Table 1: Detailed results for Dragonfly - patch reflection attack - Nonces and keys

Case	Nonce	IA_AP	IA_C	NIA_AP	NIA_C	IAK_AP	IAK_C	NIAK_AP	NIAK_C	S_AP	S_C	KF_AP	KF_C
No misgeneration	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Leak Always	sk_C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
Leak Always	m_C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
Leak Always	sk_{AP}	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Leak Always	m_{AP}	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Reuse Always	sk_C	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Always	m_C	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Always	sk_{AP}	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Always	m_{AP}	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$sk_C = sk_C$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$sk_C = m_C$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$sk_C = sk_{AP}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$sk_C = m_{AP}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$m_C = m_C$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$m_C = sk_{AP}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$m_C = m_{AP}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$sk_{AP} = sk_{AP}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$sk_{AP} = m_{AP}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$m_{AP} = m_{AP}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