

CLAIMS

1. A computer-implemented method comprising one or more instances of a challenge-response mapping operation, the challenge-response mapping operation comprising:

- from a submitting party, receiving challenge data comprising a secondary challenge, from among a set of multiple possible secondary challenges;
- inputting a primary challenge into a physically unclonable function, PUF, to generate a corresponding primary response;
- inputting the received secondary challenge and the generated primary response into a deterministic transform function in order to generate a secondary response, being a response to the secondary challenge, the transform function being a function of the secondary challenge and the primary response; and

— outputting response data comprising the secondary response or data derived therefrom.

2. The method of claim 1, wherein the transform function comprises a hash function.

~~3. The method of claim 2, wherein the hash function is a cryptographic hash function.~~

43. The method of claim 2 ~~or 3~~, wherein the hash function is performed on a preimage wherein the preimage comprises a combination of the received secondary challenge and the generated primary response.

~~54.~~ The method of claim 2 ~~or 3~~, wherein the hash function is performed on a preimage, wherein the preimage comprises the received secondary challenge and the hash is initialized with the generated primary response.

~~65.~~ The method of any preceding claim, wherein the PUF is capable of generating only a single challenge-response pair, consisting of said primary challenge and primary response.

~~76.~~ The method of any preceding claim, wherein the received challenge data further comprises the primary challenge, and the generation of the primary response by the PUF is based on the primary challenge as received in the challenge data.

~~87.~~ The method of any preceding claim, comprising a further challenge-response operation comprising:

- detecting receipt of a challenge comprising only the primary challenge, not a value of the secondary challenge, and in response thereto, switching to a non-expanded mode whereby the received primary challenge is input to the PUF to generate the primary response without using the transform function to generate the secondary response.

~~98.~~ The method of any preceding claim, wherein access to the challenge-response operations is restricted to only a limited set of one or more submitting parties-

~~10~~ — ~~The method of claim 9,~~ wherein the access is restricted by one or both of:

_____ - implementing access control logic in software or circuitry which restricts the access by requiring one or more credentials from the submitting party in order to grant access-, or

~~11.~~ — ~~The method of claim 9 or 10, wherein the access is restricted by~~ ___ - restricting access to a physical interface required to access the challenge-response mapping operations.

~~12.~~ — ~~The method of claim 9, 10 or 11, wherein the access is restricted by restricting access to the primary challenge.~~

~~139.~~ The method of any preceding claim, wherein the secondary response generated by at least one of the challenge-response mapping operations is generated for use as a cryptographic key or to derive a cryptographic key-

~~14.~~ — ~~The method of claim 13,~~ wherein the cryptographic key is generated for use as a key to sign a part or all of a transaction to be recorded on a blockchain.

~~15~~10. The method of any preceding claim, wherein said one or more challenge-response mapping operations comprises a plurality of the challenge-response mapping operations, at least some of which use a different respective one of the possible values of the secondary challenge to generate a different respective secondary response based on the same primary challenge and primary response, the response data output by each challenge-response mapping operation comprising the respective secondary response or data derived therefrom.

~~16~~11. The method of any preceding claim, wherein the response data output by at least one of the challenge-response mapping operations is output for use in a verification process used to enable one or more verifying parties to verify an identity of a target, the target being a target party or a device of the target party.

~~17~~12. The method of claim ~~16~~11 as dependent on claim ~~15~~10, wherein the plurality of challenge-response operations comprise a set of multiple challenge-response operations performed as part of a set-up phase of the verification process, the submitting party from which the challenge data is received during the set-up phase being a setting-up party;
 wherein in said set of multiple challenge-response mapping operations, said outputting comprises outputting the respective response data to be stored in a storage medium store in association with evidence of the identity of the target, to be made available to the one or more verifying parties for verifying an identity of the target in a verification phase of the verification process.

~~18~~13. The method of claim ~~17~~12, wherein the response data from the set of challenge-response mapping operations are output to be stored in said storage medium as a record of a set of respective challenge-response pairs, to be made available to the one or more verifying parties for verifying the identity of the target, wherein each challenge-response pair comprises a respective pair of one of the secondary challenges and the respective secondary response, and the record of each challenge-response pair comprises an indication of the respective secondary response stored in association with an indication of the respective secondary challenge.

