United States Patent

Hedin

[15] **3,641,498**

[45] **Feb. 8, 1972**

[54] **KEYS FOR ELECTRONIC SECURITY APPARATUS**

[72] Inventor: **Robert A. Hedin**, San Pedro, Calif.

[73] Assignee: **R. B. Phinizy**, Anaheim, Calif.

[22] Filed: **Mar. 27, 1970**

[21] Appl. No.: **23,272**

Related U.S. Application Data

[63] Continuation-in-part of Ser. No. 628,599, Apr. 5, 1967, abandoned, Continuation-in-part of Ser. No. 889,666, Dec. 31, 1969.

[52] **U.S. Cl.** ....**340/164 R,** 340/166 R

[51] **Int. Cl.** **H04q 9/00**

[58] **Field of Search**....................340/149, 166, 173, 164, 147; 235/61.11 A

[56] **References Cited**

UNITED STATES PATENTS

3,178,803	4/1965	Schibli et al.	340/166 UX
2,973,507	2/1961	Grondin	340/164
3,183,485	5/1965	Gubbage	340/166 X
3,191,151	6/1965	Price	340/166
3,245,697	4/1966	Nugent	340/149 UX
3,360,785	12/1967	Ishidate	340/166 X
3,384,879	5/1968	Stahl et al.	340/166 X
3,396,379	8/1968	Chapman et al.	340/147 X
3,399,473	9/1968	Jaffee	40/2.2
3,428,953	2/1969	Baxter et al.	340/166 X
3,525,083	8/1970	Slob et al.	340/166 X

OTHER PUBLICATIONS

"Optical Hole Sensing Using Fiber Optics" Stahl et al *Applied Optics* July 1966, Vol. 5, No. 7, p 1203-1206 (250-227)

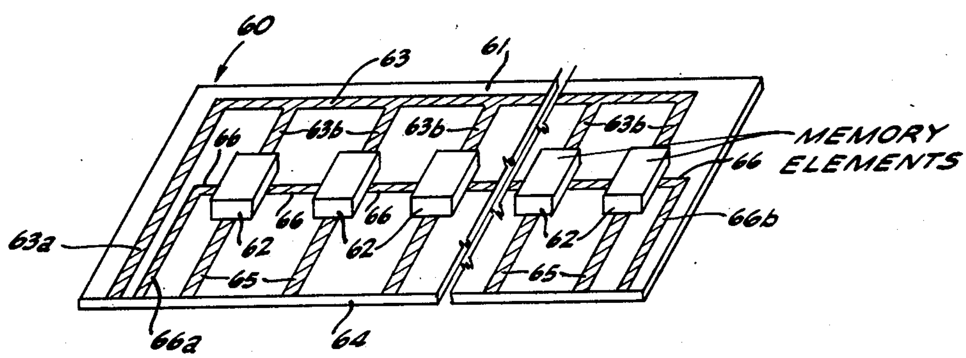
"Memory Array Demit et al *IBM Technical Disclosure Bulletin* Vol. 10, No. 1, June 1967 p 95 (340-173 sp)

Primary Examiner—Donald J. Yusko
Attorney—Teagno & Toddy

[57] **ABSTRACT**

A key is constructed with a base member of epoxy glass on which are electrically conductive contact strips offering a binary code permutation of open and closed circuit paths for controlling a security apparatus such as an electronic lock or computer. The code permutation can be established in the key by applying electric current that changes the state of the circuits on the key. For the purpose, the key circuits are equipped with fusible elements or magnetic memory elements. The memory elements may be of a type that will change the code when the key is used. The key may have a portion forming an identification card. In further forms the key will have eddy current rings that will react when applied to proper key-receiving means, and the key may comprise an optical mask containing a binary code in the form of a pattern of opaque and translucent areas.

