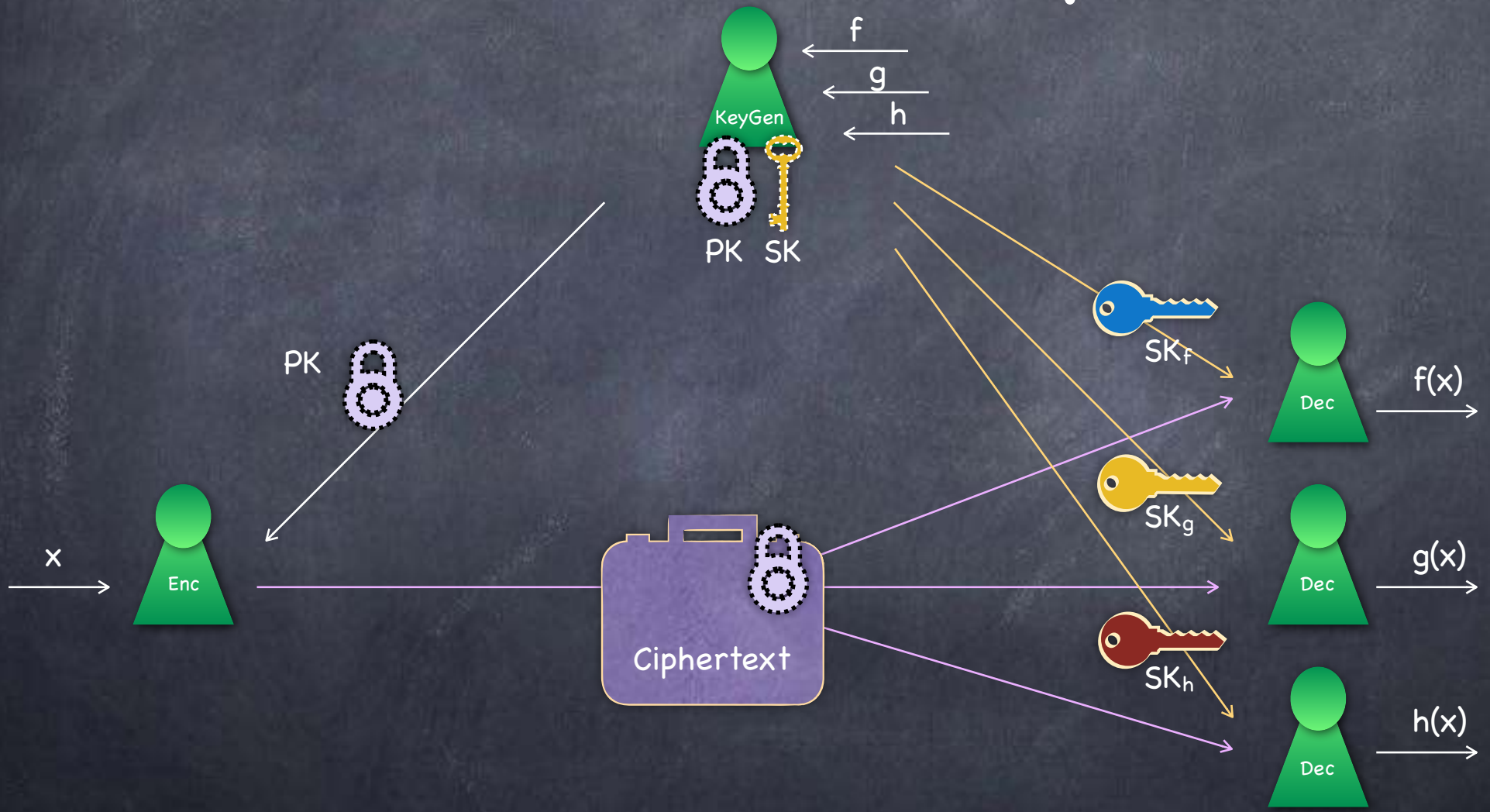
Functional Encryption

Lecture 23

ABE from LWE

Functional Encryption



Index-Payload Functions

- Message $x=(\alpha,m)$, and functions f_π s.t. $f_\pi(x)=(\alpha,$ m iff $\pi(\alpha)=1)$
  - α is the index which is public, and m is output iff $\pi(\alpha)=1$, where π is a predicate
  - Identity-Based Encryption (IBE): $\pi_\beta(\alpha) = 1$ iff $\alpha=\beta$
  - Attribute-Based Encryption (ABE)
    - Key-Policy ABE: $\alpha \in \{0,1\}^n$ and π a circuit (policy) over n Boolean variables
    - Ciphertext-Policy ABE: α a circuit (policy) over n Boolean variables, and π evaluates an input circuit on a fixed assignment
- Predicate Encryption: $x=(\alpha,m)$ and function f_π contains a predicate π s.t. $f_\pi(x) = m$ iff $\pi(\alpha)=1$ ($\perp$ otherwise).
  - Note: Not public-index, as α remains hidden

