Modern Cryptology - Problem Set 4. name: Guy Levy. ID: 206865362.

1 . Homomorphic Encryption and CRHF

1. let $y \in \mathbb{F} : y \neq 0 \Rightarrow \exists j \in [n] : y_j \neq 0$

$$Pr_{x \in_R \mathbb{F}}\Big[< x, y >= 0\Big] = Pr_{x \in_R \mathbb{F}}\Big[\sum_{i=0}^{n} x_i y_i = 0\Big]$$

$$= Pr_{x \in_R \mathbb{F}}\Big[- x_j y_j = \sum_{i \neq j}^{n} x_i y_i\Big]$$

$$= Pr_{x \in_R \mathbb{F}}\Big[x_j = -y_j \cdot (\sum_{i \neq j}^{n} x_i y_i)\Big]$$

(note : $-y_j \cdot (\sum_{i \neq j}^{n} x_i y_i$ is some random number in $\mathbb{F}$ as x is random.)

$$= Pr_{a \in_R \mathbb{F}}\Big[a = b\Big]$$

(for some b)

$$= \frac{1}{|\mathbb{F}|}$$

2. Adversary chooses $x \in_R \mathbb{F}^n$ at random,
we saw in (1) that if $y \neq 0$:

$$Pr_{x \in_R \mathbb{F}}\Big[< x, y >= 0\Big] = \frac{1}{|\mathbb{F}|}$$

And in the case that $y = 0$ that probability is 1.

3. Assume there exists Adversary A and $p(n)$ polynomial such that:

$$Pr_{k \in_R G(1^n), y \in_R \mathbb{F}^n}\Big[A(E_k(y)) = x :< x, y >= 0\Big] \geq \frac{1}{|\mathbb{F}|} + \frac{1}{p(n)}$$

Will show (G, E, D) not CPA secure, In contradiction to assumption.
Thus will get what we wanted to prove.

Construct A' to break (G, E, D)'s CPA security:

A' sends challenger $m_0 \in_R \{0, 1\}^n, m_1 \in_R \{0, 1\}^n$.
Challenger sends back $E_k(m_b)$ for random $b \in_R \{0, 1\}$.
A' computes $A(E_k(m_b))$ to get some x.
If $< m_0, x >= 0$ returns $b' = 0$, else returns $b' = 1$.

Claim: A' breaks CPA:
i.e. claim $Pr[b' = b] \geq \frac{1}{2} + \frac{1}{p'(n)}$ for p' some polynomial.

$$Pr_{b \in_R \{0,1\}}[b' = b] = Pr_{b \in_R \{0,1\}}[A'(E_k(m_b)) = b]$$

$$= Pr_{b \in_R \{0,1\}}[A'(E_k(m_0)) = 0] \cdot Pr[b = 0] + Pr_{b \in_R \{0,1\}}[A'(E_k(m_1)) = 1] \cdot Pr[b = 1]$$

$$= 0.5 \cdot Pr[< m_0, x >= 0] + 0.5 \cdot Pr[< m_1, x >\neq 0]$$

$$\geq^{(*)} 0.5 \cdot (\frac{1}{|\mathbb{F}|} + \frac{1}{p(n)}) + 0.5 \cdot (1 - \frac{1}{|\mathbb{F}|} - \frac{1}{|\mathbb{F}|^n})$$

$$= \frac{1}{2} + \frac{1}{2p(n)} - \frac{1}{|\mathbb{F}|^n}$$

$$\geq^{(**)} \frac{1}{2} + \frac{1}{p'(n)}$$

$(*)$: $Pr[< m_0, x >= 0] \leq \frac{1}{|\mathbb{F}|} + Pr[x = 0]$
$(**)$: for $p'(n) = 3p(n)$. for all $n > N$ for some $N \in \mathbb{N}$

4. was not able to solve (especially was not able to use extension as I have 3 exams between 7.7 and 9.7)

5. was not able to solve

2 . Circular Security of Regev Encryption

2 .1 Circular Security

Enough to prove that we can get $enc_{pk}(s_i)\ \forall i \in [n]$ for free.
From the fact that Regev is CPA, we can conclude that its circular secure.

Given (a, τ) an encryptio for 0, Claim $(a - \frac{q}{2}u_i, \tau)$ is an encryption for s_i and thus we conclude the proof.

Proof of claim:
Lets calculate $dec_{sk}((a - \frac{q}{2}u_i, \tau))$

$$|\tau- < a - \frac{q}{2}u_i, s > | = |\tau- < a, s > + \frac{q}{2} < u_i, s > | = |\tau- < a, s > + \frac{q}{2}s_i|$$

if $s_i = 0$ this equals $|\tau- < a, s > |$ which is exactly the way we decrypt (a, τ) which is an encryption for 0. and thus $dec_{sk}((a - \frac{q}{2}u_i, \tau)) = 0$

if $s_i = 1$ this equals $|\tau- < a, s > + \frac{q}{2}|$, now because $\tau- < a, s >$ is a number in $[-B \cdot n, B \cdot n]$ then $\tau- < a, s > + \frac{q}{2}$ is in $[\frac{q}{2} - B \cdot n, \frac{q}{2} + B \cdot n]$ and so $|\tau- < a, s > + \frac{q}{2}| > \frac{q}{4}$ so $dec_{sk}((a - \frac{q}{2}u_i, \tau)) = 1$

2 .2 Key Dependent Security

Let f be some linear function over the binary field.
similarly to 2.1 lets show that an adversary can produce $enc_{pk}(f(s))$ and thus the encryption is still secure given $enc_{pk}(f(s))$.
Can calculate any linear function with XOR so enough to show that adversary can produce $enc_{pk}(s_i \oplus s_j)$.

