE “compresses” exponentially many pk’s into a short pp

CPA-Secure IBE systems (IND-IDCPA) [**B**-Franklin'01]

Semantic security when attacker has few private keys



Challenger

$pp, mk \leftarrow S(1^\lambda)$

pp

Attacker A

id

$sk_{id} \leftarrow G(mk, id)$

$(\ id^*\ , m_0, m_1)$

$b \leftarrow \{0,1\}$

$c^* \leftarrow E(\ pp,\ id^*\ , m_b)$

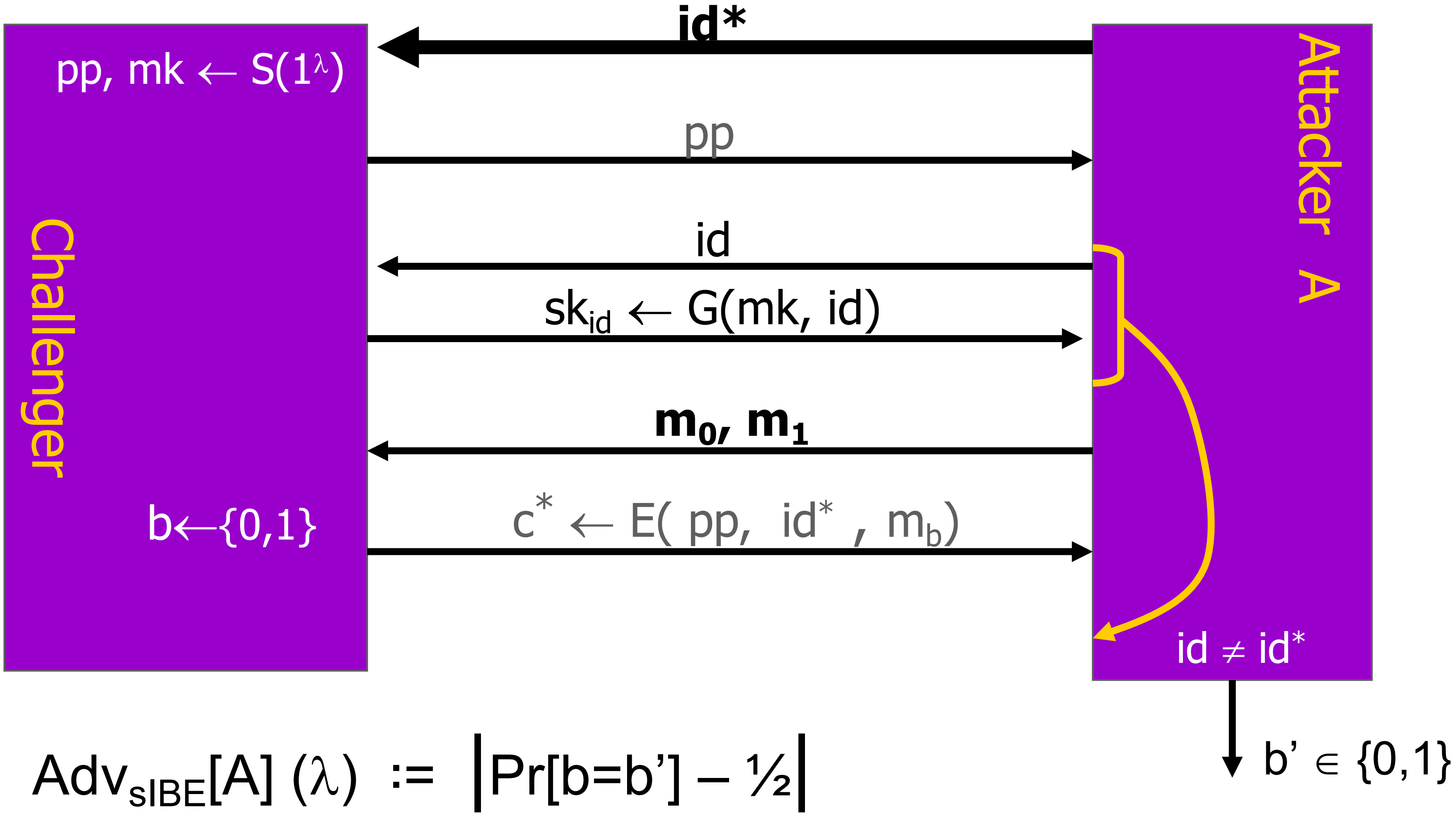
$id \neq id^*$

$b' \in \{0,1\}$

$$Adv_{IBE}[A]\ (\lambda)\ := \ \left| Pr[b=b'] - ½ \right|$$

CPA-Secure IBE systems (IND-sIDCPA) [CHK'04]

