Security of Two-Party Identity-Based Key Agreement

Colin Boyd and Kim-Kwang Raymond Choo

Information Security Institute,
Queensland University of Technology,
GPO Box 2434, Brisbane Q4001, Australia
boyd@isrc.qut.edu.au, k.choo@qut.edu.au

Abstract. Identity-based cryptography has become extremely fashionable in the last few years. As a consequence many proposals for identity-based key establishment have emerged, the majority in the two party case. We survey the currently proposed protocols of this type, examining their security and efficiency. Problems with some published protocols are noted.

1 Introduction

One of the main purposes of using public-key cryptography, in comparison to shared-key cryptography, is to make key distribution easier. Public keys by their nature need not be kept confidential. On the other hand, integrity of public keys is critical for security and therefore public key certificates have been used for many years. Management of public key certificates has proven to be a harder task than was initially realised and so new directions have been sought. Identity-based cryptography removes the need for certificates since the identity of the owner is the public key. Such public keys can include any descriptive information including temporal information.

Public key cryptography (and identity-based cryptography in particular) only addresses management of long-term public keys which are not suitable for bulk cryptographic processing. For such purposes symmetric keys are usually required which are established freshly for each individual session. Protocols for establishing such *session keys* come in many different types and have a reputation for being difficult to design correctly. One of the simplest and most common types of key establishment protocols are key agreement protocols in which the session key is defined by inputs from the protocol participants.

In the past few years there has been extreme interest in the use of identity-based cryptography, mainly due to the use of elliptic curve pairings to realise cryptographic structures that did not seem possible before. Amongst the many resulting new tools that have been proposed have been a large number of key agreement protocols based on pairings. In the rush to exploit the new ideas many of these protocols have been published without a careful security analysis or a systematic comparison with alternatives. The situation is somewhat like

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 229–243, 2005.
© Springer-Verlag Berlin Heidelberg 2005

that 20 years ago when key establishment protocols for conventional public key cryptography were routinely published without a proper security analysis.

The purpose of this paper is to make a critical appraisal of the current status of identity-based key agreement protocols, limited to the two-party case. We examine the security properties and efficiency achieved in a large number of published protocols. We emphasise the importance of precise security models and note deficiencies in several protocols.

The rest of this paper is structured as follows. The following section defines the subject matter in more detail by discussing relevant background on identity-based cryptography and key agreement protocols. Section 3 surveys the field of existing published protocols and analyses their comparitive security and efficiency. The conclusion speculates where subsequent progress may be likely.

2 Identity-Based Cryptography and Key Agreement

The original idea for identity-based cryptography goes back to Shamir [30] over 20 years ago. Identity-based cryptography does away with public keys altogether so no certificates are required (although the authenticity of public parameters needs to be assured). This is of great benefit in simplifying key management. However, a drawback of all true identity-based schemes is that users cannot be allowed to generate their own private keys (otherwise anyone could find any user's private key) and therefore key escrow is inevitable.

Shamir gave an algorithm for identity-based signatures but was unable to obtain an identity-based encryption algorithm. However, in 1987 Okamoto [24,25] published the first identity-based key agreement protocol. It uses a composite modulus n whose factorisation is known only to a trusted authority. The authority chooses values e and d as in the RSA algorithm, so that $ed \bmod \phi(n) = 1$, and an element g that is primitive in both the integers mod p and the integers mod q. The values g and e are made public.

Before engaging in the key agreement protocol each user must register with the authority to obtain a private key. Party P_i's identification string, ID_i, is treated as an integer modulo n. The authority calculates the value $s_i = ID_i^{-d} \bmod n$ and distributes s_i securely to user I. Once this registration is completed users may agree fresh session keys without recourse to any other information other than the fixed parameters e and n and the identity of the partner with which the key is to be shared.

Protocol 1 shows the key agreement message flows. The shared secret is defined as $Z_{AB} = g^{er_Ar_B}$. On the assumption that it is necessary to know either s_A or s_B in order to find Z_{AB}, the scheme prevents an adversary from learning the session key.

Mambo and Shizuya [22] and later Kim *et al.* [18] provided a security proof against active attacks. They showed a reduction of attacks on the protocol to the Diffie–Hellman problem or to the RSA problem. Their model is similar to the Bellare–Rogaway security model [3,4] discussed below.