Efficient One-Round Key Exchange in the Standard Model*

Colin Boyd[1], Yvonne Cliff[1], Juan Gonzalez Nieto[1], and Kenneth G. Paterson[2]

[1] Information Security Institute,
Queensland University of Technology,
GPO Box 2434 Brisbane Qld 4001, Australia
y.cliff@isi.qut.edu.au, {c.boyd,j.gonzaleznieto}@qut.edu.au
[2] Information Security Group,
Royal Holloway University of London,
Egham, Surrey TW20 0EX, U.K.
Kenny.Paterson@rhul.ac.uk

Abstract. We consider one-round key exchange protocols secure in the standard model. The security analysis uses the powerful security model of Canetti and Krawczyk and a natural extension of it to the ID-based setting. It is shown how KEMs can be used in a generic way to obtain two different protocol designs with progressively stronger security guarantees. A detailed analysis of the performance of the protocols is included; surprisingly, when instantiated with specific KEM constructions, the resulting protocols are competitive with the best previous schemes that have proofs only in the random oracle model.

Keywords: Key exchange, standard model.

1 Introduction

There has been a recent rapid growth of interest in efficient cryptographic primitives of all kinds that carry proofs in the standard model. Avoiding the random oracle model (ROM) or generic group model is to be preferred, given the known problems with instantiating these models in practice [8]. However, the usual price to be paid for working in the standard model is a loss of efficiency.

This paper initiates the systematic study of key exchange protocols whose security can be analyzed in the standard model. Our focus here is on two-party, one-round protocols — protocols in which only two message flows are required to securely establish a key between two parties. We provide two related, yet distinct, approaches to building such protocols using KEMs [1], both in the ID-based setting and the traditional PKI-based setting. Our security proofs use the Canetti-Krawczyk model (appropriately adapted for the identity-based case), which is sufficiently powerful to allow the capture of a variety of security properties including basic session key security, key compromise impersonation resistance, and various types of forward security.

* See [6] for the full version of this paper.

Y. Mu, W. Susilo, and J. Seberry (Eds.): ACISP 2008, LNCS 5107, pp. 69–83, 2008.

In the identity-based setting, there is no shortage of protocols with security analysis in the ROM, with Chen, Cheng and Smart [10] providing a useful survey and comparison of these. Our protocols appear to be the first explicit constructions that are proven secure in the standard model in this setting. A recent preprint [22] also considers ID-based key exchange in the standard model, but the security analysis therein is incomplete – we comment in more detail on this below. We consider the instantiation of our ID-based protocol designs with a variety of suitable concrete KEM components. These are derived from ID-based KEMs of Kiltz [14], Kiltz-Galindo [16] and Gentry [12]. By modifying these to operate in the setting of asymmetric pairings and ordinary elliptic curves, we are able to produce concrete ID-based protocols with security proven in the standard model that are only 2.5 times slower than the most efficient protocols with security established in the ROM, the comparison being made on elliptic curves with a 128-bit security level.

In the PKI setting we also obtain efficient, one round, concrete protocol designs in the standard model, which compare favorably with the protocols of Jeong, Katz and Lee [13], Krawczyk [18] and Okamoto [21] which are to our knowledge the only one-round protocols secure in the standard model. The protocols are reasonably efficient even when compared to the best ROM protocols. For example, they can be instantiated with standard model KEMs to yield protocols with a computational increase of a factor around 3 when compared with HMQV [19].

Our first protocol design is the most efficient of the two, and provides key-compromise impersonation (KCI) resistance but not forward secrecy (FS). The basic idea of our first protocol design is very simple: the two parties simply send each other a random secret value using the IB-KEM and then use a randomness extractor to derive a session key from the combined secrets. Our second protocol design is based on the first, but adds an independent Diffie-Hellman exchange to achieve forward secrecy. It also achieves KCI resistance.

1.1 Related Work

Following the development of practical schemes for identity-based encryption many other identity-based primitives have been designed; due to their practical importance, these have included many key exchange protocols. Chen et al. [10] have provided a useful survey and comparison of work to date on identity-based key exchange.

Initially all security proofs for identity-based primitives relied on the random oracle model. More recently there has been a focus on providing new identity-based encryption (IBE) and identity-based key encapsulation (IB-KEM) schemes with security proofs in the standard model. Recent and quite efficient proposals include those of Waters [23], Kiltz [14], Gentry [12] and Kiltz–Galindo [16,17].

Up until now, all proofs for identity-based key exchange protocols have continued to rely on the ROM, with the exception [22] noted. However, although Wang et al. [22] propose three protocols, a proof for only one is provided; the other two proofs supposedly use similar techniques. The protocol with a claimed proof applies a key derivation function H_2 to the shared secret, exchanged messages