1 Goldwasser-Micali Cryptosystem

The Goldwasser-Micali (GM) Cryptosystem is a public-key encryption algorithm developed in 1982. It is the first probabilistic public-key encryption scheme which is provably secure under standard cryptographic assumptions.

It is based on the intractability of the Quadratic Residuosity Assumption modulo a composite $N$. Very roughly, we select uniformly at random Quadratic Residues from $\mathbb{Z}_N^*$ to encrypt 0 bit and to encrypt 1 bit we select quadratic non-residue from $\mathbb{Z}_N^*$. However, since the distribution of quadratic residues and quadratic non-residues are not same in $\mathbb{Z}_N^*$, we confine ourselves to a subset of $\mathbb{Z}_N^*$ where the number of quadratic residues is equal to the number of quadratic non-residues.

1.1 Quadratic Residues Modulo a Prime

In a group $G$, an element $y \in G$ is a quadratic residue if there exists an $x \in G$ with $x^2 = y$. In this case, we call $x$ a square root of $y$.

**Proposition 1.** Let $p > 2$ be prime. Every quadratic residue in $\mathbb{Z}_p^*$ has exactly 2 square roots.

**Proof.** Let $y \in \mathbb{Z}_p^*$ be a quadratic residue. First we will show that there exist at least 2 square roots for $y$. Let $x \in \mathbb{Z}_p^*$ such that $x^2 = y \mod p$. $(-x)^2 = (x)^2$. Also $-x \neq x \mod p$. (If $x = x \mod p$ then $2x = 0 \mod p$, which implies $p|2x$. Not possible since $p$ is prime). So $y$ has at least 2 square roots.

Now we show that there cannot exist more than 2 distinct square roots. Let $x' \in \mathbb{Z}_p^*$ be a square root of $y$.

\[
x'^2 = x^2 \\
x'^2 - x^2 = 0 \mod p \\
(x - x')(x + x') = 0 \mod p \\
(x - x')(x + x') = 0 \mod p \\
x' = \pm x \mod p \quad \Box
\]

Define function $sq_p : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$ as $sq_p(x) \overset{\text{def}}{=} [x^2 \mod p]$. The above proof shows that $sq_p$ is a two-to-one function when $p > 2$ is prime. That is exactly half the elements of $\mathbb{Z}_p^*$ are
quadratic residues modulo $p$, which can be denoted by $\mathcal{QR}_p$. Let the quadratic non-residues modulo $p$ be denoted by $\mathcal{QNR}_p$.

$$|\mathcal{QR}_p| = |\mathcal{QNR}_p| = \frac{Z_p^*}{2} = \frac{p-1}{2}$$

(1)

1.1.1 Jacobi symbol

Define $\mathcal{J}_p(x)$, the Jacobi symbol of $x$ modulo $p$ as follows.

$$\mathcal{J}_p(x) = \begin{cases} +1 & \text{if } x \in \mathcal{QR}_p \\ -1 & \text{if } x \notin \mathcal{QR}_p. \end{cases}$$

(2)

where $p > 2$ is prime and $x \in Z_p^*$

1.1.2 Characterizing quadratic residues in $Z_p^*$

Let $g$ be generator of $Z_p^*$. Order of $g$ is clearly $(p-1)$.

$$Z_p^* = \{g^0, g^1, \ldots, g^{\frac{p-1}{2}-1}, g^{\frac{p-1}{2}}, g^{\frac{p-1}{2}+1}, \ldots, g^{p-2}\}$$

Squaring and taking modulo $p$ in the exponent,

$$\mathcal{QR}_p^* = \{g^0, g^2, g^4, \ldots, g^{p-3}, g^0, g^2, g^4, \ldots, g^{p-3}\}$$

This shows that quadratic residues are exactly those elements which can be written of the form $g^i$ where $i$ is even. This leads to Proposition 2 which gives us a simple way to compute the Jacobi symbol.

