1 QIP

In this section, we prove that QIP is at least as hard as QR (quadratic residuosity); one way to prove this is to reduce QR to QIP; technically speaking, in doing that we might face the following subproblem: prove that the two distributions below are identical or evaluate/discuss their statistical/computational difference.

Let \( s \leftarrow S \) denote the random process of uniformly and independently choosing an element \( s \) from the set \( S \). Let \( z \leftarrow A(x, y, \ldots) \) denote the output \( z \) of an algorithm \( A \) with input \( (x, y, \ldots) \). Given a security parameter \( m \), let \( BW(1^m) \) denote the set of \( m \)-bit primes \( p \) such that \( p = 3 \mod 4 \). For a positive integer \( n > 1 \), let \( Z\mathbb{Z}^* \) denote the set of positive integers which are less than and coprime to \( n \). Let \( QR \) denote the set of quadratic residues modulo \( n \) and let \( Z_{n-1}^+ \) (resp. \( Z_{n-1}^- \)) be the elements of \( Z\mathbb{Z}^* \) which have Jacobi symbol equal to \( +1 \) (resp. \( -1 \)).

Quadratic Residuosity Problem (QRP). The QRP problem consists of efficiently distinguishing the following two distributions:

\[
E_0(1^m) = \{ p, q \leftarrow BW(1^m); n \leftarrow p \cdot q; \\
\quad s \leftarrow Z_{n^{-1}}^+ \cup QR(n) : (n, s) \}
\]
\[
= \{ p, q \leftarrow BW(1^m); n \leftarrow p \cdot q; \\
\quad s \leftarrow CS(n, s \in Z_{n^{-1}}^+ \cup QR(n)) : (n, s) \}
\]
\[
E_1(1^m) = \{ p, q \leftarrow BW(1^m); n \leftarrow p \cdot q; \\
\quad s \leftarrow Z_{n}^* : (n, s) \}
\]
\[
= \{ p, q \leftarrow BW(1^m); n \leftarrow p \cdot q; \\
\quad s \leftarrow CS(n, s \in Z_{n}^*) : (n, s) \}.
\]

We say that algorithm \( A \) has advantage \( \epsilon \) in solving QRP if we have that:

\[
| \Pr[(n, s) \leftarrow E_0(1^m) : A(n, s) = 1] \\
- \Pr[(n, s) \leftarrow E_1(1^m) : A(n, s) = 1] | = \epsilon.
\] (1)

We say that QRP is intractable if all polynomial time (in \( m \)) algorithms have a negligible (in \( m \)) advantage in solving QRP.
Quadratic Indistinguishability Problem (QIP). The QIP problem consists of efficiently distinguishing the following two distributions:

\[ D_0(1^m) = \{ p, q \leftarrow \text{BW}(1^m); n \leftarrow p \cdot q; h \leftarrow \mathbb{Z}_n^+; \\
\quad s \leftarrow \text{CS}(n, s^2 - 4h \in \mathbb{Z}_n^{-1} \cup QR(n)) : (n, h, s) \} \]

\[ D_1(1^m) = \{ p, q \leftarrow \text{BW}(1^m); n \leftarrow p \cdot q; h \leftarrow \mathbb{Z}_n^+; \\
\quad s \leftarrow \mathbb{Z}_n^* : (n, h, s) \} \]

\[ = \{ p, q \leftarrow \text{BW}(1^m); n \leftarrow p \cdot q; h \leftarrow \mathbb{Z}_n^+; \\
\quad s \leftarrow \text{CS}(n, s \in \mathbb{Z}_n^*) : (n, h, s) \}. \]

We say that algorithm \( A \) has advantage \( \epsilon \) in solving QIP if we have that:

\[ | \Pr[(n, h, s) \leftarrow D_0(1^m) : A(n, h, s) = 1] - \Pr[(n, h, s) \leftarrow D_1(1^m) : A(n, h, s) = 1]| = \epsilon. \quad (2) \]

We say that QIP is intractable if all polynomial time (in \( m \)) algorithms have a negligible (in \( m \)) advantage in solving QIP.

Before proving the equivalence of QRP and QIP, we prove the equivalence of QIP and QIP\(_0\).

