REF ID:A66552

ROUTING SLIP

NEVER USE FOR APPROVALS, DISAPPROVALS, CONCURRENCES, OR SIMILAR ACTIONS.

TO NAME OR TITLE Mr Friedman	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION S/Asst	DATE		COORDINATION
2		✓	FILE
		✓	INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

Declassified and approved for release by NSA on 05-08-2014 pursuant to E.O. 13526

FROM NAME OR TITLE C C Tison	DATE 11 April
ORGANIZATION AND LOCATION NSA-314	TELEPHONE 3391

942/U23

DD FORM 1 FEB 50 94 REPLACES NME FORM 94, 1 FEB 49, WHICH MAY BE USED. 10—56263-2 GPO

IFF SECURITY PROPOSAL WITH FACILITIES FOR SECURE DATA TRANSMISSION

INTRODUCTION

1. This paper presents a description of the cryptomathematical aspects of a device consisting of a shift register, several storage registers and two correspondence generators. Under proper usage this system should provide a means for secure IFF, secure personal identification (PI), and a secure data transmission system.

2. The basic system was initially proposed by the Communications Laboratory of AFCRC and it was there that the first models of this system were constructed.

DESCRIPTION OF ENCIPHERMENT

1. Operations

a. In order to simplify the description given in the following sections, it will be necessary to define symbols for the various operations used in the encipherment: +, $\oplus$, G, S, Q. The first two will be explained initially; the other three will then be defined by making use of a seven stage device, as shown in Figure 2.

b. Vector addition, or ordinary non-carry binary addition, will be designated by +; e.g. $\emptyset+\emptyset = 1+1 = \emptyset$, $1+\emptyset = \emptyset+1 = 1$. The $\oplus$ shall stand for the operation of combining two vectors a and b in such a way that if a = 110110001 and b = 01011, then a $\oplus$ b = (110110001) $\oplus$ (01011) = 11011000101011.

c. In Figure 2 there is exhibited a seven stage device. This system will be used as an example in explaining the different operations of the device.

d. The correspondence generator is merely a permutation arranged so that for any distinct set of three bits read from stages 4, 5, and 6 in the shift register there is one and only one.output. As an example of this operation, let the contents of the seven stages be represented by x_1, x_2, ... x_6, x_o i.e.

$$\begin{aligned} X &= x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_o \\ &= 1\ 1\ 0\ 1\ 1\ 0\ 0. \end{aligned}$$

Since $x_4\ x_5\ x_6$ maps or is permuted into an output (1,2,3), an input of 110 into the correspondence generator becomes an output of 011, see Figure 2. This is then added to $x_1\ x_2\ x_3$ to yield X' as follows:

$$\begin{aligned} X &= 1\,1\,0\,1\,1\,0\,0 \\ \text{Output} &= \underline{0\,1\,1} \\ X' &= 1\,0\,1\,1\,1\,0\,0 \end{aligned}$$

Let this operation of reading of the value of the contents of stages 4, 5, 6, permuting this value into any of the eight possible values, and then adding the result by non-carry binary addition (+) to stage 1, 2, and 3 of the shift register be defined by the operator G. That is in symbols X G = X'.

e. Let S be an operator designating a cyclic shift from right to left with the contents of stage 1 being carried end around to stage Ø. For example

$$X = 1\,1\,0\,1\,1\,0\,0$$

$$X\,S = 1\,0\,1\,1\,0\,0\,1.$$

f. Let $Q \equiv G\,S$, where the operations are carried out from left to right in sequence as follows:

$$X = 1\,1\,0\,1\,1\,0\,0$$

$$X\,Q = X\,G\,S = (XG)S = (1\,0\,1\,1\,1\,0\,0)S$$

$$= 0\,1\,1\,1\,0\,0\,1.$$

Basically these are the only operations involved in the system.

