Title: A RADIO FREQUENCY IDENTIFICATION (RFID) SECURITY SYSTEM HAVING AN RF EMULATING CIRCUIT

Abstract

A Radio Frequency Identification (RFID) security (10) uses an electronic key (12) for storing data. A reading mechanism (14) is provided and is used for reading a modulated signal having the data stored on the electronic key (12) when the electronic key (12) is coupled to the reading mechanism (14). An RF emulating circuit (16) is coupled to the reading mechanism (14) for emulating an RF energy signal to the electronic key (12) for allowing the reading mechanism (14) to read the data stored on the electronic key (12) when the electronic key (12) is coupled to the reading mechanism (14).
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AL</td>
<td>Albania</td>
<td>ES</td>
<td>Spain</td>
<td>LS</td>
<td>Lesotho</td>
<td>SI</td>
<td>Slovenia</td>
<td>LG</td>
<td>Slovenia</td>
<td>Slovenia</td>
<td>LG</td>
</tr>
<tr>
<td>AM</td>
<td>Armenia</td>
<td>FI</td>
<td>Finland</td>
<td>LT</td>
<td>Lithuania</td>
<td>SK</td>
<td>Slovakia</td>
<td>SN</td>
<td>Senegal</td>
<td>Senegal</td>
<td>SN</td>
</tr>
<tr>
<td>AT</td>
<td>Austria</td>
<td>FR</td>
<td>France</td>
<td>LU</td>
<td>Luxembourg</td>
<td>SZ</td>
<td>Swaziland</td>
<td>TD</td>
<td>Chad</td>
<td>Chad</td>
<td>TD</td>
</tr>
<tr>
<td>AU</td>
<td>Australia</td>
<td>GB</td>
<td>United Kingdom</td>
<td>MC</td>
<td>Monaco</td>
<td>TG</td>
<td>Togo</td>
<td>TJ</td>
<td>Tajikistan</td>
<td>Tajikistan</td>
<td>TJ</td>
</tr>
<tr>
<td>AZ</td>
<td>Azerbaijan</td>
<td>GE</td>
<td>Georgia</td>
<td>MD</td>
<td>Republic of Moldova</td>
<td>TM</td>
<td>Turkmenistan</td>
<td>TR</td>
<td>Turkey</td>
<td>Turkey</td>
<td>TR</td>
</tr>
<tr>
<td>BA</td>
<td>Bosnia and Herzegovina</td>
<td>GH</td>
<td>Ghana</td>
<td>MG</td>
<td>Madagascar</td>
<td>TT</td>
<td>Trinidad and Tobago</td>
<td>UA</td>
<td>Ukraine</td>
<td>Ukraine</td>
<td>UA</td>
</tr>
<tr>
<td>BB</td>
<td>Barbados</td>
<td>GN</td>
<td>Guinea</td>
<td>MK</td>
<td>The former Yugoslav</td>
<td>UG</td>
<td>Uganda</td>
<td>US</td>
<td>United States of America</td>
<td>UZ</td>
<td></td>
</tr>
<tr>
<td>BE</td>
<td>Belgium</td>
<td>GR</td>
<td>Greece</td>
<td>ML</td>
<td>Mali</td>
<td>VN</td>
<td>Viet Nam</td>
<td>YU</td>
<td>Yugoslavia</td>
<td>Yugoslavia</td>
<td>YU</td>
</tr>
<tr>
<td>BF</td>
<td>Burkina Faso</td>
<td>HU</td>
<td>Hungary</td>
<td>MN</td>
<td>Mongolia</td>
<td>ZW</td>
<td>Zimbabwe</td>
