

Table 6.5: WAGE hardware area estimates and pre-PAR implementation results

Component	Estimate per unit [GE]	Count	Estimate per component [GE]
State registers	3.75	259	971
Feedback XORs	2.00	70	140
Feedback multiplier <sup>†</sup>			6
WGP <sup>†</sup>	258	2	516
SB <sup>†</sup>	58	4	227
constant LFSR <sup>†</sup>			50
other XORs	56	2	112
Permutation without muxes (estimate)			<b>2022</b>
Permutation without muxes (synthesized) <sup>†</sup>			1984
Absorb muxes	2.00	70	140
AED XORs	2.00	70	140
Dom-sep muxes	2.00	7	14
Dom-sep XORs	2.00	7	14
Replace muxes	2.00	70	140
Pad NOTs	0.75	7	5
Pad muxes	2.00	7	14
Input-enable AND	1.50	21	32
Non-linear muxes	2.00	28	56
Extra circuitry for sponge mode			555
Complete datapath (estimate)			<b>2577</b>
Complete datapath (synthesized) <sup>†</sup>			2831
FSM (synthesized) <sup>†</sup>			202
Complete cipher (estimate)			<b>2779</b>
Complete cipher (synthesized) <sup>†</sup>			3034

<sup>†</sup> implementation results (synthesized)