Equivalent Key Recovery Attacks against HMAC and NMAC with Whirlpool Reduced to 7 Rounds

Jian Guo, Yu Sasaki, Lei Wang, Meiqin Wang, Long Wen

Nanyang Technological University, Singapore
NTT Secure Platform Laboratories, Japan
Shandong University, China

ASIACRYPT 2013 Rump Session, India
03 Dec 2013

another work from ASK 2013

HMAC-Whirlpool

- HMAC: $H(K\oplus opad \| H(K\oplus ipad \| M))$, designed by Mihir Bellare, Ran Canetti and Hugo Krawczyk in Crypto 1996; standarized by ANSI, IETF, ISO, NIST from 1997.

- Whirlpool: 512-bit hash function designed by Barreto and Rijmen in 2000, standarized by ISO/IEC, follows Miyaguchi-Preneel mode, i.e., $f(h, M) = E_h(M)\oplus h\oplus M$, with AES-Like compression function.

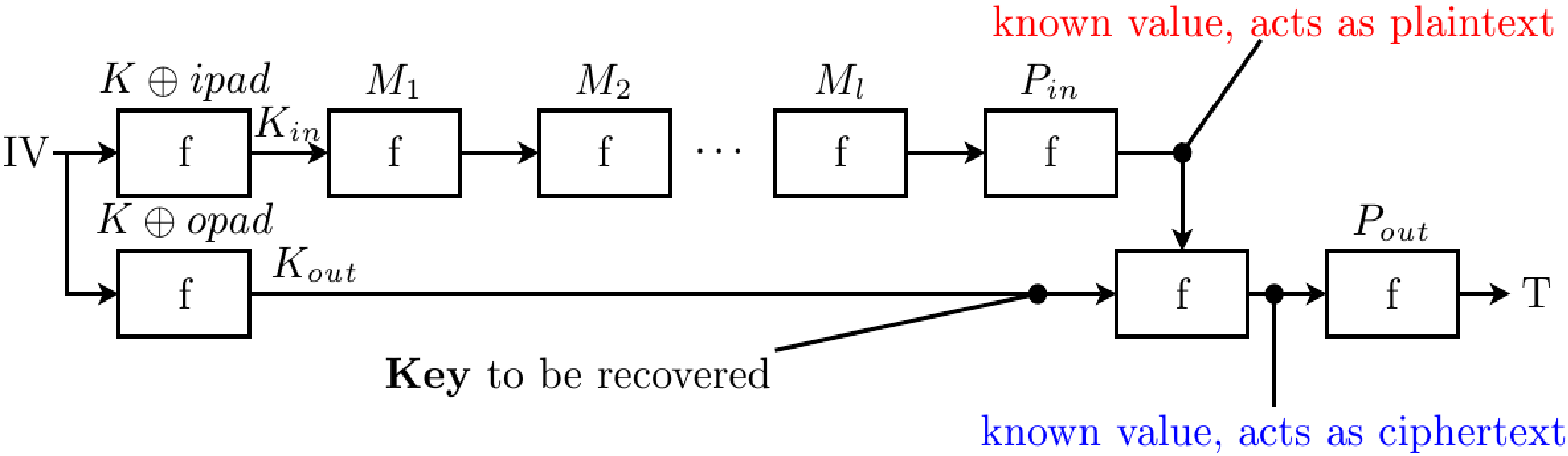
The Best Attack

- Yet to be presented, by Guo-Sasaki-Wang-Wu at Asiacrypt 2013, works for Whirlpool reduced to 6 out of 10 rounds

- Equivalent with chosen plaintext attack on the underlying AES-like block cipher

How it worked ?

Filter plaintext for structured collisions



New Attack

Convert most recent chosen plaintext attacks on reduced AES to known plaintext attack.

+ Combine with the attack framework by Guo et al.

=> Equivalent keys (including K_{in} and K_{out}) Attack for HMAC-Whirlpool reduced to 7 rounds, **mor**e rounds than all existing collision/preimage attacks against Whirlpool.