**Proposition 2.** Let $p > 2$ be a prime. Then $\mathcal{J}_p(x) = x^{\frac{p-1}{2}} \mod p$.

**Proof.** We will consider the following two cases. Let $g$ be a generator

- $x \in \mathcal{QR}_p \Rightarrow \mathcal{J}_p(x) = +1$

  $$x^{\frac{p-1}{2}} = (g^{2j})^{\frac{p-1}{2}} = g^{(p-1)j} = (g^{p-1})^j = 1^j = 1 \mod p$$

- $x \in \mathcal{QNR}_p \Rightarrow \mathcal{J}_p(x) = -1$

  $$x^{\frac{p-1}{2}} = (g^{2j+1})^{\frac{p-1}{2}} = (g^{2j})^{\frac{p-1}{2}} \cdot g^{\frac{p-1}{2}} = 1 \cdot g^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} \mod p$$

Now,

$$\left( g^{\frac{p-1}{2}} \right)^2 = g^{p-1} = 1 \mod p$$

Therefore square root of $g^{p-1} = \pm 1 \mod p$. That is $g^{\frac{p-1}{2}} = \pm 1 \mod p$. Since $g$ is a generator, it has order $p-1$ and so $g^{\frac{p-1}{2}} \neq 1 \mod p$. Hence, $x^{\frac{p-1}{2}} = -1 = \mathcal{J}_p(x) \mod p$
Proposition 2 directly gives a polynomial-time algorithm for testing whether an element \( x \in \mathbb{Z}_p^* \) is a quadratic residue.

**Algorithm 1: Deciding quadratic residuosity modulo a prime**

<table>
<thead>
<tr>
<th>Data: A prime ( p ); an element ( x \in \mathbb{Z}_p^* )</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Result:</strong> ( J_p(x) ) (or, equivalently, whether ( x ) is a quadratic residue or quadratic non-residue)</td>
</tr>
<tr>
<td>( b := \left[ x^{\frac{p-1}{2}} \mod p \right] )</td>
</tr>
<tr>
<td>if ( b = 1 ) then</td>
</tr>
<tr>
<td>return ”Quadratic Residue”;</td>
</tr>
<tr>
<td>else</td>
</tr>
<tr>
<td>return ”Quadratic Non-Residue”;</td>
</tr>
<tr>
<td>end</td>
</tr>
</tbody>
</table>

Now we look at some of the multiplicative properties of quadratic residues and quadratic non-residues modulo \( p \).

**Proposition 3.** Let \( p > 2 \) be a prime, and \( x, y \in \mathbb{Z}_p^* \). Then

\[
J_p(xy) = J_p(x) \cdot J_p(y)
\]

**Proof.** Using Proposition 2

\[
J_p(xy) = (xy)^{\frac{p-1}{2}} = (x)^{\frac{p-1}{2}} \cdot (y)^{\frac{p-1}{2}} = J_p(x) \cdot J_p(y) \mod p
\]

**Corollary 4.** Let \( p > 2 \) be prime, and say \( x, x' \in \mathbb{QR}_p \) and \( y, y' \in \mathbb{QNR}_p \). Then:
1. \( [xx' \mod p] \in \mathbb{QR}_p \)
2. \( [yy' \mod p] \in \mathbb{QR}_p \)
3. \( [xy \mod p] \in \mathbb{QNR}_p \)

To conclude, if we take any element from \( \mathbb{Z}_p^* \), we can easily characterize if it is a quadratic residue or not using Algorithm 1. So \( \mathbb{Z}_p^* \) cannot be used directly in the encryption scheme.

### 1.2 Quadratic Residues Modulo a Composite

Consider \( \mathbb{Z}_N^* \) where \( N = pq \). We will see the properties of quadratic residues and see how they can be used in an encryption scheme. To characterize the quadratic residues modulo \( N \), we need the Chinese Remainder Theorem along with previous propositions.
Theorem 5. Chinese Remainder Theorem
Let \( p, q \) be coprime. Then the system of equations

\[
\begin{align*}
    y &= y_p \mod p \\
    y &= y_q \mod q
\end{align*}
\]

has a unique solution for \( y \) modulo \( pq \).