<td>AL</td>
<td>Albania</td>
<td>Albania</td>
<td>AL</td>
</tr>
<tr>
<td>BG</td>
<td>Bulgaria</td>
<td>IE</td>
<td>Iceland</td>
<td>MR</td>
<td>Mauritania</td>
<td>AM</td>
<td>Armenia</td>
<td>AT</td>
<td>Austria</td>
<td>Austria</td>
<td>AT</td>
</tr>
<tr>
<td>BJ</td>
<td>Benin</td>
<td>IL</td>
<td>Israel</td>
<td>MW</td>
<td>Malawi</td>
<td>CI</td>
<td>Côte d'Ivoire</td>
<td>CM</td>
<td>Cameroon</td>
<td>Cameroon</td>
<td>CM</td>
</tr>
<tr>
<td>BR</td>
<td>Brazil</td>
<td>IS</td>
<td>Iceland</td>
<td>NX</td>
<td>Mexico</td>
<td>CN</td>
<td>China</td>
<td>CU</td>
<td>Cuba</td>
<td>Cuba</td>
<td>CU</td>
</tr>
<tr>
<td>BY</td>
<td>Belarus</td>
<td>JP</td>
<td>Japan</td>
<td>NE</td>
<td>Niger</td>
<td>CZ</td>
<td>Czech Republic</td>
<td>DE</td>
<td>Germany</td>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>CA</td>
<td>Canada</td>
<td>KE</td>
<td>Kenya</td>
<td>NL</td>
<td>Netherlands</td>
<td>CH</td>
<td>Switzerland</td>
<td>CF</td>
<td>Central African Republic</td>
<td>CG</td>
<td></td>
</tr>
<tr>
<td>CF</td>
<td>Central African Republic</td>
<td>KG</td>
<td>Kyrgyzstan</td>
<td>NO</td>
<td>Norway</td>
<td>CI</td>
<td>Côte d'Ivoire</td>
<td>CM</td>
<td>Cameroon</td>
<td>Cameroon</td>
<td>CM</td>
</tr>
<tr>
<td>CG</td>
<td>Congo</td>
<td>KP</td>
<td>Democratic People's Republic of Korea</td>
<td>NZ</td>
<td>New Zealand</td>
<td>PL</td>
<td>Poland</td>
<td>PT</td>
<td>Portugal</td>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>CH</td>
<td>Switzerland</td>
<td>KR</td>
<td>Republic of Korea</td>
<td>RO</td>
<td>Romania</td>
<td>RU</td>
<td>Russian Federation</td>
<td>SD</td>
<td>Sudan</td>
<td>Sudan</td>
<td>SD</td>
</tr>
<tr>
<td>CI</td>
<td>Côte d'Ivoire</td>
<td>LC</td>
<td>Saint Lucia</td>
<td>SE</td>
<td>Sweden</td>
<td>SG</td>
<td>Singapore</td>
<td>AL</td>
<td>Albania</td>
<td>Albania</td>
<td>AL</td>
</tr>
<tr>
<td>CM</td>
<td>Cameroon</td>
<td>LI</td>
<td>Liechtenstein</td>
<td>SI</td>
<td>Slovenia</td>
<td>LG</td>
<td>Luxembourg</td>
<td>LT</td>
<td>Lithuania</td>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>CN</td>
<td>China</td>
<td>LK</td>
<td>Sri Lanka</td>
<td>SG</td>
<td>Singapore</td>
<td>AM</td>
<td>Armenia</td>
<td>AT</td>
<td>Austria</td>
<td>Austria</td>
<td>AT</td>
</tr>
<tr>
<td>CU</td>
<td>Cuba</td>
<td>LR</td>
<td>Liberia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A RADIO FREQUENCY IDENTIFICATION (RFID) SECURITY SYSTEM HAVING AN RF EMULATING CIRCUIT

