Cryptanalysis of HMAC/NMAC-Whirlpool

Jian Guo, Yu Sasaki, Lei Wang, Shuang Wu

NANYANG TECHNOLOGICAL UNIVERSITY

NTT

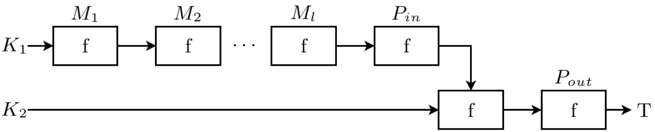
ASIACRYPT, Bangalore, India
4 December 2013

Talk Overview

1. Introduction
   - HMAC and NMAC
   - The Whirlpool Hash Function
   - Motivation
2. Key Recovery Attacks
3. Conclusion

HMAC and NMAC

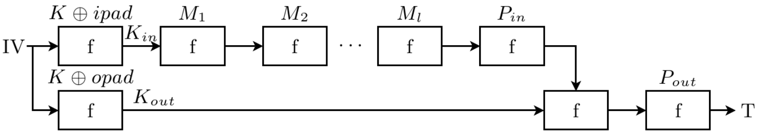
- Designed by Mihir Bellare, Ran Canetti and Hugo Krawczyk in Crypto 1996
- Standarized by ANSI, IETF, ISO, NIST from 1997
- **The** most widely deployed hash-based MAC construction.



NMAC

HMAC and NMAC

- Designed by Mihir Bellare, Ran Canetti and Hugo Krawczyk in Crypto 1996
- Standarized by ANSI, IETF, ISO, NIST from 1997
- **The** most widely deployed hash-based MAC construction.



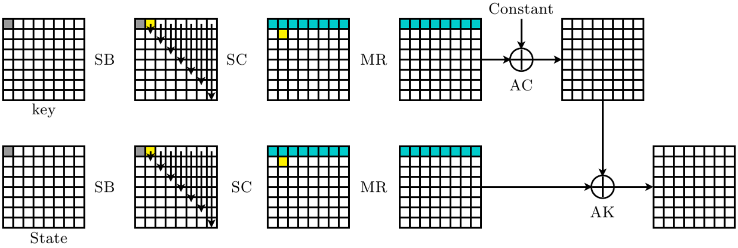
HMAC

Whirlpool

- designed by Barreto and Rijmen in 2000 with 512-bit digest
- standarized by ISO/IEC, approved by NESSIE (New European Schemes for Signatures, Integrity, and Encryption).
- follows Merkle-Damgård strengthening, and Miyaguchi-Preneel mode, *i.e.*, $f(H, M) = E_H(M) \oplus H \oplus M$
- both state and key follow the AES-like process, with 10 rounds.

Whirlpool

- designed by Barreto and Rijmen in 2000 with 512-bit digest
- standarized by ISO/IEC, approved by NESSIE (New European Schemes for Signatures, Integrity, and Encryption).
- follows Merkle-Damgård strengthening, and Miyaguchi-Preneel mode, *i.e.*, $f(H, M) = E_H(M) \oplus H \oplus M$
- both state and key follow the AES-like process, with 10 rounds.



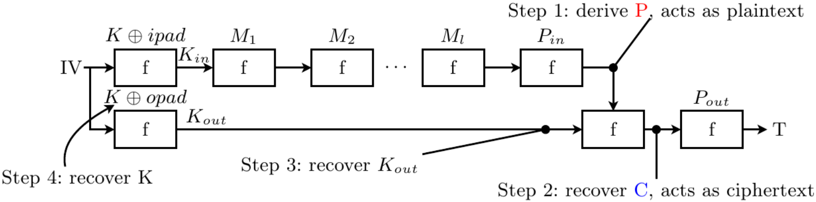
Key: $AC \circ MR \circ SC \circ SB$; State: $AK \circ MR \circ SC \circ SB$

Motivation

AES,1998	Whirlpool, 2000
⇓	⇓
First Cryptanalysis	
Ferguson et al. 2000, etc.	Mendel et al. 2009, etc.
⇓	⇓
Analysis on MAC Applications	
follows naturally	**Ours**

