Bard, Gregory V.

If a block cipher $E(k, p)$ (key $k \in \{0, 1\}^l$, plaintext $p \in \{0, 1\}^l$, e.g. in AES $l_p = 128$, $l_k \in \{128, 192, 256\}$) is transformed using permutations $M_1$, $M_2$, $M_3$ (of suitable size), then the transformed fraudulent function $\hat{E}(k, p) = M_3 E(M_1 k, M_2 p)$ remains a block cipher and its security properties would be preserved. The encryption function can be expressed using polynomials over $\{0, 1\}$ and systems of polynomials for the original and transformed function will be equivalent. This allows to reduce the fraud detection problem to logical satisfiability problem which can be solved using standard off-the-shelf software packages.

Reviewer: Jaak Henno (Tallinn)

MSC:
94A60 Cryptography
68T20 Problem solving in the context of artificial intelligence (heuristics, search strategies, etc.)
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)

Keywords:
algebraic cryptanalysis; block ciphers; circuit equivalence; intellectual property fraud detection; isomorphism of polynomials; logical satisfiability solvers; SAT-solvers; polynomials mod 2

Software:
Magma; SageMath

Full Text: DOI

References:
[2] MiniSAT, or


[37] Vaudenay, S., On measuring resistance to linear cryptanalysis, (Mikulášská Kryptobesídka. Mikulášská Kryptobesídka, Prague, Czech Republic (2003)), available at

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original
paper as accurately as possible without claiming the completeness or perfect precision of the matching.