ABSTRACT

Nowadays, the success of many online applications relays on keeping the data sent through the global networks secure and far away from hackers. To carry out this task, the two communicating parties must exchange keys during their session. Some of key exchange protocols are called key agreement protocols. The Elliptic Curve-Diffie Hellman (ECDH) is one of the most efficient algorithms for securing data. The ECDH is more efficient than other traditional techniques (such as Rivest-Shamir-Adleman (RSA)) in terms of key size, computation and network bandwidth. The Authenticated Key Agreement (AKA) protocol is used for establishing a common session key between the two communicating parties. The common session key is used for subsequent cryptography goals. Most of the key agreement protocols (e.g. Menezes-Qu–Vanstone (MQV) family) generate one key per session therefore increasing the opportunities for guessing the session key. The YAK protocol (as a robust key agreement based on public key authentication) is a variant of the two-pass HMQV protocol, but uses zero-knowledge proofs for proving knowledge of ephemeral values. The YAK protocol lacks joint key control and perfect forward secrecy attributes, and is vulnerable to some attacks including unknown key-share and key-replication attacks. This invalidates the semantic security of the protocol in several security models. There are also other considerations regarding the impersonation and small subgroup attacks.

In this thesis, we focused on developing an enhanced multiple sessions key which is based on ECDH. We propose an efficient and secure AKA protocol which is based on the ideas of the hashed MQV (HMQV), the YAK protocol and multiple session keys.

The proposed protocol differs from other protocols (YAK, MQV and HMQV) in that it produces multiple session keys in one session and thus making it hard for hackers

to guess the session keys. In addition, the results from the Scyther simulator showed that proposed protocol provided Perfect Forward Secrecy (PFS), whereas the other protocols (MQV, HMQV and YAK) did not. Also, the result from Scyther simulator showed that the proposed protocol is proofed to be secure against the Unknown Key Share (UKS), Key Compromise Impersonation (KCI-R) and the extended Canetti–Krawczyk (eCK) attacks, whereas the other protocols (MQV, HMQV and YAK) are not vulnerable against them. Finally, the proposed protocol provided a digital signature feature which validates the authenticity and integrity of a digital message based on image identity algorithm and hashing technique, whereas the other protocols leakage this feature. Beside that the result showed that the proposed protocol is not vulnerable against the Known Key Security (KKS-R) attack, but the MQV is vulnerable against it. However, the result from this thesis showed that the number of Point Multiplication (PM) of the proposed protocol is higher than the PM in the related works. Since, in the related works, there is only one session key produced while in the proposed protocol there are nine session keys produced.