

(11) (21) (C) **2,196,482**
(22) 1997/01/31
(43) 1997/09/28
(45) 2001/03/27

(72) Raghavachari, Partha, US

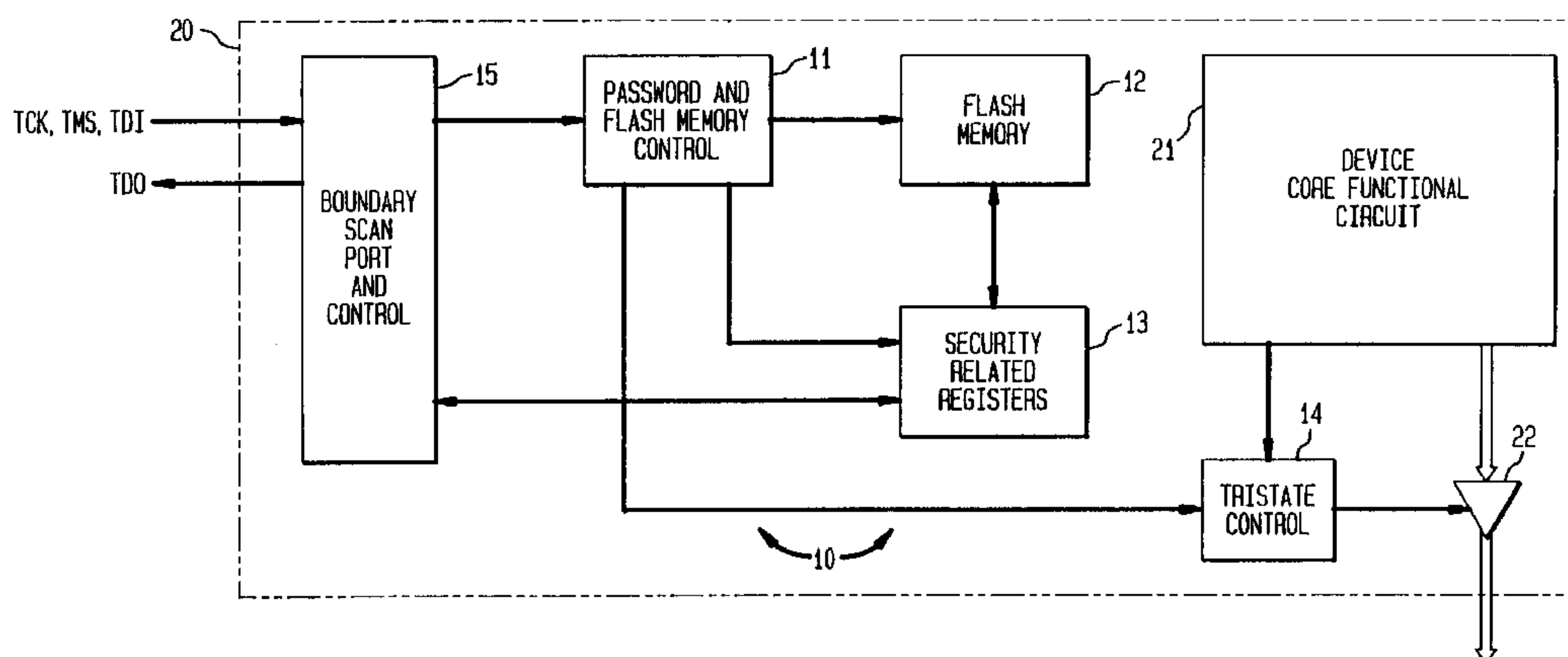
(73) LUCENT TECHNOLOGIES INC., US

(51) Int.Cl.⁶ G06F 12/14, G08B 31/00

(30) 1996/03/28 (623,271) US

(54) **METHODE ET MATERIEL POUR AMELIORER LA SECURITE
ET DIMINUER LE VOL DE COMPOSANTS VLSI ET ULSI**

(54) **METHOD AND APPARATUS FOR ENHANCING SECURITY IN
AND DISCOURAGING THEFT OF VLSI AND ULSI DEVICES**



(57) Les composants VLSI et ULSI comme les microprocesseurs et la mémoire DRAM sont sujets au vol à grande échelle dans les manufactures et les entrepôts. Une méthode proposée visant à réduire le vol consiste à incorporer une petite quantité de mémoire flash non volatile dans ces composants. La mémoire flash contient un mot de passe, le numéro de série, et l'information relative à l'utilisateur. À la mise sous tension, le composant déclenche une session de vérification du mot de passe crypté par une interface standard. Si le mot de passe fourni par l'utilisateur n'est pas le bon, les ports opérationnels du composant (tout bus de données ou de commande) est mis en état flottant, rendant ainsi le composant inutilisable. Le numéro de série et l'information relative à l'utilisateur sont utiles pour déterminer la propriété de composants volés quand ils sont retrouvés.

(57) VLSI and ULSI devices like microprocessors and DRAM devices are prone to large scale theft from factories and warehouses. A proposed method of reducing the theft incorporates a small amount of non-volatile flash memory in these devices. The flash memory contains password, device serial number and user identification information. On power-up, the device initiates an encrypted password verification session through a standard interface. If the user supplied password fails, the device's operational ports (any data or control output buses) are tri-stated, thus making the device unusable. The device serial number and user identification information are useful in determining ownership of stolen devices when recovered.

**METHOD AND APPARATUS FOR ENHANCING SECURITY IN AND
DISCOURAGING THEFT OF VLSI AND ULSI DEVICES**

5

ABSTRACT OF THE DISCLOSURE

VLSI and ULSI devices like microprocessors and DRAM devices are prone to large scale theft from factories and warehouses. A proposed method of reducing the theft incorporates a small amount of non-volatile flash memory in these devices. The flash memory contains password, device serial number and user identification information. On power-up, the device initiates an encrypted password verification session through a standard interface. If the user supplied password fails, the device's operational ports (any data or control output buses) are tri-stated, thus making the device unusable. The device serial number and user identification information are useful in determining ownership of stolen devices when recovered.

**METHOD AND APPARATUS FOR ENHANCING SECURITY IN AND
DISCOURAGING THEFT OF VLSI AND ULSI DEVICES**

5

FIELD OF THE INVENTION

This invention relates to integrated circuit devices, and more particularly to a method and apparatus for protecting large scale integrated devices from theft.

10

BACKGROUND OF THE INVENTION

Integrated circuit devices such as microprocessors and memory chips are becoming more and more powerful, and thus more complex. Such devices, which routinely contain circuits with millions of transistors, are classified as Very Large Scale Integrated (VLSI) or Ultra Large Scale Integrated (ULSI) devices. The cost of these devices depends on several factors including device complexity, usefulness, and demand. For example, high density Dynamic Random Access Memory (DRAM), which can reach capacity levels of 64 megabits in a single chip, can cost up to several hundred dollars per device.

A big problem faced by manufacturers of high priced microprocessor and memory devices is theft. Since these devices are so small in size, a large number can be easily stolen at one time. For example, a shoe box full of these devices, worth several thousand dollars, can be easily concealed and transported without notice. In fact, there have been numerous reports of armed gangs robbing such high-priced silicon devices

from device manufacturers' foundries and warehouses. It is estimated that the monetary value of these losses runs into the tens of millions of dollars annually.

Heretofore, there are no known methods or devices that have been implemented to reduce or eliminate the theft associated with such large scale high-priced devices.

5 Moreover, since the stolen devices do not contain serial numbers, their ownership is very difficult to trace and they are easily absorbed into the consuming market.

SUMMARY OF THE INVENTION

Accordingly, the present invention is directed to a method and apparatus for
10 substantially reducing theft losses associated with large scale integrated devices, and providing a means for tracing ownership of stolen devices when recovered. To attain this, the present invention provides a built-in security mechanism that disables the functionality of the device until a random security challenge is met and a password is supplied upon device power up. In addition, the present invention provides a built-in
15 ownership log that can be accessed upon meeting the random security challenge and supplying the password to trace ownership of that device. As a result, a device having the security mechanism of the present invention is rendered substantially useless to those who can not meet the random security challenge and supply the password, namely thieves.

20 In general, the built-in security mechanism provides a non-volatile facility (in the form of flash memory) for storing a reprogrammable password and other user information on the device. Moreover, upon each power-up of the device, the security

mechanism provides a security clearance session that issues a random challenge to the external source or medium trying to access or use the device. As a result, unless the external source can meet the random challenge and supply the password, the device remains locked and thus unusable.

5 In one embodiment of the invention, the security mechanism also provides a built-in ownership log in the non-volatile memory facility. As a result, upon meeting the random challenge and supplying the password, the security mechanism enables the remote source to access and reprogram the user and manufacturer information, as well as reprogram the password. Moreover, since the ownership log maintains user
10 information and manufacturer information between power-ups, the security mechanism can provide information that is useful to determine the owner of a stolen device, when recovered. Thus, the present invention overcomes, to a large extent, the limitations associated with the prior art.

 In accordance with one aspect of the present invention there is provided a large
15 scale integrated device having a core functional circuit and at least one output port, said device comprising: a security mechanism; a controller to control the operation of the security mechanism; a boundary scan port electrically coupled to said controller, said boundary scan port providing an interface between the security mechanism and an external medium; a flash memory electrically coupled to said controller, said flash
20 memory providing the security mechanism with non-volatile storage of predetermined information and data; a set of security registers for providing functional support to said controller, said security registers electrically coupled to said flash memory, said

A

3a

controller and said boundary scan port; and tristate control logic for providing said controller with functional control over the core functional circuit and the output ports of the large scale integrated device, said tristate logic control electrically coupled to said controller, the core functional circuit and output ports of the device.

5 In accordance with another aspect of the present invention there is provided a method of protecting large scale integrated devices from theft, the large scale integrated devices having a core functional circuit and output ports, the method comprising the steps of: entering into a security session between a security mechanism and an external medium to protect unauthorized access to the core functional circuit and the output
10 ports from said external medium; and controlling access to the core functional circuit and the output ports through tristate control logic by verifying a requested password from said external medium.

