How great would it be if there was a way to share all the data (including the private stuff) and permit the use of that data, without having to worry about compromising the privacy interests inherent in the data set? Until recently this seemed like an insurmountable challenge. The exciting recent work being done in homomorphic encryption research suggests that this may not be as impossible as one might think.

Homomorphic encryption, or rather Fully Homomorphic Encryption or FHE, is a group of encryption mechanisms which enable the performing of operations on encrypted data without decrypting it. A quick example is helpful in understanding how it works:

- We encrypt integer A (which has the value 34,535) using FHE encryption key k, as de341.
- We also encrypt integer B (which has the value 1,546) using the same key k, as f433.
- We provide the encrypted strings de341 and f433, but not the encryption key k, to a person who can run an FHE multiplication algorithm for us. The algorithm generates the encrypted result df436e7.

We can now decrypt df436e7 with FHE key k, to reveal the answer 53,391,110.

Note that the person running the FHE algorithm did not get our encryption key and could therefore not see the actual data. The data was therefore not at risk, from a privacy perspective, while shared in encrypted form.

FHE is a technology still in its infancy – it was first implemented for the addition and multiplication operations in 2010 - but there has been a good amount of academic advancement in this area in recent years.

One of the primary challenges in FHE is the significant computational horsepower required to implement current FHE algorithms. The development of new algorithms and more efficient approaches bring more meaningful applications of FHE closer to implementation.

The potential for FHE implementations once they are more computationally reasonable is significant. For example:

- It allows the outsourcing of any dataset for any desired computation.
- Any highly private data set becomes available for analytics towards understanding trends and patterns in that data. This could be a significant boon to money laundering and suspicious transaction detection in private consumer records maintained by institutions such as banks.
- In medical research it would greatly enhance broader and deeper study of health data.
- In the internet of things, it may enable broader encryption of sensors and systems.
- We could boost the fight against cybersecurity threats by encrypting more datasets at rest.
- Secret ballot voting could be improved to reduce, if not eliminate, the risk of a corrupt vote tally.

I will continue to watch this area of research with great interest and encourage you to do the same. Check out the Homomorphic Encryption Standardization Academic Consortium at https://homomorphicencryption.org for more insights, and be sure to follow them on twitter: @HomomorphicEnc

I recently attended a conference on cybersecurity and cybercrime where several presenters talked about privacy enhancing technologies and specifically something called “homomorphic encryption”. Even though I try to stay on top of technical trends in cybersecurity, the excitement around this technology had escaped me, and surprised me. I decided to look into it some more to understand it better. Having done so, I believe that the work in this area is important and promising and may help us solve a number of thorny problems.