

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] The accompanying appendices and/or drawings illustrate various non-limiting, example, innovative aspects in accordance with the present descriptions:

[0007] The leading number of each reference number within the drawings indicates the figure in which that reference number is introduced and/or detailed. As such, a detailed discussion of reference number 101 would be found and/or introduced in Figure 1. Reference number 201 is introduced in Figure 2, etc.

[0008] Figure 1 is a block diagram depicting access by users of an MPEC.

[0009] Figure 2 is a block diagram depicting use of an MPEC for allowing two data owning users to access one another's data.

[0010] Figure 3 is a flowchart depicting an operational scenario using an MPEC.

[0011] Figures 4-6 are block diagrams depicting various processing flows of an MPEC.

[0012] Figures 7-8 depict example computer and software components that can be used with the operations described herein.

SUMMARY

[0012a] According to a first aspect of the present invention, there is provided a method for use within secure multi-party computation, comprising: storing, by one or more data processors, an operation preference including an allowed database operation and a cryptographic preference, which are both associated with a data set; storing, by the one or more data processors, the data set based on the operation preference and the cryptographic preference; analyzing, by the one or more data processors, a query associated with at least the data set; determining, by the one or more data processors, that processing the query involves performing an allowable operation on the data set based on the operation preference selecting, by the one or more data processors, one or more cryptographic protocols based on the first cryptographic preference; and using, by the one or more data processors, the one or more cryptographic protocols to perform the allowable operation on the data set, wherein merchant data owners jointly

process their pooled data to perform transactional data analysis while keeping their respective data private from one another, with a summarized version of the transactional data analysis provided to one of the merchant data owners.

[0012b] According to a second aspect of the present invention, there is provided a system for use within secure multi-party computation, comprising: a memory; and one or more processors disposed in communication with the memory and configured to issue processing instructions stored in the memory to: store, by one or more data processors, an operation preference including an allowed database operation and a cryptographic preference, which are both associated with a data set; store, by the one or more data processors, the data set based on the operation preference and the cryptographic preference; analyze, by the one or more data processors, a query associated with at least the data set; determine, by the one or more data processors, that processing the query involves performing an allowable operation on the data set based on the operation preference; select, by the one or more data processors, one or more cryptographic protocols based on the first cryptographic preference; and use, by the one or more data processors, the one or more cryptographic protocols to perform the allowable operation on the data set, wherein merchant data owners jointly process their pooled data to perform transactional data analysis while keeping their respective data private from one another, with a summarized version of the transactional data analysis provided to one of the merchant data owners.

[0012c] According to a third aspect of the present invention, there is provided a processor-readable non-transitory medium storing processor-issuable instructions to: store, by one or more data processors, an operation preference including an allowed database operation and a cryptographic preference, which are both associated with a data set; store, by the one or more data processors, the data set based on the operation preference and the cryptographic preference; analyze, by the one or more data processors, a query associated with at least the data set; determine, by the one or more data processors, that processing the query involves performing an allowable operation on the data set based on the operation preference; select, by the one or more data processors, one or more cryptographic protocols based on the first cryptographic

preference; and use, by the one or more data processors, the one or more cryptographic protocols to perform the allowable operation on the data set, wherein merchant data owners jointly process their pooled data to perform transactional data analysis while keeping their respective data private from one another, with a summarized version of the transactional data analysis provided to one of the merchant data owners.

[0013] Computer-implemented systems and methods are disclosed herein, such as, for use within secure multi-party computations. For example, a system and method are disclosed for storing preferences. A data set is stored based on the preferences. A determination is made that processing the query involves performing an allowable operation on the data set based on the preferences.

Claims:

1. A method for use within secure multi-party computation, comprising:
 - storing, by one or more data processors, an operation preference including an allowed database operation and a cryptographic preference, which are both associated with a data set;
 - storing, by the one or more data processors, the data set based on the operation preference and the cryptographic preference;
 - analyzing, by the one or more data processors, a query associated with at least the data set; determining, by the one or more data processors, that processing the query involves performing an allowable operation on the data set based on the operation preference;
 - selecting, by the one or more data processors, one or more cryptographic protocols based on the first cryptographic preference; and
 - using, by the one or more data processors, the one or more cryptographic protocols to perform the allowable operation on the data set, wherein merchant data owners jointly process their pooled data to perform transactional data analysis while keeping their respective data private from one another, with a summarized version of the transactional data analysis provided to one of the merchant data owners.
2. The method of claim 1, wherein a centralized database warehouse stores transactional data from multiple merchants and payment service providers.
3. The method of claim 1, wherein the cryptographic preference is selected from a plurality of pre-defined cryptographic protocols.
4. The method of claim 1, wherein the operation preference includes an allowed join operation.
5. The method of claim 1, wherein the operation preference includes an allowed retrieval operation.
6. The method of claim 1, wherein a two tiered system is used where methods which require large in-memory usage for each data element can use distributed files system and methods which require less in-memory usage use in-memory databases.

7. A system for use within secure multi-party computation, comprising:
 - a memory; and
 - one or more processors disposed in communication with the memory and configured to issue processing instructions stored in the memory to:
 - store, by one or more data processors, an operation preference including an allowed database operation and a cryptographic preference, which are both associated with a data set;
 - store, by the one or more data processors, the data set based on the operation preference and the cryptographic preference;
 - analyze, by the one or more data processors, a query associated with at least the data set;
 - determine, by the one or more data processors, that processing the query involves performing an allowable operation on the data set based on the operation preference;
 - select, by the one or more data processors, one or more cryptographic protocols based on the first cryptographic preference; and
 - use, by the one or more data processors, the one or more cryptographic protocols to perform the allowable operation on the data set, wherein merchant data owners jointly process their pooled data to perform transactional data analysis while keeping their respective data private from one another, with a summarized version of the transactional data analysis provided to one of the merchant data owners.
8. The system of claim 7, wherein a centralized database warehouse stores transactional data from multiple merchants and payment service providers.
9. The system of claim 7, wherein the cryptographic preference is selected from a plurality of pre-defined cryptographic protocols.
10. The system of claim 7, wherein the operation preference includes an allowed join operation.
11. The system of claim 7, wherein the operation preference includes an allowed retrieval operation.

12. The system of claim 7, wherein a two tiered system is used where systems which require large in-memory usage for each data element can use distributed files system and systems which require less in-memory usage use in-memory databases.

13. A processor-readable non-transitory medium storing processor-issuable instructions to:
store, by one or more data processors, an operation preference including an allowed database operation and a cryptographic preference, which are both associated with a data set;

store, by the one or more data processors, the data set based on the operation preference and the cryptographic preference;

analyze, by the one or more data processors, a query associated with at least the data set;

determine, by the one or more data processors, that processing the query involves performing an allowable operation on the data set based on the operation preference;

select, by the one or more data processors, one or more cryptographic protocols based on the first cryptographic preference; and

use, by the one or more data processors, the one or more cryptographic protocols to perform the allowable operation on the data set, wherein merchant data owners jointly process their pooled data to perform transactional data analysis while keeping their respective data private from one another, with a summarized version of the transactional data analysis provided to one of the merchant data owners.