 These and other features of the invention are described in more complete detail in the following detailed description of embodiments of the invention when taken with
15 the drawings. The scope of the invention, however, is limited only by the claims appended hereto.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a device having one embodiment of the security mechanism of the present invention.

A

Fig. 2 is a pictorial view of the non-volatile flash memory organization of the embodiment shown in Fig. 1.

Fig. 3 is a block diagram of the security related registers of the embodiment shown in Fig. 1.

5 Fig. 4 is a block diagram of the random challenge registers of the embodiment shown in Fig. 1.

Fig. 5 is a block diagram of the boundary scan port of the embodiment shown in Fig. 1.

Fig. 6 is a block diagram of the interaction between security related registers and
10 a security data dialog register of the embodiment shown in Fig. 1.

Fig. 7 is a state diagram of the test access port controller in the boundary scan port of the embodiment shown in Fig. 1.

Fig. 8 is a block diagram of the password and non-volatile memory control circuit of the embodiment shown in Fig. 1.

15 Fig. 9 is a flow chart of the controller circuit actions for various requests from the external medium.

Fig. 10 is a block diagram of a linear feedback shift register that performs polynomial division.

20 **DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION**

Referring now to Fig. 1 there is shown a large scale integrated device or device
20 having one embodiment of a built-in security mechanism 10 according to the present

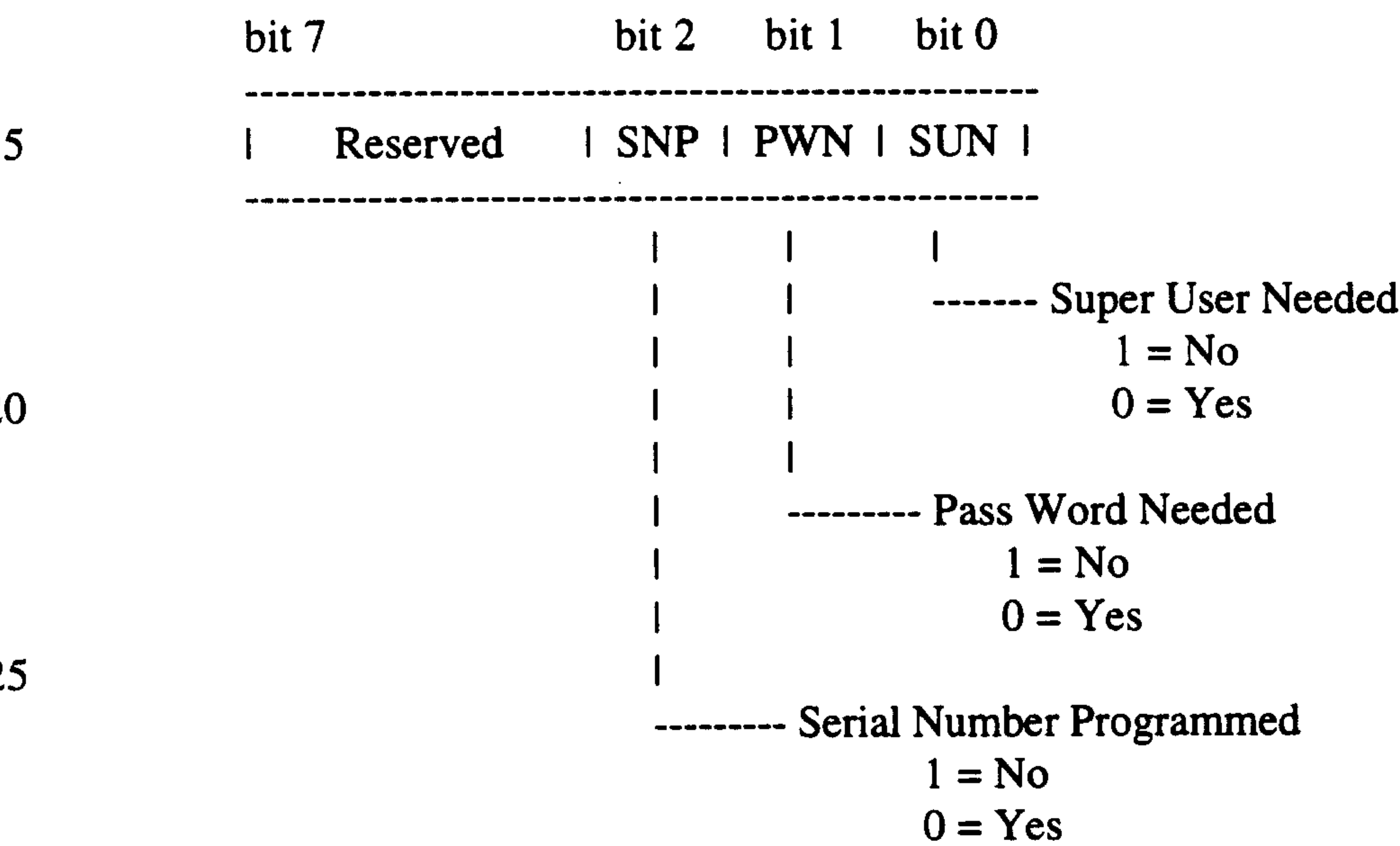
invention. As shown, security mechanism 10 has a password and flash memory control or controller 11 that is electrically connected to flash memory 12, security registers 13, tri-state control 14 and boundary scan port and control 15. Boundary scan port and control 15 is electrically connected to security registers 13 and an external interface (not shown). Flash memory 12 is electrically connected to security registers 13. Tri-state control 14 is electrically connected to the core functional circuit 21 of device 20 and device output ports 22. Core functional circuit 21 is the main feature of device 20. For example, core functional circuit 21 may be a microprocessor circuit or a DRAM memory circuit.

10 In operation, controller 11 interprets commands sent by the external medium (not shown), manages flash memory 12 and security registers 13, verifies the password supplied by the external medium for unlocking the device, supplies the external medium with data (device serial number, user identification information, etc.) after verifying the authenticity of the request for that data, and controls output ports 22 of core functional
15 circuit 21 through tri-state logic 14. Flash memory 12 contains information such as password, device serial number, user identification information, random security challenge, security session status and failure information. Flash memory 12 provides the ability to save the stored information between power-ups and provides the ability to change the stored information without having to remove the memory from a system
20 board, as required by EEPROM memory.

Controller 11 uses security registers 13 to perform its several functions as listed above. In addition, security registers 13 maintain portions of data stored in flash

memory 12, and data required in an exchange between flash memory 12 and the external medium (not shown). Boundary scan port and control 15 facilitates dialog between the external medium (not shown) and the security mechanism 10 during a security clearance session. Basically, boundary scan port and control 15 provides an interface between an external medium (not shown) and controller 11. Fig.'s 2-10 give a more detailed view of the above described functional parts of security mechanism 10.

Referring now to Fig. 2 there is shown one embodiment of flash memory 12. As shown, flash memory 12 contains 128 bytes of data, wherein the default value of all the bits in an unprogrammed flash memory at the time of manufacture is a logic 1. Byte 0 of the flash memory 12 contains security status bits. The following diagram shows the layout of this byte:



Bit 0 tells controller 11 whether a super user access is needed to unlock device 20. This bit may be set when the number of failed unlocking attempts exceeds a failure

threshold. Bit 1 tells controller 11 whether a password security session is needed to unlock device 20, and Bit 2 tells controller 11 whether a serial number has been programmed into device 20. Note that the unprogrammed values of these bits correspond to a security unprotected device.

5 The next byte, Byte 1, of flash memory 12 contains the security failure threshold value. As a result, the failure threshold value could be from 0 to 255. Thus, if this byte is programmed to a value k, controller 11 will permit up to k consecutive failed unlocking attempts before requiring a super user intervention. The next byte, Byte 2, of flash memory 12 contains the number of consecutive failed unlocking attempts. Thus, at
10 the conclusion of a successful unlocking session, controller 11 resets this byte to a count of 0.

 Bytes 3 through 47 are assigned to store user identification information. This could be the user's name, social security number, etc. This information may be represented using the ASCII character set which uses a byte of memory for each
15 character. Thus, using the ASCII character set, the user identification information could contain up to 45 characters.

 Bytes 48 through 63 contain the security password information. As a result, the password information is 128 bits wide. Bytes 64 through 95 are used for assigning a serial number to device 20. These 32 bytes could also be represented using the ASCII
20 character set. And finally, bytes 96 through 127 contain the random security challenge. As described above, the contents of these 32 bytes for the random security challenge will

Referring now to Fig. 3 there is shown a block diagram of security registers 13. As shown, registers 13 are a collection of working registers. Controller 11 uses these registers to perform some of its various functions listed above. Security registers 13 include a status register 31 that contains status information about the security session. Status register 31 may be accessed in a read-only mode by the external medium (not shown). As a result, the external medium cannot modify the contents of register 31. Rather, controller 11 writes the different bits of register 31. The following diagram shows the layout of register 31:

	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0	
	RDY	CPF	SUF	UIF	PWF	SNP	PWN	SUN	
15									
									----- Super User Needed
									1 = No
									0 = Yes
20									
									----- Pass Word Needed
									1 = No
									0 = Yes
25									
									----- Serial Number Programmed
									1 = No
									0 = Yes
30									
									----- Pass Word Failure
									1 = Password OK/not tried
									0 = Password failed
									----- User Identification Failure
									1 = Session to change user identification
									successful/not tried

				0 = Session to change user identification failed
			-----	Super User Failure
				1 = Superuser password OK/not tried
5				0 = Superuser password failed
			-----	Change Password Failure
				1 = Session to change user password successful/not tried
				0 = Session to change user password failed
10				
			-----	Ready
				1 = Security Control Circuit is ready
				0 = Security Control Circuit is busy
15				
				Bits 0, 1 and 2 are the same as bits 0, 1 and 2 in byte 0 of flash memory 12. Bit 3
				gives an indication of the pass/fail status of a password unlocking session to the external
				medium. Bit 4 indicates the pass/fail status of a session to modify the user identification
				information in flash memory 12. Bit 5 indicates the pass/fail status of a session needing a
				superuser to unlock device 20. Bit 6 indicates the pass/fail status of a session to change
20				the user password in flash memory 12.