2. IFF

a. To use this system as a secure IFF we must be able to encipher, in a manner which can be duplicated on the ground, a randomly selected challenge ($C = c_0\,c_1\,c_2\,c_3\,c_4\,c_5\,c_6$). Several different methods have been tried but the one method which appears to offer the most complexity is that of serial loading.

b. The device in its normal state of rest will have the additive key (X_0) inserted in the shift register and will be ready to receive the interrogation pulses as they arrive. The interrogation will be preceeded by a series of synchronization pulses which will indicate what mode of operation is to be performed. After receiving the synchronization pulses and setting up the proper gates for calculating a normal IFF reply the operation will proceed as follows. Let X_0 be the initial setting of the shift register, that is let X_0 be the additive key. Then as the first bit c_0 of the interrogation is received it is added (+) to the zero stage of the shift register, or symbolically $X_0 + c_0 = x_1\,x_2\,x_3\,x_4\,x_5\,x_6\,(x_0{+}c_0)$.

Next $X_o + c_o$ is operated on by Q. Let the result of this operation be designated by X_1, thus $(X_o+c_o)\ Q = X_1$. When the second bit c_1 arrives, it is added to position zero of the shift register. Q again is applied, giving X_2. This process can be represented symbolically as follows:

$$X_o = \text{additive key}$$

$$X_1 = (X_o+c_o)\ G\ S = (X_o+c_o)\ Q$$

$$X_2 = (X_1+c_1)\ Q$$

$$X_3 = (X_2+c_2)\ Q$$

$$X_4 = (X_3+c_2)\ Q$$

$$X_5 = (X_4+c_4)\ Q$$

$$X_6 = (X_5+c_5)\ Q$$

$$X_7 = (X_6+c_6)\ Q$$

or

$$X_7 = (((((((X_o+c_o)Q+c_1)Q+c_2)Q+c_3)Q+c_5)Q+c_6)\ Q.$$

All bits of the interrogation have now been loaded into the shift register. However, the degree of complexity involving the last several bits (c_4, c_5, c_6) is not sufficient to give the system adequate security. Therefore, Q shall be applied seven more times as follows:

$$(((((((X_7)Q)Q)Q)Q)Q)Q)Q \equiv (X_7)\ Q^7.$$

This completes the encipherment.

c. In order to obtain the reply, read the values of any three of the stages (in the example stages 1, 2, and 3 are used) and transmit their value as the reply.

d. The detailed operations involved in a complete encipherment are illustrated in Figure 3.

e. The preceding paragraphs described the method of calculation of a reply from an interrogation for a 7-stage shift register. Now, let us extend this operation to the 24-stage system. The operator G will now represent the reading from 4 stages instead of 3, permuting this value simultaneously through two correspondence generators and adding (+) the results to 2 distinct sets of 4 stages each in the shift register. These sets will be distinct from the reading set. See Figure 1. The operator S is the same (cyclic shift from right to left with end around carry). The interrogation will now consist of 24 bits, $C = c_0 \; c_1 \; c_2 \cdots c_{22} \; c_{23}$, and 4 bits instead of 3 will be used in the reply.

f. The reply is calculated as follows: first, determine X_{48}, $X_{48} = (((\ldots(((X_0+c_0)Q+c_1)Q+c_2)Q+\ldots+c_{22})Q+c_{23})Q)\;Q^{24}$; second, from X_{48} select 4 bits say $x_1 \; x_2 \; x_3 \; x_4$ as the reply.

g. The interrogator, who is on the other end of this transmission, performs the same operations on the challenge (interrogation) that he has transmitted, then holds the result until he receives the reply. Upon receiving the reply he compares this with the one he has calculated and upon a series of say 10 such comparisions he is able to distinguish friends from enemies.

3. Secure Personal Identification

a. The operations of this system when used for secure PI are basically the same with two slight exceptions: first the contents of the entire shift register are transmitted in the reply, and second the interrogator, as we will see later, must be able to shift his shift register in either direction.

b. After having received the synchronization pulses, which are different from those used in IFF, the device is automatically set up to perform the following operations (upon receipt of the interrogation $C \equiv c_o\ c_1\ \ldots\ c_{23}$, which is identical to the preceding challenge); First, determine X_{24} where $X_{24} = (\ldots((X_o+c_o)Q+c_1)Q+\ldots+c_{23})\ Q$. Second, to X_{24} add (+) the PI or PI $\oplus$ A (see 1b) where A might be an indication of the amount of fuel remaining, i.e. $X_{24} + (PI \oplus A) \equiv X'_{24}$. Third, determine X'_{48} where $X'_{48} = (X'_{24})\ Q^{24}$. Finally the reply X'_{48} (all 24 bits) is transmitted to the interrogator.

