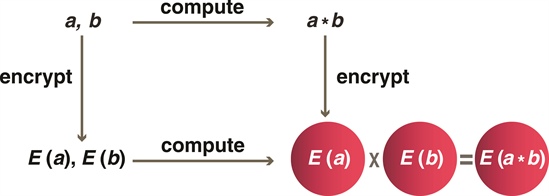
Private Artificial Intelligence: Machine Learning on Encrypted Data[[1]](#footnote-1)

By [Kristin Lauter](https://sinews.siam.org/About-the-Author/kristin-lauter)

Artificial intelligence (AI) refers to the science of utilizing data to formulate mathematical models that predict outcomes with high assurance. Such predictions can be used to make decisions automatically or give recommendations with high confidence. Training mathematical models to make predictions based on data is called machine learning (ML) in the computer science community. Tremendous progress in ML over the last two decades has led to impressive advances in computer vision, natural language processing, robotics, and other areas. These applications are revolutionizing society and people’s overall way of life. For example, smart phones and smart devices currently employ countless AI-based services in homes, businesses, medicine, and finance.

However, these services are not without risk. Large data sets—which often contain personal information—are needed to train powerful models. These models then enable decisions that may significantly impact human lives. The emerging field of *responsible AI*intends to put so-called guard rails in place by developing processes and mathematical and statistical solutions. Humans must remain part of this process to reason about policies and ethics, and to consider proper data use and the ways in which bias may be embedded in existing data. Responsible AI systems aim to ensure fairness, accountability, transparency, and ethics, as well as privacy, security, safety, robustness, and inclusion.

Here I focus on the privacy problem in AI and the intersection of AI with the field of cryptography. One way to protect privacy is to lock down sensitive information by encrypting data before it is used for training or prediction. However, traditional encryption schemes do not allow for any computation on encrypted data. We therefore need a new kind of encryption that maintains the data’s structure so that meaningful computation is possible. Homomorphic encryption allows us to switch the order of encryption and computation so that we get the same result if we first encrypt and then compute, or if we first compute and then encrypt (see Figure 1).



**Figure 1.** Diagram of homomorphic encryption. If one begins with two pieces of data aa and bb, the outcome is the same when following the arrows in either direction: across and then down (compute, then encrypt) or down and then across (encrypt, then compute). Figure courtesy of SIAM.

A solution for a homomorphic encryption scheme that can process any circuit was first proposed in 2009 [3]. Since then, cryptography researchers have worked to find solutions that are both practical and based on well-known hard math problems. In 2012, the “ML confidential” paper introduced the first solution for training ML models on encrypted data [5].  Four years later, the CryptoNets paper [4] demonstrated the evaluation of deep neural network predictions on encrypted data — a cornerstone of private AI. *Private AI* uses homomorphic encryption to protect the privacy of data while performing ML tasks, both learning classification models and making valuable predictions based on such models.

The security of homomorphic encryption is based on the mathematics of lattice-based cryptography. A lattice can be thought of as a discrete linear subspace of Euclidean space, with the operations of vector addition, scalar multiplication, and inner product; its dimension nn is the number of basis vectors. New hard lattice problems were proposed from 2004 to 2010, but some were related to older problems that had already been studied for several decades: the approximate Shortest Vector Problem (SVP) and Bounded Distance Decoding. The best-known algorithms for attacking the SVP are called lattice basis reduction algorithms, which have a more than 30-year history. This history starts with the Lenstra-Lenstra-Lovász algorithm [9], which runs in polynomial time but finds an exponentially bad approximation to the shortest vector. More recent improvements include BKZ 2.0 and exponential algorithms like sieving and enumeration. The Technical University of Darmstadt’s [Hard Lattice Challenge](https://www.latticechallenge.org/) is publicly available online for anyone who wants to try to attack and solve hard lattice problems of large size to break the current record.

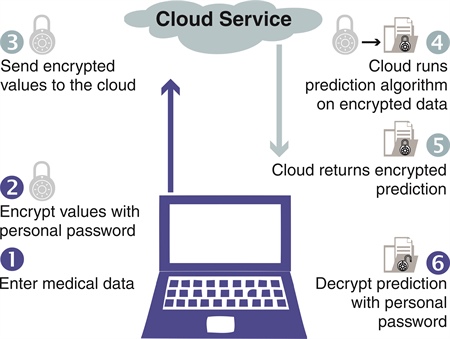
Cryptographic applications of lattice-based cryptography were first proposed by Jeffrey Hoffstein, Jill Pipher, and Joseph Silverman in 1996 and led to the launch of NTRU Cryptosystems [6]; compare this to the age of other public key cryptosystems such as RSA (1975) or Elliptic Curve Cryptography ECC (1985). Because lattice-based cryptography is a relatively new form of encryption, standardization and regulation are needed to build public trust in the security of the schemes. In 2017, we launched [HomomorphicEncryption.org](https://homomorphicencryption.org/): a consortium of experts from industry, government, and academia to standardize homomorphic encryption schemes and security parameters for widespread use. The community approved the first Homomorphic Encryption Standard in November 2018 [1].

Homomorphic encryption scheme parameters are set so that the best-known attacks take exponential time (exponential in the dimension nn of the lattice, meaning roughly 2n2n time). Lattice-based schemes have the advantage that there are no known polynomial time quantum attacks, which means that they are good candidates for post-quantum cryptography (PQC) in the ongoing five-year [PQC competition](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography). Nowadays, all available major homomorphic encryption libraries from around the world implement schemes that are based on the hardness of lattice problems. These libraries include [Microsoft SEAL (Simple Encrypted Arithmetic Library)](http://sealcrypto.org/)—which became publicly available in 2015—as well as other publicly available libraries like IBM’s [HELib](https://github.com/shaih/HElib" \t "_blank), Duality Technologies’ [PALISADE](https://palisade-crypto.org/), and Seoul National University’s [HEEAN](https://github.com/kimandrik/HEAAN).