Bit 7 indicates the ready/busy status of controller 11. On power-up, bit 7 is reset to a value of logic 0. As a result, after power-up, controller 11 loads registers 13 from flash memory 12 sets Bit 7 to a logic 1, indicating its ready status. Thus, if controller 11 is busy, it will ignore any commands from the external medium requiring its attention.

25 For instance, after a successful password session, the external medium may want to read the user identification information in the flash memory. Since, during this period, controller 11 takes time to access flash memory 12, the ready bit will be set to a logic 0. As a result, the external medium needs to read this bit to guarantee that the user identification information is valid.

Also shown in Fig. 3 is security command register 32. Command register 32 contains information about what action that external medium (not shown) desires of controller 11. The external medium writes these commands into register 32. The following table shows the commands supported thereby:

5

10

15

20

25

30

security command	Definition
register CR[7:0]	
(value in hex)	

00H	Idle/Reset
01H	Password unlocking session request
02H	Password change session request
03H	Device serial number change
	session request
04H	Failure threshold change session
	request
05H	User identification information
	change session request
06H	Device serial number (low) read
	session request
07H	Device serial number (high) read
	session request
08H	User identification information (one)
	read session request
09H	User identification information (two)
	read session request
0AH	User identification information
	(three) read session request
0BH	Password security disable session
	request
0CH through FFH	Reserved

35

Also shown in Fig. 3 is failure threshold register 33 and failure count register 34. Failure threshold register 33 is identical to byte 1 in the flash memory, whereas failure count register 34 is loaded from byte 2 of flash memory 12 at the beginning of a power-

up session as an initial failure count. Basically, the number of failed password unlocking attempts for the current session is added to the initial value in failure count register 34. As a result, every time register 34 is updated, byte 2 of flash memory 12 is also updated.

Also shown, is a device password register 35. Device password register 35
5 contains the 128 bits of password information. At the beginning of each power-up session, the contents of bytes 48 through 63 of flash memory 12 are copied into device password register 35 so that any successful modification of the password is also copied into register 35.

Also shown is random challenge register 36 which contains the random challenge
10 information. Basically, at the beginning of each power-up session, the contents of bytes 96 through 127 of flash memory 12 are copied into register 36. As a result, each password unlocking session updates random challenge register 36. Thus, random challenge register 36 is essentially a Linear Feedback Shift Register (LFSR) which produces all possible bit patterns (except the all 0's bit pattern) before it repeats a
15 pattern. This is achieved by tapping selected bit positions of register 36 and feeding them to an exclusive-OR tree 41 shown in Fig. 4. The output of tree 41 is fed back to the shift input of register 36. As shown in Fig 4, random challenge register 36 has a circuit 42 that provides LSFR capability. In operation, mode control signal 45 determines if data is recirculated in register 36 or if a new bit pattern is loaded therein.

20 Finally, Fig. 3 shows a temporary data register 37 as part of security registers 13. Temporary data register 37 acts as a conduit between the external medium and flash memory 12. Basically, temporary data register 37 is used for updating password and

user identification information in flash memory 12, and to read device 20's serial number and user identification information from flash memory 12.

Referring now to Fig. 5, there is shown a block diagram of boundary scan port 15 containing a Test Access Port (TAP) controller 51, an instruction register 52, an instruction decoder 53, a device bypass register 54 and a boundary scan register 55 which are all required by the IEEE 1149.1 interface standard. An additional register, security dialog data register 56, provides secure dialog between the external medium (not shown) and device 20. Security dialog data register 56 is a 128 bit wide register which handles any data exchange between the external medium (not shown) and security registers 13, or between the external medium and flash memory 12.

Instruction register 52 controls the access of various registers in mechanism 10 during the boundary scan mode. Through the IEEE 1149.1 standard, this access requires a basic set of instructions including extest, sample and bypass. To facilitate the dialog between the external medium and security registers 13, however, some additional instructions have been defined. Namely, a boundary scan instruction register that is 5 bits wide is proposed with the following additional boundary scan instructions.

20	-----		
	Instruction	Definition	
	Register		
	IR[4:0]		
25	-----		
	00000	extest	
	00001	select bypass register	
	0001x	sample	
	00100	write failure threshold register	
	00101	read failure threshold register	
	00110	read failure count register	
	00111	select bypass register	

	01xxx	select bypass register	
	10000	read security status register	
	10001	write security command register	
	10010	read random security challenge register(low)	
5	10011	read random security challenge register(high)	
	10100	write security password register	
	10101	write device serial number register(low)	
	10110	write device serial number register(high)	
	10111	read device serial number register	
10	11000	select bypass register	
	11001	write user ID information register(one)	
	11010	write user ID information register(two)	
	11011	write user ID information register(three)	
	11100	read user ID information register	
15	11101	select bypass register	
	11110	select bypass register	
	11111	select bypass register	

20 note: x = don't care

Referring now to Fig. 6, there is shown the interaction between security dialog data register 56 and security registers 13 that are necessary to implement the read and write instructions in the table above. Since the device serial number and user identification information are not always stored in security registers 13, they are stored in temporary data register 37 on demand. Thus, a write operation from the external medium to a device serial number register stores the data in temporary data register 37 from which it is transferred to flash memory 12. Similarly, a request by the external medium to read the user identification information causes a data transfer from flash memory 12 to temporary data register 37, from which the data is transferred to the external medium (not shown).

Referring now to Fig. 7 there is shown one embodiment of Test Access Port (TAP) controller 70 in boundary scan port 15. As shown, Fig. 7 illustrates the operation of the read and write instructions during the boundary scan mode. To illustrate, consider the instruction "write security command register" (code 10001). To execute this

5 instruction, the external medium has to follow these steps:

1. Put the TAP controller in the test-logic-reset state.
2. Traverse through the states (run-test-idle -> select-DR-scan -> select-IR-scan -> capture-IR -> shift-IR -> exit1-IR -> update-IR) to load the instruction register with the code 10001. The five bit code is shifted into the instruction
10 register in the shift-IR state.
3. Traverse through the DR shift portion of the TAP controller to write the data in the security command register. This step requires traversing the states (select-DR-scan -> capture-DR -> shift-DR -> exit1-DR -> update-DR -> run-test-idle). The
15 eight bits of data to be written to the security command register are shifted in through the TDI lead in the shift-DR state. The least significant bit of data is shifted in first in this state.

In step 3, the data is shifted into the security dialog data register in the shift-DR state. In
20 the update-DR state, the contents of the security dialog data register are transferred to the security command register. Note that the security dialog data register is chosen automatically during the DR shift states for all the read and write boundary scan instructions.

To compare instructions consider the instruction "read device serial number
25 register"(code 10111). To execute this instruction, the external medium has to follow these steps:

1. Put the TAP controller in the test-logic-reset state.
2. Traverse through the states (run-test-idle -> select-DR-scan -> select-IR-scan -> capture-IR -> shift-IR -> exit1-IR -> update-IR) to load the instruction

register with the code 10111. The five bit code is shifted into the instruction register in the shift-IR state.

5 3. Traverse through the DR shift portion of the TAP controller to read the device serial number register. This step requires traversing the states (select-DR-scan -> capture-DR -> shift-DR -> exit1-DR -> update-DR -> run-test-idle). The thirty two bits of data to be read are loaded into the security dialog data register from the temporary data register in the capture-DR state. In the shift-DR state, the contents of the security dialog data register are shifted out through the TDO lead.

10

Referring now to Fig. 8, there is shown a block diagram of one embodiment of controller 11. As shown, controller 11 has combination logic 81 electrically connected to state machine flip-flops 82 which, in turn is electrically connected to combination logic 83. From these devices, controller 11 decodes a request from the external medium in the security command register of registers 13, monitors the sequence of write and read operations of the external medium for each request, controls the address and data ports to the flash memory, controls the read and write operations of various security related registers, and controls the tri-state control of device output ports 22. Figure 9 shows a detailed flow chart of the actions taken by controller 11 for various requests from the external medium.

20

As described above, during each security clearance session, the external medium needs to compute a function $f(\text{password}, \text{random challenge})$. To test the validity of the external medium's computation, controller 11 computes this same function. One way to implement this function is by using LFSR and polynomial division. A circuit for LFSR and polynomial division is illustrated in Fig. 10, herein after referred to as LFSR 101. As shown, LFSR 101 consists of flip-flops 102, exclusive-OR gates 103 and constant multipliers 104. For the constant 1, a connection is made for constant multipliers 104,

25

whereas for the constant 0 there is no such connection. Since a serial input stream into LFSR 101 is a polynomial, LFSR 101 has its characteristic polynomial defined by the constants $C_0, C_1, \dots, C_r$.

LFSR 101 divides any input polynomial by the characteristic polynomial and
5 leaves the remainder in the circuit. If we assume the characteristic polynomial as being defined by the password and the input polynomial as being defined by the random challenge bit stream, then the remainder in the LFSR circuit 101 is the function $f(\text{password}, \text{random challenge})$. Some of the various algorithms for password unlocking, changing user identification information and reading the device serial number and user
10 identification information is described below.

In operation, all actions during a security dialog session are initiated by the external medium. Thus, device 20 responds to these commands as a slave. The general sequence of events for various operations includes: (1) writing from the external medium to the security command register with a request to indicate the action desired of
15 controller 11; and (2) stepping through a sequence of register read and write instructions defined in the boundary scan instruction register. The following table shows the sequence of events, in chronological order, between the external medium and controller 11 for various operations:

20	-----		
		Password Unlocking Session	

		External Medium Action	Device Password Control Action

		Read security status register	
25		to ensure device security	
		control circuit is ready.	