25 Claims, 21 Drawing Figures



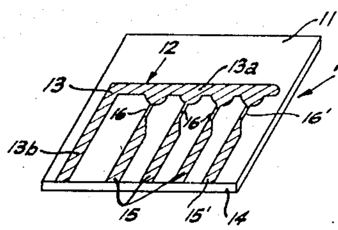


Fig 1

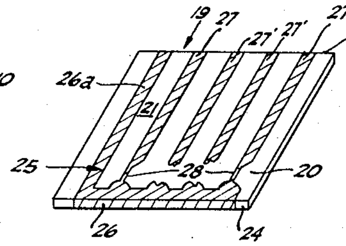


Fig 2a

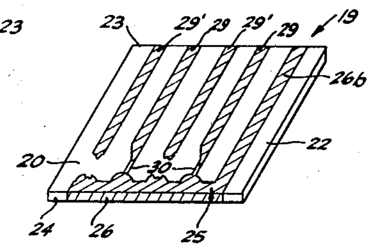


Fig 2b

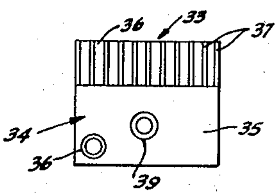


Fig 3a

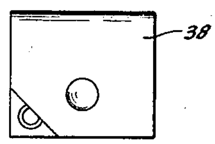


Fig 3b

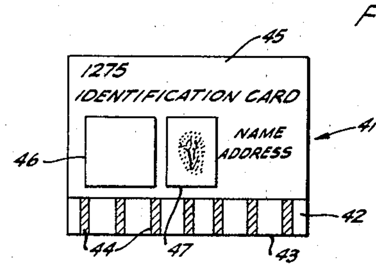


Fig 4

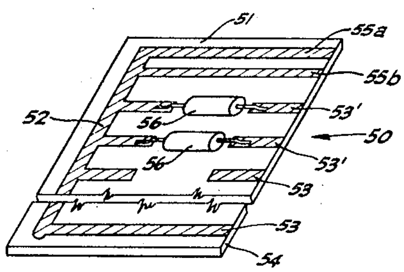


Fig 5

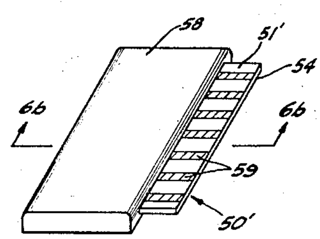


Fig 6a

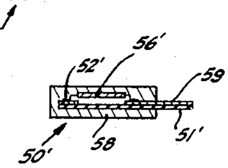


Fig 6b

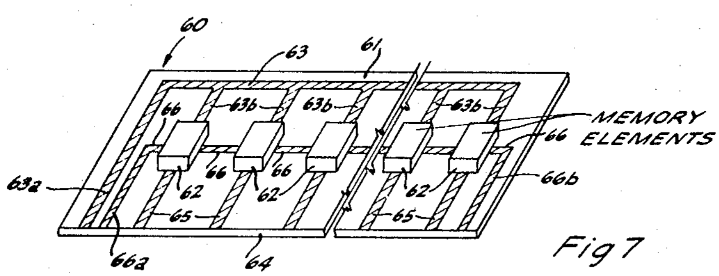


Fig 7

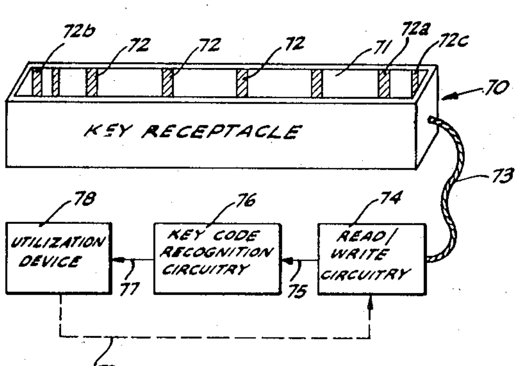


Fig 8

INVENTOR.
ROBERT A. HEDIN

BY Teague & Teddy

ATTORNEYS

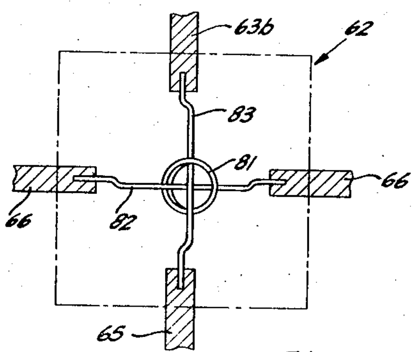


Fig 9a

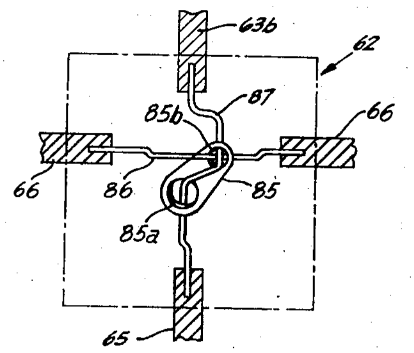


Fig 9b

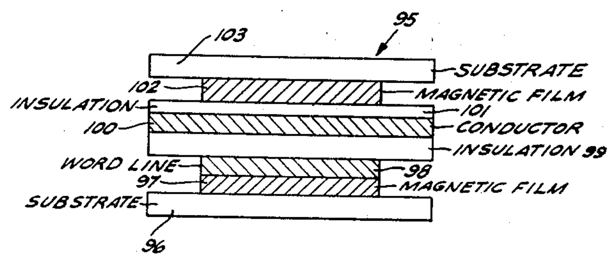


Fig 10

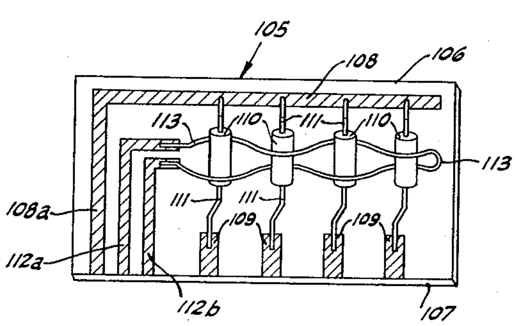


Fig 11

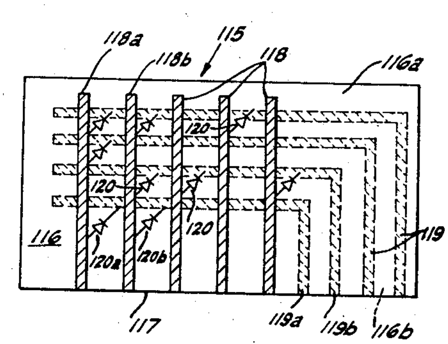


Fig 12

INVENTOR.
ROBERT A. HEDIN

BY [signature]

ATTORNEYS

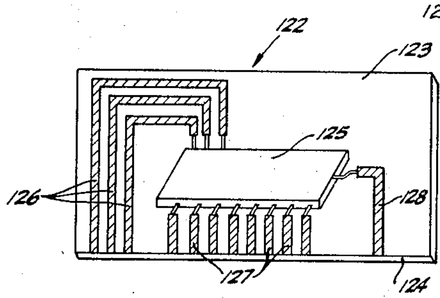


Fig 13

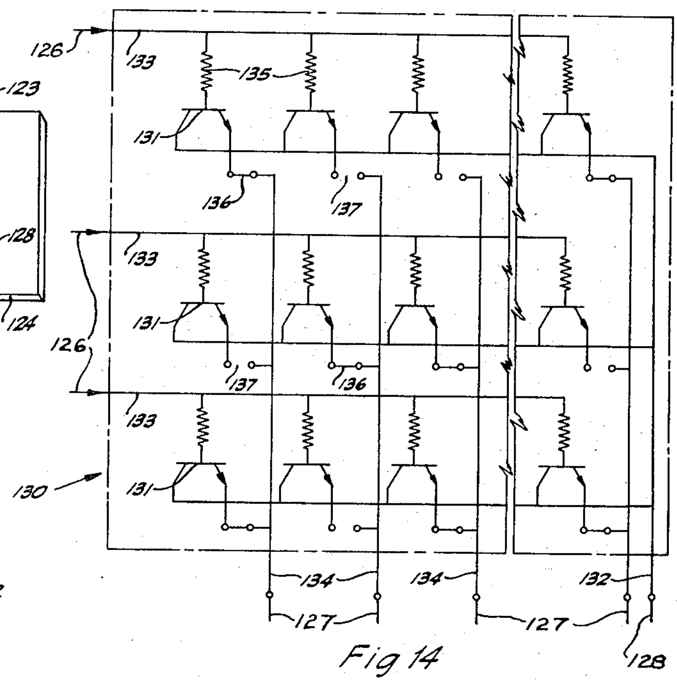


Fig 14

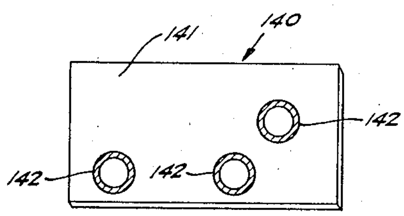


Fig 15

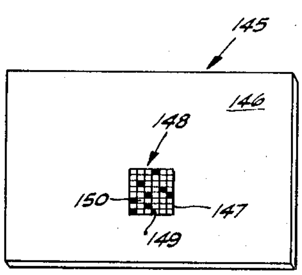


Fig 16

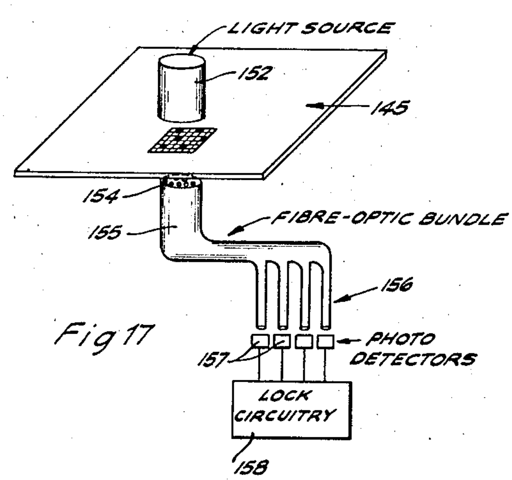


Fig 17

INVENTOR.
ROBERT A. HEDIN

BY Tiegno & Toddy

ATTORNEYS

KEYS FOR ELECTRONIC SECURITY APPARATUS

This application is a continuation-in-part of the earlier U.S. Pat. applications of Hedin Ser. No. 628,599 filed Apr. 5. 1967, now U.S. Pat. No. 3,544,769 entitled Electronic Identification and Credit Card System, and of Hedin et al. Ser. No. 889,666 filed Dec. 31, 1969, entitled Key Controlled Electronic Security System.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to keys that are utilized with electronic locks and other electronic security apparatus and more particularly to keys having a binary permutation code stored in a form which may be accessed electrically, magnetically or optically.

