Homomorphic Encryption: What Is It, and Why Does It Matter?

Internet Society

December 2023

Homomorphic encryption (HME) is getting a lot of attention. For example, it is proposed as a way to scan encrypted data for illegal content. But some of the claims being made about it are unrealistic and could lead to ill-informed policy decisions. This briefing paper will help you understand the concepts, practicalities, and implications of this emerging technology, so that you can make informed decisions about it.

The Goal of Homomorphic Encryption

The goal of conventional modern encryption is to protect the confidentiality of stored or transmitted data. Good encryption should ensure that even if someone can access encrypted data, they cannot understand it. In the digital context, the general principle is that encrypted data should be indistinguishable from random data. The less scrambled a message is, the more information it leaks. Perfectly encrypted data leaks no information. In a strong conventional encryption system, there is no feasible way to extract information from the encrypted data itself unless you have the decryption key.

Homomorphic encryption (HME) has a different goal. It should be possible to perform computations on encrypted data without decrypting it, and without access to the key for the encrypted data. For example, if you have an encrypted customer database, you should be able to get an answer to the question "how many customers are located in Ohio?" without decrypting the database. In this respect, one could argue that HME represents less-than-ideal encryption, because it does not completely prevent information from being extracted from the encrypted data – but this is a nuanced problem, which we will examine in more detail below.

Why Is It Important, and to Whom?

The main impetus for the development of homomorphic encryption is cloud computing. Some businesses are only commercially viable because they can use cheap, scalable cloud computing services. Because they lodge all their data with a third party, the prospect of being able to encrypt remotely-stored data, but still work with it, is very appealing.

Aside from cloud computing, HME is also of interest as a means of implementing federated learning[1]. Federated learning is the use of multiple machine learning systems to "compete" with each other to deliver better and better results. For example, to generate increasingly realistic human faces or increasingly accurate interpretation of medical diagnostic images[2]. This use case has two prerequisites:

1. A generative adversarial network (GAN), which consists of two neural networks competing to produce increasingly realistic outputs based on their training datasets (e.g., human facial images)
2. Distributed training datasets (e.g., medical records)

Because the training datasets in a federated learning system are distributed, one approach might be to make a centralized copy of them, but this may be impractical for reasons of privacy or security. Federated learning with homomorphic encryption allows neural networks to use distributed training datasets without needing to decrypt them.

Homomorphic encryption's potential is also attracting other stakeholders. Governments want to crack down on illegal online content, but they cannot simply ban encryption without creating other unpalatable problems. They hope that HME might provide a way to determine whether encrypted content is illegal without having to decrypt it. Their approach seems to be, "If we can insist that encrypted messaging services only use HME, we will be able to identify illegal content, while assuring users that their conversations are still encrypted and therefore confidential." This is a flawed assumption.

Not All Homomorphisms Are the Same

There are three principal forms of HME: partial, "somewhat", and full. If the algorithm allows only a single operation (e.g., addition or multiplication, but not both) it is referred to as partially homomorphic. If it allows more than one operation, but still in fixed, finite combinations, it is referred to as "somewhat homomorphic" (SHE). Further, if you have implemented a PHE or SHE system to perform one function or set of functions, you can't change your mind later and request other functions on the data: the available functions are predetermined by the way the data is encrypted.

The goal of fully homomorphic encryption (FHE) is to allow arbitrary operations to be applied to encrypted data in unconstrained combinations—in other words, fully programmable functionality, in which both the program's inputs and its results are encrypted, throughout processing.

[1] https://arxiv.org/abs/2005.03793

[2] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7779924/

Practicalities

Homomorphic encryption is very computationally intensive. Compared to processing the same data in clear, it is slower, less efficient, and more energy-consuming. How much slower varies depending on the technique used, but as a rule of thumb, FHE processing is currently several thousand times slower than the equivalent plaintext processing[3]. Partially homomorphic encryption exists and is usable today[4]. It offers better performance than fully homomorphic encryption, but as noted above, it has the disadvantages of being restricted to a fixed set of basic mathematical operations, and therefore lacks flexibility once implemented.

