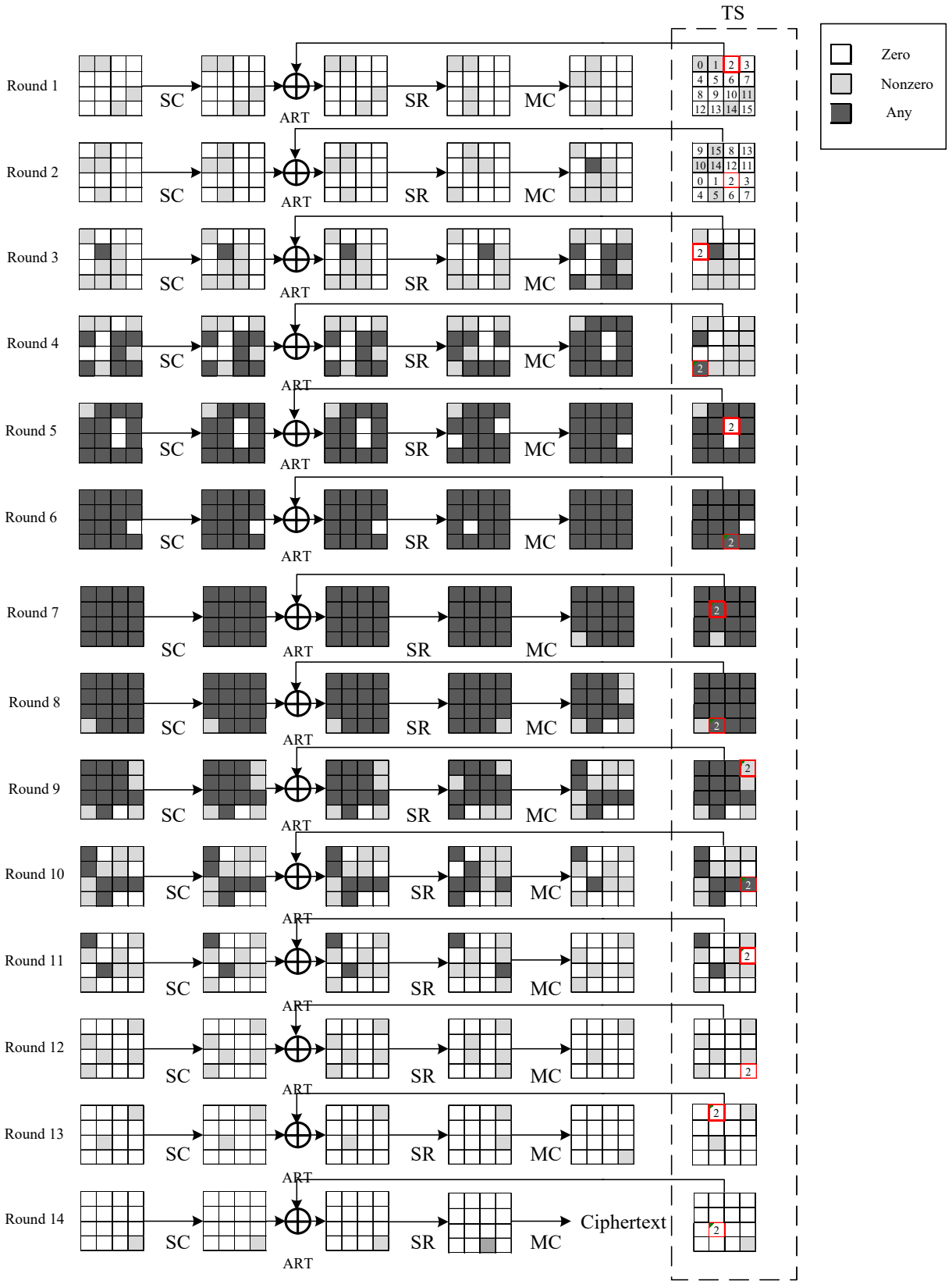

Fig. 4 14-round distinguisher for SKINNY-n-$2n$: the cells' values are colored as the legeng shown; and the cells in red frame form the Γ sequence

