

## Constructing White-Box Implementations Based on Threshold Shares and Composite Fields

**Authors :** Tingting Lin, Manfred von Willich, Dafu Lou, Phil Eisen

**Abstract :** A white-box implementation of a cryptographic algorithm is a software implementation intended to resist extraction of the secret key by an adversary. To date, most of the white-box techniques are used to protect block cipher implementations. However, a large proportion of the white-box implementations are proven to be vulnerable to affine equivalence attacks and other algebraic attacks, as well as differential computation analysis (DCA). In this paper, we identify a class of block ciphers for which we propose a method of constructing white-box implementations. Our method is based on threshold implementations and operations in composite fields. The resulting implementations consist of lookup tables and few exclusive OR operations. All intermediate values (inputs and outputs of the lookup tables) are masked. The threshold implementation makes the distribution of the masked values uniform and independent of the original inputs, and the operations in composite fields reduce the size of the lookup tables. The white-box implementations can provide resistance against algebraic attacks and DCA-like attacks.

**Keywords :** white-box, block cipher, composite field, threshold implementation

**Conference Title :** ICICS 2019 : International Conference on Information and Communications Security

**Conference Location :** San Francisco, United States

**Conference Dates :** June 06-07, 2019