This invention relates generally to a Radio Frequency Identification (RFID) security device and, more specifically, to an RFID security system wherein the RFID tag and its complementary reader/interrogator device utilize an RF emulating circuit which substitutes the RF portion of the data communication with a hardwired secure bus.

Electronic keys have long been used to prevent 15 unauthorized entry to restricted areas. Presently, there are several different types of electronic keys in the market place. While each of these types of keys do work, they each have certain drawbacks.

One such type of an electronic key is a serial EEPROM 20 based electronic key. Serial EEPROM based keys require 4 to 5 separate contacts in order to operate. One contact is used for each of power, ground, clock, and data. Two contacts may be used for data transfer (i.e., one as an input contact and one as an output contact). Each of the multiple contacts in the serial EEPROM based key must make proper contact in order to transfer clock and data through them. In apartment or hotel applications, users returning from a swimming pool may insert a wet key into the lock. This causes poor contact or shorts between the contacts which prevents proper transfer of data, thereby preventing the lock from opening. Furthermore, the wrong polarity of key insertion into the lock will cause damage to the lock electronics or EEPROM device, thereby rendering the key useless. Thus, moisture, polarity of insertion, and wear and/or damage to the multiple contacts are problematic in this type of electronic key.

A second type of electronic key utilizes access control 10 RFID tags. In these types of keys, a card or tag is presented to a reading device to gain access to a building. In most cases, this type of electronic key is used for identification applications rather than for security. Using this type of electronic key for security (apartment and hotel locks) creates a problem since these types of keys are not very secure. Covert readers, even battery powered readers, can power-up the tag and steal its code without the owner’s knowledge, even if the tag is in the owner’s pocket or purse.
One way to solve the problems associated with access control RFID tags is to have an encrypted electronic key. Several types of electronic keys include encryption algorithms on the die itself. Some encryption algorithms will allow the code on the electronic key to be encrypted and changed every time the key is read. While these types of electronic keys prevent unauthorized “code grabbing”, they are considerably more expensive than RFID tag devices. Thus, the security comes at the expense of cost.

Therefore, a need existed to provide an improved RFID security device. The improved RFID security should require few contacts for data transfer. The improved RFID security device must further be universal in polarity. The improved RFID security device must be resistant to environmental elements. The improved RFID security device must also be able to be used for security and must further be resistant to “code grabbing”. The improved RFID security device would be a low cost solution to solving the above mentioned problems. The improved RFID security system would replace the RF portion of both the electronic key and the reading mechanism with simpler lower cost circuitry.

In accordance with one embodiment of the present invention, it is an object of this invention to provide an improved RFID security device.

It is another object of the present invention to provide an improved RFID security device that requires few contacts for data transfer.

It is still another object of the present invention to provide an improved RFID security device that is universal in polarity.

It is yet another object of the present invention to provide an improved RFID security device that is resistant to environmental elements.

It is still a further object of the present invention to provide an improved RFID security device that is able to be used for security and must further be resistant to “code grabbing”.

It is still a further object of the present invention to provide an improved RFID security device that would be a low cost solution to solving the above mentioned problems.
It is still another object of the present invention to provide an improved RFID security system that would replace the RF portion of both the electronic key and the reading mechanism with lower cost circuitry.

In accordance with one embodiment of the present invention, a Radio Frequency Identification (RFID) security system is disclosed. The RFID security system uses an electronic key for storing data. A reading mechanism is provided and is used for reading a modulated signal having the data stored on the electronic key when the electronic key is coupled to the reading mechanism. An RF emulating circuit is coupled to the reading mechanism for emulating an RF energy signal to the electronic key for allowing the reading mechanism to read the data stored on the electronic key when the electronic key is coupled to the reading mechanism.

The foregoing and other objects, features, and advantages of the invention will be apparent from the following, more particular, description of the preferred embodiments of the invention, as illustrated in the accompanying drawing.

Figure 1 is a simplified electrical block diagram of the present invention.

Figure 2 is a simplified electrical block diagram of one embodiment of the present invention.

Figure 3 is a simplified electrical schematic of one embodiment of the RF emulating circuit used in the present invention.

Figure 4 is a simplified electrical schematic of a second 10 embodiment of the RF emulating circuit used in the present invention.

Figure 5 is an electrical block diagram of the simplified reading mechanism used in the present invention.

Figure 6A is a timing diagram of the modulated RF energy 15 carrier signal.

Figure 6B is a timing diagram of the demodulated base band data signal.

