(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 October 2011 (13.10.2011)

PCT

(10) International Publication Number
WO 2011/126587 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/US2011/021412

(22) International Filing Date:
14 January 2011 (14.01.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/755,792 7 April 2010 (07.04.2010) US

(71) Applicant *(for all designated States except US)*: **XILINX, INC.** [US/US]; 2100 Logic Drive, San Jose, CA 95124 (US).

(72) Inventors: **LESEA, Austin, H.**; 2100 Logic Drive, San Jose, CA 95124 (US). **TRIMBERGER, Stephen, M.**; 2100 Logic Drive, San Jose, CA 95124 (US).

(74) Agents: **CARTIER, Lois, D.** et al.; Xilinx, Inc., 2100 Logic Drive, San Jose, CA 95124 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: A METHOD AND INTEGRATED CIRCUIT FOR SECURE ENCRYPTION AND DECRYPTION

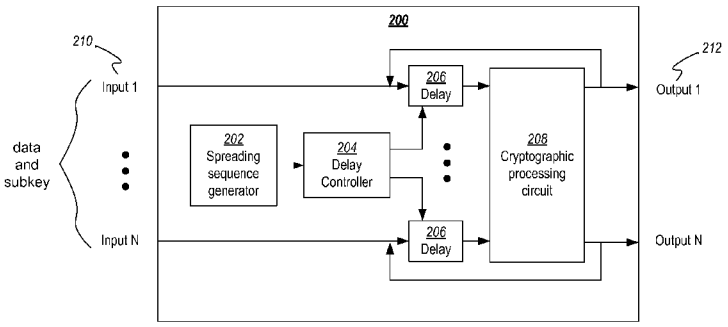

FIG. 2

(57) Abstract: In one embodiment, a secure cryptographic circuit arrangement is provided (200). The secure cryptographic circuit includes a cryptographic processing block (208), a spreading sequence generator (202), and a delay control circuit (204). The cryptographic processing block has a plurality of signal paths (210). One or more of the plurality of signal paths includes respective adjustable delay circuits (206). The spreading sequence generator is configured to output a sequence of pseudo-random numbers (114). The delay control circuit has an input coupled to an output of the spreading sequence number generator and one or more outputs coupled to respective delay adjustment inputs of the adjustable delay circuits. The delay control circuit is configured to adjust the adjustable delay circuits based on the pseudo-random numbers (116 & 118).

WO 2011/126587 A1

A METHOD AND INTEGRATED CIRCUIT FOR SECURE ENCRYPTION AND DECRYPTION

FIELD OF THE INVENTION

The present invention generally relates to encryption, and more particularly to the encryption of data used to reconfigure programmable logic.

BACKGROUND

Programmable logic circuits are integrated circuits (ICs) that are user configurable and capable of implementing digital logic operations. There are several types of programmable logic ICs, including Complex Programmable Logic Devices (CPLDs) and Field Programmable Gate Arrays (FPGAs). CPLDs include function blocks based on programmable logic array (PLA) architecture and programmable interconnect lines to route and transmit signals between the function blocks. FPGAs include configurable logic blocks (CLBs) arranged in rows and columns, input output blocks surrounding the CLBs, and programmable interconnect lines that route and transmit signals between the CLBs. Each CLB includes look-up tables and other configurable circuitry that is programmable to implement a logic function. The function blocks of CPLDs, CLBs of FPGAs and interconnect lines are configured by data stored in a configuration memory of the respective devices.

Designs implemented in programmable logic have become complex. Due to the time and investment required for design and debugging, it is desirable to protect the design from unauthorized copying. Efforts have been made to encrypt designs and provide the encrypted designs to the target devices. Several encryption algorithms, for example, the standard Data Encryption Standard (DES) and the more secure Advanced Encryption Standard (AES) algorithms, are known for encrypting blocks of data. Additionally, a one-time encryption pad may be used as a cipher for encrypting blocks of data by XORing blocks of data with blocks of the one-time pad (OTP). These approaches require provision of a key to the structure that decrypts the design, and the key must be protected from unauthorized discovery.

A decryption key can be stored in nonvolatile memory of a programmable integrated circuit. An encrypted bitstream can then be loaded into the IC and decrypted using the key within the programmable logic. This prevents an attacker from reading the bitstream as it is being loaded into the programmable logic IC. However, this structure must also protect from modes of attack in which the attacker attempts to obtain the decryption key stored in the programmable IC. If the attacker obtains the decryption key, the attacker can decrypt an intercepted bitstream to reveal the unencrypted design.

One method through which an attacker may attempt to discover the decryption key is known as power analysis. In a power analysis attack, current used by a device is monitored while the device is decrypting. During normal operation, the amount of power used by a device varies depending on the logic gates activated at a given time. By monitoring variations in the power consumption while the device is decrypting a configuration bitstream, for example, the attacker can identify operations that are performed and determine the decryption key.

The present invention may address one or more of the above issues.

SUMMARY

In one embodiment, a secure cryptographic circuit arrangement is provided. The secure cryptographic circuit includes a cryptographic processing block, a spreading sequence generator, and a delay control circuit. The cryptographic processing block has a plurality of signal paths. One or more of the plurality of signal paths includes respective adjustable delay circuits. The spreading sequence generator is configured to output a sequence of pseudo-random numbers.

The delay control circuit has an input coupled to an output of the spreading sequence number generator and one or more outputs coupled to respective delay adjustment inputs of the adjustable delay circuits. The delay control circuit is configured to adjust the adjustable delay circuits based on the pseudo-random numbers.

