No identity-based encryption in the generic group model

Peeter Laud

Cybernetica AS

September 29th, 2012

Identity-based encryption

- Public-key encryption, where "public key" = "name"
  - no PKI necessary
  - Instead of a *certification authority*, there is a *key generation centre*.
  - Some commercialization: `http://www.voltage.com`
  - Fancy functionalities can be built on top of it.
- Formally, 4-tuple of algorithms:
  - Master public key **G**eneration
  - Secret **K**ey construction
  - **E**ncryption
  - **D**ecryption

IBE algorithms

- $\mathbf{G}(msk)$ outputs mpk.
  - Master secret key $\rightarrow$ master public key
- $\mathbf{K}(msk, \mathrm{ID})$ outputs sk_{ID}.
- $\mathbf{E}(mpk, \mathrm{ID}, m; r)$ outputs c.
  - We always take $m \in \{0, 1\}$.
- $\mathbf{D}(mpk, sk_{\mathrm{ID}}, c)$ outputs m.

Functionality: For all msk, ID, m:

$$\mathbf{D}(\mathbf{G}(msk), \mathbf{K}(msk, \mathrm{ID}), \mathbf{E}(\mathbf{G}(msk), \mathrm{ID}, m; r)) = m$$

with probability (over r) at least $1/2 + \sigma$ where σ is significantly large.

Weak IND-CPA security for IBE

INDistinguishability against **C**hosen **P**laintext **A**ttacks

- The adversary picks the identities $ID_1, \ldots, ID_l, ID_\star$ as bit-strings of length ℓ and gives them to the environment.
  - l must be not too large — polynomial in runtime of $\mathbf{G}, \mathbf{K}, \mathbf{E}, \mathbf{D}$.

Weak IND-CPA security for IBE

INDistinguishability against **C**hosen **P**laintext **A**ttacks

- The adversary picks the identities $ID_1, \ldots, ID_l, ID_\star$ as bit-strings of length ℓ and gives them to the environment.
  - l must be not too large — polynomial in runtime of $\mathbf{G}, \mathbf{K}, \mathbf{E}, \mathbf{D}$.
- The environment generates $msk \in \{0,1\}^\ell$, $m \in \{0,1\}$ and the randomness r, computes
  - $mpk = \mathbf{G}(msk)$;
  - $sk_i = \mathbf{K}(msk, \mathrm{ID}_i)$. (for all $i \in \{1, \ldots, l\}$);
  - $c = \mathbf{E}(mpk, \mathrm{ID}_\star, m; r)$.

Weak IND-CPA security for IBE

INDistinguishability against **C**hosen **P**laintext **A**ttacks

- The adversary picks the identities $ID_1, \ldots, ID_l, ID_\star$ as bit-strings of length ℓ and gives them to the environment.
  - l must be not too large — polynomial in runtime of $\mathbf{G}, \mathbf{K}, \mathbf{E}, \mathbf{D}$.
- The environment generates $msk \in \{0,1\}^\ell$, $m \in \{0,1\}$ and the randomness r, computes
  - $mpk = \mathbf{G}(msk)$;
  - $sk_i = \mathbf{K}(msk, \mathrm{ID}_i)$. (for all $i \in \{1, \ldots, l\}$);
  - $c = \mathbf{E}(mpk, \mathrm{ID}_\star, m; r)$.
- Gives $mpk, sk_1, \ldots, sk_l, c$ to the adversary.

Weak IND-CPA security for IBE

INDistinguishability against **C**hosen **P**laintext **A**ttacks

- The adversary picks the identities $ID_1, \ldots, ID_l, ID_\star$ as bit-strings of length ℓ and gives them to the environment.
  - l must be not too large — polynomial in runtime of $\mathbf{G}, \mathbf{K}, \mathbf{E}, \mathbf{D}$.
- The environment generates $msk \in \{0,1\}^\ell$, $m \in \{0,1\}$ and the randomness r, computes
  - $mpk = \mathbf{G}(msk)$;
  - $sk_i = \mathbf{K}(msk, \mathrm{ID}_i)$. (for all $i \in \{1, \ldots, l\}$);
  - $c = \mathbf{E}(mpk, \mathrm{ID}_\star, m; r)$.
- Gives $mpk, sk_1, \ldots, sk_l, c$ to the adversary.

The adversary must guess m. The scheme is weakly IND-CPA-secure if the correctness probability of the guess is only insifnificantly larger than $1/2$.

Generic group model

- A cyclic group where "all details of representation are hidden / unusable".
- One can only
  - generate a random element of the group;
  - perform algebraic operations with the constructed elements.
- Group size $p \in \mathbb{P}$, $p < 2^{\ell}$ is also known.
- Can be used to analyse group-theory-related hardness assumptions in a generic manner.
- Introduced by Nechaev, Shoup, Schnorr in late 1990s.

Generic group model (GGM)

- A machine $\mathcal{M}$, accessible to all parties of a protocol.
  - Similar to random oracles in this sense.
- Internally keeps a partial map $\mu : \{0, \ldots, p-1\} \to \{0,1\}^{\ell}$.
- Accepts queries of the form $((h_1, a_1) \ldots, (h_k, a_k))$.
  - Returns $\mu(a_1 \cdot \mu^{-1}(h_1) + \cdots + a_k \cdot \mu^{-1}(h_k))$
    - Think of it as corresponding to $h_1^{a_1} \cdots h_k^{a_k}$
  - Undefined points of μ will be randomly defined.

