IDENTITY-BASED ENCRYPTION

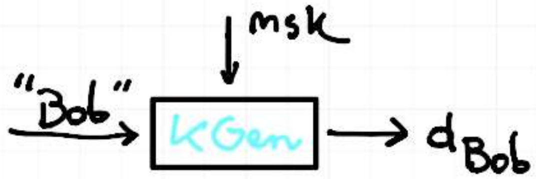
Motivation: The bottleneck of PKE is the need for certificates!

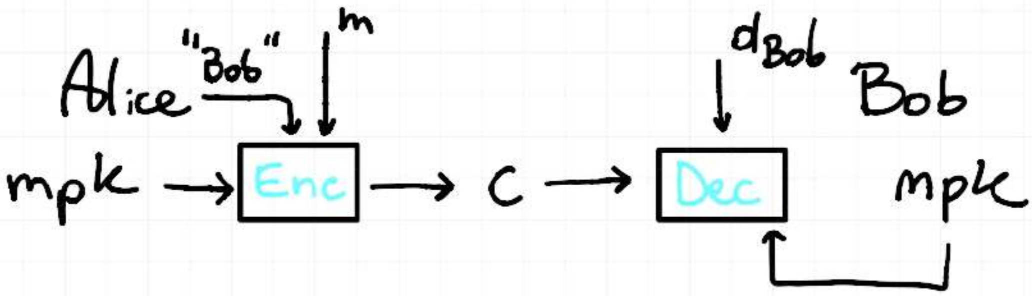
Solution: PKE without certificates

master secret / public key

$$\Pi = (\text{Setup}, \text{KGen}, \text{Enc}, \text{Dec})$$

$(mpk, msk) \leftarrow\$ \text{Setup}(1^\lambda)$ KEY GENERATION CENTER





Main advantage: No certificates!

Main disadvantage: Key escrow (Many mitigations possible)

Why is this interesting?

- Natural
- As we will show, IBE implies signatures and CCA PKE

Plan: Security model / constructions, then applications.

History: IBE proposed by Shamir in 1984.
First construction by Boneh & Franklin (ROM)

Today: Efficient IBE from standard assumptions.

<u>Correctness:</u> $\forall \lambda \in \mathbb{N}$, $\forall (mpk, msk) \leftarrow\$ Setup(1^\lambda)$,
$\forall ID \in \{0,1\}^*$, $\forall d_{ID} \leftarrow\$ KGen(1^\lambda, msk, ID)$

per ogni messaggio $P[Dec(d_{ID}, Enc(mpk, ID, m)) = m] = 1$

<u>Security:</u> IND-ID-CPA

$$GAME^{IND\text{-}ID\text{-}CPA}_{\Pi,\mathcal{A}}(\lambda, b)$$

$$\begin{array}{ccc}
\mathcal{A}(1^\lambda) & & \mathcal{C}(1^\lambda) \\
& \xleftarrow{\quad mpk \quad} & (mpk, msk) \leftarrow\$ Setup(1^\lambda) \\
& \xrightarrow{\quad ID \neq ID^* \quad} & \\
& \xleftarrow{\quad d_{ID} \quad} & d_{ID} \leftarrow\$ KGen(msk, ID) \\
& \xrightarrow{\quad m_0^*, m_1^*, ID^* \quad} & c \leftarrow\$ Enc(ID^*, m_b^*) \\
\text{di nuovo training} & \xleftarrow{\quad c \quad} & \\
& \xrightarrow{\quad b' \quad} &
\end{array}$$

We can also consider a weaker variant called selective IND-ID-CPA, where the attacker must choose ID^* before receiving mpk.

<u>Construction</u>: Using bilinear groups.

$$(\mathbb{G}, \mathbb{G}_T, g, q, \hat{e}) \leftarrow \$ \text{ BilGroupGen}(1^\lambda)$$

Recall: DDH easy in $\mathbb{G}$ because a DDH tuple $g^\alpha, g^\beta, g^\gamma$ s.t.

$$\hat{e}(g^\alpha, g^\beta) = \hat{e}(g, g^\gamma) \qquad [g^\gamma = g^{\alpha\beta}]$$

What about $\hat{e}(g,g)^{\alpha\beta\gamma}$?

<u>DEF</u>: The DECISIONAL BILINEAR DH (DBDH) assumption holds with respect BilGroupGen if $\forall$ PPT $\mathcal{A}$:

$$(\text{params}, g^\alpha, g^\beta, g^\gamma, \hat{e}(g,g)^{\alpha\beta\gamma}) \approx_c$$

$$(\text{params}, g^\alpha, g^\beta, g^\gamma, T) \qquad T \leftarrow \$ \mathbb{G}_T$$

Side note: we can get IBE from DDH! (But complex construction)

Much simpler construction from DBDH.