Referring to Figure 1, an improved RFID security system 10 (hereinafter system 10) is shown. The system 10 uses a Radio Frequency Identification (RFID) tag device 12. The RFID tag device 12 is configured as an electronic key and is programmed to store data on the electronic key. When the RFID tag 12 is coupled to the reading mechanism 14 via the RF emulating circuit 16, the data stored on the RFID tag device 12 will be read by the reading mechanism 14. If the proper RFID tag 12 has been
inserted into the reading mechanism 14, the reading mechanism 14 will release a locking device (not shown) or perform other actions according to its specific application.

In order to read the data on the RFID tag device 12, an energizing circuit needs to be coupled to the RFID tag device 12 and the reading mechanism 14. In the present invention, the RF portions of both the RFID tag device 12 and the reading mechanism 14 have been replaced with lower cost circuitry. The present invention uses an RF emulating circuit 16. The RF emulating circuit 16 is used to emulate an RF energy carrier signal to the RFID tag device 12. A “modulated” signal is then sent back to the reading mechanism 14. The reading mechanism 14 is able to filter out the carrier signal in order to read the data stored on the RFID tag device 12.

Referring now to Figure 2 wherein like numerals and symbols represent like elements, one embodiment of how the RFID tag device 12 is configured as an electronic key 18 is shown. The electronic key is basically comprised of two main components: the RFID tag device 12 and a contact device 20. As stated above, the RFID tag device 12 is used to store the data to be read by the reading mechanism 14. The RFID tag device 12 is coupled to the contact device 20. The contact device 20 is used to couple the RFID tag device 12 to the RF emulating circuit 16. When the electronic key 18 is coupled to the RF emulating circuit 16, the RF emulating Circuit 16 will emulate and send an RF energy carrier signal to the RFID tag device 12. The RFID tag device 12 is energized by the incoming RF energy carrier signal and is activated. Once it is activated, the RFID tag device 12 sends back the contents of its memory by modulating the incoming RF energy carrier signal. This “modulated” signal is then sent back to the reading mechanism 14. The reading mechanism 14 is then able to filter out the carrier signal and read the data stored on the RFID tag device 12.

Referring to Figure 3 wherein like numerals and symbols represent like elements, one embodiment of the RF emulating circuit 16 is shown. The RF emulating circuit 16 will replace the L-C circuit of both the prior art electronic key and of the reading mechanism thereby allowing for the simplified electronic key 18 and the simplified reading mechanism 14 which form part of the present invention. In the embodiment depicted in Figure 3, the RF emulating circuit 16 uses a switching element
22. In the preferred embodiment of the present invention, the switching element 22 is a transistor. A resistor 24 has a first terminal coupled to the switching element 22 and a second terminal coupled to a voltage source Vcc. A second resistor 26 has a first terminal coupled to the switching element 22 and a second terminal coupled to a contact device 28. The contact device 28 is used to couple the RF emulating circuit 16 to the electronic key 18 (Figures 1 and 2) when the electronic key 18 (Figures 1 and 2) is inserted into the reading mechanism 14 (Figures 1 and 2) when the electronic key 18 (Figures 1 and 2) is inserted into the reading mechanism 14 (Figures 1 and 2).

The first resistor 24 and the second resistor 26 form a voltage divider circuit. The switching element 22 along with the first 24 and the second resistor 26 form a drive circuit to simulate the carrier signal to the RFID tag device 12 (Figures 1 and 2). Careful selection of the resistors 24 and 26 and the on resistance of the switching element 22 will allow the RF emulating circuit 16 to drive the RFID tag device 12 (Figures 1 and 2) with sufficient current and voltage for power up and proper operation of the RFID tag device 12.

When the RFID tag device 12 (Figures 1 and 2) is powered by the carrier signal from the RF emulating circuit 16, the RFID tag device’s internal clock runs synchronously with the carrier signal and the stored data in the RFID tag device 12 is used to “modulate” the carrier signal. This modulated RF signal is fed to the simplified RFID reader 14 via the RF emulating circuit 16. In the embodiment depicted in Figure 3, the on resistance of the RFID tag device 12 causes a square wave to be superimposed on the carrier signal present at point B (see Figure 6A). The reading mechanism 14 (Figures 1 and 2) can then demodulate the signal and extract the tag data stream to obtain the data stored on the RFID tag device 12.

