Applications of Secure Multi-Party Computation in Secret Sharing for Tactical Environments

In the previous report we introduced a scheme in which instead of encrypting the data and storing it on a single machine, we break down the data into N pieces in a way that any selection of K pieces is enough to reconstruct the data without imposing any significant overhead on the pieces, which means the total size of the K pieces is virtually equal to the size of the original data. We accomplished this by multiplying the data encoded in a matrix D with K rows by a NxK Vandermonde matrix V in which every row is a geometrical progression; this will result in a matrix M with N rows and each row is a single piece of data in out scheme – i.e, V x D = M. The benefit of the Vandermonde matrix is that any selection of K rows of it creates a non-singular KxK matrix for which an inverse can be easily calculated in a Galois Field; thus, once we have acquired K rows of M, we can calculate the inverse of a Vandermonde matrix V^{-1} with only the equivalent rows as our K pieces, and now by multiplying V^{-1} by M, we will reconstruct D – i.e, V^{-1} x M = V^{-1} x (V x D) = (V^{-1} x V) x D = D [1]. Additionally, this scheme enables us to add new pieces of data as desired; i.e, we can increase N once we have access to at least K pieces, simply by adding a new row to the Vandermonde matrix and multiplying it with the data matrix.

Following the improvements mentioned in the first progress report, namely the ability to reconstruct data with any selection of at least K pieces and to add new unique pieces at any moment, we faced a new challenge in the data reconstruction process. In this progress report we will first explain the problem, then provide a solution using a relatively new branch of Cryptology called secure Multi-Party Computation (MPC). The goal of this field is to create protocols that enable multiple parties to compute a function collectively without having any of them reveal their inputs.

In the previous model, reconstruction of the data required simultaneous access to at least K pieces which requires one machine to carry all of them during the reconstruction process. This, in practice, turns that machine into a point of weakness in the whole system; the reason is that since the person interested in accessing the data may often have to move from point to point and collect the

pieces from different machines until he has enough to reconstruct the data, an adversary can target that specific person in hopes of capturing many pieces all at once. It turns out that if we look at the reconstruction function closely, most of the work can be done using single pieces of data on separate machines, and the only step that needs access to all of the already processed pieces is a single matrix addition operation, for which secure multi-party algorithms already exist [2]. Furthermore, not only the processed pieces do not provide any information about the original piece, but also we improvised the multi-party algorithm in a way that they change depending on the selection and the order of the K pieces. Using this method enables us to keep each piece private while reconstructing the data, so even if an adversary gained access to a set of already processed pieces, it will be effectively useless for him.

[1] Althaus, H.; Leake, R., "Inverse of a finite-field Vandermonde matrix (Corresp.)," Information Theory, IEEE Transactions on , vol.15, no.1, pp.173,173, Jan 1969. doi: 10.1109/TIT.1969.1054253.

[2] Damgård, I.; Cramer, R.; Nielsen, J. B., “Secure Multiparty Computation and Secret Sharing – An Information Theoretic Appoach,” pp. 8, draft.