Cryptanalysis of PMACx, PMAC2x, and SIVx

Kazuhiko Minematsu\textsuperscript{1}  Tetsu Iwata\textsuperscript{2};\textsuperscript{*}

\textsuperscript{1}NEC Corporation, Japan
\textsuperscript{2}Nagoya University, Japan

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

\footnotesize{\textsuperscript{*}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

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Type</th>
<th>Provable security bound</th>
<th>Attack complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMACx</td>
<td>PRF</td>
<td>$O\left(\frac{q^2}{2^{2n}} + \frac{q^3}{2^{3n}}\right)$ [LN17]</td>
<td>$q = O(2^{n/2})$</td>
</tr>
<tr>
<td>PMAC2x</td>
<td>PRF</td>
<td>$O\left(\frac{q^2}{2^{2n}} + \frac{q^3}{2^{3n}}\right)$ [LN17]</td>
<td>$q = O(2^{n/2})$</td>
</tr>
<tr>
<td>SIVx</td>
<td>DAE</td>
<td>$O\left(\frac{q^2}{2^{2n}} + \frac{q^3}{2^{3n}}\right)$ [LN17]</td>
<td>$q = O(2^{n/2})$</td>
</tr>
</tbody>
</table>

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

---

\[ (M[1], \ldots, M[m]) \overset{n}{\leftarrow} M, \ |M[m]| = n \]
\[(M[1], \ldots, M[m]) \leftarrow^n M, \ |M[m]| < n\]
\( O(2^{n/2}) \) Attack on PMAC2x

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

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Type</th>
<th>Provable security bound</th>
<th>Attack complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMACx</td>
<td>PRF</td>
<td>$O(q^2/2^{2n} + q^3/2^{3n})$ [LN17]</td>
<td>$q = O(2^{n/2})$</td>
</tr>
<tr>
<td>PMAC2x</td>
<td>PRF</td>
<td>$O(q^2/2^{2n} + q^3/2^{3n})$ [LN17]</td>
<td>$q = O(2^{n/2})$</td>
</tr>
<tr>
<td>SIVx</td>
<td>DAE</td>
<td>$O(q^2/2^{2n} + q^3/2^{3n})$ [LN17]</td>
<td>$q = O(2^{n/2})$</td>
</tr>
</tbody>
</table>
http://eprint.iacr.org/2017/220