In another embodiment, the delay control circuit is configured to adjust each of the adjustable delay circuits based on different bits of the pseudo-random numbers.

In another embodiment, the one or more of the plurality of signal paths each include a respective input of the cryptographic processing block. The respective adjustable delay circuits are coupled to the respective inputs of the cryptographic processing block.

In another embodiment, the spreading sequence number generator includes a ring oscillator and a linear feedback shift register circuit. The linear feedback shift register circuit has an input coupled to an output of the ring oscillator and an input coupled to the output of the spreading sequence number generator.

In another embodiment, the ring oscillator is configured to oscillate at a first frequency and the linear feedback shift register are driven by a clock having a second frequency different from the first frequency.

In another embodiment, the delay control circuit is configured to adjust each of the adjustable delay circuits by a respective delay value. The respective delay values are selected from a lookup table according to the pseudo-random number.

In another embodiment, a method is provided for resisting power analysis during configuration of a programmable integrated circuit (IC). An encrypted bitstream is input to the programmable IC. The encrypted bitstream is decrypted with a decryption circuit. Configuration memory of the programmable IC is programmed with the decrypted bitstream. Concurrently with the decrypting of the encrypted bitstream, respective delays on one or more signal paths of the decryption circuit are adjusted to produce power fluctuations that are resistant to power analysis.

In another embodiment, respective delays on one or more signal paths are adjusted by generating a pseudo-random spreading sequence and adjusting respective delays on one or more signal paths based on the pseudo-random spreading sequence.

In another embodiment, the one or more signal paths includes at least a first signal path and a second signal path. Respective delays on one or more signal paths are adjusted by: setting the delay of the first signal path to a first delay value; and setting the delay of the second signal path to a second delay value.

In another embodiment, the one or more signal paths includes at least a first signal path and a second signal path. Respective delays on one or more signal paths are adjusted to set the respective delays of the one or more signal paths to a common delay value.

In another embodiment, the one or more signal paths are critical signal paths.

In another embodiment, the pseudo-random spreading sequence is a truly random spreading sequence.

In yet another embodiment, a method is provided for resisting power analysis during decryption of data in an integrated circuit. Encrypted data is input to the integrated circuit and decrypted. Concurrently with the decrypting of the encrypted data, respective delays on one or more signal paths of the integrated circuit are adjusted to produce power fluctuations that are resistant to power analysis.

In another embodiment, respective delays on one or more signal paths are adjusted by generating a pseudo-random spreading sequence and adjusting the respective delays on one or more signal paths based on the pseudo-random spreading sequence.

In another embodiment, the one or more signal paths includes at least a first signal path and a second signal path. The adjusting respective delays on one or more signal paths includes setting the delay of the first signal path to a first delay value and setting the delay of the second signal path to a second delay value.

In another embodiment, the one or more signal paths includes at least a first signal path and a second signal path. The adjustment of respective delays on one or more signal paths sets the respective delays of the one or more signal paths to a common delay value.

In another embodiment, the one or more signal paths are critical signal paths.

In another embodiment, noise is generated on a power supply line of the integrated circuit concurrently with the decrypting of the encrypted data.

In another embodiment, the adjustment of respective delays on one or more signal paths based on the pseudo-random spreading sequence includes

adjusting resistances of the one or more signal paths based on the pseudo-random spreading sequence included.

In yet another embodiment, the adjustment of respective delays on one or more signal paths based on the pseudo-random spreading sequence includes adjusting capacitances of the one or more signal paths based on the pseudo-random spreading sequence included.

In another embodiment, the integrated circuit comprises a programmable integrated circuit; the encrypted data comprises an encrypted bitstream for configuring the programmable integrated circuit; and decrypting the encrypted data generates a decrypted bitstream for configuring the programmable integrated circuit. The method may further comprise programming configuration memory of the programmable integrated circuit with the decrypted bitstream.

It will be appreciated that various other embodiments are set forth in the Detailed Description and Claims which follow.

BRIEF DESCRIPTION OF THE DRAWINGS

Various aspects and advantages of the invention will become apparent upon review of the following detailed description and upon reference to the drawings, in which:

FIG. 1 shows a flowchart of an example process for configuration of programmable logic;

FIG. 2 shows a block diagram of an example circuit for encryption/decryption;

FIG. 3 shows a block diagram of an example random number generator that may be used to implement encryption and decryption circuits; and

FIG. 4 illustrates a block diagram of an example programmable integrated circuit for implementing cryptographic operations.

DETAILED DESCRIPTION

During configuration of programmable logic, the configuration bitstream data can be intercepted and used to make unauthorized copies of the design. Although the configuration bitstream can be encrypted, the decryption key is vulnerable to discovery through power analysis. In a power analysis attack, current used by a device is monitored over time. During normal operation, the

amount of power used by a device varies depending on the logic gates activated at a given time. By monitoring variations in the power consumption during decryption, the attacker can identify operations that are performed and determine the decryption key. The present invention provides countermeasures that may be implemented with software or hardware to improve resistance to power analysis attacks.

In a simple power analysis (SPA) attack, current used by a device is monitored over time. During normal operation, the amount of power used by a device varies depending on the logic gates activated at a given time. By monitoring variations in the power consumption, the attacker can identify different operations that are performed. For example, if a programmable IC implements DES encryption, sixteen rounds of encryption/decryption are performed on each block of data. Because similar operations are performed for each round, a power consumption data can be identified for each round. Comparison of power consumption of different rounds can identify key dependent operations and, ultimately, the key used for decryption. For example, the DES key schedule is produced by rotating 28-bit key registers. The rotations are generally implemented using a right shift operation where a zero is shifted into the most significant bit by default. If the bit of the key shifted out of the register is a one, an additional operation is needed to cause the most significant bit to be equal to one. Therefore, a different power signature will be produced for each rotation depending on the bit of the decryption key. As used herein, a power signature may be referred to as power fluctuations, a power consumption signature, or a power consumption waveform, and such terms are used interchangeably herein. Other encryption ciphers, including both symmetric and asymmetric ciphers, also include key dependent operations that are susceptible to power analysis.

