CLAIMS

1. A computer-implemented method of performing a computation, the method comprising, by target computer equipment of a target party, being the computer equipment which is to perform the computation:

obtaining a cryptographic key derived from a response generated by PUF module comprising a physically unclonable function, PUF, the response having been generated by the PUF module based on the PUF in response to a corresponding challenge input to the PUF module, wherein key information comprising the cryptographic key or a corresponding public key is also made available to a verifying party;

from an issuing party, receiving a computation request specifying the computation to be performed;

in response to the computation request, performing the computation in order to generate a computation result;

signing a message comprising the computation result with the cryptographic key; and

making the signed message available to the verifying party by sending the signed message to be recorded on a blockchain.

2. The method of claim 1, wherein the issuing party is the verifying party.

3. The method of claim 1 or 2, wherein the sending of the signed message comprises:

- the target party formulating a template blockchain transaction comprising the signed message; and

- the target party sending the template transaction to the verifying party, thereby causing the verifying party to verify the signature on the message, and in dependence thereon to complete the template transaction at least by signing with a signature of the verifying party, and forward the completed transaction to be recorded on the blockchain.

4. The method of claim 3, wherein the message comprises at least part of the template transaction.

5. The method of claim 3 or 4, wherein the completed transaction pays the target party for the computation once recorded on the blockchain.

~~6. The method of claim 5, wherein the completed transaction pays the target party by comprising an input that points to an output of a funding transaction on the blockchain, and an output that assigns at least some funds of the issuing party from the output of the funding transaction to the target party; wherein the output of the funding transaction comprises a time-out condition that enables the funds to be transferred back to the issuing party if not assigned to the target party after a specified time-out period.~~

~~7~~6. The method of any preceding claim, wherein the obtaining of the cryptographic key is performed, and the key information made available to the verifying party, in a set-up phase prior to the target party receiving the computation request.

~~8~~7. The method of any preceding claim, wherein said obtaining comprises:

receiving the response from the issuing party, verifying party or a trusted third party, the challenge having been input into the PUF module to generate the response by the issuing party, verifying party or trusted third party on behalf of the target party, and generating of the public-private key pair being based on the received response.

~~9~~8. The method of any of claims 1 to ~~7~~6, wherein said obtaining comprises:

receiving the public key from the issuing party, verifying party or a trusted third party, the challenge having been input into the PUF by the issuing party, verifying party or trusted third party to generate the response and derive the cryptographic key pair on behalf of the target party.

~~10. The method of claim 8 or 9, wherein the third party makes the key information available to the verifying party.~~

~~11~~9. The method of any of claims 1 to ~~7~~6, wherein said obtaining comprises: the target party performing the inputting of the challenge to the PUF module to generate the response and derive the cryptographic key by the target party.

~~12. The method of claim 11, wherein the target computer equipment takes the form of a self-contained target device, and one of:~~

~~- the PUF module is incorporated in a same housing as the target device, or~~

~~- the PUF module is implemented in an external peripheral connected to the target device by a cable but not a network.~~

~~13. The method of claim 11 or 12, or any of claims 1 to 9, wherein the method comprises the target party making the key information available to the verifying party.~~

~~14. The method of any preceding claim, wherein the making available of the key information to the verifying party comprises: sending the key information to the verifying party.~~

~~15~~10. The method of any ~~of~~preceding claim~~s 1 to 13~~, wherein the making available of the key information to the verifying party comprises: storing the key information linked to an identity of the target party or target computer equipment, in a key information storage medium accessible to the verifying party~~.~~;

~~16. The method of claim 15,~~ ____wherein the key information storage medium is implemented in third party server equipment comprising one or more server units at one or more physical sites~~.~~

~~17. The method of claim 16~~, wherein the key information storage medium is a blockchain or other peer-to-peer publication medium.

~~18. The method of any preceding claim, wherein the cryptographic key comprises a private key of an asymmetric public-private key pair comprising the private key and a corresponding public key, the key public private key pair being derived from said response, wherein the key information made available to the verifying party comprises the public key.~~

~~19. The method of any of claims 1 to 17, wherein the cryptographic key comprises a key of a symmetric authentication scheme, wherein the key information made available to the verifying party also comprises said cryptographic key.~~

~~20~~11. The method of any preceding claim, comprising encrypting the computation result so as to require a decryption key to decrypt, wherein the computation result is made available able to the verifying party only in encrypted form, and the decryption key is made available to the verifying party and/or issuing party.

~~21~~12. The method of claim ~~20~~11, wherein the encryption comprises encrypting the computation result before signing with the private key.

~~22~~13. The method of claim ~~20~~11, wherein the encryption comprises encrypting the message after signing with the private key.

~~23~~14. The method of any of claims ~~20~~11 to ~~22~~13, wherein the decryption key is derived from another response generated by the PUF module, or another PUF module, in response to another challenge input to the PUF module by the target party, verifying party, issuing party or a trusted third party.

~~24~~15. The method of claim ~~23~~14, wherein the method comprises the target party inputting said other response to generate the other challenge, and deriving the decryption key.

~~25~~16. The method of any of claims ~~20~~11 to ~~24~~15, comprising the target party making the decryption key available to the verifying party and/or issuing party.

~~26~~17. The method of any of claims ~~20~~11 to ~~25~~16, wherein the making available of the decryption key to the verifying party and/or issuing party comprises: sending the decryption key to the verifying party and/or issuing party.

~~27~~18. The method of any of claims ~~20~~11 to ~~25~~16, wherein the making available of the decryption key to the verifying party and/or issuing party comprises: storing the decryption key in a decryption key storage medium accessible to the verifying and/or issuing party.

~~28~~19. The method of claim ~~27~~18, wherein the decryption key storage medium is implemented in third party server equipment comprising one or more server units at one or more physical sites.

~~29~~20. The method of claim ~~27~~18, wherein the decryption key storage medium is a blockchain or other peer-to-peer publication medium.

~~30~~21. The method of any preceding claim, wherein the receiving of the computation request comprises accessing an electronic advertisement medium to retrieve the computation request~~.~~

~~31. The method of claim 30, wherein the electronic advertisement medium is implemented in third party server equipment or computer equipment of the verifying party.~~

~~32. The method of claim 30~~, wherein the electronic advertisement medium is a blockchain or other peer-to-peer publication medium.

~~33. The method of any preceding claim, comprising sending an acceptance signal from the target party to the verifying party accepting the computation.~~

~~34~~22. The method of any preceding claim, wherein the target computer equipment is one of a plurality of pieces of computer equipment involved in a distributed computing system performing distributed computing, said computation being part of the distributed computing.

~~35~~23. The method of claim ~~34~~22, wherein the distributed computing is performed on a pay per computation basis, wherein the target party receives a payment for performing the

computation on condition that the verifying party verifies the signature of the target party based on the key information.

~~36. The method of any preceding claim, wherein message further comprises a time stamp indicating a time of performing the computation at the target computer equipment.~~

~~37. The method of any preceding claim, wherein the PUF module comprises a PUF and a deterministic transform function, and is configured to generate the response by:~~

~~- inputting a base input into the PUF to generate a corresponding base output; and~~

~~- inputting the challenge and into the transform function in conjunction with the generated base output in order to generate the response, the transform function being a function of the challenge and the generated base output.~~

~~38~~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.

~~39~~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 ~~37~~23.