Cryptanalysis of PMACx, PMAC2x, and SIVx

Kazuhiko Minematsu[1] Tetsu Iwata[2,*]

[1]NEC Corporation, Japan

[2]Nagoya University, Japan

FSE 2017, Rump Session
March 7, 2017, Tokyo International Forum, Tokyo, Japan

[*]Supported in part by JSPS KAKENHI, Grant-in-Aid for Scientific Research (B), 26280045. Work was carried out while visiting Nanyang Technological University, Singapore.

Overview

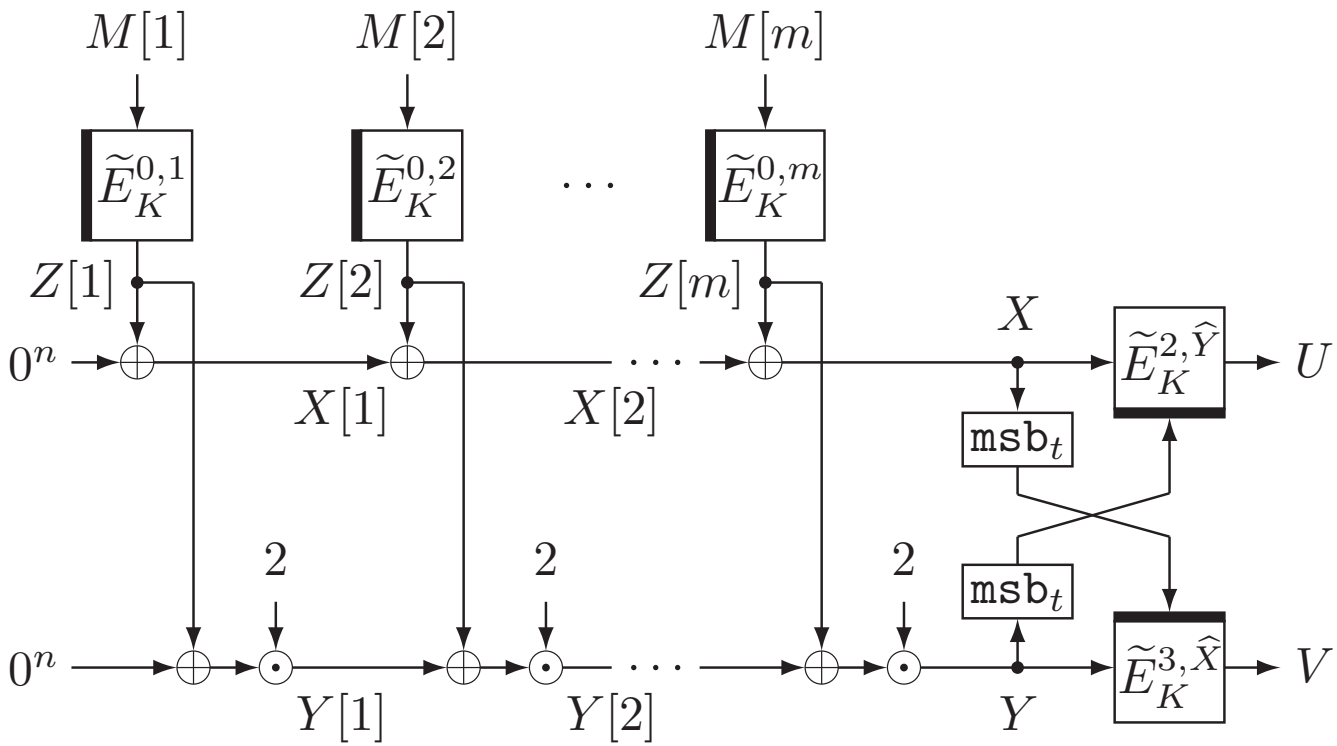
Scheme	Type	Provable security bound	Attack complexity
PMACx	PRF	$O(q^2/2^{2n} + q^3/2^{3n})$ [LN17]	$q = O(2^{n/2})$
PMAC2x	PRF	$O(q^2/2^{2n} + q^3/2^{3n})$ [LN17]	$q = O(2^{n/2})$
SIVx	DAE	$O(q^2/2^{2n} + q^3/2^{3n})$ [LN17]	$q = O(2^{n/2})$

