Bilinear Pairings in Cryptography:

Identity Based Encryption

Dan Boneh

Stanford University

Recall: Pub-Key Encryption (PKE)

PKE Three algorithms : (G, E, D)

$G(\lambda) \rightarrow (pk, sk)$ 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}

$E(\ pk_{alice}\ ,\ msg\ )$

Example: ElGamal encryption

- G(λ): $(G, g, q) \leftarrow \text{GenGroup}(\lambda)$

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

- E(pk, $m \in G$): $s \leftarrow Z_q$ and do $c \leftarrow (g^s, \; m \cdot h^s)$

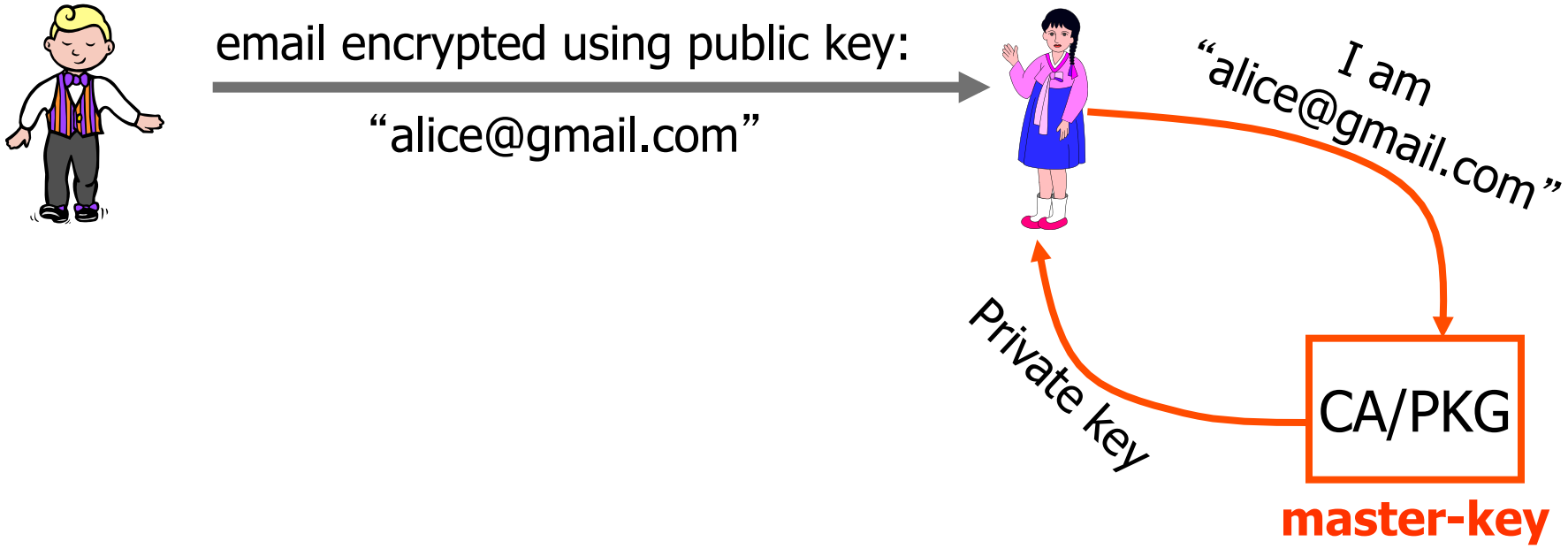
- D(sk=α, $c=(c_1,c_2)$): observe $c_1^{\alpha} = (g^s)^{\alpha} = h^s$

- Security (IND-CPA) based on the DDH assumption:

  (g, h, g^s, h^s) indist. from (g, h, g^s, g^{rand})

Identity Based Encryption [Sha '84]

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



Identity Based Encryption

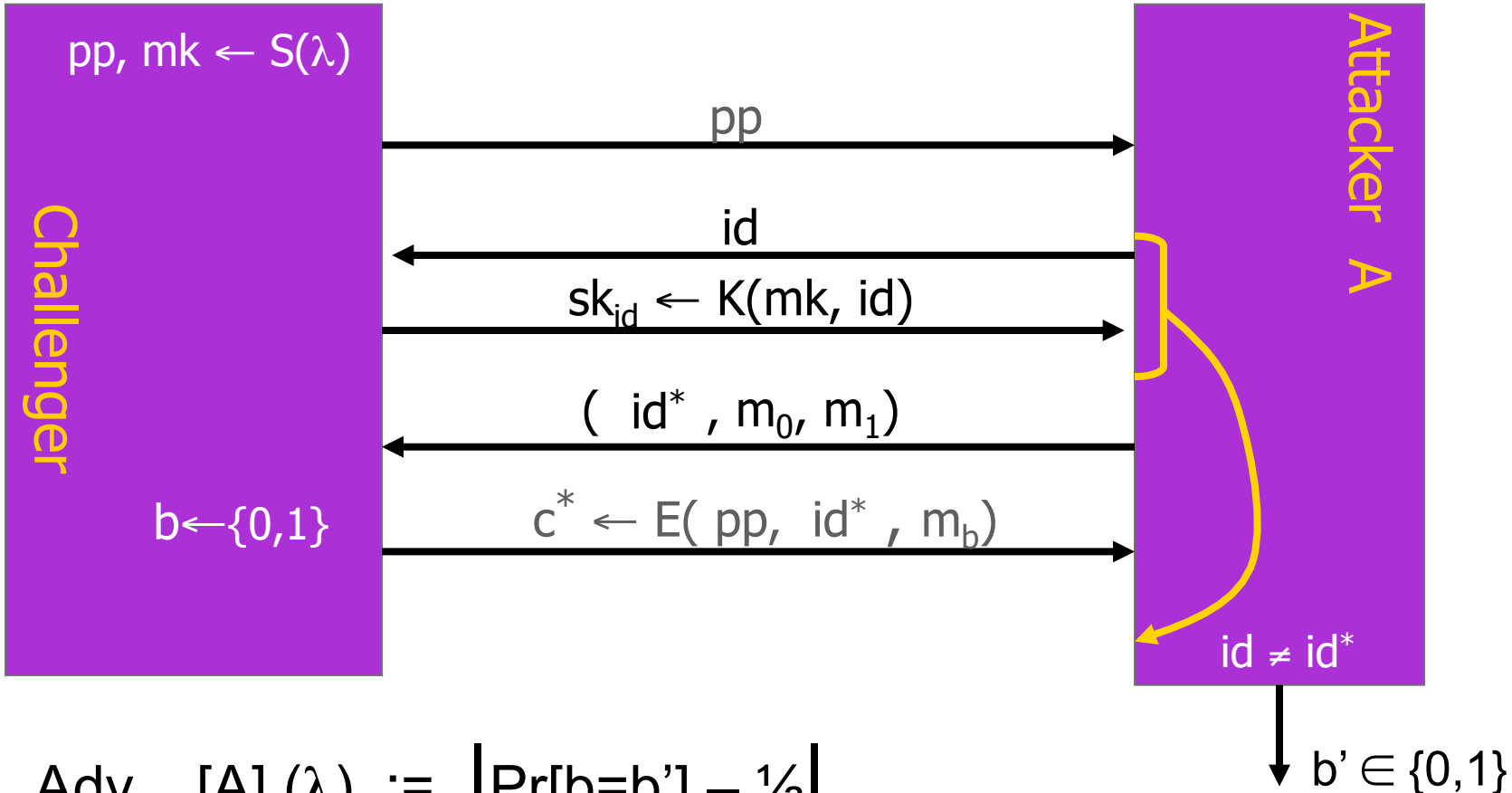
Four algorithms : (S,K,E,D)

