Bar Ilan Winter School. Feb. 2013

Bilinear Pairings in Cryptography: **Identity Based Encryption**

Dan Boneh

Stanford University

(2 hours)

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

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

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

- $E(pk, m \in G)$: $s \leftarrow Z_q$ and do $c \leftarrow \left(g^s , \quad m \cdot h^{\mathbf{s}} \right)$

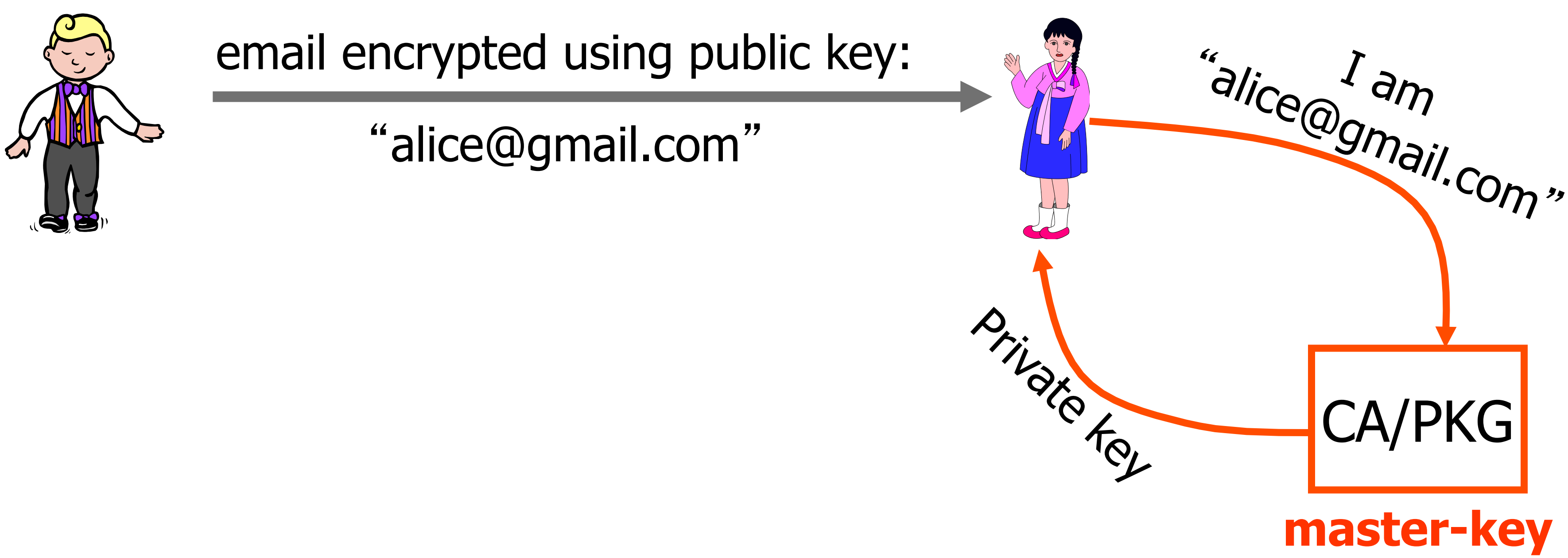
- $D(sk=\alpha, c=(c_1,c_2))$: observe $c_1^{\alpha} = (g^s)^\alpha = h^s$

- 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 <u>arbitrary</u> string
  - e.g. e-mail address, phone number, IP addr…



Identity Based Encryption [Sha ' 84]