QIP\(_0\) Problem. The QIP\(_0\) problem consists of efficiently distinguishing the following two distributions:

\[ D_{0,0}(1^m) = \{ p, q \leftarrow \text{BW}(1^m); n \leftarrow p \cdot q; h \leftarrow \mathbb{Z}_n^+; \\
\quad s \leftarrow \text{CS}(n, s^2 - 4h \in \mathbb{Z}_n^{-1} \cup QR(n)) : (n, h, s) \} \]

\[ D_{0,1}(1^m) = \{ p, q \leftarrow \text{BW}(1^m); n \leftarrow p \cdot q; h \leftarrow \mathbb{Z}_n^+; \\
\quad s \leftarrow \text{CS}(n, s \in \mathbb{Z}_n^*) : (n, h, s) \}. \]

Recall that given a finite set \( C \) and any two subsets \( A \) and \( B \), we have

\[ |A \cup B| \leq |C| \quad \text{and} \quad |A \cap B| \geq |A| + |B| - |C| \]

so that

\[ |A \Delta B| = |A \cup B| - |A \cap B| \leq |C| - (|A| + |B| - |C|) = 2|C| - |A| - |B|. \quad (3) \]

Since addition by a non-zero element is a 1-1 map on \( \mathbb{Z}_n \), we have

\[ |4h + \mathbb{Z}_n^*| = |\mathbb{Z}_n^*| = (p - 1)(q - 1) \]

so that, by Equation 3,

\[ |4h + \mathbb{Z}_n^* \Delta \mathbb{Z}_n^*| \leq 2pq - (p - 1)(q - 1) - (p - 1)(q - 1) = 2(p + q - 1). \]
Thus the advantage of an adversary distinguishing the two distributions

\[
D'_1(1^m) = \{ p, q \gets BW(1^m); n \gets p \cdot q; h \gets Z_n^{+1}; \\
    s \gets CS(n, s \in Z_n^*) : (n, h, s) \}
\]

\[
D'_{0,1}(1^m) = \{ p, q \gets BW(1^m); n \gets p \cdot q; h \gets Z_n^{+1}; \\
    s \gets CS(n, s \in 4h + Z_n^*) : (n, h, s) \}
\]

is at most

\[
\frac{2(p + q - 1)}{(p - 1)(q - 1)}. \tag{4}
\]

In particular, the advantage of an adversary distinguishing the two distributions

\[
D''_1(1^m) = \{ p, q \gets BW(1^m); n \gets p \cdot q; h \gets Z_n^{+1}; \\
    s \gets CS(n, s^2 \in Z_n^*) : (n, h, s) \}
\]

\[
D''_{0,1}(1^m) = \{ p, q \gets BW(1^m); n \gets p \cdot q; h \gets Z_n^{+1}; \\
    s \gets CS(n, s^2 \in 4h + Z_n^*) : (n, h, s) \}
\]

is at most

\[
4 \cdot \frac{2(p + q - 1)}{(p - 1)(q - 1)/4} = \frac{8(p + q - 1)}{(p - 1)(q - 1)}. \tag{5}
\]

Now,

\[s^2 - 4h \in Z_n^* \iff s^2 \in 4h + Z_n^* \quad \text{and} \quad s \in Z_n^* \iff s^2 \in Z_n^*\]

so that the advantage of an adversary distinguishing the two distributions

\[
D_1(1^m) = \{ p, q \gets BW(1^m); n \gets p \cdot q; h \gets Z_n^{+1}; \\
    s \gets CS(n, s \in Z_n^*) : (n, h, s) \}
\]

\[
D_{0,1}(1^m) = \{ p, q \gets BW(1^m); n \gets p \cdot q; h \gets Z_n^{+1}; \\
    s \gets CS(n, s^2 - 4h \in Z_n^*) : (n, h, s) \}
\]

is at most

\[
\frac{8(p + q - 1)}{(p - 1)(q - 1)}. \tag{6}
\]

Hence \(D_{0,1}(1^m)\) and \(D_1(1^m)\) are indistinguishable and the problems QIP and QIP\(_0\) are equivalent (since \(D_{0,0}(1^m)\) and \(D_0(1^m)\) are the same distribution).

So, to prove the equivalence of QRP and QIP, we only need to prove the equivalence of QRP and QIP\(_0\). Given a distinguisher \(A\) for QIP\(_0\), which takes as input \((n, h, s)\) where \(n\) is a Blum-Williams integer, \(h \gets Z_n^{+1}\) and \(s \in Z_n^*\), and outputs a bit \(b\) indicating \((n, h, s)\) is from the distribution \(D_{0,b}(1^m)\), we simulate a distinguisher \(B\) for QRP, which takes as input \((n, s)\) where \(n\) is a Blum-Williams integer and \(s \in Z_n^*\), and outputs a bit \(b\) indicating \((n, s)\) is from the distribution \(E_b(1^m)\) as follows

1. \(B\) randomly chooses \(\sigma \gets Z_n^*\) and sets \(h = \sigma^{s^2} - s^2\).
Since $s = \sigma^2 - 4h$, $(n, h, \sigma) \leftarrow D_{0,0}(1^m)$ implies that

if $b = 0$, $\sigma \leftarrow \text{CS}(n, s \in Z_n^{-1} \cup QR(n))$;
else if $b = 1$, $\sigma \leftarrow \text{CS}(n, s \in Z_n^{+1})$.