In other words, Chinese Remainder Theorem says \( \mathbb{Z}_N^* \simeq \mathbb{Z}_q^* \times \mathbb{Z}_p^* \), and we let \( y \leftrightarrow (y_p, y_q) \) denote the correspondence guaranteed by the theorem.

1.2.1 Characterizing Quadratic Residues Modulo a Composite

Proposition 6. Let \( N = pq \) with \( p, q \) distinct primes, and \( y \in \mathbb{Z}_N^* \) with \( y \leftrightarrow (y_p, y_q) \). Then \( y \) is a quadratic residue modulo \( N \) if and only if \( y_p \) is a quadratic residue modulo \( p \) and \( y_q \) is a quadratic residue modulo \( q \).

Proof. If \( y \) is a quadratic residue modulo \( N \) then, by definition, there exists an \( x \in \mathbb{Z}_N \) such that \( x^2 = y \mod N \). Let \( x \leftrightarrow (x_p, x_q) \). Then

\[
(y_p, y_q) \leftrightarrow y = x^2 \leftrightarrow (x_p, x_q)^2 = ([x_p^2 \mod p], [x_q^2 \mod p])
\]

where \((x_p, x_q)^2\) is simply the square of the element \((x_p, x_q)\) in the group \( \mathbb{Z}_p^* \times \mathbb{Z}_q^* \). We have thus shown that

\[
y_p = x_p^2 \mod p \quad \text{and} \quad y_q = x_q^2 \mod q
\]

and \( y_p, y_q \) are quadratic residues (with respect to the appropriate moduli).

The converse can be proved by reversing the arguments (since all are equality and 1-1 correspondence).

Observation 7. Each quadratic residue \( y \in \mathbb{Z}_N^* \) has exactly four square roots.

Let \( y \leftrightarrow (y_p, y_q) \) be a quadratic residue modulo \( N \) and let \( x_p, x_q \) be square roots of \( y_p, y_q \) modulo \( p \) and \( q \), respectively. Then the four square roots of \( y \) are given by the elements in \( \mathbb{Z}_N^* \) corresponding to

\[
(x_p, x_q), \quad (-x_p, x_q), \quad (x_p, -x_q), \quad (-x_p, -x_q)
\]

The Chinese Remainder Theorem ensures that all 4 are unique square roots.

Let \( Q\mathcal{R}_N \) denote the set of Quadratic residues modulo \( N \)

\[
\frac{|Q\mathcal{R}_N|}{|\mathbb{Z}_N^*|} = \frac{|Q\mathcal{R}_p| \cdot |Q\mathcal{R}_q|}{|\mathbb{Z}_N^*|} = \frac{p^{-1} \cdot q^{-1}}{(p-1)(q-1)} = \frac{1}{4}
\]

The second equality holds from Proposition 2. This means exactly \( 1/4 \) of the elements in \( \mathbb{Z}_N^* \) are quadratic residues.

Figure 1 shows the structure of \( \mathbb{Z}_p^* \) and \( \mathbb{Z}_N^* \).
1.2.2 Jacobi Symbol for a Composite

For any \( x \) relatively prime to \( N = pq \),

\[
\mathcal{J}_N(x) \overset{\text{def}}{=} \mathcal{J}_p(x) \cdot \mathcal{J}_q(x) \\
= \mathcal{J}_p([x \mod p]) \cdot \mathcal{J}_q([x \mod q]).
\]

\[
\mathcal{J}^+_N = \text{Set of elements in } \mathbb{Z}_N^* \text{ having Jacobi symbol } +1 \\
\mathcal{J}^-_N = \text{Set of elements in } \mathbb{Z}_N^* \text{ having Jacobi symbol } -1
\]