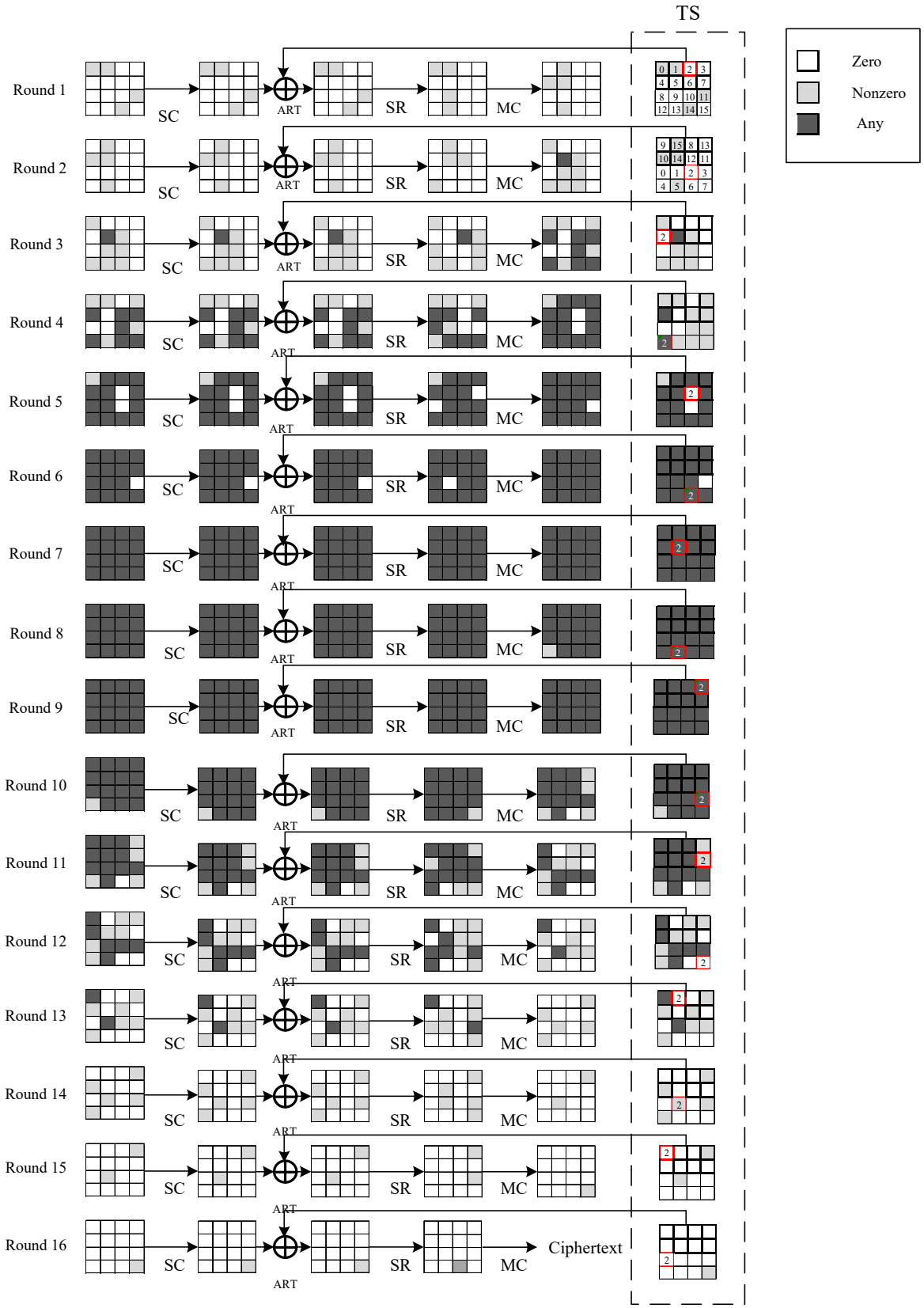

Fig. 5 16-round distinguisher for SKINNY-n-3n: the cells' values are colored as the legeng shown; and the cells in red frame form the Γ sequence

