MPC Alliance

A SHORT INTRODUCTION TO MULTIPARTY COMPUTATION (MPC)

JAKOB ILLEBORG PAGTER · JULY 7, 2020

Multiparty Computation (MPC) is a technology that allows you to compute on encrypted values. This might sound impossible at first – but in fact, using the right kind of cryptography, it is indeed possible. Using MPC, a number of servers can jointly compute any function without learning the inputs to the function. This technique eliminates the classic dependency on any single “trusted third party” to maintain the privacy and security of confidential data and presents a framework for increasing the integrity and availability of services. MPC replaces such a “trusted third party” with a consortium, where no single member (or a group of member, in some settings) has full control over the data and its processing.

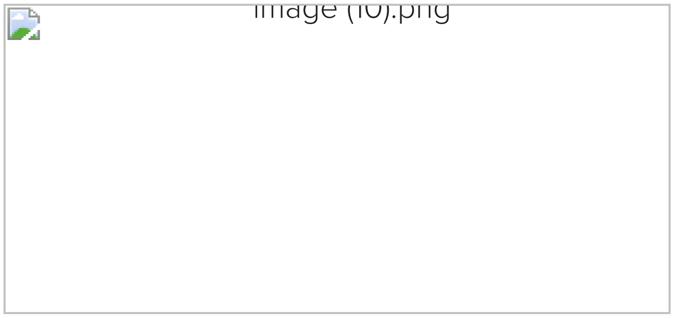
A small example is that of a group of people desiring to compute their average salary, without any individual group member revealing her personal salary to the others or a trusted third party. Using MPC it is possible for them to jointly compute a function which takes as input the secret salary of each group member and reveal only one piece of information: the average of all these (secret) numbers.

SECRET SHARING

One cryptographic tool which allows you to do MPC is secret sharing. Suppose that a secret x=42 is to be shared among two computers. If we choose two random numbers x1 and x2 such that x=x1+x2 (e.g. x1=50 and x2=-8) and give x1 to the first computer and x2 to the

50+"anything" can result in anything. Similarly, we might secret share another number y=23 between the two computers (e.g. y1=20 and y2=3). The two computers can now compute x+y and make the result public, without either computer learning x nor y. The first computer simply computes x1+y1 and sends the result to the computer server, which can then compute x1 + y1 + x2 + y2 = x + y, all of this without any computer learning anything about x nor y, other than the sum.

The interested reader can use these ideas about secret sharing to design a protocol for computing the average salary (the case mentioned above), assuming that the number of group members is public knowledge.



A central result in cryptography is that secret sharing and similar ideas can be extended to allow the computation of any function that a traditional computer can compute. Of course, due to the complexity and distributed nature of this computation, performance is impacted.

There are techniques to mitigate these impacts, but deep MPC protocol knowledge is required to assure that performance is optimized without introducing security vulnerabilities.

THRESHOLD CRYPTOGRAPHY

NIST has initiated projects categorized as “Threshold Cryptography” to reflect that it is possible to build a cryptographic security module based on secret sharing and MPC. Instead of relying on tamper protection of a physical box, we instead rely on strength in numbers.

one share of the key (in the spirit of secret sharing). Furthermore, we use a threshold, T (1 ≤ T ≤ N), so that any T+1 (but no less) shares will allow you to re-construct the key. In other words, as long as an attacker cannot successfully compromise at least T (the threshold) servers, the key is secure.

APPLICATIONS

MPC can be applied to a virtually limitless variety of applications. In practice, the increased computational nature of MPC typically limits application to cases where more resilient and sustainable security or privacy is required, and/or reliance on a central party of trust is either undesirable or unacceptable.

Depending on the particular application, MPC protocols can be designed to operate on virtual servers ranging from mobile phones, personal security and IoT devices, to laptops, physical servers, VMs, containers, or clouds.

Many MPC Alliance member companies, such as Sepior apply MPC and secret sharing for cryptographic key management, encryption and decryption, digital signing, secure statistics, and other functions. Using MPC, a set of virtual servers can, for instance, encrypt a value without seeing this value nor the key used to encrypt it. Similarly, a set of virtual servers can be used by multiple parties to approve a transaction and generate a digital signature without any party every having visibility to a full private key.

Other MPC Alliance member companies use MPC to provide privacy preserving functions such as auctions, predictions, matching, surveys, Machine Learning and more.

FACEBOOK TWITTER PINTEREST 0 LIKES

BANKS READY TO CUSTODY CRYPTOCURRENCIES?

NEXT

WHAT IS WRONG WITH LEGACY ENCRYPTION TOOLS?

Contact Us

Membership

Join our email list

Bylaws