Chapter 8
Homomorphic Encryption

Jean-Pierre Hubaux

8.1 Introduction

Homomorphic Encryption (HE) is a technique in cryptography that allows for performing operations on encrypted data. The encrypted result can then be decrypted to obtain the result of the operation, making it possible to perform computations on sensitive data without revealing it. However, with recent advancements and the increasing demand for data protection, HE is expected to become more relevant soon and be used in many industries. In Switzerland, IBM, Inpher, and Tune Insight are among the companies that have developed HE libraries and offer solutions for secure computation. These solutions can provide better protection and reduce the vulnerability of data entrusted to Swiss companies.

8.2 Definition and Analysis

In some application areas, performing operations (additions, multiplications, etc.) on the encrypted form of data is desirable. This is precisely what homomorphic encryption does. The encrypted result can then be decrypted to obtain the result of the operation. The obtained result will be the same as if the computation had been performed in cleartext. This technique makes it possible to ask a third party, such as a cloud service provider, to perform operations on data that it hosts on behalf of a customer, but without seeing this data.

J.-P. Hubaux (✉)
EPFL, Lausanne, Switzerland
e-mail: jean-pierre.hubaux@epfl.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_8

The basic idea is several decades old, and partial solutions were already proposed in the late twentieth century. In 2009, Craig Gentry proved that it was possible to operate under fully homomorphic encryption (FHE) to support any computation [1]. Since then, many improvements were made, notably to increase performance.

For sensitive data, such as healthcare information, homomorphic encryption can enable new services by removing privacy barriers inhibiting data sharing, or increasing the security of existing services. For example, due to medical data privacy concerns, predictive analytics in healthcare can be hard to apply via a third-party service provider. However, these privacy concerns are diminished if the predictive analytics service provider can operate on encrypted data instead. Moreover, even if the service provider's system is compromised, the data would remain secure [2].

For many years, homomorphic encryption has suffered from two significant weaknesses: Limitations on the nature of the computations that could be performed and high computational costs (and thus higher energy consumption and slower execution). The former has been addressed by the advent of the already mentioned FHE and the subsequent enhancements brought after that; polynomials of the appropriate degree can approximate non-polynomial functions. In addition, several software optimizations have mitigated the latter. Nevertheless, many additional improvements (several orders of magnitude) are expected by deploying specialized hardware accelerators that should become available by 2025.

8.2.1 Trends

Well-established cryptographic algorithms and security protocols provide vital data protection at rest and in transit. Homomorphic encryption fills the critical data gap in processing, a need that will become more relevant in the future. This trend will be fueled by an increasing demand for data protection (motivated notably by numerous and recent data leakage scandals, including in Switzerland), increased performance of the software libraries, remarkable progress on the front of fully homomorphic encryption, hardware accelerators, better development tools, and progress on standardization [3, 4].

In particular, homomorphic encryption can be competitive compared to hardware-based solutions (enclaves or Trusted Execution Environments as described in Chap. 18). Indeed, the latter suffer from (i) the need to trust a hardware vendor, (ii) side-channel attacks, and (iii) high costs when systems need to be retrofitted after the discovery of a vulnerability. However, the equivalent problems are less salient with HE. Indeed, (i) trusting a software vendor is easier to achieve because its code can be scrutinized; moreover, (ii) the absence of side-channel attacks can be demonstrated by mathematical proofs; finally, (iii) hardware accelerators are meant to be replaced only rarely.

8.3 Consequences for Switzerland

On the business side, considering how heavily Switzerland is involved in the service sector, including data-intense activities, it is expected that homomorphic encryption can be of high relevance. In particular, better protection can reduce the vulnerability of data entrusted to Swiss companies.

In Switzerland, the three main industry-level activities related to HE are as follows. In its Zurich Research Lab, IBM has developed an HE library called HElib. HElib is a free and open-source cross-platform software. It implements various forms of homomorphic encryption. It is based on the Brakerski-Gentry-Vaikuntanathan (BGV) fully homomorphic encryption scheme. It also includes several optimizations, such as Smart-Vercauteren ciphertext packing techniques. It is written in C++.

