

the master public key mpk comprises $(s \cdot Q, Q, P)$, where P is a generator of cyclic group G_1 with prime order q defined over an elliptic curve, Q is a generator of cyclic group G_2 with prime order q and s is a parameter obtained from the master secret key msk ;

the second element k_j is defined as $k_j = (b \cdot P, b \cdot Q)$; and

the common secret cs_j is computed using an asymmetric bilinear map $e: G_1 \times G_2 \rightarrow G$ where G is cyclic group with prime order q defined over the elliptic curve, and cs_j is defined as $cs_j = e(a \cdot P, s \cdot Q)^b$.

40. A second device j for generating a common session key SK for encoding digital communications between the first device i and the second device j , comprising:
- a processor; and
 - a non-transitory media readable by the processor, the non-transitory media storing instructions that when executed by the processor, cause the processor to:
 - receiving, by the second device, a master public key mpk and a private key from a secure server;
 - receiving a first element k_i and the identity id_i of the first device from the first device i ;
 - compute a second element k_j based on a second random value b generated by the second device, and the master public key mpk ;
 - compute signature σ_j by signing the first element k_i and the second element k_j using a signing function of an Identity Based Signature Scheme and the private key sk_j ;
 - transmit to the first device the second element k_j and the signature σ_j ;
 - receive a signature σ_i from the first device;
 - verify, by the second device, the signature σ_i using the verification function of the Identity Based Signature Scheme and the identity of the first device id_i , and when the signature σ_i is verified,
 - compute a common-secret cs_j based on the first element k_i , the master public key mpk , and the second random value b , and generating the common session key SK by providing the common-secret cs_j to the Key Deriving Function.