2. Description of the Prior Art

Recent years have seen increasing acceptance of electronic systems for controlling entrances to protected areas and for identifying individuals without the requirement for a guard. Typically, a door may be provided with an electronic lock which responds to a preselected binary permutation code contained on a key. A person wishing to gain entrance through the door inserts his key in a receptacle associated with the lock, and lock circuitry determines if the key has the correct coding. If so, an actuation signal is provided to an electric door latch or strike; if the key has an improper code, there will be no actuation signal, and at the same time the system may generate an alarm signal.

Electronic locks have several significant advantages as compared with conventional lock systems. For example, a very large number of codes are available on a key of small size. The number of combinations available may be expressed as follows:

Total number of combinations $=(n!/r!(n-r)!)$ where n is the number of available binary coded elements on the key, and r is the number of stored binary one bits required to energize the electronic lock. For example, for a key having 20 binary coded elements (n=20) used with an electronic lock requiring r=10 stored binary one bits for energization, a total of (20!/10! 10!)=184,756 combinations are available.

In electronic locks, very simple circuit changes permit the lock rapidly to be changed so as to be actuated by any of the potentially available key codes. The large number of key combinations, together with the ease with which alarm means may be incorporated in the lock, make electronic locks significantly harder to pick than mechanical systems. Moreover, a large number of remote electronic key identification stations can be monitored at a single central control station.

An electronic lock using a binary permutation coded key is described in U.S. Pat. No. 3,392,558 to R. A. Hedin et al. The circuitry employed will recognize a particular binary permutation code stored on a key and will apply a signal to actuate a door latch or other utilization device. Other electronic lock circuitry and central electronic security systems incorporating such circuitry are set forth in the copending application Ser. No. 889,666, mentioned above.

The use of binary coded keys is not limited permutation of the circuits to control of with contacts protected key-receiving means for applying the code permutation to an electronic security apparatus, said electronic security apparatus being actuatable in response to a predetermined code permutation being applied thereto and being nonactuatable upon the application of a code permutation other than said predetermined code permutation thereto, a substantially flat, electrically nonconductive base member a plurality of electrically conductive strips mounted in spaced relation to one another on said base member, each of said strips extending longitudinally on a forward portion of said member and presenting a surface for engaging a contact of said key-receiving uses are described in the article by Robert A. Hedin entitled "Electronic Identification of the Human Population for Controlled Access and Automatic Crediting", appearing in the periodical *Industrial Security*, Vol. 11, No. 2.

Described herein are a variety of keys for use in electronic locks, automatic crediting systems and the like. While referring merely to "keys", it is to be understood that the keys may be formed with a portion that will bear information such as is needed on a credit or other identification card. The keys disclosed include both permanently coded and alterable data configurations. The latter keys are particularly well suited for application wherein data is to be periodically updated.

SUMMARY OF THE INVENTION

In accordance with the present invention, there are set forth various keys for use with electronic locks that respond to a binary permutation code stored in the key. I mention locks for convenience of description, and when referring to a lock I intend to include other electronic security apparatus that will be controlled by a key. In different embodiments, the code may be entered in the key at the time of manufacture, entered subsequent to manufacture and thereafter permanently retained, or entered and/or revised at any time. Depending upon the embodiment, the codes may be sensed electrically, magnetically or optically.

In one form, the key code may comprise a permutation of open or closed AC or DC electrical paths in a circuit printed or etched on an electrically insulative substrate or base member. Keys of this type may be precoded at the time of manufacture. However, as a feature of my invention I may equip the keys with elements for subsequent entry of a binary code permutation.

More particularly, the keys may have memory elements for storage of the code. These memory elements may comprise single- or multiple-apertured magnetic cores or other magnetic storage elements, or may comprise a diode or transistor matrix. Certain of the magnetic memory element keys are particularly well adapted for the storage of data which is to be altered from time to time.

Another key embodiment incorporates a plurality of electrically conductive strips of ring shape located at selected positions on an electrically insulative, nonmagnetic base member substrate. The location of these eddy current rings, the presence of which may be sensed magnetically, represent the code of the key. In yet another embodiment, the key may include an optical mask containing a pattern of transparent and opaque areas that form the coding of the key. The position of the optically coded regions may be sensed using a fiber optic bundle and an associated plurality of photodetectors.

Thus, it is an object of the present invention to provide improved keys for use with an electronic lock or other electronic device that will respond to a binary code permutation of electrical circuits.

It is another object of the present invention to provide keys for electronic locks, which keys contain binary codes which may be sensed electrically, magnetically or optically.

Another object of the present invention is to provide various embodiments of keys for electronic locks, wherein a code may be represented on a key by open or closed electrical paths in a printed circuit, by data stored in magnetic or other memory elements, by positions of active components in a diode or transistor matrix, by the location of eddy current rings on a nonmagnetic substrate, or by the juxtaposition of opaque and transparent regions in an optical mask.

Still another object of the present invention is to provide keys having planar, electrically insulative base members or substrates, a set of spaced, parallel conductive strip terminals adjacent a common edge of the substrate and means for electrically connecting or disconnecting selected terminals to a common conductor also disposed on the substrate.

It is still another object of the present invention to provide keys incorporating an electrically insulative substrate or base member having a plurality of conductive members offering contact-engaging surfaces thereon, and including memory elements associated with selected members for storing a binary permutation code.

A further object of the present invention is to provide a coded device useful as an identification or credit card for use with electronic code recognition circuitry, the device containing memory elements permitting storage of alterable coded data.

It is a further object of the present invention to provide a key wherein the coding is represented by the positions of a plurality of eddy current rings on a nonmagnetic substrate.

Yet a further object of the preset invention is to provide a key including an optical mask having juxtaposed opaque and transparent regions, the coding represented thereby being determinable by use of a fiber optic bundle in conjunction with a plurality of photodetectors.

BRIEF DESCRIPTION OF THE DRAWINGS

Still other objects, features and attendant advantages of the present invention will become apparent to those skilled in the art from a description of the preferred embodiments constructed in accordance herewith, taken in conjunction with the accompanying drawings, wherein like numerals designate like parts in the several figures, and wherein:

FIG. 1 is a plan view of a printed circuit key having fusible elements for the entry of a code;

FIGS. 2*a* and 2*b* respectively show the top and bottom view of another key embodiment having a pattern of open and closed electrical paths in a printed circuit;

FIGS. 3*a* and 3*b* illustrate one manner in which a key of the type shown in FIG. 1 may be constructed to obscure the coding thereof;

FIG. 4 shows a key constructed according to the invention and including an identification or credit card portion;

FIG. 5 is a simplified perspective view of a key embodiment wherein a binary code is represented by a permutation of open or closed AC electrical paths;

FIGS. 6*a* and 6*b* respectively show perspective and cross-sectional views of an encapsulated key for an electronic lock;

FIG. 7 is a perspective view of a key incorporating a plurality of memory elements which store coded data;

FIG. 8 is a simplified electrical block diagram of utilization circuitry for a key of the type shown in FIG. 7;

FIGS. 9*a* and 9*b* show various types of magnetic core devices which may be employed as memory elements in the key of FIG. 7;

FIG. 10 is a sectional view of a thin film magnetic memory element that may be utilized in the key of FIG. 7;