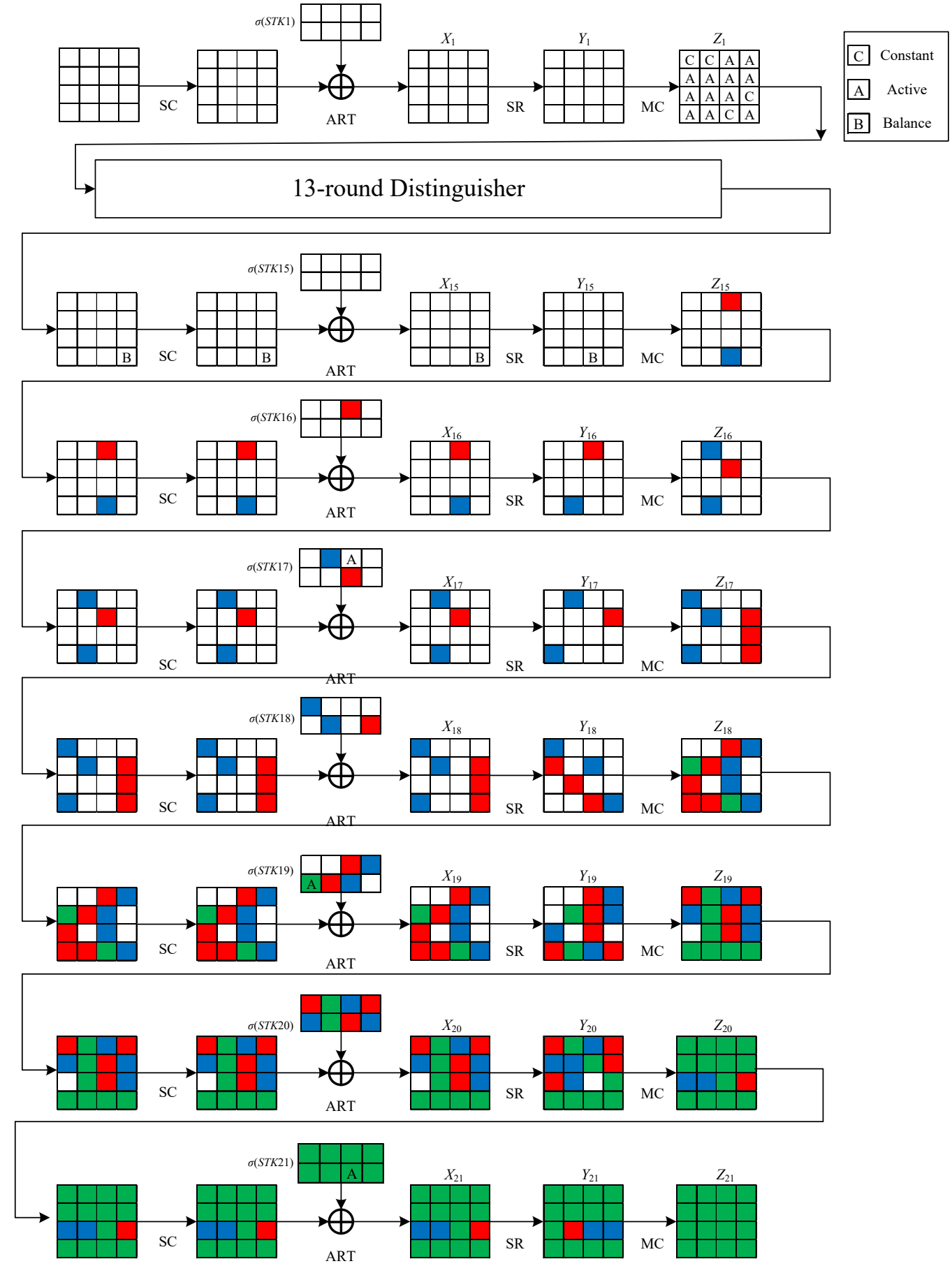

Fig. 6 21-round key recovery attack: The red cells and green cells are used to compute $Z_{15}[2]$, while the blue cells and green cells are used to compute $Z_{15}[14]$

