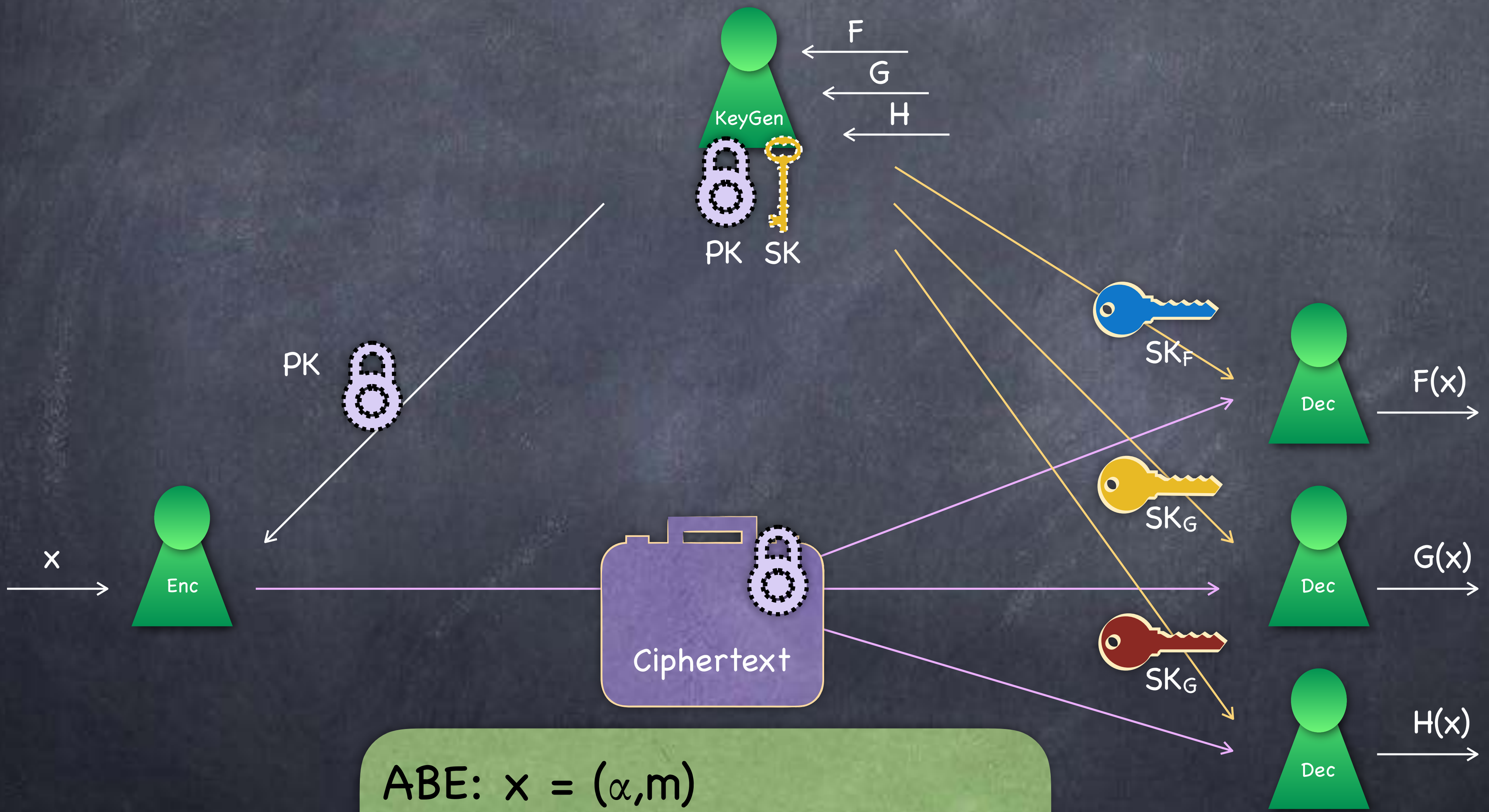
Functional Encryption

Lecture 24

ABE from LWE (ctd.)