Homomorphic encryption schemes are susceptible to attack just as conventional encryption systems are. Researchers have demonstrated side-channel attacks, which can extract plaintext from a homomorphic encryption system in operation[5].

In many HME implementations the ciphertext is limited to numeric data and even sometimes to integers, making it less random than it could be. At least one attack[6] exploited this. This is less-than-ideal encryption by its very nature, and is a serious practical issue. The use of HME for content scanning relies on matching hash values of suspicious content to the hashes of known illegal material: If homomorphically encrypting the hashes reduces their entropy, the incidence of false positives will go up, because the total number of possible hash values is reduced[7].

When we see claims that homomorphic encryption is the answer to secure, privacy-preserving scanning of encrypted messaging, we should treat them with skepticism. At this point, FHE does not look practical, either in functional terms (semantic analysis), or operational terms (scalability). Of course, technology evolves quickly, but if you need to process 100 billion messages a day[8], multiplying the server-side processing by 1,000 is unlikely ever to be a practical step.

If your secure messages took 1,000 times longer to arrive than they do now, that would probably kill the market entirely. If processing them took 1,000 times the server power it does now, it would be an ecological and commercial nightmare. And if scanning for illegal content results in significant numbers of false positives, that's a bad outcome for users, for law enforcement, and for the credibility of the policy itself.

[3] "Fully HE-based (FHE) processing remains 1,000 to 1,000,000 times slower than equivalent plaintext operations." – Ulf Mattsson, Protegrity Corp., June 2021 https://www.globalsecuritymag.com/Security-and-Performance-of,20210601,112333.html

[4] See, for example: https://homomorphicencryption.org, https://en.wikipedia.org/wiki/Homomorphic_encryption

[5] North Carolina State University, March 2022: https://news.ncsu.edu/2022/03/stealing-homomorphic-encryption-data/

[6] Hu and Wang, 2012 – An Attack on a FHE Scheme: https://eprint.iacr.org/2012/561.pdf

[7] Prof. Ross Anderson, 2022 – Chat Control or Child Protection?, pp.5-6 https://www.cl.cam.ac.uk/~rja14/Papers/chatcontrol.pdf

[8] As Techcrunch reported for WhatsApp in October 2020

Policy Implications

At this stage, fully homomorphic encryption is not a good tool for semantic analysis of text to identify illegal material, nor for analysis of images. In operational terms, the issues of scalability and false positives, mean that FHE is unlikely to be proportionate or practical as a law enforcement measure. Therefore, when claims about FHE are used in support of policies that oblige messaging platforms to scan for illegal content, we must treat the resulting policy proposals with skepticism.

Security Implications

In addition to these general policy implications, HME is also likely to raise specific and serious security concerns. Analyzing these concerns very quickly gets into deep technicalities. Simply put: HME systems are designed so that only the "owner" of the data holds the keys needed to read the results of the homomorphic processing. The law enforcement use case described above is based on the assumption that someone other than the end user can act on those results. In an end-to-end encrypted messaging system, this represents a systemic flaw, since it means that the user controls neither the HME functionality implemented on the server nor the keys used. As this analysis[9] illustrates, the server-side functions can then be used in ways that entirely undermine the confidentiality of the system.

Conclusions

Given the limitations above, it is reasonable to draw two conclusions about homomorphic encryption schemes, at least in the short to medium term:

1. PHE is not suitable for trying to interpret text strings in encrypted text, and to the extent that HME in general might attempt that function, it introduces performance demands that make it unlikely to scale to mass consumer volumes of data-in-motion. This is principally because the mathematics of HME mean that evaluating or comparing data involves processing the data bit by bit, not as larger variables.

   This is significant because advocates of HME often claim is that it offers a way to scan encrypted message contents for illegal material on systems like Signal and WhatsApp. Not only is that quite different from the paradigm of simple arithmetic operations on numerical data, it also implies very high throughput. For example, by late 2020, WhatsApp was delivering 100 billion messages a day, double the 2014 volume.

2. What makes content illegal is often a matter of contextual and semantic interpretation. Based on current HME capabilities, the idea that it can be used to identify semantically harmful content seems unrealistic, to say the least, let alone at the volumes indicated above.

[9] https://educatedguesswork.org/posts/eu-csam-proposal/