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

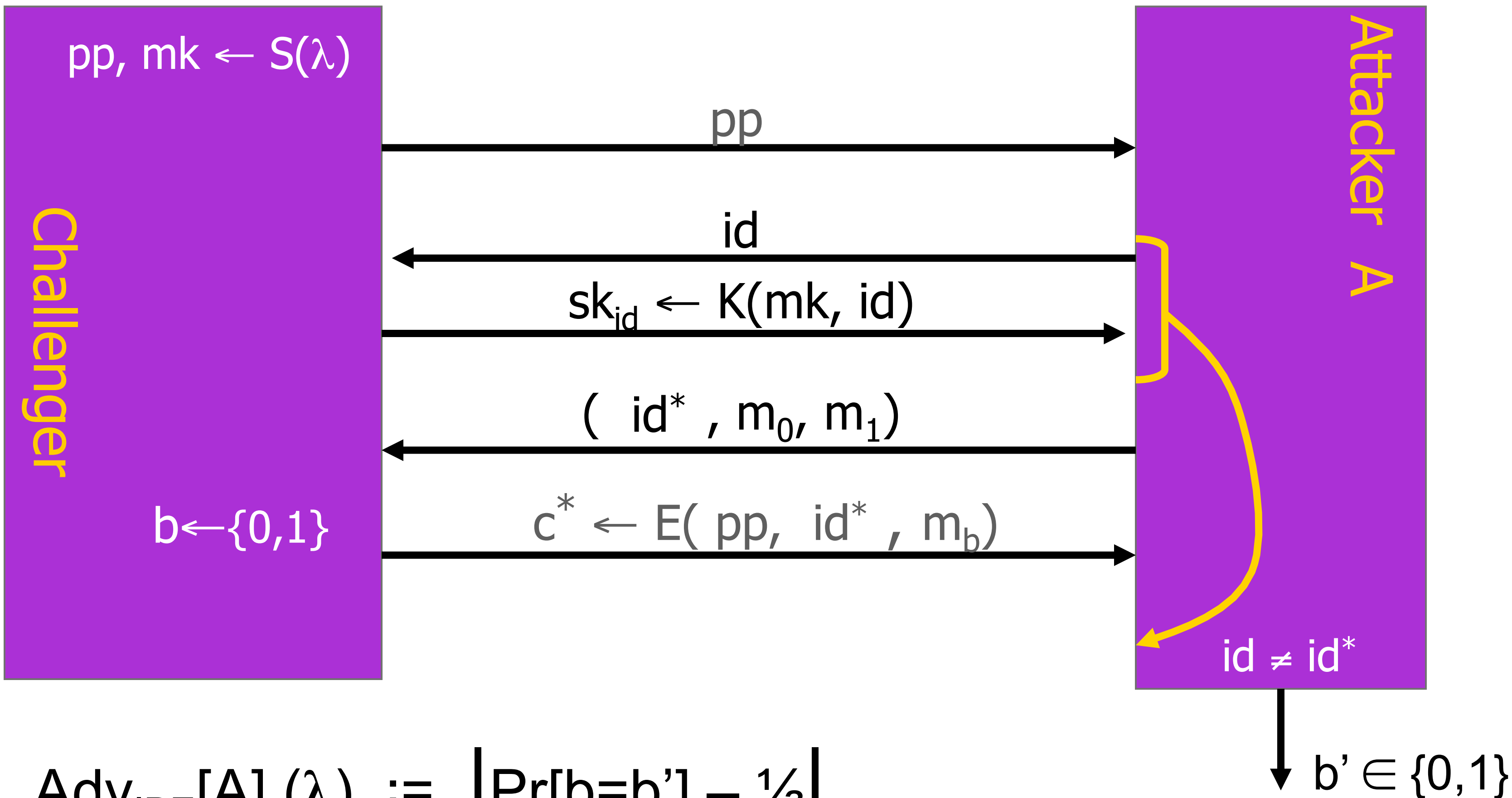
E(pp, ID, m) $\rightarrow$ c encrypt m using pub-key ID (and pp)

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

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

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

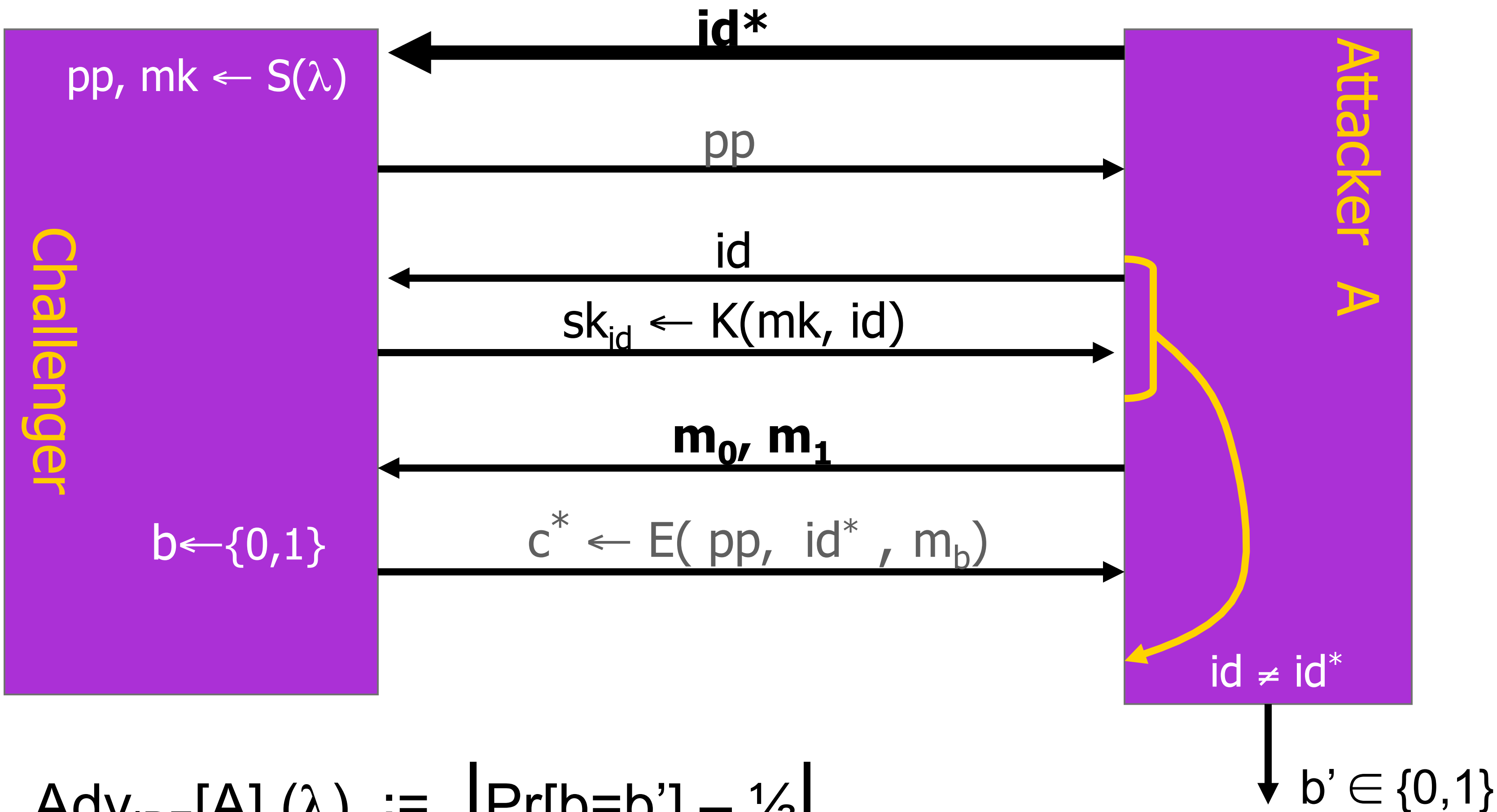
Semantic security when attacker has few private keys



