

CLAIMS

1. A method performed by a secure multi-party computing system configured for performing multi-party computations on secret shared values, the secure multi-party computing system comprising a trusted dealer computing system and a plurality of party computing systems in secure networked communication, the method for casting a secret shared value from a first modular representation to a second modular representation, the method comprising:
 - each of the party computing systems storing a respective secret share of the secret shared value in the first modular representation,
 - wherein the first modular representation has a range defined by a most significant bit position and a least significant bit position of the first modular representation;
 - the trusted dealer computing system storing a masking value and communicating to each of the party computing systems a respective secret share of the masking value in the first modular representation so that the masking value is secret shared between the party computing systems in the first modular representation;
 - the trusted dealer computing system:
 - determining a subrange in which the masking value resides, wherein the subrange is selected from a plurality of predetermined non-overlapping subranges representing the range of the first modular representation,
 - encoding the determined subrange into a numerical subrange identifier, and
 - communicating to each of the party computing systems a respective secret share of the numerical subrange identifier so that the numerical subrange identifier is secret shared between the party computing systems;
 - the trusted dealer computing system transforming the masking value, in a first transformation, into a transformed masking value by at least performing a first mathematical lift on the masking value;
 - the trusted dealer computing system communicating to each of the party computing systems a respective secret share of the transformed masking value in the second modular representation so that the transformed masking value is secret shared between the party computing systems in the second modular representation,

wherein the second modular representation has a range defined by a most significant bit position and a least significant bit position of the second modular representation, and wherein the most significant bit position of the second modular representation is greater than the most significant bit position of the first modular representation;

the party computing systems collaboratively computing and revealing a sum of the secret shared value and the masking value as a masked value without revealing the secret shares of the secret shared value or the secret shares of the masking value;

transforming the masked value, in a second transformation, into a first transformed masked value by at least performing a second mathematical lift on the masked value;

transforming the masked value, in a third transformation, into a second transformed masked value by at least performing a third mathematical lift on the masked value,

wherein the first mathematical lift, the second mathematical lift and the third mathematical lift are each different from one another; and

the party computing systems collaboratively computing the secret shared value in the second modular representation such that each of the party computing systems computes a respective secret share of the secret shared value in the second modular representation based on:

the first transformed masked value,

the second transformed masked value,

for each party computing system, the respective secret share of the numerical subrange identifier, and

for each party computing system, the respective secret share of the transformed masking value.

2. The method of claim 1,

wherein the first mathematical lift and the second mathematical lift produce values relative to each other that are offset by one quarter of the range of the first modular representation, and

wherein the second mathematical lift and the third mathematical lift produce values relative to each other that are offset by one half of the range of the first modular representation.

3. The method of claim 1, wherein the first mathematical lift, the second mathematical lift, and the third mathematical lift are each selected from a group consisting of:
 - a quartermod lift parameterized by $2^{M_{\text{msb}}}$, where $(M_{\text{msb}} - 1)$ is the most significant bit position of the first modular representation,
 - a centermod lift parameterized by $2^{M_{\text{msb}}}$, and
 - a posmod lift parameterized by $2^{M_{\text{msb}}}$.
4. The method of claim 1,
 - wherein the first mathematical lift is a quartermod lift on the masking value parameterized by $2^{M_{\text{msb}}}$,
 - wherein the second mathematical lift is a centermod lift on the masked value parameterized by $2^{M_{\text{msb}}}$,
 - wherein the third mathematical lift is a posmod lift on the masked value parameterized by $2^{M_{\text{msb}}}$, and
 - where $(M_{\text{msb}} - 1)$ is the most significant bit position of the first modular representation.
5. The method of claim 4,
 - wherein a quartermod lift on x parameterized by 2^M is defined as a unique real $\tilde{x} \in \left[-\frac{2^M}{4}, \frac{3 \cdot 2^M}{4}\right)$ such that $\tilde{x} - x \in 2^M \mathbb{Z}$,
 - wherein a centermod lift on x parameterized by 2^M is defined as a unique real $\tilde{x} \in \left[-\frac{2^M}{2}, \frac{2^M}{2}\right)$ such that $\tilde{x} - x \in 2^M \mathbb{Z}$, and
 - wherein a posmod lift on x parameterized by 2^M is defined as a unique real $\tilde{x} \in [0, 2^M)$ such that $\tilde{x} - x \in 2^M \mathbb{Z}$.
6. The method of claim 5,
 - wherein the first transformation further comprises:
 - rounding a result of the first mathematical lift to a nearest multiple of $2^{p'_{\text{lsb}}}$,
 - where p'_{lsb} is the least significant bit position of the second modular representation,
 - and
 - taking a modulo $2^{M'_{\text{msb}}}$ of the rounding, where $(M'_{\text{msb}} - 1)$ is the most significant bit position of the second modular representation;

wherein the second transformation further comprises:

rounding a result of the second mathematical lift to a nearest multiple of $2^{p'_{lsb}}$,

and

taking a modulo $2^{M'_{msb}}$ of the rounding; and

wherein the third transformation further comprises:

rounding a result of the third mathematical lift to a nearest multiple of $2^{p'_{lsb}}$,

and

taking a modulo $2^{M'_{msb}}$ of the rounding.

