6.892 Computing on Encrypted Data November 23, 2013

Lecture 25

Lecturer: Vinod Vaikuntanathan *Scribe: Adin Schmahmann*

1 Trapdoors

Given l matrices $A_1, A_2, ...A_l$ and a "trapdoor" for A_i (for some i) one can find a trapdoor for $[A_1||A_2...||A_l]$.

$TrapFind(A_1, \ldots, A_l, (i, T_{A_i})) = T_{[A_1||\ldots||A_l]}$

Whereby the "trapdoor" means that $[A_1||\ldots||A_l]\begin{pmatrix} t1 \\ t2 \\ \vdots \\ tn \end{pmatrix} = 0 \implies A_1t_1 + \ldots + A_lt_l = 0.$

The trapdoors from TrapFind are such that:

$$\forall_{i,j} \ \ (\text{TrapSamp}(A_1, \ldots, Al, (i, T_{A_i})), A_1, \ldots A_l) \approx_s (\text{TrapSamp}(A_1, \ldots, Al, (j, T_{A_j})), A_1, \ldots, A_l)$$

2 IBE

Mpk $= \begin{pmatrix} A_{1,0} & \cdots & A_{l,0} \\ A_{1,1} & \cdots & A_{l,1} \end{pmatrix}, y$ with each $A_{j,k} \in \mathbb{Z}_q^{n\times m}$ and $y \in_R \mathbb{Z}_q^n$

Msk $= (T_{A_{1,0}}, T_{A_{1,1}})$

sk_{id}: Assume $id \in \{0,1\}^l$

$A_{id} \in \mathbb{Z}_q^{n\times m\times l} \triangleq [A_{1,id_1}||\ldots||A_{l,id_l}]$

Generate Trapdoor T_{id} for A_{id}

$sk_{id} =$ short r s.t. $A_{id} \cdot r = y$

$\mathsf{Enc}(id, \mu) = \mathsf{dualRegev.ENC}(pk, \mu) = c$

where $\mu \in \{0,1\}$, $pk = (A_{id}, y)$, and $c = A_{id}^{\intercal}s + e, y^{\intercal}s + e\prime + \mu\lceil q/2\rfloor$

$\mathsf{Dec}(sk_{id}, c) = \mathsf{dualRegev.DEC}(r, c)$

Note: In the simulation based security model depicted below selecting id^* first weakens security, but makes the proof significantly easier.

2.1 Simulator

$$
\begin{array}{r|l}
\text{Challenger} & \text{Adversary} \\
\xrightarrow{MPK} & \\
 & \xleftarrow{id} \\
\xrightarrow{sk_{id}} & \\
 & \xleftarrow{id^*,(\mu_0,\mu_1)} \\
\xrightarrow{sk_{id}} & \\
\text{Select } b \text{ from } \{0,1\} & \\
\xrightarrow{\text{Enc}(id^*,\mu_b)} & \\
 & \xleftarrow{b'}
\end{array}
$$

2.2 Reduction

$$
\begin{array}{r|l}
\text{Challenger} & \text{Adversary} \\
 & \xleftarrow{id^*} \\
\xrightarrow{\text{PK}=[B_1,\ldots B_l],y} & \\
 & \text{MPK} = (A_{i,j}), y \\
 & A_{i,id_i^*} = B_i \\
 & A_{i,\overline{id_i^*}} = \text{Generate randomly with trapdoor} \\
 & \xleftarrow{(\mu_0,\mu_1)} \\
\text{Select } b \text{ from } \{0,1\} & \\
\xrightarrow{\text{dualRegev}(pk,\mu_b)} & \\
 & \xleftarrow{id}
\end{array}
$$

3 ABE

Enc(X, μ) where $X \in \{0,1\}^l$ and $\mu \in \{0,1\}$
Dec(sk_F, c_x) and should get $\mu \iff F(x) = 1$

Mpk $= \begin{pmatrix} A_{1,0} & \cdots & A_{l,0} \\ A_{1,1} & \cdots & A_{l,1} \end{pmatrix}, y$ with each $A_{j,k} \in \mathbb{Z}_q^{n \times m}$ and $y \in_R \mathbb{Z}_q^n$