Random noise may be generated and added to modulate a power consumption waveform and conceal key dependent processes. However, even when the magnitude of the variations in power consumption are small in comparison to other power signals or noise, power variations of each operation can be detected and isolated using frequency filters and statistical analysis. This is known as differential power analysis (DPA). In DPA, a large number of samples are gathered by repeating encryption over a number of cycles.

Samples gathered from each cycle are compared and analyzed to identify a common power signature among the repeated cycles from which the decryption can be identified. For example, added noise can be negated through statistical averaging. When random noise is evenly distributed, the noise will have little effect on the average of power consumption data from repeated rounds of decryption.

The embodiments of the present invention provide a method and circuit in which timing is adjusted on a pseudo-random basis. The timing adjustment increases the complexity of statistical analysis because power consumption waveforms compared from different encryption rounds may not be aligned in the time domain. When waveforms are not aligned, more advanced algorithms and/or larger data samples are needed by an attacker to identify similarities in various rounds of repeated decryption. The embodiments of the present invention may be used alone or in combination with other DPA mitigation techniques such as random noise generation, signal to noise reduction, or clock skipping.

In one embodiment of the present invention, a pseudo-random spreading sequence is generated and is used to adjust one or more adjustable delays included in encryption/decryption circuitry. By adjusting the delays, different logical portions of the encryption/decryption circuitry will be triggered at slightly different times. Because different logical portions are triggered at different times, transistors will not change state in a uniform consistent fashion. Rather, the transistors will switch on or off according to the programmed delay. Although the amount of delay is not enough to affect the logical functions of the circuit, the adjustment has a significant effect on DPA. When transistors are synchronized to switch on at substantially the same time, a large peak is created in the power consumption waveform. By distributing variation in the time in which transistor switching occurs, peaks of the power consumption waveform are smoothed and widened. In this manner, it becomes more difficult to identify or distinguish different cryptographic operations using DPA.

FIG. 1 shows a flowchart of an example process for configuration of programmable logic. An encrypted configuration bitstream 102 is received by a programmable IC. Each frame (step 104) of the encrypted configuration bitstream is decrypted at step 110. In this example, AES decryption is

implemented. In AES, the decryption process 120 is repeated for fourteen rounds (step 112) for each frame of the encrypted bitstream, assuming a 256-bit key is used. When decryption of a frame has completed, configuration memory of the programmable IC is programmed with the decrypted frame at step 122. The process is repeated at decision step 124 until all frames have been decrypted. During decryption, adjustable delay elements are set to delay input signal lines to the decryption block. The adjustable delay elements are controlled based on a pseudo-random spreading sequence. In each round, a pseudo-random spreading sequence is generated at step 114. A delay value for each of the adjustable delays is determined from the pseudo-random number at step 116. Input signal lines are delayed at step 118. Because some signal lines are delayed, different portions of the decryption logic will become active at slightly different times.

The delay is selected such that timing is varied within an operable tolerance. For example, if a system control clock cycle of the circuit is selected to be 100 nanoseconds, a delay adjustment of +-10 nanoseconds is not likely to affect correct operation because all transistors can switch before the falling edge of the system control clock.

One skilled in the art will recognize that the described embodiments are applicable to a number of other synchronous encryption algorithms such as DES, DES-3, Blowfish, etc; as well as asynchronous encryption algorithms such as RSA, DSA, etc.

While DPA of the resulting power consumption waveform is difficult, the power consumption waveform can be easily modulated through timing adjustment with little additional hardware or processing. In one embodiment, a circuit is provided for DPA resistant encryption and decryption. FIG. 2 shows a block diagram of a circuit for encryption/decryption. Circuit 200 includes a cryptographic processing circuit 208 for encrypting/decrypting data. In this example, the cryptographic processing circuit 208 includes a number of signal inputs 210 for receiving data blocks and sub-keys. The circuit includes a number of adjustable delay elements 206 coupled to receive signals from inputs 210, and output the data values to the cryptographic processing circuit 208 after a particular delay has passed. The amount of time by which a signal is delayed by an adjustable delay circuit 206 is controlled by delay controller 204. The delay

controller 204 acts with spreading sequence generator 202, to randomize delay times. The delay controller 204 uses a spreading sequence output from the spreading sequence generator 202 to determine a respective delay value for each adjustable delay 206. In some embodiments, the spreading sequence generator may be implemented using a random or pseudo-random number generator to output pseudo-random numbers that will be used as the spreading sequence.

The delay controller 204 may determine a delay value in a number of different ways. In one example implementation, a delay value may be taken directly from one or more bits of the output of the spreading sequence generator. In another example implementation, one or more bits of the output of the spreading sequence generator may be used to select a delay value from a table of delay values. In yet another example implementation, one or more bits of the output of the spreading sequence generator may be used to select adjustable delays that are to be delays in a given clock cycle. One skilled in the art will recognize that other algorithms or techniques may also be used to control the amount of delay.

