(12) UK Patent Application (19) GB (11) 2 452 732 (13) A

(43) Date of A Publication 18.03.2009

(21) Application No: 0717783.5

(22) Date of Filing: 12.09.2007

(71) Applicant(s):
Seiko Epson Corporation
(Incorporated in Japan)
4-1 Nishi-Shinjuku 2-chome, Shinjuku-ku,
Tokyo 163-0811, Japan

Cambridge Enterprise Limited
(Incorporated in the United Kingdom)
The Old Schools, Trinity Lane,
CAMBRIDGE, CB2 1TN, United Kingdom

(72) Inventor(s):
Philip Christopher Paul
Simon Tam
Simon Moore

(74) Agent and/or Address for Service:
Miller Sturt Kenyon
9 John Street, LONDON, WC1N 2ES,
United Kingdom

(51) INT CL:
G06F 21/06 (2006.01) ***G06F 21/04*** (2006.01)
G06K 19/073 (2006.01)

(56) Documents Cited:
EP 0495645 A1 **DE 010326089 B3**
DE 102005016294 A1

(58) Field of Search:
INT CL **G06F, G06K**
Other: **WPI, EPODOC & the Internet**

(54) Abstract Title: **Smart-card chip with organic conductive surface layer for detecting invasive attack**

(57) A smart-card chip arrangement includes a smart-card chip, an organic conductive layer disposed on a surface of the chip, and signal-deriving means for deriving a signal dependent on one or more properties of the organic conductive layer. The organic conductive layer and the signal-deriving means are configured such as to detect an invasive attack on the chip. By this means the unauthorized detection of a cryptographic key, which is employed by the chip, can be prevented.

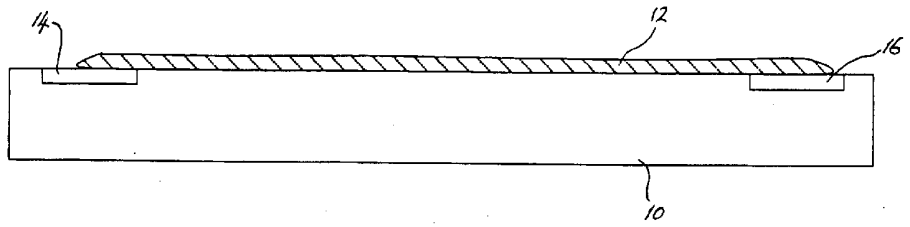

Fig. 1

GB 2 452 732 A

SMART-CARD CHIP ARRANGEMENT

The present invention relates to a smart card chip arrangement and a method for protecting a smart-card chip arrangement from unauthorized tampering.

Smart cards are used for a multitude of applications and, in order to protect the user or provide identification for the relevant application, they generally perform some form of encryption or decryption. To this end, a secret key is stored on the chip to render the cryptographic function unique. Attacks from unauthorised parties aim to retrieve this secret key and hence allow the attacker to duplicate or otherwise misuse the smart card. There are two classes of attack: non-invasive and invasive. The present invention is directed toward finding a solution to the latter.

Invasive attacks on smart cards are performed by partially or completely removing the packaging of the microchip of the smart card. The depackaging step may be achieved using acids, solvents, laser cutters, or chemical mechanical polishing. A comprehensive description of the various techniques employed is given in the paper "Design Principles for Tamper-Resistant Smartcard Processors" by Oliver Kömmerling and Markus Kuhn, Proc. of the USENIX Workshop on Smartcard Technology, Chicago, 10-11 May, 1999, pp. 9-20. Once the microchip has been depackaged, attacks are conducted by probing metal tracks. A focus ion beam (FIB) technique could be employed to drill fine holes in the insulating layer in order to expose fine metal tracks without disturbing other components.

A standard countermeasure against invasive attacks is to cover the chip surface with a metal protection grid. More specifically, the topmost metal layer of the microchip is patterned to cover the chip with a meandering grid. This grid prevents access to the circuitry below and also shields the chip circuitry from electromagnetic emissions, which may leak sensitive information (see, e.g., the Dallas DS5002FPM secure microprocessor). Damage to the protection grid is detected, which triggers an

alarm and thus causes the chip to refuse further operation.

A second method for protecting the encryption keys is to randomly distribute small particles directly into the packaging of the microchip. The cryptographic key is then derived from measuring the distribution of these particles. To achieve this, the chip includes sensors that are sensitive to at least one physical property of the particles (e.g. magnetism). If the packaging is damaged or removed, the encryption key is lost. This structure is the subject of U.S. Patent Application No. US 7,005,733 by Kömmerling et al.

A drawback with the use of metal protection grids is that the depackaging procedure leaves the protection grid intact. Generally speaking, it is necessary to actively break the metal protection grid in order to trigger the alarm. However, since the feature size of the metal grid is much bigger than what the FIB can achieve, it is highly likely that the grid will be unable to provide sufficient protection (as demonstrated by Kömmerling and Kuhn in the above-mentioned paper). A small hole can be excavated between grid lines to expose signal wires for probing by the attacker, without triggering the alarm.

As regards the particle-distribution technique, this solution is elegant in principle, but requires a multitude of sensors to be positioned on the chip surface. This is expected to consume significant area on the chip and complicate routing, not least because metal wires running above a sensor will shield it from the relevant property of the packaging, thereby defeating the purpose.

In accordance with a first aspect of the present invention there is provided a smart-card chip arrangement, comprising: a smart-card chip; an organic conductive layer disposed on a surface of the chip; and signal-deriving means for deriving a signal dependent on one or more properties of the organic conductive layer; wherein said organic conductive layer and said signal-deriving means are configured such as to detect

an invasive attack on said chip.

The organic conductive layer may be an organic semiconductor layer, which may be composed of a material from a group consisting of F8T2, P3HT and pentacene. Alternatively, or additionally in another region of the chip, the organic conductive layer may be an organic conductive polymer. Such an organic conductive polymer may be composed of a material from a group consisting of PEDOT and PSS.

The organic conductive layer may be a layer covering at least those areas of the chip containing circuitry, which, if invaded, could lead to the detection of a cryptographic key employed by the chip. It may be constituted as a strip of organic conductive material arranged in a meandering pattern on said chip surface. The meandering pattern may be a spiral or a wave-like shape.

The organic conductive layer may be provided as two or more layers separated by an insulative layer. Viewed looking down onto said organic conductive material, the meandering pattern of one of said layers may at least partially overlap the spaces inside the meandering pattern of another of said layers.

The meandering pattern may comprise first and second castellated strips of the organic conductive material, the first and second castellated strips each comprising first strip sections, which are formed in one of the two layers and are extensive in a direction substantially orthogonal to the general direction of the meandering pattern, and second strip sections, which are formed in the other of the two layers, are extensive in substantially the general direction of the meandering pattern and link neighbouring ends of the first strip sections.

The meandering pattern may be in discrete sections, said discrete sections being associated with respective said signal-deriving means. Alternatively, the meandering pattern may be in one continuous length.

Advantageously, a surface of said organic conductive layer facing away from said chip may vary in height above said chip surface over at least part of the extent of the organic conductive layer. There may be an insulative layer disposed between said chip surface and said organic conductive layer, wherein said insulative layer varies in thickness over at least part of the extent of the organic conductive layer.

The signal-deriving means may be configured such as to apply a first electrical quantity to one part of said organic conductive layer and to detect a second electrical quantity at another part of said organic conductive layer, said second electrical quantity, or differences between said first and second electrical quantities, being due to the application of said first electrical quantity and being determined by properties of said organic conductive layer, and to compare said second electrical quantity or said differences with a reference electrical quantity or reference differences, respectively.

The first electrical quantity may be a voltage or a current, and said control means may be configured such as to detect a time delay with which said voltage or current appears at said another part of said organic conductive layer, said time delay being compared with a reference time delay characterizing said smart-card chip arrangement in an uninvaded state thereof.

The first and second electrical quantities may be first and second waveforms, respectively, and said control means may be configured to compare said second waveform, or differences between said first and second waveforms, with a reference second waveform or reference differences, respectively, characterizing said smart-card chip arrangement in an uninvaded state thereof.

The signal-deriving means may be configured to determine a transfer function of said organic conductive layer and to compare said transfer function with a reference transfer function characterizing said smart-card chip arrangement in an uninvaded state

thereof.

The signal-deriving means may be configured to apply a voltage or a current to one part of said organic conductive layer, and to detect a time delay with which said voltage or current appears at another part of said organic conductive layer, said control means comprising combining means for combining said detected time delay with reference data, thereby to provide a cryptographic key employed by the chip, and comparing means for comparing said cryptographic key with a cryptographic key obtained in an uninvaded state of said smart-card chip arrangement.

There may be two of said organic conductive layers and said signal-deriving means may comprise: a signal-input means for inputting an input signal to one part of each of said organic conductive layers; a signal-output means for outputting an output signal from another part of each of said organic conductive layers; a first comparison means for forming a first comparison between said output signals, and a second comparison means for forming a second comparison between the results of the first comparison and a reference signal held in a memory.

The first comparison means may be a difference-determining means for forming a difference between said output signals, or a dividing means for forming a ratio of said output signals.

The organic conductive layers may be in different layers with an insulative layer therebetween, said organic conductive layers at least partially overlapping each other. Alternatively, or additionally, the organic conductive layers may be side-by-side in the same layer.

In a second aspect of the present invention, a smart card is provided comprising a smart-card chip arrangement as described above.

The invention further provides, in a third aspect thereof, a method for protecting a smart-card chip arrangement from unauthorized tampering, said smart-card chip arrangement comprising: a smart-card chip protected by a cryptographic key, and an organic conductive layer disposed on a surface of the chip; said method comprising the steps of: performing a self-characterization process, in which an initial signal dependent on one or more of the initial properties of said organic conductive layer before tampering is derived; performing one or more subsequent tests on said smart-card chip arrangement in order to derive subsequent signals dependent on said one or more of the properties of said organic conductive layer; comparing said subsequent signals with said initial signal, and, if said subsequent signals differ substantially from said initial signal, providing to said chip a signal indicative of said tampering.

