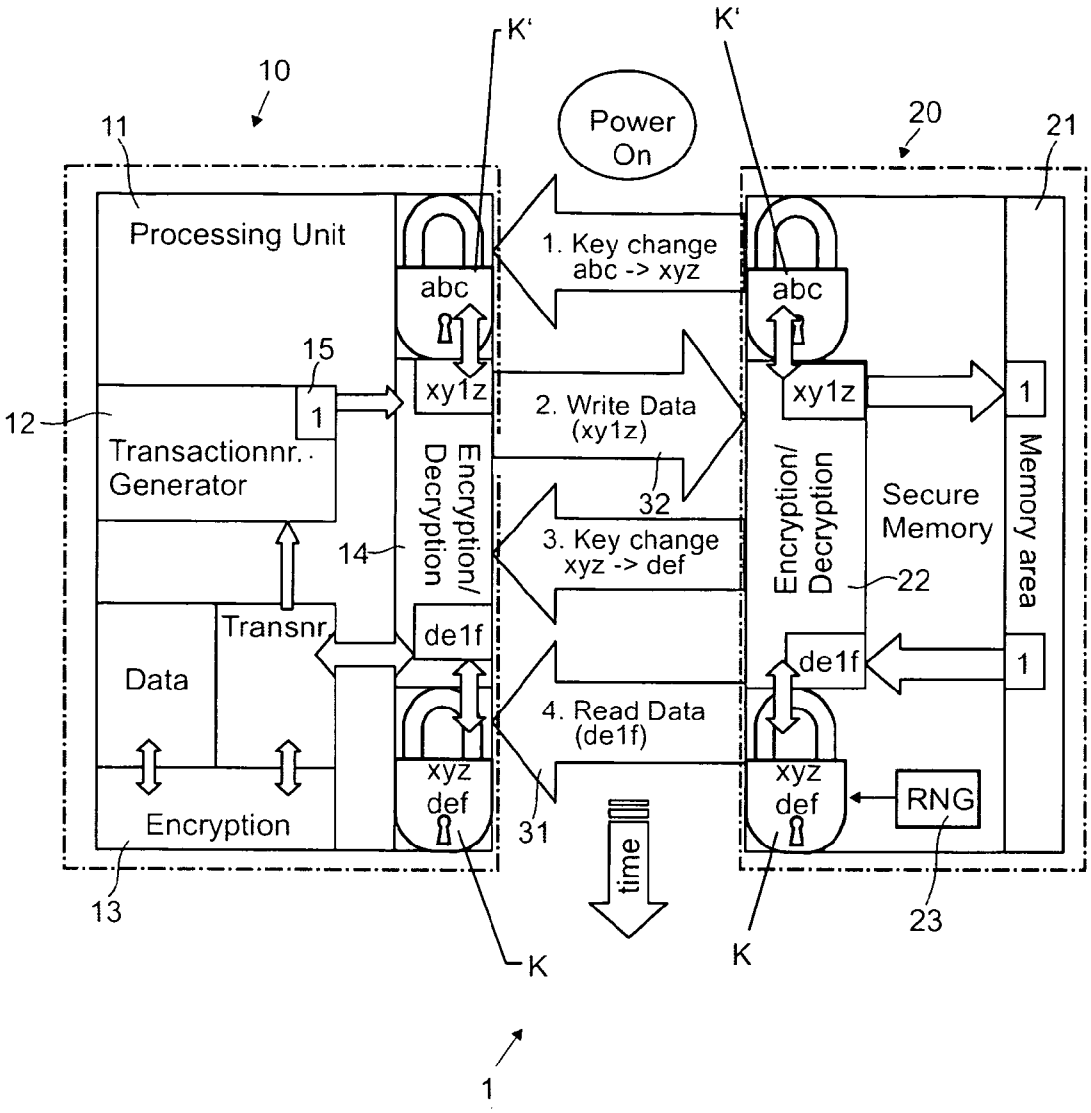
10
11
Processing Unit
12
15
1
Transactionnr. Generator
14
Transnr
Data
Encryption
13
K'
abc
xy1z
Encryption/ Decryption
de1f
xyz
def
K
Power On
1. Key change abc -> xyz
2. Write Data (xy1z)
32
3. Key change xyz -> def
4. Read Data (de1f)
31
time
1
20
21
abc
xy1z
Encryption/ Decryption
22
de1f
xyz
def
RNG
23
Secure Memory
Memory area
1

