A Keyed Sponge Construction with Pseudorandomness in the Standard Model

Donghoon Chang

Third SHA-3 Candidate Conference
March 22, 2012

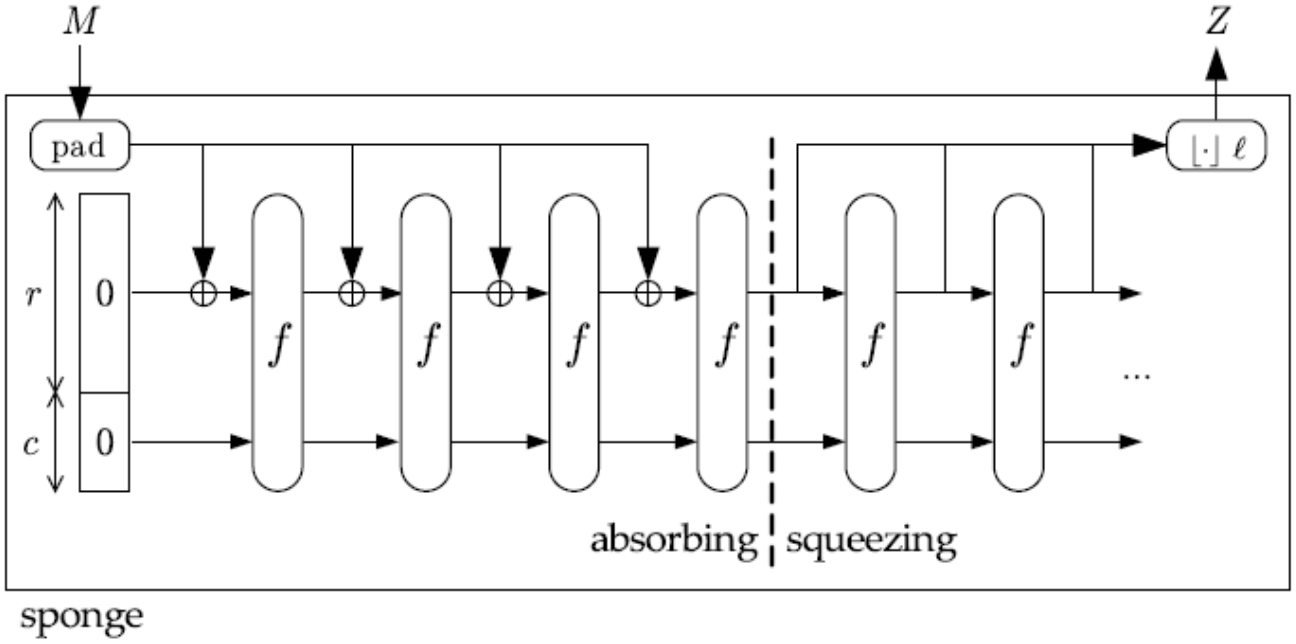
Joint work with

- Morris Dworkin[1]
- Seokhie Hong[2]
- John Kelsey[1]
- Mridul Nandi[3]

[1] National Institute of Standards and Technology (NIST), USA
[2] CIST, Korea University, Korea
[3] Indian Statistical Institute (ISI), Kolkata, India