A fourth aspect of the present invention features a method for protecting a smart-card chip arrangement from unauthorized tampering, said smart-card chip arrangement comprising: a smart-card chip protected by a cryptographic key, and an organic conductive layer disposed on a surface of the chip; said method comprising the steps of: establishing an initial value of said key before tampering, said value being dependent on determined properties of said organic conductive layer; performing one or more subsequent tests on said smart-card chip arrangement in order to reassess the value of said key; comparing said reassessed key-value with said initial key-value, and, if said reassessed key-value differs from said initial key-value, providing to said chip a signal indicative of said tampering.

Either of these methods may include the further step of using said tampering-indicative signal to prevent the reading of said cryptographic key.

The initial value of the key may be established from a combination of a parameter, which is dependent on said determined properties, and a predetermined pre-key component. The parameter may be a response time of said organic conductive layer to an input signal applied to said organic conductive layer.

Embodiments of the invention will now be described in detail purely by way of example, with the aid of the attached drawings, of which:

Fig. 1 is a side view of a first embodiment of a smart-card chip arrangement in accordance with the invention;

Fig. 2 is a block diagram of a control arrangement associated with the first embodiment;

Fig. 3 is a block diagram of a control arrangement associated with a second embodiment of the invention;

Fig. 4 is a block diagram of a control arrangement associated with a third embodiment of the invention;

Fig. 5 is a flowchart showing the mode of operation of the first two embodiments;

Fig. 6 is a flowchart showing the mode of operation of the third embodiment;

Fig. 7 is a side view of a smart-card chip arrangement in accordance with the invention in a variant thereof;

Fig. 8 is a side view of a smart-card chip arrangement in accordance with the invention in a further variant thereof;

Figs. 9(a) and 9(b) provide top and side views, respectively, of a smart-card chip arrangement in accordance with a still further variant thereof;

Fig. 10 is a block diagram of a control arrangement associated with a fourth embodiment of a smart-card chip arrangement in accordance with the invention;

Figs. 11(a) and 11(b) are top views of a fifth embodiment of a smart-card chip arrangement in accordance with the invention; and

Figs. 12(a), 12(b) and 12(c) are top views of a sixth embodiment of a smart-card chip arrangement in accordance with the invention;

The smart-card arrangement proposed by the present inventors is based on the use of an organic conductive protection layer, which may be composed of a conductor or

a semiconductor material and is preferably disposed in a grid pattern, as are the known metallic protection layers. Organic materials are damaged by all of the depackaging techniques that are currently employed and can therefore provide excellent protection against tampering. Furthermore, a preferred embodiment of the invention deposits the organic protection layer as a back-end process – that is, the structure is made after the chip has been fabricated. This means that a standard smart-card chip can be obtained and the organic protection layer deposited on a surface of this standard chip. Since therefore minimal changes have to be made to the chip itself, costs are reduced.

Furthermore, by using inkjet or similar deposition or patterning techniques, it is possible to dynamically vary the structure of the protection layer (grid) without significantly increasing fabrication costs, since it is not necessary to use lithography masks. Individual chips of the same fabrication run can be structured differently, which has the advantage of making reverse-engineering and spoofing (the mimicking of protection-grid behaviour by an attacker) much more difficult. This flexibility is not available when using metal protection grids.

A wealth of organic materials are known, which are suitable for use as the protection layer. The most commonly used materials for this function are PEDOT (poly(3,4-ethylenedioxythiophene)), which is a conductive polymer material usually doped with PSS (poly(stryenesulfonate)), and F8T2 (poly(9,9-dioctylfluorenyl-2,7-dyl)-co-bithiophene)) or P3HT (poly(3-Hexylthiophene)), both of which are semiconducting materials. All three of these materials are readily deposited by inkjet techniques and are therefore particularly suitable for use in the present invention. A further material, pentacene, is a semiconducting molecular material, which is usually deposited by thermal evaporation under vacuum conditions. It is also possible to deposit liquid precursors and subsequently anneal the precursors to form pure pentacene. This material may also be used for the semiconducting structures of the protection layer. In addition, PVP (poly(4-vinylphenol)) is an insulating polymer that can be used as a topography-forming layer or as an interfacial insulator or a passivation layer. The use of

such layers is discussed later.

The above list of materials is by no means exhaustive, there being others that may equally well be used in the present application.

It is preferred that the organic protection layer be combined with an outer layer (e.g. a resin) to form a packaging layer enclosing the overall device (e.g. a smart card), such that, when the packaging layer is damaged during a tampering process or an invasive attack, the organic material is destroyed or degrades to such an extent that the process or attack is detected electronically.

In general, to provide good protection, the protection layer must be sure to be damaged in an attack and its integrity must be easily verifiable. Ideally also, any signalling that takes place must be difficult to mimic by an attacker. The protection layers provided by the various embodiments of the present invention attempt to meet these criteria.

A first embodiment of a smart-card chip arrangement in accordance with the invention is illustrated in Figs. 1 and 2. In Fig. 1 a smart-card chip 10, which may be a standard chip supplied by a suitable supplier, has applied to its upper surface a single organic conductive layer 12. The organic conductive layer 12, which, as already stated, may have conducting or semiconducting properties, is applied as a strip of material in a grid configuration over the upper surface of the chip 10. This strip is connected at its two ends to respective bond pads 14, 16, which in turn are connected to suitable control circuitry located on the chip. The control circuitry provides operating signals for at least indirectly assessing the properties of the organic layer.

In this embodiment the layer is used as an RC (resistor-capacitor) delay line and the control circuitry feeds a pulse into one end of the delay line and measures the time it takes for the pulse to reach the other end. An alarm is triggered if the response time

changes. Such a change in response time could result from a tampering attempt, which alters the electrical properties of the layer, and thereby the delay time. A block diagram of this control arrangement is shown in Fig. 2. In Fig. 2 a waveform generator 20 supplies a voltage or current pulse to the bond pad 14 shown in Fig. 1 and the voltage/current on the other bond pad 16 is monitored by a detector circuit 22. The protection layer 12 is shown in Fig. 2 as a simple RC network. A timer 24 is also provided, which is started by the appearance of the pulse from the waveform generator 20 and is stopped by the appearance of the delayed pulse as detected by the detector 22. The delay time measured by the timer is then compared in a comparator 26 with a predetermined reference delay value stored in a non-volatile memory 28, which is directly integrated in the chip circuitry in the form of an embedded non-volatile memory or ROM. The memory is preferably of the write-once variety for reasons to be explained later. An example of a write-once memory is described in U.S. Patent No. 6,804,136 by L. Forbes. If the two delay times are substantially identical, then the comparator outputs a "PASS" signal, otherwise a "FAIL" signal is output. These two signals are represented by a logic HIGH/LOW signal (in either order) at the output of the comparator.

A second embodiment of the invention is depicted in Fig. 3. This embodiment likewise makes use of the single organic-layer arrangement shown in Fig. 1, but in this case applies not a single pulse to the protection layer at pad 14, but a waveform from a random waveform generator 30, which may be, e.g., a pseudo-random waveform generator. A detector 32 detects the waveform on the pad 16 of the protection layer and takes snapshots of this waveform at discrete moments in time. These snapshots are then compared with a reference profile stored in a memory 34, which as before is preferably a write-once non-volatile memory mounted directly on the chip. Again, if the two values substantially agree, a "PASS" signal is output from the detector 32, whereas if they differ, a "FAIL" signal is output. As with the first embodiment, any attempt to invade the smart-card chip will result in damage done to the protection layer, which in turn changes the electrical properties of this layer. This affects the values of the

snapshots taken by the detector 32. An advantage of this arrangement is that the times at which the snapshots are taken may be made to vary. This is acceptable, provided the same variation is employed each time the protection layer is "read". Since an attacker is unlikely to know the pattern of this variation, a degree of protection against spoofing is provided. Furthermore, the variation in the snapshot times may be different for different smart-card chips, which provides even greater protection.

The detector 32 in Fig. 3 is preferably configured to form a measurement of the impedance or transimpedance of the RC network between the pads 14 and 16. Thus, either the random waveform generator 30 delivers a current and the resulting voltage on pad 16 is read, or vice-versa. In either case the detector forms the quotient of these two quantities.

A third embodiment of the present invention is shown in Fig. 4. In this embodiment the protection layer is once again considered as a delay line, just as in the first embodiment. However, in this instance the comparator 26 shown in Fig. 2 is replaced by a "transform logic" circuit 40 and the memory 28 contains not reference delay-time values, but a number of pre-key bits. These pre-key bits may be predetermined values or may be purely random. Transform logic circuit 40 combines these pre-key bits with the delay time output by the timer 24 and delivers at its output a number of key bits, which together function as the cryptographic key for the smart card. This key will change if the protection layer is damaged, e.g. as a result of tampering or an attack, since the layer's electrical properties will change, which will change the delay time registered by the timer 24, and consequently also the key bits output by the transform logic circuit 40.

To derive the encryption key from the delay time and pre-key bits, the analogue delay time detected by the timer 24 must be digitised. This may be achieved either by counting the number of clock cycles the signal takes to reach a certain threshold at the receiving end of the delay line, or by using a digital-to-analogue converter (DAC). The

voltage at the input of the DAC is converted to a digital signal after a fixed time, which is chosen such that it coincides with charging of the receiving node (i.e. when the pulse reaches the far end, and the voltage has not yet reached its steady state). The number of bits constituting the delay time will vary, depending on the achievable accuracy. To increase accuracy, it may be necessary to compensate for environmental conditions such as ambient temperature. Depending on the materials employed, the conductivity of the protection layer will vary - usually the conductivity increases with temperature. The capacitance, however, will remain fixed, resulting in shorter delay times. Compensation can be simply achieved by providing a temperature sensor on the chip (e.g. a diode - temperature sensors are readily available for CMOS technology) and a lookup table containing the compensation coefficients. For best spread of output key values, a hash function may be used to derive the actual encryption key from both inputs. As is well known, a hash function is a complex function that combines data in such a way that a change in a single value changes the result significantly. It is also a one-way function - i.e. the original values cannot be derived from the result.