Example: CDH is hard in generic group model

- **CDH:** Environment generates g, a, b. Defines $g_a = \mathcal{M}((g, a))$ and $g_b = \mathcal{M}((g, b))$. Gives g, g_a, g_b to adversary which returns h. Environment checks $h \stackrel{?}{=} \mathcal{M}((g, ab))$.

Example: CDH is hard in generic group model

- **CDH:** Environment generates g, a, b. Defines $g_a = \mathcal{M}((g, a))$ and $g_b = \mathcal{M}((g, b))$. Gives g, g_a, g_b to adversary which returns h. Environment checks $h \stackrel{?}{=} \mathcal{M}((g, ab))$.
- Adversary can only create group elements of the form $g_a^x g_b^y g^z = g^{ax+by+z}$ for x, y, z chosen by him.

Example: CDH is hard in generic group model

- **CDH:** Environment generates g, a, b. Defines $g_a = \mathcal{M}((g, a))$ and $g_b = \mathcal{M}((g, b))$. Gives g, g_a, g_b to adversary which returns h. Environment checks $h \stackrel{?}{=} \mathcal{M}((g, ab))$.
- Adversary can only create group elements of the form $g_a^x g_b^y g^z = g^{ax+by+z}$ for x, y, z chosen by him.
- For randomly chosen a, b: $g^{ax+by+z} = g^{ax'+by'+z'}$ implies $x = x', y = y', z = z'$ with high probability.
- For randomly chosen a, b: $g^{ax+by+z} \neq g^{ab}$ with high probability.
  - Schwartz-Zippel lemma

DDH is similarly hard.

Things to notice

- The attacker's computational power was not constrained.
  - The attacker only had to pay for the access to $\mathcal{M}$.
- The proof was all about polynomials in the exponents of g.
  - Indeed, we could change $\mathcal{M}$: let the domain of μ be polynomials, not $\{0, \ldots, p-1\}$.
  - This change would be indistinguishable.
- All other hardness assumptions for cyclic groups are also true in GGM.
  - Otherwise the cryptographic community wouldn't accept them.

Example: public-key encryption in GGM

- Generate $a \in \{0, \ldots, p-1\}$, $g \in \{0,1\}^\ell$. Let $h = \mathcal{M}((g, a))$.
  - (g, h) is public key.
  - a is secret key.
- Encryption:
  - Generate $r \in \{0, \ldots, p-1\}$. Let
    - $c_1 = \mathcal{M}((g, r))$;
    - $c_2 = \mathcal{M}((g, m), (h, r))$.
  - Send (c_1, c_2).
- Decryption: Compare $\mathcal{M}((c_1, -a), (c_2, 1))$ with $\mathcal{M}()$.
  - $\mathcal{M}()$ returns the representation of the unit element.

That's El-Gamal.

No IBE in GGM

Theorem

There are no weakly IND-CPA-secure identity-based encryption schemes in the generic group model.

- *I.e. a computationally unconstrained adversary will break any IBE scheme.*
  - *Only constraint — must pay for the access to $\mathcal{M}$.*

No IBE in GGM

Theorem

There are no weakly IND-CPA-secure identity-based encryption schemes in the generic group model.

- *I.e. a computationally unconstrained adversary will break any IBE scheme.*
    - *Only constraint — must pay for the access to $\mathcal{M}$.*

- What does this mean?
- Must use other hardness assumptions for IBE
    - Bilinear pairings and associated hardness assumptions
    - Factorization-related hardness assumptions
    - ...

No IBE in GGM

Theorem

There are no weakly IND-CPA-secure identity-based encryption schemes in the generic group model.

- *I.e. a computationally unconstrained adversary will break any IBE scheme.*
  - *Only constraint — must pay for the access to $\mathcal{M}$.*

- What does this mean?
- Must use other hardness assumptions for IBE
  - Bilinear pairings and associated hardness assumptions
  - Factorization-related hardness assumptions
  - ...

Related work

Dan Boneh, Periklis A. Papakonstantinou, Charles Rackoff, Yevgeniy Vahlis, and Brent Waters. On the impossibility of basing identity based encryption on trapdoor permutations. FOCS 2008.

The setup of IBE in GGM

- Algorithms:
  - $\mathbf{G}^{(\cdot)}(\cdot)$, $\mathbf{K}^{(\cdot)}(\cdot,\cdot)$, $\mathbf{E}^{(\cdot)}(\cdot,\cdot,\cdot;\cdot)$, $\mathbf{D}^{(\cdot)}(\cdot,\cdot,\cdot)$

  such that for all *msk*, ID, *m*, *r*:

$$\Pr[\mathbf{D}^{\mathcal{M}}(\mathbf{G}^{\mathcal{M}}(msk),\mathbf{K}^{\mathcal{M}}(msk,\mathrm{ID}),\mathbf{E}^{\mathcal{M}}(m,\mathbf{G}^{\mathcal{M}}(msk),\mathrm{ID};r))=m]\geq 1/2+\sigma$$

  where probability is taken over the choice of *r*.
- W.l.o.g.: No algorithm submits values received from $\mathcal{M}$ back to $\mathcal{M}$.

The most important parameter

Let each algorithm make at most q queries to its oracle.

In the rest of the talk we show an adversary $\mathcal{A}$ that breaks the weak IND-CPA security of the scheme.