$S(\lambda) \rightarrow (pp, mk)$	output params, pp, and master-key, mk
$K(mk, ID) \rightarrow d_{ID}$	outputs private key, d_{ID} , for ID
$E(pp, ID, m) \rightarrow c$	encrypt m using pub-key ID (and pp)
$D(d_{ID}, c) \rightarrow m$	decrypt c using d_{ID}

IBE "compresses" exponentially many pk's into a short pp

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

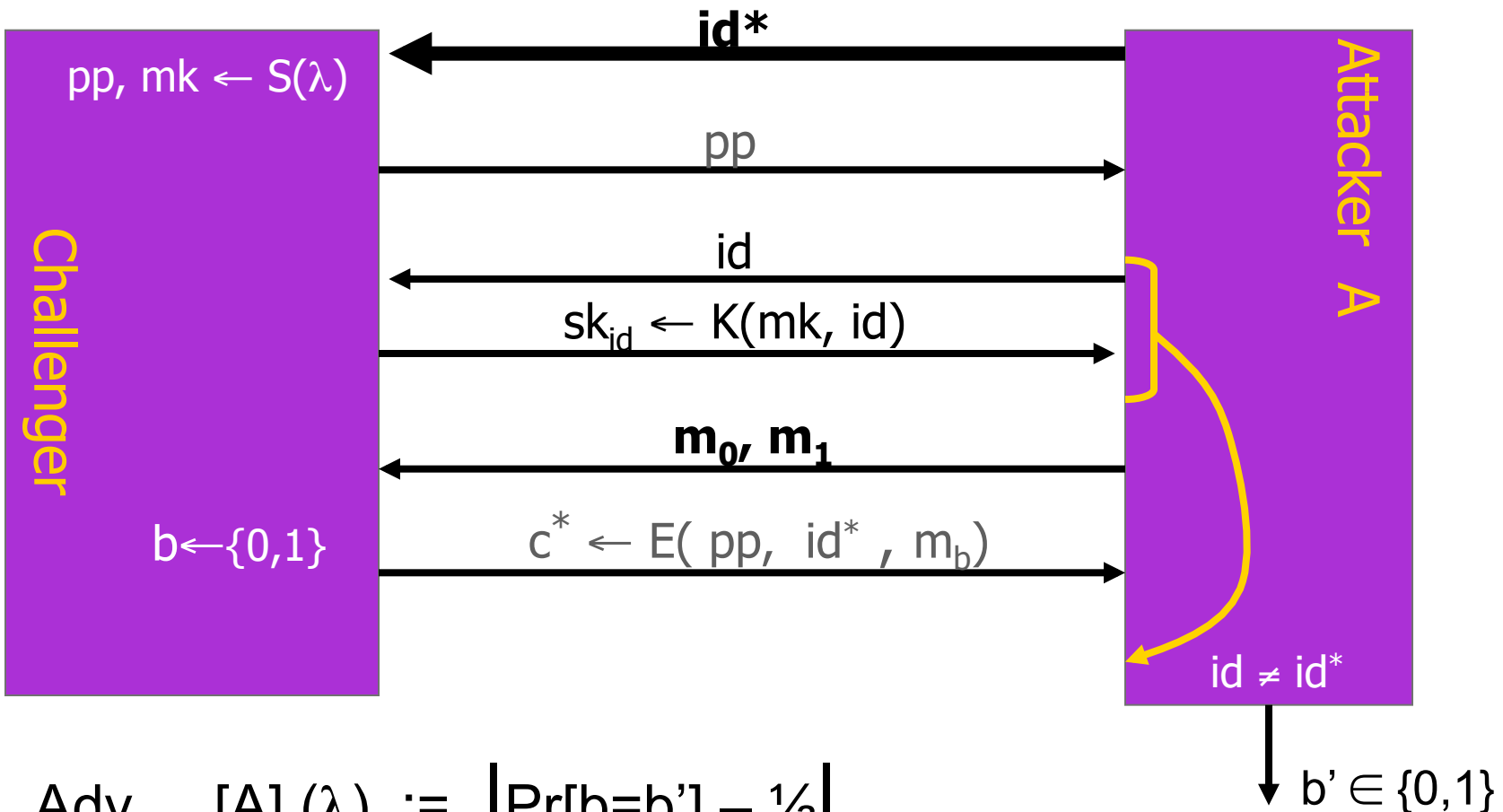
Semantic security when <u>attacker has few private keys</u>



$$Adv_{IBE}[A](\lambda) := \left|Pr[b=b'] - \tfrac{1}{2}\right|$$

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

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



$$Adv_{sIBE}[A](\lambda) := \left|Pr[b=b'] - \tfrac{1}{2}\right|$$

selective ⟶ full: generic conversion [BB'04]

