On Session Key Construction in Provably-Secure Key Establishment Protocols*

Kim-Kwang Raymond Choo, Colin Boyd, and Yvonne Hitchcock

Information Security Institute,
Queensland University of Technology,
GPO Box 2434, Brisbane, QLD 4001, Australia
{k.choo, c.boyd, y.hitchcock}@qut.edu.au

Abstract. We examine the role of session key construction in provably-secure key establishment protocols. We revisit an ID-based key establishment protocol due to Chen & Kudla (2003) and an ID-based protocol 2P-IDAKA due to McCullagh & Barreto (2005). Both protocols carry proofs of security in a weaker variant of the Bellare & Rogaway (1993) model where the adversary is not allowed to make any Reveal query. We advocate the importance of such a (Reveal) query as it captures the known-key security requirement. We then demonstrate that a small change to the way that session keys are constructed in both protocols results in these protocols being secure without restricting the adversary from asking the Reveal queries in most situations. We point out some errors in the existing proof for protocol 2P-IDAKA, and provide proof sketches for the improved Chen & Kudla's protocol. We conclude with a brief discussion on ways to construct session keys in key establishment protocols.

1 Introduction

Key establishment protocols are used for distributing shared keying material in a secure manner. For example, today's cryptosystems, such as AES, use key establishment schemes to establish shared keying material. However, despite their importance, the difficulties of obtaining a high level of assurance in the security of almost any new, or even existing, protocols are well illustrated with examples of errors found in many such protocols years after they were published [1,12,20].

The treatment of computational complexity analysis adopts a deductive reasoning process whereby the emphasis is placed on a proven reduction from the problem of breaking the protocol to another problem believed to be hard. Such an approach for key establishment protocols was made popular by Bellare & Rogaway [4] who provided the first formal definition for a model of adversary capabilities with an associated definition of security (which we refer to as the BR93 model in this paper). Since then, many research efforts have been oriented

* This work was partially funded by the Australian Research Council Discovery Project Grant DP0345775.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 116–131, 2005.

towards this end which have resulted in numerous protocols with accompanying computational proofs of security proposed in the literature. In 1995, Bellare and Rogaway analysed a three-party server-based key distribution (3PKD) protocol [5] using an extension to the BR93 model. A more recent revision to the BR93 model was proposed in 2000 by Bellare, Pointcheval and Rogaway [3]. In independent yet related work, Bellare, Canetti, & Krawczyk [2] built on the BR93 model and introduced a modular proof model. However, some drawbacks with this formulation were discovered and this modular proof model was subsequently modified by Canetti & Krawczyk [9], and will be referred to as the CK2001 model in this paper.

The BR93 model is probably one of the most widely used proof models in the computational complexity approach for protocol analysis. In the model, the probabilistic polynomial-time (PPT) adversary controls all the communications that take place between parties via a pre-defined set of oracle queries, namely: Send, Reveal, and Corrupt. The Reveal query allows an adversary to expose session keys for uncorrupted parties, whilst the Corrupt query allows the adversary to corrupt any principal at will, and thereby learn the complete internal state of the corrupted principal. We observe that several protocols proven secure in the BR93 model restrict the adversary from asking the Reveal query. However, we argue that such a query is realistic in a real-world implementation as an adversary is often assumed to have the capability to acquire session keys. Such a (Reveal) query is essential as it allows us to model the scenario whereby each session key generated in one protocol round is independent and determines whether the particular session key will be exposed if other secret keys are compromised. In other words, the Reveal query captures the known-key security requirement in key establishment protocols, whereby a protocol should still achieve its goal in the face of a malicious adversary who has learned some other session keys [7,14]. In addition, omission of the Reveal query to the owner of the Test session in the proof model could also result in protocols vulnerable to reflection attacks being proven secure in such a model.

We revisit an ID-based key establishment protocol due to Chen & Kudla [10] and an ID-based protocol 2P-IDAKA due to McCullagh & Barreto [18]. Both protocols are role-symmetric and carry proofs of security in the BR93 model. However, the existing proofs of both protocols restrict the adversary from asking any Reveal query. Their arguments follow on from earlier work of Blake-Wilson, Johnson, & Menezes [6] who pointed out that it does not seem possible for role-symmetric protocols to be secure in the BR93 model if the Reveal query is allowed. In recent work, Jeong, Katz, & Lee [15] present two protocols $\mathcal{TS}1$ and $\mathcal{TS}2$, both with proofs of security in the BR93 model. This work contradicts the claim of Blake-Wilson *et al.* [6] as both protocols $\mathcal{TS}1$ and $\mathcal{TS}2$ are similar to the protocols analysed by Blake-Wilson *et al.* [6] in the BR93 model, but without restricting the adversary from asking the Reveal query.

We examine the existing arguments on the restriction of the Reveal query. We then demonstrate that by making a simple change to the construction of the session key (and not changing the protocol details), we are able to prove Chen &