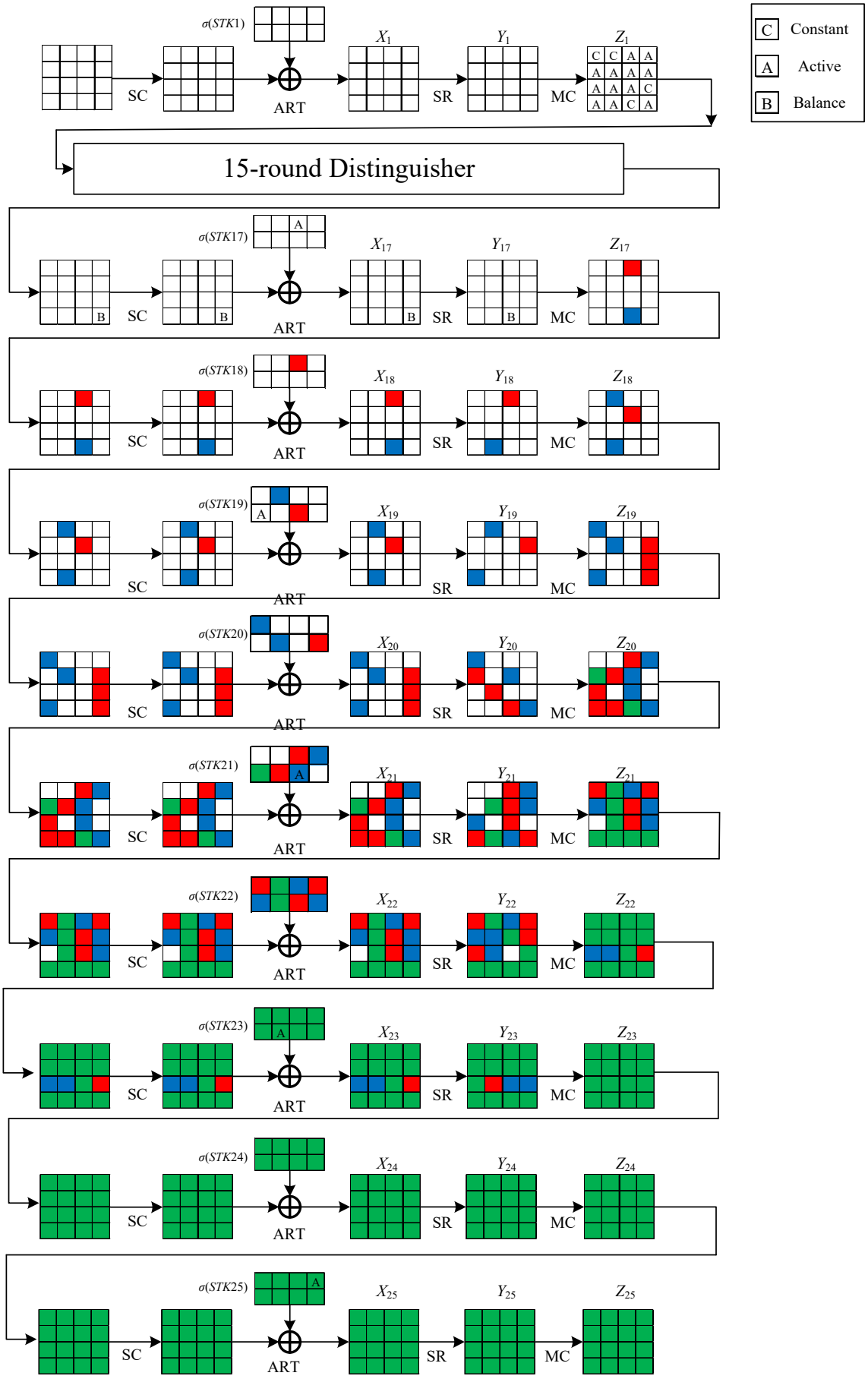

Fig. 7 25-round key recovery attack: The red cells and green cells are used to compute $Z_{17}[2]$, while the blue cells and green cells are used to compute $Z_{17}[14]$

Table 4 Procedure for computing $Z_{15}[2]$

Guessed key	Data (Log_2)	Stored texts	Memory (Log_2)	Time (Log_2)
-	$16c$	X_{21}[0,4,12], X_{21}[1,5,13], X_{21}[2,6,10,14], X_{21}[3,7,11,15],ΔTK_{21}[6],ΔTK_{19}[4]	$16c$	$16c$
STK_{21}[2,6]	$13c$	X_{21}[0,4,12], X_{21}[1,5,13], Y_{20} [6,14], X_{21}[3,7,11,15],ΔTK_{19}[4]	$15c$	$18c$
STK_{21}[1,5]	$12c$	X_{21}[0,4,12], Y_{20} [1,13], Y_{20} [6,14], X_{21}[3,7,11,15],ΔTK_{19}[4]	$16c$	$17c$
STK_{21}[3,7]	$12c$	X_{21}[0,4,12], Y_{20} [1,13],Y_{20} [6,14],Y_{20} [3,7,11,15],ΔTK_{19}[4]	$18c$	$18c$
STK_{21}[0,4]	$12c$	Y_{20} [0,8,12], Y_{20} [1,13], Y_{20} [6,14],Y_{20} [3,7,11,15],ΔTK_{19}[4]	$20c$	$20c$
-	$12c$	X_{20}[0,12], X_{20}[1,5,9,13], X_{20}[6,10,14], X_{20}[3,15],ΔTK_{19}[4]	-	-