Functional Encryption



ABE: $x = (\alpha, m)$

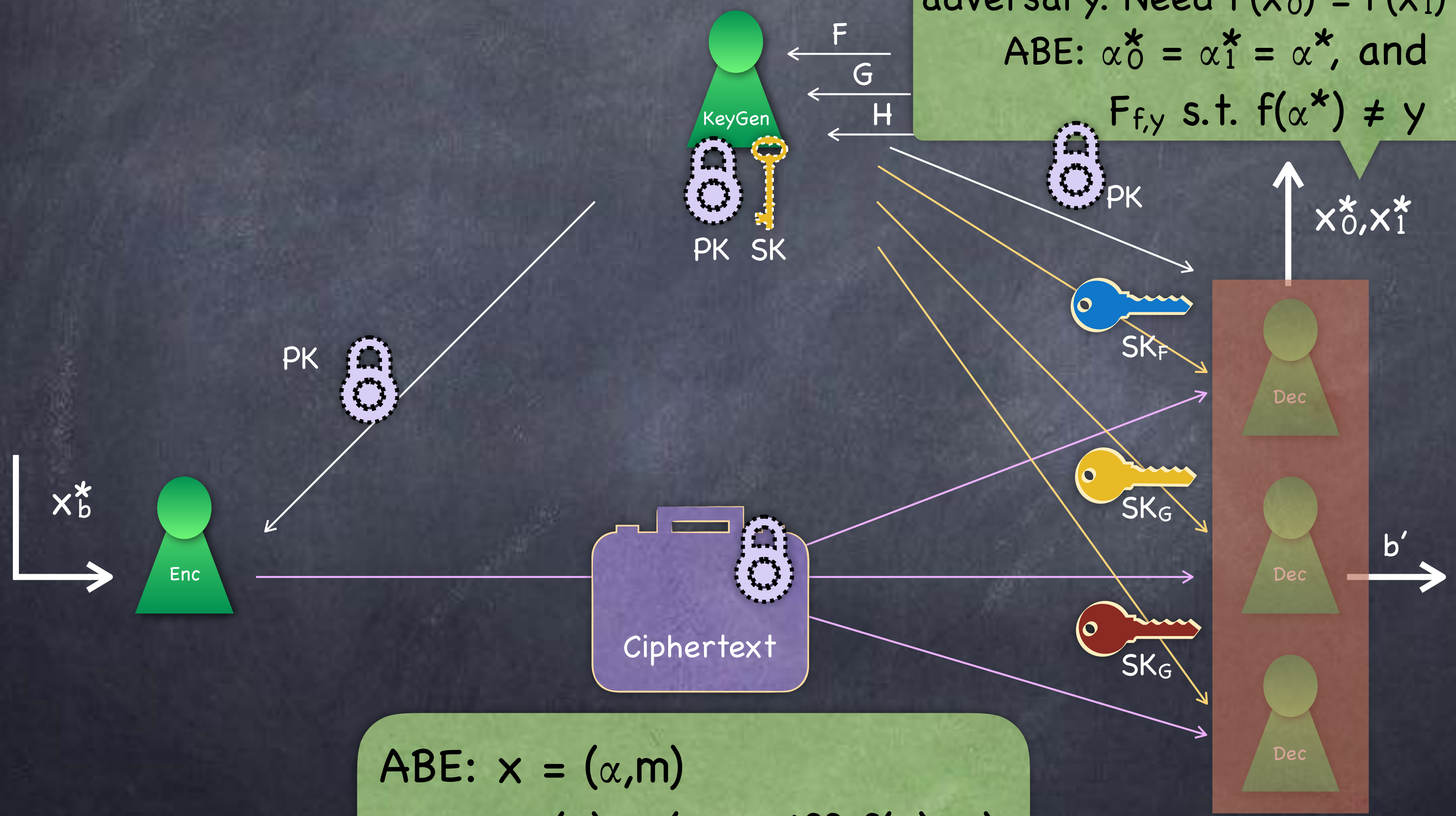
$F_{f,y}(x) = (\alpha,\ m \text{ iff } f(\alpha)=y)$

Functional Encryption

Security

F etc. adaptively chosen by adversary. Need $F(x_0^*) = F(x_1^*)$ etc.

