# Fine-grained access control to encrypted data

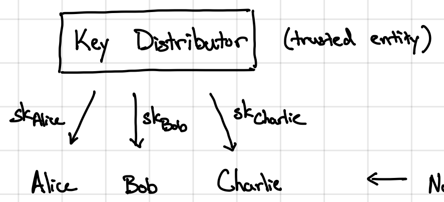
Standard public-key encryption: knowledge of public key needed to encrypt
public-key is an <u>algebraic</u> object — complex to remember and send

Can the public key be a username or an email address?
↳ Notion of identity-based encryption first proposed by Shamir in 1984
↳ First solved by Boneh and Franklin in 2001 using bilinear maps and concurrently by Cocks from quadratic residuosity
↳ Now also known from CDH or factoring [Döttling - Garg 2017]

We will see a lattice-based construction by Gentry - Peikert - Vaikuntanathan

IBE syntax:
- Setup → mpk, msk
- KeyGen (msk, id) → $sk_{id}$
- Encrypt (mpk, id, m) → ct
- Decrypt (sk, ct) → m

Model is different from PKE

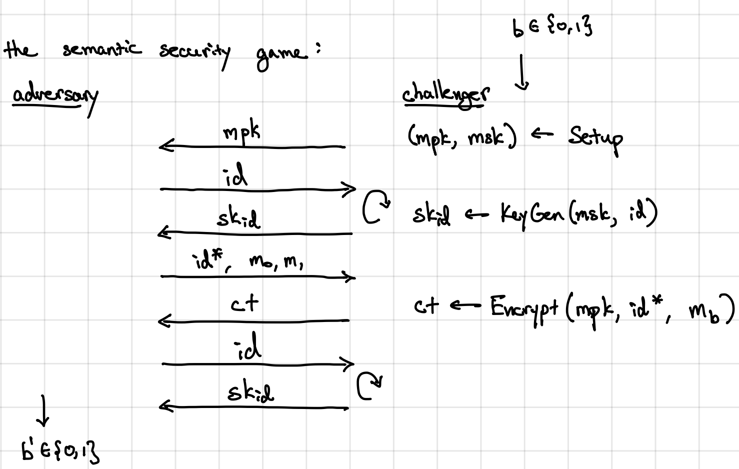



← Normally, users would pick their own key

Correctness: for all identities id and all messages m,

$$\Pr\left[\text{Decrypt}(sk, ct) = m : \begin{array}{l} (mpk, msk) \leftarrow \text{Setup} \\ sk \leftarrow \text{KeyGen}(msk, id) \\ ct \leftarrow \text{Encrypt}(mpk, id, m) \end{array}\right] = 1.$$

Security: consider the semantic security game:




We say the IBE scheme is secure if for all efficient $\mathcal{A}$:

$$\left|\Pr[b' = 1 \mid b = 0] - \Pr[b' = 1 \mid b = 1]\right| \leq \text{negl.}$$

Main challenge: IBE "compresses" many user keys (one per identity) into a set of short public parameters

Starting point: "dual Regev encryption" where public key is random and ciphertext contains an LWE sample

Setup: $A \xleftarrow{R} \mathbb{Z}_q^{n \times m}$ $\quad pk = (A, b)$

$r \xleftarrow{R} \{0,1\}^m \quad b = Ar \quad sk = r$

Encrypt$(pk, \mu)$: $s \xleftarrow{R} \mathbb{Z}_q^n$ $\quad ct = (s^T A + e^T, \; s^T b + e' + \mu \cdot \lfloor \frac{q}{2} \rfloor)$

$e \leftarrow \chi^m$

$e' \leftarrow \chi$

Decrypt$(\overset{=r}{sk}, (c_1^T, c_2))$: compute $c_2 - c_1^T r$ and round

Correctness: $c_2 - c_1^T r = s^T(Ar) + e' + \mu \cdot \lfloor \frac{q}{2} \rfloor - (s^T A + e^T) r$

$= \mu \cdot \lfloor \frac{q}{2} \rfloor + \underbrace{(e' - e^T r)}_{}$

correct as long as $|e' - e^T r| < \frac{q}{4}$

if $\chi$ is $B$-bounded, then $|e' - e^T r| \leq B + mB$, so we can set $q > 4B(m+1)$.