The reliability level afforded by this third embodiment is higher than that afforded by either of the first and second embodiments. This is because, whereas the first and second embodiments provide a single-bit test decision only (i.e. an indication of "PASS" or "FAIL"), in the third embodiment the test result forms the cryptographic key. An incorrect cryptographic key results in failure of the smart card device without the need for pass/fail signals and associated circuitry (that could likewise be tampered with).

The mode of operation of the first two embodiments is illustrated in the flowchart of Fig. 5. It is assumed first of all that the delay time (first embodiment) or waveform snapshot values (second embodiment) have been determined in an initial test carried out before the smart-card chip is issued and put to use, and that this time or these values have been saved to the write-once non-volatile memory. This initial procedure might be termed a self-characterizing phase. After this self-characterizing phase, a

dedicated memory cell is used to flag successful initialization of the memory and allow the chip to function normally. During subsequent use of a smart card containing such a chip, the card is inserted into a reader and is powered on (step S100), allowing the control circuitry illustrated in Fig. 2 or Fig. 3 to operate. Before a transaction is carried out (such a transaction may be, for example, the withdrawal of funds where the card is a bank card of some kind), and assuming the flag mentioned earlier has been set, a subsequent test is carried out on the protection layer (step S102) using either the delay-line principle or the waveform-snapshot principle described in connection with Figs. 2 and 3, respectively. A decision is then made as to whether or not the protection layer is intact (see step S104). If it is (i.e. an output signal "PASS" is delivered), then the requested transaction is performed (step S106), e.g. the funds are withdrawn. On completion of the transaction the smart-card chip arrangement goes into a standby mode (step S108) in readiness for a possible further transaction. Should no further transaction be desired, the card will be removed from the reader, resulting in removal of power from the card. Should a "FAIL" signal be output by the comparator 26 or detector 32 in Figs 2 and 3, respectively, then the transaction is disallowed (step S110). This will trigger a suitable alarm, advising the user (which in this case may be the attacker rather than the authorised card user) of such disallowal and preferably also alerting the user to the possibility that tampering has occurred and that the card's security has been compromised. Preferably also, the control circuitry of the smart-card chip arrangement will erase the memory containing the cryptographic key of the chip, so that there is no possibility that the key could be hacked in any subsequent attack on the same card.

It is possible that an attacker could successfully unset the afore-mentioned flag, in which case the self-characterization routine will be restarted. In that event, the tampered-with protection layer will be read and its resulting characteristics taken to be the original initial ones, leading to the possibility that the attacker could use the card to withdraw funds, etc. It is under these circumstances that the use of a write-once memory is beneficial, since the new self-characterizing values cannot be written to the memory. Thus the characteristic values of the damaged protection layer will not match

the characteristic values stored in memory, leading to a "FAiL" indication, as mentioned earlier.

Fig. 6 shows the corresponding sequence of events for the third embodiment shown in Fig. 4. Before a card containing the smartcard chip is issued, the protection layer is "read" by determining its response to an input pulse. This is the pre-characterizing phase. As already explained, this response is in the form of a delay time, which is used in conjunction with a set of pre-key bits in non-volatile memory 28 to derive the cryptographic key for the chip at the output of the transform logic circuit 40. Subsequently, when the smartcard is used, it is inserted into a card reader, which powers on the card (step S120). The protection layer is then re-read in a characterisation step (S122), which derives the key once again (step S124) based on the updated properties of the protection layer. If those properties remain the same, the key will remain the same, indicating that the layer has not been damaged and so tampering has not occurred. Consequently, the transaction (e.g. the withdrawal of funds) can proceed (step S126). Once the transaction has been completed, the control circuitry of the smart-card chip arrangement remains idle in readiness for another transaction. In the event the layer is not intact, the key will not match the originally derived key and therefore the user, which again may well be the attacker or tamperer, will be unable to go through with the requested transaction. In this manner the bank account, for example, of the card holder is protected from fraudulent withdrawal.

In all these embodiments, the organic protection layer also provides some degree of shielding for the various signals arising from the operation of the smart-card chip. This is important if the risk of attack is to be reduced. The effectiveness of this shielding will dependent to some extent on how large the gaps are in the grid structure of the layer. The protection layer will carry its own signals, of course, which can escape to the outside. It is envisaged that additional protective measures, such as the provision of one or more dedicated shielding layers, may be provided in order to mitigate this drawback.

A refinement of the embodiments just described will now be explained with the aid of Fig. 7. Fig. 7 shows essentially the same smart-card chip arrangement shown in Fig. 1, but this time the semiconductor layer 12 is not applied directly to the surface of the chip 10, but is applied to an insulation layer 50, which has first been applied to the chip surface. The insulation layer 50 is deliberately made uneven in its topography, as can be clearly seen in Fig. 7. In other words, it assumes different depths at different points on the chip surface. Consequently, should an attacker decide to employ a chemical mechanical polishing (CMP) technique in order to gain access to the chip circuitry, this will remove the higher parts of the semiconductor layer, thereby damaging this layer and altering its characteristics. These changes in characteristics are picked up using one of the methods already described in connection with the first, second and third embodiments, thereby protecting the chip key from unauthorised discovery. This refinement has the advantage that the CMP-based tampering can be detected before the shielding properties of the layer are degraded significantly.

A further refinement involves the addition of a further layer, which enhances the damage done to the protection layer. An example of this is shown in Fig. 8, which includes in addition to the topographical insulation layer 50 shown in Fig. 7 a passivation layer 52 disposed directly on top of the organic protection layer 12. A further layer 54 is provided, which encapsulates the chip arrangement and is of a material conventionally employed for this purpose, e.g. a plastics or resin material. The material of layer 52 is chosen so that its removal requires techniques which efficiently damage the organic layer – for example, the acid-based removal technique. Alternatively, layer 52 may be so tightly bound to the protection layer, that the latter is automatically damaged, destroyed or removed when the former is attacked.

A particularly advantageous variant of the embodiments so far described involves the use of multiple organic protection layers on the same chip. Figs. 9(a) and 9(b) show top and side views, respectively, of such an arrangement, in which an upper

organic protection layer 60 is disposed above a lower organic protection layer 62, the two layers being separated by an intervening insulating layer 64. Both protection layers are in the form of an organic conductor strip, which follows a wave-like configuration over at least an area of the chip containing sensitive circuitry, attacks on which could result in discovery of the cryptographic key. Although the size of the gap between the grid lines can be made very small (sub-hundred nanometer dimensions, typically), it is desirable to reduce the gap still further in order to be sure of detecting an attack. In the Fig. 9 arrangement this is achieved by arranging for the lower strip to fill in the gaps left by the upper strip, and vice-versa. Consequently, an attack at any part of the protection-layer arrangement will show itself as a change in the characteristics of at least one of the two layers, leading to a "FAIL" result in the tests carried out in, for example, Figs. 5 and 6. Indeed, the two layers can be made to co-operate by monitoring the appearance of a signal between the two layers, such a signal indicating that a short-circuit has taken place, possibly through tampering. Thus a detector could be provided with inputs connected to points A and B, for example. A signal on both inputs would indicate tampering and result in a "FAIL" indication in the control circuitry, as described earlier.

For the sake of completeness, Fig. 9(a) shows not only the protection-layer arrangement, but also more peripheral parts of the chip package containing the various bond-pads required for the operation of the chip. It should be noted that the various component parts of this drawing are shown in representative fashion only and are not limited to the actual relative dimensions shown.

The use of at least two separate protection layers allows the use of a fourth embodiment of the invention, which is illustrated in Fig. 10. In this embodiment a first organic protection layer, which is modelled as an RC network 70 in Fig. 10, is formed as a lower layer (e.g. the layer 62 in Fig. 9), while a second organic protection layer, which is modelled as an RC network 72 in Fig. 10, is formed as an upper layer (the layer 60 in Fig. 9). Both layers are tested for their time-delay in response to a pulse input from a generator 74, these time delays being detected by respective timers 76, 78, which

receive input signals from respective signal detectors 80, 82. In addition a memory 84 has stored therein the value of a reference time delay. So far the testing circuit for each layer in Fig. 10 resembles that shown in Fig. 2 for testing the single layer shown in Fig. 1. An additional component in Fig. 10, however, is a processor circuit 86, which takes as its inputs the outputs of the timers 76 and 78 and the output of the memory 84.

The processor circuit 86 compares the characteristics of the two layers, so that any significant relative change in characteristics is taken to indicate the occurrence of an attack. The initial testing phase of this embodiment will assess the "correct" (i.e. "untampered") time-delay difference between the two layers and place that in the memory 84 as the reference value. In subsequent tests, in the event that no tampering or attack has taken place, the difference in time delays will remain unaltered, providing a "PASS" decision at the output of the processor circuit 86. On the other hand, where one of the layers has been tampered with, the delays will be appreciably different, providing a "FAIL" decision at the processor-circuit output. It may be possible, by strict control of the deposition conditions of the two organic layers, for the electrical characteristics – and hence the time delay – of the two layers to be almost identical. In that case, the reference value in the memory 84 will be ideally zero or, more realistically, a narrow spread of values in view of the small finite difference in the characteristics of the two layers. Any difference value outside the reference value will result in a "FAIL" signal at the output of the processor circuit 86, otherwise a "PASS" indication is given. Instead of a zero time delay, other reference values may be stored in the memory 84. Two possibilities are a fixed ratio of delays or a fixed absolute time-delay difference.