5			
	Write security command		
	register with a password		
10	unlock request.		
15	Read random security challenge		
	register (low).		
20	Read random security challenge		
	register (high).		
25	Compute f(password, challenge)		
	and write it in security		
	password register.		
20		Compare contents of security	
		password register with computed	
		value. Indicate pass/fail status	
20		in security status register.	
		Update random challenge, failure	
		count, etc.	
25			
	Read security status register		
	to check password pass/fail		
25	status.		

	Password Change Session	

	External Medium Action	Device Password Control Action

5	Write security command	
	register with a password	
	change request.	
10	-----	
	Execute a password unlocking session for existing password.	

	Read security status register	
	to ensure device security	
15	control circuit is ready.	

	Read random security challenge	
	register (low).	

20	Read random security challenge	
	register (high).	

	Compute f(password, challenge)	
	and write it in security	
25	password register.	

		Compare contents of security
		password register with computed
		value. Indicate pass/fail status
30		in security status register.
		Update random challenge, failure
		count, etc.

	Change existing password	

35	Write security password	
	register with new password.	

	Write security password	
40	register a second time with	
	new password.	

		Check for password consistency.
		Update device password register,

		failure count, flash memory,	
		security status register, etc.	

5	Read security status register		
	to check password change		
	pass/fail status.		

10	Device Serial Number Change Session		

	External Medium Action	Device Password Control Action	

15	Read security status register		
	to ensure device security		
	control circuit is ready.		

20	Write security command		
	register with a serial number		
	change request.		

	Write device serial number		
	register (low).		

25	Write serial number register		
	(low) to flash memory.		

30	Read security status register		
	to ensure device security		
	control circuit is ready.		

	Write device serial number		
	register (high).		

35	Write serial number register		
	(high) to flash memory.		

40	Update flash memory and security		
	status register.		

	Failure Threshold Change Session	

5	External Medium Action	Device Password Control Action

	Write security command	
	register with a failure	
	threshold change request.	
10	-----	
	Execute a password unlocking session for existing password.	

	Read security status register	
	to ensure device security	
15	control circuit is ready.	

	Read random security challenge	
	register (low).	

20	Read random security challenge	
	register (high).	

	Compute f(password, challenge)	
	and write it in security	
25	password register.	

		Compare contents of security
		password register with computed
		value. Indicate pass/fail status
30		in security status register.
		Update random challenge, failure
		count, etc.

	Change Failure Threshold	
35	-----	
	Write failure threshold	
	register with new value.	

		Write new threshold value to
40		flash memory.

User Identification Change Session	
5	External Medium Action Device Password Control Action
10	Write security command register with a user ID change request.
15	Read security status register to ensure device security control circuit is ready.
20	Read random security challenge register (low).
25	Read random security challenge register (high).
30	Compute $f(\text{password}, \text{challenge})$ and write it in security password register.
35	Compare contents of security password register with computed value. Indicate pass/fail status in security status register. Update random challenge, failure count, etc.
40	Change User Identification
45	Write user ID information register (one).
50	Write user ID information register (one) to flash memory.
55	Read security status register to ensure device security

	control circuit is ready.		

	Write user ID information		
	register (two).		
5	-----		
		Write user ID information	
		register (two) to flash memory.	

10	Read security status register		
	to ensure device security		
	control circuit is ready.		

	Write user ID information		
	register (three).		
15	-----		
		Write user ID information	
		register (three) to flash memory.	

20		Update flash memory and security	
		status register.	

25		Device Serial Number Read Session	

	External Medium Action	Device Password Control Action	

30	Write security command		
	register with a device serial		
	number read request.		

		Load device serial number	
		(high or low) into temporary	
		data register.	
35	-----		
	Read security status register		
	to ensure device security		
	control circuit is ready.		

40	Read device serial number		
	register.		

	User Identification Read Session		

	External Medium Action	Device Password Control Action	
5	-----		
	Write security command		
	register with a user ID		
	read request.		

10	Execute a password unlocking session for existing password.		

	Read security status register		
	to ensure device security		
	control circuit is ready.		
15	-----		
	Read random security challenge		
	register (low).		

	Read random security challenge		
20	register (high).		

	Compute f(password, challenge)		
	and write it in security		
	password register.		
25	-----		
		Compare contents of security	
		password register with computed	
		value. Indicate pass/fail status	
		in security status register.	
30		Update random challenge, failure	
		count, etc.	

	Read User Identification		

35		Load user identification	
		information (one or two or three)	
		into temporary data register.	

	Read security status register		
40	to ensure device security		
	control circuit is ready.		

	Read user ID information		
	register.		

	Password Security Disable Session	
5	-----	
	External Medium Action	Device Password Control Action

	Write security command	
	register with a password	
10	security disable request.	

	Execute a password unlocking session for existing password.	

	Read security status register	
15	to ensure device security	
	control circuit is ready.	

	Read random security challenge	
	register (low).	
20	-----	
	Read random security challenge	
	register (high).	

	Compute f(password, challenge)	
25	and write it in security	
	password register.	

		Compare contents of security
		password register with computed
30		value. Indicate pass/fail status
		in security status register.
		Update random challenge, failure
		count, etc.

35	Disable Password Security	

		Update flash memory and security
		status register.

40

Note, the superuser unlocking session requires an unadvertised encoding (OCH to FFH) in the security command register. This encoding is known only to the device

2196482

25

manufacturer. As a result, the superuser unlocking sequence is hardwired into device 20.

For instance, the sequence may be a finite sequence of write operations containing definite data patterns to the security dialog data register. Thus, the superuser unlocking session may be performed by either the manufacturer or a third party working on behalf

5 of the manufacturer.

Claims:

1. A large scale integrated device having a core functional circuit and at least one output port, said device comprising:

a security mechanism;

5 a controller to control the operation of the security mechanism;

a boundary scan port electrically coupled to said controller, said boundary scan port providing an interface between the security mechanism and an external medium;

a flash memory electrically coupled to said controller, said flash memory providing the security mechanism with non-volatile storage of predetermined

10 information and data;

a set of security registers for providing functional support to said controller, said security registers electrically coupled to said flash memory, said controller and said boundary scan port; and

15 tristate control logic for providing said controller with functional control over the core functional circuit and the output ports of the large scale integrated device, said tristate logic control electrically coupled to said controller, the core functional circuit and output ports of the device.

2. The device of claim 1 wherein said controller includes combinational logic and state machine flip-flops to interpret commands sent by said external medium, manage
20 said flash memory and said security registers, verify passwords for unlocking the

A

device, supply said external medium with said predetermined data, and control the output ports of the core functional circuit through said tristate logic.

3. The device of claim 1 wherein said flash memory provides 128 bytes of memory to store said predetermined information and data, each said byte being eight bits wide
5 and having a separate location address, wherein the first byte is location address 0 and the last byte is location address 127.

4. The device of claim 3 wherein said predetermined information and data includes user identification information, a password, a device serial number, a random security challenge, security session status information, and failure information.

10 5. The device of claim 4 wherein said security status information is stored in location address 0, said failure information is stored in location addresses 1 and 2, said user identification is stored in location addresses 3-47, said password is stored in location addresses 48-63, said serial number is stored in location addresses 64-95, and said random security challenge is stored in location addresses 96-127.

15 6. The device of claim 4 wherein said random security challenge is a test, wherein said test requires said external medium to return a value at the beginning of each power-up of the device to unlock the device.

7. The device of claim 1 wherein said security registers include a security status register, a security command register, a failure threshold register, a failure count register, a device password register, a random challenge register, and a temporary data register.

5 8. The device of claim 1 wherein said boundary scan port further comprises a test access port controller, an instruction register, an instruction decoder, a device bypass register and a boundary scan register.

9. A built-in security mechanism for a large scale integrated device, the device having a core functional circuit and output ports, the security mechanism comprising:

10 a controller to control the operation of the security mechanism;

a boundary scan port electrically coupled to said controller, said boundary scan port providing an interface between the security mechanism and an external medium;

a flash memory electrically coupled to said controller, said flash memory providing the security mechanism with non-volatile storage of predetermined

15 information and data;

a set of security registers for providing functional support to said controller, said security registers electrically coupled to said flash memory, said controller and said boundary scan port; and

A

tristate control logic for providing said controller with functional control over the core functional circuit and the output ports of the large scale integrated device, said tristate logic control electrically coupled to said controller and the core functional circuit and output ports of the device to prevent unauthorized use thereof.

5 10. The device of claim 9 wherein said controller includes combinational logic and state machine flip-flops to interpret commands sent by said external medium, manage said flash memory and said security registers, verify passwords for unlocking the device, supply said external medium with said predetermined data, and control the output ports of the core functional circuit through said tristate logic.

10 11. The device of claim 10 wherein said flash memory provides 128 bytes of memory to store said predetermined information and data, each said byte being eight bits wide and having a separate location address, wherein the first byte is location address 0 and the last byte is location address 127.

15 12. The device of claim 11 wherein said predetermined information and data includes user identification information, a password, a device serial number, a random security challenge, security session status information, and failure information.



13. The device of claim 12 wherein said security status information is stored in location address 0, said failure information is stored in location addresses 1 and 2, said user identification is stored in location addresses 3-47, said password is stored in location addresses 48-63, said serial number is stored in location addresses 64-95, and
5 said random security challenge is stored in location addresses 96-127.
14. The device of claim 12 wherein said random security challenge is a test, wherein said test requires said external medium to return a value at the beginning of each power-up of the device to unlock the device.
15. The device of claim 9 wherein said security registers include a security status
10 register, a security command register, a failure threshold register, a failure count register, a device password register, a random challenge register, and a temporary data register.
16. The device of claim 15 wherein said boundary scan port further comprises a test access port controller, an instruction register, an instruction decoder, a device bypass
15 register and a boundary scan register.
17. A method of protecting large scale integrated devices from theft, the large scale integrated devices having a core functional circuit and output ports, the method comprising the steps of:
- 

entering into a security session between a security mechanism and an external medium to protect unauthorized access to the core functional circuit and the output ports from said external medium; and

controlling access to the core functional circuit and the output ports through
5 tristate control logic by verifying a requested password from said external medium.