~~19. The method of claim 18, wherein the indication of the respective secondary response of each challenge-response pair comprises an explicit value of the respective secondary response.~~

~~20~~14. The method of claim ~~18~~13, wherein the indication of the respective secondary response of each challenge-response pair comprises an attestation of the respective secondary response, the attestation comprising a transformation of the secondary response against which the secondary response can be checked but which does not disclose the secondary response.

~~21~~15. The method of claim ~~20~~14, wherein said transformation comprises a hash or double hash.

~~22. The method of any of claims 18 to 21, wherein in the record of each challenge-response pair, the indication of the respective secondary challenge comprises an explicit value of the respective secondary challenge.~~

~~23~~16. The method of any of claims ~~18~~13 to ~~21~~15, wherein the recordal in association with an indication of the secondary challenges comprises recording in association with a master challenge from which the verifying party can derive the secondary challenges.

~~24~~17. The method of claim ~~17~~12, wherein the response data output by each of the set of challenge-response mapping operations comprises a respective public key of a respective public-private key pair derived from the respective secondary response.

~~25~~18. The method of claim ~~24~~17, comprising one of:

- the target signing a message with the public key to enable the verifying party to verify the identity of the target based on the signed message and private key of the public-private key pair, or

- establishing a secure communication channel between the target party and one of the verifying parties based on the public-private key pair.

~~26~~19. The method of any of claims ~~17-12~~ to ~~25~~18, wherein the one or more verifying parties are a plurality of verifying parties, wherein the response data from different challenge-response mapping operations from amongst said set are made available to different ones of the verifying parties for verifying the target.

~~27.~~ The method of any of claims 17 to 26, wherein the setting-up party is the target party.

~~28.~~ The method of claim 27, wherein the storage medium is a storage medium of a trusted third party, and the method comprising establishing a secure communication channel between the target party and the trusted third party over a network, secured based on a shared secret shared between the target party trusted third party; wherein the method comprises using the secure channel for one or both of:

——— receiving the challenges from the trusted third party to use to generate the responses in the set-up phase; and/or

——— establishing the identity of the target party with the trusted third party.

~~29.~~ The method of any of claims 17 to 26, wherein the setting-up party is a trusted third party.

~~30.~~ The method of claim 29, wherein said storage medium is a storage medium of the trusted third party.

~~31.~~ The method of any of claims 17 to 30, wherein said storage medium is a storage medium of the verifying party.

~~32~~20. The method of any of claims ~~17-12~~ to ~~31~~19, wherein said storage medium is a public storage medium.

~~33~~21. The method of claim ~~32~~20, wherein said storage medium is a blockchain.

~~3422.~~ The method of any of claims ~~16-11~~ to ~~3321~~, wherein the one or more challenge-response mapping operations comprise at least one challenge-response mapping operation performed in a verification phase of the verification process, the submitting party from which the challenge data is received in the verification phase being one of the verifying parties who verifies that the response data generated in the verification phase matches an expectation established in a preceding set-up phase.

~~35.— The method of claim 34, wherein the verifying party is remote from the PUF, the challenge data being received, and the secondary response output back, over a network.~~

~~36.— The method of claim 35, wherein the verifying party is local to the PUF, submitting the challenge data by interacting directly with a device comprising the PUF.~~

~~37.— The method of any of claims 34 to 36, as dependent on at least claim 17, wherein one of the one or more verifying parties is the setting-up party.~~

~~38.— The method of any of claims 34 to 36, as dependent on at least claim 17, wherein the setting-up party is a trusted third party other than the target party and any of the one or more verifying parties.~~

~~3923.~~ The method of ~~any of claims 33 to 3822~~, as dependent on at least claim ~~1813~~, wherein the verification comprises checking whether the response data of one of the challenge-response pairs in the data store matches the response data as output in the verification phase, the identity of the target being verified on condition of said match.

~~40.— The method of claim 39 as dependent on at least claim 19, wherein said checking comprises comparing the value of one of the secondary responses in the data store with the secondary response as output in the verification phase.~~

~~41.— The method of claim 39, as dependent on at least claim 20, wherein said checking comprises comparing one of the attestations in the data store with a corresponding value~~

~~obtained by applying the same transformation to the secondary response output in the verification phase.~~

~~42. The method of any of claims 34 to 38, as dependent on at least claim 24, wherein the verification comprises using one of the public keys in the data store to verify a cryptographic signature applied by the target to a message using the corresponding private key of the respective public-private key pair.~~

~~43~~24. 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 preceding claim.

~~44~~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 claims 1 to ~~42~~23.