- <u>Setup(1^λ)</u>: params $\leftarrow \$$ BilGroupGen(1^λ)

  useful to think $g_2 = g^\beta$

  $\alpha \leftarrow \$ \mathbb{Z}_q$, $h \leftarrow \$ \mathbb{G}$, $g_2 \leftarrow \$ \text{Gen}$

  g_1=g^alpha

  $mpk = (\text{params}, g_1, g_2, h)$

  $msk = (g_2^\alpha)$

- $\underline{\mathrm{KGen}(msk, ID \in \mathbb{Z}_q)}$:

  Pick $r \leftarrow \$ \mathbb{Z}_q$

  $d_{ID}: (d_0, d_1) = (g_2^{\alpha} \cdot F(ID)^r, g^r)$

  $F: \mathbb{Z}_q \to \mathbb{G}$; $F(ID) = g_1^{ID} \cdot h$

- $\underline{\mathrm{Enc}(ID, m \in \mathbb{G}_T)}$:

  Pick $\gamma \leftarrow \$ \mathbb{Z}_q$ and output

  $c = (u, v, w) = (\underbrace{\hat{e}(g_1, g_2)}_{}{}^{\gamma} \cdot m, g^{\gamma}, F(ID)^{\gamma})$

  $\hat{e}(g_1, g_2)^{\gamma} = \hat{e}(g, g)^{\alpha\beta\gamma}$

- $\underline{\mathrm{Dec}(d_{ID} = (d_0, d_1), c)}$:

  Return $\dfrac{u \cdot \hat{e}(d_1, w)}{\hat{e}(v, d_0)}$

<u>Correctness</u>: Indeed

$$\frac{u \cdot \hat{e}(d_1, w)}{\hat{e}(v, d_0)} = \frac{\overbrace{\hat{e}(g_1, g_2)^{r} \cdot m}^{u} \cdot \hat{e}(\overset{d_1}{g^r}, \overset{w}{F(ID)^{\gamma}})}{\hat{e}(\underset{v}{g^{\gamma}}, \underset{g_2}{g^{\alpha}} \cdot \underset{d_0}{F(ID)^{r}})}$$

$$= \frac{\cancel{\hat{e}(g_1, g_2)^{\gamma}} \cdot m \cdot \cancel{\hat{e}(g, F(ID))^{r \cdot \gamma}}}{\cancel{\hat{e}(g^{\gamma}, g_2^{\alpha})} \cdot \cancel{\hat{e}(g, F(ID))^{r \cdot \gamma}}}$$

$$= m.$$

Note: The ID space is $\mathbb{Z}_q$. We can extend that to $\{0,1\}^*$ by means of CRH $H: \{0,1\}^* \to \mathbb{Z}_q$

THM: Above IBE is selective IND-ID-CPA under DBDH.

Proof: We will consider a HYB experiment.

$$\text{GAME}_{\Pi, \mathcal{A}}^{\text{IND-ID-CPA}}(\lambda, b)$$

$\mathcal{A}(1^\lambda)$ $\qquad\qquad\qquad\qquad$ $\mathcal{C}(1^\lambda)$

$\xrightarrow{\quad ID^* \quad}$

$mpk = (\text{params}, g_1 = g^{\alpha}, g_2 = g^{\beta}, h)$

$\xleftarrow{\quad mpk \quad}$ $\qquad msk = g_2^{\alpha}$

$\xrightarrow{\quad ID \neq ID^* \quad}$ $\qquad r \leftarrow \$ \mathbb{Z}_q, F(ID) = g_1^{ID} \cdot h$

$\xleftarrow{\quad d_{ID} = (d_0, d_1) \quad}$ $\qquad d_0 = g_2^{\alpha} \cdot F(ID)^r$

$d_1 = g^r$

$\xrightarrow{\quad m_0^*, m_1^* \quad}$

$\xleftarrow{\quad c = (u, v, w) \quad}$ $\qquad u = \hat{e}(g_1, g_2)^{\gamma} \cdot m^*$

$v = g^{\gamma}, w = F(ID)^{\gamma}$

$$\xrightarrow{ID \neq ID}$$
$$\xleftarrow{d_{ID}}$$
$$\xrightarrow{b'}$$

In the HYB experiment, we change how c is computed:

$$u = T \cdot m^* \qquad T \leftarrow \$ \mathbb{G}_T$$ (T random and independent of b)

And as u carries no information of b, no attacker can distinguish between $HYB(0,\lambda)$ and $HYB(1,\lambda)$.