- The two models are equivalent in the RO model

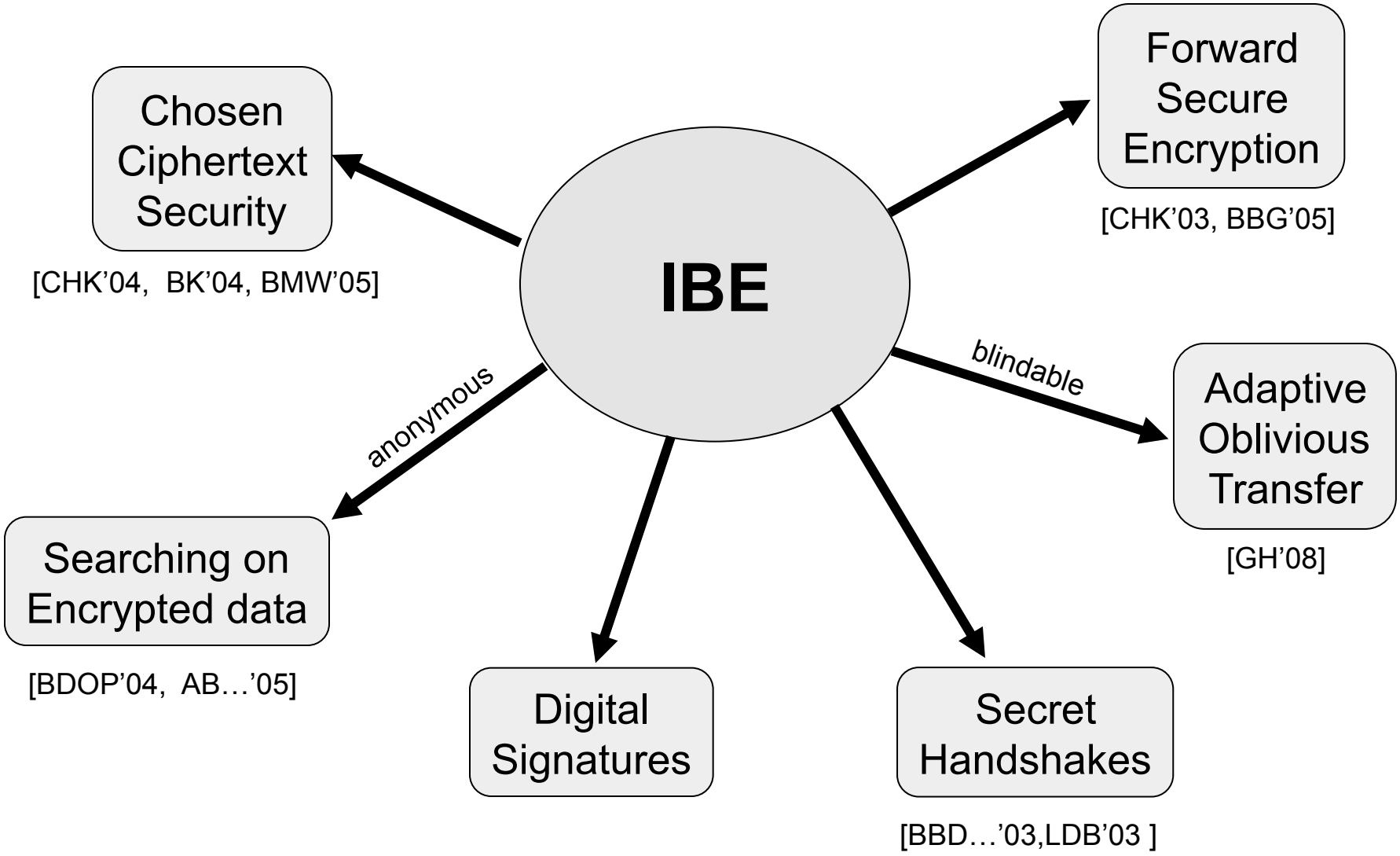
$$E(pp, id, m) \quad \longrightarrow \quad E(pp, H(id), m)$$

- In the standard model: complexity leveraging

Lemma: $\forall A \exists B$: $Adv_{\mathbf{IBE}}[A] \leq \mathbf{2^n} \cdot Adv_{\mathbf{sIBE}}[B]$

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

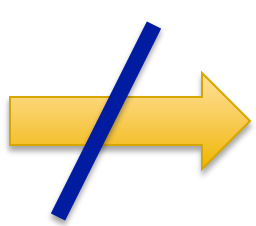
Why ID Based Encryption?



Black box separation [BPRVW'08]

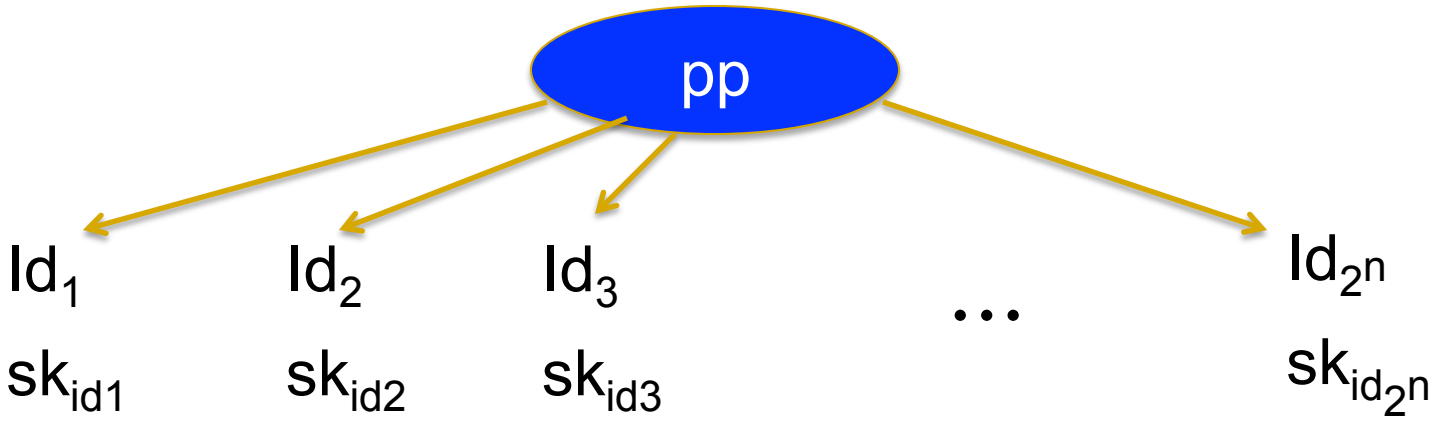
Trapdoor functions

CCA-secure public-key enc.



