$e_{127}$ 

 $e_{126}$ 

 $e_{125}$ 

 $e_{124}$ 

 $e_{123}$ 

 $e_{122}$ 

 $e_{121}$ 

$e_{15}$	$e_{14}$	$e_{13}$	$e_{12}$	$e_{11}$	$e_{10}$	$e_9$	$e_8$	$e_7$	$e_6$	$e_5$	$e_4$	$e_3$	$e_2$	$e_1$	$e_0$	$v_n$
$e_{31}$	$e_{30}$	$e_{29}$	$e_{28}$	$e_{27}$	$e_{26}$	$e_{25}$	$e_{24}$	$e_{23}$	$e_{22}$	$e_{21}$	$e_{20}$	$e_{19}$	$e_{18}$	$e_{17}$	$e_{16}$	$v_{n+1}$
$e_{47}$	$e_{46}$	$e_{45}$	$e_{44}$	$e_{43}$	$e_{42}$	$e_{41}$	$e_{40}$	$e_{39}$	$e_{38}$	$e_{37}$	$e_{36}$	$e_{35}$	$e_{34}$	$e_{33}$	$e_{32}$	$v_{n+2}$
$e_{63}$	$e_{62}$	$e_{61}$	$e_{60}$	$e_{59}$	$e_{58}$	$e_{57}$	$e_{56}$	$e_{55}$	$e_{54}$	$e_{53}$	$e_{52}$	$e_{51}$	$e_{50}$	$e_{49}$	$e_{48}$	$v_{n+3}$
$e_{79}$	e <sub>78</sub>	e <sub>77</sub>	$e_{76}$	$e_{75}$	$e_{74}$	$e_{73}$	$e_{72}$	$e_{71}$	$e_{70}$	$e_{69}$	$e_{68}$	$e_{67}$	$e_{66}$	$e_{65}$	$e_{64}$	$v_{n+4}$
$e_{95}$	$e_{94}$	$e_{93}$	$e_{92}$	$e_{91}$	$e_{90}$	$e_{89}$	$e_{88}$	e <sub>87</sub>	$e_{86}$	$e_{85}$	$e_{84}$	$e_{83}$	$e_{82}$	$e_{81}$	$e_{80}$	$v_{n+5}$
$e_{111}$	$e_{110}$	$e_{109}$	$e_{108}$	$e_{107}$	$e_{106}$	$e_{105}$	$e_{104}$	$e_{103}$	$e_{102}$	$e_{101}$	$e_{100}$	$e_{99}$	$e_{98}$	$e_{97}$	$e_{96}$	$v_{n+6}$
																]

## 128 bits

 $e_{119}$ 

 $e_{118}$ 

 $e_{117}$ 

 $e_{115}$ 

 $e_{116}$ 

 $e_{114}$ 

 $e_{113}$ 

 $e_{112} \mid v_{n+7}$ 

 $e_{120}$