c. In the meantime the interrogator has calculated X_{24} and transferred it to a storage register awaiting the reply X'_{48}. Having received X'_{48} he proceeds to operate backwards. First he shifts his shift register, which contains X'_{48}, from left to right. Let this shift from left to right be designated by S^{-1}. Next he operates with G, which yields $X'_{47} = X'_{48}S^{-1}G$. Since $X'_{48} = X'_{47}\ Q$, let us define Q^{-1} as $S^{-1}G$, i.e. $Q^{-1} \equiv S^{-1}G$, and further let $Q^{-4} \equiv (Q^{-1})^{4} \equiv ((((X)\ Q^{-1})Q^{-1})Q^{-1})Q^{-1}$ or any other power n such that Q^{-n} means to apply Q^{-1} successively n times. Hence $X'_{24} = (X'_{48})\ Q^{-24}$. By adding (+) X_{24} to X'_{24} we have $X_{24} + X'_{24} = PI \oplus A$ which not only gives the interrogatee's PI but also gives the amount of fuel (or other vital information) to the interrogator. See Figure 4 for a detailed calculation using a seven stage device.

d. There are other types of operational procedures that can be used to obtain a PI reply from a particular aircraft rather than having all aircraft in a given area responding at once. The details of these and other modifications will not be included at this time.

4. Data Transmission

a. Even though the operations involved in using this system for data transmission are rather complex, it should be borne in mind that this facility is an extra or bonus since most of the equipment would already be present for the IFF system. The system as proposed is essentially a discrete address system wherein a set of data is sent to one receiver (or under a prearranged address system to one group of receivers).

b. Under the assumption that there will always be more than one aircraft within receiving range, it will be necessary to set up a closed circuit between the transmitter on the ground and the receiver in the aircraft. This will be accomplished as follows: First, the ground will transmit a normal challenge C which is preceeded by a special set of synchronization pulses that trigger the proper gates for data transmission operation. Then for the seven stage device he calculates X_7 as in Figure 5(a) and stores it for future use. For simplicity let $X_7 \equiv H$. Second, the aircraft receives the challenge and calculates H (X_7) and he too stores H for future use. To the value of H which is still in his shift register is added his PI and the initial value K_o of his counter (K). Call the result of this operation X''_7, where $X''_7 = H + PI \oplus K_o$. The counter (K) is a binary counter of 3 stages in the seven stage device which counts ∅, 1, 2, 3, 4, 5, 6, 7, ∅, 1, ... and it is not reset to ∅. K_o would represent some initial value and K_1 would represent the next value in the sequence. Operate on X''_7 with Q^7 to obtain X''_{14}, the reply. This entire operation in symbols is $X''_{14} = [(\cdots((X_o+c_o)Q+c_1)Q+ \ldots + c_6)Q+\{PI \oplus K_o\}]Q^7$.

The reply is then sent to the ground. See Figure 5(b). Third, the ground receives the reply (X''_{14}) and operates on it as follows: $(X''_{14})\ Q^{-7}+H = PI \oplus K_o$. The $\{PI \oplus K_o\}$ is complemented, that is Ø's become 1's and vice versa then $(H+\{PI \oplus K_o\}')\ Q^{-7} = X^*_{14} = C.\ S.$ C. S. is transmitted to the aircraft as a call sign for the aircraft with this particular PI and K_o. See Figure 5(c) and (d). Fourth, C. S. is deciphered in the aircraft as follows: $(C.\ S.)\ Q^{7}+H + (PI \oplus K_1) = 1\ 1\ 1\ 1\ 1\ 1\ 1$ when the result of this calculation is all one's he transmits a pulse indicating correct reception. In general $(a)\ Q^{n} = (b)\ Q^{n}$ if and only if a = b. Since a and b are of the form $H+\{PI \oplus K_o\}$, then the other aircraft within receiving range that have different PI's can not get all ones. Those that do not get ones would automatically ignore the message transmissions. The calculations for this step are carried out in Figure 5(e). This completes the setting up of a closed circuit.

c. The remaining operations consist of transmitting the messages. However, since K_o has already been used in the setup, the total number of messages which can be sent on one setup is limited to one less than the total number of settings of K. The messages (for the seven stage device) are enciphered as follows, where M_i is message i and EM_i is the enciphered message:

$$M_1\ (\text{Ground})(H+\{M_1 \oplus K_1\})\ Q^{-7} = EM_1;$$

$$(\text{Air})\ (EM_1)\ Q^{7}+H+K_1 = M_1 \oplus Ø;$$

Acknowledge correct receipt of M_1;