Selective security: commit to target **id*** in advance



$$Adv_{sIBE}[A](\lambda) := \left| Pr[b=b'] - ½ \right|$$

selective ⟶ full: generic conversion [BB'04]

- The two models are equivalent in the RO model

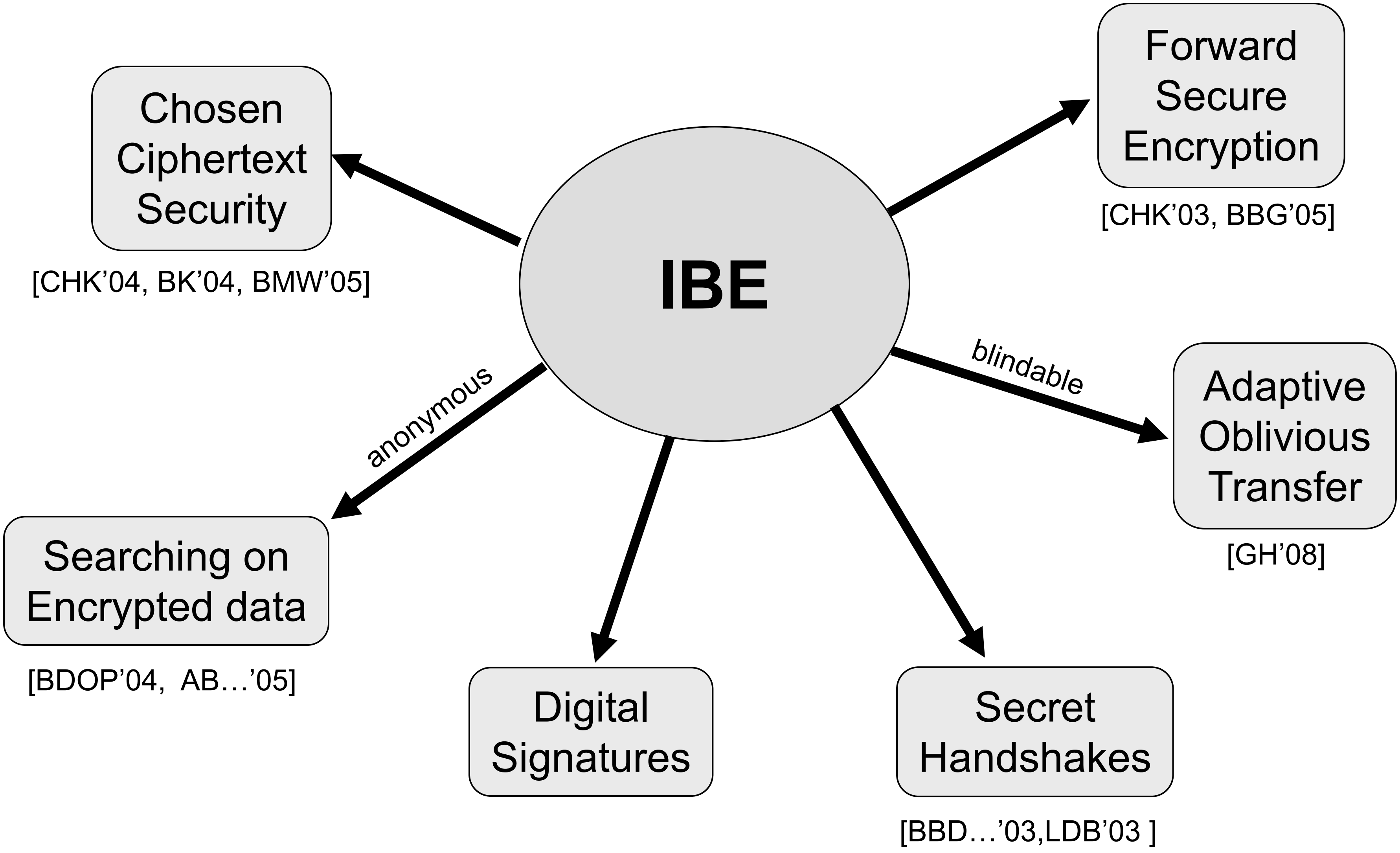
$$E(pp, id, m) \quad \longrightarrow \quad E(pp, H(id), m)$$

- In the standard model: complexity leveraging

Lemma: $\forall A \exists B: \quad \mathrm{Adv}_{\mathbf{IBE}}[A] \;\leq\; \mathbf{2^n} \cdot \mathrm{Adv}_{\mathbf{sIBE}}[B]$

where $n = |\,ID\,|$ e.g. $n = 256$

Why ID Based Encryption?



