

CLAIMS

1. A computer-implemented method for enabling one or more verifying parties to verify an identity of a target comprising a target party or device of the target party; the method comprising, in a set-up phase:

storing, in a data store, a respective piece of response data for each of a set of one or more responses resulting from a setting-up party inputting a respective set of one or more challenges into a PUF module comprising a physically unclonable function, PUF, to generate the one or more responses based on the PUF; and

storing an indication of the set of challenges in the data store, wherein the indication does not comprise a value of each of the challenges in the set, but rather a master challenge from which the set of challenges is derivable by applying a derivation function to the master challenge;

thereby making at least one of the pieces of response data and the respective challenge available to the one or more verifying parties for verifying the identity of the target in a subsequent verification phase, wherein the respective piece of response data for each response comprises the respective response or data derived therefrom.

2. The method of claim 1, wherein the data store is implemented in third party computer equipment.

3. The method of claim 1 or 2, wherein the data store is a public peer-to-peer publication medium, wherein the peer-to-peer publication medium is a blockchain.

4. The method of any preceding claim, wherein the master challenge comprises identification data comprising, or derived from, one or more pieces of identification information relating to the identity of the target.

5. The method of claim 4, wherein the identification data comprises, or is generated from, a combination of a plurality of pieces of identification information of the target party.

6. The method of claim 4 or 5, wherein the method is performed by a trusted third party, and comprises determining the master challenge data based on obtaining the one or more pieces of identification information.
7. The method of claim 6, wherein said obtaining comprises receiving the one or more pieces of identification information from the target party.
8. The method of claim 4 or 5, wherein the method is performed by the target party, and the storing of the master challenge comprises the target party performing one of: determining the master challenge and sending it to be stored in the data store, or sending at least one of the one or more pieces of identification information to a trusted third party to cause the trusted third party to generate the master challenge and it store in the data store.
9. The method of claim 7 or 8, comprising establishing a secure channel between the target party and trusted third party based on a shared secret shared between the target party and trusted third party, wherein the receiving or sending of the identification information between the target party and trusted third party is performed over the secure channel.
10. The method of any preceding claim, wherein the target is one of multiple targets for which the data store stores corresponding sets of response data and master challenges, each master challenge enabling derivation of a respective set of challenges, for use in verifying the corresponding target.
11. The method of claim 10, wherein each master challenge comprises identification data of the corresponding target.
12. The method of any preceding claim, wherein the derivation function derives the set of challenges in an ordered form, and each of the pieces of response data is stored in association with an identifier specifying a different one of the challenges in said order, thus mapping different respective pieces of response data to different respective ones of the set of challenges derivable from the master challenge.

13. The method of any preceding claim, wherein the challenges of the set are derivable in a chained manner, a first of the set of challenges being derivable by applying the derivation function to the master challenge, and each successive challenge in said set being derivable by applying the derivation function to a preceding challenge in the set.

14. The method of any of claims 1 to 12, wherein the challenges of the set are derivable in a hierarchical manner, a first subset of the set of challenges being derivable by applying the derivation function to the master challenge, and each of one or more successive subsets being derivable by applying the derivation function to one of the challenges further back in the hierarchy.

15. The method of any preceding claim, wherein the derivation function or an indication thereof is also stored in the data store, thereby making the derivation function or indication thereof available to the one or more verifying parties.

16. The method of any preceding claim, wherein the derivation function is pre-known to at least one of the verifying parties and does not need to be made available or indicated to the at least one verifying party.

17. The method of any preceding claim, wherein the one or more verifying parties are a plurality of verifying parties, the set of challenges is a plurality of challenges, and the set of responses is respective plurality of responses; and wherein the storing makes only a respective subset of one or more of the pieces of response data available to each of the verifying parties, with different subsets being made available to different ones of the verifying parties.

18. The method of claim 17, wherein the subsets are exclusive of one another.

19. The method of any preceding claim, wherein each of the response data records comprises an explicit value of the respective response, but stored in the data store only in encrypted form.

20. The method of claim 19, wherein each of a plurality of subsets of one or more of the response data records is individually encrypted, each subset requiring a different respective decryption key to decrypt; and wherein the different subsets are made available to different ones of the verifying parties by distributing different ones of the decryption keys to different verifying parties.

21. The method of any of claims 1 to 18, wherein each of the pieces of response data comprises only an attestation of the respective response, not an explicit value of the response, the attestation comprising a transformation of the respective response which does not disclose the response, but which enables a verifying party to verify the identity of the target by performing the same transformation on a further instance of the respective response returned by the target and comparing with the attestation.

22. The method of claim 21, wherein the transformation comprises a hash or double hash.

23. 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.

24. 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 22.

25. A computer-implemented method whereby a verifying party verifies an identity of a target comprising a target party or device of the target party; the method comprising, by the verifying party:

accessing, from a data store, a piece of response data from among a set of response data records, each comprising either: a) a value of a response resulting from inputting a

challenge into a PUF module comprising a physically unclonable function, PUF, associated with the target, or b) an attestation comprising a transformation of the response;

accessing a master challenge from the data store, and deriving at least one of the set of challenges by applying a derivation function to the master challenge;

sending to the target a request comprising the at least one challenge to the target, and in response receiving back a further instance of the response;

performing a comparison and verifying the identity of the target on condition that the comparison results in a match, wherein the comparison comprises: in the case of a) the stored value of the response matches the further instance, or in the case of b) the attestation matches the same transformation applied to the further instance.