$\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ where $N = pq$.

$J_p(x) = +1, \quad J_q(x) = +1$ $\qquad$ $J_N(x) := J_p(x) \cdot J_q(x)$

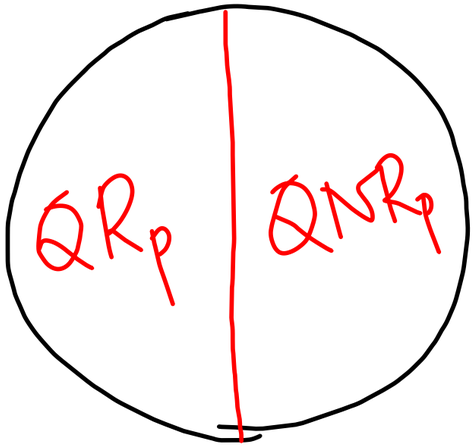
where $J_p(x) = J_p(x \bmod p)$.

$\|$ $\qquad$ $J_q(x) = J_q(x \bmod q)$

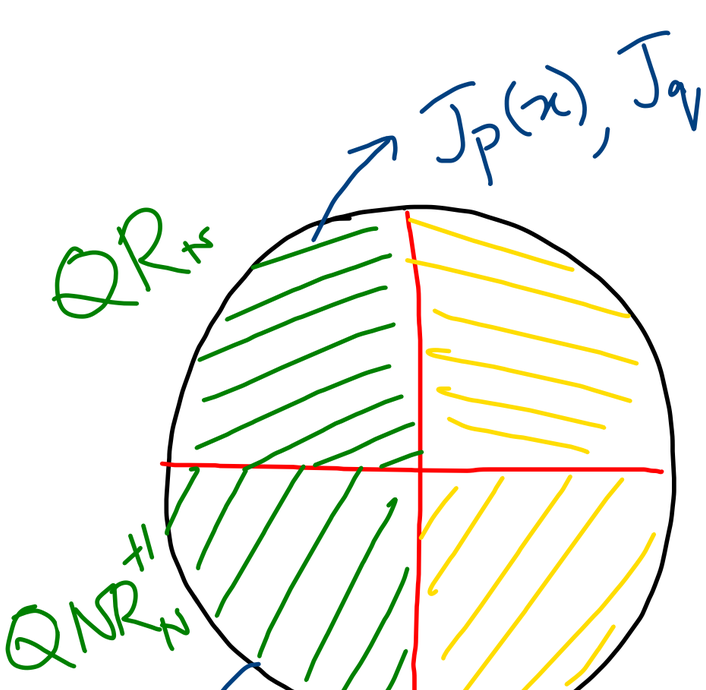
$QR_N = \{x \in \mathbb{Z}_N^* : x \text{ is a quadratic residue}\}$.

if $x \in \mathbb{Z}_N^*$ is a quadratic residue, then $J_N(x) = +1$.

$QNR_N^{+1} = \{x \in \mathbb{Z}_N^* : x \text{ is not a quadratic residue, but } J_N(x) = +1\}$.



$\mathbb{Z}_p^*$, p is a prime



$\mathbb{Z}_N^*$, where $N = p \cdot q$.

$J_N(x)$

$J_p(x \bmod p),\ J_q(x \bmod q)$

$J_p(x)$,
$J_q(x) = -1$

Left half is denoted by J_N^{+1}

Right " " " " J_N^{-1}

Quadratic Residuosity Assumption:

DIST-QR

Challenger: Adversary:

1^n ←

$(N,p,q) \leftarrow$ Gen Modulus (1^n)

$b \leftarrow \$ \{0,1\}$

if $b=0$

sample $x \leftarrow \$ QR_N$

if $b=1$

sample $x \leftarrow \$ QNR_N^{+1}$

(N, x) →

guess a bit b'

b' ←

Outputs 1 if $b=b'$

Defn: We say deciding quadratic residuosity is hard relative to GenModulus. if for PPT algorithm D, $\exists$ a negligible fn negl( ) such that

$$\left| Pr\left[D(N, qr) = 1 \right] - Pr\left[D(N, qnr) = 1 \right] \right| \leq negl(n)$$

where $qr \leftarrow \$ QR_N$ and $qnr \leftarrow \$ QNR^{+1}_N$.

If factorization is easy, then deciding quadratic residuosity is easy. $QRP \leq_p FACT$

Goldwasser-Micali Encryption Scheme.

$m \in \{0,1\}$. $\mathbb{Z}_{512}^*$

KeyGen: On i/p 1^n, it invokes GenModulus(1^n) to obtain (N, p, q). Set the $pk = N$ and $sk = (p, q)$.

Enc: To encrypt a '0', it randomly samples $x \leftarrow\$ QR_N$
To encrypt a '1', it randomly samples $x \leftarrow\$ QNR_N^{+1}$
and set the ciphertext $c = x$.

Dec: Receiver checks whether c is a quadratic residue or not.
If it is, then it output 0, else output 1.