FIG. 1

step	Transaction number (Data)	Key processor	Communication line	Key Memory	Memory	
Power up	-	abc (default)		abc(default)	-	
Key change	-	xyz	axbycz ->	abc	-	
Key changed	-	xyz	-	xyz	-	
Data write	1	xyz	xy1z ->	xyz	1	
Key change	-	def	xdyezf ->	xyz	1	200
Key changed	-	def	-	def	1	
Data read	1	def	<- de1f	def	1	
Data write	2	def	de2f ->	def	2	
...	2 -> 10	...	...	...	10	
Power Down						
Power up		abc (default)	-	abc(default)	10	
Hacking		(ghi)	axbycz ->	abc	10	
Hacking		(ghi)	-	xyz	10	
Hacking		(ghi)	xy1z ->	xyz	1	
Hacking		(mno)	xdyezf ->	xyz	1	200
Hacking		(mno)	-	def	1	
Hacking	Invalid Data	mno	<- de1f	def	1	
Hacking		(mno)	de2f ->	def	2	
Power Down					2	
Power up		abc(default)		abc(default)	2	
	...	...	...	...	...	

FIG. 2

step	Transaction number (Data)	Key processor	Communication line	Key Memory	Memory	
Power up	-	abc (default)	-	abc (default)	10	
Key change	-	abc	<- axbycz	xyz	10	300
Key changed	-	xyz	-	xyz	10	
Data read	10	xyz	<- xy10z	xyz	10	
Data write	11	xyz	xy11z ->	xyz	11	
Key change	-	xyz	<- xdyezf	def	11	
Key changed	-	def	-	def	11	
Data read	11	def	<- de11f	def	11	
Data write	12	def	de12f ->	def	12	
...	12 -> 24	...	...	...	24	
Power Down						
Power up	-	abc (default)	-	abc (default)	24	
Hacking	-	abc	<- axbycz	(ghi)	24	300
Hacking		xyz	-	(ghi)	24	
Hacking	10	xyz	<- xy10z	(ghi)	24	
Hacking	11	xyz	xy11z ->	ghi	Invalid Data	