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

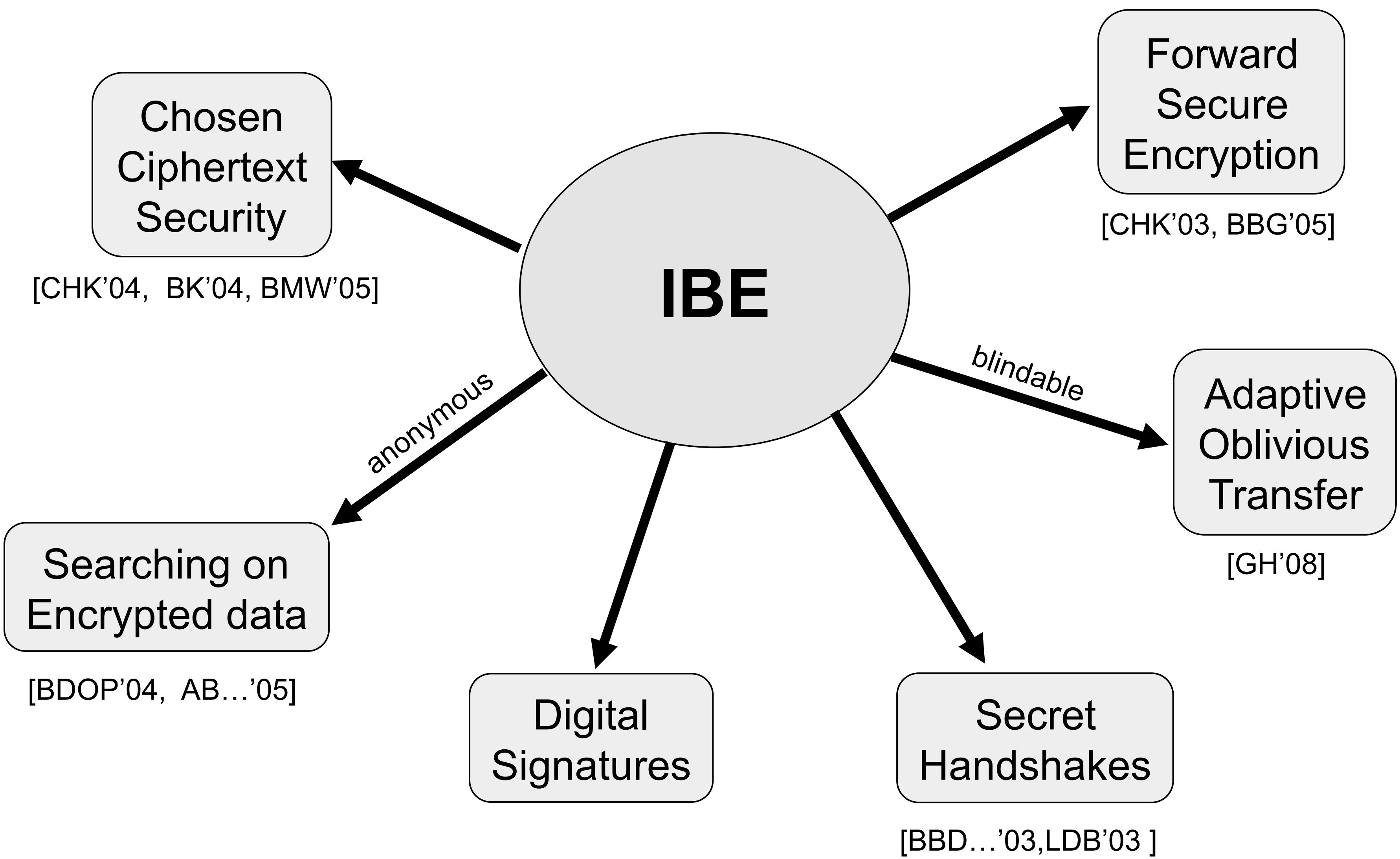
CPA-Secure IBE systems (IND-sIDCPA) [CHK'04]