A number of different circuits may be used to implement the adjustable delay circuits. Propagation delay of each signal line can be influenced by capacitance, resistance or inductance of the signal path circuit. The adjustable delay may include a switchable circuit to adjust the rise and fall of signals based on one or more of these factors. The adjustable delay may also be implemented using one or more switchable buffers, such as an inverter. For example, the delay may be increased by enabling a number of buffers in the signal path. The delay may be decreased by bypassing or disabling one or more of the buffers. One skilled in art will recognize that numerous other circuits may be used to insert delay into signal lines as well.

FIG. 3 shows a block diagram of an example random number generator that may be used to generate a spreading sequence. The random number generator 300 includes a ring oscillator circuit 301, a sampling circuit 303, and a linear feedback shift register (LFSR) circuit 321. The ring oscillator circuit 301 consists of XOR gates 302_1 through 302_N (collectively referred to as XOR gates 302). The XOR gates 302 are interconnected to form a "generalized N-bit ring oscillator" which operates at a first frequency dictated by the operating delay of

the implementing circuit. Each one of the XOR-based ring oscillators is connected with its two neighbors (the boundary gates are considered neighbors), thereby creating a ring of oscillators. The ring oscillator circuit 301 is coupled to the sampling circuit 303. The output data terminals of the sampling circuit 303 are coupled to input data terminals of the LFSR 321. The LFSR 321 operates synchronously using a clock signal coupled to the sampling circuit 303. The clock signal operates at a different frequency than the ring oscillator. The LFSR 321 scrambles the output of the sampling circuit 303 to produce high-quality random numbers. The LFSR 321 comprises a set of XOR gates 322_1 through 322_N (collectively referred to as XOR gates 322) and a set of storage cells 324_1 through 324_N. In one embodiment, each of the storage cells comprises a D-type flip-flop (collectively referred to as flip-flops 324). The XOR gates 322 and the flip-flops 324 implement an N-cell LFSR. Because the LFSR 321 operates at a different frequency than the ring oscillator 301, truly random N-bit binary numbers have a uniform probability distribution using only digital logic. The operation of this and other random number generators is described in detail in U.S. Patent 7,389,316. Those skilled in the art will recognize that other random or pseudo-random number generators, implemented in hardware or in software, may be used to generate random numbers in the described embodiments.

FIG. 4 is a block diagram of an example field programmable gate array (FPGA) which is configurable. FPGAs can include several different types of programmable logic blocks in the array. For example, FIG. 4 illustrates an FPGA architecture (400) that includes a large number of different programmable tiles including multi-gigabit transceivers (MGTs 401), configurable logic blocks (CLBs 402), random access memory blocks (BRAMs 403), input/output blocks (IOBs 404), configuration and clocking logic (CONFIG/CLOCKS 405), digital signal processing blocks (DSPs 406), specialized input/output blocks (I/O 407), for example, clock ports, and other programmable logic 408 such as digital clock managers, analog-to-digital converters, system monitoring logic, and so forth. Some FPGAs also include dedicated processor blocks (PROC 410).

In some FPGAs, each programmable tile includes a programmable interconnect element (INT 411) having standardized connections to and from a corresponding interconnect element in each adjacent tile. Therefore, the programmable interconnect elements taken together implement the

programmable interconnect structure for the illustrated FPGA. The programmable interconnect element INT 411 also includes the connections to and from the programmable logic element within the same tile, as shown by the examples included at the top of FIG. 4.

For example, a CLB 402 can include a configurable logic element CLE 412 that can be programmed to implement user logic plus a single programmable interconnect element INT 411. A BRAM 403 can include a BRAM logic element (BRL 413) in addition to one or more programmable interconnect elements. Typically, the number of interconnect elements included in a tile depends on the height of the tile. In the pictured embodiment, a BRAM tile has the same height as four CLBs, but other numbers (e.g., five) can also be used. A DSP tile 406 can include a DSP logic element (DSPL 414) in addition to an appropriate number of programmable interconnect elements. An IOB 404 can include, for example, two instances of an input/output logic element (IOL 415) in addition to one instance of the programmable interconnect element INT 411. As will be clear to those of skill in the art, the actual I/O pads connected, for example, to the I/O logic element 415 are manufactured using metal layered above the various illustrated logic blocks, and typically are not confined to the area of the input/output logic element 415.

In the pictured embodiment, a columnar area near the center of the die (shown shaded in FIG. 4) is used for configuration, clock, and other control logic. Horizontal areas 409 extending from this column are used to distribute the clocks and configuration signals across the breadth of the FPGA.

Some FPGAs utilizing the architecture illustrated in FIG. 4 include additional logic blocks that disrupt the regular columnar structure making up a large part of the FPGA. The additional logic blocks can be programmable blocks and/or dedicated logic. For example, the processor block PROC 410 shown in FIG. 4 spans several columns of CLBs and BRAMs.

Note that FIG. 4 is intended to illustrate only an exemplary FPGA architecture. The numbers of logic blocks in a column, the relative widths of the columns, the number and order of columns, the types of logic blocks included in the columns, the relative sizes of the logic blocks, and the interconnect/logic implementations included at the top of FIG. 4 are purely exemplary. For example, in an actual FPGA more than one adjacent column of CLBs is typically

included wherever the CLBs appear, to facilitate the efficient implementation of user logic.

The present invention is thought to be applicable to a variety of systems for encryption and decryption. Other aspects and embodiments of the present invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and illustrated embodiments be considered as examples only, with a true scope and spirit of the invention being indicated by the following claims.