<u>LEMMA</u>: $HYB(\lambda, b) \approx_c GAME(\lambda, b)$

Proof: Fix $b \in \{0,1\}$. Consider the following reduction to DBDH

$$\begin{array}{ccccc}
\mathcal{A}(1^\lambda) & & \mathcal{B}(1^\lambda) & & \mathcal{C}(1^\lambda) \\
& \xleftarrow{\text{START}} & & \xleftarrow{params, g_1, g_2, g_3, T} & params \\
& \xrightarrow{ID^*} & & & \\
& \xleftarrow{mpk \ (1)} & & & g_1 = g^{\alpha},\ g_2 = g^{\beta},\ g_3 = g^{\gamma} \\
& \xrightarrow{(2)\ ID \neq ID^*} & & & T \nearrow \hat{e}(g,g)^{\alpha\beta\gamma} \\
& \xleftarrow{d_0, d_1} & & & \searrow \$ \mathbb{G}_T \\
& \xrightarrow{m_0^*, m_1^* \ (3)} & & & \\
& \xleftarrow{u, v, w} & & & \\
& \xrightarrow{ID \neq ID^*} & & & \\
& \xleftarrow{d_0, d_1} & & & \\
& \xrightarrow{b'} & & \xrightarrow{b'} &
\end{array}$$

① Simulation of mpk.

Pick $a \leftarrow \$ \mathbb{Z}_q$ and let

$mpk = (params, g_1, g_2, h)$

$h = g^{-ID^*} \cdot g^{a}$ IDENTICALLY DISTR. TO $h \leftarrow \mathbb{G}$

g_1

③ Simulation of CTX $c = (u, v, w)$

Naturally, $u = T \cdot m^*_b$, $v = g^{\gamma}$

In both experiments, $w = F(ID^*)^{\gamma}$.

The reduction instead sets $w = g_3^{a}$

Because $F(ID^*)^{\gamma} = (g_1^{ID^*} \cdot h)^{\gamma} = (g_1^{ID^*} \cdot g^{-ID^*} \cdot g^{a})^{\gamma} = g_3^{a}$

② Key extraction queries. in realtà prer farlo necessiti di msj

In both experiments $d_0 = g_2^{\alpha} \cdot F(ID)^{r}$, $d_1 = g^{r}$

non conosciamo alpha

The reduction instead picks $r \leftarrow \$ \mathbb{Z}_q$ and outputs

$d_0 = g_2^{-a/ID-ID^*} \cdot F(ID)^{r}$

$d_1 =$ (In the natural way following d_0)

Why? $d_0 = g_2^{-a/ID-ID^*} \cdot F(ID)^{r}$

$$= g_2^{-\frac{a}{ID-ID^*}} \cdot (g_1^{ID} \cdot g_1^{-ID^*} \cdot g^{a})^{r}$$

Testo

$$= g_2^{-\frac{a}{ID-ID^*}} \cdot (g_1^{ID-ID^*} \cdot g^{a})^{r}$$

$$= (g_1^{ID-ID^*} \cdot g^a)^{\beta/ID-ID^*} \cdot g_2^{-\frac{a}{ID-ID^*}} \cdot \frac{(g_1^{ID-ID^*} \cdot g^a)^r}{(g_1^{ID-ID^*} \cdot g^a)^{\beta/ID-ID^*}}$$

$$= g_1^{\beta} \cdot \cancel{g_1^{a\beta/ID-ID^*}}_{\,g} \cdot \cancel{g^{-a\beta/ID-ID^*}} \cdot \underbrace{(g_1^{ID-ID^*} \cdot g^a)}_{F(ID)}{}^{r-\beta/ID-ID^*}$$

msk

$$= g_2^{\alpha} \cdot F(ID)^{\tilde{r}}$$

where $\tilde{r} = r - \beta/_{ID-ID^*}$ is UNIFORM

Now, what should d_1 look like?

$$d_1 = g^{\tilde{r}} = g^r / g_2^{1/ID-ID^*}$$

non conosciamo beta quindi lo scriviamo cosi

SELECTIVE IND-ID-CPA vs. IND-ID-CPA

Think of the set of identities as $[2^n]$ for $ID \in \{0,1\}^n$ and let $N = 2^n$.

We can show that any selective IND-ID-CPA IBE is also IND-ID-CPA IBE with security loss proportional to N with security loss proportional to N. complexity leverage

<u>THM</u>: An IBE Π that is (t, q, ε)-selective IND-ID-CPA is also $(t, q, N\cdot\varepsilon)$-IND-ID-CPA.