As an example, assume that the RFID tag device 12 has an on resistance of 10k ohms and an off resistance of 100k ohms. Both the first resistor 24 and the second resistor 26 have a resistance of 10k ohms. The voltage source will supply a voltage level of 5 volts. In operation, the switching element 22 will receive a carrier signal from the reading mechanism 14 (Figures 1 and 2). The carrier signal will have a high and low voltage level which will activate and deactivate the switching element 22 (i.e.,
the carrier signal may have a voltage level from 0 to 5 volts). When the switching element 22 is activated, the voltage at Point B will be a square wave with a voltage level of 0 volts. When the switching element is deactivated, the voltage at Point B will be either 4.2 volts for the off resistance level of the RFID tag device 12 or 1.7 volts for the on resistance level of the RFID tag device 12. The modulated carrier signal is shown in Figure 6A. The signal is demodulated to extract the data content of the memory in the RFID tag device 12. The simplified reader 14 also has a microcontroller (or processor) to decode the demodulated signal. See Figures 6A and 63 for modulate and demodulated signals respectively. The carrier signal can be filtered out in the simplified reader 14 with a simple filter or comparator circuit. The data stream (see Figure 6B) from 1.7 volts to 4.2 volts can then be driven into a data decoding circuitry (microcontroller) with no amplification.

Referring now to Figure 4 wherein like numerals and symbols represent like elements, a second embodiment of the RF emulating circuit 16 is shown. As stated above, the RF emulating circuit 16 will replace the L-C circuit of both the prior art electronic key and of the reading mechanism thereby allowing for the simplified electronic key 18 (Figure 1 and 2) and the reading mechanism 14 (Figure 1 and 2) which form part the present invention. In the embodiment depicted in Figure 4, the RF emulating circuit 16 uses a single resistor 30. The resistor has a first terminal coupled to an output of the reading mechanism 14 (Figures 1 and 2) and a second terminal coupled to an input of the reading mechanism 14 (Figures 1 and 2). The second terminal of the resistor 30 is also coupled to a contact circuit 28. The contact circuit 28 is used to couple the RF emulating circuit 16 to the electronic key 18 (Figures 1 and 2) when the electronic key 18 (Figures 1 and 2) is inserted into the reading mechanism 14 (Figures 1 and 2). The operation of the embodiment depicted in Figure 4 will operate in a similar manner to that disclosed in Figure 3. The carrier signal will be driven onto the resistor 30. The voltage level at Point B will again be one of three voltage levels. The carrier signal can be filtered out with a simple filter or comparator circuit. As the RFID tag device 12 is activated, a modulated signal appears at Point B. The data signal can be obtained by demodulating the output signal. The resulting signal can then be driven into a data decoding circuitry with no amplification.
Referring to Figure 5 wherein like numerals and symbols represent like elements, the reading mechanism 14 used in the present invention is shown. The reading mechanism 14 greatly simplifies the RFID readers currently being used to read RFID tag devices. The reading mechanism 14 is used for reading the data stored on the electronic key when the electronic key is coupled to the reading mechanism 14. The reading mechanism 14 uses a processor for reading the data stream containing the data stored on the electronic key 18 (Figure 2) when the electronic key 18 (Figure 2) is coupled to the reading mechanism 14 via the RF emulating circuit 16 (Figures 1-4). In the embodiment depicted in Figure 5, the processor is a microcontroller. A timing device 34 is coupled to the processor 32 and to the RF emulating circuit 16. The timing device 34 is used for providing a clock signal to both the processor 32 and to the RF emulating Circuit 16. The timing device 34 may be an oscillator or any other type of device that may generate a clock signal. A signal passing circuit 36 (i.e., demodulator) is coupled to the processor 32 and to the RF emulating circuit 16. The signal passing circuit 36 is used for demodulating and filtering out the carrier signal and for driving the data stream into the processor 32 with no amplification. It should be noted that a comparator circuit coupled to a reference signal or a low pass filter are two examples of a signal passing circuit 36. In the preferred embodiment of the present invention, a low pass filter is used.

