Zhaoyi Zhang
zzhang825

1. Alice pick $x \leftarrow \mathbb{Z}_q$ and send g^x to Bob
The Adversary gets g^x from Alice, picks $x' \leftarrow \mathbb{Z}_q$ and sends $g^{x'}$ to Bob.
Bob picks $y \leftarrow \mathbb{Z}_q$ and sends to g^y to Alice
The Adversary gets g^y from Bob, picks $y' \leftarrow \mathbb{Z}_q$ and sends $g^{y'}$ to Alice
Alice thinks the key is $k_A = (g^{y'})^x$ and Bob thinks the key is $k_B = (g^{x'})^y$

2. Given the knowledge of x, compute $\frac{(C_1)^x}{C_2}$
If $b=0$, $\frac{(C_1)^x}{C_2} = \frac{(g^y)^x}{h^y} = \frac{g^{xy}}{(g^x)^y} = 1$

If $b=1$, $\frac{(C_1)^x}{C_2} = \frac{g^{xy}}{g^z} \neq 1$ unless $z = xy$ which has negligible probability

4. $s := k \oplus r$
$u := s \oplus t = k \oplus r \oplus t$
$w := u \oplus r = k \oplus r \oplus t \oplus r = k \oplus t$
$k := w \oplus t = k \oplus t \oplus t = k$
so Alice and Bob has the same key
The eavesdropper knows s, u, w, and $k := s \oplus u \oplus w$.
Thus, the eavesdropper can compute the key, the scheme is not secure

3.