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, by a setting-up party other than any of the one or more verifying parties:

inputting a set of one or more challenges into a PUF module comprising a physically unclonable function, PUF, in order to generate a respective set of one or more responses based on the PUF; and

storing a respective response data record for each of the set of responses in a data store external to any equipment of the target party or any of the one or more verifying parties, the data store either being part of third party computer equipment or being a public peer-to-peer publication medium, thereby making the response data records available to the one or more verifying party to verify the identity of the target in a subsequent verification phase, wherein the response data record for each response comprises the respective response or data derived therefrom.

2. The method of claim 1, wherein the setting-up party is the target party and the method is performed by the target party using computer equipment of the target party.

3. The method of claim 2, wherein the PUF module is integrated in the computer equipment of the target party.

4. The method of claim 2, wherein the PUF module is an external peripheral to the computer equipment of the target party.

5. The method of any of claims 2 to 4, wherein the data store is part of the third party computer equipment, and the target party receives the set of challenges from the third party, the set of challenges input to the PUF module being the set as received from the third party.

6. The method of claim 1, wherein the setting-up party is a trusted third party.

7. The method of claim 6, wherein the data store is part of the third party computer equipment, and the method is performed by the trusted third party using the third party computer equipment.

8. The method of claim 7, wherein the PUF module is an external peripheral or removable component of the third party computer equipment, and the method comprises physically sending the PUF module to the target party after the set-up phase to enable the target party to respond to challenges from the verifying party in the verification phase.

9. The method of any of claims 1 to 6, wherein the data store is the peer-to-peer publication medium, wherein the peer-to-peer publication medium is a blockchain.

10. The method of claim 9, wherein the blockchain employs an output-based transaction model, the blockchain comprising a plurality of transactions each having at least one input and at least one output, wherein the input of each transaction points to the output of another transaction, and wherein the response data records are stored in one or more outputs of one or more of the transactions recorded on the blockchain; and

wherein the method further comprises updating or revoking an expired one of the response data records by recording a new transaction on the blockchain that has an input pointing to the output of the transaction storing the expired response data record.

11. The method of any preceding claim, wherein the step of storing comprises accessing the data store via a network and sending data over the network in order to create the response data records in the data store.

12. The method of any preceding claim, wherein the one or more verifying parties are a plurality of verifying parties, and wherein the storing makes only a respective subset of one or more of the response data records available to each of the verifying parties, with different subsets being made records available to different ones of the verifying parties.

13. The method of claim 12, wherein the subsets are exclusive of one another.

14. The method of any preceding claim, wherein each of the response data records comprises an explicit value of the respective response, wherein the value of each response data record is stored in the data store only in encrypted form, and wherein each response data record requires a different respective decryption key to decrypt.

15. The method of claim 14 as dependent on claim 12, 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.

16. The method of any of claims 1 to 13, wherein each of the response data records 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.

17. The method of claim 16, wherein the transformation comprises a hash or double hash.

18. The method of any of claims 1 to 13, wherein each of the response data records comprises a respective public key of a respective public-private key pair derived from the respective response.

19. The method of claim 18, wherein said derivation comprises using the respective response as a seed in an algorithm that generates the respective public-private key pair.

20. The method of claim 18 or 19, comprising sending, or making available, to one of the verifying parties, a message signed by the target using one of the public keys.

21. The method of any preceding claim, wherein the PUF module comprises a PUF, interface logic, and a deterministic transform function; wherein the interface logic causes the generation of the set of responses by:

- receiving the set of challenges;

- inputting a base challenge into the PUF to generate a corresponding primary response; and

- inputting each of the received set of challenges and into the transform function in conjunction with the generated base response in order to generate the respective response of said set of responses, the transform function being a function of the respective challenge from the received set and the generated base response.

22. The method of any preceding claim, wherein each of the response data records is stored in the data store in association with an indication of the respective challenge, thus enabling the verifying party to determine the respective challenge, or to look up the respective response based on the respective challenge, which is to be used to challenge the target in the verification; and

wherein the indication of the challenges comprises a master challenge from which the set of challenges can be derived.

23. The method of any preceding claim, wherein the target party is one of multiple target parties for which the data store records sets of response data resulting from challenges to corresponding PUFs of the multiple parties.

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.

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 23.