International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1770

(10/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Data security – Data protection

Technical guidelines for secure multi-party computation

Recommendation ITU-T X.1770

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	**X.1770–X.1789**
IMT-2020 SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1770

Technical guidelines for secure multi-party computation

Summary

Recommendation ITU-T X.1770 establishes technical guidelines for multi-party computation (MPC) and provides a technical standard basis for information and communication technology (ICT) stakeholders to use MPC to protect data in data collaboration and big data analysis scenarios. It also describes applications for which MPC can be used and how it can serve as a reference for ICT stakeholders to develop MPC applications.

Data has become one of the most important assets in ICT. Secure MPC can build trust and security in data collaboration and big data analysis-related areas by balancing usage and protection of data.

Recommendation ITU-T X.1770 includes:

– a technical framework for MPC, in which its elements and the workflow between them is determined;

– security levels of MPC protocols, used in the analysis and determination of the security model and threshold;

– applications of MPC, illustrated by use cases, including an application scenario description and processes, with appropriate security requirement recommendations.

Based on the framework and security levels established in Recommendation ITU-T X.1770, standards for MPC applications in different fields can be determined.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1770	2021-10-29	17	11.1002/1000/14807

Keywords

MPC, secure multi-party computation, technical guidelines.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

This Recommendation specifies a technical framework and application scenarios of multi-party computation (MPC) to provide guidelines for its use by information and communication technology (ICT) stakeholders for protection of data security.

With the rapid development of mobile Internet, the Internet of things, cloud computing and other information technologies, the amount of data is exploding. Data is a valuable asset and must be protected for various reasons, ranging from legal to national security to industrial competitiveness. A dichotomy exists in that some applications benefit from the sharing of data, while at the same time data should not be shared due to the protection constraints previously mentioned. For example, cybersecurity threat analytics is one example of a type of data that can only be fully utilized through collaborative analysis and integration. However, data collaboration increases the risk of information leakage.

MPC solves the problem of running collaborative processes while protecting data without revealing it. However, most organizations have no idea of how MPC works. So, it is necessary to develop recommendations that systematically determine the MPC framework, and recommend good MPC practices.

Recommendation ITU-T X.1770

Technical guidelines for secure multi-party computation

1 Scope

This Recommendation specifies a technical framework for multi-party computation (MPC), which determines its elements and their roles. Based on the technical framework, typical applications of MPC are presented. Security models and thresholds are analysed to help ICT stakeholders to use different levels of MPC in different scenarios and conditions.

The algorithms and performance details of MPC lie outside the scope of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 multi-party computation (MPC); secure MPC: A subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private.

NOTE – Based on [b-ITU-T F.748.13].

3.2.2 OpenAPI: An initiative or format for creating and designing a standard and a language-agnostic machine-readable interface that can define, consume, visualize and produce web services.

NOTE – [b-OpenAPI] defines OpenAPI as an open-source format that simplifies developing applications by allowing the creation of machine-readable API descriptions.

3.2.3 party: A computer program involving secure multi-party computation.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

GC Garbled Circuit

HE Homomorphic Encryption

MPC Multi-Party Computation

OpenAPI Open Application Programming Interface

OT Oblivious Transfer

SS Secret Sharing

5 Conventions

The word "shall" indicates mandatory requirements strictly to be followed in order to conform to this Recommendation and from which no deviation is permitted ("shall" equals is "required to").

The word "should" indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required ("should" equals is "recommended that").

The word "may" is used to indicate a course of action permissible within the limits of the standard ("may" equals is "permitted to").

The word "can" is used for statements of possibility and capability, whether material, physical or causal ("can" is equal to "able to").

6 Overview

6.1 Introduction of MPC

MPC is a technology that allows a set of parties jointly to compute their data without any information leakage beyond the computation result. It enables big data analysis with less information leakage and more trust and security, and can be used for data protection in many kinds of data collaboration scenarios. An example is the "millionaires' problem", in which two millionaires, Alice and Bob, who are interested in knowing which of them is richer without revealing their actual wealth neither to each other nor to a third party. They make use of MPC to compare the wealth values in encrypted form, when the final output shows who is richer. It is a kind of technology that could build confidence and security in data collaboration and big data analysis. It solves the data protection problem, if implemented properly with proper security controls and proper trust models.