IBE

Main reason: short pp defines exp. many public keys

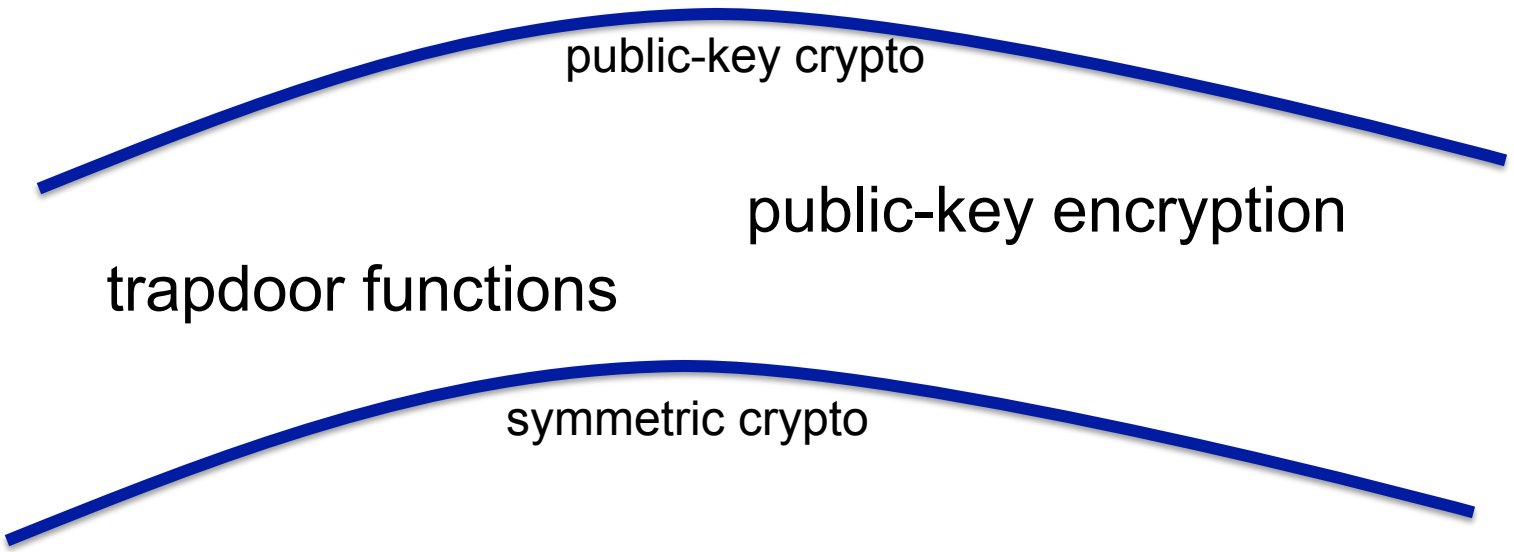


Functional encryption [BSW'11]

ABE [SW'05]

Hierarchical IBE [HL'02, GS'02]

IBE



IBE in practice

Bob encrypts message with pub-key:

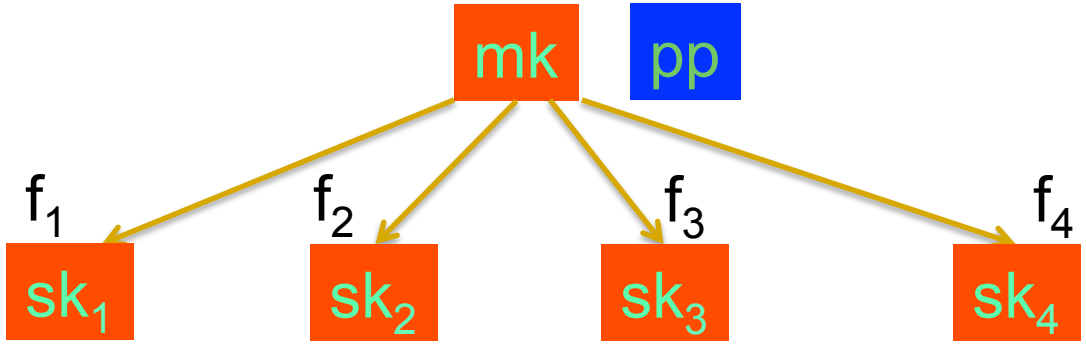
"alice@hotmail || role=accounting || time=week-num"

policy-based encryption | short-lived keys

Voltage security

Aug. 2011: "… Voltage SecureMail … with over one billion secure business emails sent annually and over 50 million worldwide users."

IBE: functional encryption view [BSW'11]



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

IBE: first non-trivial functionality

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

Constructing IBE

Can we build an IBE ??

- ElGamal is not an IBE:

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

  - 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:

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

  - Cannot map ID to (N,e)

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

    - 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, … ↔	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	some	??

Pairing-based constructions

Some pairing-based IBE constructions

- **BF-IBE** [BF'01]: BDH $\Rightarrow$ IND-IDCPA (in RO model)
- **BB-IBE** [BB'04]: BDDH $\Rightarrow$ IND-**s**IDCPA
- **Waters-IBE** [W'05]: generalizes BB-IBE

  BDDH $\Rightarrow$ IND-IDCPA (but long PP)
- **Gentry-IBE** [G'06]: q-BDHE $\Rightarrow$ IND-IDCPA and short PP
- **DualSys-IBE** [W'09]: 2-DLIN $\Rightarrow$ IND-IDCPA and short PP

  [LW'10, L'12]

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

- S(λ): $(G, G_T, g, p) \leftarrow \text{GenBilGroup}(\lambda)$, $\alpha \leftarrow F_p$

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

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

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

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

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

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

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

IBE w/o RO: a generic approach

The "all but one" paradigm

real system

Generate "**real**" PP
and "**real**" **MK**

MK: generate SK_{ID} for all id

all id

≈

simulation

Given id* do:
Generate "**fake**" PP'
and "**fake**" **MK'**

MK': all but one (id ≠ id*)

id≠ id*

challenge CT for id*
solves some hard problem

BB-IBE: IBE w/o random oracles [BB'04]

- S(λ): $(G, G_T, g, q) \leftarrow \text{GenBilGroup}(\lambda)$, $\alpha \leftarrow F_p$

  $pp := [g,\ y \leftarrow g^{\alpha},\ g_1,\ h] \in G$; $mk := g_1^{\alpha}$

- K(mk, id): $sk_{ID} \leftarrow \left(mk \cdot (y^{id} \cdot h)^{r},\ g^{r} \right)$

  $r \leftarrow F_p$

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

  $C \leftarrow \left(g^{s},\ (y^{id} \cdot h)^{s},\ m \cdot e(y, g_1)^{s} \right)$

- D((sk_1, sk_2), (c_1, c_2, c_3)):

  observe: $e(c_1, sk_1) / e(c_2, sk_2) = e(y, g_1)^{s}$

Security: the all-but-one paradigm

real system

$\alpha \leftarrow F_p$

$g_1 , h \leftarrow G$

PP: $g,\ y \leftarrow g^{\alpha},\ g_1 , h \in G$

MK: $g_1^{\alpha} \in G$

$sk_{id} \leftarrow (mk \cdot (y^{id} \cdot h)^{r} , g^{r})$

$id=id^*$

$\approx$

simulation (all but one)

Given id^* do:

$\beta \leftarrow F_p$

$g_1 , y \leftarrow G$

PP: $g,\ y,\ g_1 ,$ **$h \leftarrow y^{-id^*} \cdot g^{\beta}$**

MK': $\beta \in F_p$

$sk_{id} \leftarrow (d_0,\ d_1)$

$d_0 = g_1^{-\beta/(id-id^*)} \cdot (y^{id} \cdot h)^{r}$

$d_1 = g_1^{-1/(id-id^*)} \cdot g^{r}$

Reduction to BDDH

$$(g,\ y,\ g^r,\ g^s,\ e(y,g)^{rs}) \approx_p (g,\ y,\ g^r,\ g^s,\ R)$$

Given challenge $(g,\ y,\ g_1=g^r,\ z=g^s,\ T)$ do:

$$\mathbf{pp} = (\mathbf{g},\ \mathbf{y},\ \mathbf{g_1},\ \mathbf{h \leftarrow y^{-id^*} \cdot g^{\beta}})\ ;\quad \mathbf{mk' = \beta} \in \mathbf{F_p}$$

- Respond to adversary queries for $id \neq id^*$ using β
- Challenge ciphertext for id^* is

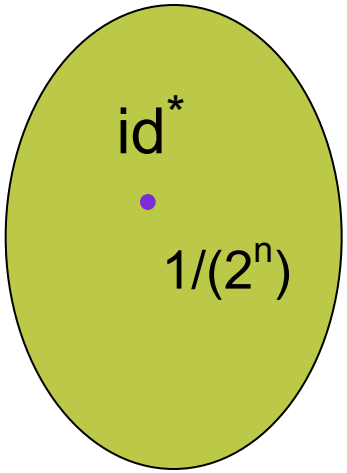
$$\mathbf{ct^* \leftarrow (\ g^s\ ,\quad (y^{id^*} \cdot h)^s\ ,\quad m \cdot e(y,g_1)^s\ )} =$$

$$\mathbf{(\ g^s\ ,\quad (g^{\beta})^s\ ,\quad m \cdot e(y,g)^{rs}\ )} =$$

$$\mathbf{(\ z\ ,\quad z^{\beta}\ ,\quad m \cdot T\ )}$$

From selective to full security [Wat '05]

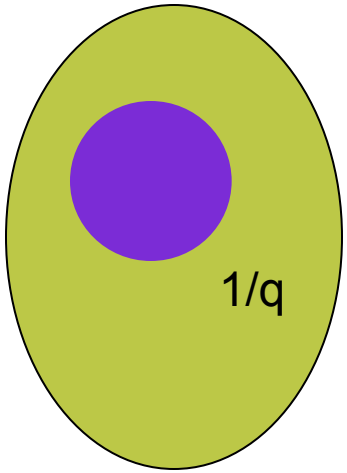
BB



id=id*

"all but one"

W



$a_1 id_1 + \ldots + a_n id_n = v$

"all but many"

(q = # private key queries from adv.)

With prob. ≈(1/q) :

all queries are "green" , but challenge id* is blue

The system [Wat '05]

- G(λ): $\alpha \leftarrow F_p$, $g_1, h, y_1, \ldots, y_n \leftarrow G$

  $pp = (g, g_1, y \leftarrow g^{\alpha}, h, y_1, \ldots, y_n) \in G$, $mk = g_1^{\alpha}$

- K(sk, id, m): $r \leftarrow F_p$, $id = b_1 b_2 \ldots b_n \in \{0,1\}^n$

  $$sk_{id} \leftarrow \left(mk \cdot (y_1^{b_1} \cdots y_n^{b_n} \cdot h)^r , g^r \right) \in G^2$$

- E(pk, $id = b_1 b_2 \ldots b_n$, m):

  $e(c_1, g) / e(y_1^{b_1} \ldots y_n^{b_n} \cdot h, c_2) = e(g_1, y)$

Gentry's IBE [Gen'06]

- S(λ): $(G, G_T, g, q) \leftarrow \text{GenBilGroup}(\lambda)$, $\alpha \leftarrow F_p$

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

- K(mk, id): $sk \leftarrow \left[\ r \leftarrow F_p \ , \ \left(h\, g^{-r}\right)^{1/(\alpha-id)} \ \right]$

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

$$C \leftarrow \left(\ y^s \cdot g^{-s \cdot id} \ , \ e(g,g)^s \ , \ m \cdot e(g,h)^{-s} \ \right)$$

$$= g^{s(\alpha-id)}$$

Proof idea (IND-IDCPA security)

Simulator knows **one** private key for **every** ID

⇒ can respond to all private key queries

⇒ tight reduction to hardness assumption

Hardness assumption (simplified): **q-BDDH** [MSK'02, BB'04, …]

given $g, v, g^{\alpha}, g^{(\alpha^2)}, \ldots, g^{(\alpha^q)}$:

$$e(g,v)^{(\alpha^{q+1})} \approx_p \text{uniform}(G_T)$$

(q = # private key queries from adv.)

note: challenge ct always decrypts correctly under simulator's secret key

Proof idea (IND-IDCPA security)

Simulator: given $g, v, g^{\alpha}, g^{(\alpha^2)}, \ldots, g^{(\alpha^q)}$

- **Setup**: rand. poly. $f(x) = a_0 + a_1 \cdot x + \ldots + a_q x^q \in F_p[x]$

  give adv. $PP := (g, y=g^{\alpha}, h \leftarrow g^{f(\alpha)})$

- **Queries**: need $sk = \left[r \leftarrow F_p , \left(h\, g^{-r}\right)^{1/(\alpha-id)} \right]$

  do: $r \leftarrow f(id)$, $\mathbf{\left(h\, g^{-r}\right)^{1/(\alpha-id)} = g^{[f(\alpha) - f(id)] / (\alpha - id)}}$

  and observe that $[f(x) - f(id)] / (x - id) \in F_p[x]$

DualSys IBE [Wat'09, LW'10, L'12]

Covered in Allison Lewko's lecture

- Full security: IND-IDCPA
- Short PP
- Security from 2-DLIN

The system: (in composite order groups) $G = G_{p1} \times G_{p2} \times G_{p3}$

- Ciphertext lives in G_p and is same as in BB
- Secret key: $sk_{ID} \leftarrow (\; mk \cdot (y^{id} \cdot h)^{r} \cdot R_{p3} \; , \quad g^{r} \cdot R'_{p3} \;)$

New Signature Systems

CDH $\Rightarrow$ short and efficient sigs (!!)