This embodiment assumes that an attack will affect the outer layer (see RC network 72) in preference to the inner layer (see RC network 70), so that a difference between their characteristics does arise. If an attack took place while the smart-card was powered up, it would be easy to detect a relative change in the characteristics of the two layers, provided sampling of the inner layer took place sufficiently quickly after the sampling of the outer layer – i.e. during the time in which the attack was taking place.

However, an attack is far more likely to occur with the card not powered up. In that case, the present invention envisages the detection of not only relative changes between the layers, but also of absolute changes – for example, by using as an additional reference value an absolute value of delay.. Thus, although, if both layers were roughly equally affected by an attack, a sufficiently great relative change might not be detected, it is very likely that the delay times of both layers will have increased beyond the absolute maximum reference-time value. This would be detected and the necessary protection provided.

An advantage of the fourth embodiment is that the differential configuration cancels out the effect of parasitic environmental influences, e.g. temperature variations or fluctuations in the chip supply voltage.

As an alternative to configuring the differential arrangement of Fig. 10 as a dual-layer arrangement, as in Figs. 9(a) and 9(b), it is possible to configure it as a side-by-side arrangement of the two organic protection structures. In that case, care must be taken to ensure that any attack results in a change in one of the layers in preference to the other layer. One way of doing this is to employ the topographical insulation layer arrangement of Fig. 7 in different ways for the two protection layers. This may be easily achieved by, e.g., the inkjet printing of a PVP insulator to form different topographical features. Thus, if an attacker uses mechanical means of depackaging, one structure will be damaged before the second structure. Alternatively, if one of the two protection structures is pre-treated with a material likely to be used for depackaging (e.g. PEDOT/PSS treated with HCl), then a depackaging attempt will only significantly affect the untreated protection structure. The use of hydrochloric acid, such as to result in a significant change in conductivity, is discussed in "Chemical and thermal treatment of PEDOT:PSS thin films for use in organic light emitting diodes, Surface and Coatings Technology", T.P. Nguyen, Volumes 180-181, Proceedings of Symposium G on Protective Coatings and Thin Films-03, of the E-MRS 2003 Spring Conference, 1 March 2004, Pages 646-649.

One possible way of configuring two or more different protection layers side-by-side on the same chip is shown in Fig. 11(a). In Fig. 11(a), which constitutes a fifth embodiment, a series of protection-layer bond-pads 90, 92, 94, 96, 98 and 100 are provided and these are connected to the ends of separate sections 102, 104, 106 and 108 of an organic protection layer. Section 102 lies between pads 90 and 92, section 104 between pads 94 and 96, section 106 between pads 90 and 96 and section 108 between pads 98 and 100. Any two of these sections could be used in the differential arrangement of Fig. 10. Indeed, all of them could be so used, though this would render the determination of the value to be placed in the memory 84 in Fig. 10 more complex.

If all sections are used, one method is to compare different pairs of sections with each other. Thus, the characteristics of sections 102 and 104 could be compared with each other against a reference value, as could also the characteristics of sections 106 and 108. Then either the two results of these comparisons could be used separately as a kind of backup indication of card integrity, or they themselves could be compared with each other to yield a single comparison result, which is used to determine card integrity. When all of the sections are compared with each other directly to yield a single comparison result, one possibility is to form an average characteristic value for the four different sections, and to then compare this value with a single reference value.

In Fig. 11(b) exactly the same pad layout is employed, but this time there is a different arrangement of the protection-layer sections between those pads. In the Fig. 11(b) arrangement the various sections are not separated, but are intermixed. This is another advantage of the invention, in that any number of different protection-layer patterns can be provided for different chips, while retaining the same basic pad layout, thereby making it more difficult for an attacker to predict the characteristics of the protection layers. Indeed, it is even possible to have different layouts for chips of the same batch. This would be difficult to achieve in the conventional metal-grid designs.

In the Fig. 11 arrangements, it is possible to employ as the initial pre-characterising phase either the delay-time testing procedure of the first embodiment (Fig. 2) or the I/V testing procedure of the second embodiment (Fig. 3). As already explained above in connection with Fig. 11(a), these procedures will yield a series of values for the different permutations of the signal paths associated with the various sections of the protection layer. Either all of these values can be stored in memory as reference values, or they could be combined by the use of some algorithm so as to yield a single reference value, which is stored. For example, a hash value could be used, which was based on a combination of the individual delay times, or the hash value of the relative proportions of delay times could be employed together with the total delay time. The benefits of using a hash value have already been explained earlier in connection with Fig. 4.

A further kind of pattern, which may be employed, is shown in Fig. 12(a). This is a sixth embodiment of the invention, in which the pattern is a spiral instead of a wave pattern, as shown in Fig. 9 and Figs. 11(a) and 11(b). The track forming this pattern can either be in single-layer form or multi-layer form. With the single-layer form, a contact pad 120 is connected to an outer end of the spiral, while a second contact pad 122 is connected to its inner end.

A two-layer version of this arrangement is illustrated in Figs. 12(b) and 12(c). Fig. 12(b) shows the constitution of an outer end-section 124 of the spiral, in which this end-section is composed of two interleaved patterns in two layers with vias joining the two layers. It is expedient to employ printed vias, as detailed in the paper "Inkjet Printing of Via Holes" by T. Kawase, H. Sirringhaus, R.H. Friend and T. Shimoda, in "Inkjet Printed Via-Hole Interconnections and Resistors for All-Polymer Transistor Circuits", Advanced Materials, 2001, 13, pages 1601-1605. The lower ends A, B of the pattern correspond to the lines A and B of Fig. 12(a). The upper ends C, D of the pattern are taken to a continuation of this same pattern, which continues all the way round the spiral. Thus the spiral consists of the same interleaved pattern throughout. At an inner

end-section 126 of the spiral the interleaved pattern comes to an end, as shown in Fig. 12(c). The ends C' and D' of Fig. 12(c) are connected to ends C and D through this continuation of the pattern all the way round the spiral. Ends E and F of the Fig. 12(c) pattern correspond to lines E and F of Fig. 12(a). Finally, Line A is connected to pad 120, line F is connected to pad 122 and line B is connected to line E.

With the arrangement just described, any short-circuit between the layers will halve the effective electrical length of the spiral pattern and be detectable using only two connection pads, as shown.

Both the single-layer spiral pattern and the two-layer spiral pattern have the drawback that they contain spaces between the track sections, which an attacker could exploit in order to gain access to the cryptographic key of the chip. With the single-layer case, a solution analogous to that shown in Fig. 9 could be implemented, in which the spiral structure is disposed in a second layer such as to fill in the gaps in the spiral structure of the first layer. As regards the two-layer structure illustrated in Figs. 12(b) and 12(c), the gaps in this structure could be filled by providing two further layers and a similar pattern structure in those two layers, but in which the pattern in the second two layers was displaced relative to that in the first two layers. A suitable displacement would be for point G in the pattern in the second two layers to be placed opposite the point G' in the first two layers (see Fig. 12(b)). Thus the pattern in the second two layers is displaced by one track thickness in the two directions x and y.

Although it has been assumed that the organic protection layer will be applied to the chip surface as a grid pattern by an inkjet technique, it may be applied by other means - for example, screen printing, micro-contact printing or, in the case of Pentacene, vacuum deposition. The screen printing technique is described in, e.g. "Screen-printed passive matrix displays based on light-emitting polymers", J. Birnstock et al, Applied Physics Letters, volume 78 number 24, 2001, pages 3905-3907, while micro-contact printing is described in J. Tate, et. al., "Anodization and Microcontact

Printing on Electroless Silver: Solution-Based Fabrication Procedures for Low-Voltage Electronic Systems with Organic Active Components", Langmuir, volume 16, number 14, 2000, pages 6054 - 6060. Furthermore, it may take the form of a continuous layer over the relevant parts of the chip surface, rather than a grid. In this case, an attack which damages part of this continuous layer will still affect the properties of the layer, so that the key may be protected. However, in comparison with a grid the sensitivity of such a layer may be less than ideal. In practice, therefore, some form of grid pattern is to be preferred.

While the electrical characteristics of the protection layer have, as so far described, been determined based on an RC time constant or the I-V transfer function, an alternative is to derive the layer's characteristics on the basis of the metal-organic interface properties. The electrical contact properties are determined by the microstructure (deposition conditions) of the organic material. For a combination of materials, a Schottky barrier is formed between the metal and organic material. This results in diode-like contact properties, with the height of the Schottky barrier varying with the materials being combined. The electrical properties (contact resistance, contact noise) of contacts between dissimilar materials are usually very sensitive to fabrication conditions and contamination, hence they are a promising candidate for both tamper sensing and providing individual characteristics for each chip. It was shown, for example by Lim et al. (Jung Ah Lim et. al., "Solvent effect of inkjet printed source/drain electrodes on electrical properties of polymer thin-film transistors," Applied Physics Letters, volume 88 No. 8, 2006), that an addition of DMSO (Di-methyl-sulf-oxide) to a PEDOT/PSS solution reduces the contact resistance/Schottky barrier.

The smart-card chip arrangement described in this specification has a number of advantages with respect to the conventional arrangements employing metal protection grids. Firstly, use of an organic protection layer allows a large number of suitable grid structures to be employed, even within the same production batch, which can help to protect against spoofing. Secondly, because this layer is disposed on top of the outer

layer of the chip, it is more exposed to tampering and hence, if it is tampered with, this can lead to shut-down of the card's services before the cryptographic key has been accessed. Thirdly, compared with a method such as Kömmerling's, as described in the afore-cited patent, no sensor structure is required on the chip. This simplifies fabrication and minimizes added complexity.

Possible applications for the smart-card chip arrangement according to the present invention are, as already mentioned, smart cards for authorizing bank transactions, but also copy-protection devices, game cartridges, inkjet or laser printer cartridges, RFID tags, pay-TV decoder cards, phone cards, etc. All of these applications, and others not specifically mentioned here, are intended to come under the term "smart-card chip arrangement" used in this specification.

