EC Integrated encryption scheme

Cryptosystem 6.2: *Simplified ECIES*

Let E be an elliptic curve defined over $\mathbb{Z}_p$ ($p > 3$ prime) such that E contains a cyclic subgroup $H = \langle P \rangle$ of prime order n in which the Discrete Logarithm problem is infeasible.
Let $\mathcal{P} = \mathbb{Z}_p{}^*$, $\mathcal{C} = (\mathbb{Z}_p \times \mathbb{Z}_2) \times \mathbb{Z}_p{}^*$, and define

$$\mathcal{K} = \{(E, P, m, Q, n) : Q = mP\}.$$

The values P, Q and n are the public key, and $m \in \mathbb{Z}_n{}^*$ is the private key.

For $K = (E, P, m, Q, n)$, for a (secret) random number $k \in \mathbb{Z}_n{}^*$, and for $x \in \mathbb{Z}_p{}^*$, define

$$e_K(x, k) = (\text{POINTCOMPRESS}(kP), x x_0 \bmod p),$$

where $kQ = (x_0, y_0)$ and $x_0 \neq 0$.

For a ciphertext $y = (y_1, y_2)$, where $y_1 \in \mathbb{Z}_p \times \mathbb{Z}_2$ and $y_2 \in \mathbb{Z}_p{}^*$, define

$$d_K(y) = y_2 (x_0)^{-1} \bmod p,$$

where

$$(x_0, y_0) = m\,\text{POINTDECOMPRESS}(y_1).$$