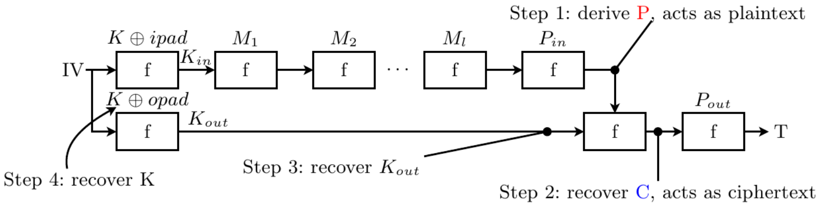
6-round HMAC-Whirlpool — Attack Overview

1. Derive many P



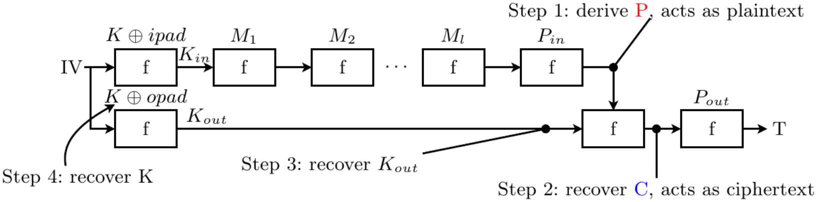
6-round HMAC-Whirlpool — Attack Overview

1. Derive many P
2. Derive corresponding C



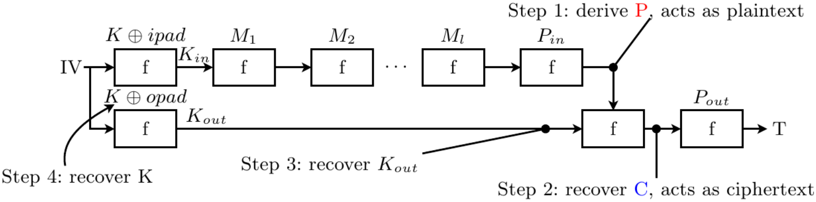
6-round HMAC-Whirlpool — Attack Overview

1. Derive many P
2. Derive corresponding C
3. Recover K_{out} from known *P*s and *C*s



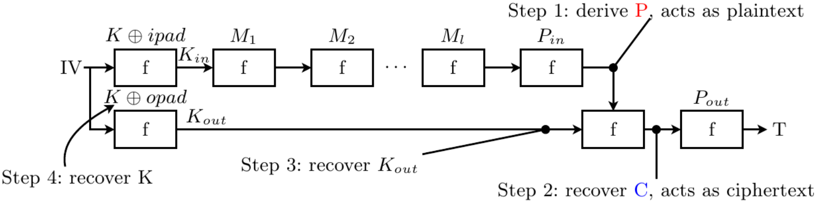
6-round HMAC-Whirlpool — Attack Overview

1. Derive many P
2. Derive corresponding C
3. Recover K_{out} from known Ps and Cs
4. Recover the original key K from K_{out}



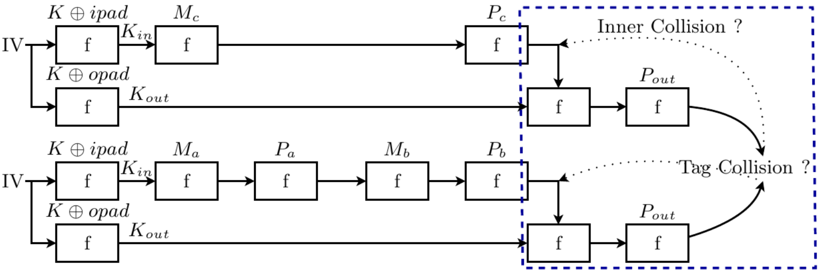
6-round HMAC-Whirlpool — Attack Overview

1. Derive many P
2. Derive corresponding C
3. Recover K_{out} from known Ps and Cs
4. Recover the original key K from K_{out}
5. Recover K_{in} (or K_1) for NMAC only.



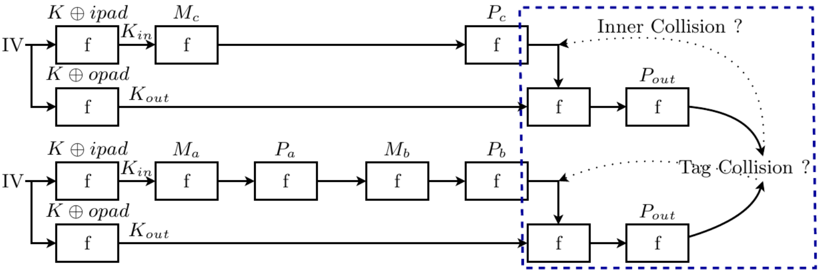
Step 1: Derive P

1. Gaëtan just showed us how to derive $h = H(K \oplus ipad \| M_a)$ for some long message M_a of around $2^{n/2}$ blocks.



