

Table 1: Detailed results for LoRaWAN 1.0 OTAA - Nonces

Case	Nonce	IA_D	IA_N	NIA_D	NIA_N	IAK	NIAK	S_D	S_N	KF_D	KF_N
No misgeneration	N/A	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓
Leak Always	<i>DevNonce</i>	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓
Leak Always	<i>JoinNonce</i>	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓
Reuse Always	<i>DevNonce</i>	✗	✗	✓	✓	✗	✓	✓	✓	✗	✓
Reuse Always	<i>JoinNonce</i>	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗
Reuse Once	<i>DevNonce = DevNonce</i>	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓
Reuse Once	<i>DevNonce = JoinNonce</i>	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓
Reuse Once	<i>JoinNonce = JoinNonce</i>	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