Sponge Construction

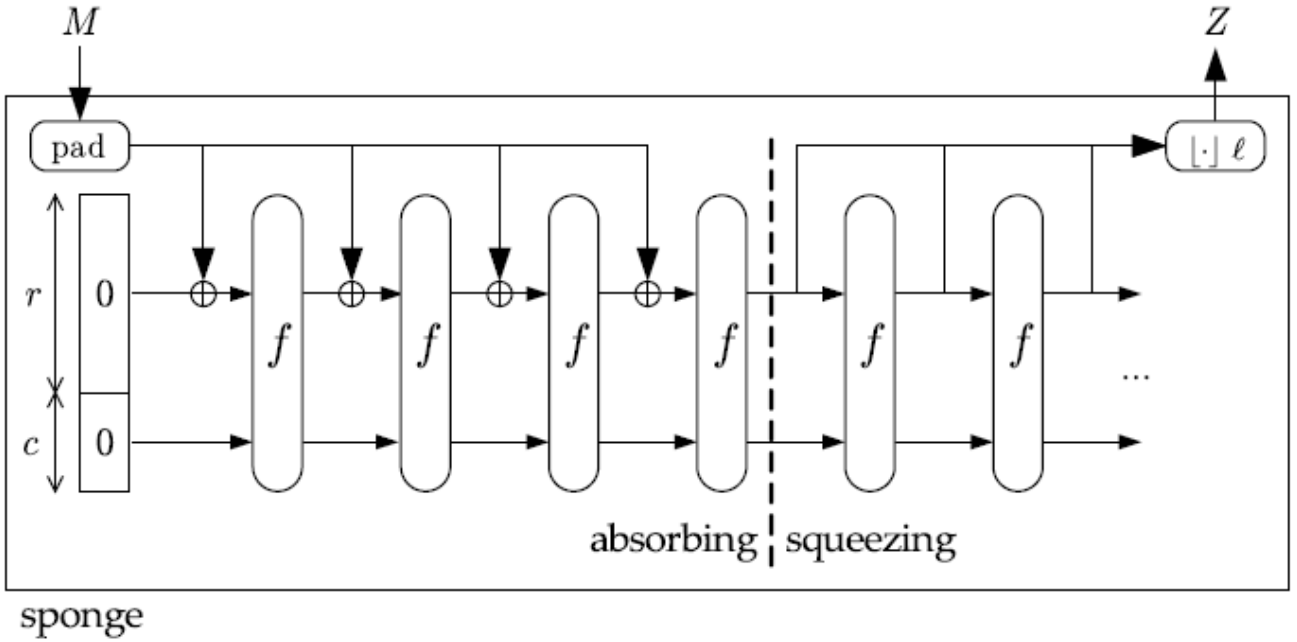
- Designed by Bertoni, Daemen, Peeters, and Van Assche (Eurocrypt ’08);
- Influenced concrete hash designs such as Keccak, PHOTON, Quark, and Spongent.



f: a b-bit permutation with $b = r + c$

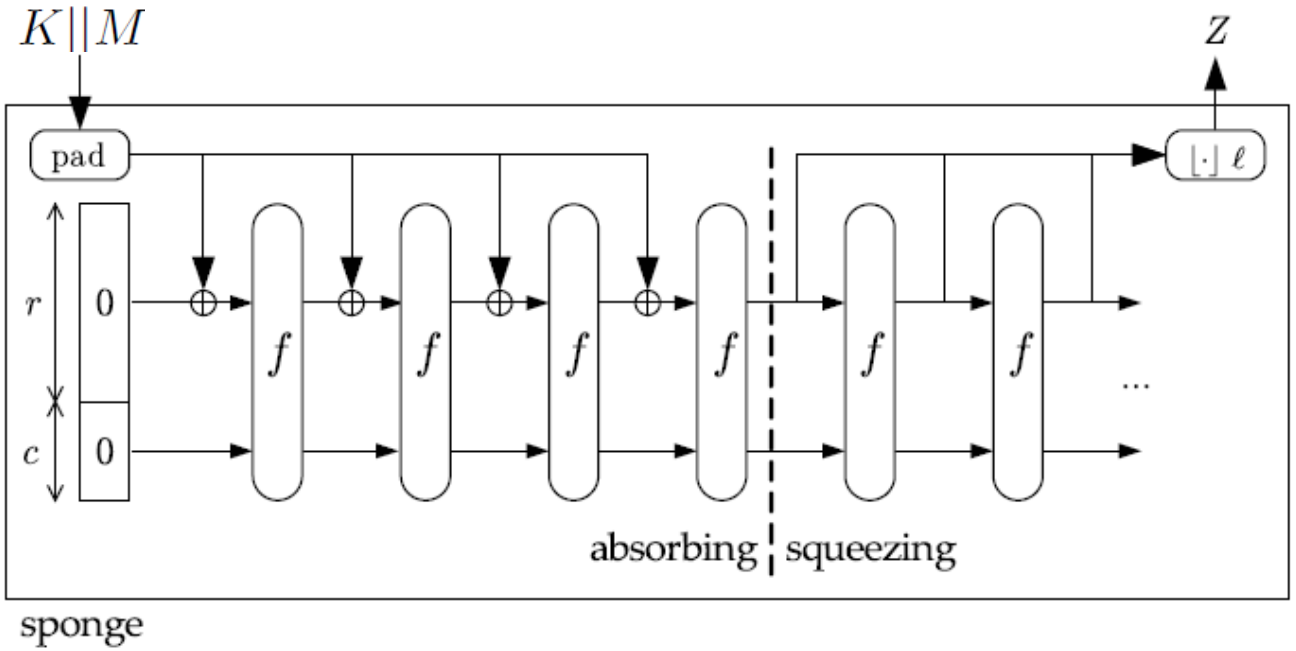
Security of Sponge Construction (Eurocrypt '08)