CLAIMS

What is claimed is:

1. A secure cryptographic circuit arrangement, comprising:

a cryptographic processing block having a plurality of signal paths, one or more of the plurality of signal paths including respective adjustable delay circuits;

a spreading sequence generator configured to output a sequence of pseudo-random numbers;

a delay control circuit having an input coupled to an output of the spreading sequence number generator and one or more outputs coupled to respective delay adjustment inputs of the adjustable delay circuits; and

wherein the delay control circuit is configured to adjust the adjustable delay circuits based on the pseudo-random numbers.

2. The secure cryptographic circuit arrangement of claim 1, wherein the delay control circuit is configured to adjust each of the adjustable delay circuits based on different bits of the pseudo-random numbers.

3. The secure cryptographic circuit arrangement of claim 1 or claim 2, wherein:

the one or more of the plurality of signal paths each include a respective input of the cryptographic processing block; and

the respective adjustable delay circuits are coupled to the respective inputs of the cryptographic processing block.

4. The secure cryptographic device of any of claims 1-3, wherein the spreading sequence number generator includes:

a ring oscillator; and

a linear feedback shift register circuit, having an input coupled to an output of the ring oscillator and an input coupled to the output of the spreading sequence number generator.

5. The secure cryptographic circuit arrangement of claim 4, wherein the ring oscillator is configured to oscillate at a first frequency and the linear feedback shift register is driven by a clock having a second frequency different from the first frequency.

6. The secure cryptographic circuit arrangement of any of claims 1-5, wherein:

the delay control circuit is configured to adjust each of the adjustable delay circuits by a respective delay value; and

the respective delay values are selected from a lookup table according to the pseudo-random number.

7. A method for resisting power analysis during decryption of data in an integrated circuit, comprising:

inputting encrypted data to the integrated circuit;

decrypting the encrypted data; and

concurrently with the decrypting of the encrypted data, adjusting respective delays on one or more signal paths of the integrated circuit to produce power fluctuations that are resistant to power analysis.

8. The method of claim 7, wherein the adjusting respective delays on one or more signal paths includes:

generating a pseudo-random spreading sequence; and

adjusting respective delays on one or more signal paths based on the pseudo-random spreading sequence.

9. The method of claim 7 or claim 8, wherein:

the one or more signal paths includes at least a first signal path and a second signal path; and

adjusting respective delays on one or more signal paths includes:

setting the delay of the first signal path to a first delay value; and

setting the delay of the second signal path to a second delay value.

10. The method of claim 7 or claim 8, wherein:

the one or more signal paths includes at least a first signal path and a second signal path; and

adjusting respective delays on one or more signal paths sets the respective delays of the one or more signal paths to a common delay value.

11. The method of any of claims 7-10, wherein the one or more signal paths are critical signal paths.

12. The method of any of claims 7-11, further comprising:

generating noise on a power supply line of the integrated circuit concurrently with the decrypting of the encrypted data.

13. The method of any of claims 8-12, wherein adjusting respective delays on one or more signal paths based on the pseudo-random spreading sequence includes adjusting resistances of the one or more signal paths based on the pseudo-random spreading sequence included.

14. The method of any of claims 8-13, wherein adjusting respective delays on one or more signal paths based on the pseudo-random spreading sequence includes adjusting capacitances of the one or more signal paths based on the pseudo-random spreading sequence included.

15. The method of any of claims 7-14, wherein:

the integrated circuit comprises a programmable integrated circuit;

the encrypted data comprises an encrypted bitstream for configuring the programmable integrated circuit;

decrypting the encrypted data generates a decrypted bitstream for configuring the programmable integrated circuit; and

the method further comprises programming configuration memory of the programmable integrated circuit with the decrypted bitstream.

