A Diffie-Hellman Key Exchange Protocol Without Random Oracles

Ik Rae Jeong[1], Jeong Ok Kwon[2,⋆], and Dong Hoon Lee[2,⋆]

[1] Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea
jir@etri.re.kr
[2] Center for Information Security Technologies (CIST), Korea University, Seoul, Korea
{pitapat, dhlee}@korea.ac.kr

Abstract. The MQV protocol of Law, Menezes, Qu, Slinas and Vanstone has been regarded as the most efficient authenticated Diffie-Hellman key exchange protocol, and standardized by many organizations including the US NSA. In Crypto 2005, Hugo Krawczyk showed vulnerabilities of MQV to several attacks and suggested a hashed variant of MQV, called HMQV, which provides the same superb performance of MQV and provable security in the random oracle model. In this paper we suggest an efficient authenticated Diffie-Hellman key exchange protocol providing the same functionalities and security of HMQV *without* random oracles. There exist some provably secure key exchange schemes using signatures in the standard model, but all of the schemes do not provide the same level of security of HMQV. So far there are no authenticated Diffie-Hellman protocols which are proven secure in the standard model and achieve the same level of security goals of HMQV efficiently yet. Dispensing of random oracles in our protocol does not require any expensive signature and encryption schemes.

Keywords: Key exchange; Diffie-Hellman protocol; Strong forward secrecy; Key compromise impersonation; Unknown key share.

1 Introduction

One of the most basic cryptographic primitives is a key exchange protocol. A two-party key exchange protocol makes it possible that two parties establish a common *session key* securely. The original Diffie-Hellman key exchange protocol [24] is a fundamental technique in designing key exchange protocols, which is considered to be secure against passive eavesdroppers, but not against active attacks; indeed, that protocol provides no authentication at all. To resist active attacks, huge number of *authenticated* Diffie-Hellman protocols have been suggested [39,27,17,11,46,22].

⋆ This work was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 37–54, 2006.

At the most basic level, an authenticated key exchange protocol must provide secrecy of a shared session key. Yet to completely define the notions of security, we must consider adversarial behaviors which should be tolerated by a protocol. *Implicit authentication* simply means secrecy of session keys against an adversary who passively eavesdrops on protocol executions and may also send messages of its choice to the various parties. A stronger notion of security (and the one that is perhaps most often considered in the cryptographic literature) is *key independence (known key security)*, which means that session keys are computationally independent from each other. A bit more formally, key independence protects against "Denning-Sacco" attacks [26] involving compromise of multiple session keys (for sessions other than the one whose secrecy must be guaranteed). Protocols achieving *weak forward secrecy* (w-FS) maintain secrecy of session keys which are shared through honest executions of the protocol without any interference by an adversary, even if the adversary is able to obtain long-term secret keys of parties. Protocols achieving *strong forward secrecy* (s-FS) maintain secrecy of session keys which have been established with interference of an adversary, even if the adversary is able to obtain long-term secret keys of parties after the session keys was established.

The above notions are most widely used in key exchange protocols. Besides above three security notions, there are various security notions such as key compromise impersonation and unknown key share [15,39,41]. If an adversary obtains a long-term secret key of a party, the adversary can trivially impersonate the party to the other parties. But the adversary may not impersonate other parties to the party. A protocol is secure against *key compromise impersonation* (KCI) attacks, if an adversary can not impersonate other parties (whose long-term secret keys are not revealed) to the parties (whose long-term secret keys are revealed). The security against *session state reveal* (SSR) is formally considered in [21,36]. This security is originated from the consideration that the random values of the sessions may be more easily leaked than the secret keys of the public keys. A protocol is secure against *unknown key share* (UKS) attacks, if the following holds: If two parties *Alice* and *Bob* compute the same session key, *Alice* should consider that she is establishing the session key with *Bob* and *Bob* should consider that he is establishing the session key with *Alice*. In our security model in Section 3, key independence implies the security against unknown key share attacks.

In many common applications parties can actually transmit messages simultaneously. It may be possible to design protocols with improved round complexity by fully exploiting the communication characteristics of the underlying network, and in particular the possibility of simultaneous message transmission. Recently, the possibility of simultaneous message transmission for two-party key exchange was exploited in [34]. They designed one-round two-party key exchange protocols assuming a (bidirectional) *duplex* channel and proved their securities. Our protocol is constructed based on the duplex channels.

1.1 Our Work in Relation to Prior Work

In [41,39], Menezes et al. suggested a two-party key exchange scheme, MQV, which was considered as the most efficient one of authenticated Diffie-Hellman