From Proposition 6 and definition of Jacobi symbol, it follows that \( x \) is a quadratic residue modulo \( N \) iff \( \mathcal{J}_p(x) = \mathcal{J}_q(x) = +1 \). Thus,

\[
\text{If } x \text{ is a quadratic residue modulo } N, \text{ then } \mathcal{J}_N(x) = +1 \quad (6)
\]

However, \( \mathcal{J}_N(x) = +1 \) can also occur when \( \mathcal{J}_p(x) = \mathcal{J}_q(x) = -1 \). That is, when both \([x \mod p]\) and \([x \mod q]\) are not quadratic residues modulo \( p \) and \( q \) (and so \( x \) is not a quadratic residue modulo \( N \)).

Thus we have found a subset of \( \mathbb{Z}_N^* \) which has both quadratic residues and quadratic non-residues. This can be useful for the Goldwasser-Micali encryption scheme. So we introduce notation \( QN^+_N \)

\[
QN^+_N := \{ x \in \mathbb{Z}_N^* | x \text{ is not a quadratic residue modulo } N, \text{ but } \mathcal{J}_N(x) = +1 \}
\]

**Proposition 8.** Let \( N = pq \) with \( p, q \) distinct odd primes. Then:

1. Exactly half the elements of \( \mathbb{Z}_N^* \) are in \( \mathcal{J}^+_N \)
2. \( QR_N \) is contained in \( \mathcal{J}^+_N \)
3. Exactly half the elements of $J_N^{+1}$ are in $QR_N$ (the other half are in $QNR_N^{+1}$)

Proof. We will consider each case separately

1. We know that $J_N(x) = +1$ if either $J_p(x) = J_q(x) = +1$ or $J_p(x) = J_q(x) = -1$.

Also, from [Quadratic Residues Modulo a Prime] we know that exactly half the elements of $Z_p^*$ have Jacobi symbol $+1$, and half have Jacobi Symbol $-1$. Thus

$$|J_N^{+1}| = |J_p^{+1} \times J_q^{+1}| + |J_p^{-1} \times J_q^{-1}|$$

$$= |J_p^{+1}| \cdot |J_q^{+1}| + |J_p^{-1}| \cdot |J_q^{-1}|$$

$$= \frac{(p-1)(q-1)}{2} + \frac{(p-1)(q-1)}{2}$$

$$= \frac{\varphi(N)}{2}$$

$$= \frac{|Z_N^*|}{2}.$$ 

So $|J_N^{+1}| = |Z_N^*|/2$.

2. We have already noted (6) that all quadratic residues modulo $N$ have Jacobi symbol $+1$, showing that $QR_N \subseteq J_N^{+1}$.

3. From Proposition 6, $x \in QR_N$ if and only if $J_p(x) = J_q(x) = +1$. Therefore

$$|QR_N| = |J_p^{+1} \times J_q^{+1}| = \frac{(p-1)(q-1)}{2} = \frac{|Z_N^*|}{4}.$$ 

So $|QR_N| = |J_N^{+1}|/2$.

This proves that half the elements of $J_N^{+1}$ are in $QR_N$.

\[ \square \]

**Proposition 9.** Let $N = pq$ be a product of distinct, odd primes, and $x, y \in Z_N^*$. Then

$$J_N(xy) = J_N(x) \cdot J_N(y).$$

**Proof.** Using definition of $J_N(\cdot)$ and Proposition 3:

$$J_N(xy) = J_p(xy) \cdot J_q(xy)$$

$$= J_p(x) \cdot J_p(y) \cdot J_q(x) \cdot J_q(y)$$

$$= J_p(x) \cdot J_q(x) \cdot J_p(y) \cdot J_q(y)$$

$$= J_N(x) \cdot J_N(y).$$

\[ \square \]

**Corollary 10.** Let $N = pq$ be a product of distinct, odd primes, and say $x, x' \in QR_N$ and $y, y' \in QNR_N^{+1}$. Then:


1. \([xx' \mod N] \in \mathcal{QR}_N\).

