PROGRAMMABLE LOGIC DEVICE HAVING SECURITY ELEMENTS LOCATED AMONGST CONFIGURATION BIT LOCATIONS TO PREVENT UNAUTHORIZED READING

More than one security bit (S1, S2, S3, S4) is used in a block of a PLD chip (10). The internal configuration and other information is left unprotected when all the security bits are in the erased state, and is protected by programming one or all the security bits. The security bits are located physically in proximity to the areas containing configuration and any other user-defined data (C1, C2), both so they are difficult to discover and so that the erasure of all security bits in an EPROM-based PLD would cause a large number of adjacent user-defined bits to be erased as well, hence making it very difficult to extract useful information from a protected device by reverse engineering. Situating security bits in a different, pseudorandom location within each block of the chip makes them difficult to find and so further inhibits reverse engineering.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AT</td>
<td>Austria</td>
<td>GB</td>
<td>United Kingdom</td>
<td>MR</td>
<td>Mauritania</td>
</tr>
<tr>
<td>AU</td>
<td>Australia</td>
<td>GE</td>
<td>Georgia</td>
<td>MW</td>
<td>Malawi</td>
</tr>
<tr>
<td>BB</td>
<td>Barbados</td>
<td>GN</td>
<td>Guinea</td>
<td>NE</td>
<td>Niger</td>
</tr>
<tr>
<td>BE</td>
<td>Belgium</td>
<td>GR</td>
<td>Greece</td>
<td>NL</td>
<td>Netherlands</td>
</tr>
<tr>
<td>BF</td>
<td>Burkina Faso</td>
<td>HU</td>
<td>Hungary</td>
<td>NO</td>
<td>Norway</td>
</tr>
<tr>
<td>BG</td>
<td>Bulgaria</td>
<td>IE</td>
<td>Ireland</td>
<td>NZ</td>
<td>New Zealand</td>
</tr>
<tr>
<td>BJ</td>
<td>Benin</td>
<td>IT</td>
<td>Italy</td>
<td>PL</td>
<td>Poland</td>
</tr>
<tr>
<td>BR</td>
<td>Brazil</td>
<td>JP</td>
<td>Japan</td>
<td>PT</td>
<td>Portugal</td>
</tr>
<tr>
<td>BY</td>
<td>Belarus</td>
<td>KE</td>
<td>Kenya</td>
<td>RO</td>
<td>Romania</td>
</tr>
<tr>
<td>CA</td>
<td>Canada</td>
<td>KG</td>
<td>Kyrgyzstan</td>
<td>RU</td>
<td>Russian Federation</td>
</tr>
<tr>
<td>CF</td>
<td>Central African Republic</td>
<td>KP</td>
<td>Democratic People's Republic of Korea</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CG</td>
<td>Congo</td>
<td>CG</td>
<td>Congo</td>
<td>SD</td>
<td>Sudan</td>
</tr>
<tr>
<td>CH</td>
<td>Switzerland</td>
<td>CI</td>
<td>Côte d'Ivoire</td>
<td>SE</td>
<td>Sweden</td>
</tr>
<tr>
<td>CI</td>
<td>Côte d'Ivoire</td>
<td>CM</td>
<td>Cameroon</td>
<td>SI</td>
<td>Slovenia</td>
</tr>
<tr>
<td>CM</td>
<td>Cameroon</td>
<td>CN</td>
<td>China</td>
<td>SK</td>
<td>Slovakia</td>
</tr>
<tr>
<td>CN</td>
<td>China</td>
<td>CS</td>
<td>Czechoslovakia</td>
<td>SN</td>
<td>Senegal</td>
</tr>
<tr>
<td>CS</td>
<td>Czechoslovakia</td>
<td>CZ</td>
<td>Czech Republic</td>
<td>TD</td>
<td>Chad</td>
</tr>
<tr>
<td>CZ</td>
<td>Czech Republic</td>
<td>DE</td>
<td>Germany</td>
<td>TG</td>
<td>Togo</td>
</tr>
<tr>
<td>DE</td>
<td>Germany</td>
<td>DK</td>
<td>Denmark</td>
<td>TJ</td>
<td>Tajikistan</td>
</tr>
<tr>
<td>DK</td>
<td>Denmark</td>
<td>ES</td>
<td>Spain</td>
<td>TT</td>
<td>Trinidad and Tobago</td>
</tr>
<tr>
<td>ES</td>
<td>Spain</td>
<td>FI</td>
<td>Finland</td>
<td>UA</td>
<td>Ukraine</td>
</tr>
<tr>
<td>FI</td>
<td>Finland</td>
<td>FR</td>
<td>France</td>
<td>US</td>
<td>United States of America</td>
</tr>
<tr>
<td>FR</td>
<td>France</td>
<td>GA</td>
<td>Gabon</td>
<td>UZ</td>
<td>Uzbekistan</td>
</tr>
<tr>
<td>GA</td>
<td>Gabon</td>
<td>MN</td>
<td>Mongolia</td>
<td>VN</td>
<td>Viet Nam</td>
</tr>
</tbody>
</table>
BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates generally to programmable logic devices (PLDs), and more particularly to security protection of internal configuration information of PLDs.