ABE: $\alpha_0^* = \alpha_1^* = \alpha^*$, and $F_{f,y}$ s.t. $f(\alpha^*) \neq y$

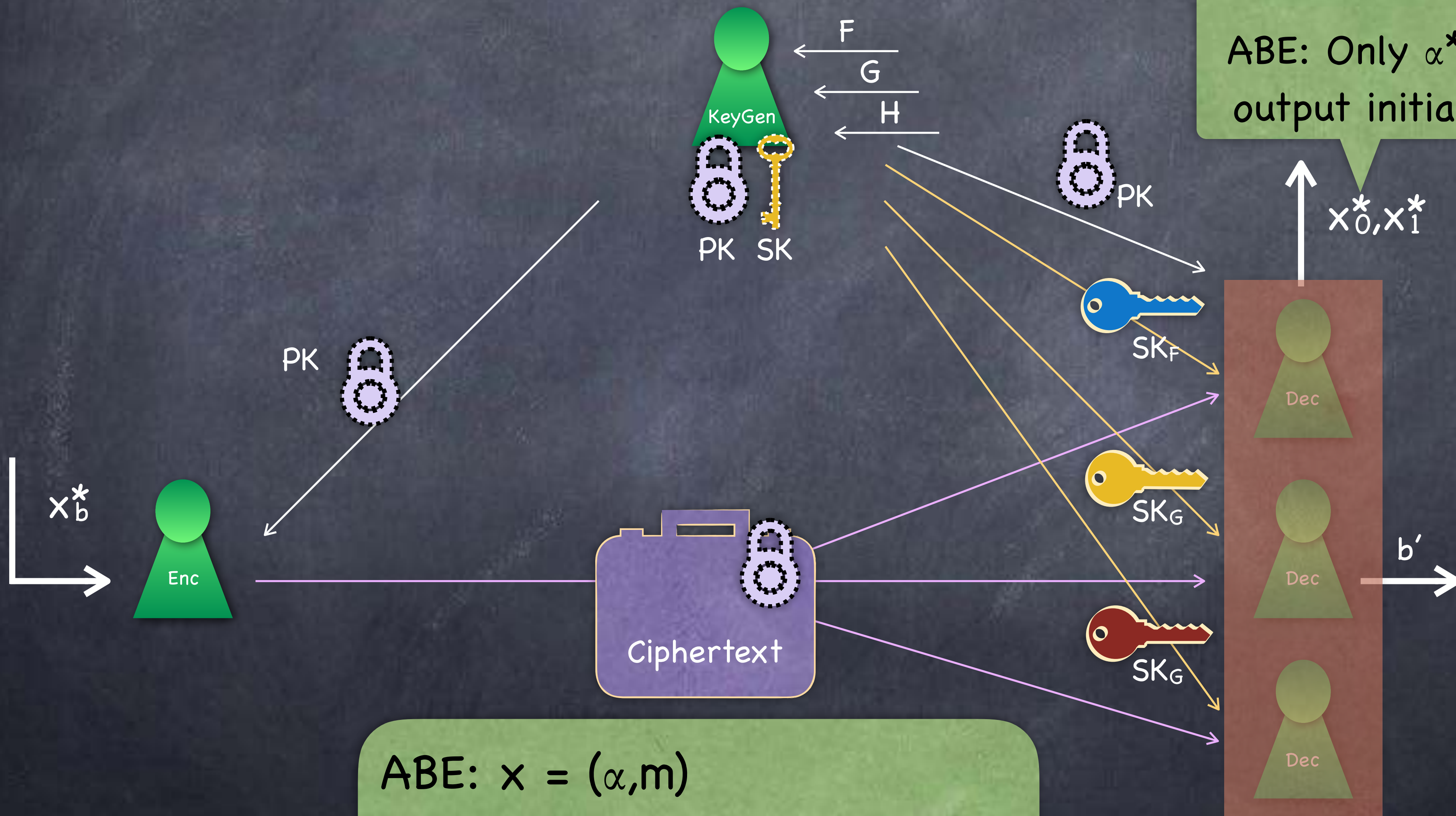


ABE: $x = (\alpha, m)$

$F_{f,y}(x) = (\alpha,\ m \text{ iff } f(\alpha)=y)$

Functional Encryption

Selective Security



Selective: (x^*_0, x^*_1) output before PK

ABE: Only α^* is output initially

ABE: $x = (\alpha, m)$

$F_{f,y}(x) = (\alpha,\ m \text{ iff } f(\alpha)=y)$

KP-ABE From LWE

KeyGen $\leftarrow (f,y)$

$PK = (K_1,\ldots,K_t,K_{mask})$

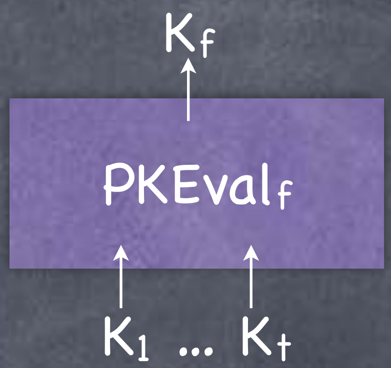
$SK_{f,y}$ can transform $Q_{f,y}(s)$ into $Mask(s;K_{mask})$

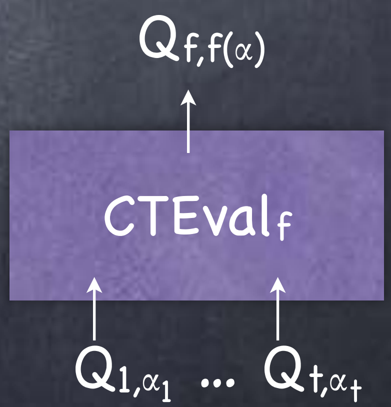
$(\alpha,m) \rightarrow$ Enc

$CT = [\ \alpha,\ Q_{1,\alpha_1}(s),\ldots,\ Q_{t,\alpha_t}(s),$
$m + Mask(s;K_{mask})\ ]$

Dec

If $f(\alpha)=y$, decode $Q_{f,f(\alpha)}$ using $SK_{f,y}$ to get $Mask(s;K_{mask})$





KP-ABE From LWE

- PK: $K_i = [\ A_0 \mid A_i\ ]$ and $K_{mask} = D$, where $A, A_i \leftarrow \mathbb{Z}_q^{n\times m}$, $D \leftarrow \mathbb{Z}_q^{n\times d}$ and MSK: Trapdoor T_{A_0} to sample small R s.t. $[A_0|A]R = D$