FIG. 3

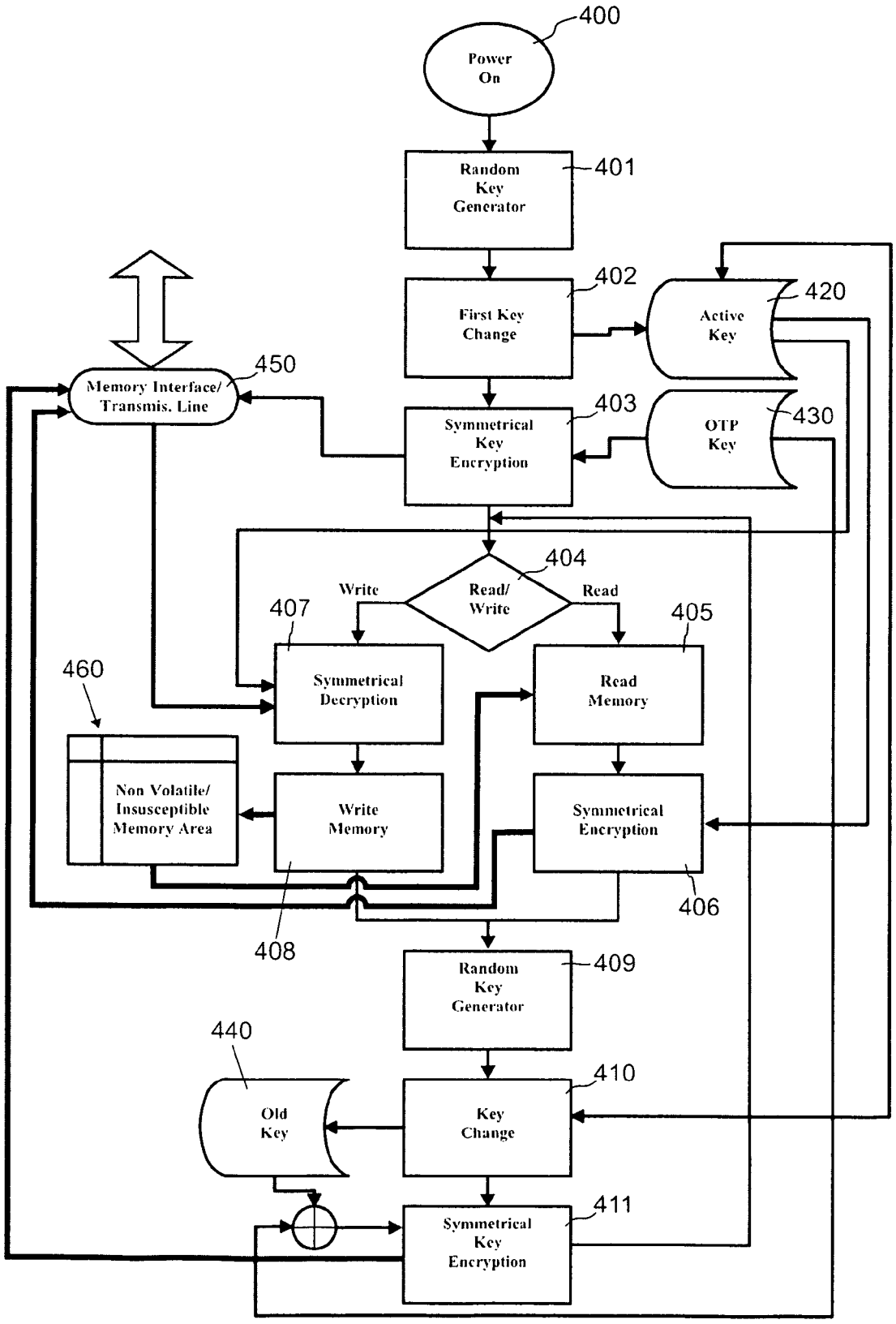
400
Power On
401
Random Key Generator
402
First Key Change
420
Active Key
450
Memory Interface/ Transmis. Line
403
Symmetrical Key Encryption
430
OTP Key
404
Read/ Write
Write
Read
407
405
460
Symmetrical Decryption
Read Memory
Non Volatile/ Insusceptible Memory Area
Write Memory
Symmetrical Encryption
406
408
409
Random Key Generator
440
410
Old Key
Key Change
411
Symmetrical Key Encryption