Msk $= \begin{pmatrix} T_{A_{1,0}} & \cdots & T_{A_{l,0}} \\ T_{A_{1,1}} & \cdots & T_{A_{l,1}} \end{pmatrix}$

sk_F : Assume $F : \{0,1\}^l \to \{0,1\}$

3.1 SK_C

1) $\forall$ wires w generate $(A_{w,0}, T_{w,0})$ and $(A_{w,1}, T_{w,1})$

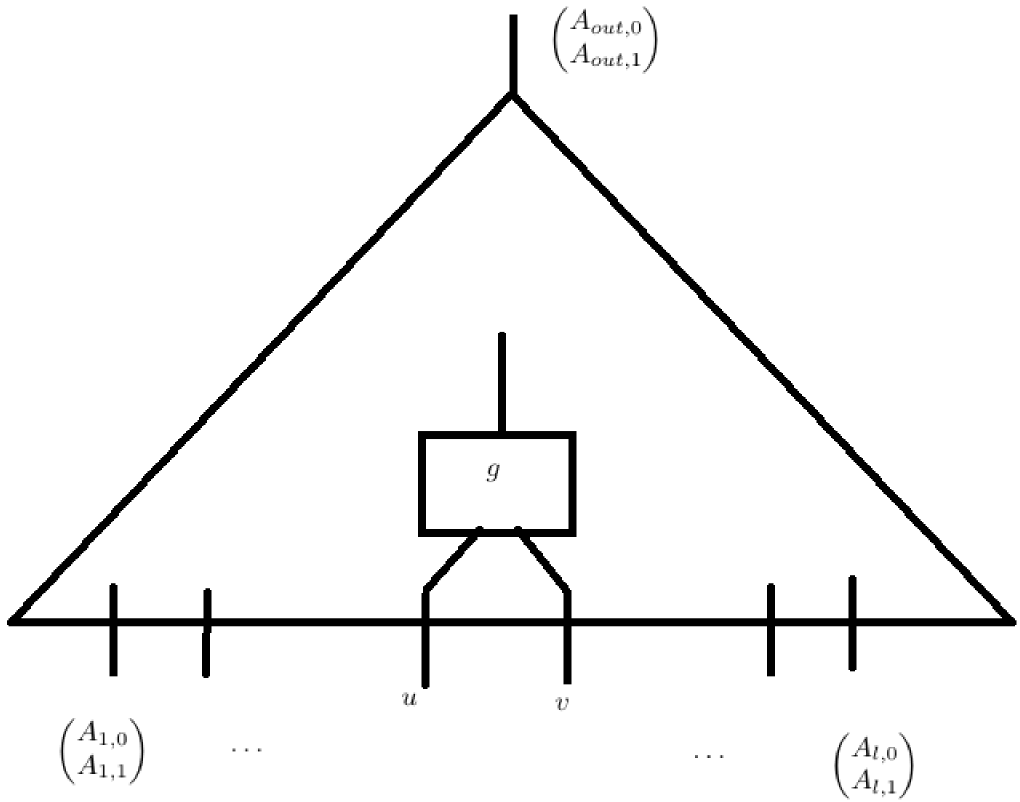

Figure 1: Schematic for ABE circuit

2) $\forall$ gates $g = (u, v; w)$ generate $R_{b,c} : A^{\intercal}_{u,b}s + A^{\intercal}_{v,c}s \implies A^{\intercal}_{w,f(b,c)}s$ for the function f that represents the gate and where $b, c \in \{0, 1\}$. For instance the NAND gate has $R_{0,0} : A^{\intercal}_{u,0}s + A^{\intercal}_{v,0}s \implies A^{\intercal}_{w,1}s$.

3) Output Gate: Publish short r such that $A_{out,1} \cdot r = y$. $sk_c = (\text{Garbled Tables}, r_{out})$

Decrypt by getting $A_{out,c(x)}s + noise$ and using $A_{out,1} \cdot r_{out} = y$ to get μ from $y^{\intercal}s + e + \mu\lceil q/2\rfloor$

What are the Garbled Tables?

Using $R_{0,0}$ an an example:
Come up with $R_{0,0}$ such that $[A_{u,0}||A_{v,0}]R_{0,0} = A_{w,g(0,0)}$ (ex: for NAND $g(0,0) = 1$)
$(s^{\intercal}[A_{u,0}||A_{v,0}] + [e_{u,0}||e_{v,0}]) \cdot R_{0,0} = s^{\intercal}A_{w,g(0,0)} + e_{w,g(0,0)}$ where $e_{w,g(0,0)} \triangleq [e_{u,0}||e_{v,0}] \cdot R_{0,0}$
$|e_{w,...}| \leq 2m \cdot \max(e_{u,0}, e_{v,0})$ (However, current technology for finding small R's requires $m^{O(1)}$ not $2m$)
$|e_{out}| \leq m^{O(d)}$
Lemma 1. *Correctness*
ABE decryption succeeds for circuits C with depth d=d(C) if $m^{O(d)} \leq q$

Compute Rs using given trapdoors for As (ex: $A_{u,0}, A_{v,0} for R_{0,0}$).

