Improved Security Analysis for Blockcipher Based PRF

Mridul Nandi

National Institute of Standards and Technology

Blockcipher based PRF

- CBC
- OMAC
- PMAC
- Many others

Similarities

- The underlying blockcipher applied in a sequence (even for parallel MAC).
- May have one or more blockcipher keys (EMAC requires two) and some other auxiliary keys (TMAC, XCBC)
- Intermediate inputs are some affine functions of intermediate outputs.
- The final output is the output of the final blockcipher outputs.

Similarities we consider

- The underlying blockcipher applied in a sequence (even for parallel MAC).
- One blockcipher key and no other auxiliary key.
- Intermediate inputs are some affine functions of intermediate outputs.
- The final output is the output of the final blockcipher outputs.
- CBC, OMAC, PMAC and also DAG based PRF

Similarities we consider

- CBC, OMAC, PMAC and also DAG based PRF
- We call the class Affine Domain Extension or ADE.

PRF-security

- PRF-Advantage for F (RF is the random function) = $|\Pr[A^F = 1] - \Pr[A^{RF} = 1]|$
- If small then we call F PRF
- How small?
- We already know $l^2q^2/2^n$.
- Bellare et al. in Crypto 2005 reduces to $lq^2/2^n$ for CBC (with prefix-free messsages).
- Later for XCBC, PMAC and TMAC.

PRF-security for ADE

- Not secure for any ADE.
- For example, if trivial collision on final output can be found with probability one.
- We say an ADE is valid if trivial collision between a final output and intermediate output can not be found with probability one (same is used for CBC).

Our Result

- **All valid ADE are PRF-secure. But** What is the bound?
- We provide a generic bound
  - PRF-advantage(F) < $sq/2^n + N(F)/2^n$
  - $N(F) < s^2$
- One may compute N(F) given the construction. We compute for CBC, PMAC, OMAC and we found $N(F) < sq/2^n$

Proof Idea

- Using Vaudenay’s Decorrelation technique.
- Combinatorial approach is used.

Open Problem

- To prove or disprove in general $N(F) < sq/2^n$