18. The method of claim 17 wherein said security session comprises the steps of:

a. requesting the external medium to return a password upon each power-up of the device;

b. comparing said returned password to a preprogrammed password in said
10 security mechanism to determine if a password match exists therebetween;

c. providing said external medium access to the device if said password match exists.

19. The method of claim 17 wherein said security session comprises the steps of:

a. requesting the external medium to return a random challenge value upon each
15 power-up of the device;

b. comparing said returned random challenge value to a random challenge value calculated by said security mechanism to determine if a challenge value match exists therebetween;

c. providing said external medium access to the device if said challenge value
20 match exists.

20. The method of claim 19 wherein said random challenge value is a value calculated by both said external medium and said security mechanism from a set of random variables.

21. The method of claim 17 wherein said security session comprises the steps of:

5 a. requesting the external medium to return a password and a random challenge value upon each power-up of the device;

b. comparing said returned random challenge value to a random challenge value calculated by said security mechanism to determine if a challenge value match exists therebetween;

10 c. comparing said returned password to a preprogrammed password in said security mechanism to determine if a password match exists therebetween;

d. providing said external medium access to the device if both said challenge value match and said password match exist.

22. The method of claim 17 wherein said security mechanism enters into a device
15 serial number change session if said external medium passes said security session.

23. The method of claim 17 wherein said security mechanism enters into a password change session if said external medium passes said security session.

A

24. The method of claim 17 wherein said security mechanism enters into a device serial number read session if said external medium passes said security session.

25. The method of claim 17 wherein said security mechanism enters into a failure threshold change session if said external medium passes said security session.