- Sponge is indifferentiable from a random oracle when f is an ideal permutation or an ideal function (in other words, a fixed-input-length random oracle).



A Keyed Sponge Construction

- Defined by Bertoni, Daemen, Peeters, and Van Assche (SKEW'11).



f: a b-bit permutation with $b = r + c$

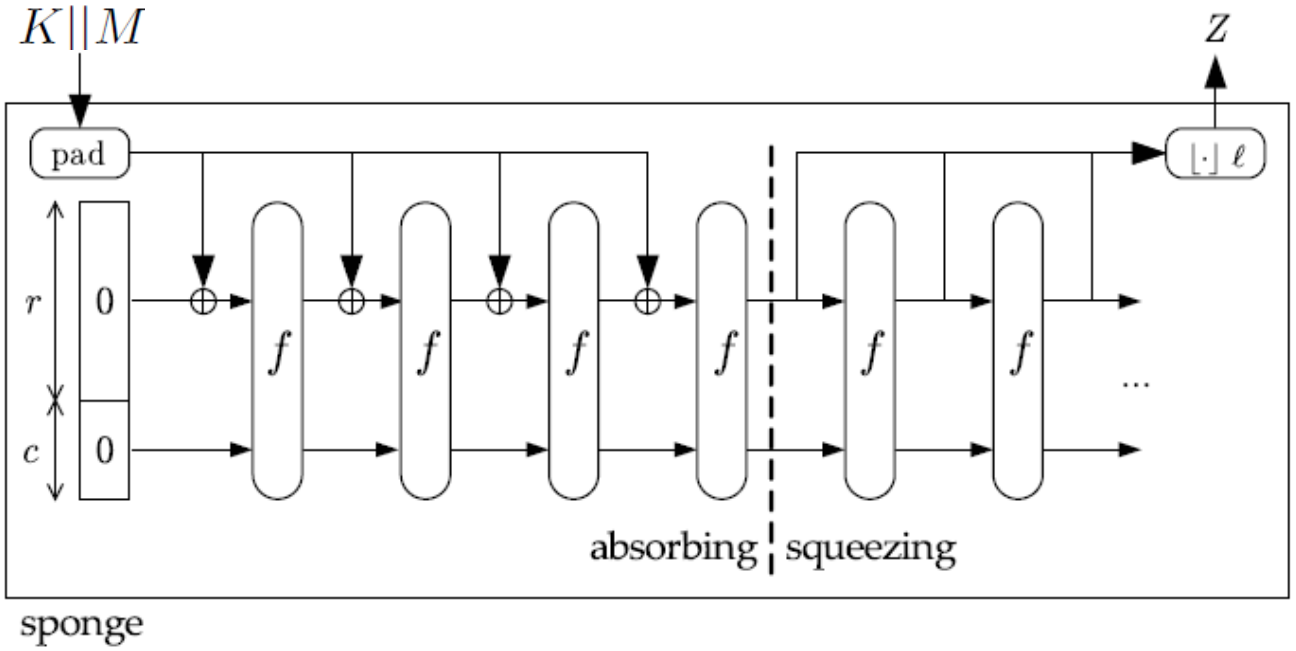
Applications of A Keyed Sponge Construction (SKEW ’11)