Observations of $\mathcal{M}$ as a vector space

- $\mathcal{A}$ runs the algorithms $\mathbf{G}, \mathbf{K}, \mathbf{E}, \mathbf{D}$.
- It can observe the queries made to $\mathcal{M}$ and their answers.
- All observations define a vector space:

Observations of $\mathcal{M}$ as a vector space

- $\mathcal{A}$ runs the algorithms $\mathbf{G}, \mathbf{K}, \mathbf{E}, \mathbf{D}$.
- It can observe the queries made to $\mathcal{M}$ and their answers.
- All observations define a vector space:
- Consider formal linear combinations $a_1 h_1 + \cdots + a_k h_k$, where $h_1, \ldots, h_l \in \{0,1\}^\ell$ and $a_1, \ldots, a_k \in \mathbb{Z}_p$.
- They give us a vector space over $\mathbb{Z}_p$.
- The observations of $\mathcal{M}$ by $\mathcal{A}$ define a subspace:

Observations of $\mathcal{M}$ as a vector space

- $\mathcal{A}$ runs the algorithms $\mathbf{G}, \mathbf{K}, \mathbf{E}, \mathbf{D}$.
- It can observe the queries made to $\mathcal{M}$ and their answers.
- All observations define a vector space:
- Consider formal linear combinations $a_1 h_1 + \cdots + a_k h_k$, where $h_1, \ldots, h_l \in \{0,1\}^\ell$ and $a_1, \ldots, a_k \in \mathbb{Z}_p$.
- They give us a vector space over $\mathbb{Z}_p$.
- The observations of $\mathcal{M}$ by $\mathcal{A}$ define a subspace:
- A query $h = \mathcal{M}((h_1, a_1), \ldots, (h_k, a_k))$ corresponds to the vector $a_1 h_1 + \cdots + a_k h_k - h$.
- The span of all these vectors describes $\mathcal{A}$'s current knowledge about $\mathcal{M}$.

Structure of $\mathcal{A}$

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$ // Fix l later
- give them to the environment
- get back $mpk, sk_1, \ldots, sk_l, c$

Structure of $\mathcal{A}$

- $\mathrm{ID}_1, \ldots, \mathrm{ID}_l, \mathrm{ID}_\star \xleftarrow{\$} \{0,1\}^\ell$ // Fix l later
- give them to the environment
- get back $mpk, sk_1, \ldots, sk_l, c$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: // Fix q_1 later
  - Compute $\mathbf{D}^{\mathcal{M}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}}(mpk, \mathrm{ID}_i, \$; \$))$

Structure of $\mathcal{A}$

- $\mathrm{ID}_1, \ldots, \mathrm{ID}_l, \mathrm{ID}_\star \xleftarrow{\$} \{0,1\}^\ell$ // Fix l later
- give them to the environment
- get back $mpk, sk_1, \ldots, sk_l, c$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: // Fix q_1 later
  - Compute $\mathbf{D}^{\mathcal{M}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}}(mpk, \mathrm{ID}_i, \$; \$))$
- Do q_2 times: // Fix q_2 later
  - Compute $\mathbf{E}^{\mathcal{M}}(mpk, \mathrm{ID}_\star, \$; \$)$

Structure of $\mathcal{A}$

- $\mathrm{ID}_1, \ldots, \mathrm{ID}_l, \mathrm{ID}_\star \xleftarrow{\$} \{0,1\}^\ell$ // Fix l later
- give them to the environment
- get back $mpk, sk_1, \ldots, sk_l, c$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: // Fix q_1 later
  - Compute $\mathbf{D}^{\mathcal{M}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}}(mpk, \mathrm{ID}_i, \$; \$))$
- Do q_2 times: // Fix q_2 later
  - Compute $\mathbf{E}^{\mathcal{M}}(mpk, \mathrm{ID}_\star, \$; \$)$

  - Let $\mathcal{V}$ be $\mathcal{A}$'s current knowledge about $\mathcal{M}$
  - Let $(sk', \mathcal{V}'; \mathrm{defs}) \leftarrow \mathcal{D}(mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$

Structure of $\mathcal{A}$

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$ // Fix l later
- give them to the environment
- get back $mpk, sk_1, \ldots, sk_l, c$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: // Fix q_1 later
  - Compute $\mathbf{D}^{\mathcal{M}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: // Fix q_2 later
  - Compute $\mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, \$; \$)$

  - Let $\mathcal{V}$ be $\mathcal{A}$'s current knowledge about $\mathcal{M}$
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
    let $c^* \leftarrow c$.

  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{M}; \mathsf{defs})}(mpk, sk', c^*)$

Structure of $\mathcal{A}$

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \xleftarrow{\$} \{0,1\}^\ell$ // Fix l later
- give them to the environment
- get back $mpk, sk_1, \ldots, sk_l, c$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: // Fix q_1 later
  - Compute $\mathbf{D}^{\mathcal{M}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: // Fix q_2 later
  - Compute $\mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, \$; \$)$

  - Let $\mathcal{V}$ be $\mathcal{A}$'s current knowledge about $\mathcal{M}$
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
    let $c^* \leftarrow c$.

  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{M}; \mathsf{defs})}(mpk, sk', c^*)$
- Output m^* as the guess.