FIG. 1

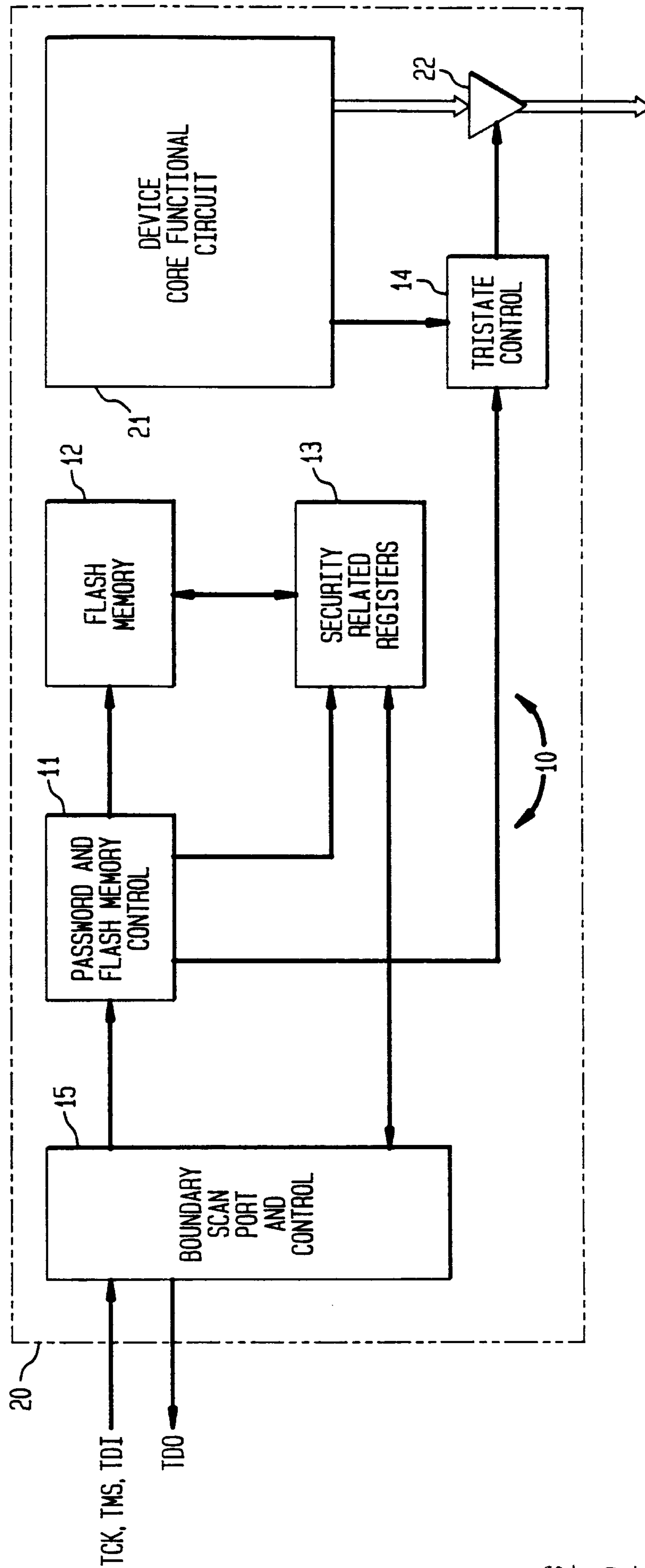


FIG. 2

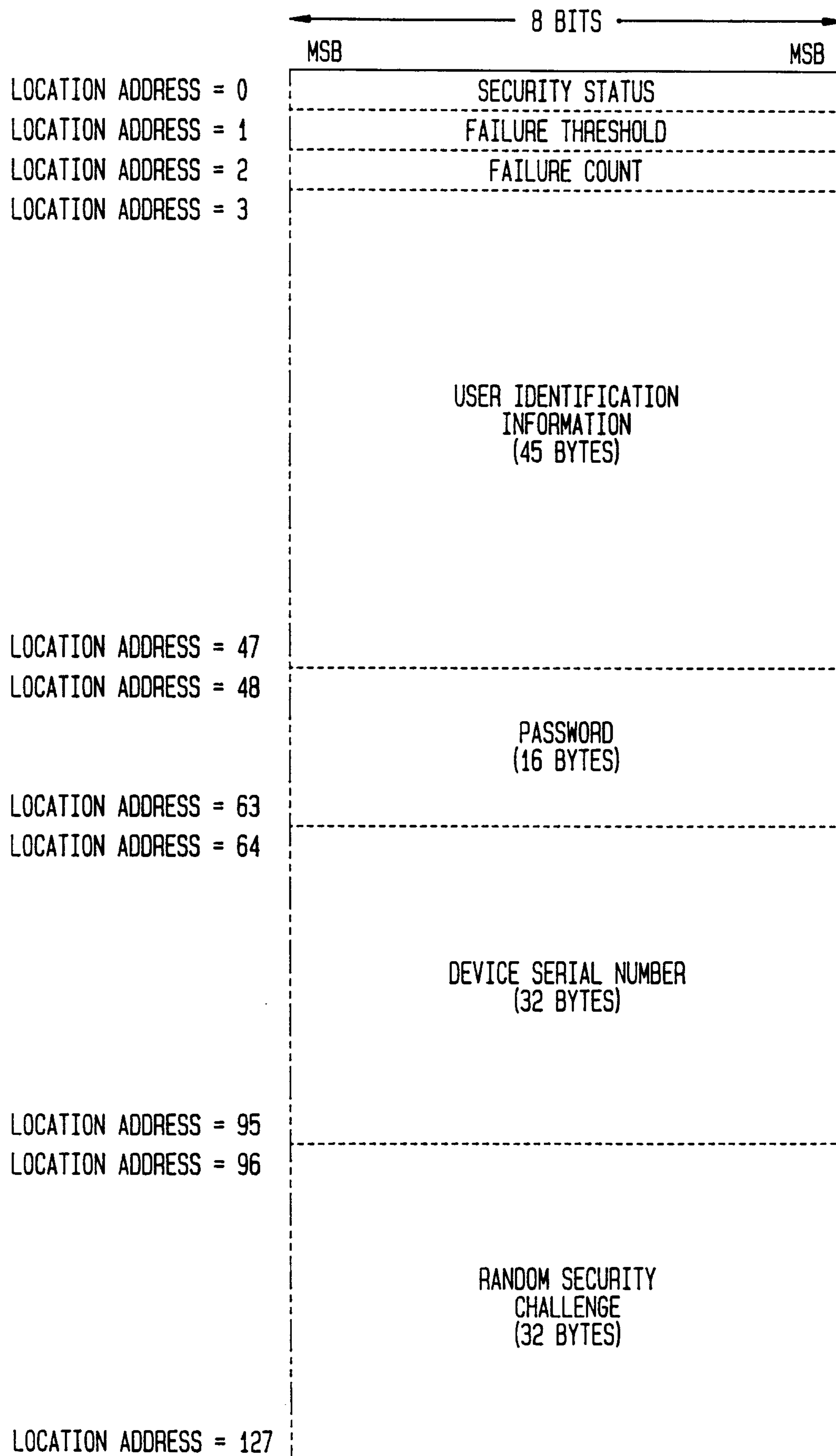


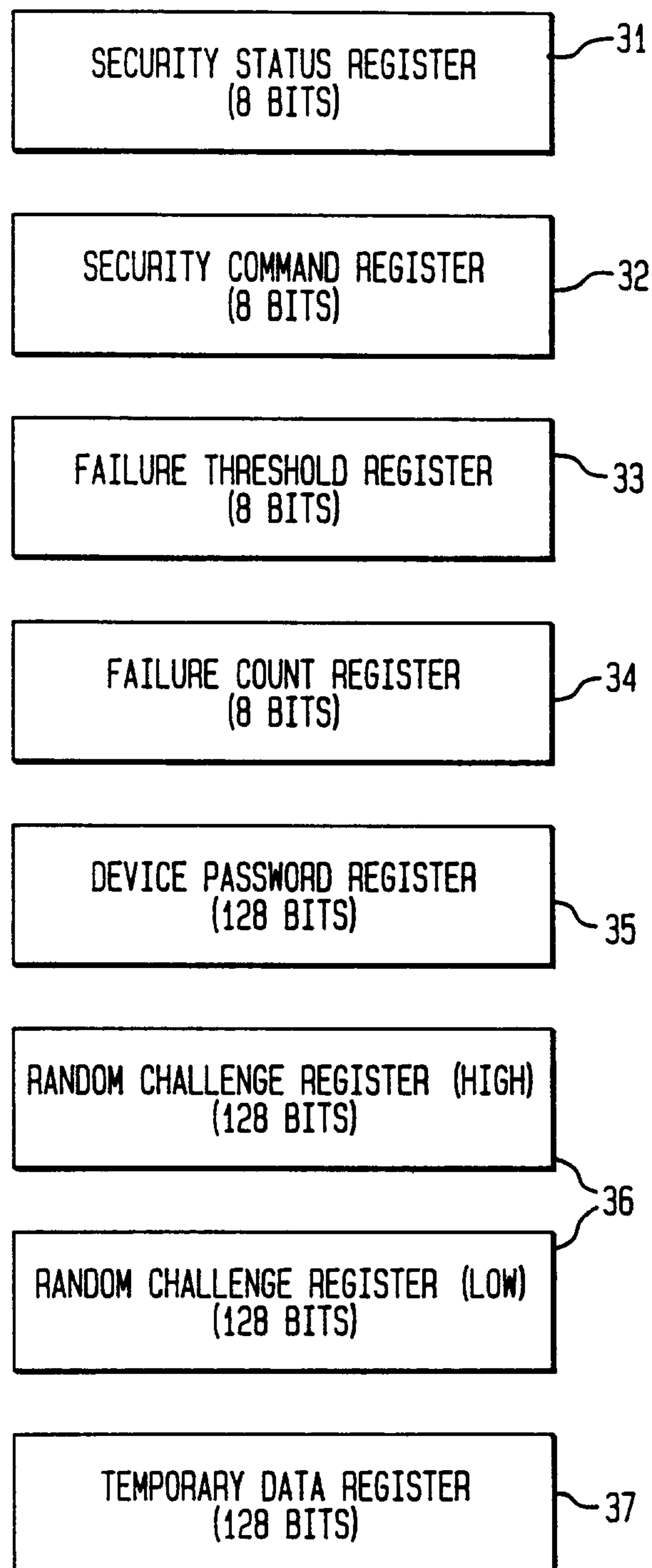
FIG. 313

FIG. 4

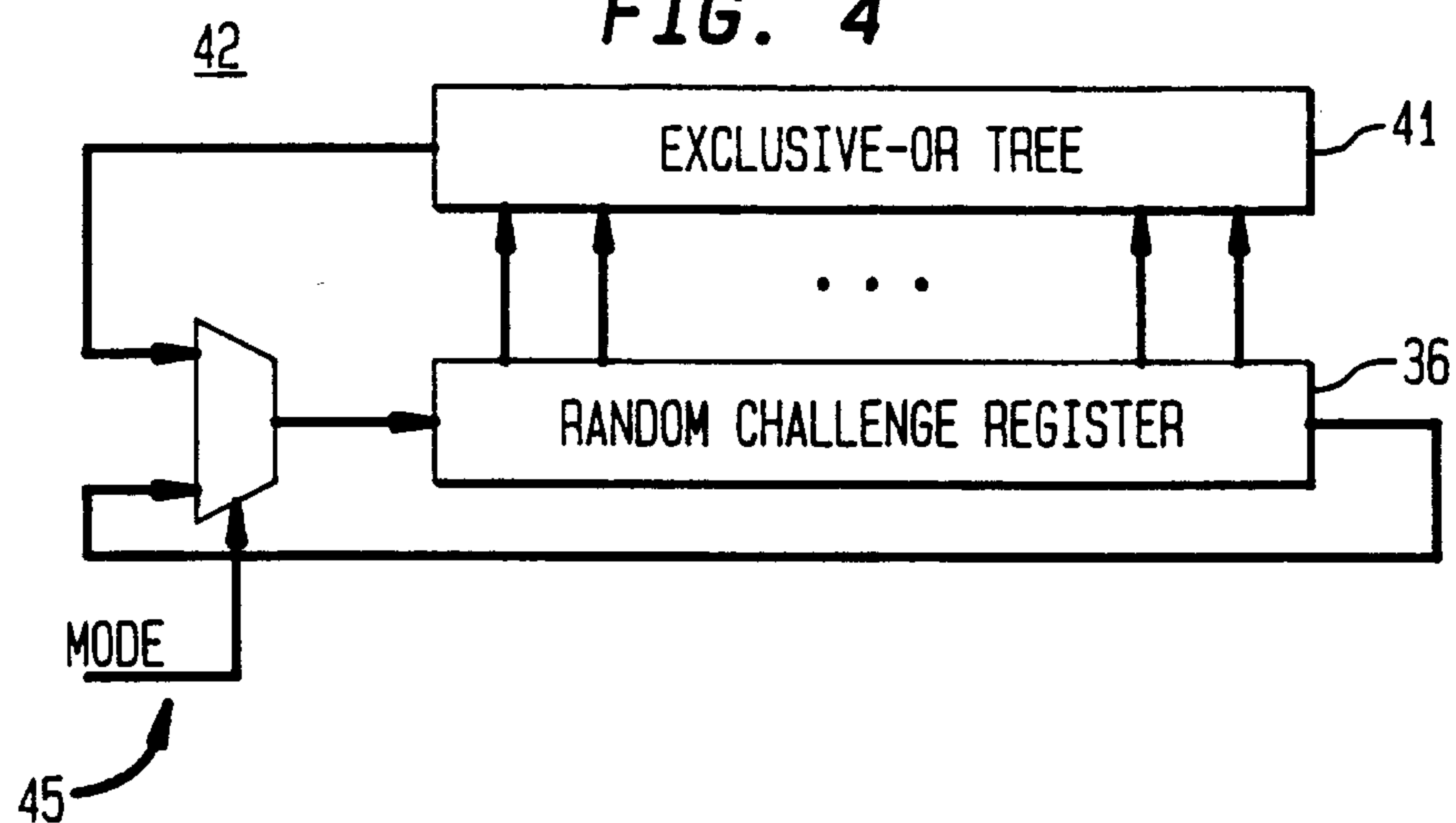