IBE

Chosen Ciphertext Security

[CHK'04, BK'04, BMW'05]

Forward Secure Encryption

[CHK'03, BBG'05]

blindable

Adaptive Oblivious Transfer

[GH'08]

anonymous

Searching on Encrypted data

[BDOP'04, AB…'05]

Digital Signatures

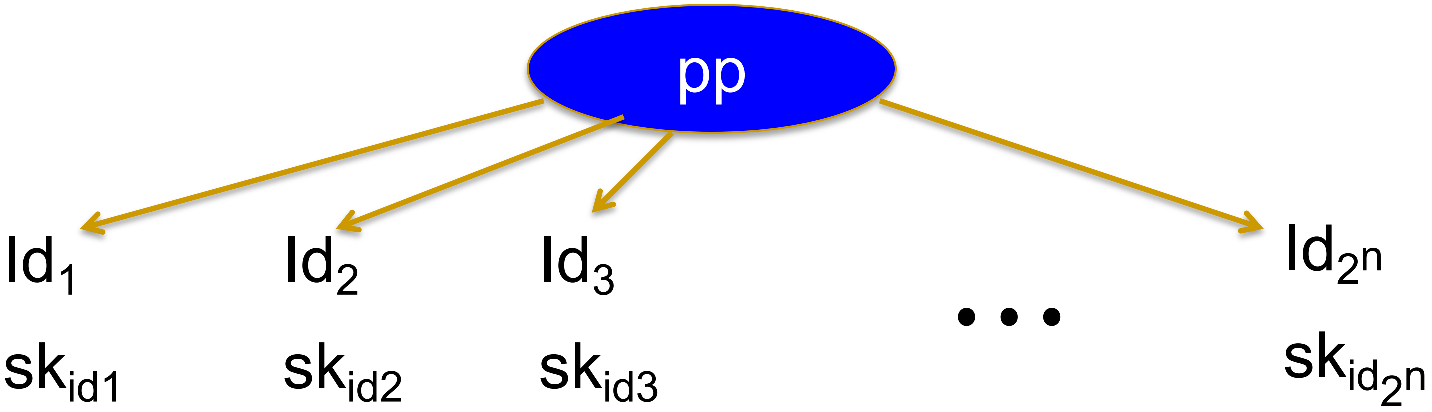
Secret Handshakes

[BBD…'03,LDB'03]

Black box separation [BPRVW'08]

$$\left.\begin{array}{l}\text{Trapdoor functions}\\[2em] \text{CCA-secure public-key enc.}\end{array}\right\} \not\Rightarrow \quad \text{IBE}$$

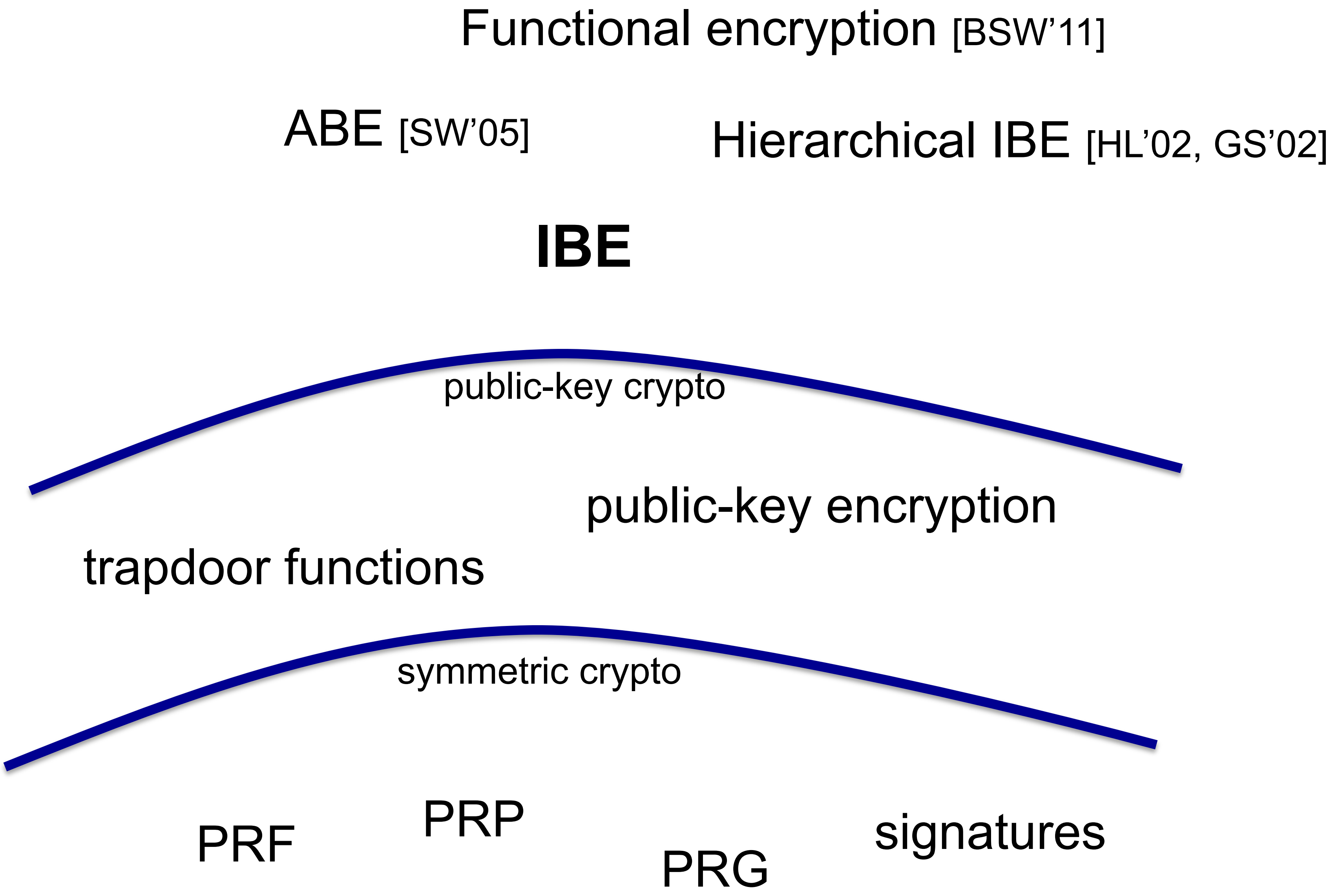
Main reason: short pp defines exp. many public keys



