RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: CRYP-R02

Constructions of Hash Functions and Message Authentication Codes

Yusi Zhang

PhD in Computer Science
University of California, Davis
yzhangad@gmail.com

RSA Conference2015

San Francisco | April 20-24 | Moscone Center

Use an Error-Correction Code for Fast, Beyond-birthday-bound Authentication

#RSAC

Motivation: Beyond-birthday-bound

- Birthday Barrier: the $2^{n/2}$ - level.
- Best Known Bounds for Some MAC Modes:
  - CMAC: $O(q\sigma/2^n)$
  - PMAC: $O(q^2\rho/2^n)$

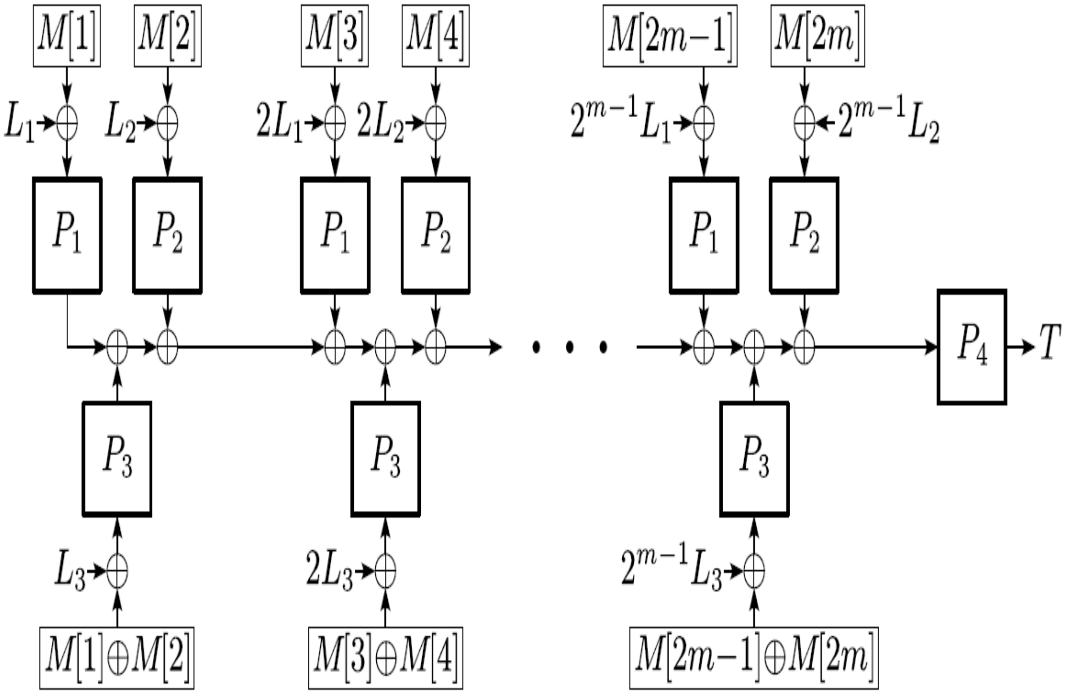
- Acceptable in Most Cases, but...

That depends on n!

Motivation Cont'd

- Problems:
  - Short 64-bit cipher is still widely deployed (financial institutions).
  - Hard to replace these ciphers (compatibility).
- Objective of this work:
  - Go beyond the Birthday Barrier.
  - Relatively Simple Modifications on an Existing Scheme (e.g. PMAC).
  - Avoid too much cost on efficiency and key setup.

Prior Work: PMAC with Parity (PMACwP) [Yasuda'12]



- Achieve a New Bound:

  $O(q^2/2^n + q\rho\sigma/2^{2n})$

- Shortcomings:
  - 4 independent keys needed.
  - 1.5 slowdown.

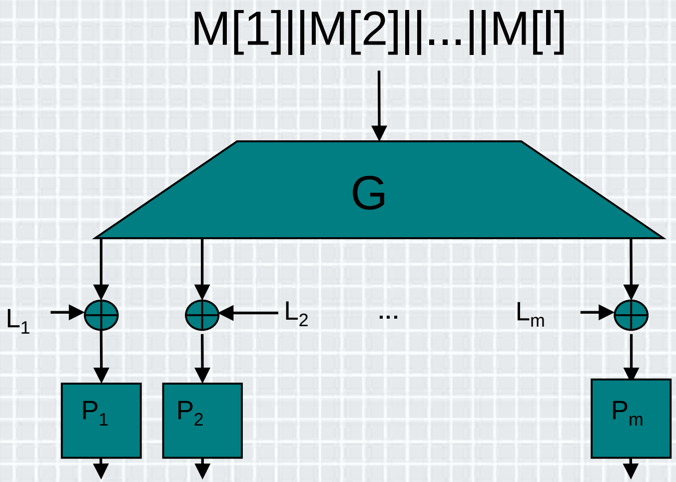
Generalizing the "Parity-processing" Stage