FIG. 5

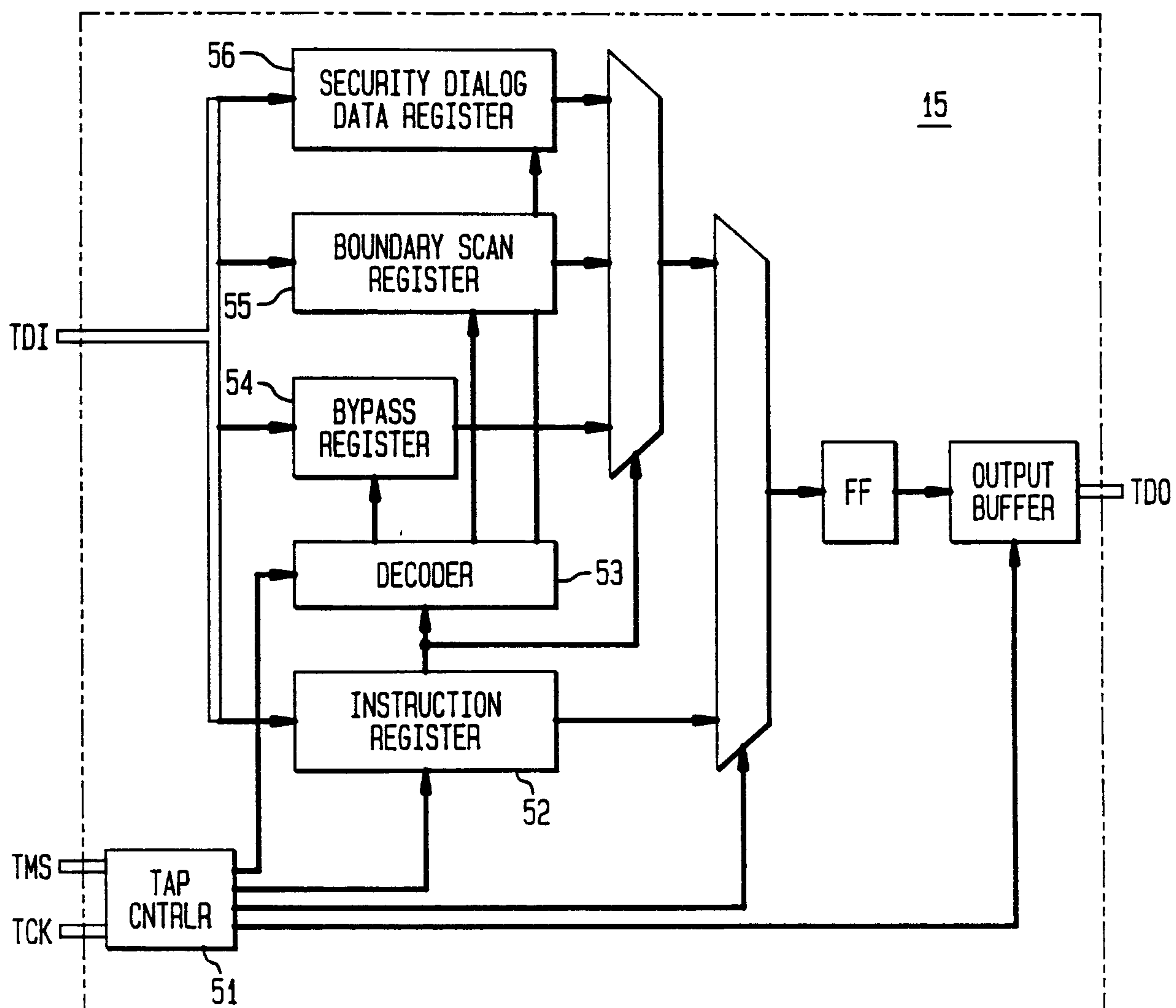


FIG. 6

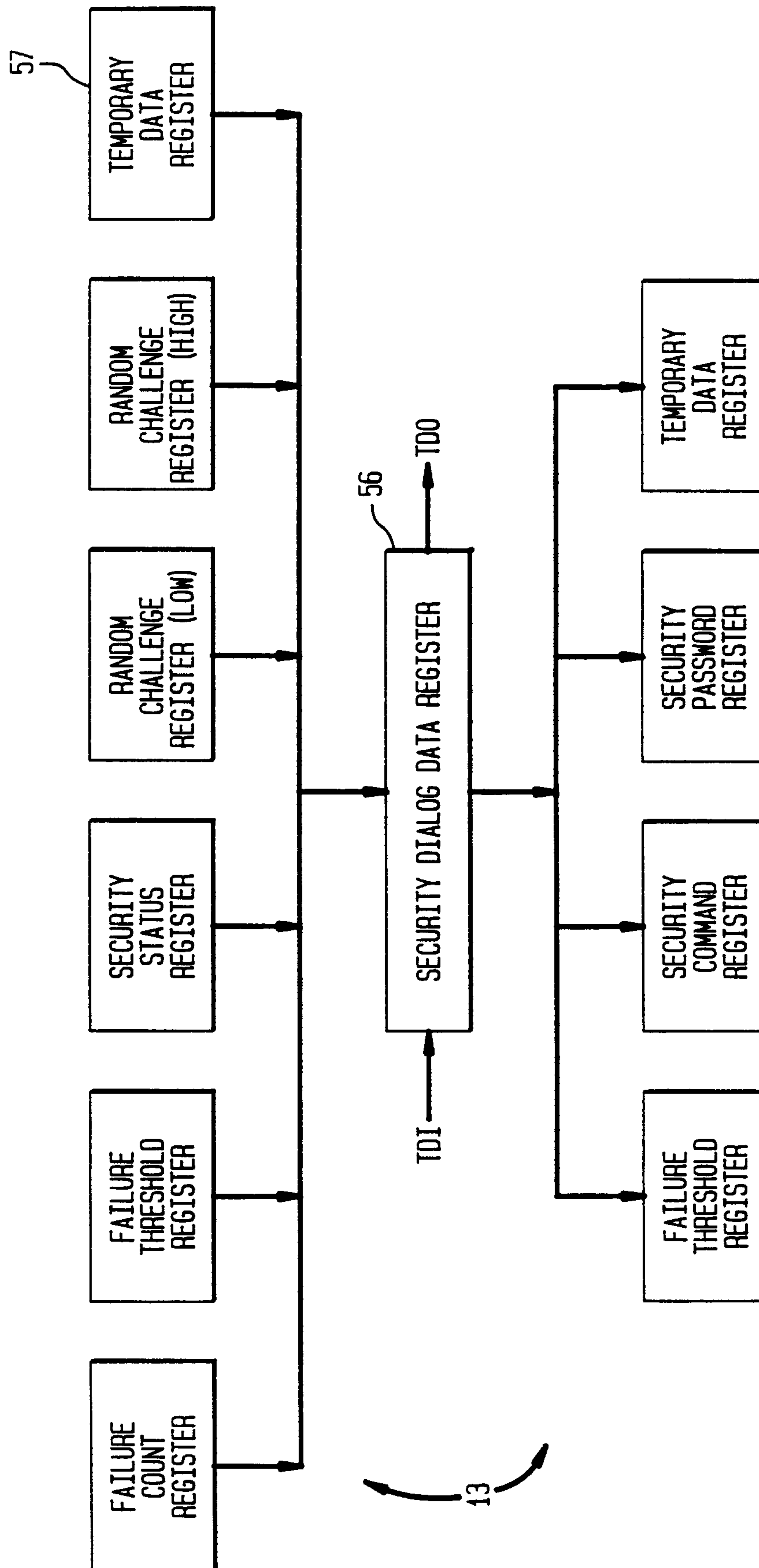


FIG. 7

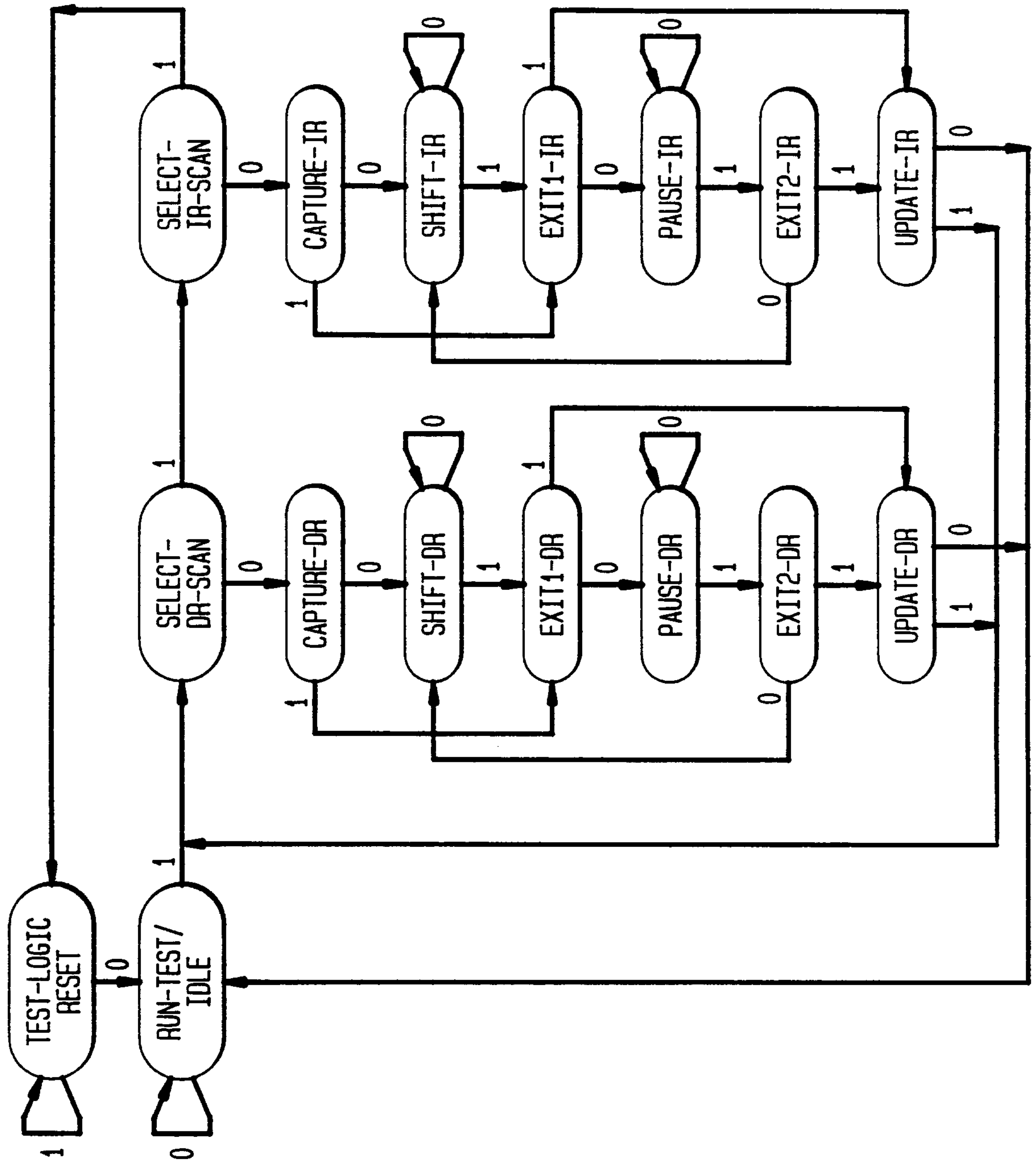


FIG. 8

11

