

bit index i	i th bit of NOT(p')	function calls	operation	pow_out
4	0	MONT_SQR(2^{31})	$2^{31 \times 2 - 64}$	2^{-2}
3	1	$2 \times \text{MONT_SQR}(2^{-1})$	$2^{-2 \times 2 - 64} \times 2$	$2^{-68} \times 2 = 2^{-67}$
2	1	$2 \times \text{MONT_SQR}(2^{-66})$	$2^{-67 \times 2 - 64} \times 2$	$2^{-198} \times 2 = 2^{-197}$
1	1	$2 \times \text{MONT_SQR}(2^{-196})$	$2^{-197 \times 2 - 64} \times 2$	$2^{-458} \times 2 = 2^{-457}$
0	0	MONT_SQR(2^{-457})	$2^{-457 \times 2 - 64}$	2^{-978}