(t, q, ε)-security: A runs in time t

makes q extraction queries

wins w.p. $\leq \varepsilon$

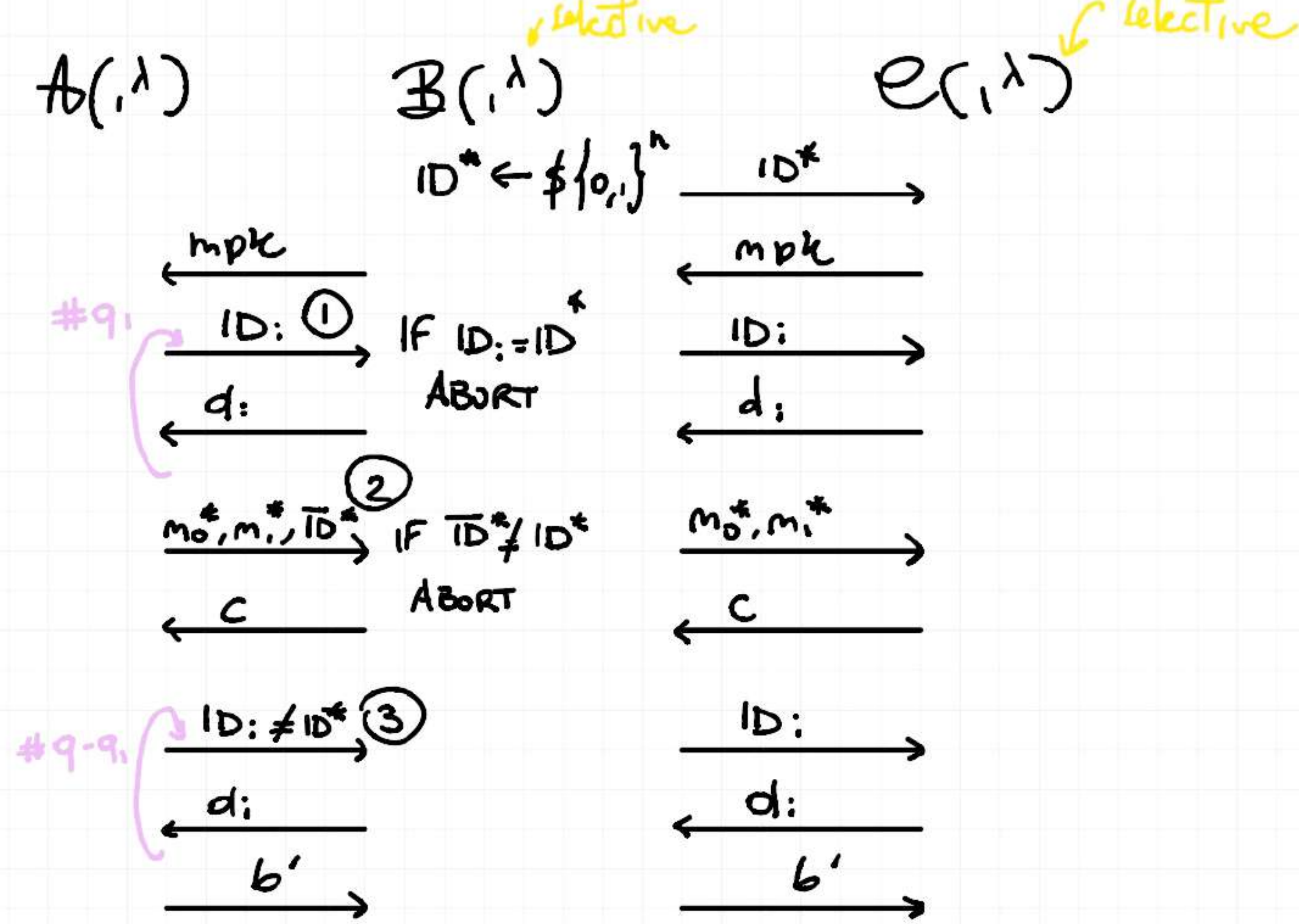
Look at $N \cdot \varepsilon = 2^n \cdot \varepsilon$. If $\varepsilon = negl(\lambda)$, then

$n = O(\log \lambda)$.

lamda

If $\varepsilon = 2^{-\alpha n}$, then $n = \omega(\log \lambda)$

<u>Proof:</u> Just a reduction to selective security.



Let GOOD be the event that the reduction reaches step (3).

$$P[\mathrm{GOOD}] = P[\mathrm{GOOD}'] \cdot P[\overline{ID}^* = ID^* \mid \mathrm{GOOD}']$$

where GOOD' is the event we don't abort in (1)

Note that $P[\neg \mathrm{GOOD}'] \leq \frac{q_1}{2^n}$

$$\Rightarrow P[\mathrm{GOOD}] \geq \left(1 - \frac{q_1}{2^n}\right)\left(\frac{1}{2^n - q_1}\right) = \frac{1}{N}$$

By a previous lemma, $\forall$ PPT $\mathcal{B}$

$$CD_{\mathcal{B}}\left(\mathrm{GAME}^{sel}(\lambda,0), \mathrm{GAME}^{sel}(\lambda,1) \right) \geq \Pr[\mathrm{GOOD}] \cdot \varepsilon$$
$$\geq \varepsilon$$