- TBC $\widetilde{E}_K : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$
- q queries
- provably secure up to 2^n queries [LN17], beyond the birthday bound security

[LN17] Eik List and Mridul Nandi. Revisiting Full-PRF-Secure PMAC and Using It for Beyond-Birthday Authenticated Encryption. CT-RSA 2017

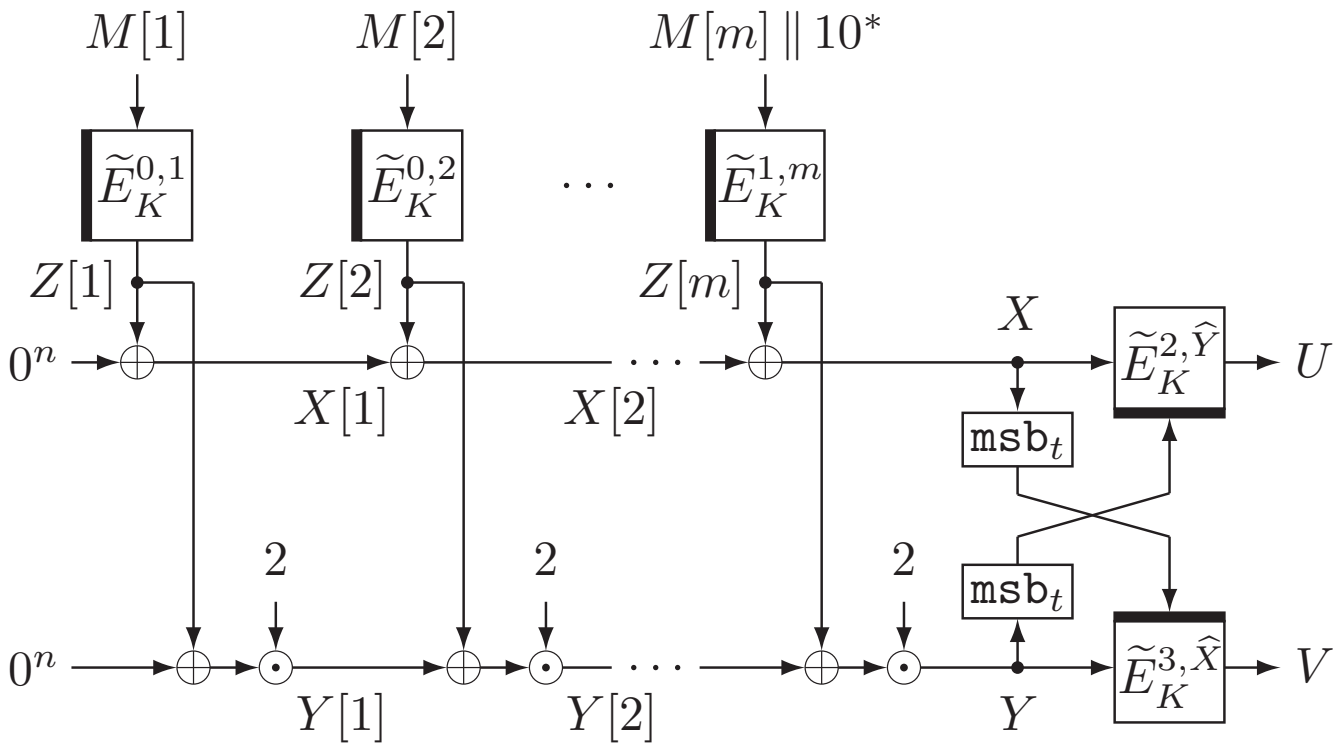
PMAC2x [LN17]