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



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

Why ID Based Encryption?



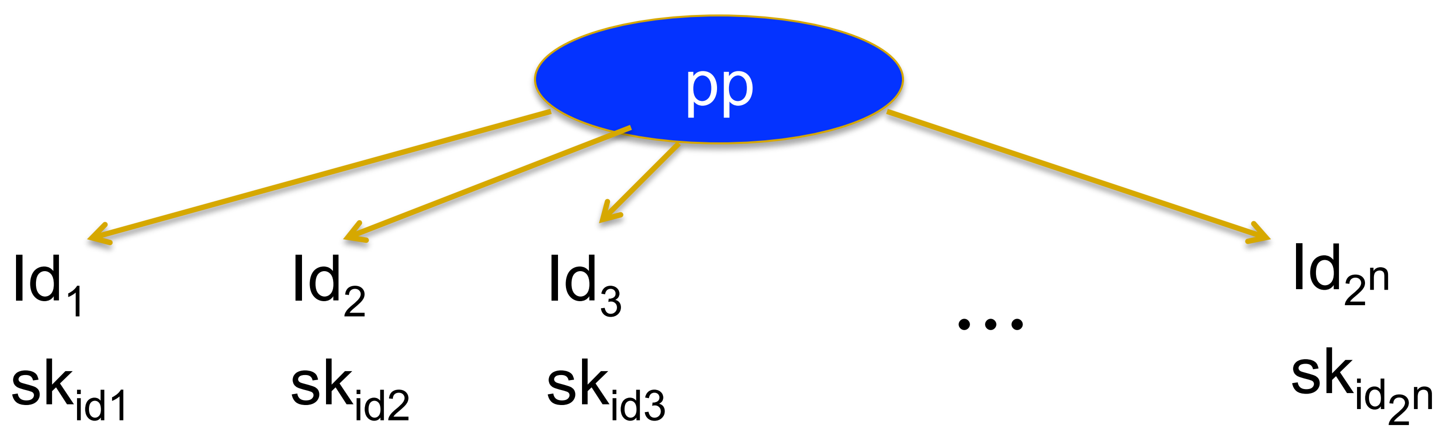
Black box separation [BPRVW'08]

Trapdoor functions

CCA-secure public-key enc.

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

Main reason: short pp defines exp. many public keys



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:

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

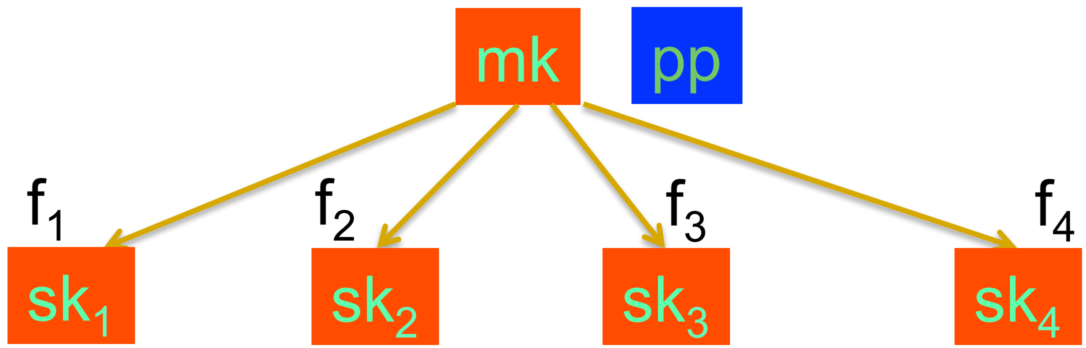
policy-based encryption

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]



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

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:

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

  - pk can be any string: **h = "*alice@gmail.com*" ∈ 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} = 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

