

CLAIMS:

1. A computer-implemented method comprising:
 - determining, at a participant of a plurality of participants, a function usable to map
finite field elements;
 - 5 generating, based on a number of participants, polynomials evaluated in a set of
points;
 - distributing the polynomials to corresponding participants of the plurality of
participants;
 - determining a sum of polynomials of each participant of the plurality of
10 participants, wherein the sum corresponds to a power of a secret; and
collectively generating, among the plurality of participants and based on the secret,
a blockchain transaction.
2. A method according to any preceding claim, wherein the set of points are a set of
elliptic curve points.
- 15 3. A method according to any preceding claim, wherein determining the sum of
polynomials is based on a Lagrange interpolation.
4. A method according to any preceding claim, further comprising determining, based at
least in part on the power of the secret, a common reference string that is determinable
by the plurality of participants.
- 20 5. A method according to any preceding claim, further comprising receiving
corresponding values of polynomials from each participant of the plurality of
participants.
6. A method according to any preceding claim, wherein off-chain communications are
utilised in the distribution of the values of the polynomials to the corresponding
25 participants.

7. A method according to any preceding claim, wherein the function usable to map the finite field elements serves as a coefficients or exponent of a generator of a group.
8. A method according to any preceding claim, wherein the plurality of participants is exactly two participants.
- 5 9. A method according to any preceding claim, wherein the secret is determined based on the sum of polynomials evaluated at a particular point.
10. A method according to claim 9, wherein the particular point is an intersection point.
11. A method according to any preceding claim, wherein the set of points excludes the intersection point.
- 10 12. A method according to any preceding claim, wherein the polynomials evaluated in the set of points are of at least order 2.
13. A method according to any preceding claim, wherein each point of the set of points is a different point.
14. A system, comprising:
 - 15 a processor; and
 - memory including executable instructions that, as a result of execution by the processor, causes the system to perform the computer-implemented method according to any preceding claim.
- 15 15. A non-transitory computer-readable storage medium having stored thereon executable instructions that, as a result of being executed by a processor of a computer system, cause the computer system to at least perform the computer-implemented method according to any of claims 1 to 13.
- 20