CLAIMS

1. A data processing device comprising:

a first circuitry component configured to send a challenge to one or more remaining circuitry components, wherein

each of the one or more remaining circuitry components is configured to receive a respective challenge and to process the challenge to produce a response;

the first circuitry component is configured to verify integrity of the data processing device based on one or more responses produced by the one or more remaining circuitry components;

each of the one or more remaining circuitry components comprises:

an instruction shift register to receive an instruction of a set of instructions, the set of instructions including at least a process challenge instruction to process a challenge and produce a response; and

a data shift register, corresponding to the process challenge instruction, to receive a challenge; and

each of the one or more remaining circuitry components is configured to, in a first mode, shift one bit at a time from its input into the instruction shift register and one bit at a time from the instruction shift register to its output.

2. The data processing device of claim 1, further comprising a memory storing mission critical information in encrypted form; and

wherein the data processing device or an aspect of the data processing device requires the mission critical information in decrypted form to function, and

wherein the first circuitry component is configured to decrypt the encrypted mission critical information using one or more device verification keys based on the one or more responses produced by the one or more remaining circuitry components.

3. The data processing device of claim 2, wherein the mission critical information comprises at least one or more of software, firmware for the data processing device or an aspect of the data processing device to function, a BIOS, an operating system kernel, a circuitry component driver, a boot loader, and a content decryption key.

4. The data processing device of claim 2, further comprising a conditional access device,

wherein the mission critical information comprises a decryption key for use by the conditional access device to control access to content consumable using the data processing device.

5. The data processing device of claim 1, wherein

an initial remaining circuitry component is configured to receive its challenge from the first circuitry component;

the challenge received by each subsequent remaining circuitry component is the response produced by a respective preceding remaining circuitry component;

a last remaining circuitry component is configured to send its response to the first circuitry component; and

the first circuitry component is configured to verify the integrity of the data processing device using the response received from the last one of the remaining circuitry components.

6. The data processing device of claim 5, wherein each of the one or more remaining circuitry components is configured to apply a non-transitive function to its challenge to produce its response.

7. The data processing device of claim 1,

wherein the one or more remaining circuitry components are connected in a chain with:

an input of an initial remaining circuitry component in the chain connected to an output of the first circuitry component,

an input of each subsequent remaining circuitry component in the chain connected to an output of a respective preceding remaining circuitry component in the chain, and

an input of the first circuitry component connected to an output of a last one of the remaining circuitry components in the chain; and

wherein the first circuitry component is configured to:

send a challenge to the input of the initial remaining circuitry component in the chain; and

receive one or more of the responses produced by the one or more remaining circuitry components at the input of the first circuitry component.

8. The data processing device of claim 7,

wherein each of the one or more remaining circuitry components is configured to:

in a second mode, shift one bit at a time from its input into the data shift register and one bit at a time from the data shift register to its output; and

in a third mode, when a process challenge instruction is in in the instruction shift register, read the challenge in the data shift register, process the challenge to produce a response and write the response to the data shift register;

wherein the first circuitry component is configured to control the mode of the one or more remaining circuitry components to:

shift respective instructions into the instruction shift registers;

shift challenges into the data shift registers;

cause the one or more remaining circuitry components to process the challenges to produce responses; and

shift responses out of the data shift registers, thereby receiving one or more responses from the one or more remaining circuitry components; and

wherein the first circuitry component is configured to control the mode of all remaining circuitry components together over a mode control line common to all remaining circuitry components.

9. The data processing device of claim 8, wherein the first circuitry component is configured to cause:

a challenge to be shifted bit by bit into the data shift register of the initial remaining circuitry component;

the initial remaining circuitry component to process the challenge and write its response to its data shift register;

the response from the data shift register of the respective preceding circuitry component in the chain to be shifted bit by bit into the data shift register of each subsequent remaining circuitry component in the chain;

each subsequent circuitry component to process the response from the respective preceding circuitry component in its data shift register as its challenge to write its response to the data shift register; and

the response written to the respective data shift register of the last remaining circuitry component in the chain to be shifted bit by bit to the input of the first circuitry component.

10. The data processing device of claim 9, wherein the first circuitry component is configured to cause a process challenge instruction to be executed by each subsequent

remaining circuitry component in the chain not before the respective preceding circuitry component in the chain has been caused to write its response to its data register.