M_2 (Ground) $(H+\{M_2 \oplus K_2\})\ Q^{-7} = EM_2$;

(Air) $(EM_2)\ Q^7+H+K_2 = M_2 \oplus \emptyset$

Acknowledge correct receipt of M_2; and so forth. See Figures 5(f) and 5(g).

d. The fact that the aircraft must obtain a Ø in the positions normally occupied by K gives an excellent check for transmission and other errors.

e. After a predetermined time the transponders in the aircraft go back into their normal state, that is in a stand-by status awaiting an interrogation.

KEY

1. The daily key will consist of the additive key, correspondence generator one and correspondence generator two.' The read, write and reply read-out positions are fixed and given in Figure 1.

2. There are $2^{24}-1$ or approximately 1.7×10^7 usable additive keys. The key consisting of all zeros will not be used.

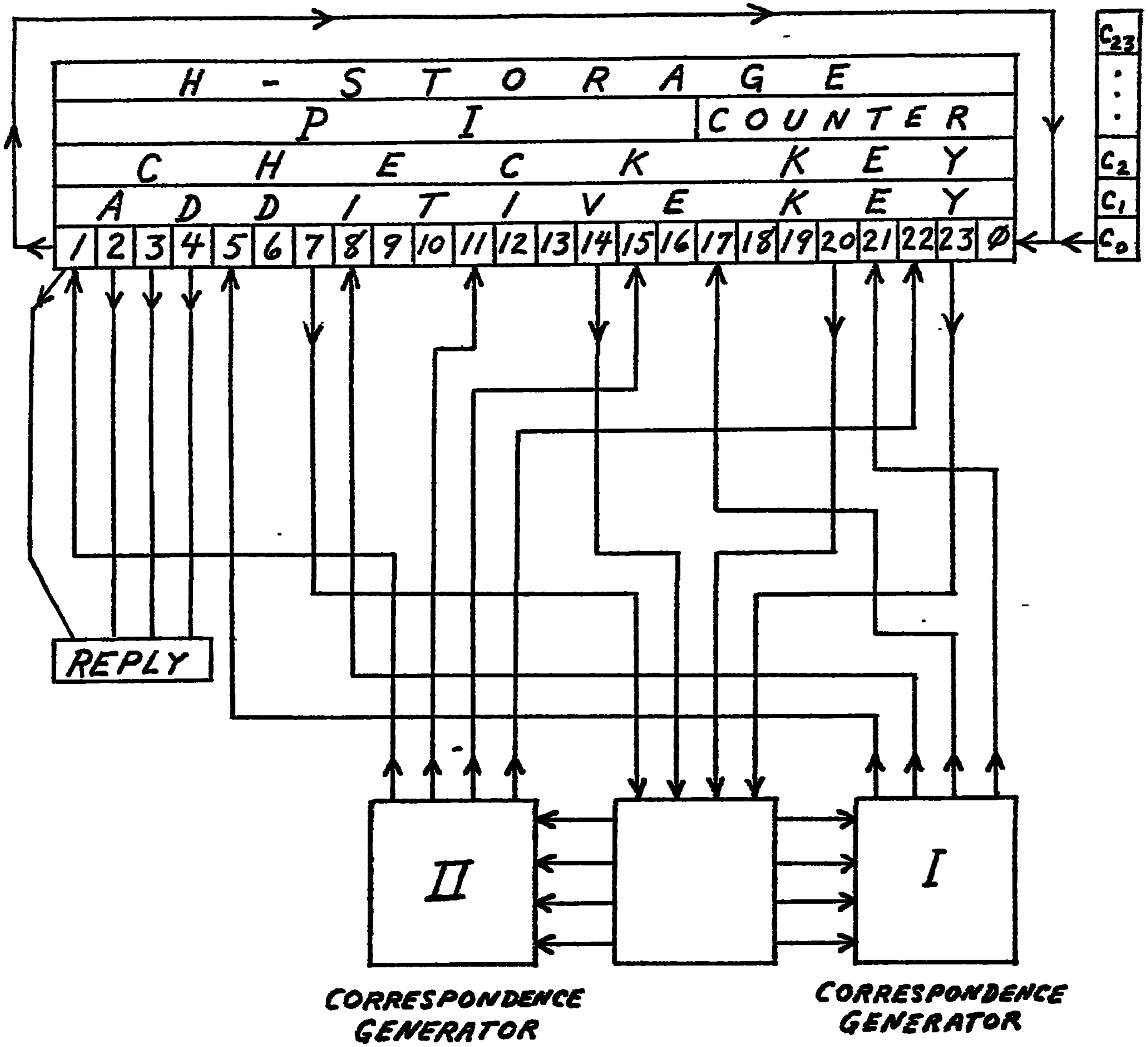
3. Since the correspondence generators are permutors of 16 elements, there are 16! or approximately 2.1×10^{13} different set-ups for each correspondence generator. However, no permutation which can be represented by a linear transformation can be used, therefore the 28,080 permutations which can be represented by linear transformation must be subtracted from the total number (2.1×10^{13}) of set-ups to give the usable number of permutations for each correspondence generator.