Figure 1 is a schematic diagram of MPC. The ellipses in the centre contain the MPC protocol, which is a virtual party collaboratively run by all the parties. Take a secret auction scenario for example, where bidders do not want others to know their bid price. All bidders input their price to run the MPC protocol together, and receive the name of winner without revealing anybody's price after the computation is finished. The information exchanged during the MPC protocol is encrypted, the participants do not need to tell a third party their price, and no one can get the prices of others. Compared to traditional solutions, MPC is decentralized, and no single trusted third party is required. In this way, trust and security are established between peer-to-peer parties, because no one has privilege.

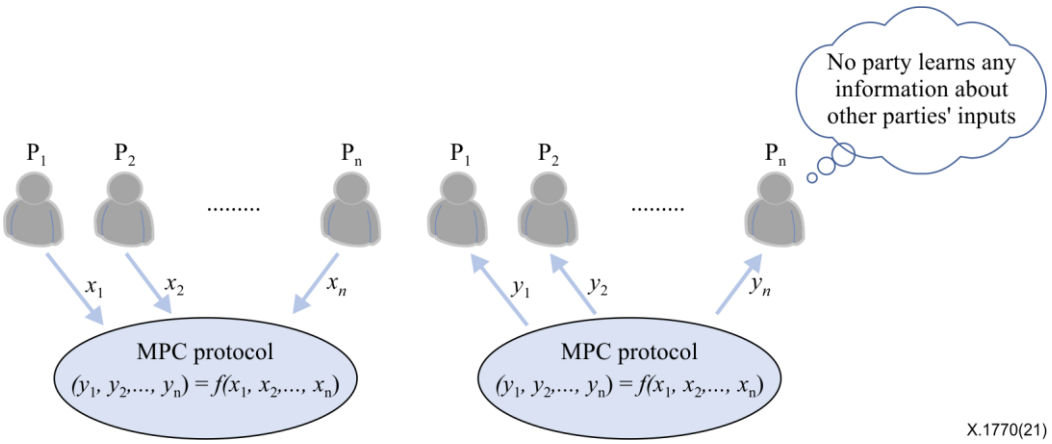

Figure 1 – Schematic diagram of MPC

6.2 Principles of MPC

The principles of MPC should include the following aspects:

1) privacy: an MPC party shall only obtain the output results of the computation that party participated in, and the information derived from its input and output;
2) independence: the input of each party shall be independent of the input of any other party;
3) fairness: any party receives output if and only if other parties receive output.

6.3 Types of MPC party

The types of MPC party are as follows:

1) honest party: a party that follows the exact prespecified protocol, and at the same time keeps his own input(s), the intermediate result(s) and the final output(s) confidential;
2) semi-honest party: a party that follows the exact prespecified protocol, at the same time, that party tries to learn others' input(s), intermediate result(s) and the final output(s);
3) malicious party: a party that executes all steps according to their wishes, not only trying to learn others' inputs, intermediate results and the final outputs, but also intending to modify input(s), outputs or intermediate results owned or received by others.

Semi-honest parties and malicious parties are also referred to as dishonest parties.

7 Technical framework of MPC

7.1 Roles in an MPC system

Multiple roles are involved in an MPC application. Figure 2 shows the roles and their relationships in an MPC system. An MPC party can play multiple roles in an application, e.g., the data provider, computing node and result demander.