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

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

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

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

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

IBE w/o RO: a generic approach

The "all but one" paradigm

real system		simulation
Generate "**real**" PP and "**real**" MK **MK**: generate SK_{ID} for all id all id	$\approx$	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): $sk_{ID} \leftarrow (\ mk \cdot (y^{id} \cdot h)^{\mathbf{r}}\ ,\ g^{\mathbf{r}}\ )$

  $r \leftarrow F_p$

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

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

- D((d_1, d_2), (c_1, c_2, c_3)):

  observe: $e(c_1, d_1) \,/\, e(c_2, d_2) = e(y, g_1)^s$

Security: the all-but-one paradigm

real system		simulation (all but one)
		Given id* do:
$\alpha \leftarrow F_p$		$\beta \leftarrow F_p$
$g_1, h \leftarrow G$		$g_1, y \leftarrow G$
PP: $g,\ y \leftarrow g^{\alpha},\ g_1, h \in G$	$\approx$	PP: $g,\ y,\ g_1,\ \boldsymbol{h \leftarrow y^{-id^*} \cdot g^{\beta}}$
MK: $g_1^{\alpha} \in G$		**MK':** $\boldsymbol{\beta \in F_p}$
$sk_{id} \leftarrow (\ mk \cdot (y^{id} \cdot h)^{\mathbf{r}},\ g^{\mathbf{r}}\ )$		$sk_{id} \leftarrow (\ d_0,\ d_1\ )$

id=id*

$$\begin{cases} d_0 = g_1^{-\beta/(id-id^*)} \cdot (y^{id} \cdot h)^r \\ d_1 = g_1^{-1/(id-id^*)} \cdot g^r \end{cases}$$

Reduction to BDDH

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

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

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

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

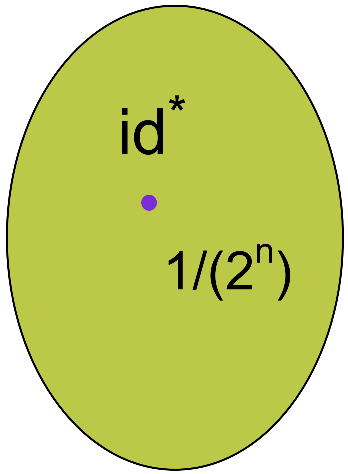
$$ct^* \leftarrow (\,g^s,\ (y^{id} \cdot h)^s,\ m \cdot e(y,g_1)^s\,) =$$

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

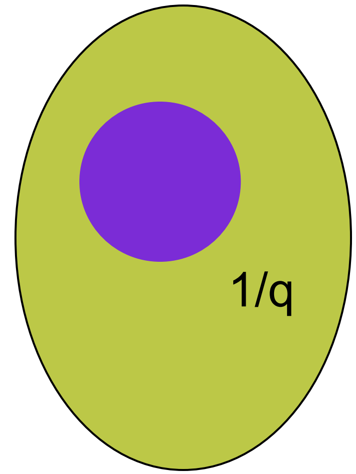
$$(\,z,\ z^{\beta},\ m \cdot R\,)$$

From selective to full security [Wat '05]

BB



W



$id = id^*$

"all but one"

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

"all but many"

(q = # private key queries from adv.)

With prob. $\approx(1/q)$:

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

The system [Wat ’05]

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

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

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

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

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

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

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

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

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

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

(q = # private key queries from adv.)

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

Proof idea (IND-IDCPA security)

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

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

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

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

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

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

DualSys IBE [Wat'09, LW'10]

Covered in Allison Lewko's lecture

New Signature Systems

CDH $\Longrightarrow$ 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

- <u>Conversely</u>: 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 secure)

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

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

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

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

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

Waters Sigs: existentially unforgeable [Wat ' 05]

- $\underline{G(\lambda)}$: $\alpha \leftarrow F_p$, $g_1, h, y_1, \ldots, y_n \leftarrow G$

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

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

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

- 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: $\mathbf{sig} \in \mathbf{G}$, without RO: $\mathbf{sig} \in \mathbf{G}^2$