CLAIMS

1. A smart-card chip arrangement, comprising:

a smart-card chip;

an organic conductive layer disposed on a surface of the chip; and

signal-deriving means for deriving a signal dependent on one or more properties of the organic conductive layer;

wherein said organic conductive layer and said signal-deriving means are configured such as to detect an invasive attack on said chip.

2. A smart-card chip arrangement as claimed in claim 1, wherein said organic conductive layer is an organic semiconductor layer.

3. A smart-card chip arrangement as claimed in claim 2, wherein said organic semiconductor layer is composed of a material from a group consisting of F8T2, P3HT and pentacene.

4. A smart-card chip arrangement as claimed in claim 1, wherein said organic conductive layer is an organic conductive polymer.

5. A smart-card chip arrangement as claimed in claim 4, wherein said organic conductive polymer is composed of a material from a group consisting of PEDOT and PSS.

6. A smart-card chip arrangement as claimed in any one of the preceding claims, wherein said organic conductive layer is a layer covering at least those areas of the chip containing circuitry, which, if invaded, could lead to the detection of a cryptographic key employed by the chip.

7. A smart-card chip arrangement as claimed in claim 6, wherein said organic

conductive layer is constituted as a strip of organic conductive material arranged in a meandering pattern on said chip surface.

8. A smart-card chip arrangement as claimed in claim 7, wherein said meandering pattern is a spiral.

9. A smart-card chip arrangement as claimed in claim 7, wherein said meandering pattern is a wave-like shape.

10. A smart-card chip arrangement as claimed in claim 7, wherein said organic conductive layer is provided as two or more layers separated by an insulative layer.

11. A smart-card chip arrangement as claimed in claim 8, wherein there are two organic conductive layers and, viewed looking down onto said organic conductive material, the meandering pattern of one of said layers at least partially overlaps the spaces inside the meandering pattern of the other of said layers.

12. A smart-card chip arrangement as claimed in claim 11, wherein the meandering pattern comprises first and second castellated strips of the organic conductive material, the first and second castellated strips each comprising first strip sections, which are formed in one of the two layers and are extensive in a direction substantially orthogonal to the general direction of the meandering pattern, and second strip sections, which are formed in the other of the two layers, are extensive in substantially the general direction of the meandering pattern and link neighbouring ends of the first strip sections.

13. A smart-card chip arrangement as claimed in any one of claims 7 to 12, wherein said meandering pattern is in discrete sections, said discrete sections being associated with respective said signal-deriving means.

14. A smart-card chip arrangement as claimed in any one of claims 7 to 12, wherein said meandering pattern is in one continuous length.

15. A smart-card chip arrangement as claimed in any one of the preceding claims, wherein a surface of said organic conductive layer facing away from said chip varies in height above said chip surface over at least part of the extent of the organic conductive layer.

16. A smart-card chip arrangement as claimed in claim 15, further comprising an insulative layer disposed between said chip surface and said organic conductive layer, wherein said insulative layer varies in thickness over at least part of the extent of the organic conductive layer.

17. A smart-card chip arrangement as claimed in any one of the preceding claims, wherein said signal-deriving means is configured such as to apply a first electrical quantity to one part of said organic conductive layer and to detect a second electrical quantity at another part of said organic conductive layer, said second electrical quantity, or differences between said first and second electrical quantities, being due to the application of said first electrical quantity and being determined by properties of said organic conductive layer, and to compare said second electrical quantity or said differences with a reference electrical quantity or reference differences, respectively.

18. A smart-card chip arrangement as claimed in claim 17, wherein said first electrical quantity is a voltage or a current, and said control means is configured such as to detect a time delay with which said voltage or current appears at said another part of said organic conductive layer, said time delay being compared with a reference time delay characterizing said smart-card chip arrangement in an uninvaded state thereof.

19. A smart-card chip arrangement as claimed in claim 17, wherein said first and second electrical quantities are first and second waveforms, respectively, and said control means is configured to compare said second waveform, or differences between said first and second waveforms, with a reference second waveform or reference differences, respectively, characterizing said smart-card chip arrangement in an uninvaded state thereof.

20. A smart-card chip arrangement as claimed in claim 17, wherein said signal-deriving means is configured to determine a transfer function of said organic conductive layer and to compare said transfer function with a reference transfer function characterizing said smart-card chip arrangement in an uninvaded state thereof.

21. A smart-card chip arrangement as claimed in any one of claims 1 to 16, wherein said signal-deriving means is configured to apply a voltage or a current to one part of said organic conductive layer, and to detect a time delay with which said voltage or current appears at another part of said organic conductive layer, said control means comprising combining means for combining said detected time delay with reference data, thereby to provide a cryptographic key employed by the chip, and comparing means for comparing said cryptographic key with a cryptographic key obtained in an uninvaded state of said smart-card chip arrangement.

22. A smart-card chip arrangement as claimed in any one of claims 1 to 16, wherein there are two of said organic conductive layers and said signal-deriving means comprises:

a signal-input means for inputting an input signal to one part of each of said organic conductive layers;

a signal-output means for outputting an output signal from another part of each of said organic conductive layers;

a first comparison means for forming a first comparison between said output signals, and

a second comparison means for forming a second comparison between the results of the first comparison and a reference signal held in a memory.

23. A smart-card chip arrangement as claimed in claim 22, wherein said first comparison means is a difference-determining means for forming a difference between said output signals.

24. A smart-card chip arrangement as claimed in claim 22, wherein said first comparison means is a dividing means for forming a ratio of said output signals.

25. A smart-card chip arrangement as claimed in any one of claims 22 to 24, wherein said organic conductive layers are in different layers with an insulating layer therebetween, said organic conductive layers at least partially overlapping each other.

26. A smart-card chip arrangement as claimed in any one of claims 22 to 24, wherein said organic conductive layers are side-by-side in the same layer.

27. A smart card comprising a smart-card chip arrangement as claimed in any one of the preceding claims.

28. Method for protecting a smart-card chip arrangement from unauthorized tampering, said smart-card chip arrangement comprising:

a smart-card chip protected by a cryptographic key, and

an organic conductive layer disposed on a surface of the chip;

said method comprising the steps of:

performing a self-characterization process, in which an initial signal dependent on one or more of the initial properties of said organic conductive layer before tampering is derived;

performing one or more subsequent tests on said smart-card chip arrangement in order to derive subsequent signals dependent on said one or more of the properties of said organic conductive layer;

comparing said subsequent signals with said initial signal, and, if said subsequent signals differ substantially from said initial signal,

providing to said chip a signal indicative of said tampering.

29. Method for protecting a smart-card chip arrangement from unauthorized tampering, said smart-card chip arrangement comprising:

a smart-card chip protected by a cryptographic key, and

an organic conductive layer disposed on a surface of the chip;

said method comprising the steps of:

establishing an initial value of said key before tampering, said value being dependent on determined properties of said organic conductive layer;

performing one or more subsequent tests on said smart-card chip arrangement in order to reassess the value of said key;

comparing said reassessed key-value with said initial key-value, and, if said reassessed key-value differs from said initial key-value,

providing to said chip a signal indicative of said tampering.

30. Method as claimed in claim 28 or claim 29, comprising the further step of:

using said tampering-indicative signal to prevent the reading of said cryptographic key.

31. Method as claimed in claim 29, wherein said initial value of said key is established from a combination of a parameter, which is dependent on said determined properties, and a predetermined pre-key component.

32. Method as claimed in claim 31, wherein said parameter is a response time of said organic conductive layer to an input signal applied to said organic conductive layer.