Description of the Prior Art

A PLD usually includes multiple configurable logic blocks, I/O blocks and an interconnect network. Figure 1 shows one enlarged configurable logic block in a PLD device, including a programmable configuration element area A, where programmable configuration elements 11 are located in a row-column array, and an area B, where the AND array, and hence the AND programmable element array are located. A typical PLD contains several such blocks. It is to be understood that the AND array B is only an example; area B can be any other programmable logic array. The programmable configuration elements in area A control multiplexers, gates, tri-state buffers, etc. to configure the block into different internal configurations, while the AND programmable elements in area B are for programming the AND array to specify different combinatorial logic functions. In addition, programmable elements are also included in the interconnect network to determine routing between the blocks. In most cases, all these programmable elements are identical for a given PLD. They may be fuses, anti-fuses, EPROM or EEPROM elements or other programmable memory elements.

Programming of a PLD is accomplished by programming each of the programmable elements. However, the most important information defining a user's chip design of the block is contained in the programmable configuration element
array in area A because the programming of these elements 11
determines the basic circuit structure the block assumes.
Normally the state pattern of these programmable elements
programmed into a PLD can, like a PROM, be read and
displayed by use of programming hardware to allow a user to
verify his design. Therefore, if no security steps are
taken, a user's design implemented by such programmed PLDs
can easily be reverse-engineered (copied) since the state
pattern of the programmable configuration elements
programmed into a PLD determines the internal configuration,
therefore the operation, of the device. Therefore, a single
security element configuration bit 12 as shown in Figure 1
is often provided in PLDs, and disables this read function
when bit 12 is in a set state. This somewhat secures the
user's design from attempts to copy or reverse engineer it.
However, no special consideration is given as to the
location of bit 12, and it has even in some cases been
physically isolated in some chips, making its location
easily discovered. In any case, if a reverse engineer
carefully examines the chip and sees what gates control the
reading operation and what disables the reading operation,
he may find the security bit 12 and restore it to its unset
or original state, and then the internal configuration
information can easily be read out again.

Erasable CMOS PLDs, commonly called EPLDs, are
considerably more secure than the above described
electrically programmable devices. EPLDs are fabricated by
a technology similar to that of EPROMs, and have a quartz
window in the chip package for UV-erasing programmed data,
and are reprogrammable. As described above, EPROM-based
PLDs have a "security bit" 12 in configuration area A as
shown in Figure 1, which, if set by the programmer, disables
reading of the internal configuration information. For such
a device, the security bit can be erased by exposure of the
chip to ultraviolet light, although in such a case, all the
configuration information in area A is erased as well, hence
ensuring the security of the design. However, the security
bit can sometimes be defeated by a diligent "reverse
engineer" who carefully examines the chip and determines
approximately where in the chip the single security bit is
located, and can erase just the area immediately surrounding
the security bit, while leaving much of the other EPROM
region unerased. In this case, the bulk of the
configuration information can still be read out, easing the
task of reverse engineering.

SUMMARY OF THE INVENTION

Accordingly, one object of this invention is to improve
design security in PLDs to prevent information entered by a
user from being read out by unauthorized personnel, thus
preventing the device from being reverse engineered.

Another object of this invention is to provide a method
for design security in PLDs which makes security bits more
difficult to be found by unauthorized personnel.

