CLAIMS

1. A device comprising:

a PUF module comprising a physically unclonable function, PUF, and internal PUF interface logic arranged to receive an input challenge and output an output response being a deterministic function of the input challenge, the deterministic function comprising the PUF; and

one or more outer layer components providing at least part of an unsecured channel for inputting the input challenge to the internal interface logic of the PUF module and receiving back the output response output by the internal interface logic;

wherein at least one of the outer layer components is susceptible to manipulation of the input challenge and/or output response by a malicious process, but the PUF module, including the internal PUF interface logic, is encapsulated within a housing of the device and separated from the one or more outer layer components, and is thus protected from manipulation by the malicious process; and

wherein the internal PUF interface logic comprises a logging mechanism arranged to automatically log a record of the input challenge and/or output response in a log medium.

2. The device of claim 1, wherein the internal interface logic is implemented partially or wholly in firmware run on a processor of the device~~.~~

~~3. The device of claim 2~~, wherein the firmware is stored partially or wholly in read only memory, ROM~~.~~

~~4. The device of claim 1 or 2, wherein the firmware is implemented partially or wholly in~~, or a secure kernel.

~~5~~3. The device of any preceding claim, wherein the internal interface logic is implemented in fixed-function hardware circuitry.

~~6~~4. The device of any preceding claim, wherein the at least one outer layer component comprises an external interface for receiving the input challenge from a source external to

the device and/or supplying the output response to a destination external to the device, the malicious process to which the at least one outer layer component is susceptible comprising interception and manipulation of the input challenge and/or output response between the source and the external interface.

~~7. The device of claim 6, wherein the source is local to the device, the external interface being operable to receive the input challenge without transmission over a network.~~

~~8. The device of claim 6, wherein the source is remote from the device, the external interface being operable to receive the input challenge from the source via a network.~~

~~9~~5. The device of ~~any of~~ claim~~s 6 to 8~~4, wherein the device comprises a dedicated PUF device.

~~10~~6. The device of any of claims 1 to ~~8~~4, wherein the at least one outer layer component comprises an application running on a processor within the housing of the device, wherein the application is configured to generate the input challenge, the malicious process to which the at least one outer layer component is susceptible comprising malware being run on the same processor as the application to manipulate the input challenge.

~~11~~7. The device of claim ~~10~~6, wherein the internal interface logic is arranged to run on either:

- a separate processor than the application~~.~~; or

~~12. The device of claim 10, wherein the internal interface logic is arranged to run on~~ - the same processor as the application but in a privileged domain of a secure processor, whereas the application runs in an application domain.

~~13~~8. The device of ~~any of~~ claim~~s 10 to 12~~6 or 7, wherein the device comprises an event data recorder, EDR, and the application comprises an EDR application.

~~14~~9. The device of claim ~~13~~8, wherein the application is configured to generate a result of a system which the EDR is configured to monitor, and the EDR is configured to record the result and a tag mapping the output response to the result.

~~15~~10. The device of claim ~~14~~9, wherein the tag comprises: a cryptographic signature generated by signing the result with the output response; or a hash-based message authentication code, HMAC, generated as a function of the result and the output response.

~~16~~11. The device of claim ~~14~~9 or ~~15~~10, wherein the input challenge comprises meaningful data used by the application, representing a state of the system being monitored.

~~17~~12. The device of claim ~~16~~11, wherein the result is dependent on said data.

~~18~~13. The device of any of claims ~~13~~8 to ~~17~~12, wherein the EDR is an EDR for a vehicle, the system which the EDR is configured to monitor comprising a system of the vehicle.

~~19~~14. The device of any preceding claim, wherein the one or more outer layer components are implemented in the same housing as the PUF module.

~~20. The device of any preceding claim, wherein the PUF module comprises an expanded PUF module whereby the input challenge is a secondary challenge and the output response is a secondary response; and the internal PUF interface logic is configured to input a challenge into the PUF to generate a primary response, and determine the secondary response as a deterministic transform of the primary response and the secondary challenge.~~

~~21. The device of claim 20, wherein the deterministic transform comprises a hash function.~~

~~22. The device of any of claims 1 to 19, wherein the interface logic is configured to input the input challenge directly to the PUF and receive the output response directly from the PUF as a function of the input response.~~

~~23~~15. The device of any preceding claim, wherein the log medium comprises a local memory of the device.

~~24~~16. The device of claim ~~23~~15, wherein said local memory is a tamperproof memory, write-once memory, and/or embedded in the interface logic.

~~25~~17. The device of any preceding claim, wherein the log medium in which the PUF interface logic is configured to log the record comprises: a publicly accessible medium external to the device.

~~26~~18. The device of claim ~~25~~17, wherein the publicly accessible medium in which the PUF interface logic is configured to log the record comprises: a blockchain.

~~27~~19. The device of any preceding claim, wherein the internal PUF interface logic is configured to perform the logging of the record in real-time in response the inputting of the individual input challenge.