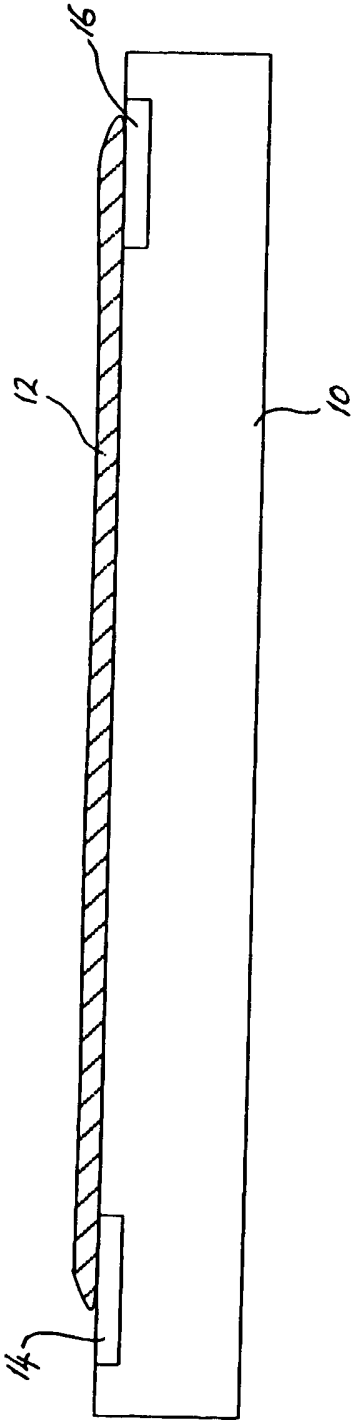

Fig. 1

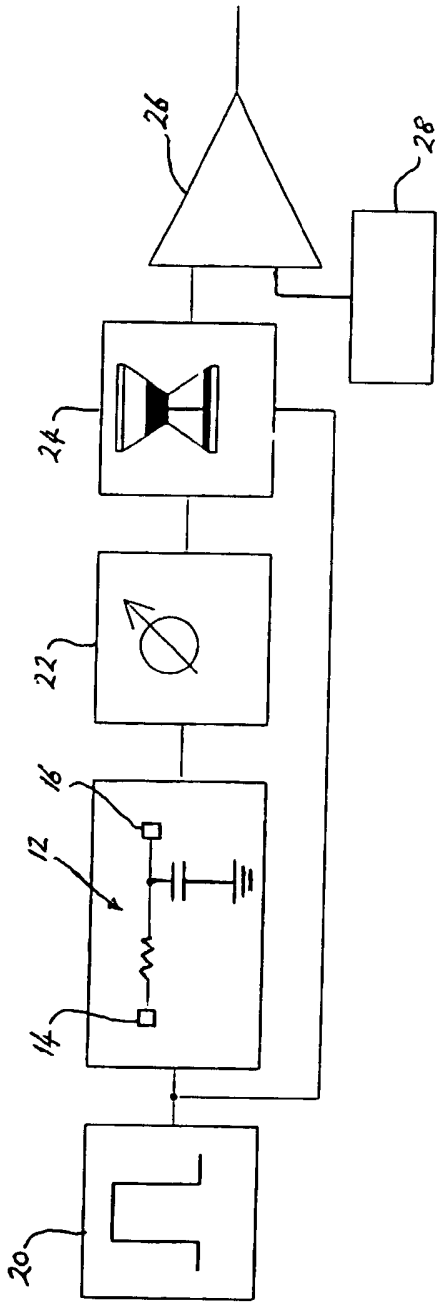

Fig. 2

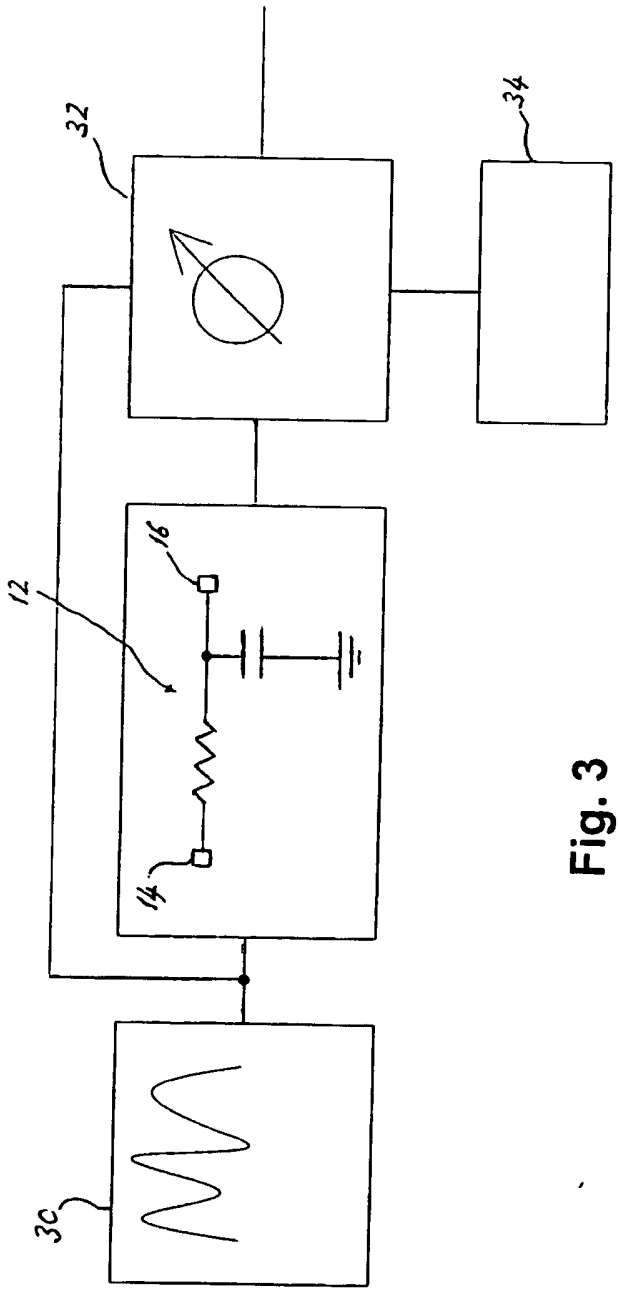

Fig. 3

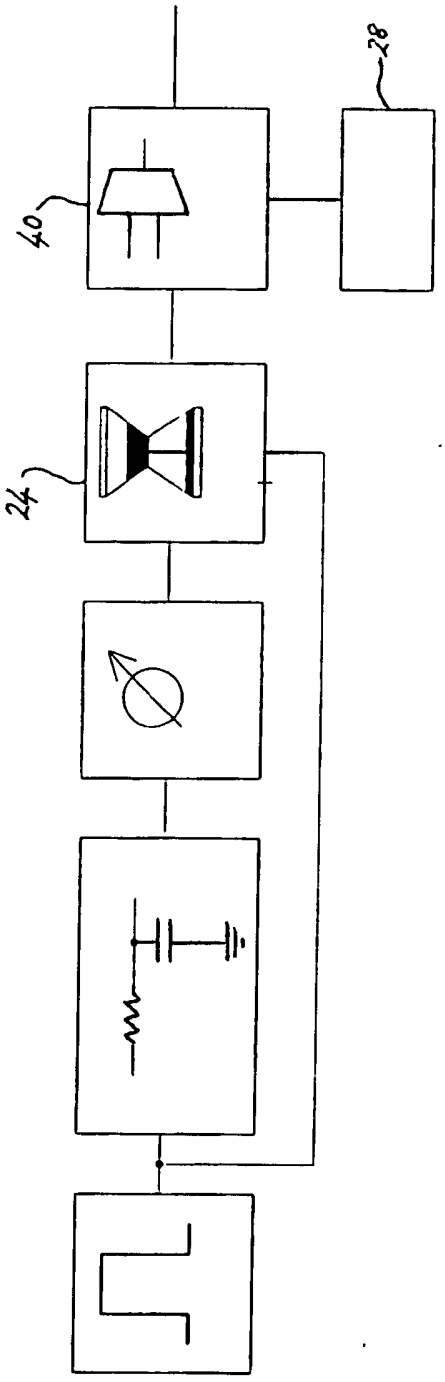

Fig. 4

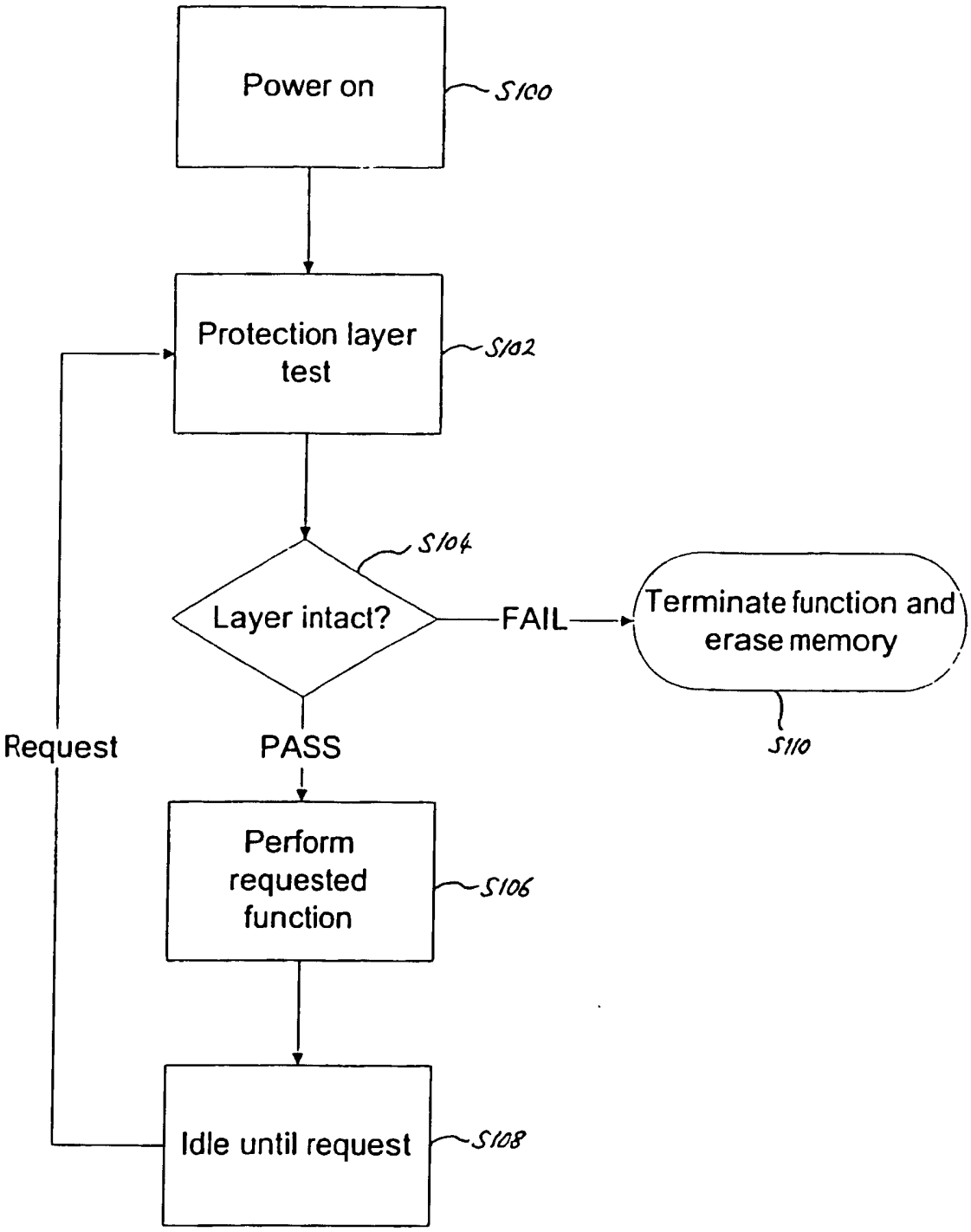
Power on
S100
Protection layer test
S102
S104
Layer intact?
FAIL
Terminate function and erase memory
S110
Request
PASS
Perform requested function
S106
Idle until request
S108