Revised GM-Encryption Scheme:

KeyGen: On i/p 1^n, it invokes GenModulus(1^n) and obtain (N, p, q). It additionally samples

$z \leftarrow\$ QNR_N^{+1}$ and set $pk = (N, z)$ and $sk = (p, q)$

Enc: To encrypt a message m, it randomly samples

$x \leftarrow\$ \mathbb{Z}_N^*$

$C = z^m \cdot x^2 \bmod N$.

z^m: QNR_N^{+1} if $m = 1$, QR_N otherwise

x^2: QR_N

Dec: Similar as before.

1. How to ensure that one can uniformly choose an element from QNR_N^{+1}, given the knowledge of the factorization of N.

q. $\mathbb{Z}_p^*$ $\{1, \ldots p-1\}$.

$\mathbb{Z}_p^*$. $\mathbb{Z}_q^*$. By CRT

x_p. x_q. $(x_p, x_q) \leftrightarrow (x)$

$x \in QNR_N^{+1} \Rightarrow J_p(x) = -1$

$J_q(x) = -1$

2. Let $\hat{y} \in \mathcal{QR}_N$.

$$Pr[x^2 \bmod N = \hat{y}] = \frac{1}{|\mathcal{QR}_N|}.$$

Let the square roots of y be

$$\{\pm x', \pm \hat{x}'\}.$$

$$Pr[x^2 \bmod n = y].$$

$$\Rightarrow Pr[x \bmod n = \sqrt{y}].$$

$$\Rightarrow Pr[x \in \{\pm x', \pm \hat{x}'\}] = \frac{4}{|\mathbb{Z}_N^*|} = \frac{1}{|\mathcal{QR}_N|}.$$

Similarly, if $z \leftarrow\$ \mathcal{QNR}_N^{+1}$ and $x \leftarrow\$ \mathcal{QR}_N$, then for any $\hat{y} \in \mathcal{QNR}_N^{+1}$.

$$Pr[z \cdot x^2 \bmod n = \hat{y}] = \frac{1}{|\mathcal{QNR}_N^{+1}|}.$$

Thm: If the quadratic residuosity problem is hard, then the GM-encryption scheme is CPA secure.

Pf: Let A be an alg. for breaking indistinguishability notion of GM-encryption scheme.

We construct an adversary A' such that it breaks the quadratic residuosity problem.

Thm: If the quadratic residuosity problem is hard, then the GM-encryption scheme is CPA secure.

Pf: Let A be an alg. for breaking indistinguishability notion of GM-encryption scheme.

We construct an adversary A' such that it breaks the quadratic residuosity problem.

Thm: If the quadratic residuosity problem is hard, then the GM-encryption scheme is CPA secure.

Pf: Let A be an alg. for breaking indistinguishability notion of GM-encryption scheme.

We construct an adversary A' such that it breaks the quadratic residuosity problem.

GM

Ch(A') | A' | A

$Gen_m(1^n)$ ← 1^n

$b \leftarrow \$\{0,1\}$

if $b=0$,
$z \leftarrow \$ QR_N$

if $b=1$,
$z \leftarrow \$ QNR_N^{+1}$

(N, z) →

$Pk = (N, z)$

$b' \leftarrow \$\{0,1\}$ ← (m_0, m_1)

$x \leftarrow \$ R_N$

$c = z^{m_{b'}} \cdot x^2$ →

$b^* = b'$ ← b^* | ↓ b^*

Output 1.

$$\left| Pr[A'(N, z) = 1] - Pr[A'(N, z) = 1] \right|$$

Case i)

$z \leftarrow \$ QNR_N^{+1}$

GM

Ch(A') | A' | A

$Gen_m(1^n)$ ← 1^n

$b \leftarrow \$\{0,1\}$

if $b=0$,
$z \leftarrow \$ QR_N$

if $b=1$,
$z \leftarrow \$ QNR_N^{+1}$

(N, z) →

$Pk = (N, z)$

$b' \leftarrow \$\{0,1\}$ ← (m_0, m_1)

$x \leftarrow \$ R_N$

$c = z^{m_{b'}} \cdot x^2$ →

$b^* = b'$

Output 1.

← b^*

↓ b^*

Case i)

$z \leftarrow \$ QNR_N^{+1}$

$$\left| Pr[A'(N, z) = 1] - Pr[A'(N, z) = 1] \right|$$

$$\Pr\left[A'(N, g, h_\gamma) = 1\right]$$

$$= \Pr\left[\underbrace{Pubk^{eav}_{QM}(A) = 1}\right] \cdot$$

$$\Pr[b' = b^*]$$

Case 2: $z \leftarrow\$ QR_N$

$$\Pr[A'(N, g, z) = 1] = \Pr[Pubk^{eav}_{\widetilde{QM}}(A) = 1] = \frac{1}{2}.$$

$$\left| P[A'(N, g, n, r) = 1] - P[A'(N, g, r) = 1] \right| > \varepsilon(n)$$

$$= \left| P[Pubk^{eav}_{G,M}(A) = 1] - \frac{1}{2} \right|$$

non-negligible