

## Courtois: nowe ataki na KeeLoq

<http://ipsec.pl/courtois-nowe-ataki-na-keeloq.html>

Nicolas Tadeusz Courtois i Gregory V. Bard opublikowali nowe ataki na algorytm KeeLoq, popularny szyfr wykorzystywany do zdalnego otwierania drzwi i rozbijania alarmu m.in. w samochodach marki Jaguar.

Algorytm jest szyfrem blokowym z 32-bitowymi blokami i 64-bitowym kluczem, ze względu na małe wymagania pamięciowe stosowanym w radiowych "kluczach" do uruchamiania droższych samochodów (używają go m.in. Chrysler i Jaguar). Badacze wybrali go ponieważ ze względu na prostą konstrukcję i niewielką liczbę rund stanowi dobry obiekt do ćwiczeń nad kryptoanalizą algebraiczną. Opracowany przez Courtois i Barda atak umożliwia odzyskanie pełnego klucza w  $2^48$  cyklach procesora.

Autorzy oceniają atak jako praktyczny. Jest on  $2^{11}$  szybszy niż wyczerpujące przeszukiwanie przestrzeni kluczy (jeśli <http://eprint.iacr.org/2007/062>). Nicolas T. Courtois, Gregory V. Bard "Algebraic and Slide Attacks on KeeLoq" (<http://ipsec.pl/contrib/keyloq.pdf>)