pp

Id_1 Id_2 Id_3 … Id_{2^n}

sk_{id1} sk_{id2} sk_{id3} $sk_{id_{2^n}}$



Functional encryption [BSW'11]

ABE [SW'05]

Hierarchical IBE [HL'02, GS'02]

IBE

public-key crypto

public-key encryption

trapdoor functions

symmetric crypto

PRF

PRP

PRG

signatures

IBE in practice

Bob encrypts message with pub-key:

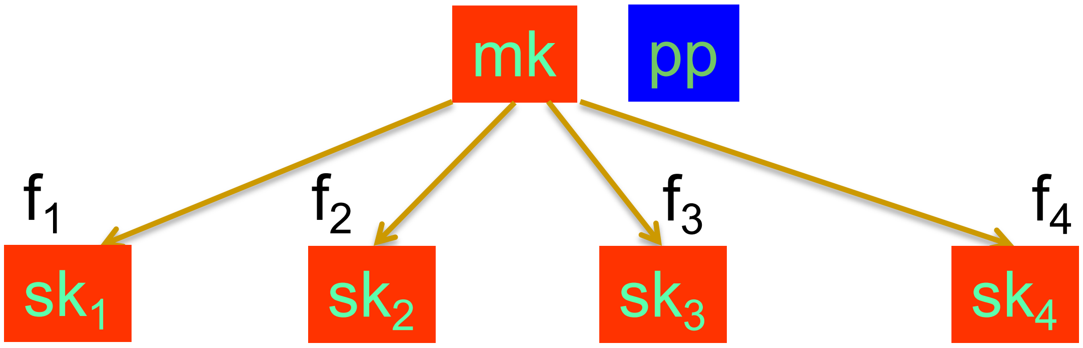
$$\underbrace{\text{“alice@hotmail} \;\; || \;\; \text{role=accounting}}_{\text{policy-based encryption}} \;\; || \;\; \underbrace{\text{time=week-num”}}_{\substack{\text{short-lived keys} \\ \Rightarrow \;\; \text{easy revocation}}}$$

Voltage

Discover, protect, and secure sensitive and high-value data

by OpenText, 2023

IBE: functional encryption view [BSW'11]



$$E(\, pp, \text{data} \,) \quad , \quad sk_1 \quad \Rightarrow \quad f_1(\text{data})$$

IBE: first non-trivial functionality

$$E\Big(pp,\ \underbrace{(id_0, m)}_{\text{data}}\ \Big)\ ,\ sk_{id} \quad \Rightarrow \quad \text{output} \begin{cases} m & \text{if } id=id_0 \\ \perp & \text{otherwise} \end{cases}$$

Constructing IBE

Can we build an IBE ??