Step 1: Derive P

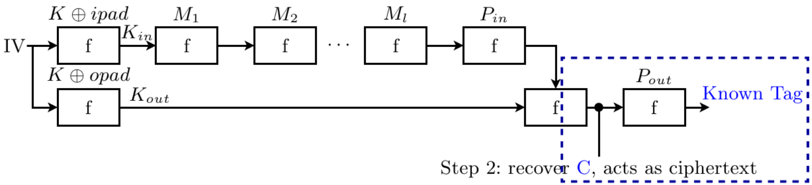
1. Gaëtan just showed us how to derive $h = H(K \oplus ipad \| M_a)$ for some long message M_a of around $2^{n/2}$ blocks.
2. Unbalanced Meet-in-the-Middle attack against $H(K \oplus ipad \| M_c)$, with $H(K \oplus ipad \| M_a \| P_a \| M_b) = f(f(f(h, P_a), M_b), P_b)$, by repeating many one-block M_b and M_c. Then we know $h' = H(K \oplus ipad \| M_c)$, hence $P = H(K \oplus ipad \| M_c \| P_c \| M_d) = f(f(h', P_c), M_d)$, for any M_d with padding satisfied, due to length-extension property of Merkle-Damgård structure.



Step 2: Derive C

The Problem

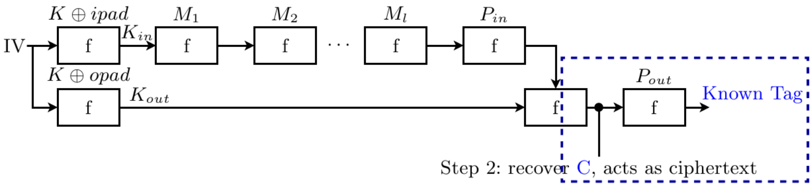
With known Tag value, and fixed message block P_{out}, find input chaining value C.



Step 2: Derive C

The Problem

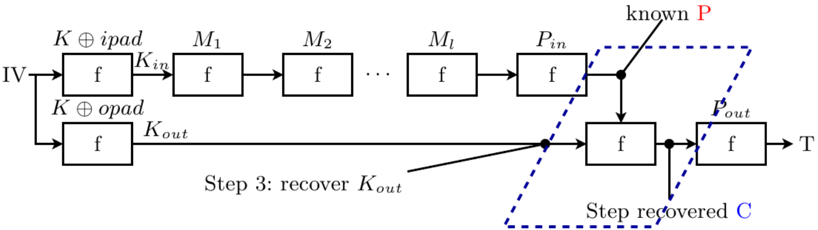
With known Tag value, and fixed message block P_{out}, find input chaining value C.



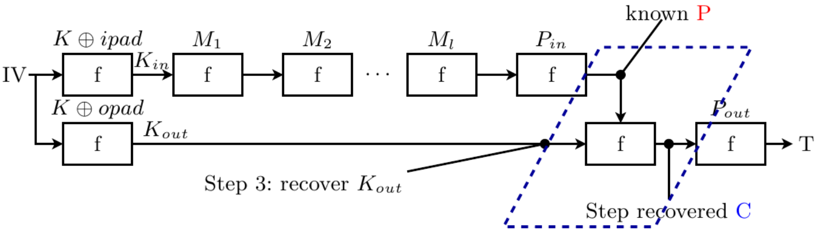
The Solution

Precompute a table $T = f(C, P_{out})$ to obtain many pairs of (C, T)