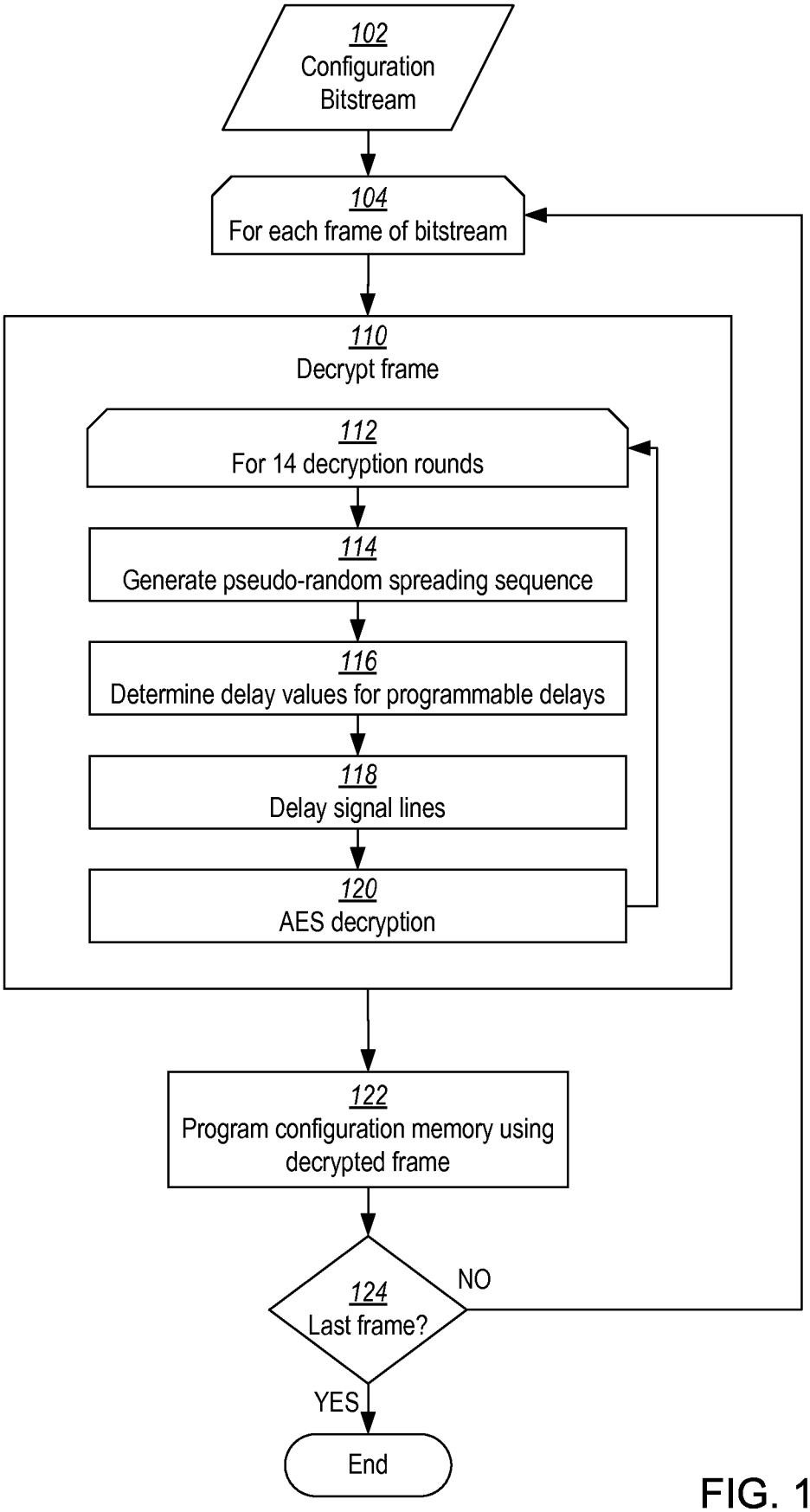
102
Configuration Bitstream
104
For each frame of bitstream
110
Decrypt frame
112
For 14 decryption rounds
114
Generate pseudo-random spreading sequence
116
Determine delay values for programmable delays
118
Delay signal lines
120
AES decryption
122
Program configuration memory using decrypted frame
124
Last frame?
NO
YES
End

FIG. 1

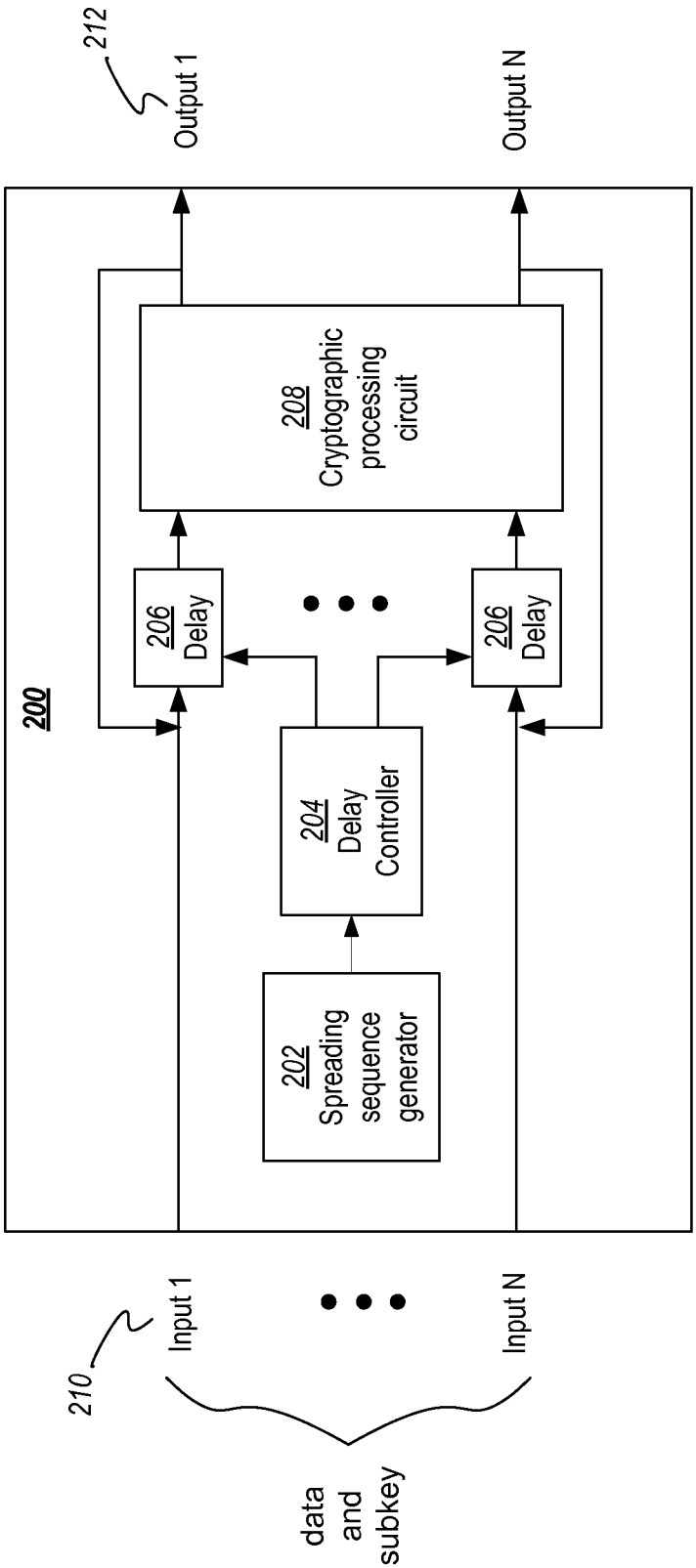
212
Output 1
Output N
208
Cryptographic processing circuit
206
Delay
206
Delay
200
204
Delay Controller
202
Spreading sequence generator
210
Input 1
Input N
data and subkey

