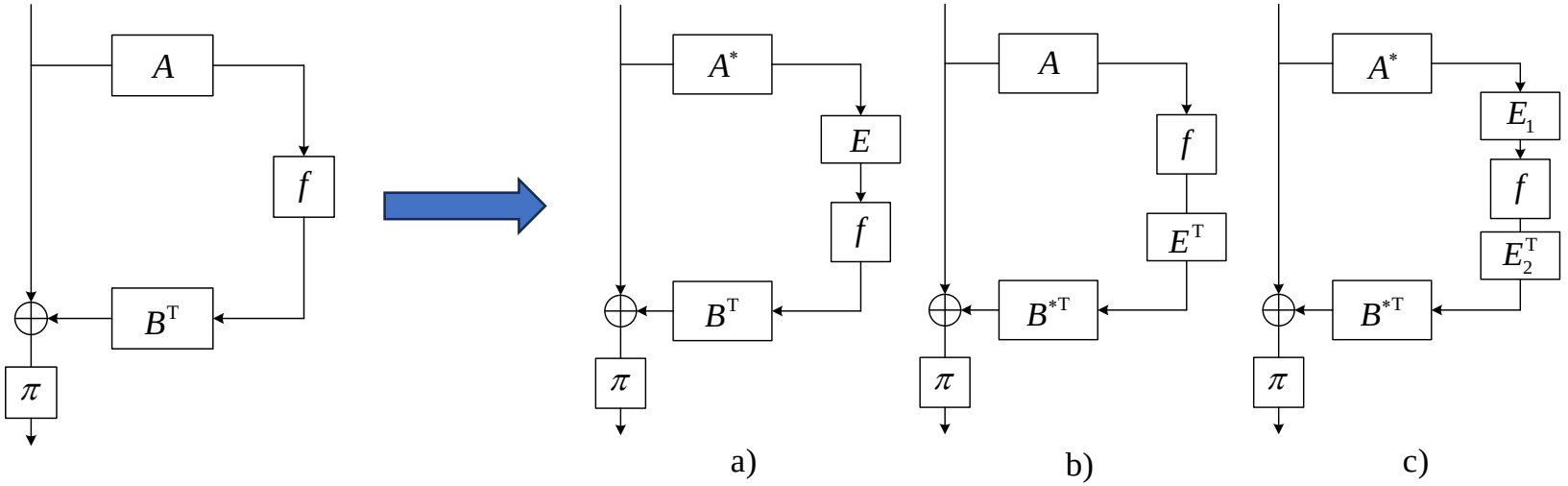
The design of Adjustable Generalized Feistel structure

Bo YU, Guoqiang LIU, Bing SUN, Chao LI, Xiaomei TANG

Frontiers of Computer Science, DOI: 10.1007/s11704-026-52078-9

Problems & Ideas

- Problems of designing new block cipher structures:
- Allows that the sizes of the round function and the branch to be different, e.g., DES and MATTER.
- The conditions of the parameters and the classification of them.
- Ideas: Transform the unified structure to three types via factoring the matrices before or after the round function. Investigate the design principles and the classification of the structures.

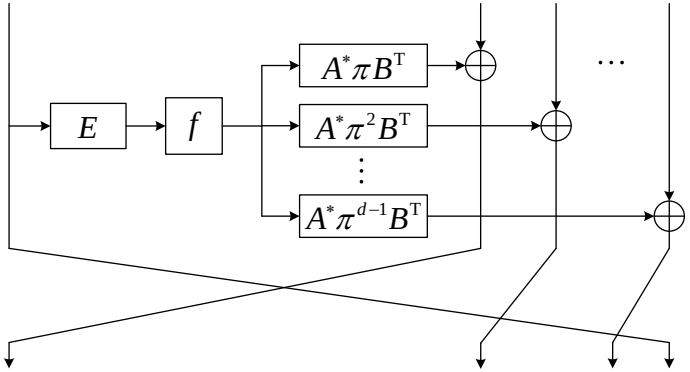


Three types by factoring the matrices of the unified structure

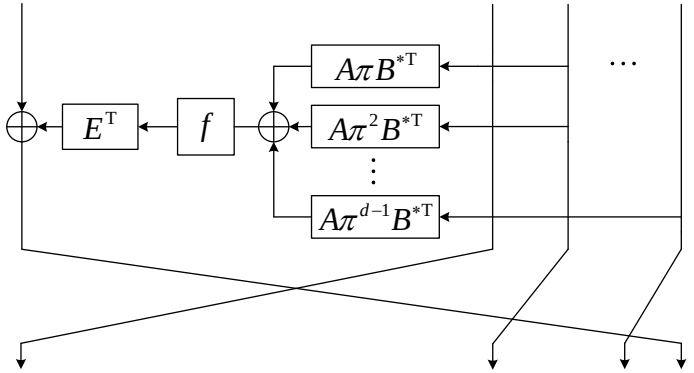
Main Contributions

➢Contributions:

- A new model called the Adjustable Generalized Feistel structure (AGFS) that allows size of the round function to be greater than or equal to the size of branch.
- A necessary and sufficient condition for the invertibility of AGFS and necessary conditions for a secure AGFS.
- Normalized forms of AGFS from the perspective of affine equivalence.



Normalized form of AGFS when the matrix ***A*** is decomposed



Normalized form of AGFS when the matrix ***B*** is decomposed