A further object with EPROM-based PLDs is for a large
number of bits per block to be erased if someone attempts to
reverse engineer a user's design.

According to the present invention, a plurality of
programmable security elements is provided in a PLD, each
element having first and second states. The plurality of
programmable security elements enables configuration and
other data to be read from the programmable logic device
only when each of the plurality of programmable security
elements is set to a given state; the plurality of
programmable security elements disables reading of user-
entered data when at least one of the programmable security
element is not set to its given state. In one embodiment,
all security elements are set to logical 1 after programming
and must be reset to logical 0 before the configuration and
other data can be read. In another embodiment, the security
bits are set after configuration to carry a selected pattern
of 0's and 1's and must all be set to the opposite states
before configuration and other data can be read.

In accordance with one aspect of the invention, at
least some of the plurality of programmable security bits
are disposed physically in close proximity to areas containing configuration data.

In accordance with another aspect of the invention, the programmable security bits are each situated in a different, pseudorandom location within each configuration EPROM region to make it difficult to find them and to cause erasure of the configuration bits surrounding the bits when an attempt to erase the security bit is made.

The above and other objects, features and advantages of the present invention will be clear from the following detailed description in conjunction with the drawings.

**BRIEF DESCRIPTION OF THE DRAWINGS**

Figure 1 is a schematic diagram showing in the prior art a single programmable security element located in a programmable configuration element array.

Figure 2 is a schematic diagram showing an embodiment of the present invention, where multiple programmable security elements are distributed over the programmable configuration element array.

**DETAILED DESCRIPTION**

Figure 2, similar to Figure 1, shows an enlarged configurable logic block (one of several on a PLD) which includes a programmable configuration element array A and an AND gate programmable element array B. According to the present invention, a plurality of programmable security elements, for example S1, S2, S3 and S4 as shown in Figure 2, are distributed among the array of programmable configuration elements (configuration bits) C1, C2, .... The security elements S1, ..., S4 are each set by the programmer after programming of the PLD, disabling the reading of the internal configuration information in the PLD block. The configuration information can be read from the PLD block only when each of the programmable security elements is located and restored to its original or unset state. Since these programmable security elements are
usually identical in physical structure to the programmable
elements C1, C2, . . . in the array A in which they are
distributed, such distribution makes location of them
difficult for a reverse-engineer. As mentioned above, the
programmable elements may be fuses, anti-fuses, EPROM or
EEPROM elements, or other programmable memory elements.

In the case of EPROM-based PLDs, the array A in Figure
2 is the configuration EPROM array, and the array B is the
AND EPROM array. Programming technology similar to that of
conventional EPROMs is employed, and configuration data
programmed into such a PLD can be UV-erased for
reprogramming of the device. Floating gate avalanche
injection MOS (FAMOS) transistors are used as programmable
security bits, or alternatively other programmable elements
may be used for the erasable part of the device. The set
state of a FAMOS transistor is erased by discharging the
floating gate of the transistor which was charged during its
programming, by exposure to UV light for a period of time.
However, it is difficult to guide the ultraviolet light to
only a single FAMOS transistor, which occupies an extremely
small area on a chip, without exposing the proximal area.
This is because the reverse engineer can only estimate the
approximate locations of the security bits after he examines
the chip. Also, reverse engineers typically lack
positioning equipment which generate a sharp enough beam to
locate and focus light on a single transistor. In a typical
case, erasing of a security bit by a reverse engineer will
therefore simultaneously erase at least 8 to 20 surrounding
configuration bits if it is disposed within the
configuration EPROM array A. Consequently, when enough
security bits are distributed over the array A, erasure of
all these security bits also erases a substantial number of
adjacent configuration bits, so that a reverse engineer or
copier would not get any significant design information from
the rest of the configuration data, causing the reverse
engineering attempt to fail.

The manner in which multiple security bits disable the
reading operation from the configuration EPROMS is similar
to the prior art where a single security bit is used. Each
security bit, like any other configuration bit, contains
data which is loaded into a latch on the chip upon power up.
The latch for the security bit in the prior art then
controls the reading operation of the configuration EPROM
cells through logic gates. When multiple security bits are
used, the outputs of corresponding security latches are
logically ORed before controlling the reading operation
through the gates. Therefore only when all the multiple
security bits are in the unset state, is the reading
operation enabled. As mentioned earlier, other embodiments
use other patterns, and reading of these other embodiments
is enabled with corresponding logic gates. For example, an
embodiment which required four security bits to carry the
pattern 0101 would use an OR gate with two inverted inputs,
and enable reading when the output was low.