IBE $\Rightarrow$ Simple digital Signatures [N' 01]

- Sign(MK, m): sig $\leftarrow$ K(MK, m)
- Verify(PP, m, sig): Test that **sig** decrypts messages encrypted using m

- Conversely: which sig. systems give an IBE?
  - Rabin signatures: [Cocks' 01, BGH' 07]
  - GPV signatures: [GPV'09]
  - Open problem: IBE from GMR, GHR, CS, …

Signatures w/o Random Oracles

Example: signature system from BB-IBE (selectively unforgeable)

- G(λ): $\alpha \leftarrow F_p$, $g_1, h \leftarrow G$

  $pk = (g, g_1, y \leftarrow g^{\alpha}, h) \in G$, $sk = g_1^{\alpha}$

- Sign(sk, m): $r \leftarrow F_p$,

  $S \leftarrow (sk \cdot (y^m h)^r, g^r) \in G^2$

- Verify(pk, m, S=(s_1,s_2)): $e(s_1, g) / e(y^m h, s_2) \stackrel{?}{=} e(g_1, y)$

Can be made exist. unforgeable in composite order groups [LW'10,GLOW'12]

Waters Sigs: existentially unforgeable [Wat '05]

- G(λ): $\alpha \leftarrow F_p$, $g_1, h, y_1, \ldots, y_n \leftarrow G$

  $pk = (g, g_1, y \leftarrow g^{\alpha}, h, y_1, \ldots, y_n) \in G$, $sk = g_1^{\alpha}$

- Sign(sk, m): $r \leftarrow F_p$, $m = m_1 m_2 \ldots m_n \in \{0,1\}^n$

  $$S \leftarrow \left(sk \cdot (y_1^{m_1} y \ldots h y_n^{m_n} \cdot h)^r , \; g^r \right) \in G^2$$

- Verify(pk, m, $S=(s_1, s_2)$):

  $e(s_1, g) \; / \; e(y_1^{m_1} \ldots y_n^{m_n} \cdot h, \; s_2) = e(g_1, y)$

Summary thus far

IBE from pairings:

- BDDH or 2-DLIN $\Rightarrow$ efficient secure IBE

Short signatures from pairings:

- CDH $\Rightarrow$ existential unforgeablility
- with RO: **sig** $\in$ **G** [BLS'01] , without RO: **sig** $\in \mathbf{G}^2$ [Wat'05]

Anonymous IBE

Simplest non-trivial example of

"private index functional encryption"

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

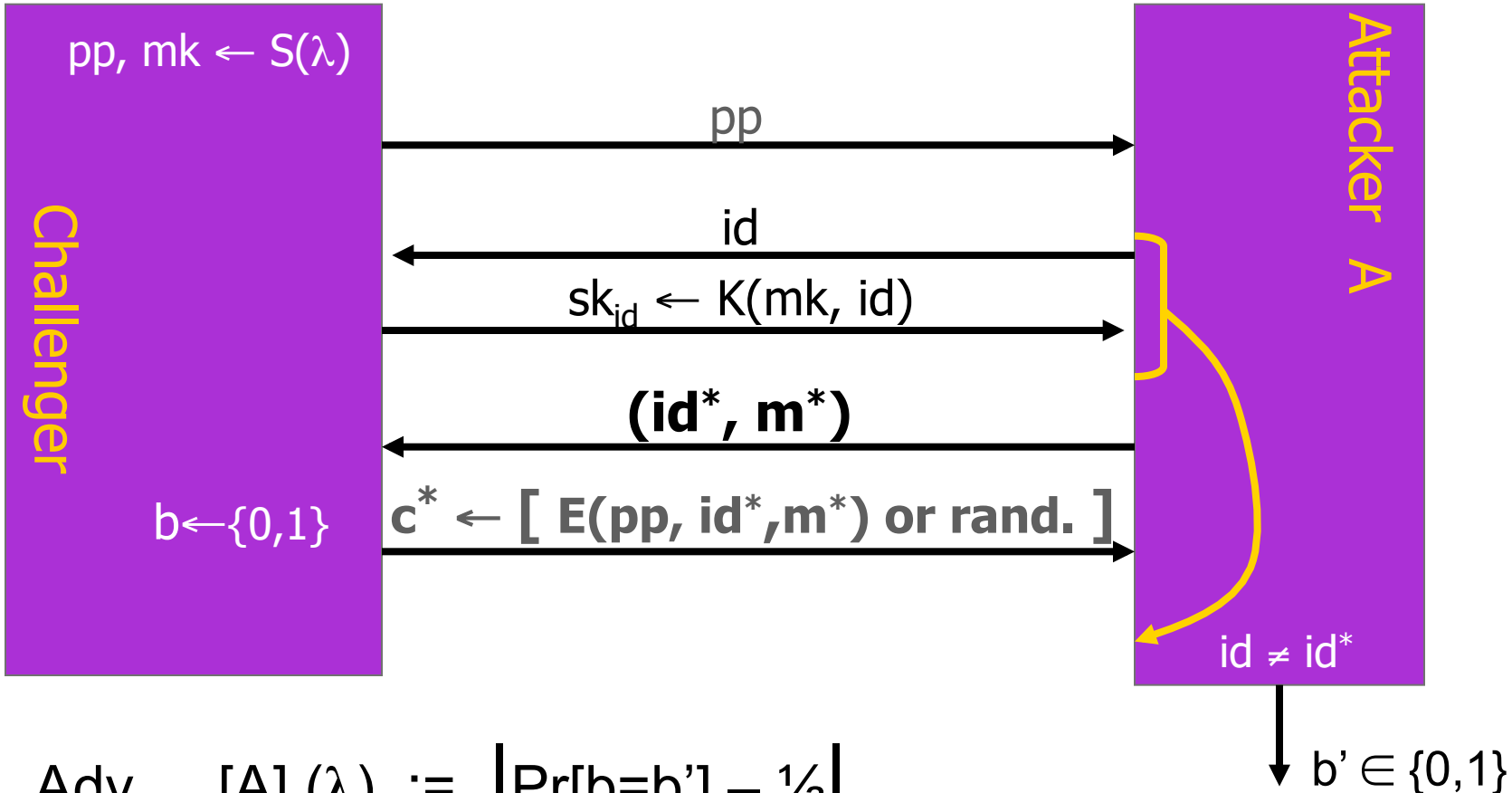
Constructions:

- 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]