- $(M[1], \ldots, M[m]) \xleftarrow{n} M$, $|M[m]| = n$



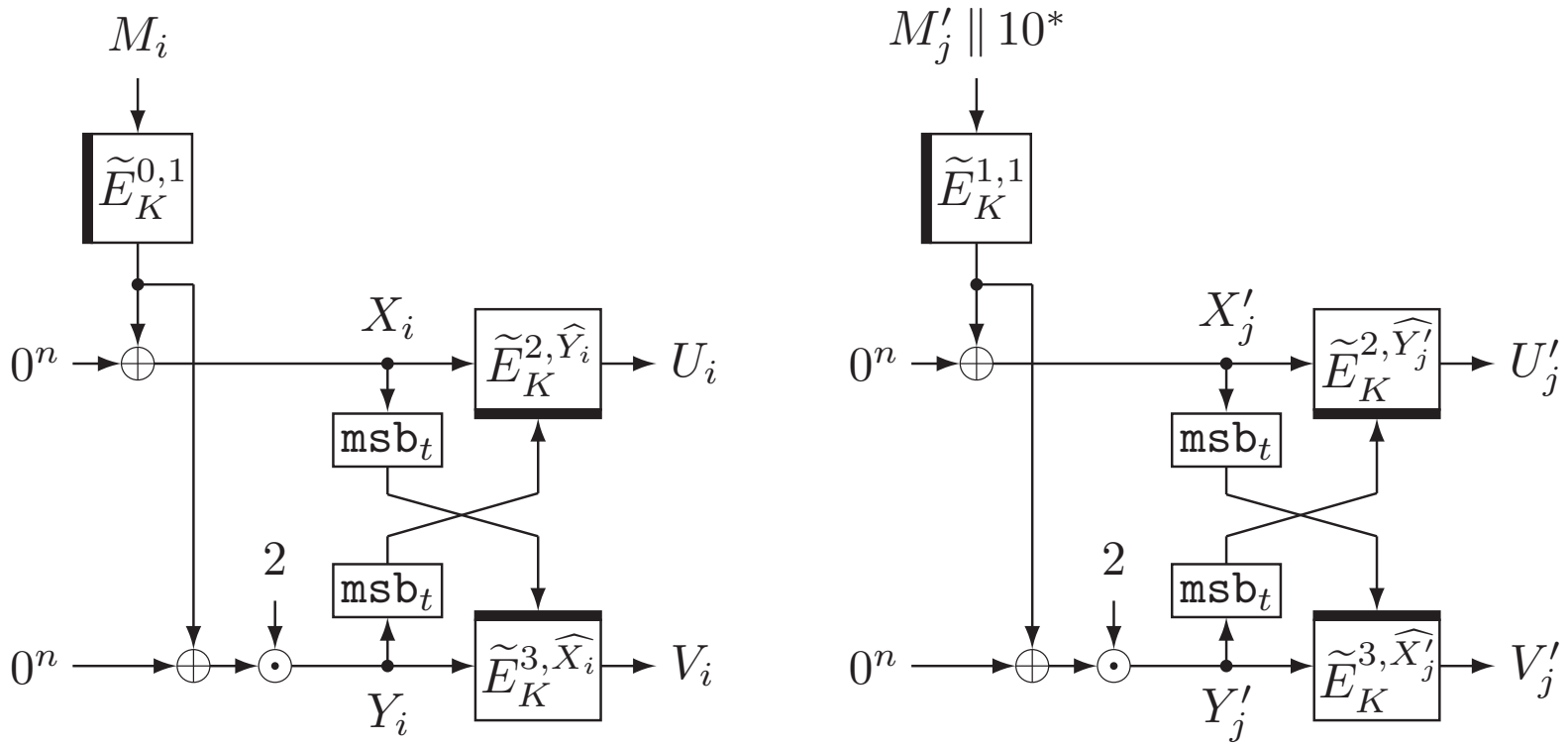
PMAC2x [LN17]