While the invention has been particularly shown and described with reference to preferred embodiments thereof, it will be understood by those skilled in the art that the foregoing and other changes in form and details may be made therein without departing from the spirit and scope of the invention.
CLAIMS

1. A Radio Frequency Identification (RFID) security system comprising:
   an electronic key for storing data;
   a reading mechanism for generating an RF clocking signal and for
demodulating and reading a modulated signal having said data stored on said electronic
key when said electronic key is coupled to said reading mechanism; and
   an RF emulating circuit coupled to said reading mechanism for emulating an RF
ergy carrier signal to said electronic key allowing said electronic key to modulate
said RF energy carrier signal and for allowing said reading mechanism to read said data
stored on said electronic key when said electronic key is coupled to said reading
mechanism.

2. A Radio Frequency Identification (RFID) security system in accordance
with Claim 1 wherein said electronic key comprises:
   an RFID tag device for storing said data on said electronic key;
   a key contact coupled to said RFID tag device for coupling said RFID tag
device to said RF emulating circuit when said electronic key is coupled to said reading
mechanism.

3. A Radio Frequency Identification (RFID) security system in accordance
with Claim 1 wherein said reading mechanism comprises:
   a processor for reading a demodulated baseband data signal having said data
stored on said electronic key when said electronic key is coupled to said reading
mechanism;
   a timing device coupled to said processor and to said RF emulating circuit for
providing clock signals to said processor and said RF emulating circuit; and
   a signal passing circuit coupled to said processor and to said RF emulating
circuit for deriving said demodulated baseband data signal and passing said
demodulated baseband data signal to said processor for said processor to read said data
stored on said electronic key.

4. A Radio Frequency Identification (RFID) security system in accordance
with Claim 3 wherein said signal passing circuit is a low pass filter.
5. A Radio Frequency Identification (RFID) security system in accordance with Claim 3 wherein said signal passing circuit is a comparator.

6. A Radio Frequency Identification (RFID) security system in accordance with Claim 1 wherein said RF emulating circuit comprises:
   - a switching device coupled to said reading mechanism;
   - a voltage divider circuit coupled to said switching device; and
   - a voltage source coupled to said voltage divider circuit.

7. A Radio Frequency Identification (RFID) security system in accordance with Claim 6 wherein said RF emulating circuit further comprises contacts coupled to said voltage divider circuit for coupling said electronic key to said RF emulating circuit.

8. A Radio Frequency Identification (RFID) security system in accordance with Claim 6 wherein said switching device is a transistor having a first terminal coupled to said voltage divider circuit, a second terminal coupled to said reading mechanism, and a third terminal coupled to ground.

9. A Radio Frequency Identification (RFID) security system in accordance with Claim 6 wherein said voltage divider circuit comprises:
   - a first resistor having a first terminal coupled to said switching device and a second terminal coupled to said voltage source; and
   - a second resistor having a first terminal coupled to said switching device and a second terminal coupled to said reading mechanism.

10. A Radio Frequency Identification (RFID) security system in accordance with Claim 1 wherein said RF emulating circuit comprises a resistor coupled to said reading mechanism.

11. A Radio Frequency Identification (RFID) security system in accordance with Claim 10 wherein said RF emulating circuit further comprises contacts coupled to said resistor for coupling said electronic key to said RF emulating circuit.

12. A Radio Frequency Identification (RFID) security system comprising:
   - an electronic key for storing data wherein said electronic key comprises:
     - an RFID tag device for storing said data on said electronic key;
a key contact coupled to said RFID tag device for coupling said RFID tag device to said RF emulating circuit when said electronic key is coupled to said reading mechanism; and

a reading mechanism for demodulating and reading a modulated signal having said data stored on said electronic key when said electronic key is coupled to said reading mechanism wherein said reading mechanism comprises:

a processor for reading a demodulated baseband data signal having said data stored on said electronic key when said electronic key is coupled to said reading mechanism;

time a timing device coupled to said processor and to said RF emulating circuit for providing clock signals to said processor and said RF emulating circuit; and

a signal passing circuit coupled to said processor and to said RF emulating circuit for deriving said demodulated baseband data signal and passing said demodulated baseband data signal to said processor for said processor to read said data stored on said electronic key; and

an RF emulating circuit coupled to said reading mechanism for emulating an RF energy signal to said electronic key for allowing said reading mechanism to modulate said RF energy carrier signal and for allowing said reading mechanism to read said data stored on said electronic key when said electronic key is coupled to said reading mechanism.

