CSE 40622 Cryptography
Writing Assignment 08
(Section 2.2 in Lecture 10-12 and Lecture 16-18)

Name: Walker Bagley (wbagley)

1. (10 pts, page 2) p, q are the prime numbers that have the same length (i.e., number of bits). Prove that $\gcd(\varphi(n), n) = 1$.

   Answer:

   Proof. Let's prove this by contradiction. We will assume that $\gcd(\varphi(n), n) \neq 1$. Then there exists a common divisor of $\varphi(n)$ and n that is greater than 1. Let b define the number of bits in p, q, so that $n = pq$ has at least $2b$ bits. We know that for $n = pq$, $\varphi(n) = (p-1)(q-1)$. So we can say $\gcd(\varphi(n), n) = \gcd((p-1)(q-1), pq) = \gcd(pq - p - q + 1, pq)$. We also know that $n = pq$ has four possible divisors, namely $1, q, p, pq$ and p, q are distinct primes. So, we examine these four divisors, ruling out pq as it does not divide $p, q, 1$. We can also rule out p and q as they are unique primes and thus cannot divide each other. So, we are left with 1, which divides both $pq - p - q + 1$ and pq, and here lies our contradiction. Therefore, $\gcd(\varphi(n), n) = 1$. □

2. (20 pts, page 11) Suppose someone found a non-integer number before multiplying μ modulo n in the decryption process, and naturally the decryption fails. How can s/he still recover m from the ciphertext? Suppose $m < p$ and $m < q$, and also suppose r is given.

   - Hint: The decryption fails, therefore $\gcd(r, n^2) \neq 1$. *W.l.o.g.,* assume $\gcd(r, n) = p$. Then, try to calculate the following and figure out how you can recover m from the value.

   $$\frac{\Big((c^{q-1} - 1) \mod q^2\Big)}{q} \mod q$$

   Answer:

   Then, s/he realizes that $\gcd(r, n^2) \neq 1$. This happens if and only if $\gcd(r, n) = p$ or $\gcd(r, n) = q$. We are assuming it was $\gcd(r, n) = p$. That means, $\gcd(r, q) = 1$.

   Then, ...

$$\begin{aligned}
&c^{q-1} \mod q^2 \\
=&\Big((1+n)^{m(q-1)} \cdot r^{n(q-1)} \mod n^2\Big) \mod q^2 \\
=&\Big((1+n)^{m(q-1)} \cdot r^{pq(q-1)} \mod n^2\Big) \mod q^2 \\
=&\Big((1+n)^{m(q-1)} \cdot r^{p\varphi(q^2)} \mod n^2\Big) \mod q^2 \\
=&\Big((1+n)^{m(q-1)} \cdot (r^{\varphi(q^2)})^p \mod q^2\Big) \mod n^2 \\
=&\Big((1+n)^{m(q-1)} \cdot (1)^p \mod q^2\Big) \mod n^2 \\
=&\Big((1+n)^{m(q-1)} \mod n^2\Big) \mod q^2 \\
=&(1+n)^{m(q-1)} \mod q^2 \\
=&1 + m(q-1)n \mod q^2 \\
=&1 + mpq^2 - pqm \mod q^2 \\
=&1 - pqm \mod q^2
\end{aligned}$$

$$\begin{aligned}
&\frac{\Big((c^{q-1} - 1) \mod q^2\Big)}{q} \mod q \\
=&\frac{\Big((1 - pqm - 1) \mod q^2\Big)}{q} \mod q \\
=&\frac{\Big(-pqm \mod q^2\Big)}{q} \mod q \\
=&\frac{\Big(-pqm + kq^2\Big)}{q} \mod q \\
=&kq - mp \mod q \\
=&-mp \mod q
\end{aligned}$$

   Then, we can calculate m from $-mp$ by dividing by $-p$.

3. (**Hard**, 50 pts, page 14) Without using the oracle $\mathcal{O}_c$, prove that Paillier cryptosystem is semantically secure if the following holds: For all PPTA $\mathcal{A}$, we have

$$\left| \Pr\left[\mathcal{A} \text{ correctly determines whether } x \text{ is an } n\text{-th residue or not} \middle| x \leftarrow_{\$} \{y^n, y\}, y \in \mathbb{Z}_{n^2}^*\right] - \frac{1}{2} \right| \leq \mathsf{negl}(\kappa)$$

* In other words, DCR problem is intractable in $\mathbb{Z}_{n^2}^*$.

- Essentially, you are asked to conduct the analysis in Section 2.2 in **Lecture 10-12** for Paillier cryptosystem.

Please follow these steps to conduct the proof.

