Cryptology ePrint Archive: Report 2011/615

On the Joint Security of Encryption and Signature in EMV

Jean Paul Degabriele and Anja Lehmann and Kenneth G. Paterson and Nigel P. Smart and Mario Strefler

Abstract: We provide an analysis of current and future algorithms for signature and encryption in the EMV standards in the case where a single key-pair is used for both signature and encryption. We give a theoretical attack for EMV's current RSA-based algorithms, showing how access to a partial decryption oracle can be used to forge a signature on a freely chosen message. We show how the attack might be integrated into EMV's CDA protocol flow, enabling an attacker with a wedge device to complete an offline transaction without knowing the cardholder's PIN. Finally, the elliptic curve signature and encryption algorithms that are likely to be adopted in a forthcoming version of the EMV standards are analyzed in the single key-pair setting, and shown to be secure.

Category / Keywords: applications / EMV, signature, encryption, attack

Publication Info: An abridged version of this work appears at CT-RSA 2012. This is the full version.

Date: received 15 Nov 2011, last revised 16 Dec 2011

Contact author: kenny paterson at rhul ac uk

Available formats: PDF | BibTeX Citation

Note: Correction of "1968" to "1984" in Table 1 and text.

Version: 20111216:140653 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]