u1

u2

Authentication	Send a request	$M_1 = request \parallel u_1 \parallel u_2$	Get RSS	Authentication
	Get RSS; Encryption; Hash; Compare RSS	$M_2 = H(E_{dk}(RSS_{v1,2}))$	Encryption; Hash	
	Encryption	$M_3 = E_{dk}(RSS_{v2,1} + 1)$	Get RSS; Decryption; Compare different RSS values	
Session key generation	Decryption	$M_4 = E_{dk}(RSS_{s2,1} \oplus r_1)$	Generate random number; Encryption	Session key generation
	Generate random number; Encryption	$M_5 = E_{dk}(RSS_{s2,1} \oplus r_2)$	Decryption	