CLAIMS

1. A method for configuring a process comprising:
converting a neural network trained to map process inputs to process outputs to operate on data in encrypted domain of a predetermined encryption and decryption scheme such that the encryption of the encryption and decryption scheme is homomorphic with respect to the operation of the converted neural network;
determining a desired process output in encrypted domain;
determining an input in encrypted domain to the converted neural network leading to an output of the converted neural network approximating the desired process output in encrypted domain; and
providing the determined input for configuration of the process.

2. The method of claim 1, comprising training the neural network to map process inputs to process outputs.

3. The method of claim 1 or 2, wherein determining the desired process output in encrypted domain comprises obtaining a desired process output and encrypting the desired process output to encrypted domain.

4. The method of any one of claims 1 to 3, comprising decrypting the determined input.

5. The method of claim 4, comprising configuring the process according to the decrypted determined input.

6. The method according to any one of claims 1 to 5, wherein the input in encrypted domain to the converted neural network is determined by searching for an input which minimizes the loss between the output that the converted neural network outputs in response to the input and the desired process output in encrypted domain.

7. The method according to any one of claims 1 to 6, wherein the input in encrypted domain to the converted neural network is determined by performing back-

propagation in the encrypted domain by utilizing polynomial approximations for computations of non-linear activation function computations and/or their gradients.

8. The method of any one of claims 1 to 7, comprising controlling a system for performing the process according to the determined input.

9. The method of any one of claims 1 to 8, wherein the process is a manufacturing process and the input specifies one or more control parameters of a manufacturing system and the method comprises controlling the manufacturing system according to the determined input.

10. The method of any one of claims 1 to 9, wherein the encryption and decryption scheme is a public key encryption and decryption scheme, specifically, a levelled or fully homomorphic encryption scheme.

11. The method of any one of claims 1 to 10, comprising performing multiple iterations of
determining a desired process output in encrypted domain; and
determining an input in encrypted domain to the converted neural network leading to an output of the converted neural network approximating the desired process output in encrypted domain;
until the determined input fulfils a predetermined quality criterion; and
providing the determined input for configuration of the process when the determined input fulfils the predetermined quality criterion.

12. The method of claim 11, wherein the predetermined quality criterion is that the determined input leads to an output of the converted neural network which approximates the desired process output in encrypted domain with a predetermined accuracy.

13. The method of any one of claims 1 to 12, further comprising: prior to converting a neural network trained to map process inputs to process outputs,

training the neural network based on plain data and encrypted data.

14. The method of claim 13, wherein the training the neural network based on plain data and encrypted data comprises performing an extended backward propagation process by optimize inputs with gradient descent.

15. The method of claim 13 or claim 14, wherein the training the neural network based on plain data and encrypted data comprises non-linear activation computations in a forward process.

16. A system comprising one or more computers, each computer comprising a communication interface, a memory and a processing unit, wherein the system is configured to perform the method of any one of claims 1 to 15.

17. A computer program element comprising program instructions, which, when executed by one or more processors, cause the one or more processors to perform the method of any one of claims 1 to 15.

18. A computer-readable medium comprising program instructions, which, when executed by one or more processors, cause the one or more processors to perform the method of any one of claims 1 to 15.