CS151: Midterm

1 Extended Euclidean Algorithm

a.

$$\begin{aligned}\gcd(216, 85) &= \gcd(46, 85) = \gcd(46, 29) = \gcd(17, 29) = \gcd(17, 12) \\ &= \gcd(5, 12) = \gcd(5, 2) = \gcd(1, 2) = 1\end{aligned}$$

b.

$$a = -2197, \quad b = 6133$$

c.

$$7843^{-1} \equiv -2197 \mod 21894$$

because

$$a \cdot 7843 = 1 - b \cdot 21897 \equiv 1 \mod 21894.$$

2 Practice with the Chinese Remainder Theorem

a.

Using the extended Euclidean algorithm, we have

$$\begin{aligned}(33 \cdot 58)^{-1} &\equiv 5 \mod 17 \\ (17 \cdot 58)^{-1} &\equiv 8 \mod 33 \\ (17 \cdot 33)^{-1} &\equiv 3 \mod 58.\end{aligned}$$

b.

We can use the inverses we computed in **part a**. By the Chinese remainder theorem, x can be computed by

$$\begin{aligned}x &\equiv 5 \cdot 5 \cdot (33 \cdot 58) + 28 \cdot 8 \cdot (17 \cdot 58) + 5 \cdot 3 \cdot (17 \cdot 33) \\ &\equiv 181429 \equiv 18736 \mod (17 \cdot 33 \cdot 58)\end{aligned}$$

3 Tricky Bits

We first prove the intermediate step:

$$|P(x_0 \leftarrow QR_N; x_1 \leftarrow -x_0; b \leftarrow \{0,1\}; b' \leftarrow \mathcal{A}(N, x_b) : b = b') - \frac{1}{2}|$$

is negligible under the quadratic residuocity assumption. Given any adversary $\mathcal{A}$, we want to construct an adversary $\mathcal{A}'$ to the quadratic residuocity problem. Consider the following construction:

Challenger

$$N \leftarrow \text{KeyGen}(1^k);\ x_0 \leftarrow QR_N;\ \ x_1 \leftarrow QNR_N;\ b \leftarrow \{0,1\}$$

$\mathcal{A}'(N, x_b)$

$$y_0 \leftarrow x_b;\ y_1 \leftarrow -x_b; d \leftarrow \{0,1\};\ b' \leftarrow \mathcal{A}(N, y_b);$$

and output b'' such that

- if $d = 0$: $b'' = b'$
- if $d = 1$: $b'' = \bar{b}'$

Next we can compute $P(b'' = b)$

$$\begin{aligned} P(b'' = b) = &\frac{1}{4}P(b'' = b|b = 0, d = 0) + \frac{1}{4}P(b'' = b|b = 0, d = 1) \\ &+ \frac{1}{4}P(b'' = b|b = 1, d = 0) + \frac{1}{4}P(b'' = b|b = 1, d = 1). \end{aligned}$$

We compute the four conditional probabilities one by one:

$$\begin{aligned} P(b'' = b|b = 0, d = 0) = P(b'' = 0|b = 0, d = 0) = P(b' = 0|x_0) \\ P(b'' = b|b = 0, d = 1) = P(b'' = 0|b = 0, d = 0) = P(b' = 1| - x_0) \\ P(b'' = b|b = 1, d = 0) = P(b'' = 1|b = 1, d = 0) = P(b' = 1|x_1) \\ P(b'' = b|b = 1, d = 1) = P(b'' = 1|b = 1, d = 1) = P(b' = 0| - x_1). \end{aligned}$$

We also have

$$P(b' = b|x_0) + P(b' = 1| - x_0) = P(b' = 1|x_1) + P(b' = 0| - x_1)$$

for $x_0 \leftarrow QR_N$ and $x_1 \leftarrow QNR_N$ using the fact that $x \mapsto -x$ is a bijection from between QR_N and QNR_N.

Therefore,

$$P(b'' = b) = P(x_0 \leftarrow QR_N; x_1 \leftarrow -x_0; b \leftarrow \{0,1\}; b' \leftarrow \mathcal{A}(N, x_b) : b = b')$$

and by the quadratic residuocity assumption, we know

$$|P(x_0 \leftarrow QR_N; x_1 \leftarrow -x_0; b \leftarrow \{0,1\}; b' \leftarrow \mathcal{A}(N, x_b) : b = b') - \frac{1}{2}|$$

is negligible.

