Comments on the SM2 Key Exchange Protocol

Jing Xu and Dengguo Feng
State Key Laboratory of Information Security,
Institute of Software, Chinese Academy of Sciences, Beijing, P.R.China
xujing@is.iscas.ac.cn

Abstract. SM2 key exchange protocol is one part of the public key
cryptographic algorithm SM2 which has been standardized by Chinese
state cryptography administration for commercial applications. It be-
came publicly available in 2010 and since then it was neither attacked
nor proved to be secure. In this paper, we show that the SM2 key ex-
change protocol is insecure by presenting realistic attacks in the Canetti-
Krawczyk model. The demonstrated attack breaks session-key security
against an adversary who can only reveal session states. We also propose
a simple modification method to solve this problem.

Keywords: Key exchange protocol, SM2, security model, attack.

1 Introduction

Key exchange protocols are cryptographic primitives that specify how two or
more parties communicating over a public network establish a common session
key. This session key is then typically used to build a confidential or integrity-
preserving communication channel among the involved parties. Therefore, key
exchange protocols form a crucial component in many network protocols. The
most famous example is the classic Diffie-Hellman (DH) key exchange protocol
that marked the birth of modern cryptography [1]. However, the original DH
protocol did not provide authentication of the communicating parties, suffering
from active attacks such as a man-in-the-middle attack. Authenticated key ex-
change (AKE) not only allows parties to compute the shared key but also ensures
authenticity of the parties. AKE protocols operate in a public key infrastructure
and the parties use each other’s public keys to construct a shared secret.

1.1 Security Attributes

For authenticated key exchange protocols, it is desirable to possess the following
security attributes:

(1) (implicit) key authentication: an agreed-upon session key should be known
only by identified parties;
(2) forward secrecy: an agreed-upon session key should remain secret, even if
both parties’ long-term secret key is compromised;
key compromise impersonation resilience: An adversary who reveals a long-term secret key of some party $A$ should be unable to impersonate other parties to $A$ (still, an adversary can impersonate $A$ to anyone else).

In addition to above basic properties, another desirable attribute is resistance to unknown key-share (UKS) attacks. In an unknown key-share attack, a party $A$ is coerced into sharing a key with any party $E$ when in fact she thinks that she is sharing the key with a party $B$. UKS attacks were first discussed by Diffie et al. [2] and have been found in a number of protocols including MTI/A0 [3], the STS-MAC variant of the Station-to-Station (STS) protocol [4], MQV [5] and KEA [6]. Consider the situation where $B$ is a bank system and $A$ is an account holder. If the UKS attack described above is successful, then the adversary $E$ could impersonate $B$ (a banking system) and obtain $A$’s credit card number over the resulting private communication link. Therefore, it is very significant to design protocols secure against UKS attacks.

1.2 Related Works and Our Contribution

The design and analysis of secure key exchange protocols have been proved to be a non-trivial task, with a large body of work written on the topic, including [7-12] and many more. Of these protocols, the most famous, most efficient and most standardized is the MQV protocol. The MQV protocols [7] are a family of authenticated Diffie-Hellman protocols and have been widely standardized [13-15]. The HMQV protocol [12] is a hashed variant of the MQV key agreement protocol with a rigorous security proof, which is currently being standardized by IEEE P1363 standards group [16].

SM2 key exchange protocol [17] is one part of the public key cryptographic algorithm SM2, which has been standardized by Chinese state cryptography administration for commercial applications and has been released in December 2010. This standard aims to provide a reference of products and techniques for security manufacturers in China, promoting the credibility and interoperability of security products. Indeed, SM2 key exchange protocol appears to be a remarkable protocol which provides the same efficiency as the MQV protocol. However, one question that has not been settled so far is whether the protocol can be proven secure in a rigorous model of key exchange security. In order to provide an answer to this question we analyze the SM2 protocol in the Canetti-Krawczyk security model. Unfortunately, we show that SM2 protocol is vulnerable to unknown key-share attacks in this model. The demonstrated attack breaks session-key security against an adversary who can only reveal session states. Then we present a simple patch which fixes the security problem.

1.3 Organization

The rest of this paper is organized as follows. Section 2 reviews SM2 key exchange protocol. Section 3 provides an overview of the formal security model of key exchange protocols, on which all of our analysis work is based. Section 4 presents