STK_{20} [1,5]	$10c$	X_{20}[0,12], Y_{19} [5,13], X_{20}[6,10,14], X_{20}[3,15],ΔTK_{19}[4]	$20c$	$22c$
STK_{20} [3]	$9c$	X_{20}[0,12], Y_{19} [5,13], X_{20}[6,10,14], Y_{19} [15],ΔTK_{19}[4]	$20c$	$21c$
STK_{20} [0]	$8c$	Y_{19} [12], Y_{19} [5,13], X_{20}[6,10,14], Y_{19} [15],ΔTK_{19}[4]	$20c$	$21c$
STK_{20} [6]	$8c$	Y_{19} [12], Y_{19} [5,13], Y_{19} [2,6,10], Y_{19} [15],ΔTK_{19}[4]	$21c$	$21c$
-	$8c$	X_{19} [4,8,12], X_{19} [5,13], X_{19} [2,14],ΔTK_{19}[4]	-	-
STK_{19} [4]	$5c$	Y_{18} [4], X_{19} [5,13], X_{19} [2,14]	$19c$	$22c$
STK_{19} [2]	$4c$	Y_{18} [4], X_{19} [5,13],Y_{18} [14]	$19c$	$20c$
STK_{19} [5]	$3c$	Y_{18} [4],Y_{18} [9],Y_{18} [14]	$19c$	$20c$
-	$3c$	X_{18} [7,11,15]	-	-
STK_{18} [7]	c	Y_{17} [7]	$18c$	$20c$
-	c	X_{17} [6]	-	-
STK_{17} [6]	c	Y_{16} [2]	$19c$	$19c$
-	c	X_{16} [2] = Z_{15}[2]	-	-

[1] $c = 4$ if $n = 64$, or $c = 8$ if $n = 128$.