4. The total number of usable keys is $(2^{24}-1)(16!-28,080)(16!-28,080)$ or approximately $(1.7 \times 10^{7})(2.1 \times 10^{13})(2.1 \times 10^{13}) = 7 \times 10^{33}$.

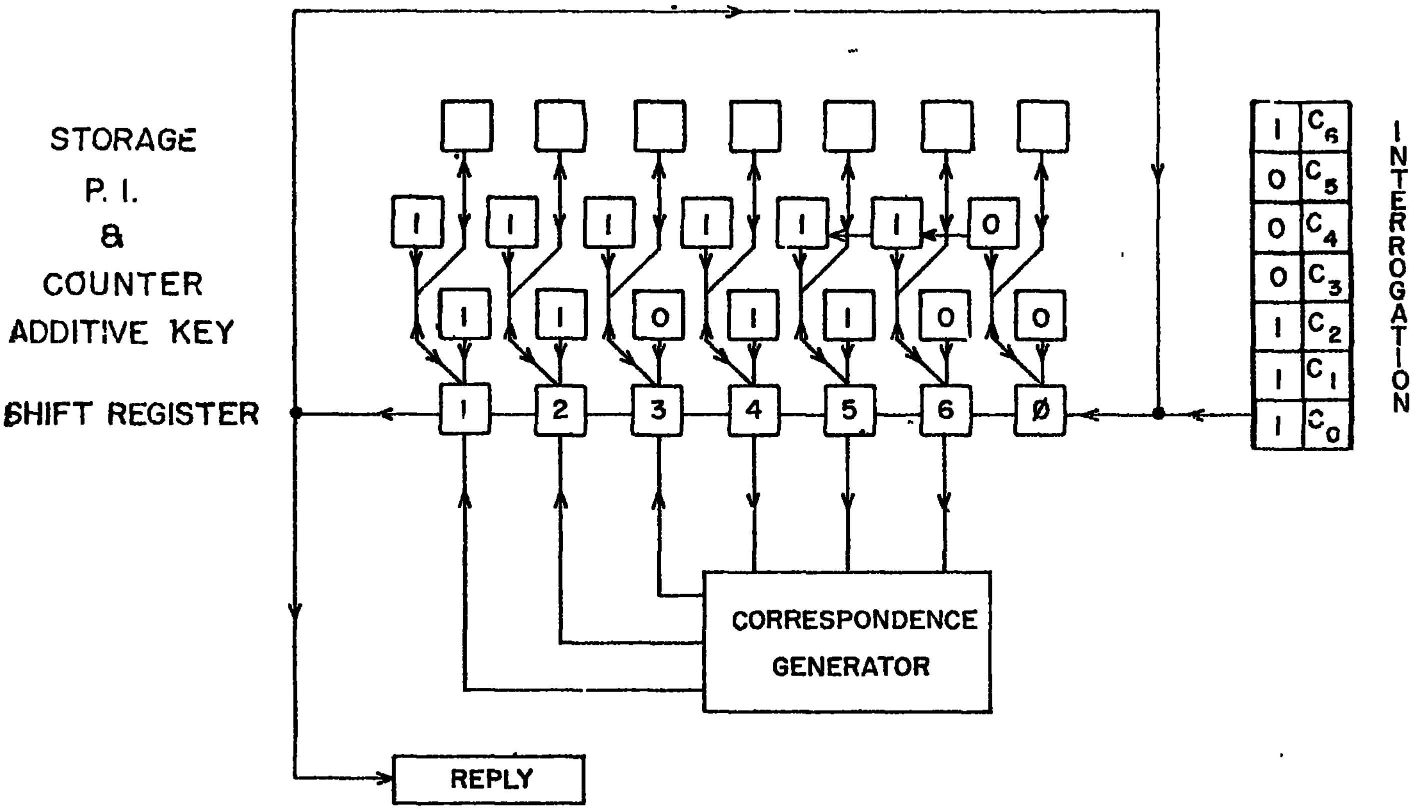
5. In order to avoid the selection of a linear permutation for use in the key list the proposed key could be simply tested for linearity by a properly designed digital computor program.