13. A Radio Frequency Identification (RFID) security system in accordance with Claim 12 wherein said signal passing circuit is a low pass filter.

14. A Radio Frequency Identification (RFID) security system in accordance with Claim 12 wherein said signal passing circuit is a comparator.

15. A Radio Frequency Identification (RFID) security system in accordance with Claim 12 wherein said RF emulating circuit comprises:

a switching device coupled to said reading mechanism;

a voltage divider circuit coupled to said switching device; and

a voltage source coupled to said voltage divider circuit.

16. A Radio Frequency Identification (RFID) security system in accordance with Claim 15 wherein said RF emulating circuit further comprises contacts coupled to
said voltage divider circuit for coupling said electronic key to said RF emulating circuit.

17. A Radio Frequency Identification (RFID) security system in accordance with Claim 15 wherein said switching device is a transistor having a first terminal coupled to said voltage divider circuit, a second terminal coupled to said reading mechanism, and a third terminal coupled to ground.

18. A Radio Frequency Identification (RFID) security system in accordance with Claim 15 wherein said voltage divider circuit comprises:

   a first resistor having a first terminal coupled to said switching device and a second terminal coupled to said voltage source; and

   a second resistor having a first terminal coupled to said switching device and a second terminal coupled to said reading mechanism.

19. A Radio Frequency Identification (RFID) security system in accordance with Claim 12 wherein said RF emulating circuit comprises a resistor coupled to said reading mechanism.

20. A Radio Frequency Identification (RFID) security system in accordance with Claim 19 wherein said RF emulating circuit further comprises contacts coupled to said resistor for coupling said electronic key to said RF emulating circuit.
Fig. 5

Fig. 6a

Fig. 6b
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**
IPC 7 G06K7/00

According to international Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**
Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>FR 2 336 741 A (KREFT HANS DIEDRICH) 22 July 1977 (1977-07-22) page 1, line 20 - line 36 page 3, line 40 - page 4, line 39 page 6, line 35 - page 8, line 20 figure 7</td>
<td>1-5, 12-14</td>
</tr>
<tr>
<td>A</td>
<td>US 5 841 390 A (TSUI PHILIP Y W) 24 November 1998 (1998-11-24) abstract column 1, line 20 - column 2, line 34 column 3, line 35 - column 6, line 27</td>
<td>A, 1,3,12</td>
</tr>
<tr>
<td>A</td>
<td>US 4 990 756 A (HOEMANN JAMES D) 5 February 1991 (1991-02-05) abstract column 1, line 5 - column 2, line 36 column 5, line 8 - column 6, line 3</td>
<td>A, 1,3,12</td>
</tr>
</tbody>
</table>

**X** Further documents are listed in the continuation of box C.  

**X** Patent family members are listed in annex.

* Special categories of cited documents:
  
  "A" document defining the general state of the art which is not considered to be of particular relevance
  
  "E" earlier document but published on or after the international filing date
  
  "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  
  "O" document referring to an oral disclosure, use, exhibition or other means
  
  "P" document published prior to the international filing date but later than the priority date claimed

Date of the actual completion of the international search: 18 April 2000

Date of mailing of the international search report: 27/04/2000

Name and mailing address of the ISA: European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer: Jacobs, P.
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>US 5 679 945 A (RENNER G FRED ET AL)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21 October 1997 (1997-10-21)</td>
<td></td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6005508 A</td>
</tr>
<tr>
<td>US 4990756 A</td>
<td>05-02-1991</td>
<td>NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2217052 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9630857 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 4321192 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 69216907 D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 69216907 T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HK 1003017 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 5349649 A</td>
</tr>
</tbody>
</table>