[BLS'01] [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

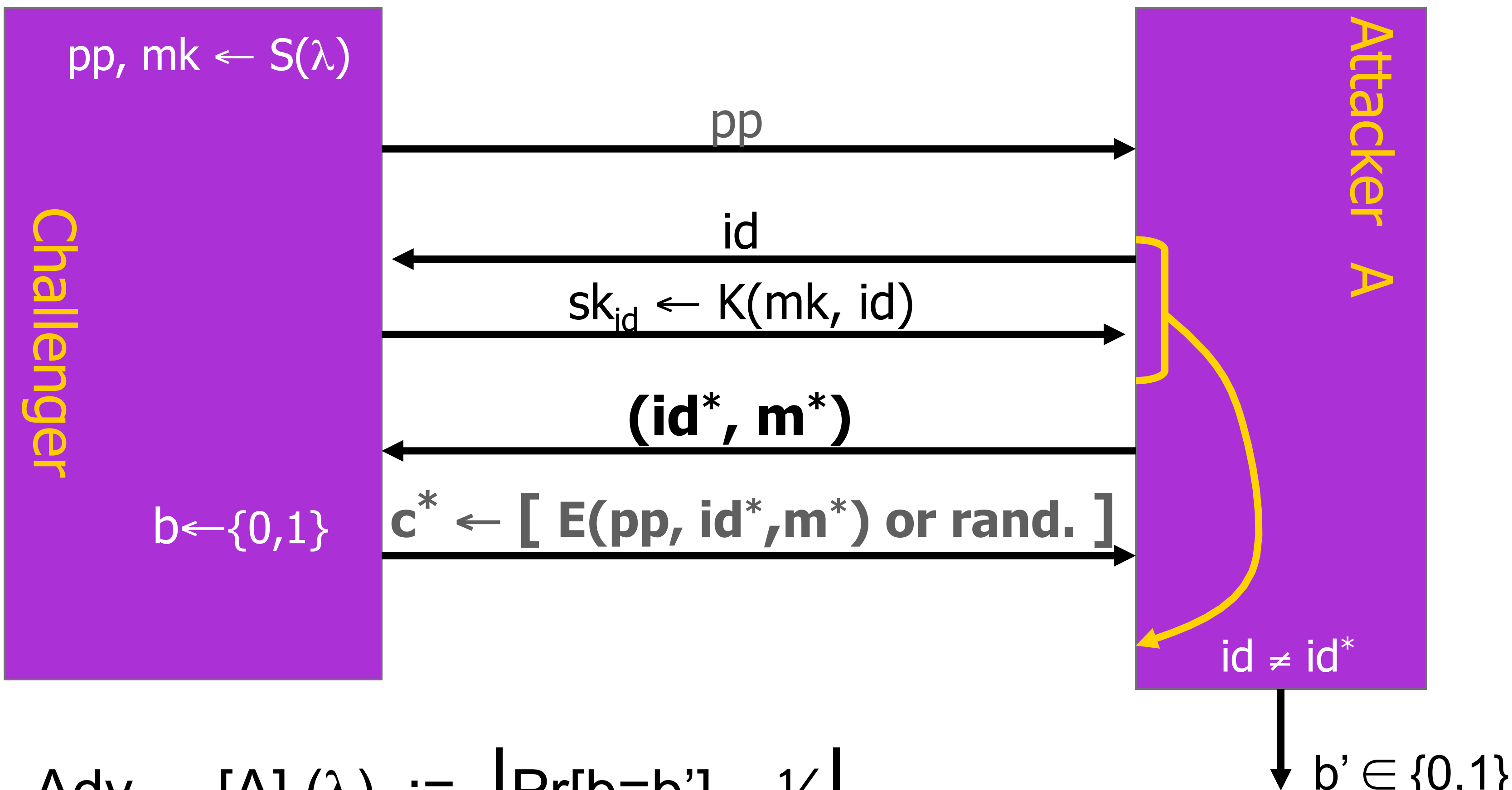
Constructions:

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

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

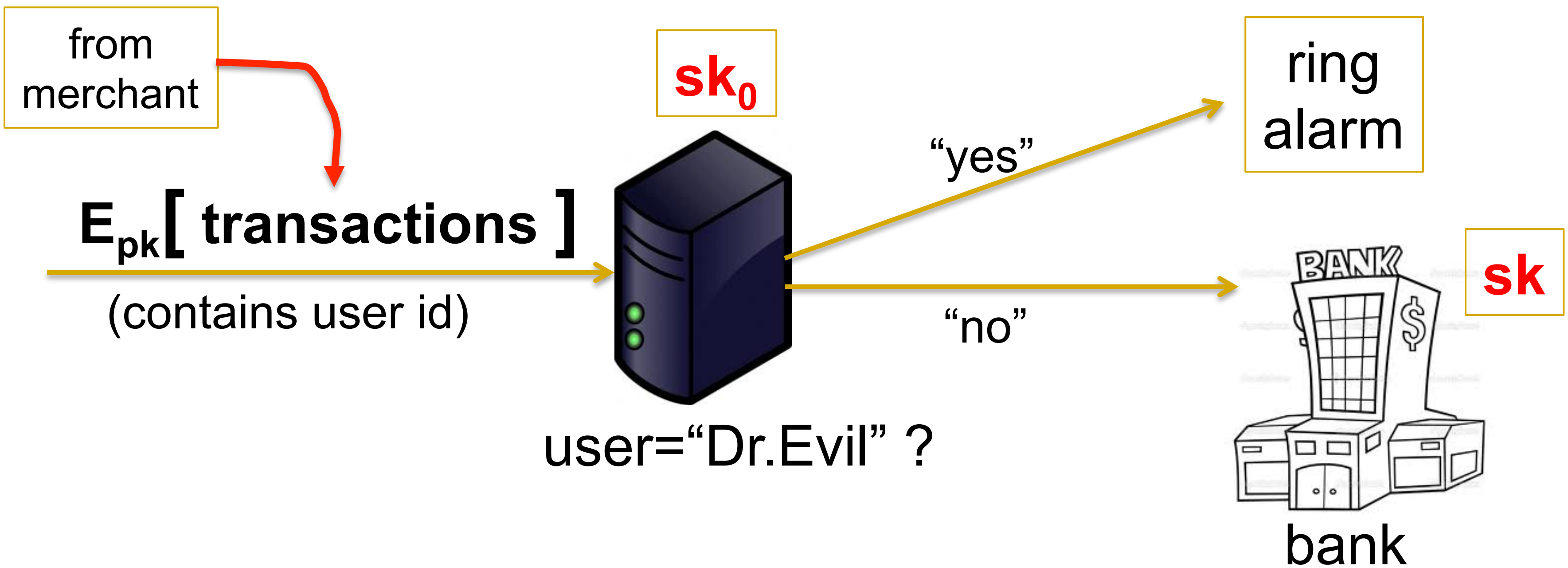
Anon. IBE systems (anonIND-IDCPA)