6. In order to insure that the key is properly set up in the device a test setting $(X_0)Q^{96}$ will be inserted into a separate register. The Officer who inserts the key will push a button and have the device with its new key run thru the 96 settings and check the 96th setting against the check setting furnished by the key list. If the two settings are identical, then the Officer knows that the key has been properly inserted and that the crypto-unit is functioning properly. After the initial test the device will automatically check itself at regular intervals, say every two minutes. Any time a failure occurs the device rechecks itself several times; if the system continues to fail then the system is automatically switched into emergency mode of operation and the pilot is informed.

Carey C. Tison
NSA-314
30 March 1955



AFCRC COMM. LAB IFF WITH DATA TRANSMISSION
FIGURE 1



CORRESPONDENCE
GENERATOR

	INPUT				OUTPUT			
STAGES	4	5	6		1	2	3	STAGES
	0	0	0	$\xrightarrow{G}$	0	1	0	
	0	0	1		1	0	0	
	0	1	0		1	0	1	
	0	1	1		1	1	1	
	1	0	0		0	0	1	
	1	0	1		0	0	0	
	1	1	0		0	1	1	
	1	1	1	$\xrightarrow{G}$	1	1	0	

SEVEN STAGE DEVICE

FIGURE 2

SHIFT REGISTER

	1	2	3	4	5	6	Ø		
Additive.Key	1	1	0	1	1	0	0		X_o
Output 0 1 1	0	1	1				1	c_o	Input 1 1 0
	1	0	1	1	1	0	1		$X_o' = (X_o+c_o) G$
	0	1	1	1	0	1	1		$X_1 = X_o' S$
Output 0 0 0	0	0	0				1	c_1	Input 1 0 1
	0	1	1	1	0	1	0		$X_1' = (X_1+c_1) G$
	1	1	1	0	1	0	0		$X_2 = X_1' S$
Output 1 0 1	1	0	1				1	c_2	Input 0 1 0
	1	0	0	1	0	1	0		$X_3 = (X_2+c_2) Q$
Output 0 0 0	0	0	0				0	c_3	Input 1 0 1
	0	0	1	0	1	0	1		$X_4 = (X_3+c_3) Q$
	1	0	1				0	c_4	
	0	0	0	1	0	1	1		X_5
	0	0	0				0	c_5	
	0	0	1	0	1	1	0		X_6
	1	1	1				1	c_6	
	1	0	0	1	1	1	1		X_7
	1	1	0						
	1	0	1	1	1	1	0		X_8
	1	1	0						
	1	1	1	1	1	0	0		X_9
	0	1	1						
	0	0	1	1	0	0	1		X_{10}
	0	0	1						
	0	0	1	0	0	1	0		X_{11}
	1	0	0						
	0	1	0	0	1	0	1		X_{12}
	1	0	1						
	1	1	0	1	0	1	1		X_{13}
	0	0	0						
	1	0	1	0	1	1	1		X_{14}
	1	0	1						Reply