- $K_f = [\ A_0 \mid A_f\ ]$ where A_f = PKEval$(f,A_1,\ldots,A_t)$
- For a key A and $x \in \mathbb{Z}_q$ let $A\boxplus x$ denote $[A_0 \mid A + xG]$, where G is the matrix to invert bit decomposition
- $Q_{i,\alpha_i}(\underline{s}) \approx (A_i\boxplus\alpha_i)^T\underline{s}$ where $\underline{s} \leftarrow \mathbb{Z}_q^n$ and ≈ stands for adding a small noise (as in LWE). (Only one copy $\approx A_0^T\underline{s}$ included.)
- $\text{Mask}(\underline{s};D) \approx D^T\underline{s}$. Include $\text{Mask}(\underline{s};D) + \lfloor q/2 \rfloor\, m$.
- $Q_{f,f(\alpha)}(\underline{s})$ = CTEval$(f,\alpha,Q_{1,\alpha_1}(\underline{s})\ldots,Q_{t,\alpha_t}(\underline{s})) \approx (A_f\boxplus f(\alpha))^T\underline{s}$
- $SK_{f,y}$: Compute A_f. Use T_{A_0} to get $R_{f,y}$ s.t. $(A_f\boxplus y)\, R_{f,y} = D$
- Decryption: If $f(\alpha)=y$, then $R_{f,y}^T \cdot Q_{f,f(\alpha)}(\underline{s}) \approx D^T\underline{s}$. Recover $m \in \{0,1\}^d$.

