White-Box Security Notions for Symmetric Encryption Schemes*

Cécile Delerablée, Tancrède Lepoint, Pascal Paillier, and Matthieu Rivain

CryptoExperts, 41 boulevard des Capucines, 75002 Paris, France
{firstname.lastname}@cryptoexperts.com

Attacks on *implementations* of cryptographic primitives have become a major threat due to side-channel information leakage such as execution time, power consumption or electromagnetic emanations.

White-box cryptography was introduced in 2002 by Chow, Eisen, Johnson and van Oorschot as the ultimate, *worst-case* attack model. This model considers an attacker far more powerful than in the classical black-box model (and thus more representative of real-world attackers); namely the attacker is given full knowledge and full control on both the algorithm and its execution environment. However, even such powerful capabilities should not allow her to e.g extract the embedded key. White-box cryptography can hence be seen as a restriction of general obfuscation where the function to protect belongs to some narrower class of cryptographic functions indexed by a secret key. From that angle, the ultimate goal of a white-box implementation is to leak nothing more than what a black-box access to the function would reveal. An implementation achieving this strong property would be as secure as in the black-box model, in particular it would resist *all existing and future* side-channel and fault-based attacks. Several white-box implementations of standard block-ciphers (DES, AES) have been proposed but they have all been broken. On the other hand, neither evidence of existence nor proofs of impossibility have been provided for this particular setting. This might be in part because it is still quite unclear what white-box cryptography really aims to achieve and which security properties are expected from white-box programs in applications.

Our work builds a first step towards a practical answer to this question by translating folklore intuitions behind white-box cryptography into concrete security notions. Specifically, we formalize the notion of *white-box compilers* for a symmetric encryption scheme and introduce several security notions for such compilers. A white-box compiler turns a symmetric encryption scheme into randomized white-box programs, and we capture several desired security properties such as one-wayness, incompressibility and traceability for white-box programs. We also give concrete examples of white-box compilers that already achieve some of these notions. Overall, our results open new perspectives on the design of white-box programs that securely implement symmetric encryption.

* An extended version of this abstract appeared in the proceedings of SAC 2013.