

Title: Encryption Switching Protocols

Geoffroy Couteau, École Normale Supérieure de Paris, France

We formally define the primitive of encryption switching protocol (ESP), allowing to switch between two encryption schemes.

Intuitively, this two-party protocol converts given ciphertexts from one scheme into ciphertexts of the same messages under the other scheme, for any polynomial number of switches, in any direction.

Although ESP is a special kind of two-party computation protocol, it turns out that ESP implies general two-party computation (2-PC) under natural conditions. In particular, our new paradigm is tailored to the evaluation of functions over rings. Indeed, assuming the compatibility of two additively and multiplicatively homomorphic encryption schemes, switching ciphertexts makes it possible to efficiently reconcile the two internal laws.

Since no such pair of public-key encryption schemes appeared in the literature, except for the non-interactive case of fully homomorphic encryption which still remains prohibitive in practice, we build the first multiplicatively homomorphic ElGamal-like encryption scheme over (\mathbb{Z}_n, \times) as a complement to the Paillier encryption scheme over $(\mathbb{Z}_n, +)$, where n is a strong RSA modulus. Eventually, we also instantiate secure ESPs between the two schemes, in front of malicious adversaries. This enhancement relies on a new technique called refreshable twin ciphertext pool, which we show being of independent interest. We additionally prove this is enough to argue the security of our general 2-PC protocol against malicious adversaries.