The US-Swiss company Inpher has developed an open-source HE library called TFHE [5]. It is written in C/C++ and based on the ring variant of the Gentry, Sahai, and Waters (GSW) cryptosystem. TFHE is distinct from the company's flagship product, XOR, a software product providing secure multi-party computation features. However, XOR and TFHE can be used jointly in some cases. The company is funded mainly by US banks and operates primarily in that sector, but it also invests in the health sector.

Finally, the EPFL spin-off Tune Insight SA that was founded in 2021 has developed a HE library called Lattigo, written in GoLang [6]. The library is based on the Cheon-Kim-Kim-Song (CKKS) crypto scheme and thus provides floating point operations and supports fast bootstrapping.

For cloud computing, homomorphic encryption can respond to the legal uncertainty generated by the Schrems II ruling of the European Court of Justice. Indeed, Schrems II has challenged the agreement that was previously set up between the US and EU authorities in terms of processing of data related to EU citizens by US companies [7]. Homomorphic encryption is a response to this concern because, with HE, Swiss-based users can use US-operated cloud services while retaining the exclusive knowledge of their decryption keys and, therefore, all their data.

For an overview of HE libraries (including those unrelated to Switzerland), the reader is referred to the Wikipedia article on HE [2]. For applications aiming at building intelligence out of siloed data, homomorphic encryption can be combined with secure multi-party computation (SMC) which is described in Chap. 17.

8.3.1 Implementation Possibilities: Make or Buy

As with cryptographic solutions in general, it is not recommended to develop proprietary HE implementations, but rather to rely on well-established and standardized solutions.

8.3.2 Variations and Recommendation

At the time of this writing (November 2022), HE is still in a maturation phase, and much more information can be found about the HE tools themselves than about real-world applications. Nevertheless, we briefly provide three real-world examples related to the three companies mentioned above with Swiss-based technical activities on HE.

Organizations can use IBM's HElib to scale their stream processing applications into the infrastructure-as-a-service clouds elastically. Moreover, the proposed solution not only elastically scales data stream processing applications into public clouds but also preserves the privacy of such applications [8].

Inpher's technical solutions, XOR and TFHE, can be used to support privacy-preserving techniques in financial services. More specifically, these tools can be instrumental in fighting financial crime such as money laundering and enable enforcement use cases [9].

Finally, armasuisse and Tune Insight SA are collaborating on sharing cybersecurity intelligence [10]. Tune Insight has already deployed its privacy-preserving distributed data analysis solution among several university hospitals.

8.4 Conclusion

Homomorphic encryption can be a transformative technology to reinforce digital trust. The availability of domestic research and solutions is a competitive advantage for Switzerland.

References

1. Craig Gentry. A fully homomorphic encryption scheme. *Stanford PhD thesis*, 2009.
2. Wikipedia, Homomorphic encryption. https://en.wikipedia.org/w/index.php?title=Homomorphic_encryption&oldid=1099292061, July 2022.
3. Homomorphic Encryption Standardization – An Open Industry / Government / Academic Consortium to Advance Secure Computation. https://homomorphicencryption.org/, August 2022.
4. Abbas Acar, Hidayet Aksu, Selcuk Uluagac, and Mauro Conti. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys*, 2019.
5. TFHE Fast Fully Homomorphic Encryption over the Torus. https://tfhe.github.io/tfhe/, August 2022.
6. Lattigo: lattice-based multiparty homomorphic encryption library in Go. https://github.com/tuneinsight/lattigo, August 2022.
7. Mildebrath Hendrik. The CJEU judgment in the Schrems II case, September 2020.
8. Rodrigo Arosha, Dayarathna Miyuru, and Sanath Jayasena. Latency-aware secure elastic stream processing with homomorphic encryption. *Data Science and Engineering*, 2020.

9. Inpher's privacy-preserving cross-border analytics case study published in global ffis report. https://inpher.io/news/inphers-privacy-preserving-cross-border-analytics-case-study-published-in-global-ffis-report/.
10. Strengthening collective cyber resilience. https://www.ar.admin.ch/en/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.detail.news.html/ar-internet/news-2022/news-w-t/staerkung-der-kollektiven-cyber-resilienz.html.