Structure of $\mathcal{A}$

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$ // Fix l later
- give them to the environment
- get back $mpk, sk_1, \ldots, sk_l, c$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: // Fix q_1 later
  - Compute $\mathbf{D}^{\mathcal{M}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: // Fix q_2 later
  - Compute $\mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, \$; \$)$
- Let $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times: // Fix q_3 later
  - Let $\mathcal{V}$ be $\mathcal{A}$'s current knowledge about $\mathcal{M}$
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
    let $c^* \leftarrow c$.
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{M}; \mathsf{defs})}(mpk, sk', c^*)$
- Output m^* as the guess.

Structure of $\mathcal{A}$

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$ // Fix l later
- give them to the environment
- get back $mpk, sk_1, \ldots, sk_l, c$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: // Fix q_1 later
  - Compute $\mathbf{D}^{\mathcal{M}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: // Fix q_2 later
  - Compute $\mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, \$; \$)$
- Let $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times: // Fix q_3 later
  - Let $\mathcal{V}$ be $\mathcal{A}$'s current knowledge about $\mathcal{M}$
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - If s-th time, let $c^* \leftarrow c$.
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{M}; \mathsf{defs})}(mpk, sk', c^*)$
- Output m^* as the guess.

Structure of $\mathcal{A}$

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \xleftarrow{\$} \{0,1\}^\ell$ // Fix l later
- give them to the environment
- get back $mpk, sk_1, \ldots, sk_l, c$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: // Fix q_1 later
  - Compute $\mathbf{D}^{\mathcal{M}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: // Fix q_2 later
  - Compute $\mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, \$; \$)$
- Let $s \xleftarrow{\$} \{1, \ldots, q_3\}$. Do s times: // Fix q_3 later
  - Let $\mathcal{V}$ be $\mathcal{A}$'s current knowledge about $\mathcal{M}$
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - If s-th time, let $c^* \leftarrow c$.
  - If not yet s-th time, let $c^* \leftarrow \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, \$; \$)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{M}; \mathsf{defs})}(mpk, sk', c^*)$
- Output m^* as the guess.

The sampler $\mathcal{D}$

Inputs: $mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V}$

- Execute:
  - Initialize $\mathcal{M}'$ with $\mathcal{V}$

The sampler $\mathcal{D}$

Inputs: $mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V}$

- Execute:
  - Initialize $\mathcal{M}'$ with $\mathcal{V}$
  - $msk' \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
  - $mpk' \leftarrow \mathbf{G}^{\mathcal{M}'}(msk')$
  - For each $i \in \{1, \ldots, l\}$: $sk'_i \leftarrow \mathbf{K}^{\mathcal{M}'}(msk', \mathrm{ID}_i)$

The sampler $\mathcal{D}$

Inputs: $mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V}$

- Execute:
  - Initialize $\mathcal{M}'$ with $\mathcal{V}$
  - $msk' \xleftarrow{\$} \{0,1\}^\ell$
  - $mpk' \leftarrow \mathbf{G}^{\mathcal{M}'}(msk')$
  - For each $i \in \{1, \ldots, l\}$: $sk'_i \leftarrow \mathbf{K}^{\mathcal{M}'}(msk', \mathrm{ID}_i)$
- Filter: $mpk = mpk'$, $sk'_i = sk_i$ for all i.

The sampler $\mathcal{D}$

Inputs: $mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V}$

- Execute:
  - Initialize $\mathcal{M}'$ with $\mathcal{V}$
  - $msk' \xleftarrow{\$} \{0,1\}^{\ell}$
  - $mpk' \leftarrow \mathbf{G}^{\mathcal{M}'}(msk')$
  - For each $i \in \{1, \ldots, l\}$: $sk'_i \leftarrow \mathbf{K}^{\mathcal{M}'}(msk', \mathrm{ID}_i)$
  - $sk' \leftarrow \mathbf{K}^{\mathcal{M}'}(msk', \mathrm{ID}_\star)$
  - Let $\mathcal{V}'$ be the internal state of $\mathcal{M}'$
- Filter: $mpk = mpk'$, $sk'_i = sk_i$ for all i.

The sampler $\mathcal{D}$

Inputs: $mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V}$

- Execute:
  - Initialize $\mathcal{M}'$ with $\mathcal{V}$
  - $msk' \xleftarrow{\$} \{0,1\}^\ell$
  - $mpk' \leftarrow \mathbf{G}^{\mathcal{M}'}(msk')$
  - For each $i \in \{1, \ldots, l\}$: $sk'_i \leftarrow \mathbf{K}^{\mathcal{M}'}(msk', \mathrm{ID}_i)$
  - $sk' \leftarrow \mathbf{K}^{\mathcal{M}'}(msk', \mathrm{ID}_\star)$
  - Let $\mathcal{V}'$ be the internal state of $\mathcal{M}'$
- Filter: $mpk = mpk'$, $sk'_i = sk_i$ for all i.
- Output: $sk', \mathcal{V}'$

The sampler $\mathcal{D}$

Inputs: $mpk, \mathrm{ID}_1, \dots, \mathrm{ID}_l, sk_1, \dots, sk_l, \mathcal{V}$