The locations of the security bits may differ from one
model to another. The locations of the security bits are
fixed when a chip is fabricated, and the information as to
the locations is supplied in separate documents to the user.
Even if these documents fall into a reverse engineer's
hands, he still will not be able to obtain any significant
design information because of the erasing of a substantial
number of configuration bits when he tries to erase the
security bits.

The number of security bits used depends on the size of
the configuration array block to be protected. As an
example, if the configuration array has 9 bit lines and 48
bit columns, then 4 security bits are adequate because to
erase 4 security bits will erase 32 to 80 of the 432
configuration bits, causing significant loss of
configuration information. In one embodiment using a larger
array, 40 security bits are distributed through the array.

Furthermore, each of the plurality of security bits is
in one embodiment situated in a different, pseudorandom
location within each EPROM block so that they are difficult
to locate.
With the scheme described above, the configuration data may be left unprotected by simply leaving all the security bits in the unset or erased state. The configuration may be protected by programming any or all the security bits. In order to read a protected device, all the set security bits must be found and erased. Since it is very difficult to erase an individual EPROM bit using ultraviolet light without erasing some of its neighbors, erasure of each set security bits causes many adjoining configuration bits to be erased as well, hence making it very difficult to extract useful information from a protected device.

Though the above description relates to configuration information, in another embodiment, a user enters both configuration information and other data specific to the design. The security bits also protect this other information because they are embedded in the area where the configuration and other information are stored.

A legitimate user has no need to unset the security bits since if the legitimate user wants to read back the configuration data he simply does not set the security bits (or in another embodiment sets them to the pattern which will allow readback). Such a mode is used for testing. Of course the legitimate user also has access to the configuration data before it is loaded into the device.

This disclosure is illustrative and not limiting; further modifications and variations will be apparent to those skilled in the art in light of this disclosure and the appended claims. For example, the security bits can also be scattered among the programmable elements in the interconnect network or even in the AND EPROM array B; the scheme is also suitable using any light-erasable programmable element as security bit. The scope of the invention is limited only by the claims which follow.
WHAT WE CLAIM IS:

1. A method for improving design security in a programmable logic device on an integrated circuit die, comprising:
   providing on the integrated circuit die an array of programmable configuration elements;
   providing on the integrated circuit die a plurality of programmable security elements, each having a state which allows readback and a state which does not allow readback, and wherein each programmable security element is distributed among elements of said array;
   connecting said plurality of programmable security elements to the integrated circuit, wherein said plurality of programmable security elements enables data to be read out from the programmable logic device only when each of said plurality of programmable security elements is set to its state which allows readback; and said plurality of programmable security elements disables the reading of data when at least one of said programmable security elements is set to its state which does not allow readback; and
   setting at least one of said programmable security elements to its state which does not allow readback.

2. A method as in Claim 1, wherein the programmable security elements and programmable configuration elements are structurally identical.

3. A method as in Claim 2, wherein said same programmable security elements are light-erasable programmable elements.

4. A method as in Claim 3, wherein the light is ultraviolet light.

5. A method as in Claim 1, wherein said programmable security elements are disposed at irregular locations in the programmable logic device.
6. A programmable logic device comprising:
   an array of programmable configuration elements;
   a plurality of programmable security elements,
   each having a first state and a second state, each
   programmable security elements being distributed among
   elements of said array of programmable configuration
   elements;
   said plurality of programmable security elements
   enabling data to be read from the programmable logic device
   only when each of said plurality of programmable security
   elements is set to the first state; and
   said plurality of programmable security elements
   disabling the reading of data when at least one of said
   programmable security elements is set to the second state.

7. A device as in Claim 6, wherein said plurality of
   programmable security elements are distributed across said
   array in an irregular pattern.

8. A device as in Claim 6, wherein the programmable
   security elements and the programmable configuration
   elements are light-erasable elements.