FIG. 2

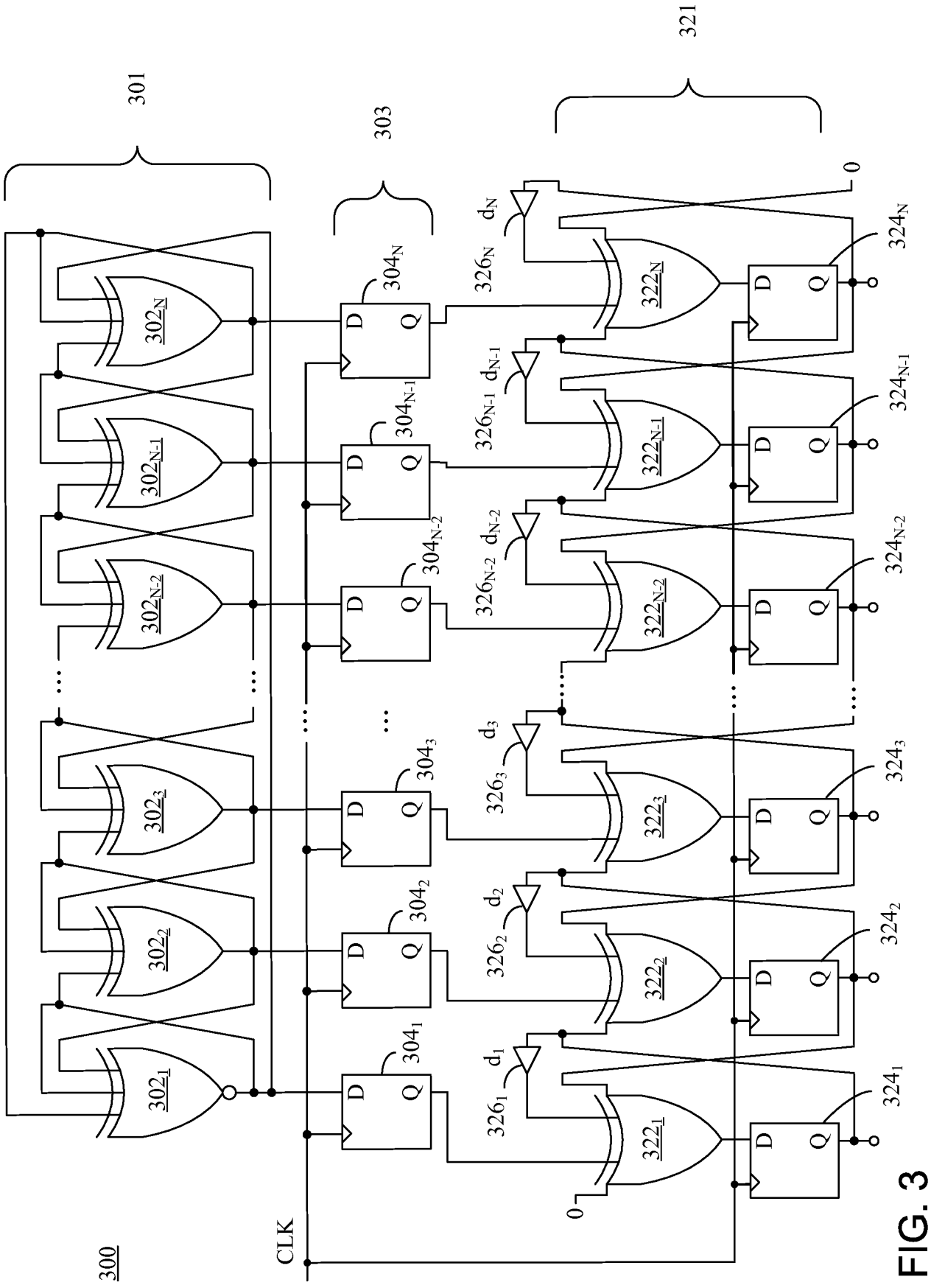
300
301
303
321
CLK
0
0
302_1
302_2
302_3
302_{N-2}
302_{N-1}
302_N
304_1
304_2
304_3
304_{N-2}
304_{N-1}
304_N
322_1
322_2
322_3
322_{N-2}
322_{N-1}
322_N
324_1
324_2
324_3
324_{N-2}
324_{N-1}
324_N
326_1 d_1
326_2 d_2
326_3 d_3
326_{N-2} d_{N-2}
326_{N-1} d_{N-1}
326_N d_N
D
Q