- ElGamal is not an IBE:

  sk := ($\alpha \leftarrow F_p$) ; pk := ($h \leftarrow g^{\alpha}$)

  - pk can be any string: **h = "*alice@gmail.com*" $\in$ G**

    … but cannot compute secret key α

  - Attempts using trapdoor Dlog [MY'92] but inefficient

Can we build an IBE ??

- RSA is not an IBE:

  $pk := (N=p\cdot q,\ \ e)$; $sk := (d)$

  - Cannot map ID to (N,e)

  - How about: fix N and and use $e_{id} = \mathrm{Hash}(id)$

    - Problem: given (N , e_{id} , d_{id}) can factor N

IBE Constructions: three families

	Pairings e: G × G → G’	Lattices (LWE)	Quadratic Residuosity
IBE w/RO	BF’01	GPV’08	Cocks’01 BGH’07
IBE no RO	CHK’03, BB’04, W’05, G’06, W’09, CW’13, …	←→ CHKP’10, ←→ **ABB’10,** MP’12 …	??
HIBE	GS’03, BB’04 BBG’05, GH’09, LW’10, …	CHKP’10, **ABB’10** **ABB’10a**	??
extensions	many	many	??

from CDH (no pairings): DG’2017 (via garbled circuits)

Pairing-based constructions

Some pairing-based IBE constructions

- **BF-IBE** [BF'01]: BDH ⇒ IND-IDCPA (in RO model)
- **BB-IBE** [BB'04]: BDDH ⇒ IND-**s**IDCPA
- **Waters-IBE** [W'05]: BDDH ⇒ IND-IDCPA (but long pp)
- **Gentry-IBE** [G'06]: q-BDHE ⇒ IND-IDCPA and short pp
- **DualSys-IBE** [W'09]: 2-DLIN ⇒ IND-IDCPA and short pp

  [LW'10, L'12, CW'13]

BF-IBE: IBE in the RO model [BF' 01]

- $S(1^{\lambda})$: $(G, G_T, g, p) \leftarrow \mathrm{GenBilGroup}(\lambda)$, $\alpha \leftarrow F_p$

  $pp := [g,\ y \leftarrow g^{\alpha}] \in G$; $mk := \alpha$

- $G(mk, id)$: $\boxed{sk \leftarrow H(id)^{\alpha}}$ $H: \mathcal{ID} \rightarrow G$

- $E(pp, id, m)$: $s \leftarrow F_p$ and do

  $$\boxed{C \leftarrow \left(g^{s} ,\quad m \cdot e(y, H(id))^{\mathbf{s}} \right)}$$

  $$= e(g^{\alpha},\ H(id)^{s})$$

- $D(\ sk,\ (c_1, c_2)\ )$:

  observe: $e(\ c_1\ , sk\ ) = e(\ g^{\mathbf{s}}\ ,\ H(id)^{\alpha}\ )$

IBE and Signature Systems

IBE ⇒ Simple digital Signatures

- Sign(MK, m): sig ← G(mk, m)
- Verify(PP, m, **sig**): Test that **sig** decrypts messages encrypted using m

- Conversely: which sig. systems extend to an IBE? Examples:
  - Rabin signatures (factoring) ⇒ Cocks-IBE, BGH-IBE
  - BLS signatures (pairings) ⇒ BF-IBE
  - GPV signatures (lattices) ⇒ GPV-IBE

BLS signatures (from a paring $e: G_0 \times G_1 \to G_T$)

- Public key: single element in G_0 or G_1
- Signature: single element in G_1 or G_0

To sign msg m: $sig \leftarrow H(m)^{sk}$, where $H: M \to G_0$

- Security: from Computational Diffie-Hellman (CDH) in the random oracle model

(when $G_0 \neq G_1$: based on co-CDH)

BLS signatures (from a paring $e: G_0 \times G_1 \rightarrow G_T$)

Properties:

- Easily aggregatable (compress many signatures into one)
- Simple (non-interactive) threshold signing
  - Either private threshold or accountable threshold
  - Proactive refresh for either model (one-round)
- Simple (one-round) blind signature

Anonymous IBE

Anonymous IBE [BDOP'04, AB…'05, BW'05, …]

Goal: IBE ciphertext E(pp, id, m)

should reveal no info about recipient id

Why?