FIG. 11 is a perspective view of a key employing plated wire memory elements;

FIG. 12 is a simplified, somewhat diagrammatic view of a key employing a diode matrix;

FIG. 13 is a perspective view of a key employing an integrated diode or transistor matrix and requiring an appropriate access code for interrogation of the key;

FIG. 14 is an electrical schematic diagram of a transistor matrix array that may be utilized in the key of FIG. 13;

FIG. 15 is a perspective view of a key incorporating a plurality of ring-shaped electrically conductive strips, the positions of which may be detected magnetically;

FIG. 16 is a top plan view of a key incorporating an optical mask coded with opaque and transparent regions;

FIG. 17 diagrammatically illustrates apparatus for accessing the code contained in the key of FIG. 16.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, and particularly to FIG. 1 thereof, there is shown a first embodiment of a key having certain features like those which are set forth in the copending applications mentioned above, Ser. No. 628,599 and Ser. No. 889,666. As illustrated in FIG. 1, key **10** comprises a substantially flat and generally rectangular base member or substrate **11** of electrically insulative material such as epoxy glass. Disposed on a surface of substrate **11** is a pattern **12** of electrically conductive strips, which may be fabricated in accordance with conventional electronic printed or etched circuit techniques.

Pattern **12** (FIG. 1) includes a substantially L-shaped conductor **13**, which I may call a common conductor, having a first portion **13*a*** extending transversely on a rearward portion of substrate **11**. Conductor **13** also includes a second portion **13*b*** extending toward front edge **14** so as to form a terminal offering a surface for engaging a contact of key-receiving means. Pattern **12** also includes a plurality of spaced parallel conductive strips **15** extending longitudinally on the forward portion of substrate **11** toward edge **14**. Each of conductive strips **15** is electrically connected to conductor portion **13*a*** via a respective fuse strip **16** formed as an integral part of pattern **12**. Preferably, the width of each of fuse strips **16** is significantly less than the width of the associated conductive strip **15**, the latter typically being at least five times as wide as the associated fuse strip **16**.

A binary code permutation of open and closed electrical paths may be provided in pattern **12** by blowing out one or more of fuse strips **16**. This may be accomplished by providing an electrical current of sufficient magnitude to destroy a fuse section **16**, but not so large as to cause damage to the associated conductive strip **15**. For example, fuse strip **16′** may be blown by providing a current of appropriate magnitude between conductor terminal portion **13*b*** and conductive strip **15′**. The resultant binary permutation code would consist of three adjacent terminals **15** which are connected to common conductor **13**, and one conductive strip **15′** which is electrically disconnected from common conductor **13**. Thus, the key **10** comprises memory means that can be changed to a state offering a particular binary code permutation that may be detected by appropriate circuitry such as that described in the aforementioned U.S. Pat. No. 3,392,558 to R. A. Hedin et al.

While key **10** (FIG. 1) is illustrated as having a coded conductive pattern **12** on one side only of substrate **11**, the invention is not so limited and both top and bottom faces of substrate **11** could be provided with coded conductive patterns. Such conductive patterns may include a separate common conductor on each face of the substrate, or may utilize a single conductor that extends on both faces.

A key having a conductor common to both faces is illustrated in FIGS. 2*a* and 2*b*. Referring thereto, a key **19** includes a generally planar, electrically insulative substrate **20** having a top face **21**, a bottom face **22**, a front edge **23** and a rear edge **24**. A pattern **25** of electrically conductive strips is formed on substrate **20** by conventional electronic printed circuitry techniques. Pattern **25** includes a common conductor **26** which extends along rear edge **24** and overlaps onto both front face **21** and rear face **22**. Conductor **26** includes terminal portions **26*a*** and **26*b*** extending on respective faces **21** and **22** to front edge **23**.

Disposed on top face **21** (FIG. 2*a*) is a first plurality of spaced parallel conductive strips **27** and **27′** each of which initially is connected to common conductor **26** via a fuse strip **28** analogous to fuse strip **16** in the key embodiment of FIG. 1. Similarly, bottom face **22** includes a plurality of conductive strips **29** and **29′**, each of which initially is connected to common conductor **26** by means of a fuse strip **30**.

In a manner similar to that described in conjunction with FIG. 1, selected ones of fuse strips **28** and **30** may be blown to enter in key **19** (FIGS. 2*a* and 2*b*) a particular binary permutation code. By making the associated electronic lock circuitry simultaneously responsive to the coded contacts on both the top and bottom of key **19**, the number of possible combinations of key **19** is considerably greater than available on a key of the same physical size but having contacts on one side only.

Alternatively, the electronic circuitry utilized with key **19** (FIGS. 2*a* and 2*b*) may be made responsive to the code on only one side (i.e., either top or bottom) of key **19**. Then, by using identical patterns on the top and bottom, key **19** would operate the electronic lock regardless of whether top face **21** or bottom face **22** were inserted in a particular direction (e.g., up or down) with respect to a key-receiving means.

Key **19** also may be employed in another mode. Specifically, different codes may be entered on the top and bottom of key **19**, and appropriate circuitry provided so that if key **19** were inserted with a particular face up, the lock would operate normally. If key **19** were inserted with the same face down, the coding could be such as to operate the lock while having a further function such as actuation of an alarm. With such a system, if the key holder were being forced to enter the controlled area, he could insert the key "upside down"; the door would open, but at the same time a silent alarm could be transmitted to a guard or other person.

FIGS. **3***a* and **3***b* show one manner in which I construct the key so that its coding cannot be observed. Thus, a typical key **33** comprises an enclosing member **34** which may be formed of a flexible plastic or like material. Member **34** includes a pouch portion **35** into which is inserted all of key **33** except its forward portion on which are front edge **36** and the contact-engaging terminals **37**. Member **34** may be held assembled by an appropriate grommet **36** extending through the substrate of key **33**. Member **34** further includes a flap **38** which encloses terminals **37** when key **33** is not in use, and which folds back as shown in FIG. **3***a* to expose terminals **37** for insertion into key-receiving means of an electronic lock. Flap **38** may be held closed (FIG. **3***b*) by a snap fastener **39**.

As an alternative to the enclosing technique just described, the rearward portion of a key of the type shown in FIGS. **1**, **2***a* or **2***b* may be coated with an opaque plastic or like material, leaving uncoated the front portion and the contact-engaging surfaces of its key terminals. Conventional identification or credit card information then may be printed and/or imbedded in the plastic coating.

A typical example of a combined credit or identification card and key is illustrated in FIG. **4**. Referring thereto, identification card key **41** includes a key of the type described herein, and including a substrate or base member **42** having a front edge **43** adjacent to which is situated a plurality of terminals **44**. Card key **41** includes a coating **45** on all but the terminal area of substrate **42**. Printed or imbedded in coating **41** is conventional identification card information, possibly including a picture **46** and fingerprint **47** identifying the user. Such indicia is particularly advantageous for credit card applications, wherein a merchant can compare the photograph and other identifying information on the card with the features of the person presenting the card.

