Title: Sample records for multi-party computation protocol

Abstract: This document includes selected research summaries sourced from Science.gov, a U.S. government portal that aggregates scientific publications from multiple federal agencies and research databases, including sources such as NASA Astrophysics Data System and PubMed. The included records focus on advancements in secure multi-party computation (SMC) and related cryptographic protocols, covering topics such as quantum-based protocols, privacy-preserving set intersection, key agreement schemes, and secure communication frameworks for applications in finance, healthcare, defense, and distributed systems. These summaries are presented for informational and research purposes, reflecting aggregated findings from publicly available scientific literature indexed by Science.gov.

1. Two Quantum Protocols for Oblivious Set-member Decision Problem

   NASA Astrophysics Data System (ADS)

   Shi, Run-Hua; Mu, Yi; Zhong, Hong; Cui, Jie; Zhang, Shun

   2015-10-01

   In this paper, we defined a new secure multi-party computation problem, called Oblivious Set-member Decision problem, which party to decide whether a secret of another party belongs to his private set in an oblivious manner. There are lots of important of Oblivious Set-member Decision problem in fields of the multi-party collaborative computation of protecting the privacy of the such as private set intersection and union, anonymous authentication, electronic voting and electronic auction. Furthermore, w presented two quantum protocols to solve the Oblivious Set-member Decision problem. Protocol I takes advantage of powerfu oracle operations so that it needs lower costs in both communication and computation complexity; while Protocol II takes phot quantum resources and only performs simple single-particle projective measurements, thus it is more feasible with the present technology.

2. Two Quantum Protocols for Oblivious Set-member Decision Problem

   PubMed Central

   Shi, Run-hua; Mu, Yi; Zhong, Hong; Cui, Jie; Zhang, Shun

   2015-01-01

   In this paper, we defined a new secure multi-party computation problem, called Oblivious Set-member Decision problem, which party to decide whether a secret of another party belongs to his private set in an oblivious manner. There are lots of important of Oblivious Set-member Decision problem in fields of the multi-party collaborative computation of protecting the privacy of the such as private set intersection and union, anonymous authentication, electronic voting and electronic auction. Furthermore, w presented two quantum protocols to solve the Oblivious Set-member Decision problem. Protocol I takes advantage of powerfu oracle operations so that it needs lower costs in both communication and computation complexity; while Protocol II takes phot quantum resources and only performs simple single-particle projective measurements, thus it is more feasible with the present technology. PMID:26514668

3. Two Quantum Protocols for Oblivious Set-member Decision Problem.

   PubMed

   Shi, Run-Hua; Mu, Yi; Zhong, Hong; Cui, Jie; Zhang, Shun

   2015-10-30

   In this paper, we defined a new secure multi-party computation problem, called Oblivious Set-member Decision problem, which party to decide whether a secret of another party belongs to his private set in an oblivious manner. There are lots of important of Oblivious Set-member Decision problem in fields of the multi-party collaborative computation of protecting the privacy of the

such as private set intersection and union, anonymous authentication, electronic voting and electronic auction. Furthermore, w
presented two quantum protocols to solve the Oblivious Set-member Decision problem. Protocol I takes advantage of powerfu
oracle operations so that it needs lower costs in both communication and computation complexity; while Protocol II takes phot
quantum resources and only performs simple single-particle projective measurements, thus it is more feasible with the present
technology.

4. Multi-party quantum summation without a trusted third party based on single particles

   NASA Astrophysics Data System (ADS)

   Zhang, Cai; Situ, Haozhen; Huang, Qiong; Yang, Pingle

   We propose multi-party quantum summation protocols based on single particles, in which participants are allowed to compute
   summation of their inputs without the help of a trusted third party and preserve the privacy of their inputs. Only one participan
   generates the source particles needs to perform unitary operations and only single particles are needed in the beginning of the

5. Multi-Party Privacy-Preserving Set Intersection with Quasi-Linear Complexity

   NASA Astrophysics Data System (ADS)

   Cheon, Jung Hee; Jarecki, Stanislaw; Seo, Jae Hong

   Secure computation of the set intersection functionality allows n parties to find the intersection between their datasets without
   anything else about them. An efficient protocol for such a task could have multiple potential applications in commerce, health c
   security. However, all currently known secure set intersection protocols for n>2 parties have computational costs that are quad
   (maximum) number of entries in the dataset contributed by each party, making secure computation of the set intersection only
   for small datasets. In this paper, we describe the first multi-party protocol for securely computing the set intersection functiona
   both the communication and the computation costs that are quasi-linear in the size of the datasets. For a fixed security parame
   protocols require O(n2k) bits of communication and Ã•(n2k) group multiplications per player in the malicious adversary setting,
   the size of each dataset. Our protocol follows the basic idea of the protocol proposed by Kissner and Song, but we gain efficien
   different representations of the polynomials associated with users' datasets and careful employment of algorithms that interpo
   evaluate polynomials on multiple points more efficiently. Moreover, the proposed protocol is robust. This means that the proto
   the desired result even if some corrupted players leave during the execution of the protocol.