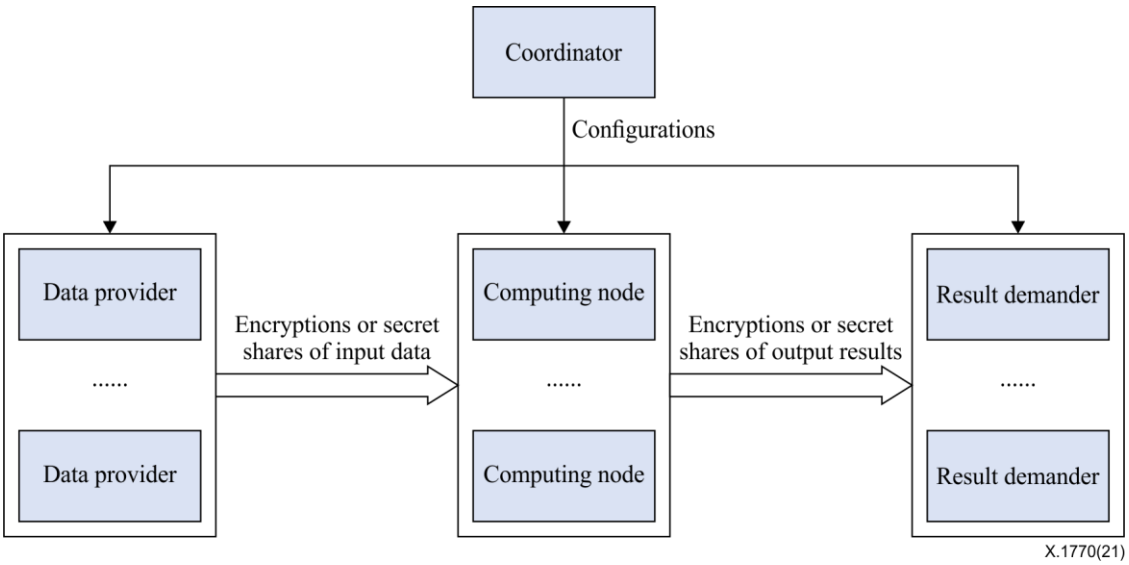

Figure 2 – Roles and their relationships in an MPC system

1) Data provider: a data provider provides its own data as input for an MPC system. There could be more than one data provider in an MPC application. There are two common practices in providing input data as follows.
   a) In a secret-sharing-based MPC system, a data provider generates shares of its input data with a secret sharing (SS) scheme, sends shares to the computing nodes and delegates the subsequent computation to the computing nodes. The MPC party acts as both a data provider and a computing node.
   b) In a homomorphic-encryption-based MPC system, a data provider encrypts its input data with a homomorphic encryption (HE) scheme, sends the encryption to one or more computing nodes.
2) Computing node: while receiving secret shares or encryptions, a computing node performs computations with other computing nodes, coordinated by the coordinator. The computations and communications are predefined in the MPC system. In a secret-sharing-based MPC system, there should be at least two computing nodes controlled by different MPC parties. In an HE-based MPC system, there should be two or more computing nodes, and they may be controlled by one or more MPC parties or even third parties.
3) Result demander: a result demander receives its result from the outputs of computing nodes. There could be one or more result demanders in an MPC system, and their results may be different.
4) Coordinator: the coordinator is responsible for managing and coordinating multiple parties to complete the MPC computation. The configuration information usually includes the IP address, port and other information of multiple parties. A coordinator is not necessary in an MPC system. There is usually only one coordinator in an MPC application.

7.2 Technical framework of an MPC system

Figure 3 shows a technical framework of an MPC system. Not all participants should deploy all functions in the technical framework. For example, if a participant only acts as a coordinator, it can only deploy a coordination function; if a participant acts as data provider, computing node and result demander, it should provide storage, MPC protocol, MPC function and application functions.

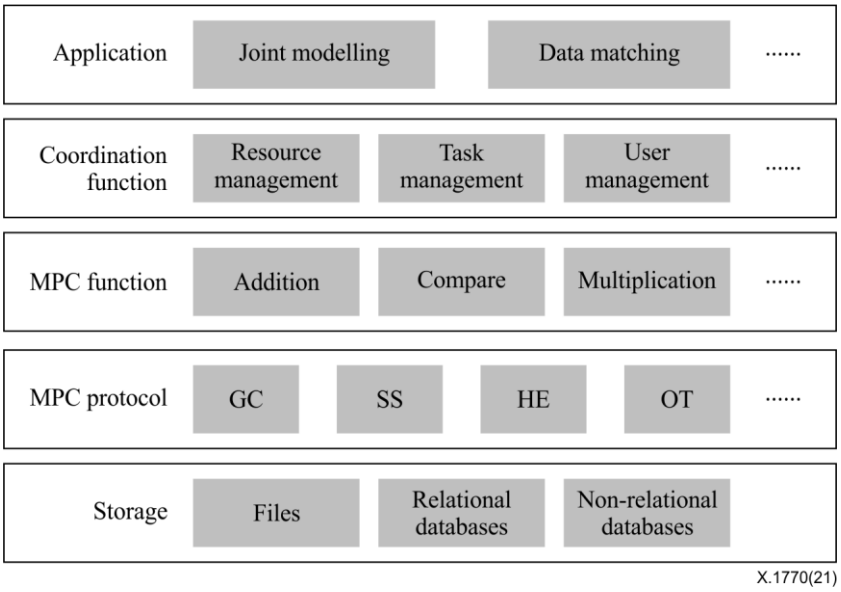

Figure 3 – Technical framework of an MPC system

7.2.1 Application

MPC can be used in financial, health, advertising and other industries on joint modelling, data matching, etc.