Referring now to FIG. **5**, there is shown an embodiment of a key **50** having features like those shown in my earlier copending application Ser. No. 889,666, including a binary code permutation of open or closed AC electrical paths. In particular, the key **50** includes a planar, electrically insulative substrate or base member **51** on the surface of which is provided what I term a common conductor strip **52**. Also provided on substrate **51** are a plurality of spaced terminals **53** and **53'** disposed along a front edge **54** of substrate **51**. Terminals **53** and **53'** are not directly electrically connected to conductor **52**. Further, key **50** is provided with a pair of conductive strip terminals **55***a* and **55***b* extending from conductor **52** toward front edge **54**. Strip terminals **55***a* and **55***b* may be used to complete a DC current path through conductor **52** when inserted into the key-receiving means of an associated electronic lock.

Referring still to FIG. **5**, one or more capacitors **56** are connected between common conductor **52** and selected ones of the terminals adjacent edge **54** of key **50**. In the embodiment shown, capacitors **56** are connected between conductor **52** and terminals **53'**. It should be apparent that while capacitors **56** complete an AC path between conductor **52** and respective terminals **53'**; neither an AC nor a DC path exists between conductor **52** and terminals **53**. Thus, an AC signal applied to either of terminals **55***a* or **55***b* will be communicated via capacitors **56** to terminals **53'**, but will not be communicated to terminals **53**. Nevertheless appropriate electronic lock circuitry will be responsive to the communicated AC signal and will detect the permutation code of key **50**.

Note that the code of key **50** (FIG. **5**) cannot be determined by measuring DC conductivity between either of terminals **55***a* or **55***b* and the remainder of terminals **53** and **53'** due to the fact that the capacitor will not pass the DC current. Further, to prevent determination of the code by visual inspection, key **50** can be encapsulated in plastic, epoxy or the like, to provide a key of the configuration shown generally in FIG. **6***a* and **6***b*. As evident therein, a key **50'** includes encapsulation material **58** covering all of substrate **51'** except for front edge **54'** and the terminals (generally designated **59**) adjacent thereto. As indicated in FIG. **6***b*, encapsulation material **58** completely encloses the capacitors **56'** connecting common conductor **52'** with selected ones of terminals **59**.

Another embodiment of a key for electronic lock or related application is illustrated in FIG. **7**. Shown therein is a key **60** having a planar, electrically insulative substrate **61** forming a base member atop which are disposed a plurality of memory elements **62**. Also disposed on substrate **61** is a common conductor **63** extending in substantially spaced parallel relation with a front edge **64** of key **60**. A conductive strip **63***a* extends between common conductor **63** and front edge **64** to form a terminal for conductor **63**. Further, a plurality of spaced parallel conductive strip members **63***b* extend from conductor **63** to respective ones of memory elements **62**. A like plurality of spaced parallel conductive terminal strips **65** extend between respective memory elements **62** and key front edge **64**. Another conductive strip **66** extends across key **60**, intersecting each of memory element **62**. The ends of conductive strip **66** extend toward front edge **64** to form terminals **66***a* and **66***b*.

The interconnections between memory elements **62**, common conductor **63**, terminal strips **65** and conductive strip **66** are described hereinbelow in conjunction with the typical memory elements shown in FIGS. **9***a*, **9***b*, and **10**. In general, each memory element **62** may comprise a magnetic or ferroelectric storage device of either the destructive or nondestructive readout type. Typically, each memory element **62** will store one binary digit (bit) of data. The data stored in memory elements **62** may be readout by providing a read current along conductive strip **66**. When such read current is provided, an output voltage will appear between common conductor terminal **63***a* and those ones of terminal strips **65** associated with memory elements **62** storing binary 1 bits. Thus, conductive strip **66** and terminal strips **65** are analogous respectively to the word line and digit drive/sense lines of a conventional magnetic core memory.

If memory elements **62** are of the destructive type, provision normally is made in the associated electronic key or related circuitry to rewrite the stored code back into memory element **62** immediately after reading the same; if nondestructive readout devices are used for memory elements **62**, such rewriting is not required. Further, means may be provided for altering data in some but not all of memory elements **62**. This is particularly useful when some of memory elements **62** are used to store an identification code and the remainder to store date (e.g., funds or credit available in an account) which may be updated each time the key is used.

Referring now to FIG. **8**, there is shown a simplified schematic diagram of circuitry for utilizing the key of FIG. **7**. Specifically, there is a key receptacle **70** that may be like the one shown in u.s. pat. No. 3,392,558, including a slot **71** into which the front portion **64** of key **60** is inserted. Within key receptacle **70** are a plurality of contacts **72** which engage and make electrical contact with terminal strips **65** of the inserted key **60**. Additional contacts **72***a*, **72***b*, and **72**c respectively engage terminal **66***a*, **66***b* and **63***a* of key **60**. A cable **73** electrically interconnects the contacts of key receptacle **70** with conventional read/write circuitry **74**. Circuitry **74** may be of the type commonly used to enter data into, or read data from magnetic core memories.

The data read by circuitry **74** from memory elements **62** is provided via a line **75** to key code recognition circuitry **76**. Circuitry **76** produces an output along a line **77** whenever the code read from a set of memory elements **62** corresponds to a code preset in code recognition circuitry **76**. Thus the occurrence of a signal on line **77** indicates that the correct key has been inserted in key receptacle **70**.

The signal on line **77** is provided to a utilization device **78** which, in the case of electronic lock, may comprise an electric door latch. In a credit card type application, the code contained in some but not all of memory element **62** on key **60** may represent the credit card number, and code recognition circuitry **76** may be programmed to determine if the credit card number is a valid one.

In such credit card applications, utilization device **78** may include a computer for determining the amount of credit or funds still available to the credit card holder. Alternatively, others of memory elements **62** may store data indicating the balance of funds or credit available to the credit card holder. In this case, utilization device **78** could add or subtract the amount of the credit card transaction from the previous balance stored on the key. The new balance then may be transmitted via line **79** (FIG. **8**) to read/write circuitry **74** for entry of the new credit balance into key **60**.

FIG. **9***a* shows a first embodiment of a memory element **62**, comprising a conventional annular magnetic core **81**. As is well known, such a magnetic core **81** has a substantially square hysteresis loop, representing two stable magnetic states. Thus if core **81** is set to the magnetic state representing a binary 1, the core will remain in this state until switched to the alternate state by subsequent application of an appropriate magnetic field.

Referring to FIG. **9***a*, core **81** is threaded by a first wire **82** extending between segments of conductive strip **66**. A second wire **83** also is threaded through core **81**, and extends between conductive strip **63***b* and terminal strip **65**.

To enter data into a core **81** which is preset to the binary 0 state, a write current is provided between terminal **66***a* and **66***b* (FIG. **7**); this current flows through wire **82**. Typically, the write current will be selected so that the resultant magnetic field about wire **82** is insufficient to magnetize core **81** to the binary 1 state. If it is desired to set core **81** to the binary 1 state, another current simultaneously is provided between terminal **63***a* and the terminal strip **65** associated with the particular core **81** to be so set. The resultant current through conductor **83**, together with the write current through conductor **82**, produce a net magnetic field which is sufficient to set core **81** to the one state. Alternatively, if a binary 0 is to be set, no current is provided through wire **83**. Since the write current through wire **82** itself is insufficient to flip core **81** from the 0 state to the 1 state, the core remains set at binary 0.

