

1 **What is claimed is:**

2 1. A method for controlling a production process for a product comprising:

- 3 - including in a design for said product, a module having a mathematical transform for
4 intercepting and transforming data flow in said product, said mathematical transform
5 requiring a key to be operable and said product requiring successful operation of said
6 mathematical transform to be operable;
7 - arranging said production process into a plurality of stages, each of said plurality of
8 stages capable of being performed by respective ones of a plurality of entities;
9 - dividing said key into a plurality of portions of sensitive data and distributing each of
10 said plurality of portions to respective ones of said plurality of entities; and
11 - distributing a mask for producing said product according to said design to a first one
12 of said plurality of entities to enable said first one of said plurality of entities to add a
13 first portion of sensitive data to said key;

14 wherein said product is operable upon adding all of said plurality of portions of sensitive
15 data.

16
17 2. A method according to claim 1 further comprising distributing an inoperable product
18 comprising said first portion of sensitive data to at least one other entity to perform
19 subsequent stages whereby subsequent portions of sensitive data are added to said key to
20 make said key operable thereby producing an operable product.

21
22 3. A method according to claim 1 further comprising establishing a communication channel
23 between a producer and said plurality of entities for securing distributing said sensitive
24 data.

25
26 4. A method according to claim 3 further comprising each of said plurality of entities
27 providing a log report to said producer upon adding a respective portion of said sensitive
28 data.

29
30 5. A method according to claim 3 wherein said producer generates said design and is
31 responsible for dividing said key.

32

- 1 6. A method according to claim 1 wherein said product is an integrated circuit (IC).
2
- 3 7. A method according to claim 6 wherein said mask is used by said first one of said
4 plurality of entities to produce a silicon wafer.
5
- 6 8. A method according to claim 1 wherein said mathematical transform is a cryptographic
7 transform and said key is a cryptographic key.
8
- 9 9. A method according to claim 8 wherein said cryptographic transform uses at least one
10 exclusive-or (XOR) operation.
11
- 12 10. A method for controlling operation of a product comprising:
13 - intercepting data provided by a first portion of said product;
14 - inputting said data into a mathematical transform;
15 - applying said mathematical transform to said data using a key to generate an output,
16 said mathematical transform requiring said key to be operable; and
17 - providing said output to a second portion of said product;
18 wherein said product requires successful operation of said mathematical transform to be
19 operable and said mathematical transform comprises a plurality of portions of sensitive
20 data each of which are added during production of said product in a plurality of stages.
21
- 22 11. A method according to claim 10 wherein said data is a boot signal.
23
- 24 12. A method according to claim 10 wherein said mathematical transform is a cryptographic
25 transform and said key is a cryptographic key.
26
- 27 13. A method according to claim 12 wherein said cryptographic transform uses at least one
28 exclusive-or (XOR) operation.
29
- 30 14. A method according to claim 10 wherein said first portion comprises protected logic, and
31 said second portion comprises unprotected logic.
32

- 1 15. A registration module included in a product for controlling operation of said product
2 comprising a mathematical transform for intercepting and transforming data flow in said
3 product; and a key stored in a memory, said mathematical transform requiring said key to
4 be operable, said product requiring successful operation of said mathematical transform to
5 be operable; wherein said key comprises a plurality of portions of sensitive data each of
6 which are added during production of said product in a plurality of stages.
7
- 8 16. A module according to claim 15 wherein said data flow is a boot signal.
9
- 10 17. A method according to claim 15 wherein said mathematical transform is a cryptographic
11 transform and said key is a cryptographic key.
12
- 13 18. A method according to claim 17 wherein said cryptographic transform uses at least one
14 exclusive-or (XOR) operation.
15
- 16 19. A method according to claim 15 wherein said data flow is output by protected logic, and
17 an output from said mathematical transform is provided to unprotected logic.
18
- 19 20. A system for controlling a production process for a product comprising a controller at a
20 first entity, said first entity being responsible for said production process; and a plurality
21 of servers at a plurality of process stages, said plurality of servers being configured for
22 receiving sensitive data from said controller in a secure manner and for sending log
23 reports to said controller; said controller being configured for distributing a mask for
24 producing said product to a first one of said plurality of servers to enable said first one of
25 said plurality of servers to add a first portion of sensitive data to a key in said product at a
26 first process stage, said key being used to operate a mathematical transform in said
27 product, said product requiring successful operation of said mathematical transform to be
28 operable; and wherein at least one other of said plurality of servers is configured for
29 adding at least one other portion of sensitive data to said key in at least one other process
30 stage.