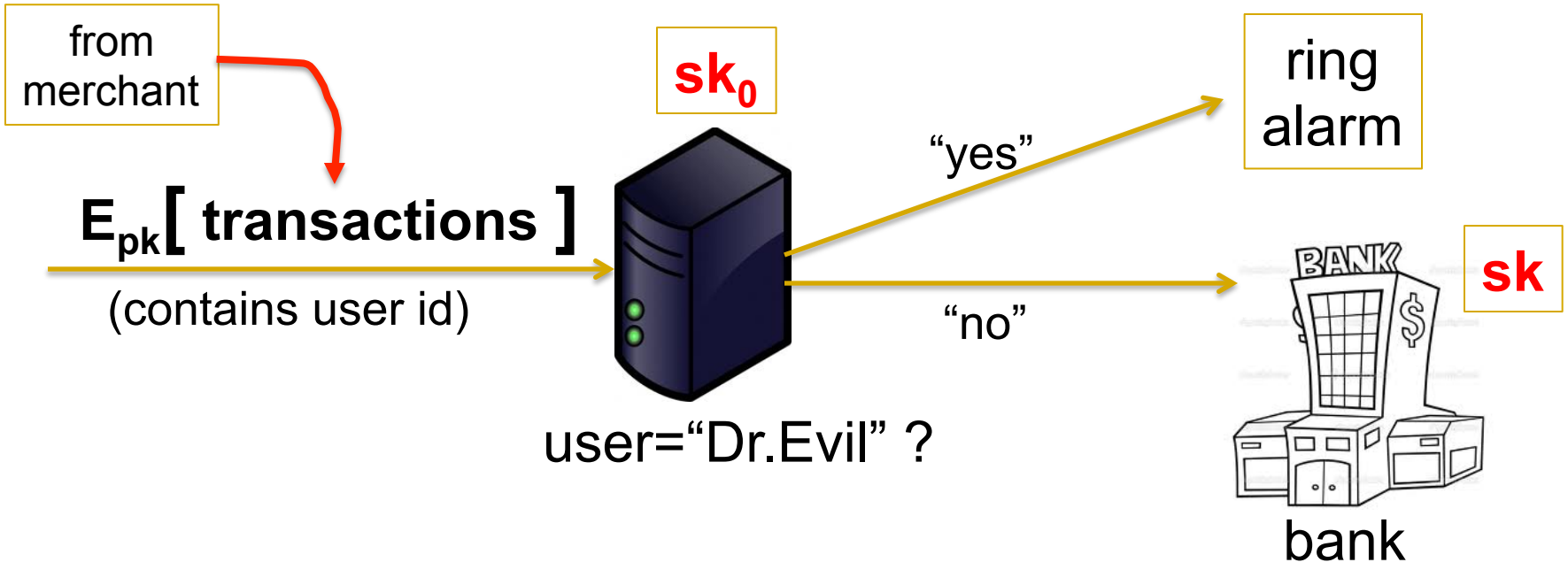
Anon. IBE systems (anonIND-IDCPA)

Semantic security when <u>attacker has few private keys</u>



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

Anon. IBE ⇒ Basic searching on enc. data



Proxy needs key that lets it test "user=Dr.Evil" and nothing else.

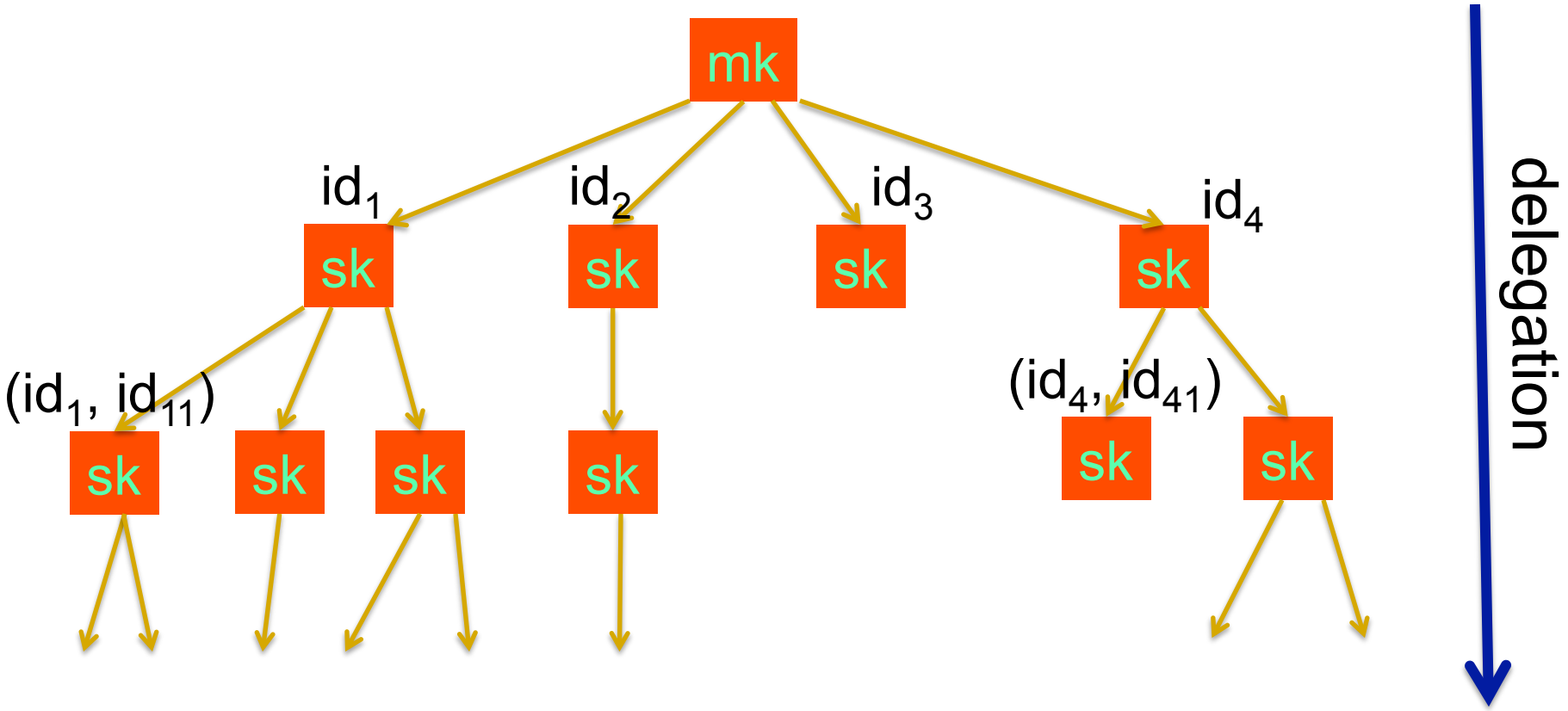
Merchant: embed $c \leftarrow E(pp, \text{user}, 1)$ in ciphertext

hidden

Proxy: has $sk_0 \leftarrow K(sk, \text{"Dr.Evil"})$; tests $D(sk_0, c) \stackrel{?}{=} 1$

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

⇒ ciphertext size grows linearly with hierarchy depth

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

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

- **BBG-HIBE** [BBG'05]: d-BDDH ⇒ IND-**s**IDCPA

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

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

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

- **BBG-HIBE** [BBG'05]: d-BDDH ⇒ IND-**s**IDCPA

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

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

  Similar size as BBG and good for poly. depth hierarchies

Example: BBG-HIBE [BBG'05]