2. \([yy' \mod N] \in \mathcal{QR}_N\).

3. \([xy \mod N] \in \mathcal{QR}_N^{+1}\). (Note the +1 in superscript)

Proof. Proof of 3. Other parts are similar

Since \(x \in \mathcal{QR}_N\), we have \(J_p(x) = J_q(x) = +1\).

Since \(y \in \mathcal{QR}_N\), we have \(J_p(y) = J_q(y) = -1\).

Using Proposition 9

\[
\begin{align*}
J_p(xy) &= J_p(x) \cdot J_p(y) = -1 \\
J_q(xy) &= J_q(x) \cdot J_q(y) = -1
\end{align*}
\]

So \(J_N(xy) = +1\). But \(xy\) is not a quadratic residue modulo \(N\), since \(J_p(xy) = -1\). Thus we conclude that \(xy \in \mathcal{QR}_N^{+1}\) \hfill \(\square\)

So we have found a subset \(\mathcal{J}_N^{+1} \subset \mathbb{Z}_N^*\) that has equal number of quadratic residues and quadratic non-residues. We can now use this to form the Quadratic Residuosity Assumption which will lead to the encryption scheme.

To kickstart the discussion towards the encryption, we see that the properties learned so far leads to an algorithm which can distinguish between a \(\mathcal{QR}_N\) element and \(\mathcal{QR}_N^{+1}\) element from \(\mathbb{Z}_N^*\). The catch here is that the algorithm requires the knowledge of factorization of \(N\). But even if the factorization is unknown, we don’t have a guarantee that distinguishing between a \(\mathcal{QR}_N\) element and a \(\mathcal{QR}_N^{+1}\) element is a hard problem. What we have is an assumption which states the hardness of this quadratic residuosity.

It is interesting to note that there exists polynomial time algorithms which can compute \(J_N(e)\) where \(e \in \mathbb{Z}_N^*\) without knowing the factorization. This is also another reason why we confine ourselves to the quarters \(\mathcal{QR}_N\) and \(\mathcal{QR}_N^{+1}\) for representing the bit in Figure [Figure]

Before we get into the Quadratic Residuosity Assumption, let’s assume \textit{GenModulus} is a PPT algorithm which takes \(1^n\) as input and outputs \((N, p, q)\) where \(p\) and \(q\) are \(n\)-bit primes and \(N = pq\), except with probability negligible in \(n\).

\textbf{Definition 1} We say ”Deciding quadratic residuosity is hard relative to \textit{GenModulus}” if for all probabilistic polynomial-time algorithms \(D\) there exists a negligible function \(\text{negl}(n)\) such that

\[
| \Pr[D(N, qr) = 1] - \Pr[D(N, qnr) = 1] | \leq \text{negl}(n)
\]

where in each case the probabilities are taken over the experiment in which \textit{GenModulus}(\(1^n\)) is run to give \((N, p, q)\), \(qr\) is chosen uniformly from \(\mathcal{QR}_N\), and \(qnr\) is chosen uniformly from \(\mathcal{QR}_N^{+1}\). \(\diamond\)
Algorithm 2: Deciding Quadratic Residuosity modulo N with Known Factorization

**Data:** N, p, q, an element \( x \in \mathbb{Z}_N^\ast \)  
**Result:** whether \( x \in \mathbb{Q}R_N \)  

Compute \( J_p(x), J_q(x) \);  
if \( J_p(x) = J_q(x) = +1 \) then  
  return "Quadratic Residue";  
else  
  return "Quadratic Non-Residue";  
end

1.3 Quadratic Residuosity Assumption

The Quadratic Residuosity Assumption is the following: There exists a \( \text{GenModulus} \) relative to which deciding quadratic residuosity is hard.

Please note that this assumption implies the hardness of factorization with respect to \( \text{GenModulus} \) because, with factors of N we can distinguish with probability 1, using the above algorithm. Now we have to make sure sender can choose a random quadratic residue/a random quadratic non-residue (only from \( \mathbb{Q}N^{\ast +1} \)), without knowing the factorization.