To read data from core **81**, a read current is applied between terminals **66***a* and **66***b*. This read current, which flows through wire **82**, is of appropriate magnitude and direction so that the resultant magnetic field will cause core **81** to flip into the zero state. If core **81** contains a binary 0, its magnetic state will not change when the read current is applied, and no voltage will be induced in wire **83**. Alternatively, if core **81** contains a binary 1, application of the read current through wire **82** will cause core **81** to flip from the binary 1 to the binary 0 state, inducing a signal in wire **83**. This induced signal will appear between terminals **63***a* (FIG. **7**) and the terminal strip **65** associated with the particular core **81**. The presence or absence of such an induced signal at each of terminals **65** of key **60** (FIG. **7**) thus is indicative of the data stored in corresponding memory elements **62**.

Readout of core **81** (FIG. **9***a*) is destructive. That is, upon readout core **81** is set to the 0 state regardless of whether a binary one or binary 0 had been stored therein. Accordingly, external circuitry is necessary to rewrite the data back into core **81** if the same data is to be maintained therein. The value of a destructive readout may be appreciated when it is understood that a key thereby may be limited to one useful operation, so that a person possessing the key may have merely a single access to the electronic apparatus. Also, the apparatus if so aligned may readily apply a different code to the key. In contradistinction, the magnetic core element illustrated in FIGS. **9***b* offer nondestructive readout. That is, data in the core can be sensed without disturbing or destroying data contained therein.

In FIG. **9***b*, a two-apertured magnetic core **85** is employed. Threading the large and small apertures **85***a* and **85***b* of core **85** is a sense/write wire **87**. Wire **87** is connected between segments of conductive strip **63***b* and terminal strip **65** so that a sense/write signal provided or generated between terminal **63***a* and a terminal strip **65** (FIG. **7**) will flow through wire **87**. A read wire **86**, connected between segments of conductive strip **66**, threads through small aperture **85***b* in core **85**. When a read current of appropriate magnitude is provided through wire **86**, a voltage is either induced or not induced in wire **87**, depending on whether core **85** is storing respectively a binary 1 or a binary 0. In either case, the magnetic state of core **85** is not switched by application of the read current; that is, readout is nondestructive and the data bit stored in core **85** subsequently can be reaccessed from the core.

FIG. **10** shows an exemplary thin film memory element **95** which may be employed as a memory element **62** in the key of FIG. **7**. Memory element **95** is formed on a substrate **96** which could either correspond to substrate **61** of key **60** or, alternatively, could be a separate substrate that is subsequently attached to key **60**. Formed on substrate **96** is a first magnetic film **97**, disposed atop which is a conductive word line **98**. Magnetic film **97** is oriented so that the easy axis of magnetization is parallel to word line **98**. Further, word line **98** may be connected in series with segments of conductive strip **66** on key **60** (FIG. **7**).

Still referring to FIG. **10**, memory element **95** includes an insulation layer **99** separating the top of word line **98** from a conductive digit sense/line **100**. Digit/sense line **100** itself is perpendicular to word line **98** and may be connected electrically between a conductive strip **63***b* and a terminal strip **65** of key **60** (FIG. **7**). Another insulation layer **101** separates conductor **100** from a second magnetic film **102**. Again, the easy axis of magnetization of magnetic film **102** is oriented parallel to word line **98**, and perpendicular to digit/sense line **100**. Finally, a protective, electrically insulating substrate **103** is disposed atop magnetic film **102**.

In planar magnetic films, such as those employed in memory element **95** (FIG. **10**) the flux is rotated rather than switched, thereby affording high speed operation. Data may be readout of memory element **95** by applying an appropriate read current along word line **98**. An output signal, indicative of the data stored in memory element **95**, is induced on digit/sense line **100**.

Yet another embodiment of a key for an electronic lock is illustrated in FIG. **11**. As seen therein, a key **105** includes a planar, electrically insulative substrate **106** having a front edge **107**. Disposed atop substrate **106** is a common conductor **108** having a generally L-shaped configuration, including a terminal portion **108***a* extending toward edge **107**. A plurality of spaced parallel terminal strips **109** are disposed atop substrate **106** adjacent front edge **107**. Mounted on substrate **106** is a like plurality of plated wire magnetic memory elements **110**. Each element **110** includes a central conductor wire **111** connected between conductor **108** and a respective one of terminal strips **109**.

Also disposed on substrate **106** of key **105** (FIG. **11**) are a pair of terminal strips **112***a* and **112***b*. Electrically connected in series between terminal strips **112***a* and **112***b* is an insulated wire **113** which functions as a word line for memory elements **110**. Insulated wire **113** is woven about each of memory elements **110**. When a current is applied between terminal strips **112***a* and **112***b*, the magnetic field induced by woven word line **113** causes output signals to be generated by those memory elements **110** which are storing binary ones. These output signals appear at the corresponding ones of terminals **109**. No such outputs are produced by memory elements **110** in which binary zeros are stored. As in the other key configurations described herein, the coding of the key is represented by the permutation of binary digits stored in memory elements **110**.

A further form of key for an electronic lock is shown in FIG. 12. In this embodiment, a key **115** incorporates a diode matrix which is capable of providing a particular binary permutation code output in response to application of a multibit interrogation code.

As indicated diagrammatically in FIG. 12, key **115** comprises a substantially flat, electrically nonconductive base member or substrate **116** having a top surface **116***a*, a bottom surface **116***b* and a front edge **117**. Disposed in spaced parallel relation on substrate top surface **116***a*, perpendicular to edge **117**, is a first plurality of conductive strips **118, 118***a*, **118***b* which serve as column conductors for the diode matrix. Disposed on substrate bottom surface **116***b* is a second plurality of conductive strips **119, 119***a*, **119***b* which form row conductors for the matrix. A set of diodes **120, 120***a*, **120***b* are electrically connected between selected intersections of row conductors **119** and column conductors **118**. For example, diode **120***a* is electrically connected between column conductor **118***a* and row conductor **119***a*. Similarly, diode **120***b* is electrically connected between column conductor **118***b* and row conductor **119***a*.

It will be appreciated that when a voltage is applied to one of row conductors **119**, a corresponding output voltage will appear only on those of column conductors **118** which are diode connected to the energized row conductor. Thus if a voltage were applied only to row conductor **119***a*, an output voltage will appear only on column conductors **118***a* and **118***b;* no output voltage will appear on the others of column lines **118**. Similarly, a different binary output permutation will be produced on column lines **118** if a voltage is supplied to one of the other row conductor, **119**. Thus, diode matrix key **115** could be used to store information of different significance in different matrix rows. For example, the binary permutation code associated with row **119***a* may represent a credit card number, while information along row **119***b* may represent a maximum amount of credit available.

Alternatively, note that a voltage could be applied simultaneously to several of the row conductors **119**, and that the resultant binary permutation output code appearing on column conductors **118** would be a function of (a) the particular ones of row conductors **119** receiving a voltage input, and (b) the specific configuration of diodes **120** in the matrix. Thus, key **115** could be accessed with a multibit interrogation code applied to row conductors **119**, and would produce a particular output code only if the diode matrix were correctly configured. With this type of operation, an extremely large number of information combinations (i.e., binary permutation codes) would be available on key **115**.

The diode matrix of FIG. 12 may be constructed by utilizing discrete diodes mounted through holes in substrate **116** at the appropriate intersections between row conductors **119** and column conductors **118**. Alternatively, the diode array may be in the form of integrated circuit fabricated with diodes at each matrix intersection. To code the matrix, at intersections where no diode is desired, the prefabricated diode may be blown or otherwise open circuited by application of a sufficiently large current. Another possibility is to fabricate the array with diodes only at certain preselected matrix intersections.