- Encryption as a stream cipher
  - Squeezing sponge($K||IV$), or
  - Random-access key stream block k_i = sponge($K||IV||i$).

- Authentication: Sponge($K||M$)=MAC.

Security of Keyed Sponge Construction (SKEW '11)

- Pseudorandomness is proved in the ideal permutation model.

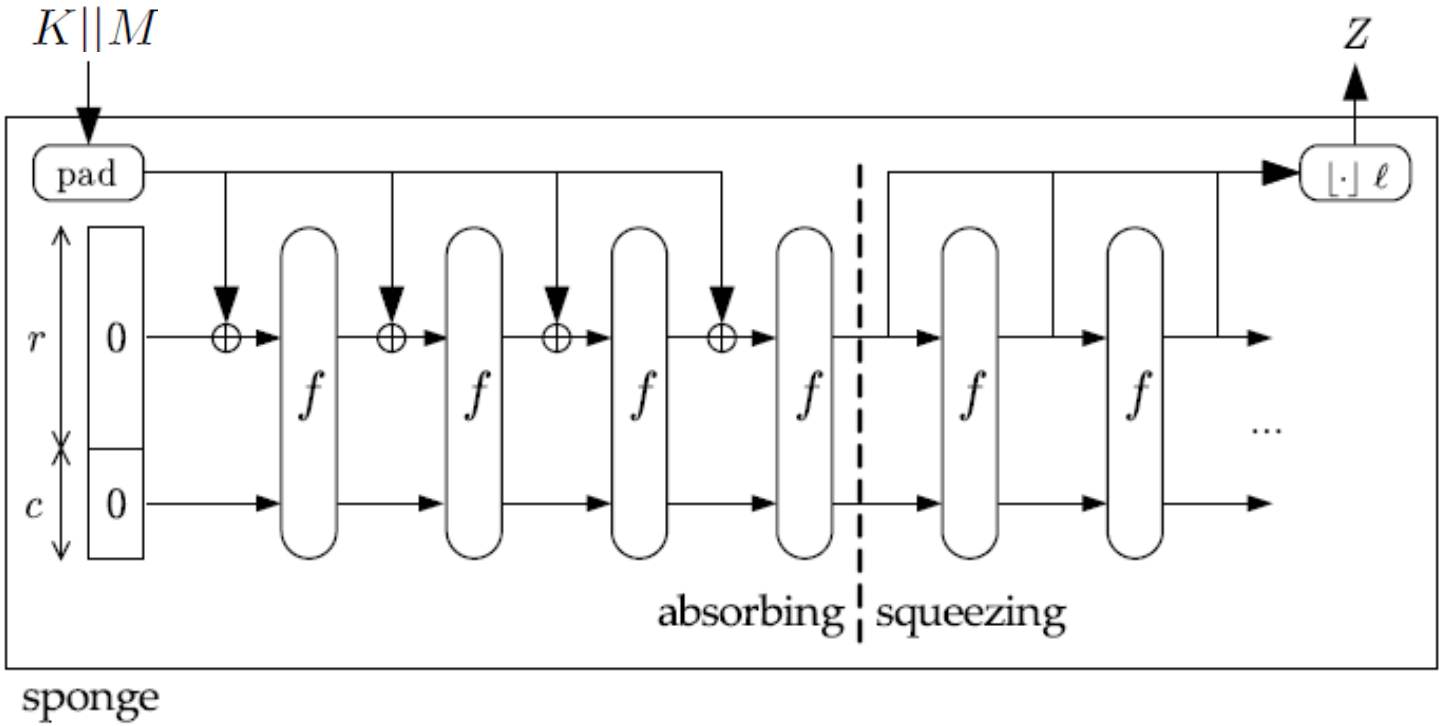


Proof assumes f is an ideal permutation.