1.4 Goldwasser-Micali Encryption Scheme

As of now, the composite number N is the only public information, and p,q are private information. We are sure about receiver having sufficient information for decryption, using the above algorithm. Now we have to make sure sender can choose a random quadratic residue/a random quadratic non-residue (only from \( \mathbb{Q}N^{\ast +1} \)), without knowing the factorization.

1.4.1 How to choose a random \( QR_N \) element

By definition of \( QR_N \), it is the collection of the squares within \( \mathbb{Z}_N^\ast \). So let’s look in that way. Let’s choose a random element \( x \in \mathbb{Z}_N^\ast \) and let \( y := x^2 \mod N \).

**Claim 11.** \( y \) will be a random quadratic residue.

**Proof.** Let’s look at the probability of \( y \) being an arbitrary element in \( QR_N \) space. If it is \( 1/|QR_N| \) then it is random. Let \( \bar{y} \) be that arbitrary element.

\[
\Pr[y = \bar{y}] = \Pr[x \text{ is a square root of } \bar{y}] \\
= \Pr[x \in \{ \pm x, \pm x' \}] \\
= \frac{4}{|QR_N|} \\
= \frac{1}{|\mathbb{Z}_N^\ast|}
\]
1.4.2 How to choose a random $\mathbb{QR}_N^{+1}$ element

It is not known how to choose a random element from $\mathbb{QR}_N^{+1}$ without knowing factorization. So we need receiver to reveal something more, rather than just $N$ as public key. Let’s assume $z \in \mathbb{QR}_N^{+1}$ be a random element chosen by the receiver and reveal it along with $N$, as public key. It is clear to see that receiver can choose $z$, as 1 in every 4 $\mathbb{Z}_N^*$ element (in expectation) will be from $\mathbb{QR}_N^{+1}$, and receiver can check it by verifying whether both Jacobian values with respect to $p$ and $q$ are -1.

With this arrangement, sender chooses a random element $x \in \mathbb{Z}_N^*$. Now let $y := z \cdot x^2 \mod N$. We have already shown that $x^2 \mod N$ will be a random element from $\mathbb{QR}_N$. So $y$ will be a random element from $\mathbb{QR}_N^{+1}$, from the corollary 10.

1.5 Goldwasser-Micali Scheme: The Construction

Now we understood that with the composite number $N$ and a pre-chosen random $\mathbb{QR}_N^{+1}$ element $z$, any sender can send a random $\mathbb{QR}_N$ element or $\mathbb{QR}_N^{+1}$ element to represent a bit. This encryption scheme can be (and should be) done without the knowledge of factorization. Receiver on the other end, can distinguish the element with the help of factorization. The Quadratic Residuosity Assumption, which blocks any adversary to distinguish between a $\mathbb{QR}_N$ element and $\mathbb{QR}_N^{+1}$ element without knowing factorization, completes the puzzle.

1.5.1 Generator Algorithm (Gen)

We assume we have a $\text{GenModulus}$ which holds the Quadratic Residuosity Assumption.

<table>
<thead>
<tr>
<th>Algorithm 3: Gen</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data:</strong> $1^n$</td>
</tr>
<tr>
<td><strong>Result:</strong> $N$, $p$, $q$, $z$</td>
</tr>
<tr>
<td>$(N,p,q) := \text{GenModulus}(1^n)$ ;</td>
</tr>
<tr>
<td>Choose a random $z$ in $\mathbb{QR}_N^{+1}$ ;</td>
</tr>
<tr>
<td>(We can sample from $\mathbb{Z}_N^*$ and use the algorithm 2 to reject or accept till we get an element from $\mathbb{QR}_N^{+1}$ )</td>
</tr>
</tbody>
</table>

Now we will have the following setting:

- **PubK**: $N, z$
- **PrivK**: $p, q$
1.5.2 Encryption Algorithm (Enc)

We encrypt 0 to a $\mathcal{QR}_N$ element, and 1 to a $\mathcal{QNR}_N^{+1}$ element. We have access to public information, and also provided with a one bit message $m$.