KP-ABE For Linear Policies

- PK: g, $Y=e(g,g)^y$, $T = (g^{t_1},\ldots, g^{t_n})$ (n attributes)
- MSK: y and t_a for each attribute a
- Enc(m,A;s) = $(A, \{ T_a^s \}_{a\in A}, m.Y^s)$
- SK for policy W (with n rows): Let $u=(u_1 \ldots u_n)$ s.t. $\Sigma_a u_a = y$. For each row a, let $x_a = \langle W_a,u\rangle/t_a$. Let Key $X = \{ g^{x_a} \}_{a\in[n]}$
- Dec $((A,\{Z_a\}_{a\in A},C); \{X_a\}_{a\in[n]})$: Get $Y^s = \Pi_{a\in A}\, e(Z_a,X_i)^{v_a}$ where $v = [v_1 \ldots v_n]$ s.t. $v_a=0$ if $a \notin A$, and $v\,W = [1\ldots1]$. $m = C/Y^s$
- A random vector u for each key to prevent collusion
- Selective (attribute) security based on Decisional-BDH

Today: KP-ABE From LWE

- Policy given as an arithmetic circuit f: $\mathbb{Z}_q^t \to \mathbb{Z}_q$ and a value y. Key $SK_{f,y}$ decrypts ciphertext with attribute α iff $f(\alpha) = y$.
- Very expressive policy $\Rightarrow$ no conceptual distinction between CP-ABE and KP-ABE
  - Can implement CP-ABE also as KP-ABE: α encodes a policy (as bits representing a circuit) and f implements evaluating this policy on attributes hardwired into it

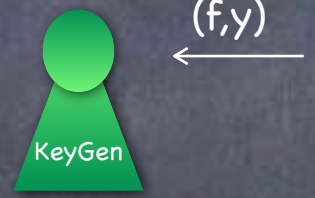
KP-ABE From IBE?

- Policy is (f,y) where f comes from a very large function family
- But suppose we had a small number of functions f
- Then enough to have a set of IBE instances one for each f
  - PK = { K_f } one for each f
  - $SK_{f,y}$ = SK for ID y under scheme for f
  - $Enc_{PK}(\alpha,m) = (\alpha, \{ Enc_{K_f}(m;f(\alpha)) \}_f)$
- At a high level, will emulate this idea. But will allow constructing K_f and $Enc_{K_f}(m;y)$ for any function f using a circuit for f from a few components (corresponding to the inputs to f)

Key-Homomorphism

- Overview:
  - PK consists of keys K_i, i=1,...,t (for t attributes)
  - K_1,..., K_1 can be transformed into a public key K_f
  - Ciphertext will have the message masked with mask(s), where s is randomly chosen
  - Ciphertext also includes $Q_{i,\alpha_i}(s)$ using key K_i and attribute α_i
  - Q_{i,α_i} can be combined into an encoding $Q_{f,f(\alpha)}(s)$ under key K_f
  - MSK can be used to compute $SK_{f,y}$ that can transform $Q_{f,y}(s)$ into mask(s).

KP-ABE From LWE

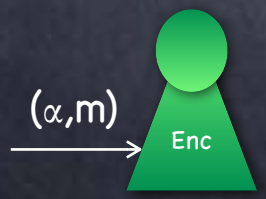


(f,y)

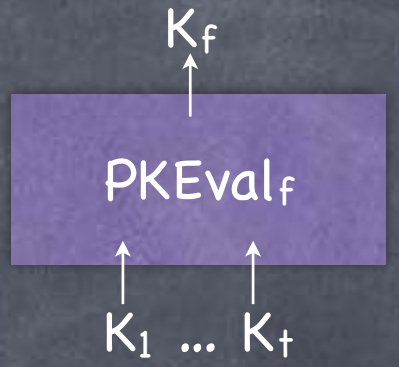
$PK = (K_1,\ldots,K_t,K_{mask})$

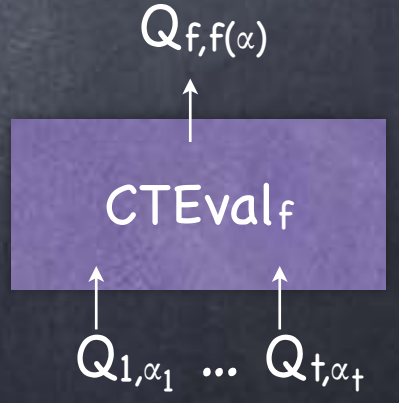
$SK_{f,y}$ can transform $Q_{f,y}(s)$ into $Mask(s;K_{mask})$