- $(M[1], \ldots, M[m]) \xleftarrow{n} M$, $|M[m]| < n$



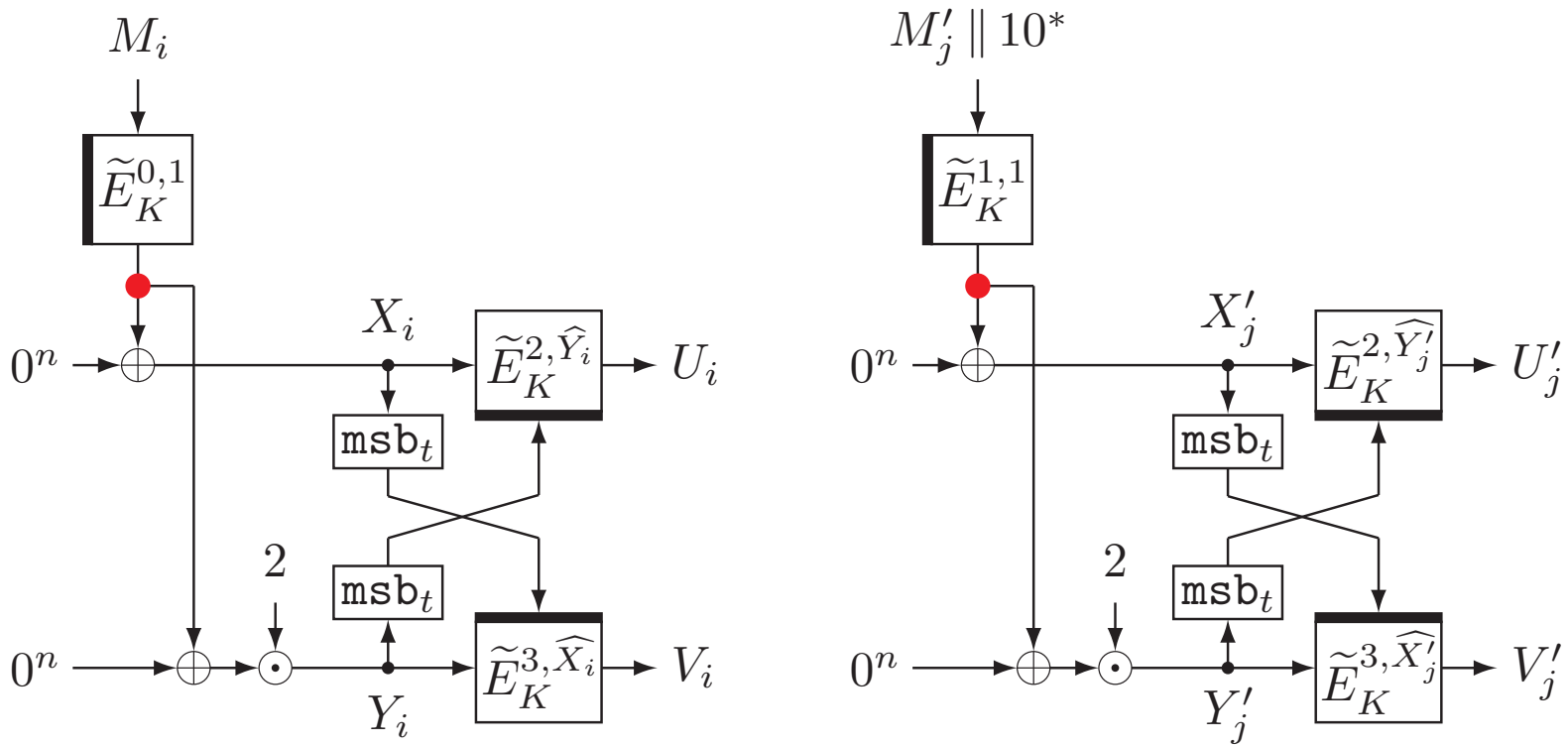
$O(2^{n/2})$ Attack on PMAC2x

- $Q = 2^{n/2-1}$
- $M_1, \ldots, M_Q$, $|M_i| = n$ for $1 \le i \le Q$ and $\{M_1, \ldots, M_Q\}$ is distinct
- $M'_1, \ldots, M'_Q$, $|M'_j| < n$ for $1 \le j \le Q$ and $\{M'_1, \ldots, M'_Q\}$ is distinct