1) User interaction interfaces should be provided, such as web pages, command lines or OpenAPI.

2) Decrypt functions that change the encrypted results into plain text should be provided.

7.2.2 Coordination function

The coordination function is responsible for scheduling and managing various resources to complete MPC tasks.

1) Resource management should be able to identify and present the computing node information and data resource related information. Computing node information includes IP address, port, and running status. Data resource related information includes size and type.

2) Task management should include creation, assignment and status monitoring of tasks.

3) User management should include user authentication and authority management.

7.2.3 MPC function

The MPC function provides basic operations based on encrypted data.

1) Common numerical computation should be provided, such as addition, multiplication and comparison.

2) Basic data types, including integers, decimals, common characters and strings, should be supported;

3) Basic data units, such as scalars, vectors, matrices and multidimensional arrays, should be supported.

7.2.4 MPC protocol

The MPC protocol is the key underlying component for an MPC system.

1) An MPC system should include at least one kind of MPC protocol. The protocols may belong to one or a combination of the following subtypes (non-exhaustive list) based on: SS; garbled circuit (GC); HE; etc.

2) Computation nodes use the MPC protocol to exchange information and jointly complete computation tasks.

3) The MPC protocols used in an MPC system should at least satisfy a security level of A1C1 as described in clause 8.

7.2.5 Storage

Storage provides the original input data in MPC system.

1) Storage should include files, relational databases and non-relational databases.

2) Database should include MySQL, Oracle, Hive and HBase.

3) File types should include txt, csv, and xml.

7.3 Process flows of an MPC task

Figure 4 shows the process flows of an MPC task. The detailed flows are described as follows:

1) the coordinator generates the configuration information (including specific MPC protocols and IP address) according to the task and sends it to the data providers and computing nodes;

2) the data providers process the input data according to the specified MPC protocols and send it to the designated computing nodes through the secure transmission channel;

3) computing nodes collaboratively carry out the computation on input data according to the MPC functions and specified MPC protocols;

4) computing nodes send the computation result to each result demander at the same time.

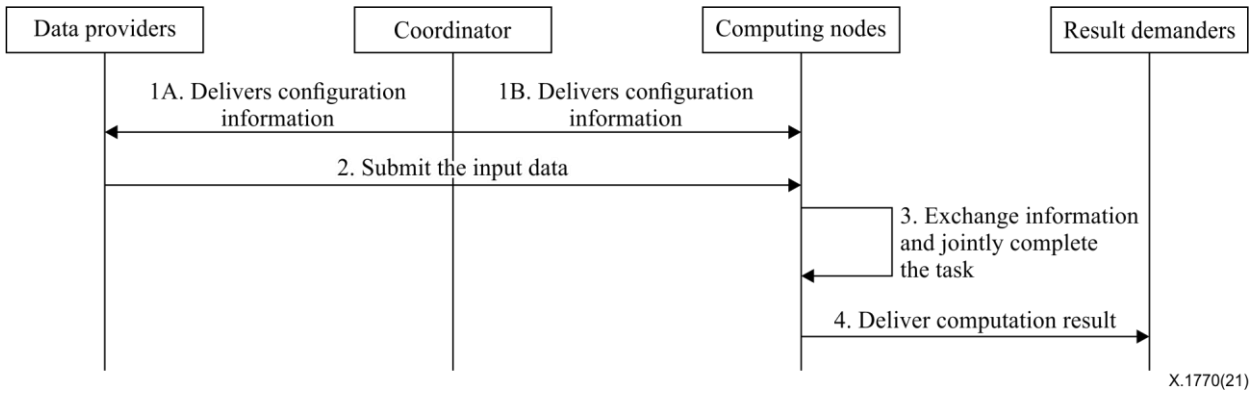

Figure 4 – Process flows of an MPC task

7.4 Recommended protections for an MPC system

7.4.1 Authentication

The authentication for an MPC system includes, but is not limited to:

1) identity authentication for parties who can access the MPC system;

2) multi-factor authentication mechanisms, e.g., password verification, mailbox verification, SMS verification and digital certification;

3) mutual authentication between different components of an MPC system, such as computing nodes controlled by different parties.

7.4.2 Access control

The access control for an MPC system includes, but is not limited to:

1) fine-grained system access control for different user roles;

2) re-authentication or re-activation of a session when it is idle for a period;

3) the encrypted data provided by data provider only be sent to the designated.