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



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 $A_0, A_i \leftarrow \mathbb{Z}_q^{n \times m}$, $D \leftarrow \mathbb{Z}_q^{n \times d}$
  - m >> n log q so that $A\underline{r}$ is statistically close to uniform even when $\underline{r}$ has small entries (e.g., bits)
- Fact: Can pick A along with a trapdoor T_A (a "good" basis for the lattice $L_A^{\perp}$) so that, given for any $\underline{u} \in \mathbb{Z}_q^n$, one can use T_A to sample $\underline{r}$ with small $\mathbb{Z}_q$ entries (from a discrete Gaussian) that satisfies $A\underline{r} = \underline{u}$
  - Also sample R with small entries so that AR=D for $D \in \mathbb{Z}_q^{n \times d}$
  - Also can sample such an R so that $[\ A \mid B\ ]R = D$ for any B
    - Need $[\ A \mid B\ ]\ [\ R_1 \mid R_2\ ]^T = D$. Sample R_2. Then use T_A to sample R_1^T s.t. $AR_1^T = D - BR_2^T$
- MSK: Trapdoor T_{A_0}

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}
- $K_f = [\, A_0 \mid A_f \,]$ where $A_f = \mathrm{PKEval}(f, A_1, \ldots, A_t)$ (To be described)
- 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
- $Q_{i,\alpha_i}(\underline{\mathbf{s}}) \approx (A_i \boxplus \alpha_i)^T \underline{\mathbf{s}}$ where $\underline{\mathbf{s}} \leftarrow \mathbb{Z}_q^n$ and $\approx$ stands for adding a small noise (as in LWE). (Only one copy $\approx A_0^T \underline{\mathbf{s}}$ included.)
- $\mathrm{Mask}(\underline{\mathbf{s}}; D) \approx D^T \underline{\mathbf{s}}$. Include $\mathrm{Mask}(\underline{\mathbf{s}}; D) + \lfloor q/2 \rfloor\, m$.
- $Q_{f,f(\alpha)}(\underline{\mathbf{s}}) = \mathrm{CTEval}(f, \alpha, Q_{1,\alpha_1}(\underline{\mathbf{s}}) \ldots, Q_{t,\alpha_t}(\underline{\mathbf{s}})) \approx (A_f \boxplus f(\alpha))^T \underline{\mathbf{s}}$ (To be described)
- $SK_{f,y}$: 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 $R_{f,y}^T \cdot Q_{f,f(\alpha)}(\underline{\mathbf{s}}) \approx D^T \underline{\mathbf{s}}$. Recover $m \in \{0,1\}^d$.

KP-ABE From LWE

- $K_f = [\ A_0 \mid A_f\ ]$ where $A_f = \mathsf{PKEval}(f, A_1, \ldots, A_t)$ (To be described)
- $Q_{f,f(\alpha)}(\underline{\mathbf{s}}) = \mathsf{CTEval}(f, \alpha, Q_{1,\alpha_1}(\underline{\mathbf{s}}) \ldots, Q_{t,\alpha_t}(\underline{\mathbf{s}})) \approx (A_f \boxplus f(\alpha))^T \underline{\mathbf{s}}$ (To be described)
- CTEval computed gate-by-gate
  - Enough to describe $\mathsf{CTEval}(f_1+f_2, (y_1,y_2), Q_{f_1,y_1}(\underline{\mathbf{s}}), Q_{f_2,y_2}(\underline{\mathbf{s}}))$ and $\mathsf{CTEval}(f_1 \cdot f_2, (y_1,y_2), Q_{f_1,y_1}(\underline{\mathbf{s}}), Q_{f_2,y_2}(\underline{\mathbf{s}}))$
  - 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)
  - $y_2 \cdot [\ A_{f_1}+y_1 G\ ]^T \underline{\mathbf{s}} - B(A_{f_1})^T [\ A_{f_2}+y_2 G\ ]^T \underline{\mathbf{s}} = [-A_{f_2} B(A_{f_1}) + y_1 y_2 G]^T \underline{\mathbf{s}}$
    - $\mathsf{err} = y_2 \cdot \mathsf{err}_1 + B(A_{f_1})^T \mathsf{err}_2$. Need y_2 to be small.

$A_{f_1 \cdot f_2}$

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 $\langle \mathbf{a}, \mathbf{s} \rangle$+noise, for the same $\mathbf{s}$ and random $\mathbf{a}$.
  - Hence all pseudorandom, including the mask $D^T\mathbf{s}$ + 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 = $Enc(x_b)$
  - 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!
  - Next time