Our work

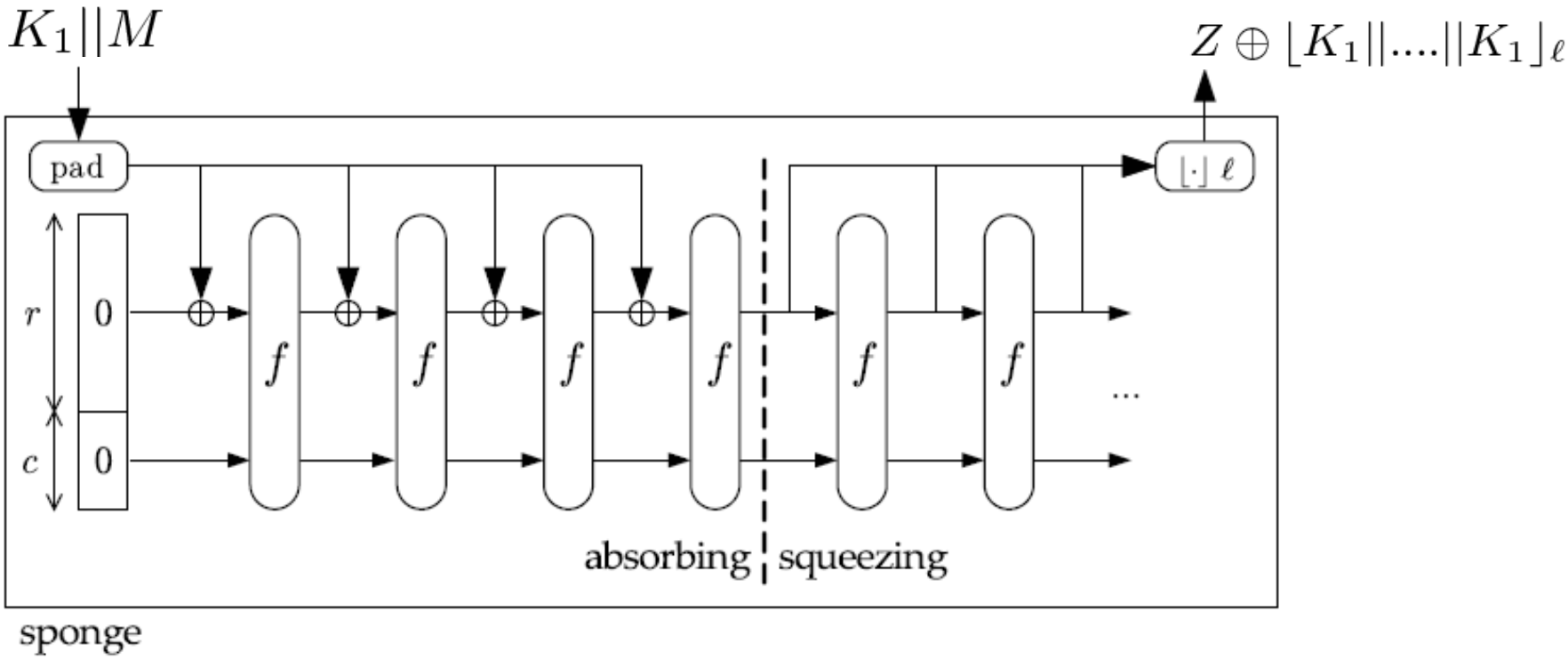
- We give a new keyed sponge construction based on the Even-Mansour permutation.
- We give variants for three key sizes.
- The security of the construction doesn’t depend on the ideal model, but on the standard model with a practical assumption.