We saw that given $enc_{pk}(0) = (a, \tau)$:
$(a - \frac{q}{2}u_i, \tau)$ is an encryption for s_i.

Claim $(a - \frac{q}{2}u_i - \frac{q}{2}u_j, \tau)$ is an encryption of $s_i \oplus s_j$.

$$|\tau - < a - \frac{q}{2}u_i - \frac{q}{2}u_j, s > | = |\tau - < a, s > + \frac{q}{2} < u_i, s > + \frac{q}{2} < u_j, s > |$$

$$= |\tau - < a, s > + \frac{q}{2}s_i + \frac{q}{2}s_j|$$

if $s_i = s_j$ this equals $|\tau - < a, s > |$ so $(a - \frac{q}{2}u_i - \frac{q}{2}u_j, \tau)$ encrypts $0 = s_i \oplus s_j$
else one of s_i, s_j is 1 and the other is 0 so equals $|\tau - < a, s > + \frac{q}{2}|$ which we saw encrypts $1 = s_i \oplus s_j$

3 . ZK for Hamiltonicity

3 .1 Interactive Proof

Denote n as the number of nodes in G.
Denote A as the adjacency matrix of G.
Denote A' as the adjacency matric of G'.
Assume H is a sequence of vertices.

Protocol:

1. P samples $\pi \in_R S_n, \forall k \in [n] : H'_k = \pi(H_k)$
2. P for all $i, j \in [n]$: $A'_{ij} = A'_{\pi(i)\pi(j)}$
   samples $r_{ij} \in_R \{0, 1\}^n$
   sends $c_{ij} = commit(r_{ij}, A'_{ij})$ to V
3. V samples $b \in_R \{0, 1\}$ and sends it to P.
4. P follows:
   if $b = 0$ sends to V : all r_{ij}, A'_{ij}, π
   if $b = 1$ sends to V : H' and the r_{uv}, A'_{uv} that correspond to edges in H'.
5. V checks:
   if $b = 0$, checks that $G' = \pi(G)$, (G' implied by A')
   if $b = 1$, checks that edges in H' exist, i.e. $commit(r_{uv}, 1) = c_{uv}$
   (V accepts if passes checks)

   soundness error: given $G \notin HC$ and for all P^*
   P^* commits to some adjacency matrix for a graph G' with no hamiltonian circle.

P^* has 3 possibilities:
(I) commit to G' not isomorphic to G with some circle H'.
(II) commit to G' isomorphic to G with invalid circle H'.
(III) commit to G' not isomorphic to G with invalid circle H'.
either way $Pr[(P^*, V)(G) = 1] \leq \frac{1}{2}$.

commitment: the prover should protect its own interest - its privacy, thus will prefer perfectly hiding commitment.

3 .2 HVZK

Will show PPT S such that $S(G) \sim View(V)$. $View(V)$ consists of commitments to adjacency matrix of G', b and what P sends in response to b.

S samples $\pi^{(1)} \in_R S_n$ produces $G' = \pi^{(1)}(G)$.
S produces commitments $c^{(1)}_{ij} = commit(r^{(1)}_{ij}, A'_{ij})$
S samples $\pi^{(0)} \in_R S_n$ produces G_d which is a simples circle graph $\pi^{(0)}(1) \rightarrow \ldots \rightarrow \pi^{(0)}(n)$.
S produces commitments $c^{(0)}_{i,i+1} = commit(r^{(0)}_{i,i+1}, 1)$, those are n commits, produce rest of commits $c^{(0)}_{ij} = commit(r^{(0)}_{ij}, 0)$.

S samples $b \in_R \{0, 1\}$
if $b = 1$ S outputs $c = c^{(1)}, b = 1, r^{(1)}, A', \pi^{(1)}$
if $b = 0$ S outputs $c = c^{(0)}, b = 0, H' = \pi^{(0)}(1) \rightarrow \ldots \rightarrow \pi^{(0)}(n)$ and 1's for adjacency matrix entrys.

$View(V) \sim S(G)$:
From perfect hiding of commit $c^{(0)}$ and $c^{(1)}$ matrices distribute the same.
Bit b sampled randomly.
If $b = 1$ S does exactly as P so view distributes the same.
If $b = 0$ verifier sees in either way a circle of random ordered n nodes and commitment verifications for 1's.

3 .3 Malicious Verifier ZK.

V^*'s freedom in the interaction is in sampling b.
claim: S_{V^*} which acts like S from before with the exception of sampling b like V^*, satisfies $S^* \sim View(V^*)$.
$View(V^*)$ given V^* chose $b = 1$ is exactly S^* given S^* chose $b = 1$.
same for $b = 0$.
so because they sample b the same it follows $S^* \sim View(V^*)$.

3 .4 Soundness Error

Suggest a new protocol (P_n, V_n).
P_n interacts with V_n exactly as P interacts with V, just that they repeat the interaction n times.
V_n accepts only if accepted all interactions.
So given $G \notin HC$, $Pr[(P_n, V_n)(G) = 1] = (Pr[(P, V)(G) = 1])^n = 2^{-n} = neg(n)$.
To get soundness error of ϵ : choose n that satisfies

$$2^{-n} = \epsilon$$

. i.e.

$$n = -log_2(\epsilon)$$

In the 3COL ZK protocol we get soundness error of less than $\frac{2}{3}$ so will have to repeat more times to reach the same goal ϵ.

$$n' = -\frac{log_2(\epsilon)}{log_2(3/2)}$$