論文内容の要旨

論文題目

The Design and Analysis of Secure Communication Systems Distributed Over Broadcast Channels

(放送型通信を利用した安全な通信システムの設計との解析)

氏名　　タニグチ エリオット タダシ

In this thesis, three main cryptographic schemes are proposed which utilize general broadcast channels. In each of these schemes, broadcast channels will the used to improve communication efficiency, anonymity, and deniability where appropriate. The first scheme focuses on improving the efficiency of mass communication using broadcast encryption over hierarchal service sets. Broadcast encryption involves securely sending an encrypted message over a broadcast channel such that only members of a dynamic user set can decode this message. The second scheme allows an arbitrary set of users to generate a common group key or private key with member remaining anonymous within this user set. The final scheme is a novel general auction scheme that allows the auction results to be deniable by the auctioneer. This ensures that the provability of all notifications send by the auctioneer stay contained within the set of register members.

The first chapter introduces the structure of the thesis, motivations for the proposed research, and outlines the major contributions of the thesis to the audience. The overlying theme of the thesis is that utilizing broadcast channels allows for very efficient one-to-many mass communication and also allows for natural verification since all information transmitted is publicly broadcasted. Using broadcast channels, key management schemes and deniability preserving communication systems can be improved and extended. Figure 1 below shows how each of the three proposed schemes related to thesis.

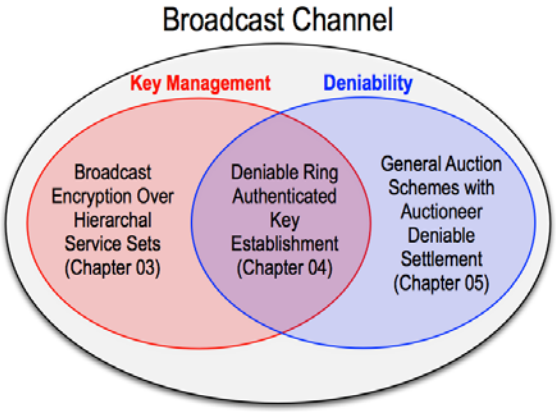

Figure 1 : Thesis Overview

The second chapter introduces the audience to the main mathematical tools and the cryptographic primitives or tools used in the subsequent chapters. The first half of the chapter focuses mainly on algebraic groups of prime finite size and Fermat's Little Theorem is also derived. The second half of the chapter introduces many of the cryptographic tools – hash functions, public-key encryption, digital signatures, and zero-knowledge proofs – used to build more complicated communication system in later chapters.

The third chapter focuses on broadcast encryption schemes that attempt to efficiently and securely send a single message to a single dynamic group of user (non-revoked user set). Only users in the non-revoked user set have the capability to decrypt the ciphertext sent over a broadcast channel. By modifying the Chick-Tavares Key Management Scheme, the proposed broadcast encryption scheme improves bandwidth and memory efficiency in the general case with multiple messages and multiple non-revoked user sets. This proposed scheme also preserves forward compatibility while simultaneously maintaining forward and backwards security. Lastly, the proposed scheme is general enough to accommodate both stateless and non-stateless receivers.

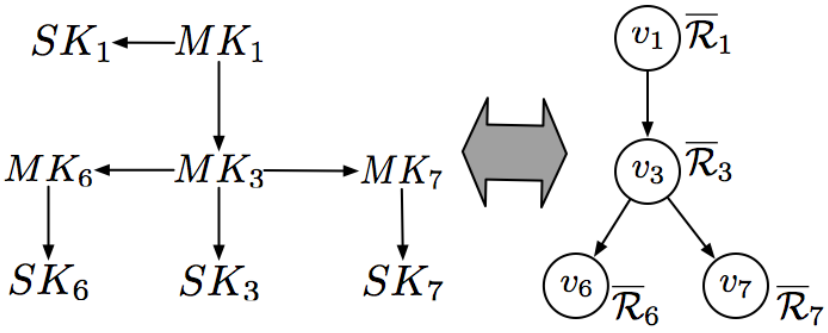

Figure 2 : Master Key and Service Key Relationship

In chapter 4, a deniable group/private key establishment scheme is proposed. This proposed deniable key establishment scheme allows both the initiator (Alice) and potential multiple recipients (Bob) to generate either a deniable group key or a deniable private key. Alice wishes to remain anonymous throughout the process and similarly Bob would also wish to remain anonymous. However, Alice wants to ensure that the anonymous

counterparty is someone within her target group of counterparties.

