

SECURE MULTI-PARTY COMPUTATION WITH NO TRUSTED INITIALIZER**ABSTRACT**

Disclosed herein are methods, systems, and apparatus, including computer programs
5 encoded on computer storage media for secure collaborative computation of a matrix product
of a first matrix including private data of a first party and a second matrix including private
data of the second party by secret sharing without a trusted initializer. One method includes
obtaining a first matrix including private data of the first party; generating a first random
matrix; identifying a first sub-matrix and a second sub-matrix of the first random matrix;
10 computing first scrambled private data of the first party based on the first matrix, the first
random matrix, the first sub-matrix, and the second sub-matrix; receiving second scrambled
private data of the second party; computing a first addend of the matrix product; receiving a
second addend of the matrix product; and computing the matrix product by summing the first
addend and the second addend.

15

FIG. 6