Table 5 Procedure for computing $Z_{15}[14]$

Guessed key	Data (Log_2)	Stored texts	Memory (Log_2)	Time (Log_2)
-	$17c$	X_{21}[0,4,8,12], X_{21}[1,5,9,13], X_{21}[2,6,10,14], X_{21}[3,7,15],ΔTK_{21}[6],ΔTK_{19}[4]	$17c$	$17c$
STK_{21}[2,6]	$15c$	X_{21}[0,4,8,12], X_{21}[1,5,9,13], Y_{20} [2,6,14], X_{21}[3,7,15],ΔTK_{19}[4]	$17c$	$19c$
STK_{21}[0,4]	$13c$	Y_{20} [4,12], X_{21}[1,5,9,13], Y_{20} [2,6,14], X_{21}[3,7,15],ΔTK_{19}[4]	$17c$	$19c$
STK_{21}[3,7]	$12c$	Y_{20} [4,12], X_{21}[1,5,9,13],Y_{20} [2,6,14], Y_{20} [11,15],ΔTK_{19}[4]	$18c$	$19c$
STK_{21}[1,5]	$12c$	Y_{20} [4,12],Y_{20} [1,5,9,13],Y_{20} [2,6,14],Y_{20} [11,15],ΔTK_{19}[4]	$20c$	$20c$
-	$12c$	X_{20}[4,12], X_{20}[1,5,9,13], X_{20}[2,14], X_{20}[7,11,15],ΔTK_{19}[4]	-	-
STK_{20} [1,5]	$10c$	X_{20}[4,12],Y_{19} [5,13], X_{20}[2,14], X_{20}[7,11,15],ΔTK_{19}[4]	$20c$	$22c$
STK_{20} [7]	$9c$	X_{20}[4,12],Y_{19} [5,13], X_{20}[2,14], Y_{19} [3,7],ΔTK_{19}[4]	$20c$	$21c$
STK_{20} [2]	$8c$	X_{20}[4,12],Y_{19} [5,13],Y_{19} [14], Y_{19} [3,7],ΔTK_{19}[4]	$20c$	$21c$
STK_{20} [4]	$7c$	Y_{19} [8], Y_{19} [5,13], Y_{19} [14],Y_{19} [3,7],ΔTK_{19}[4]	$20c$	$21c$
-	$7c$	X_{19} [4], X_{19} [6,10,14], X_{19} [3,15],ΔTK_{19}[4]	-	-
STK_{19} [6]	$5c$	X_{19} [4],Y_{18} [6], X_{19} [3,15],ΔTK_{19}[4]	$19c$	$21c$
STK_{19} [4]	$4c$	Y_{18} [0],Y_{18} [6], X_{19} [3,15],	$19c$	$20c$
STK_{19} [3]	$3c$	Y_{18} [0],Y_{18} [6],Y_{18} [15]	$19c$	$20c$
-	$3c$	X_{18} [0,12], X_{18} [5]	-	-
STK_{18} [0]	$2c$	Y_{17} [12], X_{18} [5]	$19c$	$20c$
STK_{18} [5]	$2c$	Y_{17} [12],Y_{17} [1]	$20c$	$20c$
-	$2c$	X_{17} [1,13]	-	-
STK_{17} [1]	c	Y_{16} [13]	$20c$	$21c$
-	c	X_{16} [14]=Z_{15}[14]	-	-

[1] $c = 4$ if $n = 64$, or $c = 8$ if $n = 128$.