Fig. 5

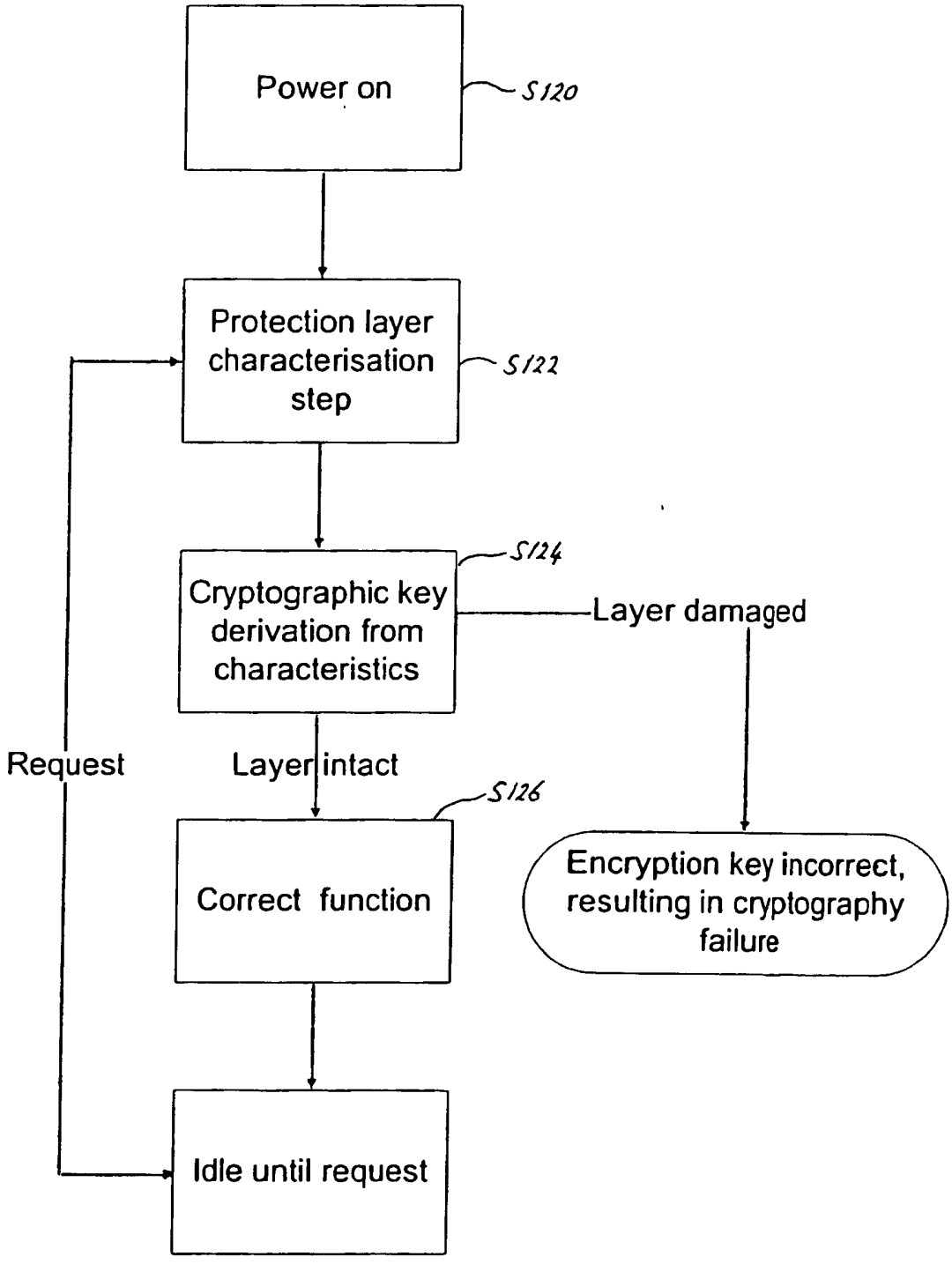
Power on
S120
Protection layer characterisation step
S122
Cryptographic key derivation from characteristics
S124
Layer damaged
Request
Layer intact
S126
Correct function
Encryption key incorrect, resulting in cryptography failure
Idle until request

Fig. 6

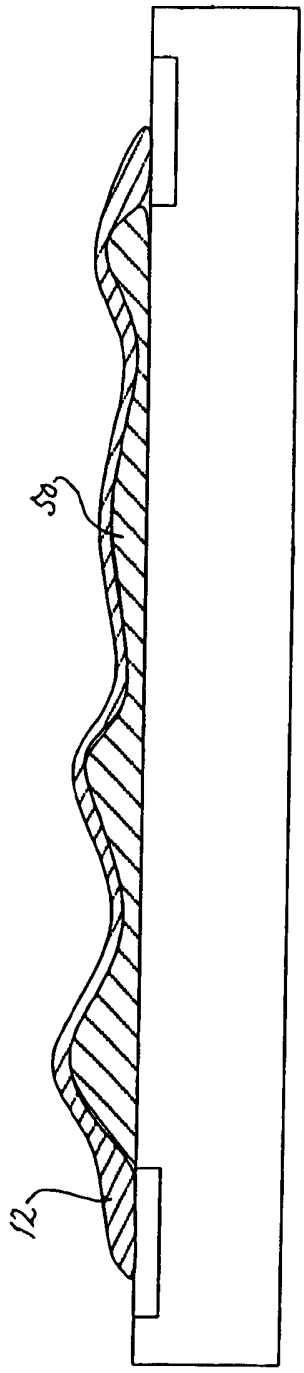

Fig. 7

Fig. 8

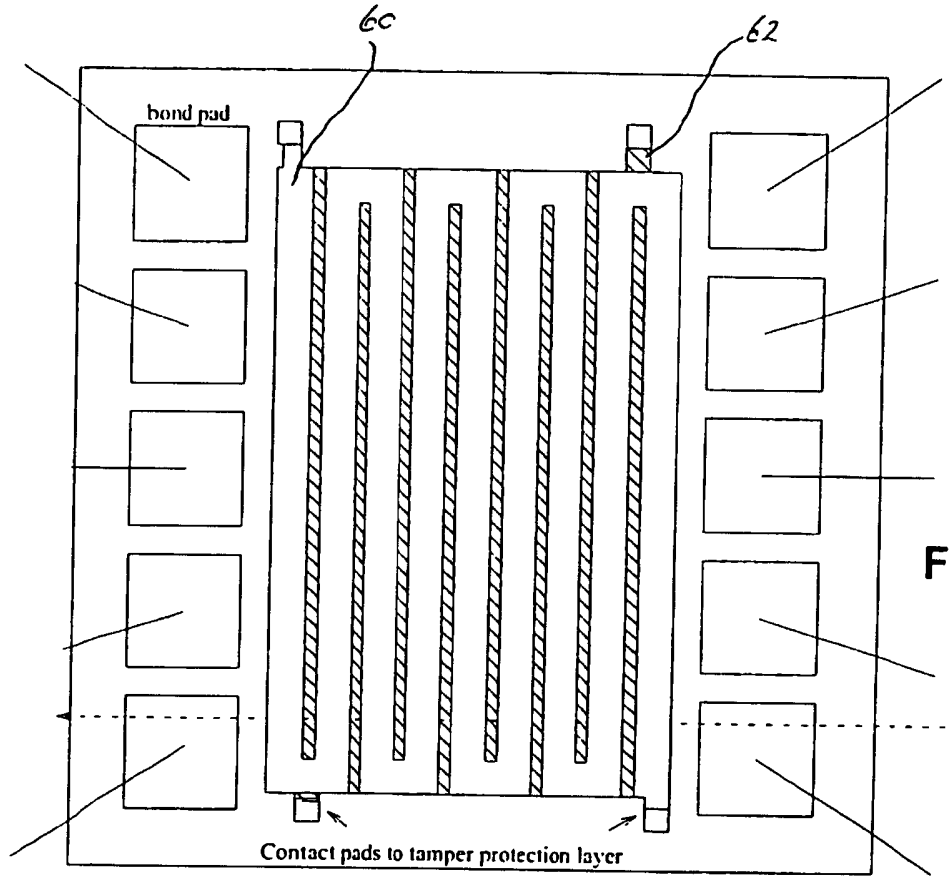
60
62
bond pad
Contact pads to tamper protection layer

Fig. 9(a)

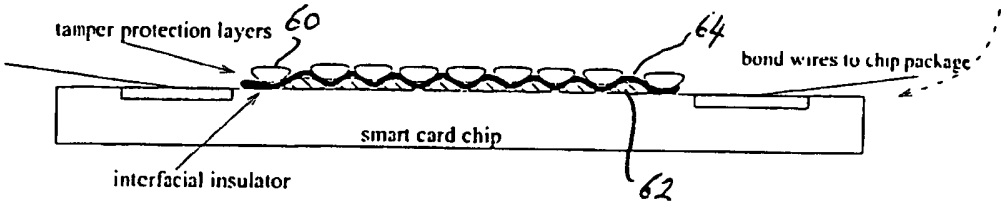
tamper protection layers
60
64
bond wires to chip package
smart card chip
interfacial insulator
62

Fig. 9(b)