FIG. 13 illustrates a key employing an integrated circuit diode or transistor matrix. As indicated therein, a key **122** includes a planar, electrically insulative substrate **123** having a front edge **124**. The diode or transistor matrix array is housed in a "flat-pack" **125** mounted on the surface of substrate **123**. Electrical connections to the row conductors of the matrix are provided by a plurality of conductive strips **126** disposed on the same surface of substrate **123** and extending to front edge **124** thereof. Similarly, electrical connections to the column conductors of the matrix are provided via a plurality of spaced parallel terminal strips **127** disposed on the same surface of substrate **123** and also extending to front edge **124** thereof. When using a transistor matrix, an additional voltage connection is made to the matrix by means of a conductive strip **128** also provided on the same surface of substrate **123**.

FIG. 14 is an electrical schematic diagram of a transistor matrix which may be utilized in key **122** of FIG. 13. In particular, matrix array **130** includes a plurality of bipolar transistors **131** arranged in a matrix of rows and columns. The collectors of all transistors in the array are electrically connected to a common conductor **132** to which is supplied a voltage via conductive strip **128** of key **122** (FIG. 13).

Transistor array **130** (FIG. 14) also includes a first plurality of row conductors **133** and a second plurality of column conductors **134** which may be conducted respectively to conductive strips **126** and terminal strips **127** of key **122** (FIG. 13). The base of each transistor **131** is connected to its respective row conductor **133** by means of a resistor **135**. Further, the emitters of selected ones of transistors **131** are electrically connected to the respective column lines **134** via conductive links **136**. The emitters of the remainder of transistors **131** are not connected to an associated column line **134**, as indicated by missing links **137**. The particular selected array of links **136** and missing links **137** may be provided by appropriate masking during fabrication of transistor matrix **130**.

It will readily be appreciated that when an interrogate voltage is supplied on one of row lines **133**, each of transistors **131** in the corresponding interrogated row will be turned on. Accordingly, a collector voltage supplied on line **132** will appear on those of column lines **134** to which transistors **131** in the interrogated row are connected by means of links **136**. No such voltage will appear on the remainder of the column lines **134**.

As in the case of the diode array described hereinabove, the matrix rows may be interrogated individually or, alternatively, a multibit interrogate code may be applied simultaneously to all of row lines **133** to produce a unique code along column lines **134**. Further, while FIG. **14** is shown to incorporate bipolar transistors, this is not required, and metal oxide semiconductor field effect transistors (MOS FET's) or other transistor types could be employed.

Another key for an electronic lock, the binary permutation code of which may be sensed magnetically, is shown in FIG. 15. Specifically, a key **140** comprises a planar, electrically insulative, nonmagnetic base member or substrate **141**. Disposed at selected locations on the surface of substrate **141** are a plurality of electrically conductive circular strips or eddy current rings **142**.

As is well known, when an annular wire or conductive strip is exposed to a changing magnetic field, an eddy current will be induced in the annulus. The eddy current itself will produce a counter magnetic field which tends to oppose the change in the field inducing the eddy current. Thus, the presence or absence of an eddy current ring **142** at a particular location on substrate **141** may be sensed by applying a changing magnetic field at that location, and determining whether the magnitude of the field is (a) changed, indicating the presence of an annular conductive strip **142**, or (b) unchanged, indicating the absence of an eddy current ring. By simultaneously or sequentially determining the presence or absence of eddy current rings **142** at a plurality of locations on the key **140**, the binary permutation code of key **140** can be sensed.

An optical key for an electronic lock is illustrated in FIG. 16. As shown therein, key **145** includes a substrate **146** having an aperture **147** therein. Disposed across aperture **147** is an optical mask **148** comprising a matrix of opaque spots **149** and transparent spots **150**. The coding of key **145** is determined by the particular locations of opaque spots **149**.

Apparatus for detecting the particular code of key **145** is illustrated in FIG. 17. As seen therein, key **145** is inserted between a light source **152** and an end **153** of a fiber optic bundle **154**. At the other end **156**, the various fibers of bundle **155** are fanned out and directed to individual photodetectors **157**. The outputs of photodetectors **157** are connected to appropriate electronic lock circuitry **158**.

In operation, the transparent spots **150** of optical mask **148** will permit light from source **152** to enter the fibers in corresponding positions in fiber optic bundle **155**. The light entering these fibers will be transmitted to bundle end **156** and impinge on the associated photodetectors **157**. These photodetectors will provide an output signal to lock circuitry **158**. The opaque spots **149** will prevent light from source **152** from entering others of the fibers in fiber optic bundle **155**. Accordingly, those of photodetectors **157** associated with nonilluminated fibers will provide no output signals to lock circuitry **158**. Thus, the permutation of signals and no signals from photodetectors **157** will be indicative of the orientation of opaque spots **149** and transparent spots **150** in optical mask **148**. Lock circuitry **158** may be prewired to be responsive only to a particular optical code included in mask **148** of key **145**.

While the invention has been described with respect to the preferred physical embodiments constructed in accordance therewith, it would be apparent to those skilled in the art that various modifications and improvements may be made without departing from the scope and spirit of the invention.

I claim:

1. A key for effecting operation of an electronic security apparatus by the application of a binary coded activating signal thereto, said key being adapted to contain a binary code permutation of circuits, said key comprising a plurality of electrically conductive members for engaging contacts of a key receiving means through which the permutation code may be applied to the electronic security apparatus, electrically changeable binary state memory means connected between said conductive members so as to be effective when activated to establish a binary coded permutation on the key, said memory means having first and second states for establishing said binary coded permutation of circuits, said memory means when in said first state establishing one binary coded permutation of circuits and when in said second state establishing another binary coded permutation of circuits, said memory means being changeable between said first and second states to establish the one and the other binary coded permutation of circuits, said key-receiving means being operably connected to a source of power for directing power from said contacts to at least one of said conductive members to energize said binary coded permutation of circuits and establish said binary coded permutation of circuits which is indicative of the state of said memory means, said binary coded permutation of circuits being operable when said memory means is in a predetermined one of said states to activate the electronic security apparatus, said binary coded permutation of circuits being ineffective to activate the electronic security apparatus when the memory means is in a state other than said predetermined one of said state.

2. A key as set forth in claim **1** including circuit means associated with said memory means on the key for the application of electric signals changing the state of said memory means.

3. A key as set forth in claim **2**, in which said key comprises an electrically nonconductive forward portion on which said electrically conductive members are mounted in position for engaging contacts of the key-receiving means, and a portion concealing said memory means on a rearward portion of the key.

4. A key as set forth in claim **2** in which said memory means comprise electronic components forming rows and columns of an integrated matrix, said columns of said matrix being connected to corresponding ones of said electrically conductive members, and further conductive members forming parts of said circuit means for placing each row of said matrix in circuit with a contact of the key receiving means.

5. A key as set forth in claim **2**, in which there is a further electrically conductive member for engaging a contact of the key-receiving means, said further member forming a part of said circuit means for the application of signals to said memory means.

6. A key as set forth in claim **5** in which said memory means comprise a magnetic memory element.

7. A key as set forth in claim **6**, in which said magnetic memory element operatively associated with said circuit means and said first-mentioned conductive members.