REPLY FOR SECURE IFF

Figure 3

~~SECRET~~

INTERROGATEE

SHIFT REGISTER

1	2	3	4	5	6	Ø		
1	1	0	1	1	0	0		X_0
0	1	1				0	c_0	
1	0	1	1	1	0	0		X_0'
0	1	1	1	0	0	1		X_1
0	0	1				0	c_1	
1	0	1	0	0	1	0		X_2
1	0	0				0	c_2	
0	1	0	0	1	0	0		X_3
1	0	1				1	c_3	
1	1	0	1	0	1	1		X_4
0	0	0				0	c_4	
1	0	1	0	1	1	1		X_5
1	1	1				0	c_5	
1	0	0	1	1	1	0		X_6
1	1	0				0	c_6	
1	0	1	1	1	0	0		X_7
1	1	1	1				PI	
				1	1	0	A	
0	1	0	0	0	1	0		X_7'
1	0	0						
1	0	0	0	1	0	1		X_8'
1	0	1						
0	1	0	1	0	1	0		X_9'
0	0	0						
1	0	1	0	1	0	0		X_{10}'
1	0	1						
0	0	0	1	0	0	0		X_{11}'
0	0	1						
0	1	1	0	0	0	0		X_{12}'
0	1	0						
0	1	0	0	0	0	0		X_{13}'
0	1	0						
0	0	0	0	0	0	0		X_{14}'
0	0	0	0	0	0	0		Reply

INTERROGATOR

SHIFT REGISTER

1	2	3	4	5	6	Ø		
1	1	0	1	1	0	0		X_0
0	1	1				0	c_0	
1	0	1	1	1	0	0		X_0'
0	1	1	1	0	0	1		X_1
0	0	1				0	c_1	
1	0	1	0	0	1	0		X_2
1	0	0				0	c_2	
0	1	0	0	1	0	0		X_3
1	0	1				1	c_3	
1	1	0	1	0	1	1		X_4
0	0	0				0	c_4	
1	0	1	0	1	1	1		X_5
1	1	1				0	c_5	
1	0	0	1	1	1	0		X_6
1	1	0				0	c_6	
1	0	1	1	1	0	0		X_7
1	0	1	1	1	0	0	Store	
0	0	0	0	0	0	0	Reply	
0	0	0	0	0	0	0	X_{14}'	
0	0	0	0	0	0	0		$X_{14}'S^{-1}$
0	1	0						
0	0	1	0	0	0	0	$X_{13}'\ S^{-1}$	
0	1	0						
0	0	1	1	0	0	0	$X_{12}'\ S^{-1}$	
0	0	1'						
0	0	0	0	1	0	0	$X_{11}'\ S^{-1}$	
1	0	1						
0	1	0	1	0	1	0	$X_{10}'\ S^{-1}$	
0	0	0						
0	0	1	0	1	0	1	$X_9'\ S^{-1}$	
1	0	1						
1	1	0	0	0	1	0	$X_8'\ S^{-1}$	
1	0	0						
0	1	0	0	0	1	0	X_7'	
0	1	0	0	0	1	0	X_7'	
1	0	1	1	1	0	0	Storage (X_7)	
1	1	1	1	1	1	0		
1	1	1	1				PI	
				1	1	0	A	

SECURE PERSONAL IDENTIFICATION

Figure 4

~~SECRET~~

~~SECRET~~

GROUND AND AIR

1	1	0	1	1	0	0		X_o
0	1	1				1	c_o	
0	1	1	1	0	1	1		X_1
0	0	0				0	c_1	
1	1	1	0	1	1	0		X_2
1	1	1				0	c_2	
0	0	0	1	1	0	0		X_3
0	1	1				1	c_3	
1	1	1	1	0	1	0		X_4
0	0	0				0	c_4	
1	1	1	0	1	0	1		X_5
1	0	1				1	c_5	
1	0	0	1	0	0	0		X_6
0	0	1				0	c_6	
0	1	1	0	0	0	1		$X_7 \equiv H$
1	1	1	1				PI	
				0	1	0	Counter (K_o)	
1	0	0	1	0	1	1	X''_7	

(a)

AIR

1	0	0	1	0	1	1	X''_7
0	0	0					
0	0	1	0	1	1	1	X''_8
1	1	1					
1	0	0	1	1	1	1	X''_9
1	1	0					
1	0	1	1	1	1	0	X''_{10}
1	1	0					
1	1	1	1	1	0	0	X''_{11}
0	1	1					
0	0	1	1	0	0	1	X''_{12}
0	0	1					
0	0	1	0	0	1	0	X''_{13}
1	0	0					
0	1	0	0	1	0	1	X''_{14}
0	1	0	0	1	0	1	Reply

(b)