Table 6 Procedure for computing $Z_{17}[2]$

Guessed key	Data (Log_2)	Stored texts	Memory (Log_2)	Time (Log_2)
-	$18c$	X_{25} [0,4,8,12], X_{25} [1,5,9,13], X_{25} [2,6,10,14], X_{25} [3,7,11,15],ΔTK_{25}[3],ΔTK_{23}[5]	$18c$	$18c$
STK_{25} [0,1,2,3,4,5,6,7]	$17c$	X_{24} [0,4,8,12], X_{24} [1,5,9,13], X_{24} [2,6,10,14], X_{24} [3,7,11,15],ΔTK_{23}[5]	$25c$	$26c$
STK_{24} [0,1,2,3,4,5,6,7]	$15c$	X_{23} [0,4,12], X_{23} [1,5,13], X_{23} [2,6,10,14], X_{23} [3,7,11,15],ΔTK_{23}[5]	$31c$	$33c$
-	$15c$	X_{23} [0,4,12], X_{23} [1,5,13], X_{23} [2,6,10,14], X_{23} [3,7,11,15],ΔTK_{23}[5]	-	-
STK_{23} [2,6]	$13c$	X_{23} [0,4,12], X_{23} [1,5,13],Y_{22} [6,14], X_{23} [3,7,11,15],ΔTK_{23}[5]	$31c$	$33c$
STK_{23} [1,5]	$11c$	X_{23} [0,4,12],Y_{22} [1,13], Y_{22} [6,14], X_{23} [3,7,11,15]	$31c$	$33c$
STK_{23} [3,7]	$11c$	X_{23} [0,4,12], Y_{22} [1,13], Y_{22} [6,14], Y_{22} [3,7,11,15]	$33c$	$33c$
STK_{23} [0,4]	$11c$	Y_{22} [0,8,12], Y_{22} [1,13], Y_{22} [6,14], Y_{22} [3,7,11,15]	$35c$	$35c$
-	$11c$	X_{22} [0,12], X_{22} [1,5,9,13], X_{22} [6,10,14], X_{22} [3,15]	-	-
STK_{22} [1,5]	$9c$	X_{22} [0,12],Y_{21} [5,13], X_{22} [6,10,14], X_{22} [3,15]	$35c$	$37c$
STK_{22} [3]	$8c$	X_{22} [0,12],Y_{21} [5,13], X_{22} [6,10,14], Y_{21} [15]	$35c$	$36c$
STK_{22} [0]	$7c$	Y_{21} [12],Y_{21} [5,13], X_{22} [6,10,14], Y_{21} [15]	$35c$	$36c$
STK_{22} [6]	$7c$	Y_{21} [12], Y_{21} [5,13], Y_{21} [2,6,10], Y_{21} [15]	$36c$	$36c$
-	$7c$	X_{21}[4,8,12], X_{21}[5,13], X_{21}[2,14]	-	-
STK_{21}[4]	$5c$	Y_{20} [4], X_{21}[5,13], X_{21}[2,14]	$35c$	$37c$
STK_{21}[2]	$4c$	Y_{20} [4], X_{21}[5,13], Y_{20} [14]	$35c$	$36c$
STK_{21}[5]	$3c$	Y_{20} [4], Y_{20} [9],Y_{20} [14]	$35c$	$36c$
-	$3c$	X_{20}[7,11,15]	-	-
STK_{20} [7]	c	Y_{19} [7]	$34c$	$36c$
-	c	X_{19} [6]	-	-
STK_{19} [6]	c	Y_{18} [2]	$35c$	$35c$
-	c	X_{18} [2]	-	-
STK_{18} [2]	c	Z_{17} [2]	$36c$	$36c$

[1] $c = 4$ if $n = 64$, or $c = 8$ if $n = 128$.

