Reflection cryptanalysis of PRINCE-like ciphers.


Summary: PRINCE is a low-latency block cipher presented at ASIACRYPT 2012. The cipher was designed with a property called $\alpha$-reflection which reduces the definition of decryption with a given key to encryption with a different but related key determined by $\alpha$. In the design document, it was shown that PRINCE is secure against known attacks independently of the value of $\alpha$, and the design criteria for $\alpha$ remained open. In this paper, we introduce new distinguishers on PRINCE-like ciphers by constructing probable or impossible relations from the cipher data located at layers that are symmetric around the middle of the cipher. We show that the probabilities of such relations, called reflection characteristics in this paper, depend crucially on the choice of the reflection parameter $\alpha$. Several classes of $\alpha$ are investigated. As a result we show that there exist values of $\alpha$ which, if used in the otherwise original PRINCE, would allow a key-recovery attack on the full 12-round cipher with the data complexity of $2^{57.98}$ known plaintexts and the time complexity of $2^{72.39}$ encryptions. While this attack is not better than the generic attack on the complete cipher, where the core cipher is protected by the whitening key, the same reflection distinguisher, when applied on the core cipher without the whitening key, yields a key-recovery attack with time complexity less than exhaustive key search and data complexity of $2^{56.21}$ known plaintexts. As a result of the new cryptanalysis method presented in this paper, new design criteria concerning the selection of the value of $\alpha$ for PRINCE-like ciphers are obtained.

Keywords: Block cipher; $\alpha$-reflection property; PRINCE; statistical attack; reflection attack