FIG. 3

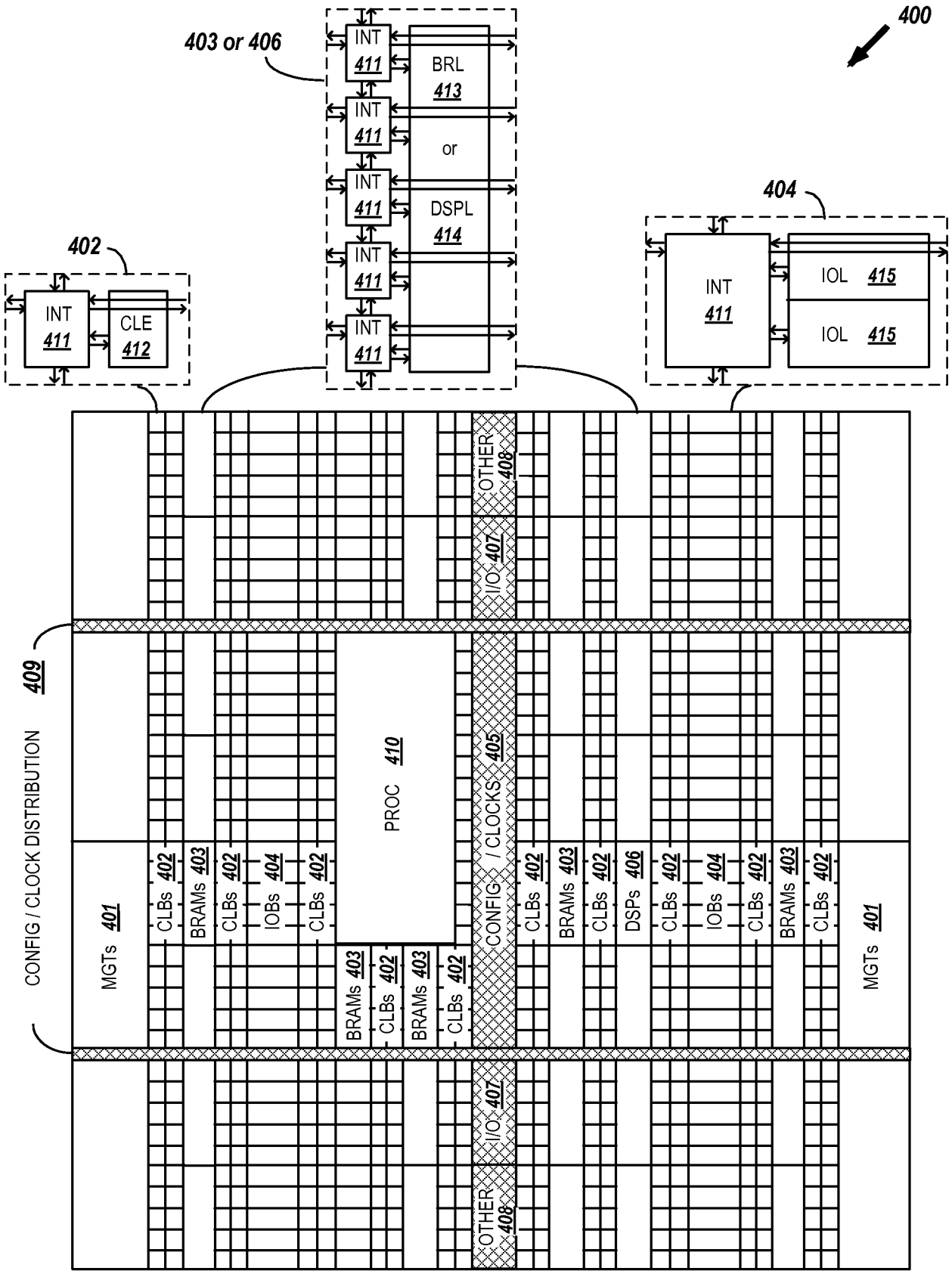
400
403 or 406
INT 411
BRL 413
or
DSPL 414
402
INT 411
CLE 412
404
INT 411
IOL 415
IOL 415
OTHER 408
I/O 407
409
CONFIG / CLOCK DISTRIBUTION
MGTs 401
CLBs 402
BRAMs 403
IOBs 404
PROC 410
CONFIG / CLOCKS 405
DSPs 406
OTHER 408
I/O 407
MGTs 401

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/021412

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
ADD.

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)
G06F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	YINGXI LU ET AL: "FPGA implementation and analysis of random delay insertion countermeasure against DPA", FIELD-PROGRAMMABLE TECHNOLOGY, 2008. FPT 2008. INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 8 December 2008 (2008-12-08), pages 201-208, XP031412827, ISBN: 978-1-4244-3783-2 abstract Section 1 Section 2 Section 3 Section 6 figures 5,6a,7 ----- -/--	1-15

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

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 April 2011	10/05/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Schäfer, Andreas

6

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BUCCI M ET AL: "A Countermeasure against Differential Power Analysis based on Random Delay Insertion", CONFERENCE PROCEEDINGS / IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS (ISCAS) : MAY 23 - 26, 2005, INTERNATIONAL CONFERENCE CENTER, KOBE, JAPAN, IEEE SERVICE CENTER, PISCATAWAY, NJ, 23 May 2005 (2005-05-23), pages 3547-3550, XP010816291, DOI: DOI:10.1109/ISCAS.2005.1465395 ISBN: 978-0-7803-8834-5 abstract Section I Section II Section III figures 2,5,6	1-15

A	DRIES SCHELLEKENS ET AL: "FPGA Vendor Agnostic True Random Number Generator", FIELD PROGRAMMABLE LOGIC AND APPLICATIONS, 2006. FPL '06. INTERNA TIONAL CONFERENCE ON, IEEE, PI, 1 August 2006 (2006-08-01), pages 1-6, XP031047635, ISBN: 978-1-4244-0312-7 figures 2,3	4

A	JOVAN DJ GOLI: "New Methods for Digital Generation and Postprocessing of Random Data", IEEE TRANSACTIONS ON COMPUTERS, IEEE SERVICE CENTER, LOS ALAMITOS, CA, US, vol. 55, no. 10, 1 October 2006 (2006-10-01), pages 1217-1229, XP007918403, ISSN: 0018-9340 [retrieved on 2006-08-22] figure 7 Section 5	5
