Au, Man Ho; Susilo, Willy; Mu, Yi

Is the notion of divisible on-line/off-line signatures stronger than on-line/off-line signatures? (English) Zbl 1267.94114


Summary: On-line/off-line signatures are useful in many applications where the signer has a very limited response time once the message is presented. The idea is to perform the signing process in two phases. The first phase is performed off-line before the message to be signed is available and the second phase is performed on-line after the message to be signed is provided. Recently, at CT-RSA 2009, C. zhi Gao et al. made a very interesting observation that most of the existing schemes possess the following structure [Lect. Notes Comput. Sci. 5473, 148–163 (2009; Zbl 1237.94108)]. In the off-line phase, a partial signature, called the off-line token is computed first. Upon completion of the on-line phase, the off-line token constitutes part of the full signature. They considered the “off-line token exposure problem” in which the off-line token is exposed in the off-line phase and introduced a new model to capture this scenario. While intuitively the new requirement appears to be a stronger notion, Gao et al. could not discover a concrete attack on any of the existing schemes under the new model. They regarded clarifying the relationship between the models as an open problem. In this paper, we provide an affirmative answer to this open problem. We construct an on-line/off-line signature scheme, which is secure under the ordinary security model whilst it is insecure in the new model. Specifically, we present a security proof under the old model and a concrete attack of the scheme under the new model. This illustrates that the new model is indeed stronger.

For the entire collection see [Zbl 1177.94016].

MSC:

94A62 Authentication, digital signatures and secret sharing

Keywords:
on-line/off-line signatures; divisible on-line/off-line signatures; OS-EU-CMA; DOS-EU-CMA

Full Text: DOI