9. An EPROM-based programmable logic device
   comprising:
   at least one EPROM array for storing user-defined
   data;
   a plurality of programmable security bits
   distributed across said EPROM array, wherein each
   programmable security bit is distributed among elements of
   said EPROM array;
   said plurality of programmable security bits
   enabling data to be read from the EPROM array when each of
   the plurality of programmable security bits is set to one of
   its binary values; and
   said plurality of programmable security bits
   disabling the reading of configuration data when at least
one of said programmable security bits is set to the other
of its binary values.

10. An EPROM-based programmable logic device as in
Claim 9, wherein said programmable security bits are
distributed among said EPROM array elements in an irregular
manner.

11. The method of Claim 1, wherein each programmable
security element is randomly distributed among the elements
of said array.

12. The device of Claim 6, wherein each programmable
security element is randomly distributed among said array of
programmable configuration elements.

13. A method for improving design security in a
programmable logic device on an integrated circuit die,
comprising:

   providing on the integrated circuit die a
   plurality of programmable security elements, each
   having a state which allows readback and a state which
does not allow readback;
   disposing each of the programmable security
   elements in proximity to areas containing said data for
   the programmable logic device on the integrated circuit
die at irregular locations in the programmable logic
device;
   connecting said plurality of programmable security
   elements to the integrated circuit, wherein said
   plurality of programmable security elements enables
date to be read out from the programmable logic device
only when each of said plurality of programmable
security elements is set to its state which allows
readback; and said plurality of programmable security
elements disables the reading of data when at least one
of said programmable security elements is set to its
state which does not allow readback; and
setting at least one of said programmable security
elements to its state which does not allow readback.

14. A programmable logic device comprising:
a plurality of programmable security elements,
each having a first state and a second state;
an array of programmable configuration elements,
wherein said plurality of programmable security
elements are distributed in an irregular pattern on
said array;
said plurality of programmable security elements
enabling data to be read from the programmable logic
device only when each of said plurality of programmable
security elements is set to the first state; and
said plurality of programmable security elements
disabling the reading of data when at least one of said
programmable security elements is set to the second
state.
1. A method for improving design security in a programmable logic device on an integrated circuit die, comprising:
   providing on the integrated circuit die an array of programmable configuration elements;
   providing on the integrated circuit die a plurality of programmable security elements, each having a state which allows readback and a state which does not allow readback, and wherein each programmable security element is distributed among programmable configuration elements of said array;
   connecting said plurality of programmable security elements to the integrated circuit, wherein said plurality of programmable security elements enables data to be read out from the programmable logic device only when each of said plurality of programmable security elements is set to its state which allows readback; and said plurality of programmable security elements disables the reading of data when at least one of said programmable security elements is set to its state which does not allow readback; and
   setting at least one of said programmable security elements to its state which does not allow readback.

2. A method as in Claim 1, wherein the programmable security elements and programmable configuration elements are structurally identical.

3. A method as in Claim 2, wherein said same programmable security elements are light-erasable programmable elements.

4. A method as in Claim 3, wherein the light is ultraviolet light.
5. A device as in Claim 1, wherein said programmable
security elements are disposed at irregular locations in the
programmable logic device.

6. A programmable logic device comprising:
an array of programmable configuration elements;
a plurality of programmable security elements,
each having a first state and a second state, each
programmable security element being distributed among
elements of said array of programmable configuration
elements;
said plurality of programmable security elements
enabling data to be read from the programmable logic
device only when each of said plurality of programmable
security elements is set to the first state; and
said plurality of programmable security elements
disabling the reading of data when at least one of said
programmable security elements is set to the second
state.

7. A device as in Claim 6, wherein said plurality of
programmable security elements are distributed across said
array in an irregular pattern.

8. A device as in Claim 6, wherein the programmable
security elements and the programmable configuration
elements are light-erasable elements.

9. An EPROM-based programmable logic device
comprising:
at least one EPROM array for storing user-defined
data;
a plurality of programmable security bits
distributed among programmable elements of said EPROM
array;
said plurality of programmable security bits
enabling data to be read from the EPROM array when each
of the plurality of programmable security bits is set
to one of its binary values; and
    said plurality of programmable security bits
disabling the reading of configuration data when at
least one of said programmable security bits is set to
the other of its binary values.