- A natural security goal
- More importantly, enables searching on enc. Data

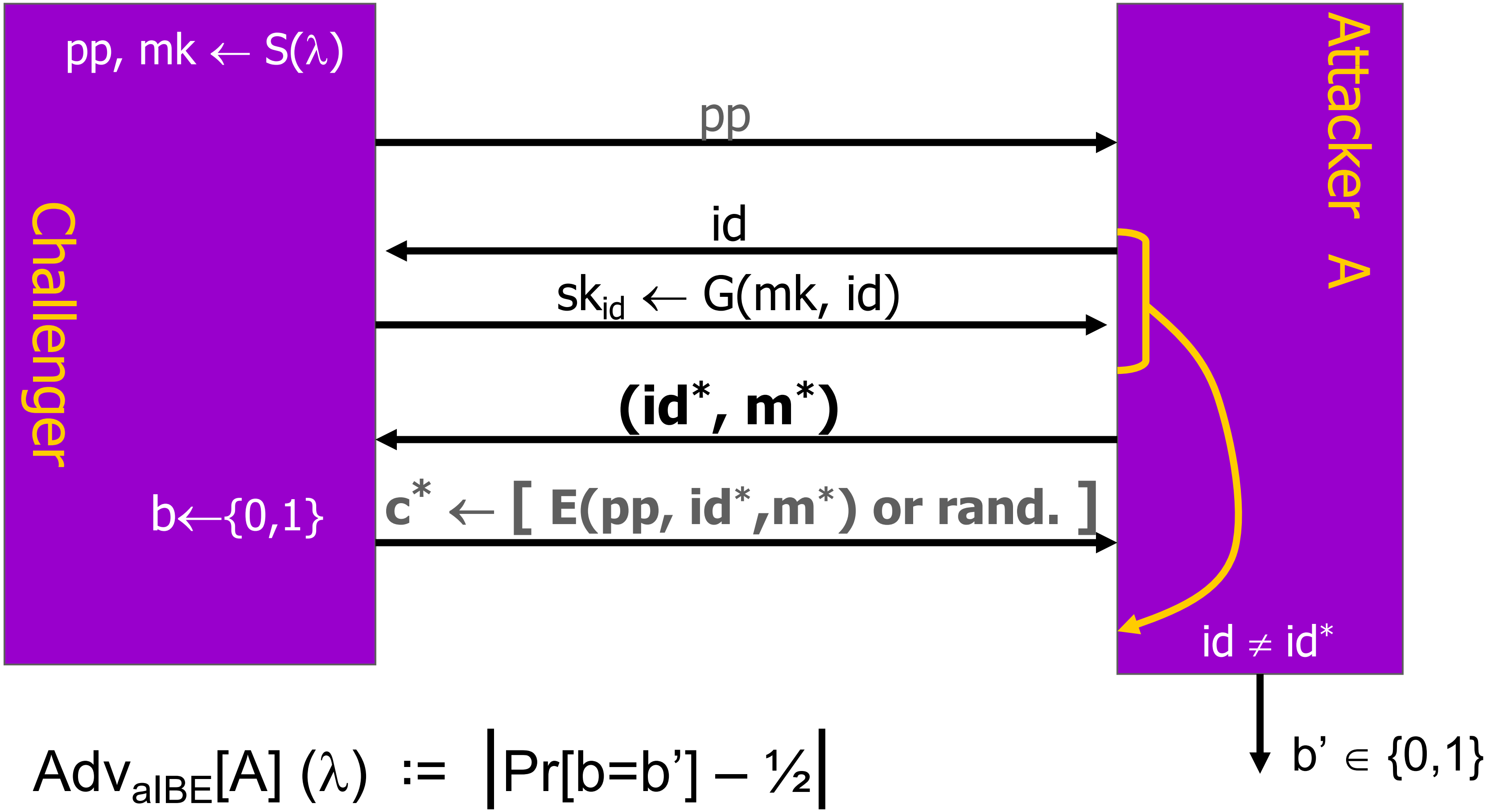
Constructions:

- RO model: BF-IBE
- std. model: 2-DLIN [BW'06], Gentry [Gen'06]
  composite order groups [BW'07,…] , and SXDH [D'10]

also many lattice-based constructions [GPV'09, CHKP'10, ABB'10,…]

