

Table 1: Red-teaming attack success rates of SafeProtein against DPLM2 on SafeProtein-Bench. Results are reported for all masking strategies. For each sequence masking ratio, the best success rate is highlighted in bold.

Gen Strategy	Masking Strategy	Sequence Masking Ratio				
		0.1	0.2	0.25	0.3	0.4
Strategy1	Conservation	<b>36.36</b>	<b>29.84</b>	<b>26.81</b>	<b>21.45</b>	<b>15.62</b>
	Random	18.88	9.56	10.02	6.06	7.29
	Tail	8.86	2.33	3.50	1.87	1.19
Strategy2	Conservation	<b>42.66</b>	<b>34.50</b>	<b>32.40</b>	<b>27.97</b>	<b>20.58</b>
	Random	21.45	9.79	10.72	6.99	7.29
	Tail	5.83	2.10	4.20	2.56	1.19
Strategy3	Conservation	<b>44.29</b>	<b>33.10</b>	<b>30.54</b>	<b>26.57</b>	<b>20.58</b>
	Random	19.58	8.63	10.02	7.46	6.06
	Tail	9.32	1.63	4.66	2.80	2.38