A Keyed Sponge Construction (SKEW ’11)



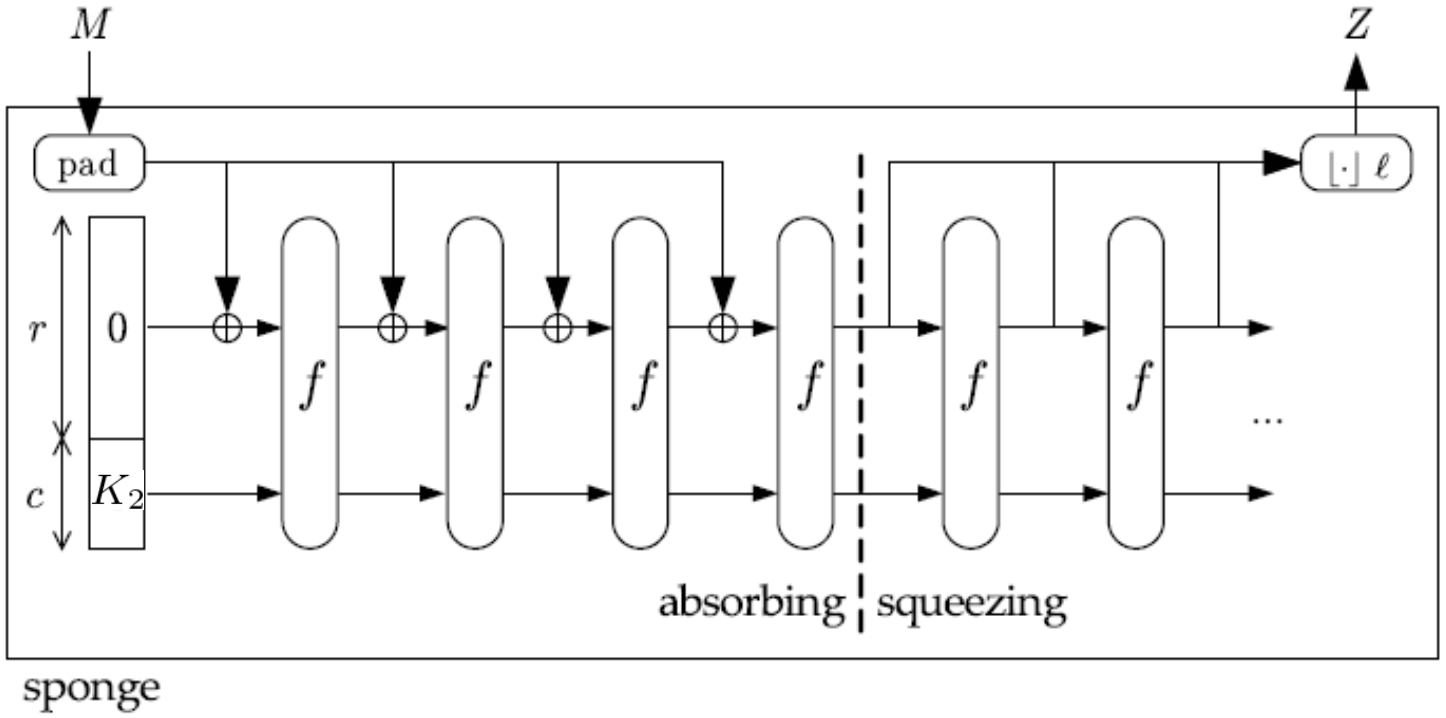
Our Keyed Sponge Construction #1 (No modification to Sponge)

- K_1 is an r-bit secret key.