- Execute:
  - Initialize $\mathcal{M}'$ with $\mathcal{V}$
  - $msk' \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
  - $mpk' \leftarrow \mathbf{G}^{\mathcal{M}'}(msk')$
  - For each $i \in \{1, \dots, l\}$: $sk'_i \leftarrow \mathbf{K}^{\mathcal{M}'}(msk', \mathrm{ID}_i)$
  - $sk' \leftarrow \mathbf{K}^{\mathcal{M}'}(msk', \mathrm{ID}_\star)$
    - Record the queries to $\mathcal{M}'$ in defs
    - defs $= \{h^{(j)} = a_1^{(j)} h_1^{(j)} + \cdots + a_{k(j)}^{(j)} h_{k(j)}^{(j)} \mid j \in \{1, \dots, q\}\}$
  - Let $\mathcal{V}'$ be the internal state of $\mathcal{M}'$
- Filter: $mpk = mpk'$, $sk'_i = sk_i$ for all i.
- Output: $sk', \mathcal{V}', \mathrm{defs}$

The combiner $\mathcal{C}(\mathcal{V}', \mathcal{M}; \mathrm{defs})$

On input $(h_1, a_1), \ldots, (h_k, a_k)$:

- If exists h, s.t. $a_1 h_1 + \cdots + a_k h_k - h \in \mathcal{V}'$ then return h.

The combiner $\mathcal{C}(\mathcal{V}', \mathcal{M}; \text{defs})$

On input $(h_1, a_1), \ldots, (h_k, a_k)$:

- If exists h, s.t. $a_1 h_1 + \cdots + a_k h_k - h \in \mathcal{V}'$ then return h.
- Apply equalities in defs to $h_1, \ldots, h_k$.
  - We get an equivalent query $(h'_1, a'_1), \ldots, (h'_{k'}, a'_{k'})$

The combiner $\mathcal{C}(\mathcal{V}', \mathcal{M}; \mathrm{defs})$

On input $(h_1, a_1), \ldots, (h_k, a_k)$:

- If exists h, s.t. $a_1 h_1 + \cdots + a_k h_k - h \in \mathcal{V}'$ then return h.
- Apply equalities in defs to $h_1, \ldots, h_k$.
  - We get an equivalent query $(h'_1, a'_1), \ldots, (h'_{k'}, a'_{k'})$
- Submit $(h'_1, a'_1), \ldots, (h'_{k'}, a'_{k'})$ to $\mathcal{M}$. Get back h.

- Return h.

The combiner $\mathcal{C}(\mathcal{V}', \mathcal{M}; \mathsf{defs})$

On input $(h_1, a_1), \ldots, (h_k, a_k)$:

- If exists h, s.t. $a_1 h_1 + \cdots + a_k h_k - h \in \mathcal{V}'$ then return h.
- Apply equalities in defs to $h_1, \ldots, h_k$.
  - We get an equivalent query $(h'_1, a'_1), \ldots, (h'_{k'}, a'_{k'})$
- Submit $(h'_1, a'_1), \ldots, (h'_{k'}, a'_{k'})$ to $\mathcal{M}$. Get back h.
- Add $a_1 h_1 + \cdots + a_k h_k - h$ to $\mathcal{V}'$.
- Return h.

The combiner $\mathcal{C}(\mathcal{V}', \mathcal{M}; \text{defs})$

On input $(h_1, a_1), \ldots, (h_k, a_k)$:

- If exists h, s.t. $a_1 h_1 + \cdots + a_k h_k - h \in \mathcal{V}'$ then return h.
- Apply equalities in defs to $h_1, \ldots, h_k$.
  - We get an equivalent query $(h'_1, a'_1), \ldots, (h'_{k'}, a'_{k'})$
- Submit $(h'_1, a'_1), \ldots, (h'_{k'}, a'_{k'})$ to $\mathcal{M}$. Get back h.
- Add $a_1 h_1 + \cdots + a_k h_k - h$ to $\mathcal{V}'$.
- Return h.

Shortly...

$\mathcal{C}(\mathcal{V}_1, \mathcal{V}_2; \ldots)$ first consults $\mathcal{V}_1$. If unsuccessful, consults $\mathcal{V}_2$ and records answer in $\mathcal{V}_1$, too.

$\mathcal{A}$ + environment

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1,\ldots,l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, m; r)$

$\mathcal{A}$ + environment

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \xleftarrow{\$} \{0,1\}^\ell$
- $msk \xleftarrow{\$} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- $m \xleftarrow{\$} \{0,1\}$; $r \xleftarrow{\$} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, m; r)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$

$\mathcal{A}$ + environment

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, m; r)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times:
  $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$

$\mathcal{A}$ + environment

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \xleftarrow{\$} \{0,1\}^\ell$
- $msk \xleftarrow{\$} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- $m \xleftarrow{\$} \{0,1\}$; $r \xleftarrow{\$} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, m; r)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
- $s \xleftarrow{\$} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - **if** s-th iter. **then** $c^* \leftarrow c$ **else** $c^* \leftarrow \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{M}\to\mathcal{V}; \mathsf{defs})}(mpk, sk', c^*)$

$\mathcal{A}$ + environment

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, m; r)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
- $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - **if** s-th iter. **then** $c^* \leftarrow c$ **else** $c^* \leftarrow \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{M}\to\mathcal{V}; \mathsf{defs})}(mpk, sk', c^*)$
- Output $(m = m^*)$

$\mathcal{A}$ + environment

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, m; r)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\rightarrow\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\rightarrow\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\rightarrow\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
- $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - **if** s-th iter. **then** $c^* \leftarrow c$ **else** $c^* \leftarrow \mathbf{E}^{\mathcal{M}\rightarrow\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{M}\rightarrow\mathcal{V}; \mathsf{defs})}(mpk, sk', c^*)$
- Output $(m = m^*)$

Question: What is the probability that **true** is output?