7.4.3 Data security

The data security requirements for an MPC system include, but are not limited to:

1) supporting secure transmission protocols or channels to ensure the security and reliability of the data transmission links;

2) supporting multiple data destruction or clean-up methods.

8 Security levels of an MPC protocol

Security model and threshold are the two most important factors when the security level of an MPC protocol should be considered.

8.1 Security model

8.1.1 A1: Semi-honest model

If the MPC protocol can achieve input privacy, output correctness and output delivery against semi-honest parties, it satisfies the semi-honest security model.

Input privacy means that none of the participating parties can learn any information beyond the computation result.

Output correctness means that the results output in the MPC manner are lossless compared to the results output in a common manner.

Output delivery means honest parties always obtain their output result whatever the dishonest parties do. In another words, dishonest parties cannot prevent honest parties from receiving their output result.

8.1.2 A2: Covert model

If the MPC protocol can achieve input privacy and output correctness (if output is delivered) against covert parties, it satisfies the covert security model. A covert party will behave maliciously just like a malicious party, but if the probability that the malicious behaviours get caught by the honest parties exceeds a certain threshold, then the covert party will follow the protocol for fear of being caught.

8.1.3 A3: Malicious model

If the MPC protocol can achieve input privacy and output correctness (if output is delivered) against malicious parties, it satisfies the malicious security model.

8.2 Security threshold

8.2.1 C1: Honest majority

Honest majority means less than half of MPC parties may be corrupted. If the MPC protocol can achieve input privacy and output correctness in an honest majority system, it is secure under the honest majority security threshold. An MPC system shall satisfy the C1 threshold at least.

8.2.2 C2: Dishonest majority

Dishonest majority means half or more of MPC parties may be corrupted. If the MPC protocol can achieve input privacy and output correctness in a dishonest majority system, it is secure under the dishonest majority security threshold. If an MPC system satisfies the C2 threshold, it means the system has stronger ability to prevent the security risks caused by corrupted MPC parties.

9 Applications of MPC

9.1 Joint modelling

Loan is a business in the financial field. Data from multiple banks or data from related financial organizations are used to evaluate the credit of the loan applicant to improve the accuracy of the evaluation results. An MPC-based machine-learning system can achieve credit joint risk control. And make loan decisions according to the result of risk control.

Figure 5 shows an MPC-based machine-learning system that can be used in credit joint risk control. The system is composed of a model-controlling platform and multiple banks as data providers. The model-controlling platform mainly includes a control module to trigger and coordinate different parties participating in machine-learning tasks. The model-controlling platform may belong to bank A, bank B or the third party. In the last case, the third party cannot get any input data, but only configuration information. Each data provider deploys a learning module locally and transmits data to a local learning module. Learning modules among different data providers exchange parameters or random numbers by using MPC protocols to achieve data sharing in order to maintain data privacy.

The MPC protocols used in a financial application should at least satisfy a security level of A1C2 as described in clause 8.

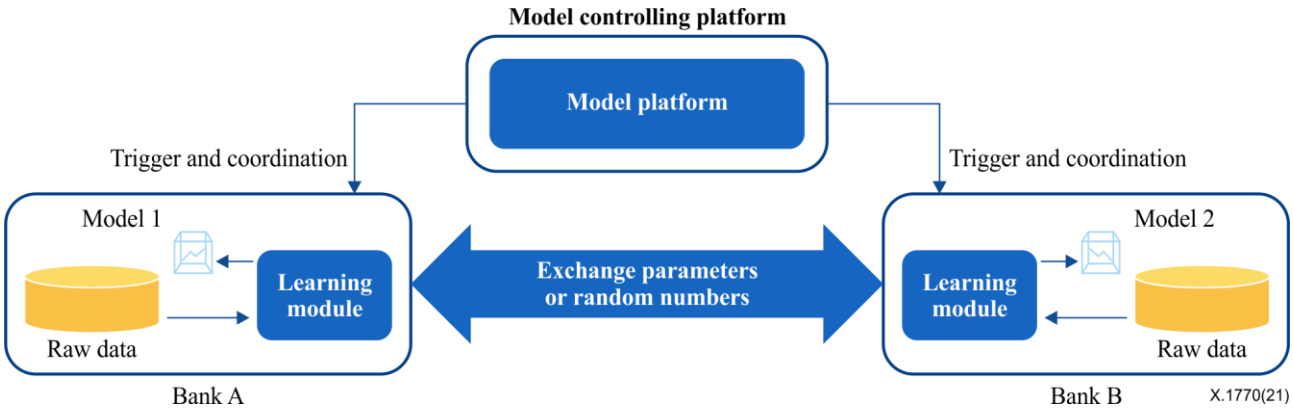

Figure 5 – MPC-based machine-learning system

9.2 Data matching

Figure 6 shows an application of MPC used in data matching. Suppose A is a book vendor, B is a movie vendor, A and B each have some registered user accounts (e.g., registered with e-mail). Now A wants to figure out the number of mutual users they both have, so that A and B can do some sales promotion together. B is willing to help, but does not want to reveal anything (such as who the mutual users are) beyond the number of mutual users for user privacy, neither does A.