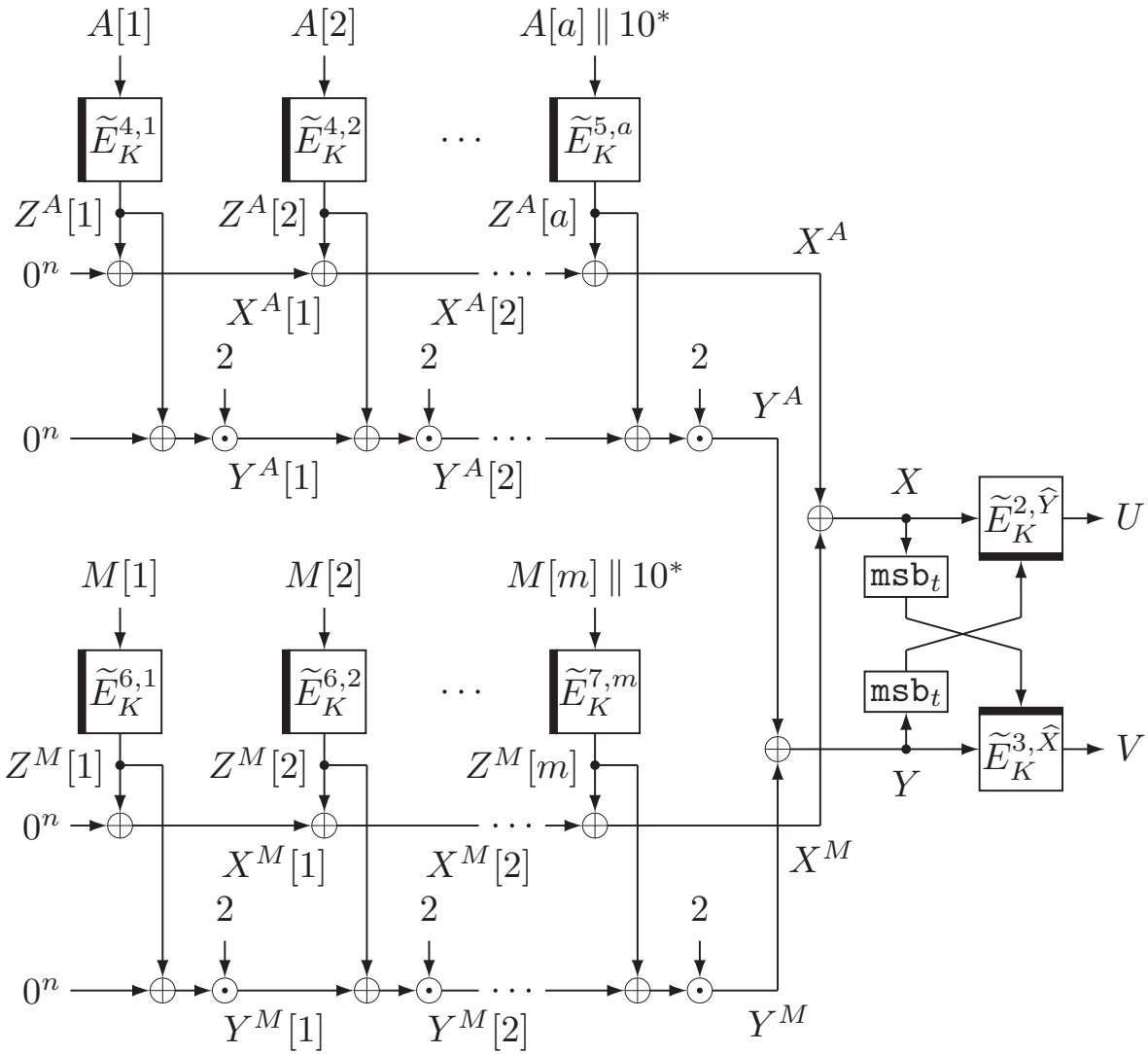
$O(2^{n/2})$ Attack on PMAC2x

- W.H.P., $X_i = X'_j$ for some i and j, in which case $Y_i = Y'_j$
- $(U_i, V_i) = (U'_j, V'_j)$ for PMAC2x, but this is unlikely for a random function that outputs $2n$ bits



$O(2^{n/2})$ Attack on PMACx and SIVx

- The attack can be adapted to break PMACx (n-bit output version of PMAC2x) and SIVx (both in privacy and authenticity)



$O(2^{n/2})$ Attack on PMACx and SIVx

- These attacks make use of the way the input is padded
  - A bug in the padding method
  - could be avoided by appropriately changing the padding method
- a variant of the attack against SIVx that does not rely on the padding (both in privacy and authenticity)
  - Changing the padding does not prevent this attack

Scheme	Type	Provable security bound	Attack complexity
PMACx	PRF	$O(q^2/2^{2n} + q^3/2^{3n})$ [LN17]	$q = O(2^{n/2})$
PMAC2x	PRF	$O(q^2/2^{2n} + q^3/2^{3n})$ [LN17]	$q = O(2^{n/2})$
SIVx	DAE	$O(q^2/2^{2n} + q^3/2^{3n})$ [LN17]	$q = O(2^{n/2})$

Thank You

http://eprint.iacr.org/2017/220