$\mathcal{A}$ + environment

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, m; r)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times:
  $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
- $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - **if** s-th iter. **then** $c^* \leftarrow c$ **else** $c^* \leftarrow \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{M}\to\mathcal{V}; \mathsf{defs})}(mpk, sk', c^*)$
- Output $(m = m^*)$

Let us do some reordering of the code

$\mathcal{A}$ + environment, reordered

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
- $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, m; r)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{M}\to\mathcal{V}; \mathsf{defs})}(mpk, sk', c)$
- Output $(m = m^*)$

$\mathcal{A}$ + environment, reordered

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
- $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, m; r)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{M}\to\mathcal{V}; \mathsf{defs})}(mpk, sk', c)$
- Output $(m = m^*)$

Let us do some lazy sampling

$\mathcal{A}$ + environment, lazily sampled

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
- Let $(\_, \mathcal{V}''; \_) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
- $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{V}''\to\mathcal{V}}(mpk, \mathsf{ID}_\star, m; r)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{V}''\to\mathcal{V}; \mathsf{defs})}(mpk, sk', c)$
- Output $(m = m^*)$

$\mathcal{A}$ + environment, lazily sampled

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times:
  $\mathbf{D}^{\mathcal{M} \to \mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M} \to \mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M} \to \mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
- Let $(\_, \mathcal{V}''; \_) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
- $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{V}'' \to \mathcal{V}}(mpk, \mathsf{ID}_\star, m; r)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{V}'' \to \mathcal{V}; \mathsf{defs})}(mpk, sk', c)$
- Output $(m = m^*)$

Let us do a more serious replacement now

$\mathcal{A}$ + environment, $\mathcal{C}(\mathcal{V}', \mathcal{V}''; \mathsf{defs})$ instead of $\mathcal{V}''$

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
- Let $(\_, \mathcal{V}''; \_) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
- $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{C}(\mathcal{V}', \mathcal{V}''\to\mathcal{V}; \mathsf{defs})}(mpk, \mathsf{ID}_\star, m; r)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{V}''\to\mathcal{V}; \mathsf{defs})}(mpk, sk', c)$
- Output $(m = m^*)$

How big a difference in output did this replacement make?

Which queries are different for $\mathcal{V}''$ and $\mathcal{C}(\mathcal{V}', \mathcal{V}'', \mathrm{defs})$?

...during encryption

Recall: $\mathcal{C}$ first tries $\mathcal{V}'$, then $\mathcal{V}''$.

- Consider query $(h_1, a_1), \ldots, (h_k, a_k)$.
  - If it can be answered according to both $\mathcal{V}'$ and $\mathcal{V}''$, then there is no difference.
  - If it cannot be answered according $\mathcal{V}'$, then there is also no observable difference
    - But with $\mathcal{C}(\cdots)$, the space $\mathcal{V}'$ is also updated.
  - If it can be answered according to $\mathcal{V}'$, but not according to $\mathcal{V}''$, then there may be difference.

Frequent queries during encryption

- Let mpk, $\mathrm{ID}_\star$ be fixed.
- Let $\mathcal{W}$ be the current state of $\mathcal{M}$, expressed as vector space.

Definition

V_E is a (δ, δ')-frequent encryption space if

- $m \xleftarrow{\$} \{0,1\}$, $r \xleftarrow{\$} \{0,1\}^\ell$, $\mathbf{E}^{\mathcal{W} \vee V_E \to \mathcal{U}}(mpk, \mathrm{ID}_\star, m; r)$;
- for all queries Q: let p_Q be the probability that $\mathcal{U}$ contains answer to it.
- Q is frequent on encryption if $p_Q \geq \delta$.
- Let $\overline{p_Q}$ be the scaled probability of Q after we have set all $p_{Q'}$ smaller than δ to 0.
- Pick a query Q according to the probabilities $\overline{p_Q}$.
- Then $\Pr[Q \text{ has answer in } V_E] \geq 1 - \delta'$.

Bad queries have small probability during encryption

Suppose q_2 is such that $\mathcal{V}$ contains a (δ_E, δ'_E)-frequent encryption space ($\mathcal{W}$ fixed before sampling $\mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}_\star, \$; \$)$.

- I.e. $(1 - \delta_E)^{q_2} \leq \delta'_E$.

Consider a query Q.

- If it is frequent, then only with probability $\leq \delta'_E$ is it not in $\mathcal{V}''$.
- If it is infrequent, then it shows up with probability $\leq \delta_E$.
- $\mathcal{V}'$ has at most $q_3(l + 4)q$ dimensions more than $\mathcal{V}''$, where the infrequent queries disturbing us may happen to lie.

Bad queries have small probability during encryption

Suppose q_2 is such that $\mathcal{V}$ contains a (δ_E, δ'_E)-frequent encryption space ($\mathcal{W}$ fixed before sampling $\mathbf{E}^{\mathcal{M}}(mpk, \mathrm{ID}_\star, \$; \$)$.

- I.e. $(1 - \delta_E)^{q_2} \leq \delta'_E$.

Consider a query Q.

- If it is frequent, then only with probability $\leq \delta'_E$ is it not in $\mathcal{V}''$.
- If it is infrequent, then it shows up with probability $\leq \delta_E$.
- $\mathcal{V}'$ has at most $q_3(l+4)q$ dimensions more than $\mathcal{V}''$, where the infrequent queries disturbing us may happen to lie.

