

THIS SHEET HAS BEEN
REPLACED

TESTING OF MEMORY CONTENT

The invention relates to the testing of the content of memory associated with a microprocessor.

5 The memory may be memory whose contents cannot be altered (Read Only Memory or ROM) or memory whose contents can be altered such as Electrically Programmable Read Only Memory (EPROM) or RAM (Random Access Memory).

10 There are many instances in which memory which holds predetermined information is required to be tested. An example is in the use of integrated credit cards, otherwise known as smart cards. Conventionally, smart card memory is tested by connecting the
15 card to a reader, reading out the memory contents and performing a check on the read-out, perhaps by way of check-sum verification or by comparison of the read-out with data which should be present. Often, the memory contents are confidential and it is possible
20 that unauthorised access to the information could be obtained by simulating a memory test. An object of the invention is to overcome this problem.

According to the invention there is provided a method of testing the content of memory associated
25 with a microprocessor in a module, the method consisting in applying predetermined data as input to the module, comparing the data internally within the module with data held in the memory and issuing a verification output from the module according to
30 whether the memory content is verified as correct or not by the comparison.

The data held in the memory may be data permanently or semi-permanently resident in the memory, such as program data and/or initialisation
35 data, or may be data written to the memory as a first step in the test method. By this latter method, the

This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

write function of an electrically alterable memory can be tested.

5 The module may be an integrated circuit including the memory and the microprocessor or may be a set of integrated circuits physically bonded by encapsulation or the like. Typically the module is an integrated circuit in a smart card.

10 By use of an internal memory comparison technique as described above the memory contents are externally inaccessible directly. All that is output is a verification signal.

15 It is possible that fraudulent attempts to determine the content of the memory may be made by automatically inputting successive sets of test data which are systematically changed in content until a verification output indicates that the memory content corresponds with the input data. There are ways of dealing with this problem.

20 According to a feature of the invention the microprocessor is programmed to delay the issue of each verification or non-verification output. The delay between successive outputs may be a matter of microseconds or seconds. The object is to render the time taken for systematic checking to be
25 prohibitively long.

Another way of preventing fraudulent memory checking would be to arrange that the input data is encrypted, for example by being operated on by a secret algorithm, before comparison. Then the input
30 data would have no clear correlation with the memory content. The algorithm or a key to it could be different from batch to batch of the smart cards.

The invention will further be described with reference to the accompanying drawing, of which the
35 sole figure is a schematic diagram illustrating a method embodying the invention.

This Sheet Has Been Replaced



- 3 -

Referring to the drawing there is shown an integrated circuit 1 having a memory 2 in the form of an EEPROM which contains certain data and a comparison device 3, for example in the form of a microprocessor which is programmed to effect data comparisons. An interface to the external world is represented by the dotted line 4. On the interface 4 are three ports 5, 6 and 7 whereby signals are passed to and fro between the integrated circuit 1 and the outside world. The internal route from port 7 splits into two paths: a write path 8 passing to the memory 2 and a read path 9 passing to comparison device 3.

Testing is carried out by inputting program data to the integrated circuit 1 and performing a comparison internally by means of the comparison device 3. The program data is generated by external means (not shown) and is passed to the comparison device 3 via the data input port 7 and the read path 9. Corresponding data stored in the memory 2 is passed to the comparison device 3 via a read path 10. In the comparison device, the data entering from the two paths 9 and 10 is compared and the outcome of the comparison is communicated to the outside world via port 5 by means of a verification signal identifying the comparison as Pass or Fail. This method prevents the memory contents from ever leaving the integrated circuit 1 and thus ensures high security. The read address and control signals can be generated by external means (not shown) and input to the integrated circuit through an address/control port 6 at the interface 4. The address/control signals are passed to the memory and control the passing of data from the memory 2 to the comparison device 3 in the conventional manner.

In an alternative embodiment (not shown) the ports 5 and 7 are combined into a single multiplexed

- 4 -

5 read/write port and the port 6 eliminated. Address
and control signals which would otherwise have used
the port 6 are instead input on a multiplex basis via
the sub-port 7 of the combined port 5/7 and the path
8.

10 The scheme also allows for the testing of the
write function of electrically alterable memory by
allowing test data to be written to the memory 2 via
the data input port 7 at the interface 4 and the write
path 8. A correct write can then be verified in the
manner outlined above, again under the control of
the address/control signals. In this way properties
such as endurance, retention time and cell margin can
all be tested.

15 It might still be possible for fraudulent
access to the contents of memory 2 by exhaustively
testing all possible combinations of memory. It can
be shown that this becomes more difficult the fewer
times a pass/fail signal is generated. For instance,
20 if the pass/fail is generated after reading a single 8
bit byte, then a maximum of 256 reads are required to
exhaustively test a byte. If a pass/fail signal is
only generated after reading a 16 bit word however
then a maximum of 65,536 reads would be required to
25 exhaustively test a word. Similarly 4,294,967,296
reads are required to exhaustively test a 32 bit word.
Exhaustive testing to extract the memory contents can
easily be made unfeasible using this scheme.

30 An additional aid to security is to ensure
that words to be tested extend over memory page
boundaries, perhaps by variable amounts.

35



THIS SHEET HAS BEEN
REPLACED

CLAIMS

1. A method of testing the content of memory associated with a microprocessor in a module, the
5 method consisting in applying predetermined data as input to the module, comparing the data internally within the module with data held in the memory and issuing a verification output from the module according to whether the memory content is verified as
10 correct or not by the comparison.
2. A method as claimed in claim 1 wherein said predetermined data is passed as a first input to a comparison device forming part of said module, wherein the content of the memory is passed as a second input
15 to said comparison device and wherein said comparison device compares the data applied at its two inputs and generates a verification output signal identifying the comparison as pass or fail.
3. A method as claimed in either one of claims 1
20 or 2 wherein said data held in the memory comprises data which is resident in the memory.
4. A method as claimed in either one of claims 1 or 2 for testing the write function of the memory wherein said data held in the memory comprises test
25 data which is applied as input to the module and written to the memory prior to the comparison.
5. A method as claimed in claims 2 and 4 wherein said memory is electrically alterable and has a write input and wherein said test data is passed to said
30 write input and is temporarily stored in said memory prior to being passed to the second input to said comparison device, as aforesaid.
6. A method as claimed in any one of the preceding claims wherein the verification signal is
35 issued only after a time delay.
7. A method as claimed in any one of the

This Sheet Has Been Replaced





- 6 -

**THIS SHEET HAS BEEN
REPLACED**

preceding claims further comprising encrypting said predetermined data before comparison.

8. A method as claimed in any one of the preceding claims wherein said microprocessor is programmed to effect said data comparisons.

9. A method as claimed in any one of the preceding claims wherein said module comprises one or more integrated circuits including said memory and microprocessor.

10. A method as claimed in claim 9 wherein said integrated circuit or circuits are formed on a smart card.

This Sheet Has Been Replaced