8. A key as set forth in claim **5** in which said memory means comprise one of said first-mentioned conductive members having a portion of relatively high-electrical resistance connected to said further conductive member whereby to be destroyed when a relatively large electric current is applied through said one conductive member and said further member.

9. A key as set forth in claim **8**, in which said portion of said one conductive member is a diode.

10. A key as defined in claim **2** wherein said memory means comprises a magnetic core having two stable magnetic states and said circuit means for changing the state of said magnetic core includes means for establishing a magnetic field about said magnetic core to set said magnetic core in a desired one of said stable magnetic states and further including second circuit means for reading the state of said magnetic core including means for establishing a magnetic field which causes said magnetic core to be in a predetermined one of said states, said magnetic core remaining in said one state if said magnetic core is in said one state prior to the application of said magnetic field by said second circuit means and said magnetic core changing to said one state if said magnetic core is in the other state prior to the application of said magnetic field by said second circuit means.

11. A key as defined in claim **10** wherein the application of said magnetic field by said second circuit means effects a destructive readout of the state of said magnetic core and sets said core to said one state regardless of the state said core was previously in.

12. A key as defined in claim **11** further including means for resetting said magnetic core to the state said magnetic core was in prior to the application of said magnetic field by said second circuit means.

13. A key adapted to contain binary code permutations of circuits to be connected to contacts of key receiving means for applying a predetermined code permutation to an electronic security apparatus to effect operation thereof comprises, an electrically nonconductive base member for the key, a plurality of electrically conductive members mounted in spaced relation to one another on said base member and having each a surface in position for engaging a contact of said key-receiving means, a plurality of electrically changeable memory elements having open circuit and closed circuit states and connected each between at least two of said electrically conductive members on the base member of the key, and circuit means associated with each memory element on the key for the application of electrical signals changing the state of that element between said open and closed circuit states so as to establish a binary code permutation of circuits on the key, said circuit means being operable to effect the establishment of said predetermined and other code permutation on said key, said key when having said other code permutation of circuits being ineffective to actuate said electronic security apparatus, said key when having said predetermined code permutation of circuits being effective to actuate said electronic security apparatus.

14. A key as set forth in claim **13** in which said base member of the key is substantially flat, each of said electrically conductive members forming a strip extending longitudinally in position on a forward portion of the base member for engaging a contact of the key-receiving means, and a conductive strip extending transversely on a rearward portion of said base member and comprising a connection between each memory element and at least two of the longitudinal strips.

15. A key as set forth in claim **13**, in which each memory element comprises a circuit connected at one end to one of said electrically conductive members and at its opposed end in common with a corresponding circuit end of each other memory element.

16. A key as set forth in claim **15**, in which said electrically nonconductive base member is epoxyglass and said memory elements comprise a relatively narrow fusible portion of one of said conductive members.

17. A key as set forth in claim 15, in which the key has a further electrically conductive member for placing the commonly connected circuit ends of said memory elements in circuit with a contact of the key-receiving means.

18. A key as set forth in claim 13 in which said memory means comprise each a magnetic memory element, said memory element being operatively associated with said circuit means for changing the state of the element, and said circuit means comprising a conductor that is adapted to engage a contact of the key receiving means.

19. A key adapted to contain a binary code permutation of circuits to be connected with contacts of key-receiving means for applying the code permutation to an electronic security apparatus, said electronic security apparatus being actuatable in response to a predetermined code permutation being applied thereto and being nonactuatable upon the application of a code permutation other than said predetermined code permutation thereto, a substantially flat, electrically nonconductive base member, a plurality of electrically conductive strips mounted in spaced relation to one another on said base member, each of said strips extending longitudinally on a forward portion of said member and presenting a surface for engaging a contact of said key-receiving means, a conductive common strip extending transversely on a rearward portion of said base member, changeable means placing each longitudinally extending strip individually in closed circuit or alternately in open circuit relation to said common transverse strip, and means for changing said changeable means on said key so that the key may be selectively equipped with said predetermined binary code permutations of closed and open circuits for actuating said electronic security apparatus or with said other binary code permutations os as to pervent the actuation of said electronic security apparatus in response to engagement of said plurality of electrically conductive strips with said contacts of said key-receiving means.

20. A key as set forth in claim 19 in which there are longitudinal strips and a common transverse strip on each opposed face of the base member so that the key may offer differing code permutations when applied in inverted positions to the key-receiving means.

21. A key as set forth in claim 19 in which the key comprises a member enclosing said changeable means on said rearward portion of said base member, and said enclosing member having flap portion that is movable relatively to a position covering said electrically conductive strips on the forward portion of the base member.

22. A key as set forth in claim 19 in which said changeable means comprise a plurality of memory elements electrically changeable between open circuit and closed circuit states, said key further including a conductive segmental strip extending transversely on a rearward portion of said base member, each of said memory elements having a circuit connected between a corresponding longitudinally extending strip and said common transverse strip and further having a circuit connected between segments of said segmental strip, and strip portions for placing said common and segmental strips in circuit with contacts of the key-receiving means, enabling signals supplied through the key- means to change the state of said memory elements whereby to establish said predetermined binary code permutation that the key can reapply to the key-receiving means to effect actuation of said electronic security apparatus.

23. A key for conveying a predetermined code to effect operation of a controlled device, said key having a plurality of electrically conductive members for engaging respective contacts of key-receiving means for conveying said predetermined code thereto to effect operation of the controlled device, a conductor in closed circuit relation to a portion of said conductive members and in open circuit relation to a further portion of said members whereby to offer a binary code permutation of circuits to said key receiving means, and a capacitor connected between said conductor and one of said conductive members, said capacitor providing a closed circuit path between said conductor and said one conductive member whereby AC current is applied therebetween to effect the application of said predetermined code to said key receiving means and providing an open circuit path to offer a code indication other than said predetermined code when DC current is applied through the conductive members.

24. A key for controlling an electronic security apparatus that is responsive to a predetermined binary code permutation, said key comprising an electrically nonconductive base member, a plurality of electrically conductive elements mounted in relative positions forming a binary code pattern on said base member which is indicative of said predetermined binary code permutation for controlling the security apparatus, each of said elements being shaped to form a closed electrical circuit, permitting the binary code pattern to be detected through the use of eddy currents that may be induced in each element upon the application of a changing magnetic field to said elements, said eddy currents producing a counter magnetic field which acts to oppose the changing magnetic field applied to said elements and enables the binary code pattern to be detected by sensing the magnitude of the applied magnetic field.

25. In a key for applying a predetermined binary coded permutation of electrical signals to an electric security system to effect actuation of the system and having a plurality of contacts through which the signals are transmitted to the system, circuit means connected to certain contacts of said plurality of contacts on the key for establishing a relationship between said certain contacts that is effective to transmit the predetermined binary coded permutation of electric signals to effect actuation of the system, electrically changeable state control means forming a part of said circuit means for controlling the coded relationship established between said certain contacts by the circuit means, said control means having a first state for enabling the key to apply said predetermined binary coded permutation of electric signals to effect actuation of the electric security system and a second state which prevents said key from applying said predetermined binary coded permutation of electric signals, said control means when in said second state rendering said key inoperative to actuate said electric security system and circuit portions through which a potential will act when externally applied to a certain combination of said contacts to change the state of said control means to said first state to enable said plurality of contacts to apply said predetermined coded permutation of signals to said electric security system to effect actuation thereof.

* * * * *