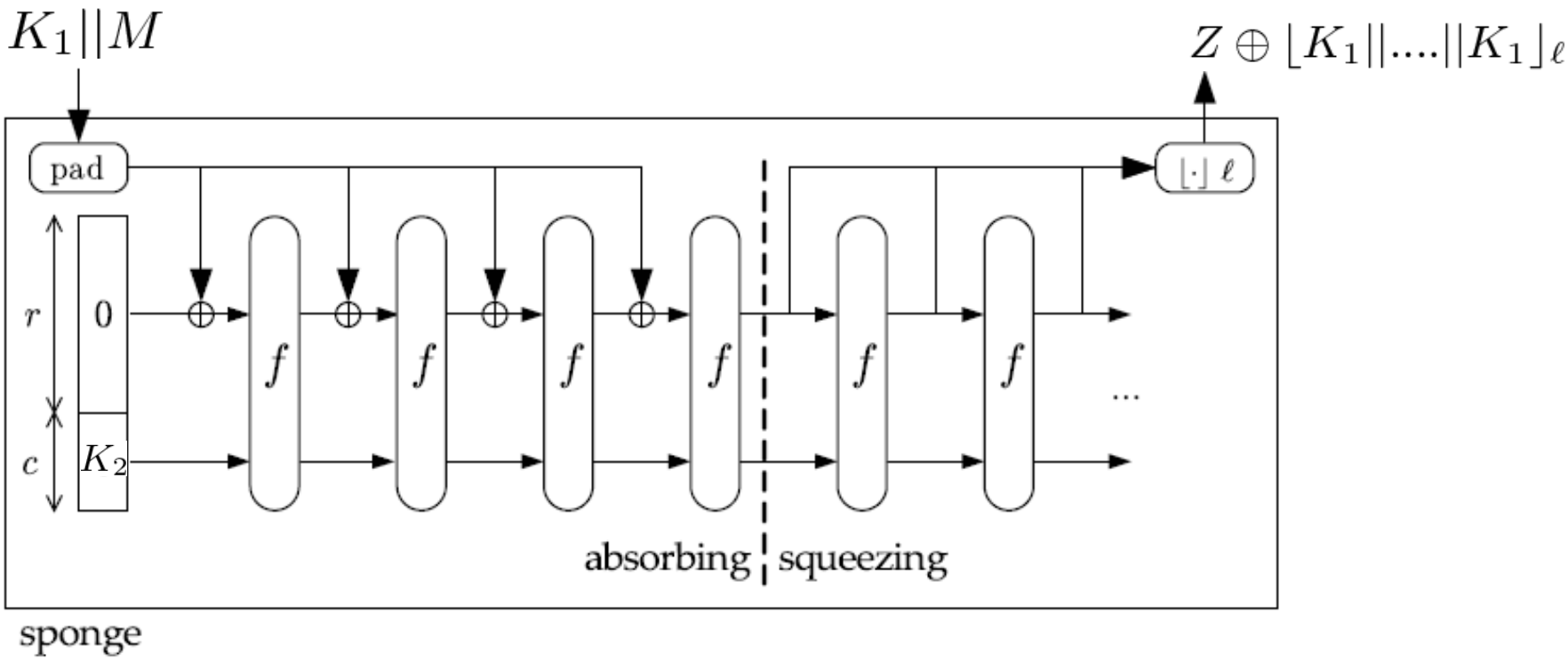
Our Keyed Sponge Construction #2 (Modify the Initial Value)

- K_2 is a c-bit secret key.



Our Keyed Sponge Construction #3 (Combination of #1 and #2)

- K_1 and K_2 are r-bit and c-bit secret keys.