KP-ABE From LWE

- $K_f = [\ A_0 \mid A_f\ ]$ where $A_f = \text{PKEval}(f, A_1, \ldots, A_t)$
- $Q_{f,f(\alpha)}(\underline{\mathbf{s}}) = \text{CTEval}(f, \alpha, Q_{1,\alpha_1}(\underline{\mathbf{s}}) \ldots, Q_{t,\alpha_t}(\underline{\mathbf{s}})) \approx (A_f \boxplus f(\alpha))^T \underline{\mathbf{s}}$
- CTEval computed gate-by-gate
  - Enough to describe $\text{CTEval}(f_1+f_2, (y_1,y_2), Q_{f_1,y_1}(\underline{\mathbf{s}}), Q_{f_2,y_2}(\underline{\mathbf{s}}))$ and $\text{CTEval}(f_1 \cdot f_2, (y_1,y_2), Q_{f_1,y_1}(\underline{\mathbf{s}}), Q_{f_2,y_2}(\underline{\mathbf{s}}))$
  - Recall $Q_{f_1,y_1}(\underline{\mathbf{s}}) \approx (A_{f_1} \boxplus y_1)^T \underline{\mathbf{s}} = [\ A_0 \mid A_{f_1} + y_1 G\ ]^T \underline{\mathbf{s}}$
  - Keep $\approx A_0{}^T \underline{\mathbf{s}}$ aside. To compute $[\ A_{g(f_1,f_2)} + g(y_1,y_2) G\ ]^T \underline{\mathbf{s}}$ for $g = +, \cdot$
  - $[\ A_{f_1} + y_1 G\ ]^T \underline{\mathbf{s}} + [\ A_{f_2} + y_2 G\ ]^T \underline{\mathbf{s}} = [\ A_{f_1+f_2} + (y_1 + y_2)\, G\ ]^T \underline{\mathbf{s}}$ with $A_{f_1+f_2} = A_{f_1} + A_{f_2}$ (errors add up)
  - $y_2 \cdot [\ A_{f_1} + y_1 G\ ]^T \underline{\mathbf{s}} - B(A_{f_1})^T [\ A_{f_2} + y_2 G\ ]^T \underline{\mathbf{s}} = [\overbrace{-A_{f_2} B(A_{f_1})}^{A_{f_1 \cdot f_2}} + y_1 y_2 G]^T \underline{\mathbf{s}}$
    - $err = y_2 \cdot err_1 + B(A_{f_1})^T err_2$. Need y_2 to be small.

KP-ABE From LWE

- Security?
- Sanity check: Is it secure when no function keys $SK_{f,y}$ are given to the adversary?
- Security from LWE
  - All components in the ciphertext are LWE samples of the form $\langle \underline{\mathbf{a}},\underline{\mathbf{s}} \rangle$+noise, for the same $\underline{\mathbf{s}}$ and random $\underline{\mathbf{a}}$.
  - Hence all pseudorandom, including the mask $D^T\underline{\mathbf{s}}$ + noise
- Do the secret keys $SK_{f,y}$ make it easier to break security?
- Claim: No!

KP-ABE From LWE

- Scheme is selective-secure (under LWE)
- Recall selective security: Adversary first outputs (x_0,x_1) s.t. $F(x_0)=F(x_1)$ for all F for which it receives keys. Challenge = $\mathrm{Enc}(x_b)$
  - ABE: $x=(\alpha,m)$ and $F_{f,y}(x) = (\alpha,\ m \text{ iff } f(\alpha)=y)$
  - $F(x_0)=F(x_1) \Rightarrow$ same α^* and $f(\alpha^*) \neq y$
- Simulated execution (indistinguishable from real) where PK* is designed such that without MSK* can generate $SK_{f,y}$ for all f and all $y \neq f(\alpha^*)$
  - Breaking encryption for α^* will still need breaking LWE!

KP-ABE From LWE

- Simulated execution (indistinguishable from real) where PK* is designed such that without MSK* can generate $SK_{f,y}$ for all (f,y) s.t. $y \neq f(\alpha^*)$
  - D, A_0 as before but without trapdoor (i.e., given from outside)
  - Other keys A_i are (differently) trapdoored: $A_i^* = A_0S_i - \alpha^*_iG$ where S_i have small entries
    - A_0S_i close to uniform (like A_i) by extraction argument
  - Consider a query (f,y) where $y \neq f(\alpha^*) =: y^*$
    - Need to give $R_{f,y}$ s.t. $(A_f \boxplus y)\, R_{f,y} = D$
    - Do not have a the trapdoor for $[\ A_0 \mid A_f - y^*G\ ]$
    - Will use a trapdoor for $A_f - y^*G$ instead!