~~28~~20. The device of any preceding claim, wherein the internal PUF interface logic is configured to periodically log any input challenges received and/or output responses generated during each instance of a periodic window of time.

~~29. The device of claim 28 as dependent on at least claims 23, 25 and 27, wherein the internal PUF interface logic is configured to log the record in the said local memory in real-time in response to the inputting of the individual input challenge, and also to perform the periodic logging to the publicly accessible medium.~~

~~30. The device of claim 29, wherein the logging mechanism is further configured to periodically clear the logged challenges and/or responses from the local memory once logged to the publicly accessible medium.~~

~~31~~21. The device of claim ~~25~~ 17 or any subsequent claim as dependent thereon, wherein the logging mechanism is configured to log the record to the publicly accessible medium in real-time in response to the inputting of the individual input challenge.

~~32. The device of any preceding claim, wherein the internal PUF interface logic is configured to log the record of at least the input challenge.~~

~~33. The device of any preceding claim, wherein the internal PUF interface logic is configured to log the record of at least the output response.~~

~~34~~22. The device of any preceding claim, wherein logging mechanism is configured to output the record, for the logging thereof, in a packet that further comprises a signature generated based on a cryptographic key of the logging mechanism applied to at least part of the packet comprising the record.

~~35~~23. The device of claim ~~34~~ 22 as dependent on at least claim ~~26~~18, wherein the packet comprises a blockchain transaction, the record being included in an output of the blockchain transaction and the signature being included in an input of the transaction.

~~36~~24. A method of using the device of any preceding claim, the method comprising:

after the record of the input challenge and/or output response has been logged in said log medium, inputting a candidate challenge to the device via the unsecured channel of the outer layer in order to cause the PUF module to generate a candidate response and return the candidate response to via the unsecured channel;

checking for evidence of manipulation by checking the candidate challenge against record of the original input challenge logged in the log medium, and/or by checking the candidate response against the record of the original output response logged in the log medium.

~~37. The method of claim 36, wherein said checking comprises at least: checking that the candidate challenge matches the record of an input challenge as recorded in the log medium.~~

~~38. The method of claim 36 or 37, wherein the internal PUF interface logic is further configured to log a record of the candidate response, and said checking comprises at least: checking that the logged record of the candidate response matches the candidate response as input to the device.~~

~~39. The method of any of claims 35 to 38, wherein said checking comprises at least: checking that the candidate response matches the record of the original output response as recorded in the log medium.~~

~~40. The method of any of claims 36 to 39, wherein the method is a method of using the device of claim 14 or any device claim as dependent thereon, the method comprising:~~

~~verifying that the device was the device that produced said result by verifying the tag based on the candidate result.~~

~~41. Computer equipment comprising:~~

~~memory comprising one or more memory units; and~~

~~processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any of claims 36 to 40.~~

~~42~~25. A computer program embodied on a non-transitory computer-readable medium and configured so as, when run on one or more processors, to perform the method of ~~any of~~ claim~~s 36 to 40~~24.

~~43. A computer-implemented method comprising, by a first entity:~~

~~sending a first messaging transaction to be recorded on a blockchain, the first messaging transaction comprising a first message, and respective information directing the first message to a second entity such that the second entity can identify the first message on the blockchain;~~

~~submitting a query to check that the first message has been recorded on the blockchain without manipulation; and~~

~~on condition that the first message is determined to have been recorded on the blockchain without manipulation according to said query, sending a second messaging transaction to be recorded on the blockchain, the second messaging transaction comprising a second message, and respective information directing the second message to the second entity such that the second entity can identify the first message on the blockchain.~~

~~44. The method of claim 43, wherein the first messaging transaction comprises an input pointing to an output of a first funding transaction, and the second messaging transaction comprises an input pointing to an output of a second funding transaction and no input pointing to any output of the first messaging transaction.~~

~~45. The method of claim 43 or 44, wherein:~~

~~the first and second messages are successive messages in a sequence of two or more messages, each having an associated index within the sequence, and each being sent in a respective messaging transaction by the first entity to be recorded on the blockchain, each messaging transaction comprising respective information enabling the second entity to identify the message on the blockchain;~~

~~the respective information in each message comprises a flag which is a function of: i) the associated index and ii) the first flag or a preceding flag in the sequence, a form of the function being known to each of the first and second entities; and~~

~~the method comprises an initial set-up phase in which the first and second entities agree the flag for the first message, thereby enabling them to subsequently communicate via the blockchain using said sequence of messages, based on the form of the function, the first flag and the index of each message.~~

~~46. Computer equipment comprising:~~

~~memory comprising one or more memory units; and~~

~~processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any of claims 43 to 45.~~

~~47. A computer program embodied on a non-transitory computer-readable medium and configured so as, when run on one or more processors, to perform the method of any of claims 43 to 4~~