Semantic security when attacker has few private keys



$$\mathrm{Adv}_{\mathrm{aIBE}}[A]\ (\lambda)\ :=\ \left|\Pr[b=b'] - 1/2\right|$$

Anon. IBE $\Rightarrow$ Basic searching on enc. data



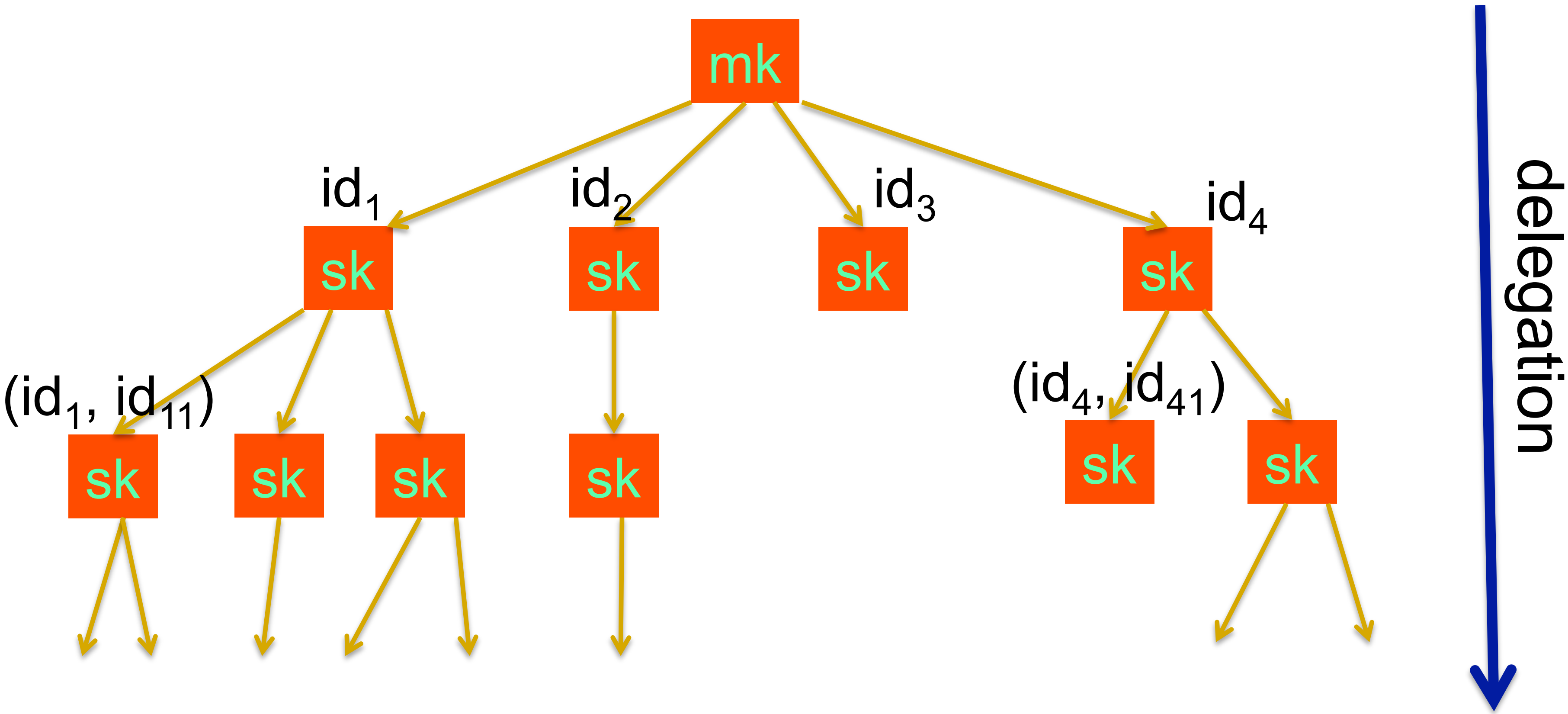
Proxy needs key that lets it test "user=Dr.Evil" and nothing else.