7. The method of claim 1, wherein the first transformation, the second transformation and the third transformation each comprises projecting a result of the associated mathematical lift onto $\mathbb{R}/2^{M'_{msb}}\mathbb{Z}$, where $(M'_{msb} - 1)$ is the most significant bit position of the second modular representation.

8. The method of claim 1, wherein the “plurality of predetermined non-overlapping subranges” consists of two equally sized subranges, and wherein the numerical subrange identifier is selected from a group consisting of the numbers 0 and 1.

9. The method of claim 8, wherein the secret shared numerical subrange identifier is used by the party computing systems collaboratively to select between the first transformed masked value and the second transformed masked value for use in calculating the secret shared value in the second modular representation.

10. The method of claim 1, wherein the first modular representation and the second modular representation are fixed point integer representations of real numbers.

11. A method performed by a secure multi-party computing system configured for performing multi-party computations on secret shared values, the secure multi-party computing system comprising a plurality of party computing systems in secure networked communication, the method for casting a secret shared value from a first modular representation to a second modular representation, the method comprising:

each of the party computing systems storing a respective secret share of the secret shared value in the first modular representation,

wherein the first modular representation has a range defined by a most significant bit position and a least significant bit position of the first modular representation;

communicating to each of the party computing systems a respective secret share of a masking value so that the masking value is secret shared between the party computing systems;

communicating to each of the party computing systems a respective secret share of an indication of a subrange in which the masking value resides, wherein the subrange is selected from a plurality of predetermined non-overlapping subranges representing the range of the first modular representation, so that the subrange indication is secret shared between the party computing systems;

transforming the masking value, in a first transformation, into a transformed masking value by at least performing a first mathematical lift on the masking value;

communicating to each of the party computing systems a respective secret share of the transformed masking value in the second modular representation so that the transformed masking value is secret shared between the party computing systems in the second modular representation,

wherein the second modular representation has a range defined by a most significant bit position and a least significant bit position of the second modular representation, and wherein the most significant bit position of the second modular representation is greater than the most significant bit position of the first modular representation;

the party computing systems collaboratively computing and revealing a sum of the secret shared value and the masking value as a masked value without revealing the secret shares of the secret shared value or the secret shares of the masking value;

transforming the masked value, in a second transformation, into a first transformed masked value by at least performing a second mathematical lift on the masked value;

transforming the masked value, in a third transformation, into a second transformed masked value by at least performing a third mathematical lift on the masked value,

wherein the first mathematical lift, the second mathematical lift and the third mathematical lift are each different from one another; and

the party computing systems collaboratively computing the secret shared value in the second modular representation such that each of the party computing systems computes a respective secret share of the secret shared value in the second modular representation based on:

- the first transformed masked value,
- the second transformed masked value,
- for each party computing system, the respective secret share of the subrange indication, and
- for each party computing system, the respective secret share of the transformed masking value.

12. The method of claim 11, wherein the first transformation, the second transformation and the third transformation each comprises projecting a result of the associated mathematical lift onto $\mathbb{R}/2^{M'_{\text{msb}}}\mathbb{Z}$, where $(M'_{\text{msb}} - 1)$ is the most significant bit position of the second modular representation.

13. The method of claim 11, wherein the “plurality of predetermined non-overlapping subranges” consists of two equally sized subranges, and wherein the numerical subrange identifier is selected from a group consisting of the numbers 0 and 1.

14. The method of claim 13, wherein the secret shared numerical subrange identifier is used by the party computing systems collaboratively to select between the first transformed masked value and the second transformed masked value for use in calculating the secret shared value in the second modular representation.

15. The method of claim 11, wherein the first modular representation and the second modular representation are fixed point integer representations of real numbers.

16. A method for performing a multiplication of a first secret shared value stored in a respective initial modular representation and a second secret shared value stored in a respective initial modular representation, the method comprising:

- casting, in accordance with the method of claim 11, at least one of the first secret shared value and the second secret shared value into a common modular representation

such that both the first secret shared value and the second secret shared value are stored in the common modular representation; and

performing a beaver multiplication on the first secret shared value and the second secret shared value in the common modular representation.

17. A method for combining a plurality of secret shared values, each being stored in a respective initial modular representation, and a corresponding plurality of static coefficients, the method comprising:

casting, in accordance with the method of claim 11, at least one of the plurality of secret shared values into a common modular representation such that all of the plurality of secret shared values are stored in the common modular representation; and

performing a linear combination on the plurality of secret shared values stored in the common modular representation and the corresponding plurality of static coefficients.

18. A method for evaluating a continuous function on a secret shared value, the method comprising:

selecting a Fourier series, based on the secret shared value, from a plurality of determined Fourier series, wherein each of the plurality of determined Fourier series is configured to approximate the continuous function on an associated subinterval of a domain of the continuous function;

based on the selection, casting, in accordance with the method of claim 11, the secret shared value from a first modular representation to a second modular representation; and

approximating a value of the continuous function on the secret shared value in the second modular representation using the selected Fourier series.

19. A system comprising a plurality of computer systems, wherein the plurality of computer systems are configured to perform the method of any one of claims 1 through 18.

20. A non-transitory computer-readable medium encoded with computer code that, when executed by a plurality of computer systems, causes the plurality of computer systems to perform the method of any one of claims 1 through 18.