Cryptology ePrint Archive: Report 2011/213

On Cipher-Dependent Related-Key Attacks in the Ideal-Cipher Model

M.R. Albrecht and P. Farshim and K.G. Paterson and G.J. Watson

Abstract: Bellare and Kohno introduced a formal framework for the study of related-key attacks against blockciphers. They established sufficient conditions (output-unpredictability and collision-resistance) on the set of related-key-deriving (RKD) functions under which an ideal cipher is secure against related-key attacks, and suggested this could be used to derive security goals for real blockciphers. However, to do so requires the reinterpretation of results proven in the ideal-cipher model for the standard model (in which a blockcipher is modelled as, say, a pseudorandom permutation family). As we show here, this is a fraught activity. In particular, building on a recent idea of Bernstein, we first demonstrate a related-key attack that applies generically to a large class of blockciphers. The attack exploits the existence of a short description of the blockcipher, and so does not apply in the ideal-cipher model. However, the specific RKD functions used in the attack are provably output-unpredictable and collision-resistant. In this sense, the attack can be seen as a separation between the ideal-cipher model and the standard model. Second, we investigate how the related-key attack model of Bellare and Kohno can be extended to include sets of RKD functions that themselves access the ideal cipher. Precisely such related-key functions underlie the generic attack, so our extended modelling allows us to capture a larger universe of related-key attacks in the ideal-cipher model. We establish a new set of conditions on related-key functions that is sufficient to prove a theorem analogous to the main result of Bellare and Kohno, but for our extended model. We then exhibit non-trivial classes of practically relevant RKD functions meeting the new conditions. We go on to discuss standard model interpretations of this theorem, explaining why, although separations between the ideal-cipher model and the standard model still exist for this setting, they can be seen as being much less natural than our previous separation. In this manner, we argue that our extension of the Bellare--Kohno model represents a useful advance in the modelling of related-key attacks. Third, we consider the topic of key-recovering related-key attacks and its relationship to the Bellare--Kohno formalism. In particular, we address the question of whether lowering the security goal by requiring the adversary to perform key-recovery excludes separations of the type exhibited by us in the Bellare--Kohno model.

Category / Keywords: secret-key cryptography / Related-key attack, Ideal-cipher model, Blockcipher

Publication Info: FSE 2011

Date: received 3 May 2011

Contact author: pooya farshim at gmail com