5.3 Identity-Based Digital Signature Schemes in WSN

5.3.1 ID-Based Signature (IBS)

Definition: The four algorithms that define the IBS scheme are *Setup*, *Key Extraction*, *Signature Generation*, and *Signature Verification*.

The *Setup* and *Key Extraction* processes are executed before the deployment of the sensor network. Usually, the sink node or base station takes the role of a PKG and performs the initialization process through *Setup* and key generation through the *Key Extraction* process.

Setup: Given a security parameter $x \in Z_q^*$ to this algorithm, it outputs system parameters PP and a master secret M_s. The master secret is only known to PKG.

Key Extraction: Given a user's identity ID_i and the master secret M_s to this algorithm, it outputs the private-key d_{ID_i}.

ID_i, d_{ID_i}, and PP are prestored in a sensor node before deployment.

Signature Generation: Given the message $m \in M$ and the private key d_{ID_i}, this algorithm outputs the signature σ.

Signature Verification: Given a message $m \in M$, the signer's identity ID_i, signature σ, and system parameters PP, this algorithm returns valid (1) or invalid (0).

5.3.2 ID-Based Online/Offline Signature (IBOOS)

The IBOOS algorithm is usually used for authenticated broadcast (Yasmin et al. 2010)

Definition: The following five algorithms define the ID-based online/offline signature (IBOOS) scheme.

Setup and *Key Extraction* are the same as defined in IBS.

The signature generation process is divided into two processes, namely, *Offline Signature Generation* and *Online Signature Generation.*

Offline Signature Generation: Given the system parameters PP and the signing key d_{ID_i}, execution of this algorithm results in a partial offline signature σ_{Off}. This phase is usually executed on a resource abundant device such as a sink node or a base station before the message to broadcast becomes available. In deployment scenarios where the sensor network is divided into clusters, cluster heads could take the responsibility of executing this algorithm. The resulting signature is stored on each sensor node before it is deployed.

Online Signature Generation: This algorithm is executed whenever a sensor node must quickly report an event to its respective sink node or its cluster head. It is performed on resource constraint devices such as sensor nodes. Given $m \in M$, σ_{Off}, and the time stamp T_s, the algorithm generates an online signature σ_{On}. The reuse of the partial offline signature σ_{Off} computed in the offline phase will considerably reduce the energy