SKENO: Secret key encryption with non-interactive opening.

Summary: In this paper, we introduce the notion of secret key encryption with non-interactive opening (SKENO). With SKENO, one can make a non-interactive proof $\pi$ to show that the decryption result of a ciphertext $C$ under a shared secret key $K$ is indeed plaintext $M$ without revealing $K$ itself. SKENO is the secret key analogue of public key encryption with non-interactive opening (PKENO). We give a generic construction of SKENO from verifiable random function (VRF) with certain stronger uniqueness, for example, the Hohenberger-Waters VRF and the Berbain-Gilbert $IV$-dependent stream cipher construction. Although the strong primitive VRF is used, by taking advantage of the features of the stream cipher, we can still achieve good performance without sacrificing much of the efficiency. Though our VRF-based SKENO construction does not require random oracles, we show that SKENO can be constructed from weak VRF (which is strictly weaker primitive than VRF) in the random oracle model.

Keywords: public/secret key encryption with non-interactive opening; verifiable random function; $IV$-dependent stream cipher