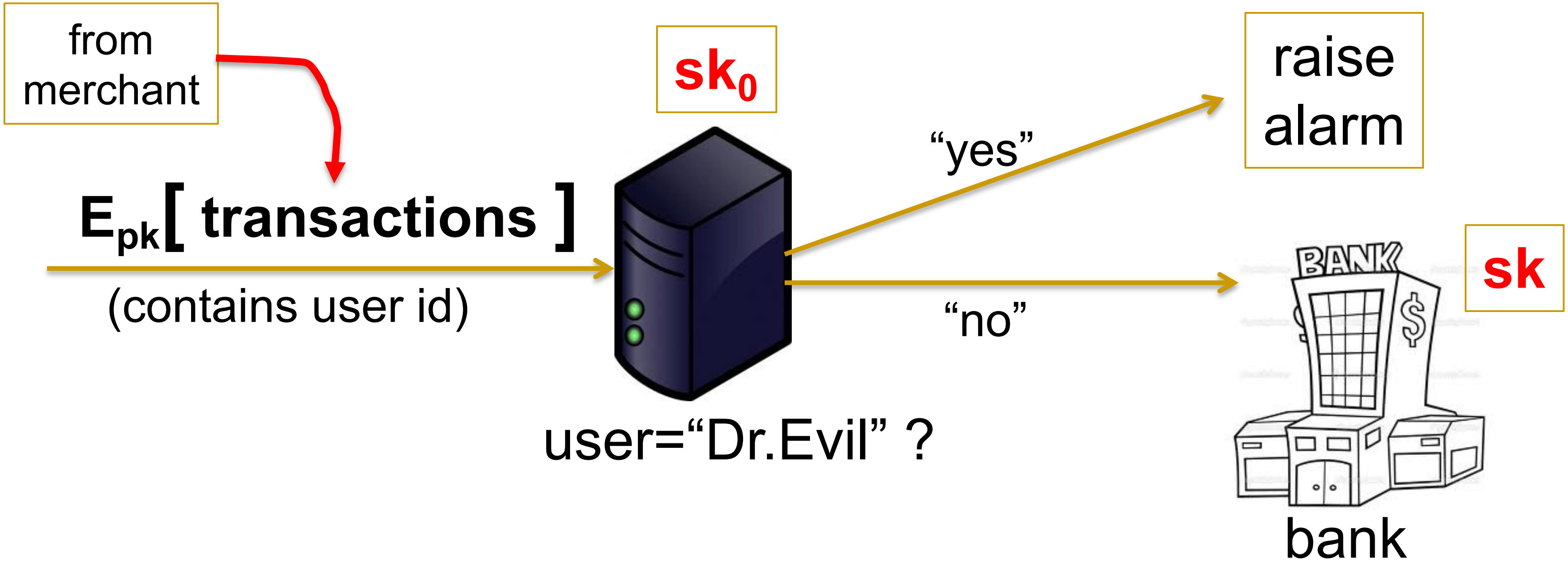
Anon. IBE systems (anonIND-IDCPA)

Semantic security when attacker has few private keys


$pp, mk \leftarrow S(\lambda)$
Challenger
$b \leftarrow \{0,1\}$
pp
id
$sk_{id} \leftarrow G(mk, id)$
(id^*, m^*)
$c^* \leftarrow [\ E(pp, id^*, m^*)$ or rand. $]$
Attacker A
$id \neq id^*$
$b' \in \{0,1\}$

$$Adv_{aIBE}[A]\ (\lambda)\ :=\ \left|Pr[b=b'] - ½\right|$$

Anon. IBE ⇒ Basic searching on enc. data



from merchant

E_{pk}[transactions]

(contains user id)

sk_0

user="Dr.Evil" ?

"yes"

raise alarm

"no"

sk

bank

Proxy needs key that lets it test "user$\overset{?}{=}$Dr.Evil" and nothing else.