- The probability that a query is bad during one encryption is at most $\delta'_E + q_3(l+4)q\delta_E$.
- Expressed via q_2 and δ_E, this is $(1-\delta_E)^{q_2} + q_3(l+4)q\delta_E$ for any δ_E.
- Over all iterations, the badness probability is at most q_3 times larger.

Changes during decryption

- Both times, we execute $\mathbf{D}^{\mathcal{C}(\mathcal{V}',\mathcal{V}'';\mathsf{defs})}(mpk, sk', c)$.
- But queries made during $\mathbf{E}^{\mathcal{C}(\mathcal{V}',\mathcal{V}'';\mathsf{defs})|\mathcal{V}''}(mpk, \mathrm{ID}_{\star}, c; r)$ may have been stored in $\mathcal{V}'$ or $\mathcal{V}''$.

Changes during decryption

- Both times, we execute $\mathbf{D}^{\mathcal{C}(\mathcal{V}',\mathcal{V}'';\mathsf{defs})}(mpk, sk', c)$.
- But queries made during $\mathbf{E}^{\mathcal{C}(\mathcal{V}',\mathcal{V}'';\mathsf{defs})|\mathcal{V}''}(mpk, \mathrm{ID}_\star, c; r)$ may have been stored in $\mathcal{V}'$ or $\mathcal{V}''$.
- Let V'_G span the queries made to $\mathcal{M}'$ by $\mathbf{G}^{\mathcal{M}'}$ when $\mathcal{V}'$ was sampled.
- Let V''_G span the queries made to $\mathcal{M}'$ by $\mathbf{G}^{\mathcal{M}'}$ when $\mathcal{V}''$ was sampled.
- The difference can only come from the difference of V'_G and V''_G.
- The difference is small because of sampling $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathrm{ID}_i, \$; \$))$

Frequent queries during decryption

Let mpk be fixed. Let V_G be the current state of $\mathcal{M}$.

Definition

$V_D \leq V_G$ is δ-frequent decryption space if

- $\mathsf{ID} \stackrel{\$}{\leftarrow} \{0,1\}^\ell$, $sk \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID})$, $c \leftarrow \mathbf{E}^{\mathcal{M}}(mpk, \mathsf{ID}, \$; \$)$, $\mathbf{D}^{\mathcal{M} \rightarrow \mathcal{U}_{\mathsf{ID}}}(mpk, sk, c)$.
- $\Pr[\mathcal{U}_{\mathsf{ID}} \cap V_G \leq V_D] \geq 1 - \delta$.

Let l and q_1 be such, that with probability greater than $(1 - \delta'_D)$, $\mathcal{V}$ contains a δ_D-frequent decryption space.

- If $(1 - \delta_D)^{q_1} \leq \delta'_D / 2l$, then for a fixed ID, the space $\mathcal{U}_{\mathsf{ID}}$ will be found with probability atl least $(1 - \delta'_D / 2l)$.
- If $l \geq 2q / \delta'_D$ then the spaces $\mathcal{U}_{\mathsf{ID}_i}$ for $\mathsf{ID}_1, \ldots, \mathsf{ID}_l$ cover the space $\mathcal{U}_{\mathsf{ID}_\star}$ with probability at least $(1 - \delta'_D / 2)$.

Bad queries have small probability during decryption

- Globally, we have a probability of at most δ'_D for coming up with a non-δ_D-frequent decryption space.
- For each execution of **D**, a query in $V_G \setminus V_D$ is made to the oracle with a probability of at most δ_D.
- Hence the decryption part brings an error of at most $\delta'_D + q_3\delta_D$.
- Recall that $(1-\delta_D)^{q_1} \leq \delta'_D/2l$ and $l \geq 2q/\delta'_D$.

$\mathcal{A}$ + environment, $\mathcal{C}(\mathcal{V}', \mathcal{V}''; \mathsf{defs})$ instead of $\mathcal{V}''$

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$
- Let $(\_, \mathcal{V}''; \_) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
- $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{C}(\mathcal{V}', \mathcal{V}''\to\mathcal{V}; \mathsf{defs})}(mpk, \mathsf{ID}_\star, m; r)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{V}''\to\mathcal{V}; \mathsf{defs})}(mpk, sk', c)$
- Output $(m = m^*)$

$\mathcal{A}$ + environment, $\mathcal{C}(\mathcal{V}', \mathcal{V}''; \text{defs})$ instead of $\mathcal{V}''$

- $\mathrm{ID}_1, \ldots, \mathrm{ID}_l, \mathrm{ID}_\star \xleftarrow{\$} \{0,1\}^\ell$
- $msk \xleftarrow{\$} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathrm{ID}_i)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathrm{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathrm{ID}_\star, \$; \$)$
- Let $(\_, \mathcal{V}''; \_) \leftarrow \mathcal{D}(mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
- $s \xleftarrow{\$} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \text{defs}) \leftarrow \mathcal{D}(mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - $m \xleftarrow{\$} \{0,1\}$; $r \xleftarrow{\$} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{C}(\mathcal{V}', \mathcal{V}''\to\mathcal{V}; \text{defs})}(mpk, \mathrm{ID}_\star, m; r)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{C}(\mathcal{V}', \mathcal{V}''\to\mathcal{V}; \text{defs})}(mpk, sk', c)$
- Output $(m = m^*)$

One more replacement...