Next we prove the indistinguishablility from the intermediate step. More precisely, given any adversary $\mathcal{A}$ to the problem

$$N \leftarrow \text{KeyGen}(1^k);\ s \leftarrow QR_N;\ b' \leftarrow \mathcal{A}(N, s^2)$$

we want to construct an adversary $\mathcal{A}'$ to our intermediate problem. Consider the following construction:

Challenger

$$N \leftarrow \text{KeyGen}(1^k);\ x_0 \leftarrow QR_N;\ x_1 \leftarrow -x_0;\ b \leftarrow \{0,1\};$$

$\mathcal{A}'(N, x_b)$

$$b' \leftarrow \mathcal{A}(N, x_b^2)$$

and outputs b'' such that

- if $b' = LSB(x_b)$: $b'' = 0$
- if $b' \neq LSB(x_b)$: $b'' = 1$

The advantage of $\mathcal{A}'$ can be computed by

$$\begin{aligned} P(b'' = b) = &\frac{1}{4}P(b'' = b|b = 0, LSB(x_0) = 0) + \frac{1}{4}P(b'' = b|b = 0, LSB(x_0) = 1) \\ &+ \frac{1}{4}P(b'' = b|b = 1, LSB(x_0) = 0) + \frac{1}{4}P(b'' = b|b = 1, LSB(x_0) = 1) \end{aligned}$$

Also, because N is an odd number, we have

$$LSB(x_0) \neq LSB(x_1).$$

The conditional probabilities can be computed by

$$\begin{aligned} P(b'' = b|b = 0, LSB(x_0) = 0) = P(b' = 0|x_0^2, LSB(x_0) = 0) \\ P(b'' = b|b = 0, LSB(x_0) = 1) = P(b' = 1|x_0^2, LSB(x_0) = 1) \\ P(b'' = b|b = 1, LSB(x_0) = 0) = P(b' = 0|x_1^2, LSB(x_0) = 0) \\ P(b'' = b|b = 1, LSB(x_0) = 1) = P(b' = 1|x_1^2, LSB(x_0) = 1) \end{aligned}$$

Using the fact that

$$x_0^2 = x_1^2,$$

we have

$$
\begin{aligned}
&P(b' = 0|x_0^2, LSB(x_0) = 0) + P(b' = 0|x_1^2, LSB(x_0) = 0) \\
&= 2P(b' = LSB(x_0)|x_0^2, LSB(x_0) = 0).
\end{aligned}
$$

and similarly

$$
\begin{aligned}
&P(b' = 1|x_0^2, LSB(x_0) = 1) + P(b' = 1|x_1^2, LSB(x_0) = 1) \\
&= 2P(b' = LSB(x_0)|x_0^2, LSB(x_0) = 1).
\end{aligned}
$$

Combined together, we have

$$
P(b'' = b) = P(b' = LSB(x_0)|x_0^2)
$$

and therefore, the indistinguishability follows from our intermediate step that

$$
|P(b'' = b) - 1/2| \leq \nu(k)
$$

for some negligible ν.

b.

In order to show the two distributions are indistinguishable, we can build an adversary to the quadratic residuocity problem from a distinguisher of the two distributions.

We start by defining the distinguisher for two distributions. Consider the following game:

Challenger

$$
N \leftarrow \text{KeyGen}(1^k);\ x_0 \leftarrow QR_N;\ x_1 \leftarrow \{0,1\};\ b \leftarrow \{0,1\}
$$

and outputs the tuple (N, x_0^2, x_b).

When $b = 0$, the output is from D_0 and when $b = 1$, the output is from D_1.

Distinguisher $\mathcal{A}$

$$
b' \leftarrow \mathcal{A}(N, x_0^2, x_b)
$$

and the advantage of the distinguisher is defined as

$$
Adv(\mathcal{A}) = |P(b' = 0|b = 0) - P(b' = 0|b = 1)|.
$$

We first show

$$
\begin{aligned}
&Adv(\mathcal{A}) \\
&= \frac{1}{4}|P(\mathcal{A}(N, s^2, 0) = 0|LSB(s = 0)) - P(\mathcal{A}(N, s^2, 1) = 0|LSB(s) = 0) \\
&+ P(\mathcal{A}(N, s^2, 1) = 0|LSB(s = 1)) - P(\mathcal{A}(N, s^2, 0) = 0|LSB(s) = 1)|.
\end{aligned}
$$

We denote the right hand side by $Adv^*(\mathcal{A})$. The intuition is that for fixed s, $LSB(s)$ is a fixed bit while the random bit b can take values 0 or 1.