Step 3: Recover K_{out}

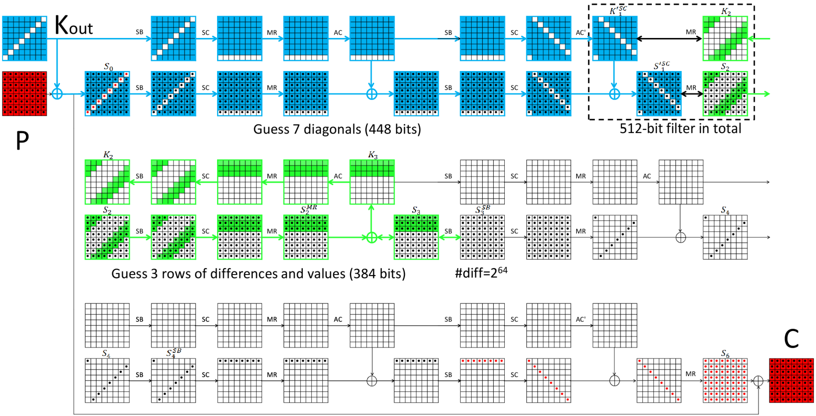


Step 3: Recover K_{out}



$$C = f(K_{out}, P) = E_{K_{out}}(P) \oplus P \oplus K_{out}$$

Step 3: 6-Round Chosen Plaintext Attack

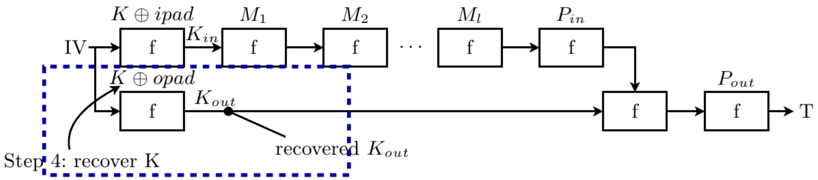


Given many (P, C) pairs, filter for 3-collision with strctured difference in diagonal of $V = MR^{-1}(P \oplus C)$.

Step 4: Recover K

The Problem

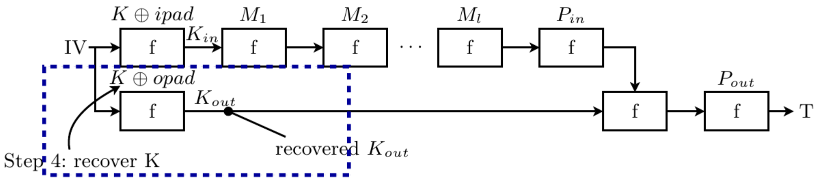
With input chaining IV, output chaining K_{out}, recover K.



Step 4: Recover K

The Problem

With input chaining IV, output chaining K_{out}, recover K.



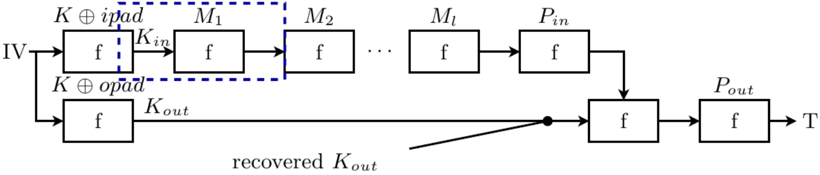
The Solution

Preimage attack by Sasaki et al. ASIACRYPT 2012.

Step 5: Recover K_{in}

The Problem

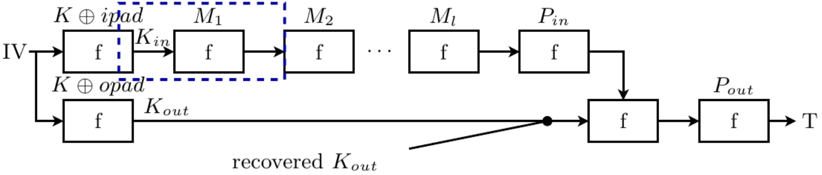
With known K_{out}, chosen M_1, recover K_{in}.



Step 5: Recover K_{in}

The Problem

With known K_{out}, chosen M_1, recover K_{in}.



The Solution

Exactly the same procedure as recovering K_{out}.

Conclusion

Target	Attack Mode	#Rounds	Source
HMAC/NMAC-Whirlpool	Key Recovery	6	Ours
HMAC/NMAC-Whirlpool	Distinguishing-H	full	Ours
Whirlpool	Collision	5	Lamberger et al. AC 2009
Whirlpool	Preimage	6	Sasaki et al. AC 2012

Conclusion

Target	Attack Mode	#Rounds	Source
HMAC/NMAC-Whirlpool	Key Recovery	6	Ours
HMAC/NMAC-Whirlpool	Distinguishing-H	full	Ours
Whirlpool	Collision	5	Lamberger et al. AC 2009
Whirlpool	Preimage	6	Sasaki et al. AC 2012

Stay tuned for universal forgery (equivalent key recovery) attacks against HMAC with **7**-round Whirlpool.

Thank you!

Questions?