<table>
<thead>
<tr>
<th>Algorithm 4: Enc</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data</strong>: $N$, $z$, $m \in {0, 1}$</td>
</tr>
<tr>
<td><strong>Result</strong>: whether $x \in \mathcal{QR}_N$</td>
</tr>
<tr>
<td>Choose a random element $x \in \mathbb{Z}_N^*$;</td>
</tr>
<tr>
<td>$y := x^2 \mod N$;</td>
</tr>
<tr>
<td>$c := z^m \cdot y \mod N$;</td>
</tr>
<tr>
<td>return $c$;</td>
</tr>
</tbody>
</table>

1.5.3 Decryption Algorithm (Dec)

We don’t need a separate algorithm for Decryption. At the receiver end, he knows the private key $p,q$ and he can use the [algorithm 2] to know the ciphertext $c$ belongs to $\mathcal{QR}_N$ or $\mathcal{QNR}_N^{+1}$. So if the algorithm outputs $\mathcal{QR}_N$, the message bit $m$ is 0. Otherwise it’s 1.

1.6 CPA Security

Here we will show that Goldwasser-Micali Encryption scheme has indistinguishable encryptions in the presence of an eavesdropper. This implies CPA security of the same. (Refer: Proposition 11.3 of [1])

We are going to prove it by reduction. We first define $\Pi$ as our Goldwasser-Micali encryption scheme. Let’s assume we have an adversary for $\mathcal{A}$ for $\Pi$. That is, with a non-negligible probability greater than half, $\mathcal{A}$ can distinguish the encryptions of two different messages in the CPA Experiment (As it is CPA Game, $\mathcal{A}$ has access to Encryption Oracle Service). Mathematically, for some polynomial $p(n)$,

$$\Pr[\text{PubK}_{\mathcal{A,II}}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$$

We now try to create an adversary $\mathcal{D}$ for deciding quadratic residuosity (i.e. to distinguish a $\mathcal{QR}_N$ element and a $\mathcal{QNR}_N^{+1}$ element). Let’s design $\mathcal{D}$ as follows.
The Game is exactly $\Pi$ if the $z$ chosen by Challenger of Quadratic Residuosity game $Ch_{QR}$ is a $QR_N^{+1}$ element. In that case, $D$ outputs 1 with same probability that $A$ wins in game $\Pi$. To start analysing the distinguishability of $D$, we have to look at the probability that $D$ outputs 1, when $z$ is from $QR_N$. This is same as the probability of success of $A$ if $z$ is a random $QR_N$ element.

Let’s call this experiment as $\Pi$. We know that both $x^2$ and $z$ are random $QR_N$ elements. From corollary 10, we know that their product will also be a random $QR_N$ element. So $A$ will be getting a random $QR_N$ element irrespective of the bit $b$ chosen. This implies the probability that $A$ succeeds is exactly $\frac{1}{2}$ in $\Pi$. Therefore, the probability of success of $D$ is also $\frac{1}{2}$ in $\Pi$.

$$\Pr[D(N, qr) = 1] - \Pr[D(N, qnr) = 1] = \Pr[PubK_{\mathcal{A},\Pi}(n) = 1] - \Pr[PubK_{\mathcal{A},\Pi}(n) = 1]$$

$$\geq \left(\frac{1}{2} + \frac{1}{p(n)}\right) - \left(\frac{1}{2}\right)$$

$$= \frac{1}{p(n)}$$

We succeeded to design a distinguisher $D$ using $A$ which can distinguish between a random $QR_N$ and $QR_N^{+1}$ element with significantly greater probability than half. This contradicts with the Quadratic Residuosity Assumption. So there does not exist any adversary for distinguishing encryptions of Goldwasser-Micali scheme with significantly greater than half probability of success. This completes the proof of CPA security.
References