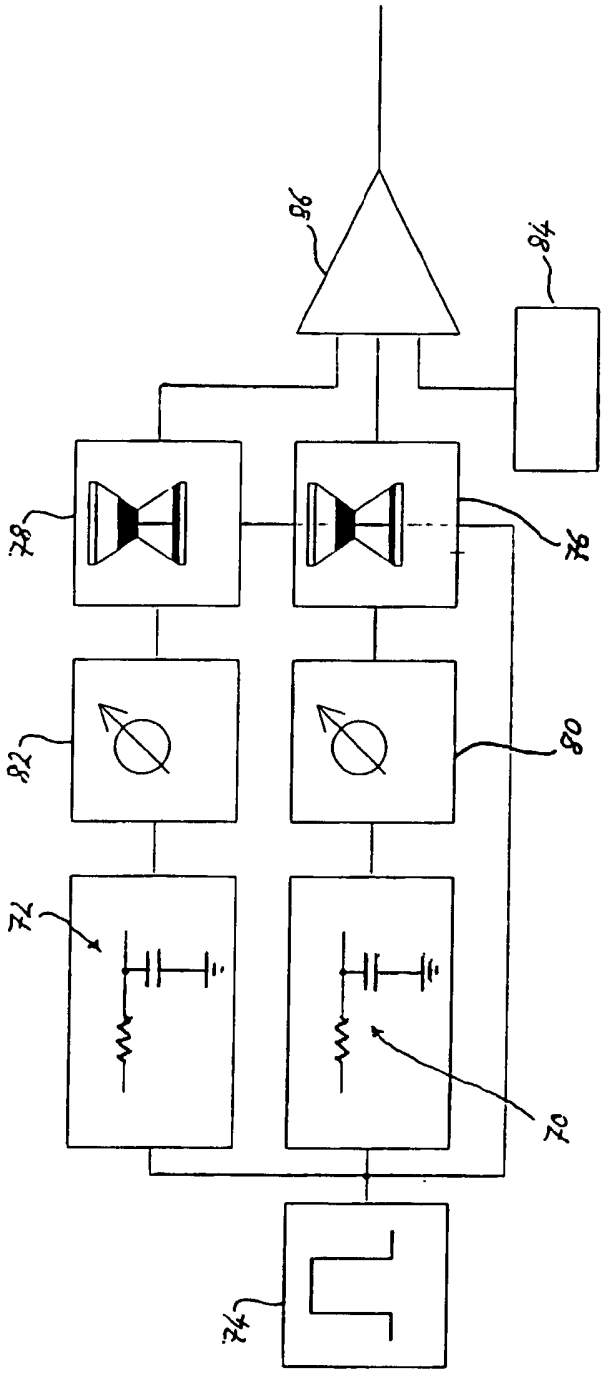

Fig. 10

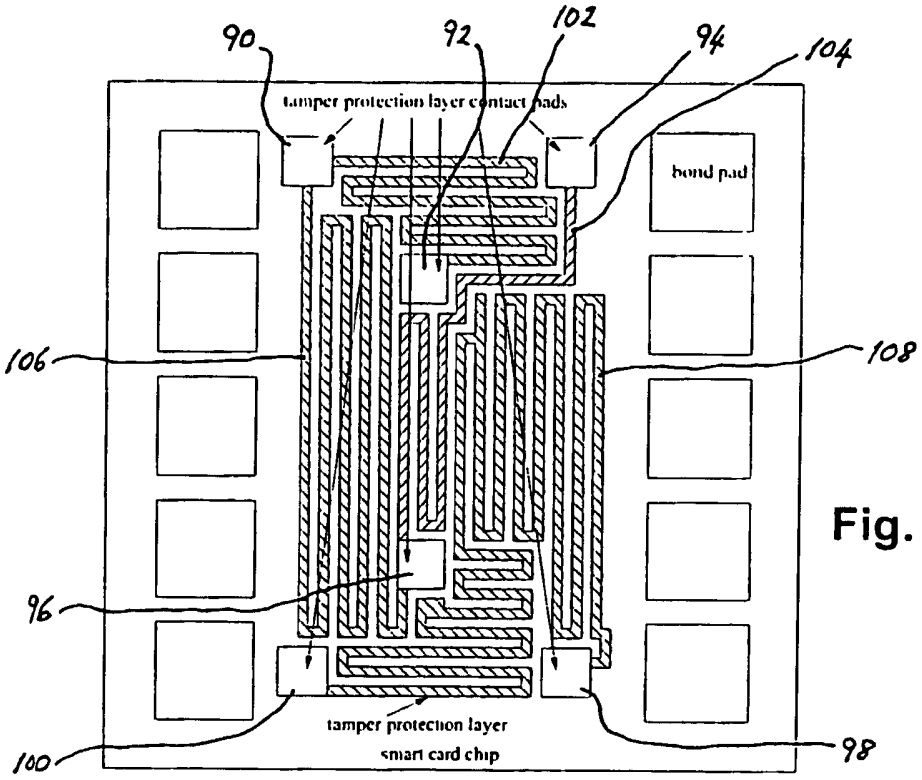

Fig. 11(a)

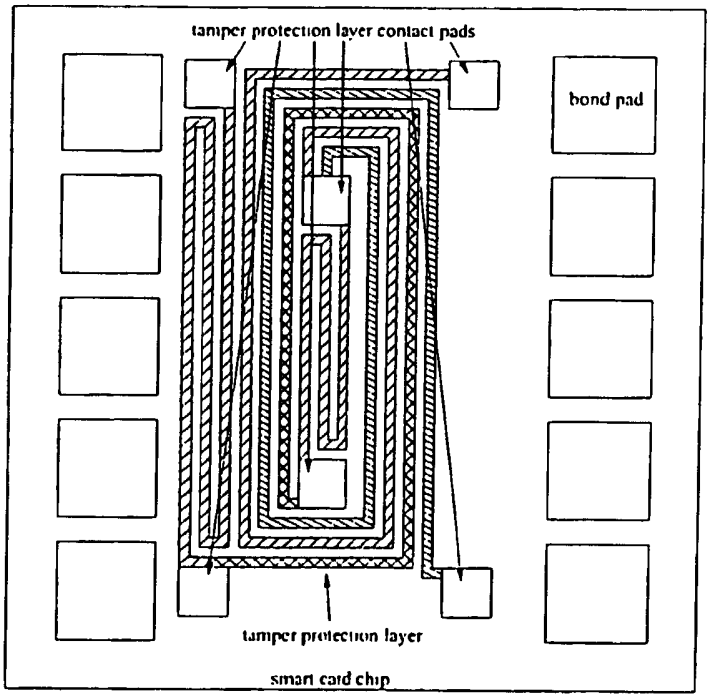

Fig. 11(b)

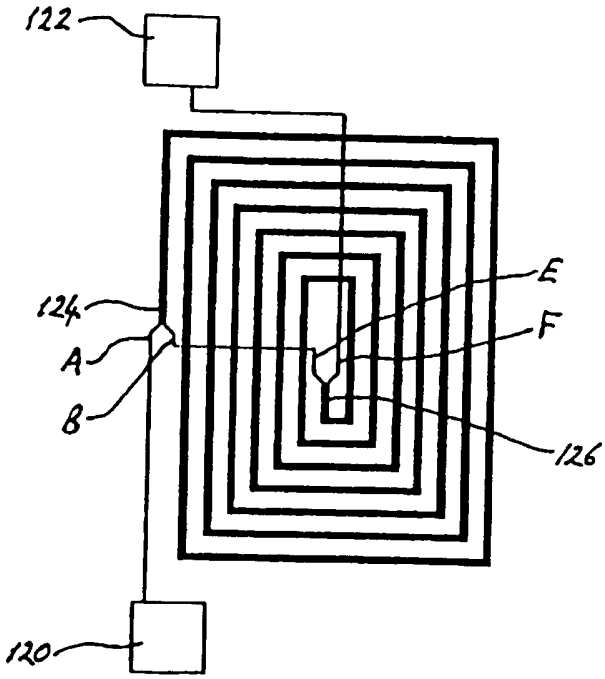

Fig. 12(a)

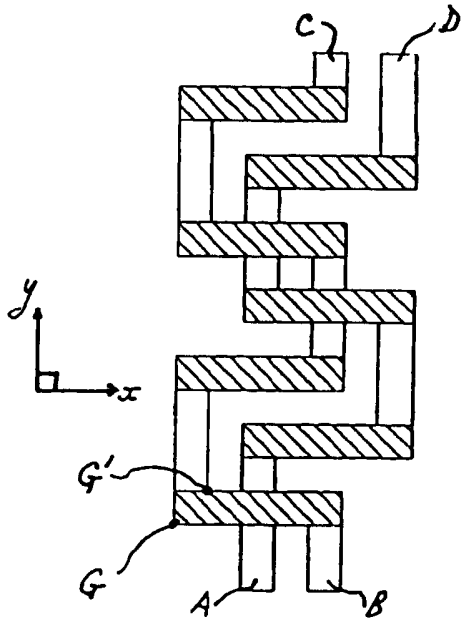

Fig. 12(b)

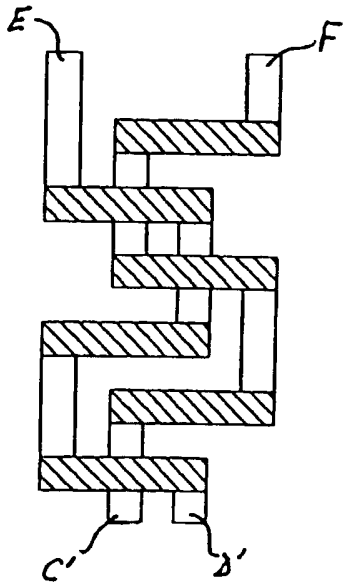

Fig. 12(c)

Intellectual Property Office

For Creativity and Innovation

30

Application No: GB0717783.5 **Examiner:** Daniel Voisey

Claims searched: 1 to 32 **Date of search:** 19 December 2007

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1, 4, 6 to 11 and 13 to 16	EP 0495645 A1 (NCR) see particularly the abstract, column 1 lines 1 to 22 and 40 to 58, column 5 line 40 to column 6 line 1, column 6 lines 33 to 37, column 9 line 14 to column 10 line 35, and figures 1 to 3, 15A to 16D, 18 and 21.
A	-	DE 102005016294 A1 (INFINEON) see particularly the abstract, paragraphs [0001], [0007] to [0009] and [0015], and figure 1.
A	-	DE 10326089 B3 (INFINEON) see particularly the abstract, paragraphs [0001], [0005], [0006], [0008], [0011], [0018] and [0019], and figures 1 to 2B.

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

G06F; G06K

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC & the Internet

International Classification:

Subclass	Subgroup	Valid From
G06F	0021/06	01/01/2006
G06F	0021/04	01/01/2006
G06K	0019/073	01/01/2006