SubkeySearch: Key recovery on pointwise-keyed weak PRFs

Antoine Sidem*†[1]

[1]Télécom Paris – Institut Mines-Télécom [Paris], Institut Polytechnique de Paris – France

Résumé

Recently, weak pseudorandom functions (wPRFs) based on the alternating moduli paradigm have been proposed as a promising class of MPC-friendly primitives. The wPRF proposed at CRYPTO 2024 by Alamati et al., in its One-to-One parameter set, has been shown to be vulnerable to a key recovery attack dubbed *Zeroed-out*, exploiting collisions in the queries.

We present a more general key recovery attack on the aforementioned wPRFs, as well as other wPRFs similar in structure, which we call *pointwise-keyed functions*.
This method, applied to wPRFs in the One-to-One parameter set attacked by *Zeroed-out*, has smaller complexity and achieves an attack with complexity below the birthday bound, while staying effective against the proposed countermeasures. For the first time, it also succeeds in attacking one of the two Many-to-One parameter sets and stays effective against one of the proposed countermeasures. Collaboration with Qingju Wang.

*Intervenant

†Auteur correspondant: antoine.sidem@telecom-paris.fr