This can be proved by writing $P(b' = 0|b)$ as sum of conditional probabilities:

$$
\begin{aligned}
&P(b' = 0|b = 0) = \frac{1}{2}P(b' = 0|LSB(x_0) = 0) + \frac{1}{2}P(b' = 0|LSB(x_0) = 1) \\
&= \frac{1}{2}P(b' \leftarrow \mathcal{A}(N, x_0^2, 0) : b' = 0|LSB(x_0) = 0) \\
&+ \frac{1}{2}P(b' \leftarrow \mathcal{A}(N, x_0^2, 1) : b' = 0|LSB(x_0) = 1)
\end{aligned}
$$

and

$$
\begin{aligned}
&P(b' = 0|b = 1) \\
&= \frac{1}{4}P(b' = 0|LSB(x_0) = 0, b = 0) + \frac{1}{4}P(b' = 0|LSB(x_0) = 1, b = 0) \\
&+ \frac{1}{4}P(b' = 0|LSB(x_0) = 0, b = 1) + \frac{1}{4}P(b' = 0|LSB(x_0) = 1, b = 1) \\
&= \frac{1}{4}P(b' \leftarrow \mathcal{A}(N, x_0^2, 0) : b' = 0|LSB(x_0) = 0) \\
&+ \frac{1}{4}P(b' \leftarrow \mathcal{A}(N, x_0^2, 1) : b' = 0|LSB(x_0) = 0) \\
&+ \frac{1}{4}P(b' \leftarrow \mathcal{A}(N, x_0^2, 0) : b' = 0|LSB(x_0) = 1) \\
&+ \frac{1}{4}P(b' \leftarrow \mathcal{A}(N, x_0^2, 1) : b' = 0|LSB(x_0) = 1)
\end{aligned}
$$

Taking the difference, we get

$$
Adv(\mathcal{A}) = Adv^*(\mathcal{A}).
$$

Given a distinguisher of the above game, we can construct an adversary to the quadratic residuocity problem by using results from **part a**. More specifically, if we can construct a LSB adversary $\mathcal{A}'$ such that

$$
|P(LSB(s) = \mathcal{A}'(N, s^2)) - \frac{1}{2}| = Adv^*(\mathcal{A}),
$$

we know the advantage of $\mathcal{A}$ is negligible under quadratic residuocity assumption. Consider the following construction:

Challenger

$$
N \leftarrow \text{KeyGen}(1^k);\ s \leftarrow QR_N;
$$

$\mathcal{A}'(N, s^2)$

$$b \leftarrow \{0,1\};\ b' \leftarrow \mathcal{A}(N, s^2, b)$$

and outputs b'' such that

- if $b = 0, b'' = b'$
- if $b = 1, b'' = \overline{b'}$

The probability that $b'' = LSB(s)$ can be computed by

$$\begin{aligned} P(b'' = LSB(s)) = \frac{1}{2}P(b'' = LSB(s)|b = 0) \\ + \frac{1}{2}P(b'' = LSB(s)|b = 1). \end{aligned}$$

Next we compute the conditional probabilities:

$$\begin{aligned} &P(b'' = LSB(s)|b = 0) \\ &= \frac{1}{2}P(b' = 0|b = 0, LSB(s) = 0) + \frac{1}{2}P(b' = 1|b = 0, LSB(s) = 1) \\ &= \frac{1}{2}(P(b' = 0|b = 0, LSB(s) = 0) + 1 - P(b' = 0|b = 0, LSB(s) = 1)) \end{aligned}$$

and

$$\begin{aligned} &P(b'' = LSB(s)|b = 1) \\ &= \frac{1}{2}P(b' = 1|b = 1, LSB(s) = 0) + \frac{1}{2}P(b' = 0|b = 1, LSB(s) = 1) \\ &= \frac{1}{2}(1 - P(b' = 0|b = 1, LSB(s) = 0) + P(b' = 0|b = 1, LSB(s) = 1)). \end{aligned}$$

Combined together, we get exactly what we need:

$$\begin{aligned} &|P(b'' = LSB(s)) - \frac{1}{2}| \\ &= \frac{1}{4}|P(b' = 0|b = 0, LSB(s) = 0) - P(b' = 0|b = 1, LSB(s) = 0) \\ &+ P(b' = 0|b = 1, LSB(s) = 1)) - P(b' = 0|b = 0, LSB(s) = 1))| \\ &= Adv^*(\mathcal{A}). \end{aligned}$$

Therefore, by quadratic residuocity assumption, no ppt adversary can guess the bit $LSB(s)$ which implies $Adv^*(\mathcal{A})$ is negligible.

c.

If the statement from **part b** is true, in each of the iterations, $b_i = LSB(s_{i-1})$ is indistinguishable from a random bit $b \leftarrow \{0,1\}$. Intuitively, the resulting bits

$$R = b_1 b_2 \dots b_L$$

should be indistinguishable from L bits randomly generated from $\{0,1\}^L$.

