ABSTRACT

Adaptive oblivious transfer (AOT) is a basic building block for secure multiparty computation and adaptive oblivious search of large database such as medical, financial, patent etc. AOT involves two parties– a sender and a receiver. The sender holds N secret information. The receiver wants to retrieve k out of N secret information without disclosing which k of them. The receiver is oblivious to other $N-k$ secret information, and the sender does not learn anything about which k secret information are learnt by the receiver. AOT completes in one initialization phase and k transfer phases. In initialization phase, the sender encrypts N secret information using some encryption scheme and publishes them. In each transfer phase, the receiver interacts with the sender and recovers the desired secret information. In this thesis, two efficient constructions of AOT protocols are presented. The proposed constructions utilize all the components of the ciphertexts during protocol execution in comparison to existing similar schemes in which some components of the ciphertext are used during simulation only. More interestingly, our first scheme achieves an extra feature which facilitates the receiver to verify the correctness of message recovered at the end of each transfer phase. Our second scheme is free form q-type assumptions.

Furthermore, *adaptive oblivious transfer with access policy* (AOT-AP) and *adaptive oblivious transfer with hidden access policy* (AOT-HAP) are studied. AOT-AP and AOT-HAP are widely used primitive to create privacy preserving databases in which each secret information is associated with an access policy, expressed in terms of attributes, roles, or rights that a receiver should have to access the secret information. Unlike AOT-AP, the access policies are kept hidden in AOT-HAP. AOT-AP and AOT-HAP are capable of restricting the unauthorized receivers to access the secret information. Authorized receivers possess an attribute set and can access secret information only if attribute set satisfy the access policy associated with the secret information. AOT-AP and AOT-HAP assume a trusted third party called *issuer*. The issuer generates attribute secret keys corresponding to the attribute sets of the receivers. The security analysis of AOT-AP and AOT-HAP is done under the restriction that the issuer never colludes with a set of receivers while no such restriction is required in *issuer-free* AOT-AP and *issuer-free* AOT-HAP which are also presented in this work.

Lastly, we design a *priced oblivious transfer* (POT) with rechargeable wallet in which each secret information (digital item) is associated with a price. POT with rechargeable wallet is extensively used in e-commerce, and it is run between a sender and multiple customers in which customers anonymously purchase digital items from the sender.

All the proposed constructions except AOT-HAP are universally composable (UC) secure under standard cryptographic assumptions assuming static corruption model in the presence of malicious adversary, who does not follow the protocol specification. In static corruption model, it is pre-decided by the adversary to whom it wants to corrupts before the execution of the protocol. The strength of the UC framework relies on the universal composable theorem which states that if a protocol is secure in UC framework, then this protocol remains secure even if composed with itself or with other protocols during concurrent execution. Computation and communication complexity of the proposed protocols are also discussed. The proposed constructions exhibit significant computation and communication efficiency as compared to existing similar schemes in literature.

Keywords: Oblivious Transfer; Universal Composable Security; Access Policy; Non-Interactive Zero-Knowledge Proofs; Attribute Based Encryption.