Claims

1. A method of controlling a production process for a product (22,22a), said method comprising:
 - including in a design (90) for said product, a module (92') having a mathematical transform (128,128a) for intercepting and transforming data flow in said product, said mathematical transform requiring a key (131) to be operable and said product requiring successful operation of said mathematical transform to be operable;
 - arranging said production process into a plurality of stages of production, each of said plurality of stages of production capable of being performed by respective ones of a plurality of entities;
 - dividing said key into a plurality of portions and distributing each portion to a respective one of said plurality of entities; and
 - initiating a first stage of production according to said design, said first stage of production comprising a first one of said plurality of entities adding a first portion of said key to said product;wherein said product is operable upon all of said plurality of portions being added to said product.
2. The method according to claim 1, further comprising distributing an inoperable product (22,22a) comprising said first portion of said key (131) to at least one other entity to perform one or more subsequent stages whereby subsequent portions of said key are added to said product to complete said key thereby producing an operable product.
3. The method according to claim 1 or claim 2, further comprising establishing a communication channel (23) between a producer (12) and said plurality of entities for securely distributing said portions.
4. The method according to claim 3, further comprising each of said plurality of entities providing a log report (R) to said producer (12) upon adding a respective portion to said product.
5. The method according to claim 3 or claim 4, wherein said producer generates said design (90) and is responsible for dividing said key (131).

6. The method according to any one of claims 1 to 5, wherein said product is an integrated circuit (IC).
7. The method according to claim 6, wherein a definition of said design is used by said first one of said plurality of entities to produce a silicon wafer.
8. The method according to any one of claims 1 to 7, wherein said mathematical transform is a cryptographic transform and said key is a cryptographic key.
9. The method according to claim 8, wherein said cryptographic transform uses at least one exclusive-or (XOR) operation.
10. A system for controlling a production process for a product (22), said system comprising a controller (16) having a processor and memory, said memory storing computer executable instructions that when executed by the processor cause a plurality of servers (16) at a plurality of process stages to perform the method according to any of the preceding claims.
11. A method of controlling operation of a product, said method comprising:
 - intercepting data provided by a first portion (120a) of said product;
 - inputting said data into a mathematical transform (128, 128a);
 - applying said mathematical transform to said data using a key (134a) to generate an output, said mathematical transform requiring said key to be operable, said key having been made operable by a plurality of portions thereof being added by respective entities during respective stages of production; and
 - providing said output to a second portion (122a) of said product;wherein said product is operable if said mathematical transform is operable.
12. The method according to claim 11, wherein said data is a boot signal.
13. The method according to claim 11 or claim 12, wherein said mathematical transform is a cryptographic transform and said key is a cryptographic key.
14. The method according to claim 13 wherein said cryptographic transform uses at least one exclusive-or (XOR) operation.

- 15.** The method according to any one of claims 11 to 14, wherein said first portion of said product comprises protected logic, and said second portion of said product comprises unprotected logic.
- 16.** A registration module (92') for a product (22,22a), said registration module for controlling operation of said product, said registration module comprising a memory for storing a key (131) and computer executable instructions for performing the method according to any one of claims 11 to 15.
- 17.** A product comprising the registration module according to claim 16.
- 18.** The product according to claim 17 comprising an integrated circuit.