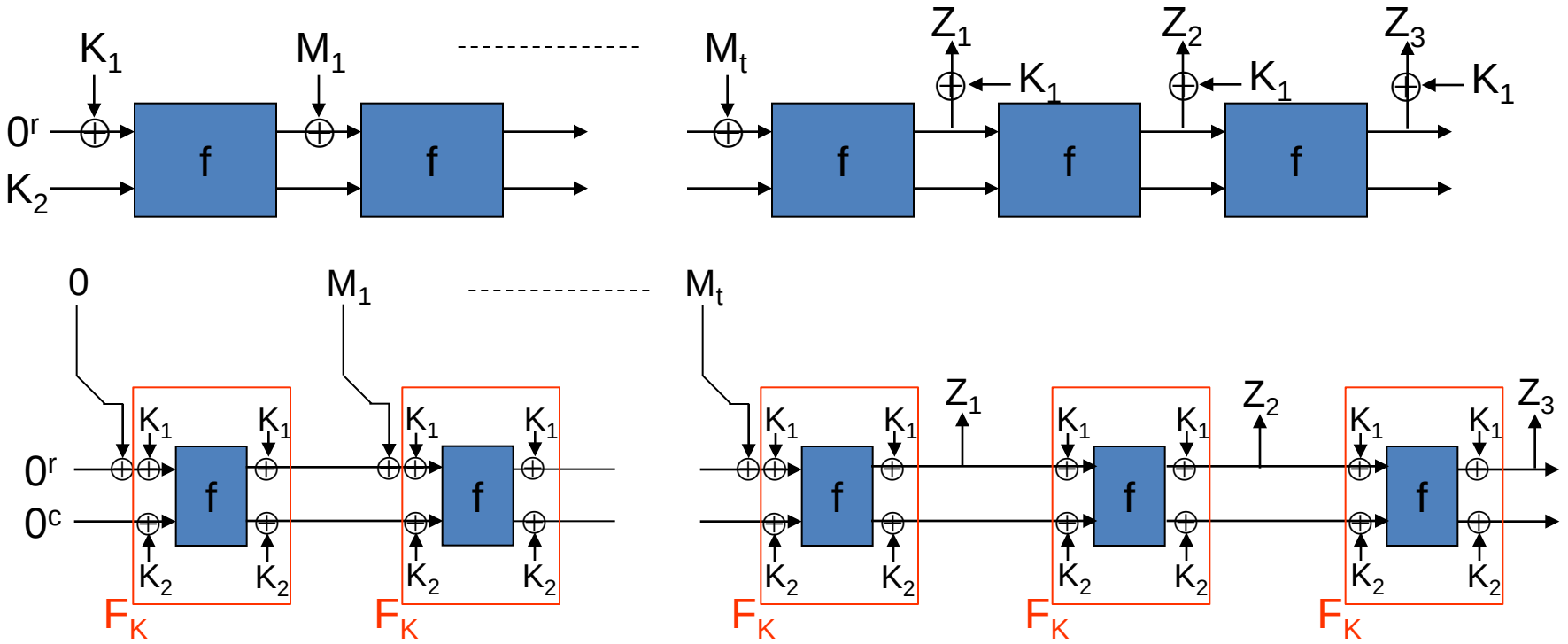


Security Assumption

- The Even-Mansour permutation with a single key is $F_K(\cdot)=f(K\oplus\cdot)\oplus K$.
- Instead of assuming $f(\cdot)$ is an ideal permutation, we assume $F_K(\cdot)$ is pseudorandom.
- If $F_K(\cdot)$ is pseudorandom, then our construction is also pseudorandom.

Underlying Proof Idea

- These two descriptions are the same.



Best-Known Attack on $F_K(\cdot)$

- Due to Dunkelman et al [Eurocrypt ’12];
- Assumes $|K|=b$;
- Known plaintext PRP attack on $F_K(\cdot)$;
- Complexity $DT=2^b$, where D and T refer to data and time complexity;
- Generic.

Conclusion

- We showed that a new keyed sponge construction is pseudorandom under the standard model.
- It is an open question whether our technique can be applied to other sponge-like constructions.