Table 7 Procedure for computing $Z_{17}[14]$

Guessed key	Data (Log_2)	Stored texts	Memory (Log_2)	Time (Log_2)
-	$19c$	X_{25} [0,4,8,12], X_{25} [1,5,9,13], X_{25} [2,6,10,14], X_{25} [3,7,11,15],ΔTK_{25}[3],ΔTK_{23}[5],ΔTK_{21}[6]	$19c$	$19c$
STK_{25} [0,1,2,3,4,5,6,7]	$18c$	X_{24} [0,4,8,12], X_{24} [1,5,9,13], X_{24} [2,6,10,14], X_{24} [3,7,11,15],ΔTK_{23}[5],ΔTK_{21}[6]	$26c$	$27c$
STK_{24} [0,1,2,3,4,5,6,7]	$17c$	X_{23} [0,4,8,12], X_{23} [1,5,9,13], X_{23} [2,6,10,14], X_{23} [3,7,15],ΔTK_{23}[5],ΔTK_{21}[6]	$33c$	$34c$
-	$17c$	X_{23} [0,4,8,12], X_{23} [1,5,9,13], X_{23} [2,6,10,14], X_{23} [3,7,15],ΔTK_{23}[5],ΔTK_{21}[6]	-	-
STK_{23} [0,4]	$15c$	Y_{22} [4,12], X_{23} [1,5,9,13], X_{23} [2,6,10,14], X_{23} [3,7,15],ΔTK_{23}[5],ΔTK_{21}[6]	$33c$	$35c$
STK_{23} [1,5]	$14c$	Y_{22} [4,12],Y_{22} [1,5,9,13], X_{23} [2,6,10,14], X_{23} [3,7,15],ΔTK_{21}[6]	$34c$	$35c$
STK_{23} [3,7]	$13c$	Y_{22} [4,12], Y_{22} [1,5,9,13], X_{23} [2,6,10,14], Y_{22} [11,15],ΔTK_{21}[6]	$35c$	$36c$
STK_{23} [2,6]	$12c$	Y_{22} [4,12], Y_{22} [1,5,9,13], Y_{22} [2,6,14], Y_{22} [11,15],ΔTK_{21}[6]	$36c$	$37c$
-	$12c$	X_{22} [4,12], X_{22} [1,5,9,13], X_{22} [2,14], X_{22} [7,11,15],ΔTK_{21}[6]	-	-
STK_{22} [1,5]	$10c$	X_{22} [4,12], Y_{21} [5,13], X_{22} [2,14], X_{22} [7,11,15],ΔTK_{21}[6]	$36c$	$38c$
STK_{22} [7]	$9c$	X_{22} [4,12], Y_{21} [5,13], X_{22} [2,14], Y_{21} [3,7],ΔTK_{21}[6]	$36c$	$37c$
STK_{22} [2]	$8c$	X_{22} [4,12], Y_{21} [5,13], Y_{21} [14],Y_{21} [3,7],ΔTK_{21}[6]	$36c$	$37c$
STK_{22} [4]	$7c$	Y_{21} [8],Y_{21} [5,13],Y_{21} [14], Y_{21} [3,7],ΔTK_{21}[6]	$36c$	$37c$
-	$7c$	X_{21}[4], X_{21}[6,10,14], X_{21}[3,15],ΔTK_{21}[6]	-	-
STK_{21}[6]	$4c$	X_{21}[4],Y_{20} [6], X_{21}[3,15]	$34c$	$37c$
STK_{21}[3]	$3c$	X_{21}[4],Y_{20} [6],Y_{20} [15]	$34c$	$35c$
STK_{21}[4]	$3c$	Y_{20} [0],Y_{20} [6],Y_{20} [15]	$35c$	$35c$
-	$3c$	X_{20}[0,12], X_{20}[5]	-	-
STK_{20} [0]	$2c$	Y_{19} [12], X_{20}[5]	$35c$	$36c$
STK_{20} [5]	$2c$	Y_{19} [12],Y_{19} [1]	$36c$	$36c$
-	$2c$	X_{19} [1,13]	-	-
STK_{19} [1]	c	Y_{18} [13]	$36c$	$37c$
-	c	X_{18} [14]= Z_{17} [14]	-	-

[1] $c = 4$ if $n = 64$, or $c = 8$ if $n = 128$.