The scheme proposed in this thesis modifies Naor's ring authentication scheme to include group and private key establishment. Group key establishment generates a common key computable by all members in the user set S. On the other hand, private key establishment generates a private key computable by only two members – Alice and (single) Bob.

In addition, two protocols were proposed with differing levels of anonymity for Alice shown in Fig. 3. The strongly anonymous initiator protocol (SAIP) allows Alice to remain perfectly anonymous since there are no restrictions on her being within or outside user set S. The weakly anonymous initiator protocol (WAIP) forces Alice to choose a target user set S such that Alice is also in that set.

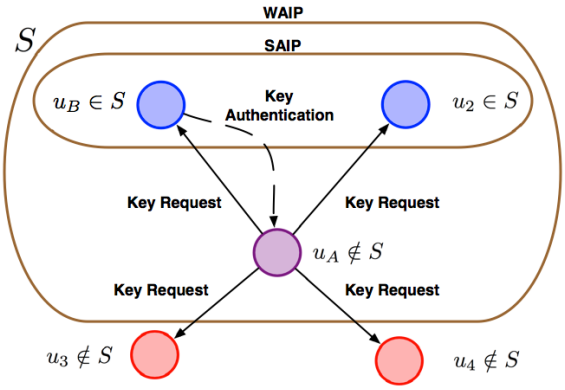

Figure 3 : SAIP and WAIP

In chapter 5, two main auctioneer-deniable single-item auctions are proposed. This proposed auction scheme satisfies many of the common auction properties such as bidder anonymity, non-repudiation by the bidder, traceability, non-forgeable, bidder fairness, public verifiability, linkable during the auction, and non-linkable over multiple auctions. In addition, the proposed auction scheme will also ensure that the winning bid notification issued by the auctioneer will satisfy two goals. First, all registered members of the auction will be completely verifiable and convinced of any notification from the auctioneer. Second, this provability and verifiability will be limited to only registered members of the auction. This condition prevents any registered member from selling or profiting from the auction results.

The proposed auction schemes are divided into two main groups – open-price auctions and sealed-bid auctions – shown in Fig. 4. For the open-price auction case, a deniable English Auction (Ascending Price Auction) is proposed for each subsequent bid must be higher than the previous highest bid to be accepted by the auctioneer. For the sealed-bid auction case, a deniable first-price sealed-bid auction scheme is also proposed where all bids are privately tallied (one bid per member) and the highest bid is announced.

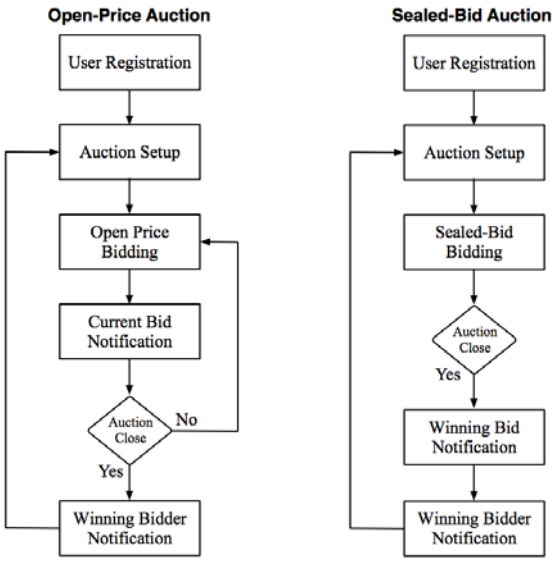

Figure 4 : Algorithm Flow of Open-Price and Sealed-Bid Auctions

Finally, each of the research contributions presented in this thesis is summarized and future areas of research are identified. The thesis contributions include improving existing broadcast encryption systems to incorporate general hierarchal service sets. Next, various deniable key establishment protocols were proposed for both the SAIP and WAIP cases. Finally, a novel general auction scheme with auctioneer deniable settlement is proposed.