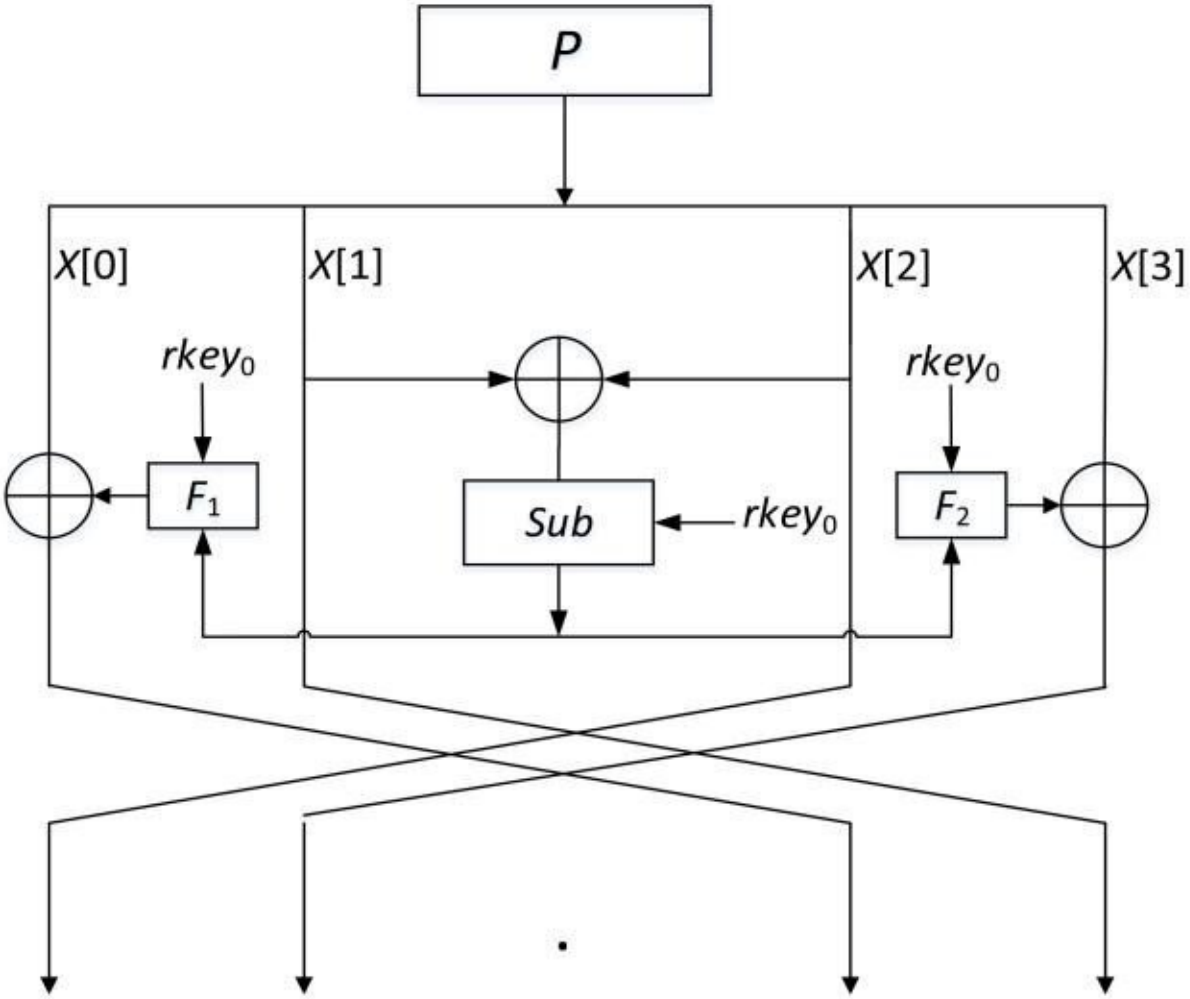
DBST: A lightweight block cipher based on dynamic S-box

June 8 2023



Credit: *Frontiers of Computer Science* (2022). DOI: 10.1007/s11704-022-1677-5

Block ciphers, a branch of modern cryptography, are playing a more prominent role in protecting information security as 5G technology develops. Although encryption algorithms of the traditional Feistel structure have great advantages in terms of consistent encryption and decryption, they have poor diffusion effects.

Additionally, they cannot adapt to the high throughput communication environment and resource-constrained devices. The S-box is the crucial nonlinear component in the block cipher and significantly determines the security of an algorithm. Unfortunately, the vast proportion of S-boxes exist in a static manner, which makes it difficult to effectively resist cryptographic attacks based on specific S-boxes.

To solve the problems, a research team led by Lang Li published their new research in *Frontiers of Computer Science*.

The team proposed a lightweight block cipher based on dynamic S-box named DBST for devices with limited hardware resources and high throughput requirements. The round function of DBST employs a novel generalized Feistel variant structure, which dramatically improves the diffusivity of the traditional Feistel structure. The S-box in the algorithm integrates bit-slice technology with subkeys to create a key-dependent dynamic S-box model that compensates for the shortcomings of static S-boxes.

In the research, they perform security analysis and hardware experiments on DBST. The experimental data demonstrate that the proposed algorithm has high security, high throughput rate and low hardware resources. Furthermore, differential analysis of the S-boxes proves that DBST's S-boxes have fewer differential properties than RECTANGLE's S-boxes.

More information: Liuyan Yan et al, DBST: a lightweight block

cipher based on dynamic S-box, *Frontiers of Computer Science* (2022). DOI: 10.1007/s11704-022-1677-5