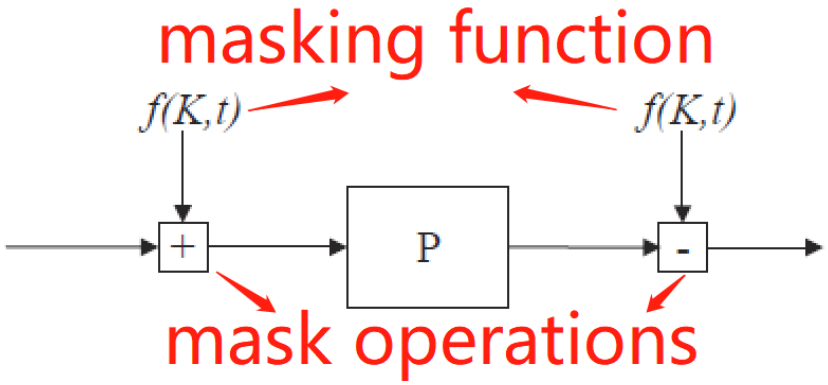
Universal Tweakable Even-Mansour Cipher and Its Applications

Ping ZHANG

Frontiers of Computer Science, DOI: 10.1007/s11704-022-1466-1

Problems & Ideas

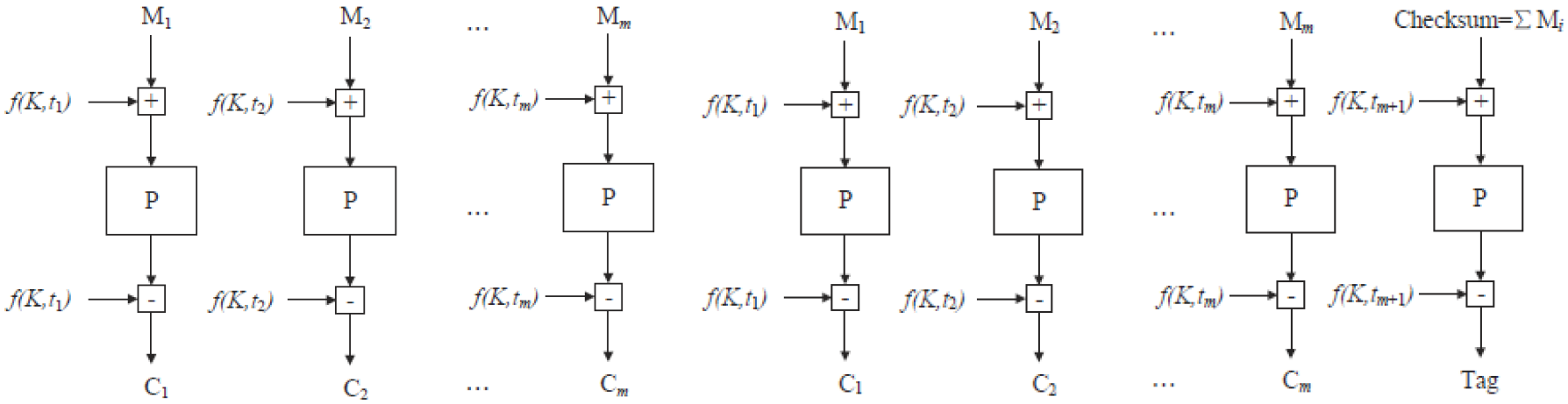
- Problems of conventional Boolean mask techniques:
  - The properties of Boolean mask techniques are not comprehensive enough and the Boolean mask operation is more vulnerable.
  - Arithmetic mask techniques are necessary to construct some cryptographic algorithms in the real world.
- Ideas: A formal definition of a universal masking function is described, a universal tweakable Even-Mansour cipher UTEM is presented, and efficient instantiations and applications of UTEM are provided.



UTEM: a universal tweakable Even-Mansour cipher. P is a random permutation, *f(K,t)* is a universal masking function with tweak *t* and key *K* schedule, and binary mask operations include Boolean and Arithmetic (addition and Multiplication) mask operations.

Main Contributions

- Contributions:
  - We describe a formal definition of a universal masking function and provide a universal tweakable Even-Mansour cipher UTEM;
  - We delineate the multi-key security and its composition of UTEM in fine granularity;
  - To concertize UTEM, some efficient instantiations of the universal masking function can be shown.
  - We present two UTEM-based provably secure encryption and authenticated encryption modes TIE-plus and IAPM-plus.



Two applications of UTEM. Left: TIE-plus, a new UTEM-based tweak incrementation encryption mode; Right: IAPM-plus, a new UTEM-based tweakable authenticated encryption mode.