Thus $\mathcal{B}$ is correct whenever $\mathcal{A}$ is. Hence QIP$_0$ is equivalent to QRP.

QIP$_1$ Problem. We define the QIP$_1$ problem as the problem of efficiently distinguishing the following two distributions:

\begin{align*}
D_{1,0}(1^m) &= \{p, q \leftarrow \text{BW}(1^m); n \leftarrow p \cdot q; d \leftarrow \{0,1\}; h_0, h_1 \leftarrow Z_n^{+1}; \\
&\quad s \leftarrow \text{CS}(n, s^2 - 4h_d \in Z_n^{-1} \cup QR(n)) : (n, h_0, h_1, s)\} \\
D_{1,1}(1^m) &= \{p, q \leftarrow \text{BW}(1^m); n \leftarrow p \cdot q; h_0, h_1 \leftarrow Z_n^{+1}; s \leftarrow Z_n^{+1} : (n, h_0, h_1, s)\}
\end{align*}

We say that algorithm $\mathcal{A}$ has advantage $\epsilon$ in solving QIP$_1$ if we have that:

\[
|\Pr[(n, h_0, h_1, s) \leftarrow D_{1,0}(1^m) : A(n, h_0, h_1, s) = 1] \\
- \Pr[(n, h_0, h_1, s) \leftarrow D_{1,1}(1^m) : A(n, h_0, h_1, s) = 1]| = \epsilon. \tag{7}
\]

We say that QIP$_1$ is intractable if all polynomial time (in $m$) algorithms have a negligible (in $m$) advantage in solving QIP$_1$.

By a simple simulation argument, we can prove the following theorem:

**Theorem 1.** The QIP$_1$ problem is intractable if and only if the QIP problem is so.

To prove the equivalence of QIP and QIP$_1$, given $D_0$ and $D_1$, we choose randomly $h_1 \leftarrow Z_n^{+1}$ and create $D_{1,0}$ and $D_{1,1}$. If we can distinguish between these two with probability $\epsilon$, then with prob $\epsilon/2$ we can distinguish between the given two distribution.

QIP$_2$ Problem. We define the QIP$_2$ problem as the problem of efficiently distinguishing the following two distributions:

\begin{align*}
D_{2,0}(1^m) &= \{p, q \leftarrow \text{BW}(1^m); n \leftarrow p \cdot q; h_0, h_1 \leftarrow Z_n^{+1}; \\
&\quad s \leftarrow \text{CS}(n, s^2 - 4h_0 \in Z_n^{-1} \cup QR(n)) : (n, h_0, h_1, s)\} \\
D_{2,1}(1^m) &= \{p, q \leftarrow \text{BW}(1^m); n \leftarrow p \cdot q; h_0, h_1 \leftarrow Z_n^{+1}; \\
&\quad s \leftarrow \text{CS}(n, s^2 - 4h_1 \in Z_n^{-1} \cup QR(n)) : (n, h_0, h_1, s)\}
\end{align*}

We say that algorithm $\mathcal{A}$ has advantage $\epsilon$ in solving QIP$_2$ if we have that:

\[
|\Pr[(n, h_0, h_1, s) \leftarrow D_{2,0}(1^m) : A(n, h_0, h_1, s) = 1] \\
- \Pr[(n, h_0, h_1, s) \leftarrow D_{2,1}(1^m) : A(n, h_0, h_1, s) = 1]| = \epsilon. \tag{8}
\]
We say that QIP\textsubscript{2} is *intractable* if all polynomial time (in $m$) algorithms have a negligible (in $m$) advantage in solving QIP\textsubscript{2}.

By a simple hybrid argument, we can prove the following theorem:

**Theorem 2.** The QIP\textsubscript{2} problem is intractable if and only if the QIP problem is so.

To prove the equivalence of QIP and QIP\textsubscript{2}, given $D_0$ and $D_1$, we choose randomly $h' \leftarrow \mathbb{Z}_n^+$ and create $D'_1$. Then we treat $D_1$ and $D'_1$ as $D_{2,0}$ and $D_{2,1}$. If we can distinguish between these two then we contradict the indistinguishability between $D_0$ and $D_1$ and between $D_0$ and $D'_1$. 