Table 1: Detailed results for Bluetooth Secure Numeric Comparison - Nonces and keys

Case	Nonce	IA_I	IA_R	NIA_I	NIA_R	IAK_I	IAK_R	NIAK_I	NIAK_R	S_I	S_R	KF_I	KF_R
No misgeneration	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Leak Always	sk_i	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Leak Always	sk_r	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Leak Always	N_r	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Leak Always	N_i	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Reuse Always	sk_i	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Always	sk_r	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Always	N_r	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Reuse Always	N_i	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Reuse Once	$sk_i = sk_i$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$sk_i = sk_r$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$sk_i = N_r$	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Reuse Once	$sk_i = N_i$	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Reuse Once	$sk_r = sk_r$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$sk_r = N_r$	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Reuse Once	$sk_r = N_i$	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Reuse Once	$N_r = N_r$	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Reuse Once	$N_r = N_i$	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Reuse Once	$N_i = N_i$	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