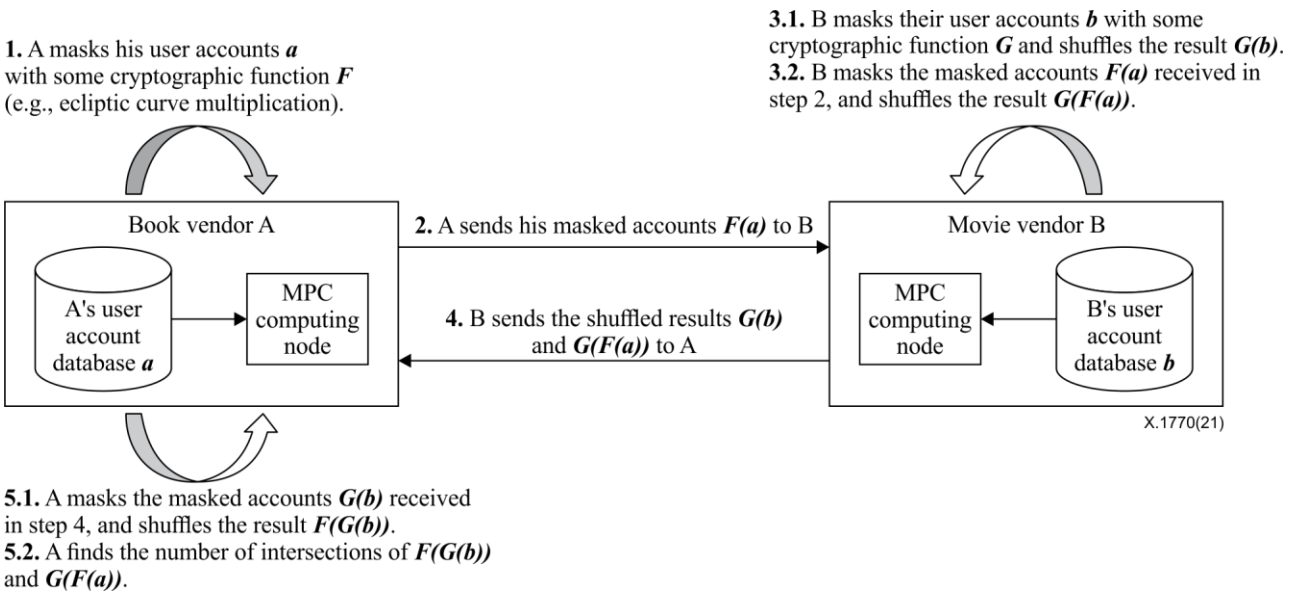

Figure 6 – MPC used in data matching

In this application, an MPC computing node is deployed in A and B exchange user accounts by using MPC protocols to share data in order to keep data privacy. A and B agree on some cryptographic mask functions such as multiplication on some elliptic curve, and each deploys a machine in their own domain to act as the computing node. A first masks A's user accounts and sends them to B, which then masks B's accounts and A's masked accounts. Note that in order to make the results unlinkable, B shuffles the results randomly before sending them back to A. As long as the two mask functions F and G are swappable, A could find the number of mutual users by computing the intersection of $F(G(b))$ and $G(F(a))$. Since the order of the lists has been randomly shuffled by B, A cannot know who the mutual users are.

The MPC protocols used in a user account-matching application should at least satisfy a security level of A1C1 as described in clause 8.

Bibliography

[b-ITU-T F.748.13] Recommendation ITU-T F.748.13 (2021), *Technical framework for the shared machine learning system.*

[b-OpenAPI] APITransform (2020). *What is OpenAPI specification?* Available [viewed 2021-11-16] at: https://apitransform.com/what-is-open-api-specification/

[b-ISO/IEC 4922-1] ISO/IEC 4922-1, *Information Security – Secure multiparty computation – Part 1: General*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021