6. Multi-party Semi-quantum Key Agreement with Delegating Quantum Computation

   NASA Astrophysics Data System (ADS)

   Liu, Wen-Jie; Chen, Zhen-Yu; Ji, Sai; Wang, Hai-Bin; Zhang, Jun

   2017-10-01

   A multi-party semi-quantum key agreement (SQKA) protocol based on delegating quantum computation (DQC) model is propos
   Bell states as quantum resources. In the proposed protocol, the participants only need the ability of accessing quantum channe
   preparing single photons {|‰ã‚€|1ã‰‰, |+ã€‰, |-ã€‰}, while the complicated quantum operations, such as the unitary operations
   Bell measurement, will be delegated to the remote quantum center. Compared with previous quantum key agreement protoco
   client-server model is more feasible in the early days of the emergence of quantum computers. In order to prevent the attacks
   outside eavesdroppers, inner participants and quantum center, two single photon sequences are randomly inserted into Bell st
   first sequence is used to perform the quantum channel detection, while the second is applied to disorder the positions of mess
   which guarantees the security of the protocol.

7. Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing

   NASA Astrophysics Data System (ADS)

   Yu, Kun-Fei; Gu, Jun; Hwang, Tzonelih; Gope, Prosanta

   2017-08-01

   This paper proposes a multi-party semi-quantum secret sharing (MSQSS) protocol which allows a quantum party (manager) to s
   secret among several classical parties (agents) based on GHZ-like states. By utilizing the special properties of GHZ-like states, th
   proposed scheme can easily detect outside eavesdropping attacks and has the highest qubit efficiency among the existing MSQ
   protocols. Then, we illustrate an efficient way to convert the proposed MSQSS protocol into a multi-party semi-quantum key dis

(MSQKD) protocol. The proposed approach is even useful to convert all the existing measure-resend type of semi-quantum secr protocols into semi-quantum key distribution protocols.

8. Secured Communication for Business Process Outsourcing Using Optimized Arithmetic Cryptography Protocol Based on Virtua

   NASA Astrophysics Data System (ADS)

   Pathak, Rohit; Joshi, Satyadhar

   Within a span of over a decade, India has become one of the most favored destinations across the world for Business Process O (BPO) operations. India has rapidly achieved the status of being the most preferred destination for BPO for companies located and Europe. Security and privacy are the two major issues needed to be addressed by the Indian software industry to have an i and long-term outsourcing contract from the US. Another important issue is about sharing employeeâ€™s information to ensu and vital information of an outsourcing company is secured and protected. To ensure that the confidentiality of a clientâ€™s inf maintained, BPOs need to implement some data security measures. In this paper, we propose a new protocol for specifically fo Secure Multi-Party Computation (SMC). As there are many computations and surveys which involve confidential data from many organizations and the concerned data is property of the organization, preservation and security of this data is of prime importa such type of computations. Although the computation requires data from all the parties, but none of the associated parties wou reveal their data to the other parties. We have proposed a new efficient and scalable protocol to perform computation on encry information. The information is encrypted in a manner that it does not affect the result of the computation. It uses modifier tok are distributed among virtual parties, and finally used in the computation. The computation function uses the acquired data an tokens to compute right result from the encrypted data. Thus without revealing the data, right result can be computed and priv parties is maintained. We have given a probabilistic security analysis of hacking the protocol and shown how zero hacking secu achieved. Also we have analyzed the specific case of Indian BPO.

9. Secure Multi-party Computation Protocol for Defense Applications in Military Operations Using Virtual Cryptography

   NASA Astrophysics Data System (ADS)

   Pathak, Rohit; Joshi, Satyadhar

   With the advent into the 20th century whole world has been facing the common dilemma of Terrorism. The suicide attacks on U towers 11 Sept. 2001, Train bombings in Madrid Spain 11 Mar. 2004, London bombings 7 Jul. 2005 and Mumbai attack 26 Nov. 2 some of the most disturbing, destructive and evil acts by terrorists in the last decade which has clearly shown their evil intent th go to any extent to accomplish their goals. Many terrorist organizations such as al Quaida, Harakat ul-Mujahidin, Hezbollah, Jais Mohammed, Lashkar-e-Toiba, etc. are carrying out training camps and terrorist operations which are accompanied with latest t and high tech arsenal. To counter such terrorism our military is in need of advanced defense technology. One of the major issu concern is secure communication. It has to be made sure that communication between different military forces is secure so tha information is not leaked to the adversary. Military forces need secure communication to shield their confidential data from ter forces. Leakage of concerned data can prove hazardous, thus preservation and security is of prime importance. There may be a perform computations that require data from many military forces, but in some cases the associated forces would not want to data to other forces. In such situations Secure Multi-party Computations find their application. In this paper, we propose a new scalable Secure Multi-party Computation (SMC) protocol and algorithm for Defense applications which can be used to perform computation on encrypted data. Every party encrypts their data in accordance with a particular scheme. This encrypted data is among some created virtual parties. These Virtual parties send their data to the TTP through an Anonymizer layer. TTP perform computation on encrypted data and announces the result. As the data sent was encrypted its actual value canâ€™t be known by with the use of Anonymizers we have covered the identity of true source of data. Modifier tokens are generated along encryptio which are distributed among virtual parties, then sent to TTP and finally used in the computation. Thus without revealing the da result can be computed and privacy of the parties is maintained. We have also given a probabilistic security analysis of hacking protocol and shown how zero hacking security can be achieved.

10. Novel Multi-Party Quantum Key Agreement Protocol with G-Like States and Bell States

    NASA Astrophysics Data System (ADS)

    Min, Shi-Qi; Chen, Hua-Ying; Gong, Li-Hua

    2018-03-01

    A significant aspect of quantum cryptography is quantum key agreement (QKA), which ensures the security of key agreement p quantum information theory. The fairness of an absolute security multi-party quantum key agreement (MQKA) protocol deman participants can affect the protocol result equally so as to establish a shared key and that nobody can determine the shared key