**MIX Server**

1. Discard Duplicates
2. Decrypt

*(rimi)edmodn*

1. Permute
2. Remove Randomness

*mi🡪rimi🡪(rimi)e*

*...*m*i’...*

*E(m­J)*

*mj*

MIXNET

MIXNET

*E(m­J)*

*mj*

*E(m­J)E(f)*

*m­Jf*

c

c

c

h

**Mj**

**M1**

keeptrack of permutatioon and reencryption

**M2**

Cx,0

Cy,0

Ci1,1

Ci2,1

Cπ2(i1),1

**C**

*G­­­­1*

*G­­­­t*

*G­­­­b*

*G­­­­b*

*G­­­­t*

*G­­­­1*

*G­­­­1*

*G­­­­b*

*G­­­­1*

*G­­­­t*

*G­­­­t*

*G­­­­b*

N-2

*M1*

1

2

3

i

j

k

N-2

N-1

N

N

N-1

i

j

k

1

2

3

2

j

k

i

3

N-1

1

N-2

N

*G­­­­1’*

*G­­­­t’*

*G­­­­b’*

*x2*

*x1*

*e2*

*e1*

*i2*

*i1*

*u2*

*u1*

*x2*

*i2*

*x1*

*i1*

*e2*

*u2*

*e1*

*u1*