Advanced Crypto – Exercises

DLP-based oblivious transfers.

Oblivious transfer is a protocol between two participants, Alice and Bob. At the start of the protocol, Alice has two secrets s_0 and s_1, and Bob has a secret bit $k \in \{0,1\}$. If executed correctly, at the end of the protocol Bob knows the secret s_k, but learns no information on Alice's other secret s_{1-k}, and Alice learns no information about Bob's bit b. In other words, Bob chooses one of Alice's secrets to learn, but Alice does not know which one. Oblivious transfer is a fundamental building block for secure multiparty computations.

I. A first protocol : Wu-Zhang-Wang construction.

Let E be an elliptic curve and P a point of large prime order ℓ, such that the DLP is hard on $\langle P \rangle$.

— Alice's secrets s_0 and s_1 are encoded as points $S_0, S_1 \in \langle P \rangle \setminus \{\mathcal{O}\}$.
— Alice picks a uniformly random integer $a \in \{1, \ldots, \ell-1\}$. She computes $A_0 = aS_0$ and $A_1 = aS_1$ and sends them to Bob.
— Bob chooses a uniformly random integer $b \in \{1, \ldots, \ell-1\}$. According to the index k of the secret he is interested in, he computes the group element $B' = bA_k$ and sends it to Alice.
— Alice computes $B = a^{-1}B'$ and sends it to Bob.
— Bob computes $b^{-1}B$.

1) Show that the protocol is correct, i.e. Bob learns S_k.
2) Suppose that Alice is *malicious* and just wants to learn Bob's secret bit k ; she can send two points A_0 and A_1 of her choosing to Bob. Can she learn information about k ?
3) Suppose that Bob is *honest-but-curious* : he follows the protocol but would like to gain information on Alice's other secret. Show that this is not possible if the computional Diffie-Hellman problem is hard.
4) Suppose now that Bob is *malicious* and sends $b(A_1 - A_0)$ to Alice. What does he get ? Does it follow the specifications of an oblivious transfer protocol ?
5) Propose a modification of this protocol that does not allow a malicious Bob to learn partial information on both secrets.
Hint : don't encode s_0 ans s_1 as points on E ; pick random S_0 and S_1, and mask s_i with S_i.
6) The construction described above is actually a *1-out-of-2* oblivious transfer protocol. Can it be transformed in a 1-out-of-n protocol ? t-out-of-n protocol ?

II. A second protocol : Naor-Pinkas construction.

Let E be an elliptic curve and P a point of large prime order ℓ, such that the DLP is hard on $\langle P \rangle$.

— Alice's secrets s_0 and s_1 are encoded as points $S_0, S_1 \in \langle P \rangle$.
— Bob chooses random integers $a, b, d \in \{1, \ldots, \ell-1\}$, sets $c_k = ab$ and $c_{1-k} = d$ where k is his secret bit. He sends Alice the tuple $(P, A, B, Q_0, Q_1) = (P, aP, bP, c_0P, c_1P)$.
— Alice checks that $Q_0 \neq Q_1$.
She then picks uniformly random integers $x_0, y_0, x_1, y_1 \in \{0, \ldots, \ell-1\}$, and computes and sends Bob the two couples $(T_0, C_0) = (x_0B + y_0P, S_0 + x_0Q_0 + y_0A)$ and $(T_1, C_1) = (x_1B + y_1P, S_1 + x_1Q_1 + y_1A)$.
— Bob computes $C_k - aT_k$.

1) Show that the protocol is correct, i.e. Bob learns S_k.
2) Security against a malicious Bob.
Since $Q_0 \neq Q_1$, at least one of the tuple (P, A, B, Q_0) and (P, A, B, Q_1) is not a valid Diffie-Hellman tuple ; let $i \in \{0,1\}$ be such that the corresponding tuple is invalid.
Show that the couple (T_i, C_i) is uniformly distributed in $\langle P \rangle^2$ and thus leaks no information on S_i.
Hint : solve for (x_i, y_i) the system $\begin{cases} T_i = \alpha P \\ C_i = \beta P \end{cases}$ by passing to the DL in basis P.
3) Under what assumption(s) is this protocol secure against a malicious Alice ? Is it always satisfied ?