A Secure and Efficient Two-party Vector Dominance Protocol

Yingpeng SANG
yingpeng@jaist.ac.jp

1 The Aim

There are many applications that require a secure two-party vector dominance protocol (STVD), such as multi-commodity private bidding. The problem of STVD compares two vectors in an “all-or-nothing” way. The two parties should merely know that whether all the elements of one party dominate the corresponding elements of the other party. If there is no such domination, nothing about the relative ordering for any element pair should be disclosed to them. We will firstly give a solution for STVD assuming the two parties are semi-honest to each other, then extend the solution to the malicious case. Security and complexity are also analyzed for both cases. In comparison with the previous work, our solution has advantages of efficiency and security.

2 Solution on the problem

The main idea of our protocol is that we use 0-encoding to reduce STVD to a few cases of the Prefix Testing problem. The protocol also employs cryptographic schemes such as homomorphic encryption, universally composable commitments and zero-knowledge proof.

2.1 Preliminaries

Our construction of STVD protocol is based on a Homomorphic Encryption (HE) scheme. There are a few cryptosystems that satisfy our requirements, and for efficiency we employ ElGamal encryption. We use a (2,2)-threshold variant of ElGamal encryption.

2.2 Building Blocks

2.2.1 0-encoding

For a n-bit integer number $b$ whose binary string is $b_n b_{n-1} ... b_1 \in \{0,1\}^n$, the 0-encoding of $b$ is the set of $S_b^0$ such that

$$S_b^0 = \{1|b_n = 0\} \cup \{b_n b_{n-1} ... b_{i+1} | b_i = 0, n-1 \geq i \geq 1\}$$

2.2.2 Privacy Preserving Prefix Test

Whether $S_b^0$ has a prefix of $a_i$ is a basic problem of STVD. If Alice and Bob want to test whether $b_i^j$ is a prefix of $a_i$ while preserving their privacies on $a_i$ and $b_i^j$, they can follow our protocol of Privacy Preserving Prefix Test.
2.2.3 The Protocol for Semi-honest Case

The main idea of our protocol for STVD is: 1) On every $b_j^i$ in $S_{b_i}^0$ for $1 \leq j \leq K_i$, PPPT is used to get $y_{ij} = E(R_{ij})$, and $y_i = E(\prod_{j=1}^{K_i} R_{ij})$. 2) $Y = \prod_{i=1}^{n} y_i = E(\sum_{i=1}^{n} \prod_{j=1}^{K_i} R_{ij})$ is got. If there is a $R_{ij} = 0$ for all $S_{b_i}^0$ ($1 \leq i \leq n$), then $D(Y) = 1$.

2.2.4 The Protocol for Malicious Case

Our protocol for malicious case forces the two parties to behavior like the protocol for semi-honest case. We add the universal commitment scheme and zero-knowledge proofs to authenticate the computation of every party on every step. In every authentication, the prover needs to convince the verifier that it has done the computation as prescribed by protocol and using the inputs it has committed; otherwise, the verifier will abort the protocol.

3 Progress of 2005

We have provided efficient and secure protocols for the problem of secure two-party vector dominance both in the semi-honest model and malicious model. The problem is reduced to the problem of privacy preserving prefix test. Homomorphic encryption, UC commitments and zero-knowledge proofs are used to protect privacy of the two parties and ensure them to act as what has been prescribed in the protocol.

4 Future directions

How to achieve higher efficiency while keeping the security is a challenging problem for our future work on STVD. We will also look for solutions of other Secure Multi-Party Computation problems in advanced distributed models, such as privacy preserving fuzzy matching in horizontally distributed database.

References