$\mathcal{A}$ + environment, $\mathcal{V}'$ instead of $\mathcal{C}(\mathcal{V}', \mathcal{V}''; \text{defs})$

- $\mathrm{ID}_1, \ldots, \mathrm{ID}_l, \mathrm{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathrm{ID}_i)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathrm{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathrm{ID}_\star, \$; \$)$
- Let $(\_, \mathcal{V}''; \_) \leftarrow \mathcal{D}(mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
- $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \text{defs}) \leftarrow \mathcal{D}(mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{V}'}(mpk, \mathrm{ID}_\star, m; r)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{V}'}(mpk, sk', c)$
- Output $(m = m^*)$

How big a difference in output did this replacement make?

Which queries are different for $\mathcal{C}(\mathcal{V}', \mathcal{V}'', \mathrm{defs})$ and $\mathcal{V}'$?

Consider a query $(h_1, a_1), \ldots, (h_k, a_k)$.

- If answer is in $\mathcal{V}'$, then no difference.
- If answer is not in $\mathcal{V}''$, then no difference.
- If answer is in $\mathcal{V}''$, but not in $\mathcal{V}'$, then there is a difference.
  - We don't know how to quantify it.

- If there's difference then we learn something new about $\mathcal{V}''$.
  - Hence the iteration up to q_3 times.
- There are at most $(l+1)q$ dimensions to learn.
  - We do not know at which iterations we learn.
  - So we pick q_3 large enough and output the result at random iteration.

Difference in probability that $m = m^*$: at most $q(l+1)/q_3$.

We know the probability of outputting **true** here...

- $\mathrm{ID}_1, \ldots, \mathrm{ID}_l, \mathrm{ID}_\star \stackrel{\$}{\leftarrow} \{0,1\}^\ell$
- $msk \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathrm{ID}_i)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathrm{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathrm{ID}_\star, \$; \$)$
- Let $(\_, \mathcal{V}''; \_) \leftarrow \mathcal{D}(mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
- $s \stackrel{\$}{\leftarrow} \{1, \ldots, q_3\}$. Do s times:
  - Let $(sk', \mathcal{V}'; \mathrm{defs}) \leftarrow \mathcal{D}(mpk, \mathrm{ID}_1, \ldots, \mathrm{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
  - $m \stackrel{\$}{\leftarrow} \{0,1\}$; $r \stackrel{\$}{\leftarrow} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{V}'}(mpk, \mathrm{ID}_\star, m; r)$
  - Let $m^* \leftarrow \mathbf{D}^{\mathcal{V}'}(mpk, sk', c)$
- Output $(m = m^*)$

We know the probability of outputting **true** here...

- $\mathsf{ID}_1, \ldots, \mathsf{ID}_l, \mathsf{ID}_\star \xleftarrow{\$} \{0,1\}^\ell$
- $msk \xleftarrow{\$} \{0,1\}^\ell$; $mpk \leftarrow \mathbf{G}^{\mathcal{M}}(msk)$
- $\forall i \in \{1, \ldots, l\}$: $sk_i \leftarrow \mathbf{K}^{\mathcal{M}}(msk, \mathsf{ID}_i)$
- For each $i \in \{1, \ldots, l\}$, do q_1 times: $\mathbf{D}^{\mathcal{M}\to\mathcal{V}}(mpk, sk_i, \mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_i, \$; \$))$
- Do q_2 times: $\mathbf{E}^{\mathcal{M}\to\mathcal{V}}(mpk, \mathsf{ID}_\star, \$; \$)$

    - Let $(sk', \mathcal{V}'; \mathsf{defs}) \leftarrow \mathcal{D}(mpk, \mathsf{ID}_1, \ldots, \mathsf{ID}_l, sk_1, \ldots, sk_l, \mathcal{V})$
    - $m \xleftarrow{\$} \{0,1\}$; $r \xleftarrow{\$} \{0,1\}^\ell$; $c \leftarrow \mathbf{E}^{\mathcal{V}'}(mpk, \mathsf{ID}_\star, m; r)$
    - Let $m^* \leftarrow \mathbf{D}^{\mathcal{V}'}(mpk, sk', c)$

- Output $(m = m^*)$

The probability of getting **true** is $1/2 + \sigma$

Getting true in $\mathcal{A}$ + environment

The probability of getting output **true** is at least

$$\frac{1}{2} + \sigma - \frac{q(l+1)}{q_3} - \delta'_D - q_3\delta_D - q_3(1-\delta_E)^{q_2} - q_3^2(l+4)q\delta_E \qquad (*)$$

Getting true in $\mathcal{A}$ + environment

The probability of getting output **true** is at least

$$\frac{1}{2} + \sigma - \frac{q(l+1)}{q_3} - \delta'_D - q_3\delta_D - q_3(1-\delta_E)^{q_2} - q_3^2(l+4)q\delta_E \qquad (*)$$

If we pick $c = \sigma/6$ and

- $l = 2q/c$
- $\delta_E = c^3/(2q/c+4)^3 q^3$
- $\delta_D = c^2/q(2q/c+4)$
- $\delta'_D = c$
- $q_1 = \frac{\log c^2/4q}{\log(1-\delta_D)} \leq \frac{\log 4q/c^2}{\delta_D}$
- $q_2 = \frac{\log(c^2/q(2q/c+4))}{\log(1-\delta_E)} \leq \frac{\log(q(2q/c+4))/c^2}{\delta_E}$
- $q_3 = q(2q/c+4)/c$

then (*) is $\geq 1/2 + c/6$ (and inequalities for δ-s hold, too).