11. The data processing device of claim 9, wherein the first circuitry component is configured to cause each of the one or more remaining circuitry components in the chain to only execute a process challenge instruction once between shifting the challenge into the data shift register of the initial remaining circuitry component in the chain and shifting the response written to the data shift register of the last remaining circuitry component in the chain to the input of the first circuitry component.

12. The data processing device of claim 1, wherein a physical layer is used for implementing communications between initial and remaining circuitry components and between remaining circuitry components is compliant with the IEEE-1149.1 Joint Test Action Group (JTAG) specification, each remaining circuitry component comprising a Test Mode Select (TMS), Test Clock (TCK), Test Data In (TDI) and Test Data Out (TDO) pin and a specification compliant state machine.

13. A method of verifying integrity of a data processing device having a plurality of circuitry components each comprising an instruction shift register to receive an instruction of a set of instructions, the set of instructions including at least a process challenge instruction to process a challenge and produce a response, and a data shift register, corresponding to the process challenge instruction, to receive a challenge, the method comprising:

sending one or more challenges to the plurality of circuitry components;

shifting, in a first mode, by each of the plurality of circuitry components, one bit at a time from its input into the instruction shift register and one bit at a time from the instruction shift register to its output;

receiving a response from the plurality of circuitry components; and

using the response to verify the integrity of the data processing device.

14. The method of claim 13, wherein receiving the response comprises receiving a response from one of the plurality of circuitry components, the response from the one of the plurality of circuitry components depending on the respective responses form the other of the plurality of circuitry components,

wherein the plurality of circuitry components provide respective responses in a sequence, a subsequent circuitry component in the sequence receiving the response of a

previous circuitry component in the sequence as a challenge and producing a response responsive to the received challenge, and

wherein the response responsive to the received challenge is produced as a non-transitive function of the received challenge.

15. The method of claim 13, further comprising using the response of the plurality of circuitry components to decrypt information that is required in decrypted form for operation of the data processing device or an aspect of the data processing device.

16. A non-transitory computer readable medium comprising instructions that when executed by a processing device having a plurality of circuitry components each comprising an instruction shift register to receive an instruction of a set of instructions, the set of instructions including at least a process challenge instruction to process a challenge and produce a response, and a data shift register, corresponding to the process challenge instruction, to receive a challenge, cause the processing device to:

send one or more challenges to the plurality of circuitry components;

shift, in a first mode, by each of the plurality of circuitry components, one bit at a time from its input into the instruction shift register and one bit at a time from the instruction shift register to its output;

receive a response from the plurality of circuitry components; and

use the response to verify the integrity of the processing device.

17. The non-transitory computer readable medium of claim 16,

wherein to receive the response comprises receiving a response from one of the plurality of circuitry components, the response from the one of the plurality of circuitry components depending on the respective responses from the other of the plurality of circuitry components,

wherein the plurality of circuitry components provide respective responses in a sequence, a subsequent circuitry component in the sequence receiving the response of a previous circuitry component in the sequence as a challenge and producing a response responsive to the received challenge, and

wherein the response responsive to the received challenge is produced as a non-transitive function of the received challenge.

18. The non-transitory computer readable medium of claim 16, wherein to use the response comprises using the response of the plurality of circuitry components to decrypt

information that is required in decrypted form for operation of the processing device or an aspect of the processing device.

19. The data processing device of claim 1,

wherein each of the one or more remaining circuitry components is configured to:

in a second mode, shift one bit at a time from its input into the data shift register and one bit at a time from the data shift register to its output; and

in a third mode, when a process challenge instruction is in in the instruction shift register, read the challenge in the data shift register, process the challenge to produce a response and write the response to the data shift register.

20. The data processing device of claim 19,

wherein the first circuitry component is configured to control the mode of the one or more remaining circuitry components to:

shift respective instructions into the instruction shift registers;

shift challenges into the data shift registers;

cause the one or more remaining circuitry components to process the challenges to produce responses; and

shift responses out of the data shift registers, thereby receiving one or more responses from the one or more remaining circuitry components; and

wherein the first circuitry component is configured to control the mode of all remaining circuitry components together over a mode control line common to all remaining circuitry components.