10. An EPROM-based programmable logic device as in
Claim 9, wherein said programmable security bits are
distributed among said programmable elements in an irregular
manner

11. The method of Claim 1, wherein each programmable
security element is randomly distributed among said
programmable configuration elements of said array.

12. The device of Claim 6, wherein each programmable
security element is randomly distributed among said array of
programmable configuration elements.

13. A method for improving design security in a
programmable logic device on an integrated circuit die,
comprising:
    providing on the integrated circuit die a
    plurality of programmable security elements, each
    having a state which allows readback and a state which
does not allow readback;
    disposing each of the programmable security
    elements in proximity to areas containing data for the
    programmable logic device on the integrated circuit die
    at irregular locations in the programmable logic
device;
    connecting said plurality of programmable security
    elements to the integrated circuit, wherein said
    plurality of programmable security elements enables
    said data to be read out from the programmable logic
device only when each of said plurality of programmable
    security elements is set to its state which allows
readback; and said plurality of programmable security
elements disables the reading of said data when at
least one of said programmable security elements is set
to its state which does not allow readback; and
setting at least one of said programmable security
elements to its state which does not allow readback.

14. A programmable logic device comprising:
a plurality of programmable security elements,
each having a first state and a second state;
an array of programmable configuration elements,
wherein said plurality of programmable security
elements are distributed in an irregular pattern on
said array;
said plurality of programmable security elements
enabling data to be read from the programmable logic
device only when each of said plurality of programmable
security elements is set to the first state; and
said plurality of programmable security elements
disabling the reading of data when at least one of said
programmable security elements is set to the second
state.
STATEMENT UNDER ARTICLE 19

Claim 1 is believed to patentably distinguish over the cited references by reciting "wherein each programmable security element is distributed among programmable configuration elements of said array". Claim 6 is believed to distinguish by reciting "each programmable security element being distributed among elements of said array of programmable configuration elements". Claim 9 is believed to distinguish by reciting "a plurality of programmable security bits distributed among programmable elements of said EPROM array". Claim 13 is believed to distinguish by reciting "disposing each of the programmable security elements in proximity to areas containing data for the programmable logic device on the integrated circuit die at irregular locations in the programmable logic device". Claim 14 is believed to distinguish by reciting "wherein said plurality of programmable security elements are distributed in an irregular pattern on said array".

None of the documents cited in the International Search Report appear to anticipate or make obvious the combination of features recited in any of independent Claims 1, 6, 9, 13, and 14 as discussed above. Dependent claims also distinguish from the references cited in the International Search Report for at least the reasons of the independent claims from which they depend.
Fig. 1
Prior Art

Fig. 2
AND EPROM array
A. CLASSIFICATION OF SUBJECT MATTER
IPC(5) : H03K 19/177; H04L 9/00; G11C 17/12
US CL. : 307/465; 380/4; 365/185
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 307/465; 380/4; 365/185,96,201; 340/825.83, 825.87

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

Electronic database consulted during the international search (name of database and, where practicable, search terms used)
APS; search terms of programmable, logic, array or device, ROM, read only memory, security, random

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US, A, 5,175,840 (Sawase et al.) 29 December 1992, column 3, line 57 - column 4, line 6; Figure 2.</td>
<td>1-4, 6, 8, 9, 13 and 14</td>
</tr>
<tr>
<td>A</td>
<td>US, A, 4,698,617 (Bauer) 06 October 1987, column 5, line 48 - column 6, line 11, Figures 2a and 2b.</td>
<td>5, 10, 11</td>
</tr>
<tr>
<td>A</td>
<td>US, A, 5,099,516 (Durkin et al.) 24 March 1992, whole document.</td>
<td>All</td>
</tr>
<tr>
<td>A</td>
<td>US, A, 5,191,608 (Geronimi) 02 March 1993, column 6, lines 16-26, Figure 1.</td>
<td>All</td>
</tr>
<tr>
<td>A,P</td>
<td>US, A, 5,224,166 (Hartman, Jr.) 29 June 1993, whole document.</td>
<td>All</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

Date of the actual completion of the international search: 25 MAY 1994
Date of mailing of the international search report: 31 MAY 1994

Name and mailing address of the ISA/US Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. N. A.

Authorized officer
Benjamin D. Driscoll
Telephone No. (703) 308-0956