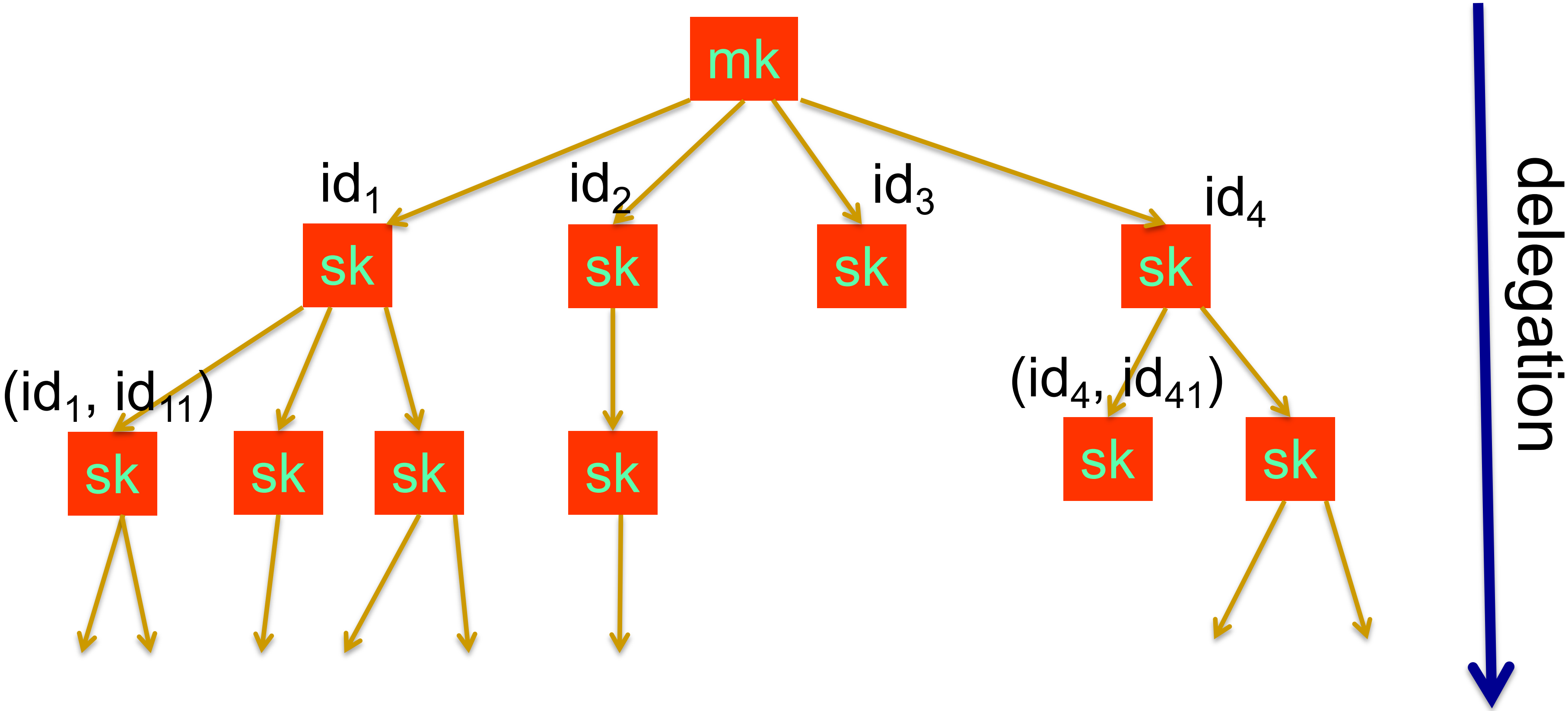
Merchant: embed c⟵E(pp, user, 1) in ciphertext

hidden

Proxy: has sk_0⟵G(sk, "Dr.Evil") ; tests D(sk_0,c) $\overset{?}{=}$ 1

Hierarchical IBE

Hierarchical IBE [HL'02, GS'02, BBG'04, …]



- Can encrypt a message to id = $(id_1, id_{11}, id_{111})$
- Only sk_{id} and parents can decrypt
  - Coalition of other nodes learns nothing

Some pairing-based HIBEs

- **GS-HIBE** [GS'03]: BDH ⇒ IND-IDCPA (in RO model)
- **BB-HIBE** [BB'04]: BDDH ⇒ IND-**s**IDCPA
- **BW-HIBE** [BW'05]: 2-DLIN ⇒ anonIND-**s**IDCPA
- Also many lattice constructions [CHKP'10, ABB'10, ABB'10a,…]

⇒ ciphertext size grows linearly with hierarchy depth

⇒ adaptive security: sec. degrades exp. in hierarchy depth

Some pairing-based HIBEs

- **GS-HIBE** [GS'03]: BDH $\Rightarrow$ IND-IDCPA (in RO model)
- **BB-HIBE** [BB'04]: BDDH $\Rightarrow$ IND-**s**IDCPA
- **BW-HIBE** [BW'05]: 2-DLIN $\Rightarrow$ anonIND-**s**IDCPA

- **BBG-HIBE** [BBG'05]: d-BDDH $\Rightarrow$ IND-**s**IDCPA

  ciphertext size **indep.** of hierarchy depth (unknown from LWE)

- **DualSys-HIBE** [LW'10]: (various, short) $\Rightarrow$ IND-IDCPA

  Similar size as BBG and good for poly. depth hierarchies

Final note: many further generalizations

- Wildcard IBE [ABCD…'06]

  encrypt to: $\text{ID} = (\ \text{id}_1,\ \ \text{id}_2,\ \ *\ ,\ \ \text{id}_3,\ \ *\ ,\ \ \text{id}_4\ )$

- Protecting the IBE master secret:
  - Threshold secret share master secret [BF'01]
  - Large incompressible master key [DGSW'22]

- More general searches on encrypted data:
  - Hidden vector encryption [BW'06]
  - Inner product encryption [KSW'08]
    - Support range queries, conjunctive queries, …

THE END