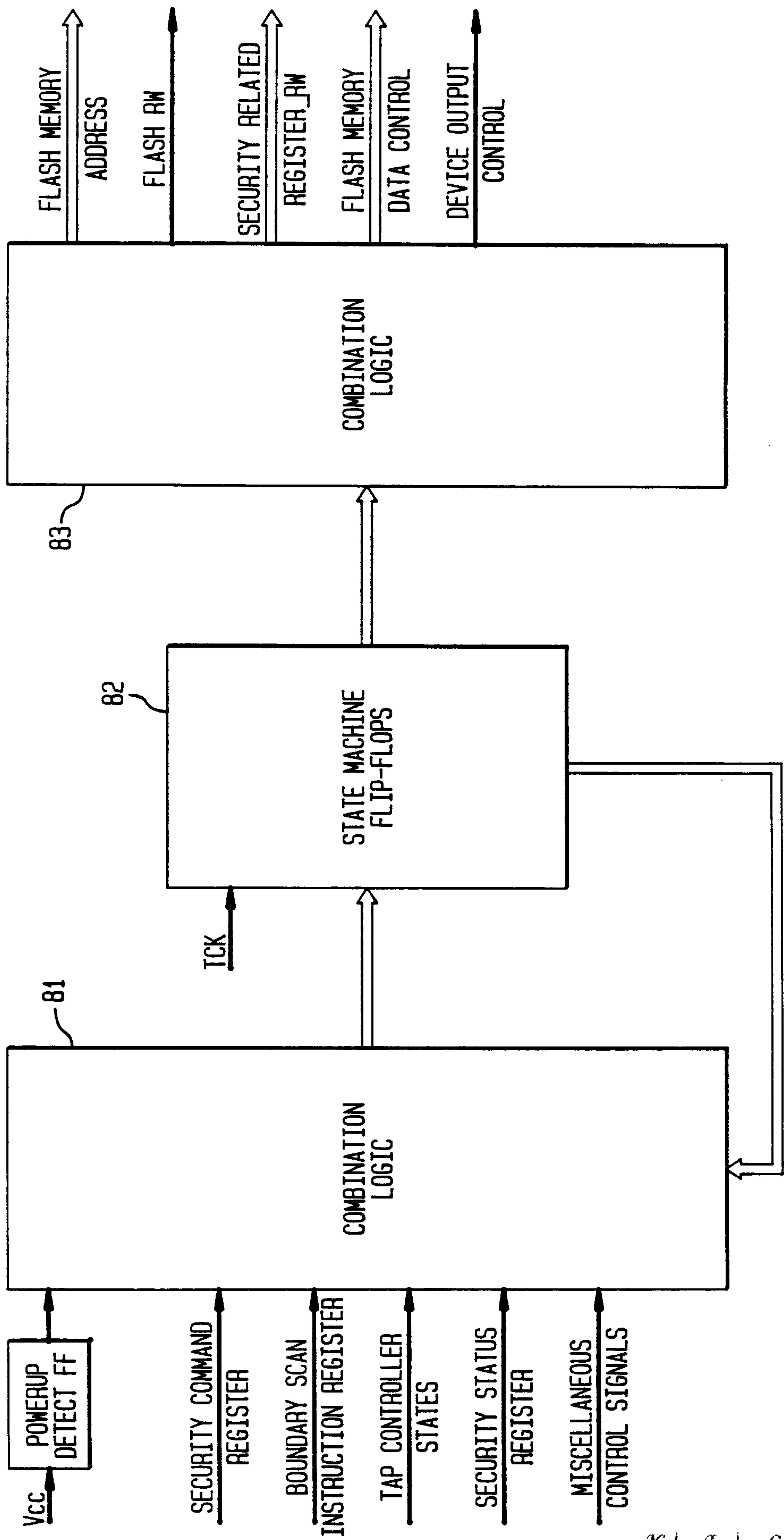
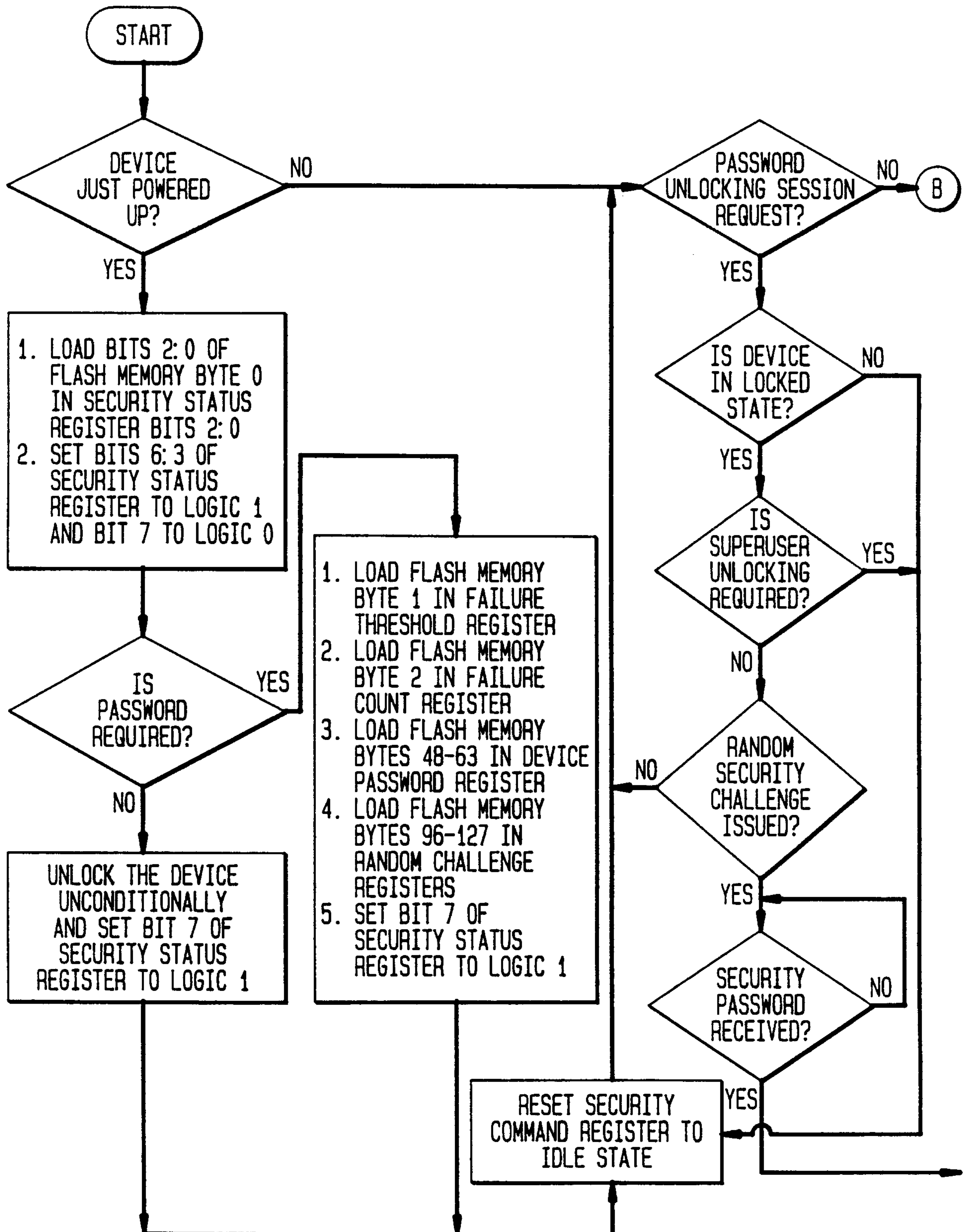


FIG. 9A



9/10

FIG. 9B

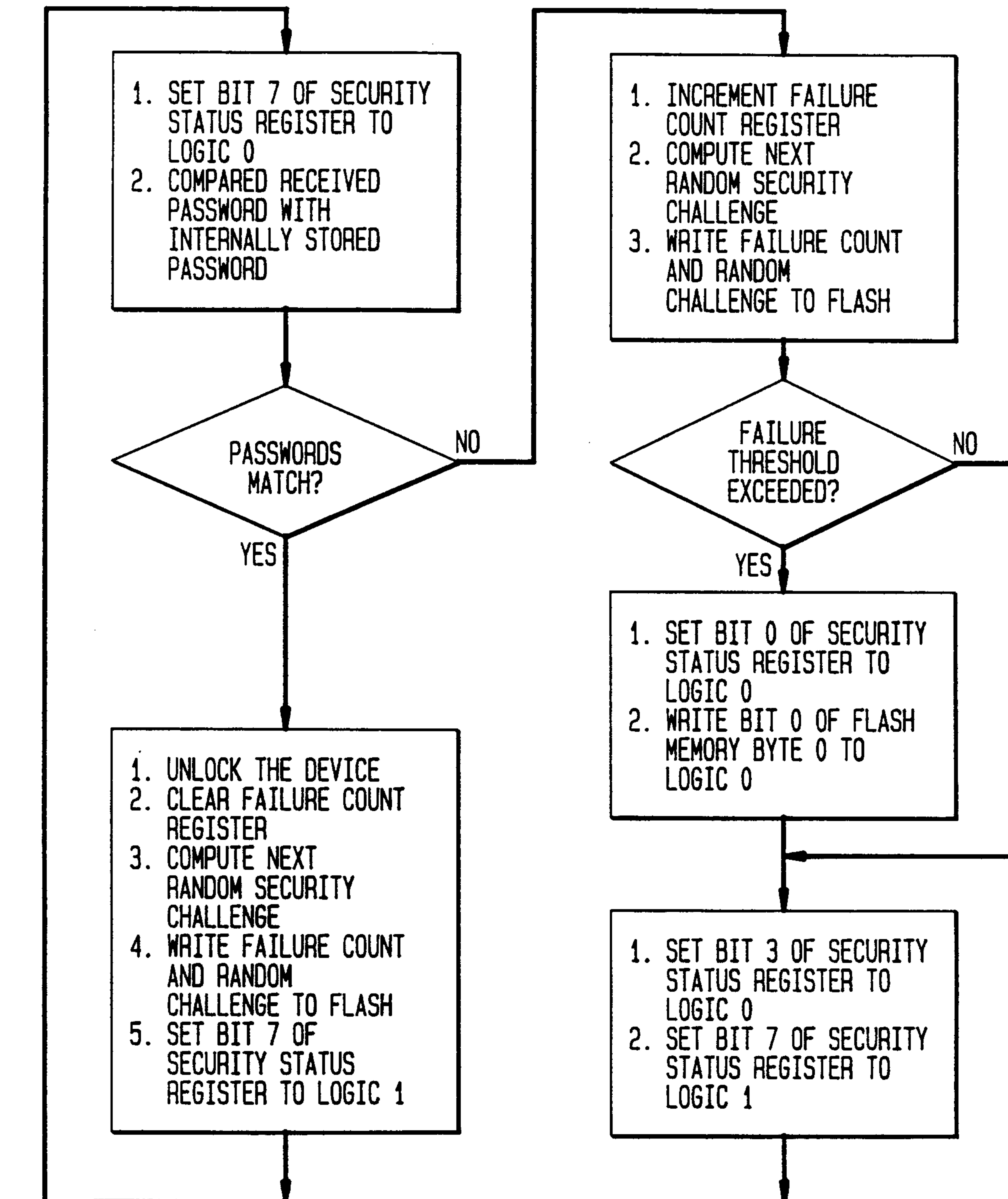


FIG. 9

FIG. 9A

FIG. 9B

FIG. 10