- S(λ): $(G, G_T, g, q) \leftarrow \text{GenBilGroup}(\lambda)$, $\alpha \leftarrow F_p$

$$pp := [g,\ y \leftarrow g^{\alpha}, g_2, g_3, h_1, \ldots, h_d] \in G \quad ; \quad mk := (g_2)^{\alpha}$$

- K(mk, $(\mathbf{id}_1,\ldots,\mathbf{id}_k)$):

$$sk \leftarrow [\ \underbrace{mk \cdot (h_1^{id_1} \ldots h_k^{id_k} g_3)^r,\ g^r}_{\text{for decryption}}\ ,\ \underbrace{h_{k+1}^r, h_{k+2}^r \ldots, h_d^r}_{\text{for delegation}}\ ]$$

Example: BBG-HIBE [BBG'05]

- $S(\lambda)$: $(G, G_T, g, q) \leftarrow \text{GenBilGroup}(\lambda)$, $\alpha \leftarrow F_p$

$$pp := [g,\ y \leftarrow g^{\alpha}, g_2, g_3, h_1, \ldots, h_d] \in G \quad ; \quad mk := (g_2)^{\alpha}$$

- **Delegation**: $sk(id_1,\ldots,id_k) \rightarrow sk(id_1,\ldots,id_k,id_{k+1})$

$$sk \leftarrow \left[\ mk \cdot (h_1^{id_1} \ldots h_k^{id_k} g_3)^r\ ,\ g^r\ ,\ h_{k+1}^r\ ,\ h_{k+2}^r \ldots,\ h_d^r\ \right]$$

absorb and re-randomize

Example: BBG-HIBE [BBG'05]

- $S(\lambda)$: $(G, G_T, g, q) \leftarrow \text{GenBilGroup}(\lambda)$, $\alpha \leftarrow F_p$

$$pp := [g,\ y \leftarrow g^{\alpha}, g_2, g_3, h_1, \ldots, h_d] \in G \quad ; \quad mk := (g_2)^{\alpha}$$

- **Delegation**: $sk(id_1,\ldots,id_k) \rightarrow sk(id_1,\ldots,id_k,id_{k+1})$

$$sk \leftarrow [\ mk \cdot (h_1^{id_1} \ldots h_k^{id_k} g_3)^{r},\ g^{r},\ h_{k+1}^{r}, h_{k+2}^{r} \ldots, h_d^{r}\ ]$$

$$sk \leftarrow [\ mk \cdot (h_1^{id_1} \ldots h_{k+1}^{id_{k+1}} g_3)^{t},\ g^{t},\ h_{k+2}^{t} \ldots, h_d^{t}\ ]$$

Example: BBG-HIBE [BBG'05]

- S(λ): $(G, G_T, g, q) \leftarrow \text{GenBilGroup}(\lambda)$, $\alpha \leftarrow F_p$

$$pp := [g,\ y \leftarrow g^{\alpha}, g_2, g_3, h_1, \ldots, h_d] \in G \quad ; \quad mk := (g_2)^{\alpha}$$

- E(pp, $(\mathbf{id}_1,\ldots,\mathbf{id}_k)$, m): $s \leftarrow F_p$ and do

$$C \leftarrow \left(g^{s}, \ (h_1^{id_1} \ldots h_k^{id_k} g_3)^{s}, \ m \cdot e(y, g_2)^{\mathbf{s}} \right)$$

Final note: many further generalizations

- Wildcard IBE [ABCD…'06]

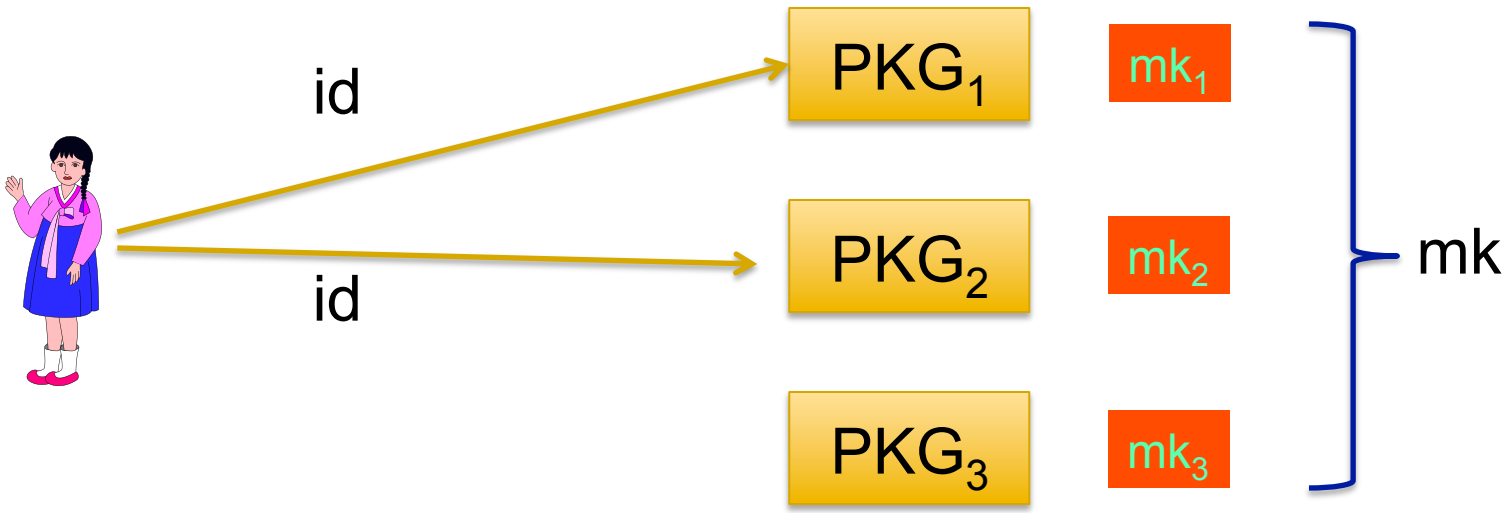
  encrypt to: ID = (id_1, id_2, * , id_3, * , id_4)

- Hidden vector encryption [BW'06] and
  Inner product encryption [KSW'08]
  - Support more general searches on encrypted data
    e.g. range queries, conjunctive queries, …

- Next topic: attribute based encryption [SW'05]

Open problems:

- HIBE or IBE w/o RO from quadratic residuosity
- Threshold IBE from LWE (and threshold signatures)



… Shamir secret sharing blows up vector length

- Gentry or DualSys IBE from LWE (IND-IDCPA, const. size PP)

THE END