FIG. 4

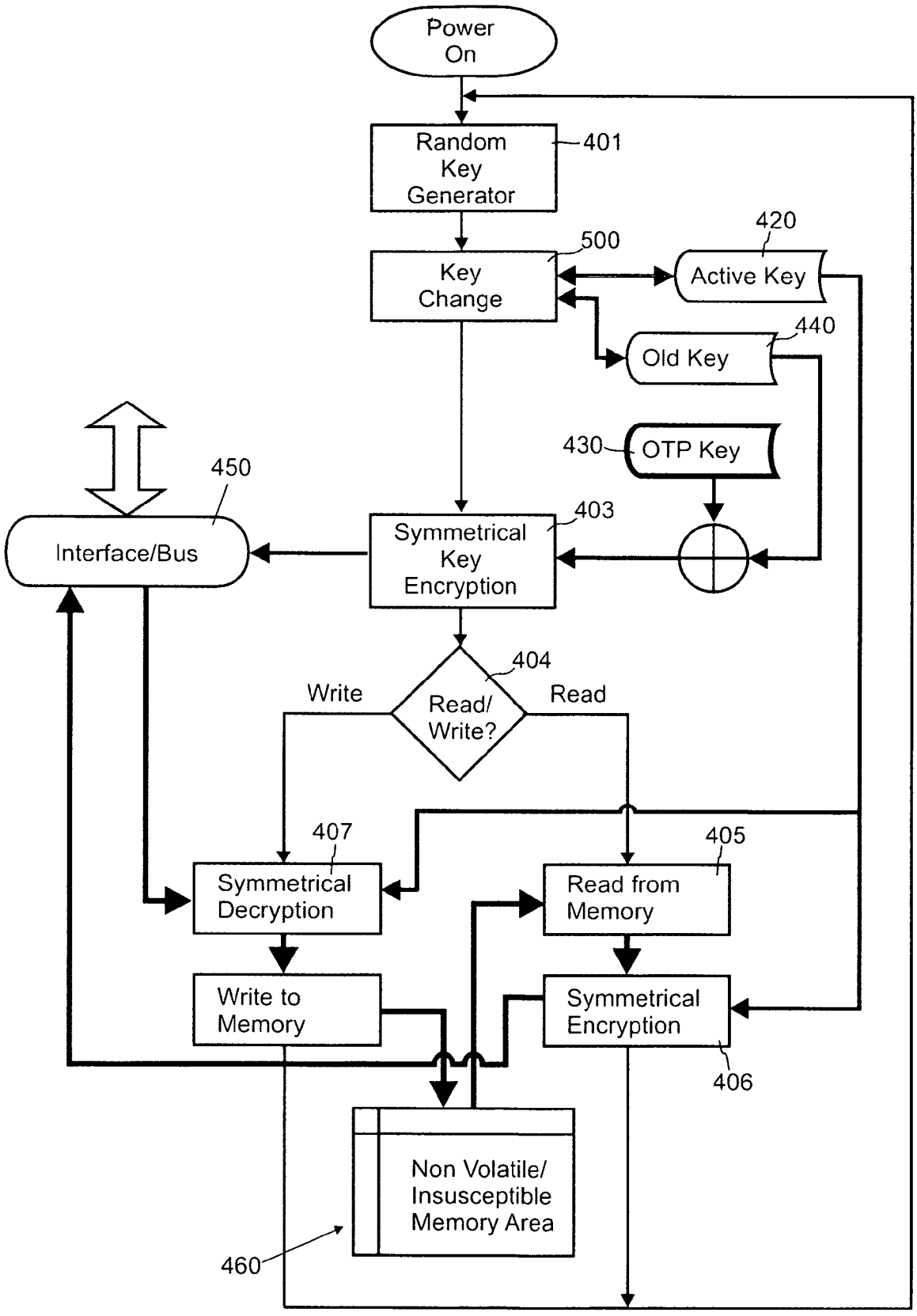
Power On
Random Key Generator
401
Key Change
500
Active Key
420
Old Key
440
OTP Key
430
Interface/Bus
450
Symmetrical Key Encryption
403
Read/ Write?
404
Write
Read
Symmetrical Decryption
407
Read from Memory
405
Write to Memory
Symmetrical Encryption
406
Non Volatile/ Insusceptible Memory Area
460