4 More Fun with One-Way Functions and Pseudorandom Generators

a.

From the definition of a PRG, it has to generate bits that are indistinguishable from a randomly uniform $y \leftarrow \{0,1\}^n$ from a random uniform key k. We can consider the OWF as in the homework:

$$f : \{0,1\}^{2k} \to \{0,1\}^{2k}, \quad f(x_1 \circ x_2) = 0^k \circ f_0(x_2)$$

for any OWF $f_0 : \{0,1\}^k \to \{0,1\}^k$. The generated distribution is obviously distinguishable from the uniform distribution because the first k bits will always be 0.

b.

$f_b = f(G(x))$ is a one-way function. Given any OWF adversary $\mathcal{A}$ to f_b, we construct a PRG adversary $\mathcal{A}'$ to G.

Challenger

$$k \leftarrow \{0,1\}^k;\ x_0 \leftarrow G(k);\ x_1 \leftarrow \{0,1\}^{2k};\ b \leftarrow \{0,1\}$$

$\mathcal{A}'(1^k, x_b)$

$$y \leftarrow f(x_b);\ x' \leftarrow \mathcal{A}(1^k, y)$$

and outputs b':

- if $f(G(x')) = y$: $b' = 0$
- if $f(G(x')) \neq y$: $b' = 1$

Next we try to compute the probability $P(b' = b)$:

$$P(b' = b) = \frac{1}{2}P(b' = 0|b = 0) + \frac{1}{2}P(b' = 1|b = 1)$$

For each of the conditional probability:

$$\begin{aligned} P(b' = 0|b = 0) &= P(\mathcal{A}\ inverts\ f(G(k))) \\ P(b' = 1|b = 1) &= 1 - P(b' = 0|b = 1) \end{aligned}$$

In order to bound the second probability, we notice

$$\begin{aligned} P(b' = 0|b = 1) &= P(f(G(\mathcal{A}(1^k, y))) = y|b = 1) \\ &= P(x_1 \leftarrow \{0,1\}^{2k};\ y \leftarrow f(x_1);\ x_1' \leftarrow G(\mathcal{A}(1^k, y)) : f(x_1) = f(x_1')). \end{aligned}$$

If this probability is not negligible, we will get an adversary to the OWF f that outputs inverse with non-negligible probability. Therefore, we have

$$|P(b' = 1|b = 1) - 1| \leq \nu_1(k)$$

for some negligible ν_1.

Combined together, we have

$$\begin{aligned} |P(b' = b) - \frac{1}{2}| &= \frac{1}{2}|P(\mathcal{A}\ inverts\ f(G(k))) - P(G(\mathcal{A})\ inverts\ f| \\ &\geq \frac{1}{2}(P(\mathcal{A}\ inverts\ f(G(k))) - \nu_1(k)). \end{aligned}$$

By our assumption that G is a PRG, we know the left hand side of the inequality is negligible and therefore

$$P(\mathcal{A}\ inverts\ f(G(k)))$$

is also negligible.

c.

$G_c(x) = G(f(x))$ is not necessarily a PRG because the range of f might not guarantee a uniform distribution over the domain of G. For instance, we can again take f such that

$$f : \{0,1\}^{2k} \to \{0,1\}^{2k};\quad f(x_1 \circ x_2) = 0^k \circ f_0(x_2) \circ 0,$$

where

$$f_0 : \{0,1\}^{k-1} \to \{0,1\}^{k-1}$$

is any length-preserving OWF.

Our PRG G will be the length-doubling Blum PRG constructed as in **Problem 3**:

$$G : \mathbb{Z}_N^* \to \{0,1\}^{4k+2},$$

where $N = pq$ with two $2k+2$-bit primes p and q. We start by showing that

Claim $f(x_1 \circ x_2) \in \mathbb{Z}_N^*$.

This can be shown by directly counting the number of bits. Both p and q are $2k$ -bits while $f(x_1 \circ x_2) \leq 2^{k+1}$. Therefore, none of p, q divides $f(x_1 \circ x_2)$, which proves our statement.

For the Blum PRG, the first step is to take the square $f(x_1 \circ x_2)^2 \bmod N$. Next we show

Claim $f(x_1 \circ x_2)^2 \leq N$.

This follows from the fact that

$$f(x_1 \circ x_2) \leq p, \quad f(x_1 \circ x_2) \leq q.$$

Finally, we conclude that the distribution generated by $G(f(x_1 \circ x_2))$ is distinguishable from the uniform random distribution on $\{0,1\}^{4k+2}$ because

$$LSB(f(x_1 \circ x_2)^2) = 0.$$

This follows from the fact that $f(x_1 \circ x_2)$ is even.