Security: By LHL, $(A, b)$ is statistically close to uniform over $\mathbb{Z}_q^{n \times m}, \mathbb{Z}_q^n$

By LWE, $s^T [A \mid b] + [e^T \mid e']$ is computationally indistinguishable from uniform.

$\Rightarrow$ Ciphertexts are pseudorandom under LWE.

We often treat $r$ as a "recoding vector." It translates an LWE instance with respect to $A$ to one with respect to $b$.

Idea for IBE: matrix $A$ is the public key

each user is associated with a dual Regev public key $pk_{id} = (A, b_{id})$ where $b_{id} = H(id)$

observe that $H(id)$ is publicly computable so public key for every user is publicly-derivable!

To decrypt, user needs to know the dual Regev decryption key: a recoding vector $r_{id}$ where $A r_{id} = b_{id} = H(id)$

- This is precisely a GPV signature on id! We can sample it by setting msk = trapdoor for $A$ (i.e., GPV signing key).

Setup: Sample $\bar{A} \xleftarrow{R} \mathbb{Z}_q^{n \times m}$

$\bar{R} \xleftarrow{R} \{0,1\}^{m \times m}$

Let $A = [\bar{A} \mid \bar{A}\bar{R} + G]$ $\quad$ (i.e., $R$ is a trapdoor for $A$)

$R = \begin{bmatrix} -\bar{R} \\ I \end{bmatrix}$

mpk = $A$ $\quad$ msk = $R$

KeyGen(msk, id): $sk_{id} \leftarrow A^{-1}(H(id))$ $\quad$ [As in GPV, this is a <u>randomized</u> procedure (to avoid leaking $R$)]

Encrypt(mpk, id, $\mu$): $s \xleftarrow{R} \mathbb{Z}_q^n$ $\quad b_{id} \leftarrow H(id)$

$e \leftarrow \chi^m$

$e' \leftarrow \chi$

$ct = (s^T A + e^T, \; s^T b_{id} + e' + \mu \cdot \lfloor \frac{q}{2} \rfloor)$ $\quad$ [Dual Regev encryption with respect to $pk_{id} = (A, b_{id})$ ]

Decrypt$(\overset{=r_{id}}{sk_{id}}, (c_1^T, c_2))$: $\mu \leftarrow \text{round}(c_2 - c_1^T r_{id})$.

Correctness: Same analysis as for dual Regev encryption (except $\|b_{id}\|$ slightly larger).

Security: Follows under LWE in random oracle model (model $H$ as ideal hash function)

$\hookrightarrow$ Rely on random oracle to answer key-generation queries

Observe that secret keys in above scheme are simply GPV signatures on the identity

↳ This is true in general: IBE scheme implies a signature scheme (signature on m is identity key for m)

Identity keys must be unforgeable as otherwise, security is trivially broken.

Drawback of IBE: central authority generates the secret keys $\longrightarrow$ single point of failure

Can we have IBE where users pick their own key?

↳ Same challenge: how to compress public keys into short set of parameters?

Notion called registration-based encryption (RBE)

Alice $\longrightarrow pk_A$
Bob $\longrightarrow pk_B$
Charlie $\longrightarrow pk_C$

} aggregated into mpk

Encrypt $(mpk, id, \mu) \to ct$ [Same syntax as plain IBE]

To decrypt, use secret key (user generated, not shared with anyone)

First lattice-based construction by Döttling-Kolonelos-Lai-Lin-Malavolta-Rahimi in 2023

- The master public key is a "Merkle hash" of the individual public keys using an SIS hash function
- Decryption essentially recodes "root ciphertext" to the key associated with a specific user