GROUND

0	1	0	0	1	0	1	X''_{14}
1	0	1	0	0	1	0	$X''_{14}S^{-1}$
1	0	0					
0	0	0	1	0	0	1	$X''_{13}S^{-1}$
0	0	1					
1	0	0	1	1	0	0	$X''_{12}S^{-1}$
0	1	1					
0	1	1	1	1	1	0	$X''_{11}S^{-1}$
1	1	0					
0	1	0	1	1	1	1	$X''_{10}S^{-1}$
1	1	0					
1	1	0	0	1	1	1	X''_9S^{-1}
1	1	1					
1	0	0	1	0	1	1	X''_8S^{-1}
0	0	0					
1	0	0	1	0	1	1	X''_7
1	0	0	1	0	1	1	X''_7
0	1	1	0	0	0	1	$X_7(H)$
1	1	1	1	0	1	0	
1	1	1	1				PI
				0	1	0	K_o
0	0	0	0	1	0	1	$\{PI \oplus K_o\}'$

(c)

GROUND

0	1	1	0	0	0	1	H
0	0	0	0	1	0	1	$\{PI \oplus K_o\}'$
0	1	1	0	1	0	0	X^*_7
0	0	1	1	0	1	0	$X^*_7S^{-1}$
0	0	0					
0	0	0	1	1	0	1	$X^*_6S^{-1}$
0	1	1					
1	0	1	1	1	1	0	$X^*_5S^{-1}$
1	1	0					
0	0	1	1	1	1	1	$X^*_4S^{-1}$
1	1	0					
1	1	1	1	1	1	1	$X^*_3S^{-1}$
1	1	0					
1	0	0	1	1	1	1	$X^*_2S^{-1}$
1	1	0					
1	0	1	0	1	1	1	$X^*_1S^{-1}$
1	1	1					
0	1	0	0	1	1	1	X^*_o
0	1	0	0	1	1	1	C. S.

(d)

Data Transmission

Figure 5

~~SECRET~~

```
AIR                                  GROUND

0 1 0 0 1 1 1   C. S.                0 1 1 0 0 0 1   H
1 1 1                                1 0 0 1         M1
0 1 0 1 1 1 1   X*1                          0 1 0   Ko
1 1 0                                            1
0 0 1 1 1 1 1   X*2                          -----
1 1 0                                        0 1 1   K1
1 1 1 1 1 1 1   X*3                  1 1 1 1 0 1 0   X*7
1 1 0                                0 1 1 1 1 0 1
0 1 1 1 1 1 0   X*4                  0 1 1
1 1 0                                1 0 0 0 1 1 0   X*6  S^-1
0 1 1 1 1 0 1   X*5                  1 1 1
0 1 1                                0 0 1 1 0 1 1   X*5  S^-1
0 0 1 1 0 1 0   X*6                  0 0 0
0 0 0                                1 0 0 1 1 0 1   X*4  S^-1
0 1 1 0 1 0 0   X*7                  0 1 1
                                     1 1 1 1 1 1 0   X*3  S^-1
0 1 1 0 1 0 0   X*7                  1 1 0
1 1 1 1 0 1 0   {PI ⊕ Ko}            0 0 0 1 1 1 1   X*2  S^-1
0 1 1 0 0 0 1   H                    1 1 0
-------------                        1 1 1 0 1 1 1   X*1  S^-1
1 1 1 1 1 1 1                        1 1 1
                                     0 0 0 0 1 1 1   X*o
One Pulse Reply
                                     0 0 0 0 1 1 1   EM1

      (e)                                 (f)
```

```
AIR

0 0 0 0 1 1 1   EM1
1 1 1
1 1 0 1 1 1 1   X*1
1 1 0
0 0 1 1 1 1 0   X*2
1 1 0
1 1 1 1 1 0 1   X*3
0 1 1
0 0 1 1 0 1 1   X*4
0 0 0
0 1 1 0 1 1 0   X*5
1 1 1
0 0 0 1 1 0 1   X*6
0 1 1
1 1 1 1 0 1 0   X*7

1 1 1 1 0 1 0   X*7
0 1 1 0 0 0 1   H
        0 1 0   Ko
            1
        -----
        0 1 1   K1
-------------
1 0 0 1 0 0 0
1 0 0 1         M1  Check
        0 0 0

     (g)
```

Figure 5 (cont)