Next, I will discuss several demos of private AI in action. We developed these as the Microsoft SEAL team to demonstrate a range of practical private analytics services in the cloud. The first demo is an encrypted fitness app: a cloud service that processes all workout, fitness, and location data in the cloud in encrypted form. The app displays summary statistics on a phone after locally decrypting the results of the analysis.

The second demo is an encrypted weather prediction service that takes an encrypted ZIP code and returns encrypted information about the weather at the location in question, which is then decrypted and displayed on the phone. The cloud service never learns the user’s location or the specifics of the weather data that was returned.

Finally, the third demo shows a private medical diagnosis application. The patient uploads an encrypted version of a chest X-ray image to the cloud service. The medical condition is diagnosed by running image recognition algorithms on the encrypted image in the cloud; the diagnosis is returned in encrypted form to the doctor or patient (see Figure 2).



Other examples of private AI applications include sentiment analysis in text, cat/dog image classification, heart attack risk analysis based on personal health data [2], neural net image recognition of handwritten digits [4], flowering time determination based on a flower’s genome, human action recognition in encrypted video [7], and pneumonia mortality risk analysis via intelligible models.

All of these processes operate on encrypted data in the cloud to make predictions and return encrypted results in a matter of seconds. Many applications were inspired by collaborations with researchers in medicine, genomics, bioinformatics, and ML. The annual [iDASH workshops](http://www.humangenomeprivacy.org/" \t "_blank), which are funded by the National Institutes of Health, attract teams from around the world to submit solutions to the Secure Genome Analysis Competition. Participating teams represent organizations such as Microsoft, IBM, start-up companies, and academic institutions from various countries around the world.

Homomorphic encryption has the potential to effectively protect the privacy of sensitive data in ML. It is interesting to consider how protecting privacy in AI through encryption intersects with other goals of responsible AI. If the data is encrypted, for example, it is not possible to inspect it for bias. However, encryption makes it harder for a malicious adversary to manipulate the AI models to produce undesirable outcomes.

For more detailed information about private AI and encryption, please see my article in the proceedings of the 2019 International Congress on Industrial and Applied Mathematics [8].

*Kristin Lauter will deliver the*[*I.E. Block Community Lecture*](https://sinews.siam.org/Details-Page/2022-siam-block-community-lecture-presented-by-dr-kristin-lauter)*at the*[*2022 SIAM Annual Meeting*](https://www.siam.org/conferences/cm/conference/an22)*, which will take place in Pittsburgh, Pa., in a hybrid format from July 11-15, 2022. She will speak about artificial intelligence and cryptography.*

**References**  
[1] Albrecht, M., Chase, M., Chen, H., Ding, J., Goldwasser, S., Gorbunov, S., Halevi, S., Hoffstein, J., Laine, K., Lauter, K., Lokam, S., Micciancio, D., Moody, D., Morrison, T., Sahai, A., & Vailkuntanathan, V. (2021). *Homomorphic encryption standard*. In *Protecting privacy through homomorphic encryption* (pp. 31-62). Cham, Switzerland: Springer Nature.  
[2] Bos, J.W., Lauter, K., & Naehrig, M. (2014). Private predictive analysis on encrypted medical data.*J. Biomed. Inform.*, *50*, 234-243.  
[3] Gentry, C. (2009). *A fully homomorphic encryption scheme* [Doctoral dissertation, Stanford University]. Applied Cryptography Group at Stanford University.  
[4] Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K., Naehrig, M., & Wernsing, J. (2016). CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy. In *Proceedings of the 33rd international conference on machine learning*, *48*, 201-210.  
[5] Graepel, T., Lauter, K., & Naehrig, M. (2012). ML confidential: Machine learning on encrypted data. In *International conference on information security and cryptology 2012* (pp. 1-21). Seoul, Korea: Springer.  
[6] Hoffstein, J., Pipher, J., & Silverman, J.H. (1998). NTRU: A ring-based public key cryptosystem. In *International algorithmic number theory symposium* (pp. 267-288). Portland, OR: Springer.  
[7] Kim, M., Jiang, X., Lauter, K., Ismayilzada, E., & Shams, S. (2021). HEAR: Human action recognition via neural networks on homomorphically encrypted data. Preprint, *arXiv:2104.09164*.  
[8] Lauter, K. (2022). Private AI: Machine learning on encrypted data. *Recent advances in industrial and applied mathematics*. In *ICIAM 2019 SEMA SIMAI Springer series*. Cham, Switzerland: Springer.  
[9] Lenstra, A.K., Lenstra Jr., H.W., & Lovász, L. (1982). Factoring polynomials with rational coefficients. *Mathematische Annal.*, *261*(4), 515-534.

Kristin Lauter is the Director of West Coast Research Science for Meta AI Research (FAIR). She served as president of the Association for Women in Mathematics from 2015-2017. Lauter was formerly a Partner Research Manager at Microsoft Research, where her group developed Microsoft SEAL: an open source library for homomorphic encryption.

1. https://sinews.siam.org/Details-Page/private-artificial-intelligence-machine-learning-on-encrypted-data?fbclid=IwAR19cJ2AmRLLPmoxtTQcj97oPk1F5PSpcdhZGJ4DCq8S6eQIxC9LpaV6Was [↑](#footnote-ref-1)