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 third party computer equipment comprises server equipment comprising one or more server units at one or more geographic sites.~~

~~9~~8. The method of claim 7 ~~or 8~~, 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.

~~10~~9. The method of any of claims 1 to 6, wherein the data store is the peer-to-peer publication medium~~.~~

~~11. The method of claim 10~~, wherein the peer-to-peer publication medium is a blockchain.

~~12~~10. The method of claim ~~11~~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

~~13. The method of claim 12,~~ 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.

~~14~~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.

~~15~~12. The method of any preceding claim, wherein the one or more verifying parties are a plurality of verifying parties~~.~~, and

~~16. The method of claim 15,~~ 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.

~~17~~13. The method of claim ~~16~~12, wherein the subsets are exclusive of one another.

~~18~~14. The method of any preceding claim, wherein each of the response data records comprises an explicit value of the respective response~~.~~

~~19. The method of claim 18~~, wherein the value of each response data record is stored in the data store only in encrypted form~~.~~

~~20. The method of claim 19~~, and wherein each response data record requires a different respective decryption key to decrypt.

~~21~~15. The method of claim ~~20~~14 as dependent on claim ~~16~~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.

~~22~~16. The method of any of claims 1 to ~~17~~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.

~~23~~17. The method of claim ~~22~~16, wherein the transformation comprises a hash or double hash.

~~24. The method of any preceding claim, comprising receiving a request from one of the verifying parties, the request comprising one of the set of challenges; and in response, inputting the further instance of the challenge into the PUF module in order to generate a further instance of the corresponding response, and returning the further instance of the response to the verifying party to enable the verifying party to verify the identity of the target based on a comparison with the response stored in the data store.~~

~~25~~18. The method of any of claims 1 to ~~17~~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.

~~26~~19. The method of claim ~~25~~18, wherein said derivation comprises using the respective response as a seed in an algorithm that generates the respective public-private key pair.

~~27~~20. The method of claim ~~25~~18 or ~~26~~19, comprising sending, or making available, to one of the verifying parties, a message signed by the target using one of the public keys.

~~28~~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.

~~29~~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

~~30. The method of claim 29, wherein the indication of each respective challenge comprises an explicit value of the respective challenge stored in association with the respective response data.~~

~~31. The method of claim 29,~~ wherein the indication of the challenges comprises a master challenge from which the set of challenges can be derived.

~~32~~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.

~~33~~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.

~~34~~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 ~~32~~23.

~~35. 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 trusted third party:~~

~~receiving response data from the target party, resulting from the target party inputting a respective challenge into a PUF module comprising a physically unclonable function, PUF, in order to generate a respective response;~~

~~storing a respective response data record for each of the one or more responses in a data store of the trusted third party, each response data record comprising the respective response or data derived therefrom; and~~

~~making the response data records available to the one or more verifying parties 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.~~

~~36. 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 claim 35.~~

~~37. 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 claim 35.~~

~~38. 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 a response data record in a data store external to any equipment of the target party or the verifying party, the data store either being part of third party computer equipment of a trusted third party or being a public peer-to-peer publication medium, wherein the response data record comprises either: a) a value of 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;~~

~~sending a request comprising the 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.~~

~~39. 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 claim 38.~~

~~40. 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 claim 38.~~