Two Trapdoors

- Given A_0, $A \in \mathbb{Z}_q^{n\times m}$ of rank n, and D, can find small R s.t. $[\ A_0 \mid A\ ]\ R = D$ if we have:

  a "small" basis T_{A_0} for $\Lambda^{\perp}{}_{A_0}$

  - Either the trapdoor T_{A_0} for sampling small R_0 s.t. $A_0R_0 = U$
  - Or (S, T_{A-A_0S}) s.t. $A - A_0S$ has full rank and S "small"
    - E.g., small S s.t. $A = A_0S + zG$ for $z \neq 0$ and G has a known trapdoor T_G (which is also a trapdoor for zG)
- In the actual construction, we used the fact that (A_0, T_{A_0}) can be generated together, to be able to give out function keys $R_{f,y}$. (A_i picked randomly, and A_f random).
- In the security proof, given an A_0 from outside, will construct $A_i = A_0S_i - \alpha_i{}^*G$ and maintain $A_f = A_0S_f - f(\alpha^*)G$. Then, can sample $R_{f,y}$ if $y \neq f(\alpha^*)$ and hence $A_f + yG = A_0S_f + zG$ for $z = y - f(\alpha^*) \neq 0$.

Simulation of Keys

- PK: A_0, D (externally given) and $A_i^* = A_0 S_i - \alpha^*_i G$
- S_f defined so that:
  - $A_f^* = A_0 S_f - f(\alpha^*)G$ where A_f^* from PKEval
  - $Q^*_{f,y}(\underline{\mathbf{s}}) = [A_f^* \boxplus y]^T \underline{\mathbf{s}}$ from CTEval
- Verify:
  - $S_{f_1+f_2} = S_{f_1} + S_{f_2}$
  - $S_{f_1 \cdot f_2} = -S_{f_2}\, B(A_{f_1}) + f_2(\alpha^*)\, S_{f_2}$
- S_f remains small if $f_2(\alpha^*)$ is small

Simulation of Keys

- Simulated KeyGen which produces keys which are statistically close to the original keys
  - Accepts A_0 from outside
  - Picks $A_i^* = A_0 S_i - \alpha^*_i G$ where S_i have small entries
    - Keys A_f^* and ciphertexts $Q^*_{f,y}(\underline{\mathbf{s}})$ defined by EvalPK and EvalCT. $A_f^* = A_0 S_f - f(\alpha^*)G$ and $Q^*_{f,y}(\underline{\mathbf{s}}) = [A_f^* \boxplus y]^T \underline{\mathbf{s}}$
  - Given (f,y) s.t. $y \neq f(\alpha^*)$, to create $R_{f,y}$ s.t. $(A_f^* \boxplus y)\, R_{f,y} = D$:
    - $A_f^* \boxplus y = [\ A_0 \mid A_f^* + yG] = [\ A_0 \mid A_0 S_f - f(\alpha^*)G + yG]$
      $= [\ A_0 \mid A_0 S_f + zG]$ where $z \neq 0$
    - So can sample small $R_{f,y}$ as required
  - Simulated keys (including function keys) are statistically indistinguishable from the keys in the real experiment

Simulation

- In the simulated experiment, challenge ciphertext can be derived from $\approx A_0^T\underline{\mathbf{s}}$ and $\approx D^T\underline{\mathbf{s}}$ (given externally) and $\{S_i\}_i$
  - $(A_i^* + \alpha_i G)^T\underline{\mathbf{s}} = (A_0 S_i)^T\underline{\mathbf{s}} = S_i^T A_0^T\underline{\mathbf{s}}$ (and $S_i^T\cdot$noise is fresh noise)
- By LWE, in the simulated experiment, adversary has negligible advantage
- View of the adversary in the simulated experiment is statistically close to that in the real experiment
- Hence the advantage of the adversary in the real experiment is also negligible