3.1. (15 pts) Suppose you are given an x which came from $x \leftarrow_{\$} \{y^n, y\}$. Describe the simulated eavesdropping game of Paillier cryptosystem that you will use to solve the DCR problem. When you do so, slightly change the steps 3. and 4. in the simulated game in **page 13 of Lecture 15-17** as follows:

- The challenger randomly chooses a bit b and computes $c := g^{m_b} x \mod n^2$ in step 3.
- The adversary does not use $\mathcal{O}_c$.

Then, describe how you would use the revised game to determine whether x is an n-th residue or not. In other words, find a way to answer whether x is an n-th residue or not based on the adversary's response.

Answer:

Simulated eavesdropping game of Paillier cryptosystem (for solving DCR problem).

i. The challenger uses n from the DCR problem and computes $g = 1 + n$. Then the challenger publishes $pk = (n, g)$.
ii. The adversary outputs a pair of messages (m_0, m_1) both of which are drawn from $\mathbb{Z}_n$.
iii. The challenger chooses $b \in \{0, 1\}$ and computes $c := g^{m_b} x \mod n^2$ and publishes c to the adversary.
iv. The adversary gives his guess b' on b.

Upon receiving b', we let the challenger behave as follows for the DCR problem.

- Answer that x is an n-th residue if and only if $b' = b$.
- Answer that x is an n-th nonresidue if and only if $b' \neq b$.

3.2. (20 pts) Present the probability that you will determine that correctly. The probability should have $\mathsf{Adv}_{\mathsf{Pai}}^{\mathcal{A}}$ if you are on the right track.

- Similar to Section 2.2 in **Lecture 10-12**, assume that the best an adversary can do when s/he receives an invalid ciphertext is to make a random guess.

Answer:

- If the given x is an n-th residue, $c = g^{m_b} x \mod n^2$ is a valid ciphertext. Then, the probability the adversary guesses b correctly is $\mathsf{Adv}_{\mathsf{Pai}}^{\mathcal{A}} + \frac{1}{2}$.
- If the given x is an n-th nonresidue, $c = g^{m_b} x \mod n^2$ is not a valid ciphertext. Then, the adversary makes a random guess and thus the probability they are correct is $\frac{1}{2}$.

Then, we have:

$$\begin{aligned} &\Pr[\text{answers whether } x \text{ is an } n\text{-th residue or not correctly}] \\ =&\Pr[\text{answers } x \text{ is an } n\text{-th residue} \wedge x \text{ is an } n\text{-th residue}] \\ &+ \Pr[\text{answers } x \text{ is an } n\text{-th nonresidue} \wedge x \text{ is an } n\text{-th nonresidue}] \\ =&\frac{1}{2}\left(\mathsf{Adv}_{\mathsf{Pai}}^{\mathcal{A}} + \frac{1}{2}\right) + \frac{1}{2}\left(\frac{1}{2}\right) = \frac{1}{2}\mathsf{Adv}_{\mathsf{Pai}}^{\mathcal{A}} + \frac{1}{2} \end{aligned} \tag{1}$$

3.3. (10 pts) Connect the probability to the above inequality to show that $\mathsf{Adv}^{\mathcal{A}}_{\mathsf{Pai}}$ is negligible *w.r.t.* κ.

Answer: We can see that the probability of correctly guessing whether or not x is an n-th residue or not is $\frac{1}{2}\mathsf{Adv}^{\mathcal{A}}_{\mathsf{Pai}} + \frac{1}{2}$, and a random guess at this would be $\frac{1}{2}$. Then the absolute difference in these probabilities would be $\frac{1}{2}\mathsf{Adv}^{\mathcal{A}}_{\mathsf{Pai}}$, which is $\leq \mathsf{negl}(\kappa)$ since the DCR problem is intractable.

3.4. (5 pts) Finally, answer why the above steps prove that Paillier cryptosystem is semantically secure (by connecting to Corollary 1. in Lecture 10-12).

Answer:

Recall that $\mathsf{Adv}^{\mathcal{A}}_{\mathsf{Pai}}$ is defined as

$$\mathsf{Adv}^{\mathcal{A}}_{\mathsf{Pai}} = \left| \Pr\left[b' = b \middle| \mathcal{A}\big(1^{\kappa}, \mathsf{pk}, c \leftarrow \mathsf{Enc}(m_b, \mathsf{pk})\big) = b'\right] - \frac{1}{2} \right|$$

in the eavesdropping game for Paillier cryptosystem.

By Corollary 1 in Lectures 10-12, an encryption scheme is semantically secure against eavesdropping attackers iff the Adv in the eavesdropping game is negligible with respect to the security parameter κ. In part 3.3, we proved that the advantage $\mathsf{Adv}^{\mathcal{A}}_{\mathsf{Pai}}$ is negligible w.r.t. κ and therefore satisfy Corollary 1, so we have shown that the Paillier cryptosystem is semantically secure. This shows that an eavesdropping attacker can do at best negligibly better than a random guess at breaking the DCR problem.