Merchant: embed $c \longleftarrow E(\, pp,\ user,\ 1\,)$ in ciphertext

Proxy: has $sk_0 \longleftarrow K(\, sk,$ "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 $\Rightarrow$ IND-IDCPA (in RO model)

- **BB-HIBE** [BB'04]: BDDH $\Rightarrow$ IND-**s**IDCPA

- **BW-HIBE** [BW'05]: 2-DLIN $\Rightarrow$ anonIND-**s**IDCPA

$\Rightarrow$ ciphertext size grows linearly with hierarchy depth

$\Rightarrow$ 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)

$\Rightarrow$ 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

  same size as BBG and good for poly. depth hierarchies

Example: BBG-HIBE [BBG'05]

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

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

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

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

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**: $\mathrm{sk}(\mathbf{id_1,\ldots,id_k}) \longrightarrow \mathbf{sk(id_1,\ldots,id_k,id_{k+1})}$

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

absorb and re-randomize

Example: BBG-HIBE [BBG'05]

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

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

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

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

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

Example: BBG-HIBE [BBG'05]

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

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

- $E\big(pp, (\mathbf{id_1,\ldots,id_k}), m\big)$: $s \leftarrow F_p$ and do

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

Final note: many further generalizations

- Wildcard IBE [ABCD…'06]

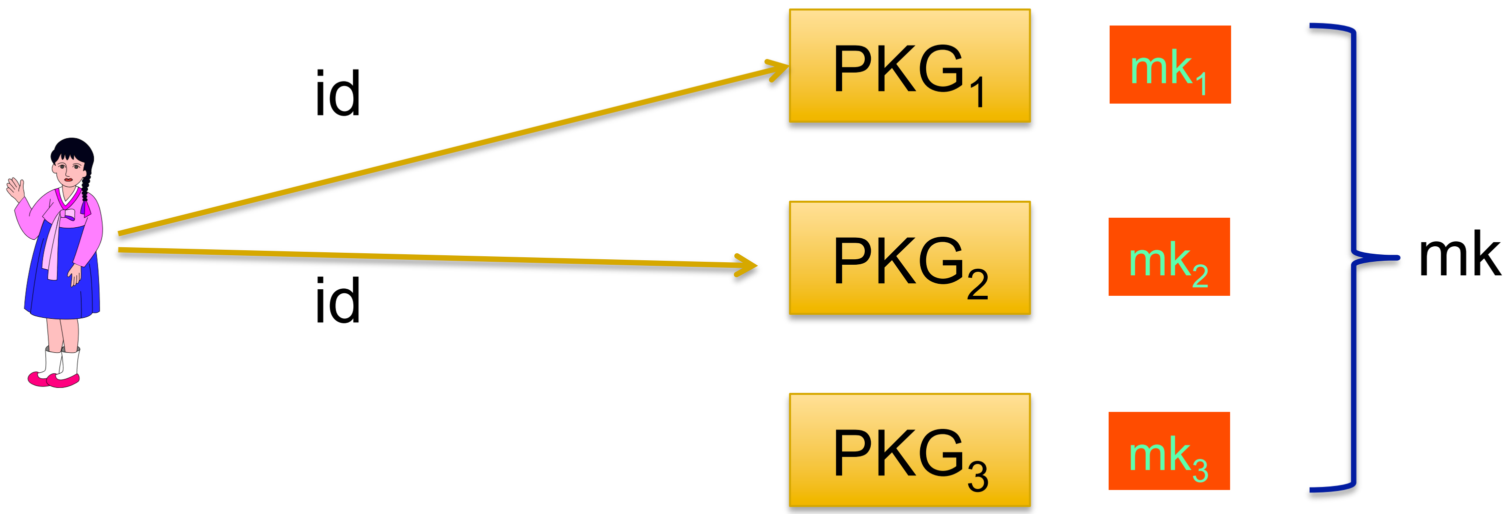
  encrypt to: $\text{ID} = (\ \text{id}_1,\ \ \text{id}_2,\ \ *\ ,\ \ \text{id}_3,\ \ *\ ,\ \ \text{id}_4\ )$

- 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