3.2 Security Reduction

$\text{pk} = [B_1, \dots B_l], y \quad \xleftarrow{x^*}$

MPK $= (A_{i,j}), y$

$A_i, xi^* = B_i$

$A_i, \overline{xi^*} =$ Generate randomly with trapdoor

$\xleftarrow{\text{c such that } c(x^*) = 0}$

$\xrightarrow{sk_c}$

$\xleftarrow{\mu_0, \mu_1}$

$\xrightarrow{\text{Enc}(x^*, \mu)}$

$\xrightarrow{\text{dualRegev}(pk, \mu_b)}$

How to generate sk_c for the adversary such that $c(x) = 0$

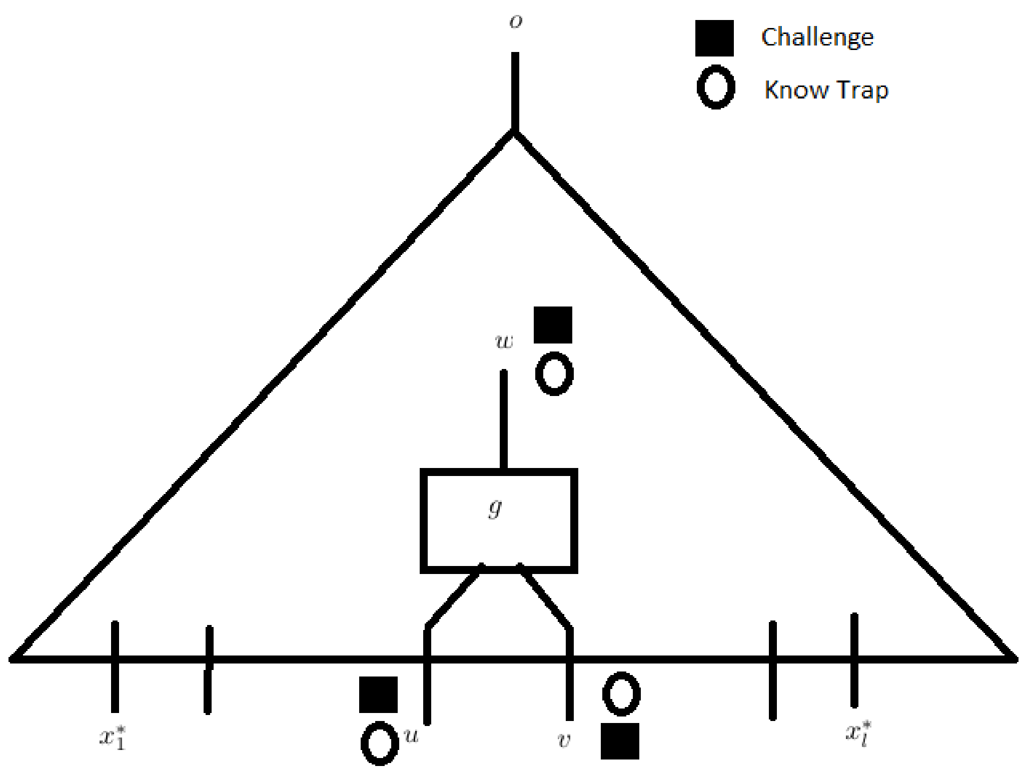

Figure 2: Schematic for NAND ABE circuit simulator

Take example where g=NAND, and say we know trapdoors for $u = 0$ and $v = 1$. We need to have a trapdoor for either $A_{w,0}$ or $A_{w,1}$, but need to find both $A_{w,0}$ and $A_{w,1}$.

$[\underline{A_{u,0}}||A_{v,0}]R_{0,0} = A_{w,1}$
$[\underline{A_{u,0}}||\underline{A_{v,1}}]R_{0,1} = A_{w,1}$

$[A_{u,1}||A_{v,0}]R_{1,0} = A_{w,1}$
$[A_{u,1}||\underline{A_{v,1}}]R_{1,1} = A_{w,0}$

We have trapdoors for underlined matrices. Pick $R_{1,0}$ from a distribution and given the $R_{1,0}$ determine $A_{w,1}$. Additionally, pick $Aw, 0$ with a trapdoor.