LIST OF NOTATIONS

Symbols	Definition
Ev	Event id
Key_{reg}	Key Shuffle for Connection Phase
$Authkey_i$	Authentication key for PUBLISH
$Ec(M_i)$	Encrypted Message for Connection Phase
b	Random number
q	Prime number
q_{root}	Prime root of q
p	Prime number
p_{root}	Prime root of p
α	Prime root
Y_a	Product of ElGamal
ID	Identity of IoT device
C_1	First Cipher from ElGamal
C_1	Second Cipher from ElGamal
m	Message length of m (integer)
n	Integer
Y_i	Product Proposed Function
T_i	Product Proposed Function
$PubEv_i$	Product Proposed Function
M_i	Product Proposed Function
$PublishEv_i$	Product Proposed Function
$KeyEv_i$	Product Proposed Function
U_i	Product Proposed Function
K_{seed}	Seed for key
$K_{publish}$	Key for encrypt PUBLISH message
rc	random characters
concat(A,B)	concatenate A and B
$Enc(A,B)$	A Encrypted with B
$Dec(A,B)$	A Decrypted with B