FIG. 5

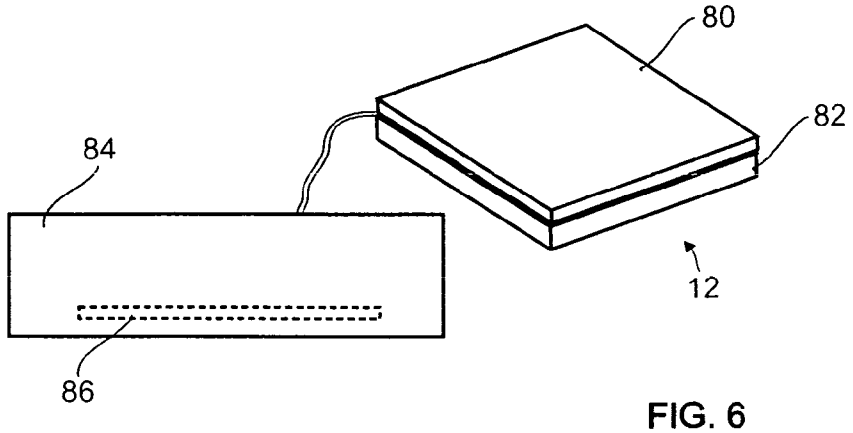
80
82
84
12
86

FIG. 6

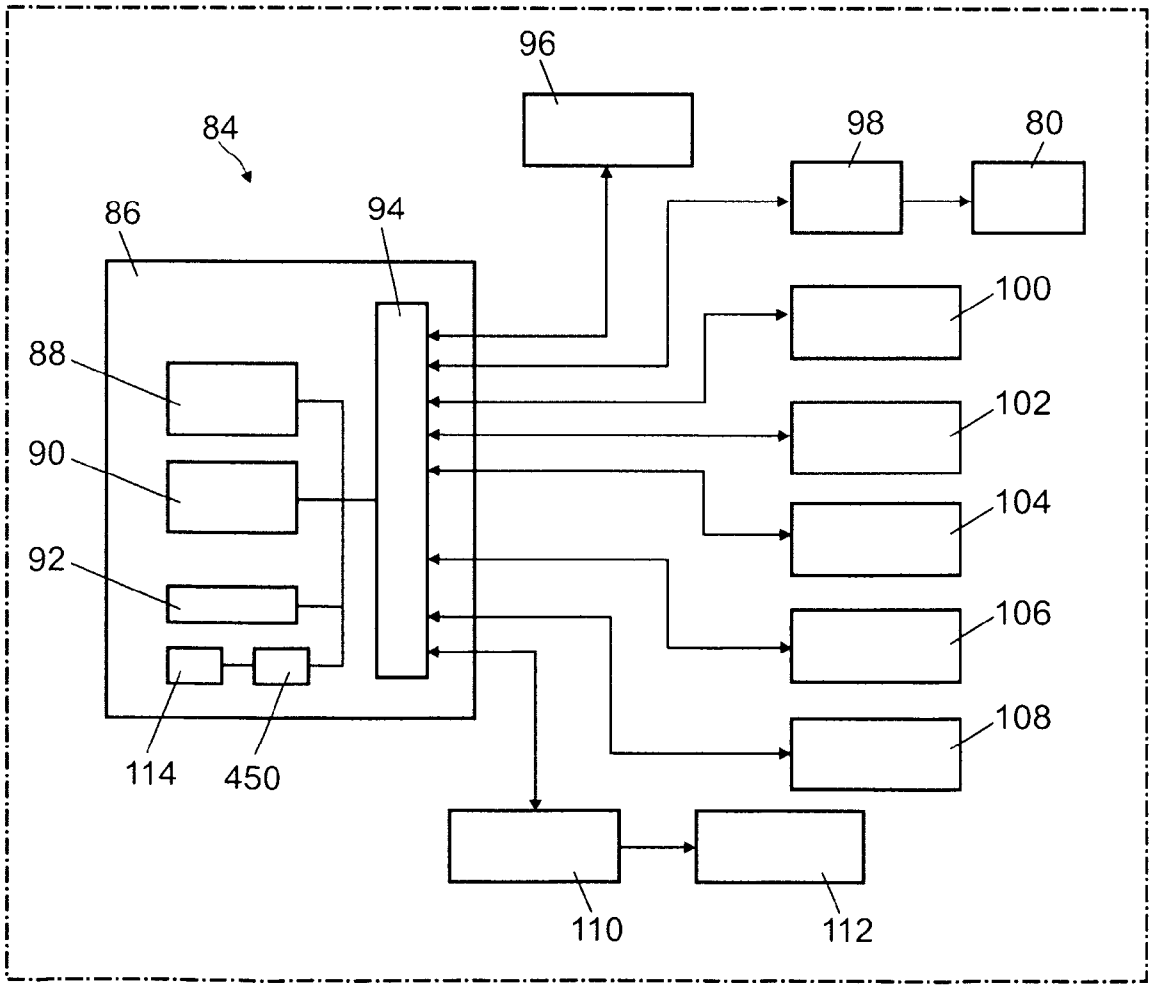
96
84
98
80
86
94
100
88
102
90
104
92
106
108
114
450
110
112

FIG. 7