- M[1], M[2] -> M[1], M[2], M[1] + M[2] in matrix form:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$$

- What about a larger matrix?
- Desired Property: As many different output blocks as possible.
- Exactly the property of an MDS code.

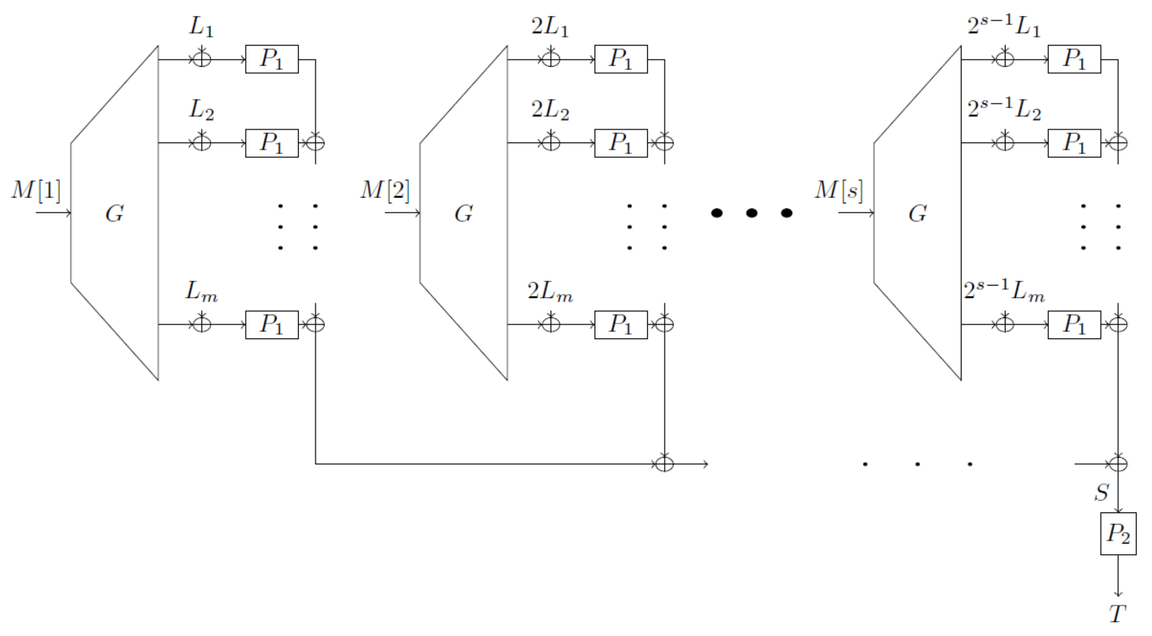
Generalization from 2 Differences to Multiple Ones



- Improve the bound to $O(q^2/2^n+q\sigma\rho^{d-1}/2^{dn})$
- But even more keys are needed...

Reduce the Number of Keys

- In the analysis, only interested in the collision of the final input.
- Possible to replace the many independent ciphers with a single one.
- Of course, a new proof becomes necessary...



Result of the New Analysis

- The bound is degraded:
  - from $O(q^2/2^n+q\sigma\rho^{d-1}/2^{dn})$ to $O(q^2/2^n+q\sigma\rho^{(d-1)/2}/2^{(d+1)n/2})$.
- **But, we've reduced the key number from m+1 to 2 only!**

Summary

- We've generalized Yasuda's PMACwP by replacing its "parity-processing" with an MDS matrix multiplication.
- Based on the basic generalization, we further reduced the number of keys to 2, at the cost of a degradation of provable security.
- Theoretically, our scheme can achieve a rate arbitrarily close to 1, a security level arbitrarily close to 2^n, by choosing large enough MDS matrices.
- Surprisingly, the above can be done by 2 independent keys only.

Candidate Topics for Future Work

- Reduce the number of keys even further: 2 to 1?
- Go beyond "birthday-barrier" for query numbers, q, as well.
- Analysis of Online Security.