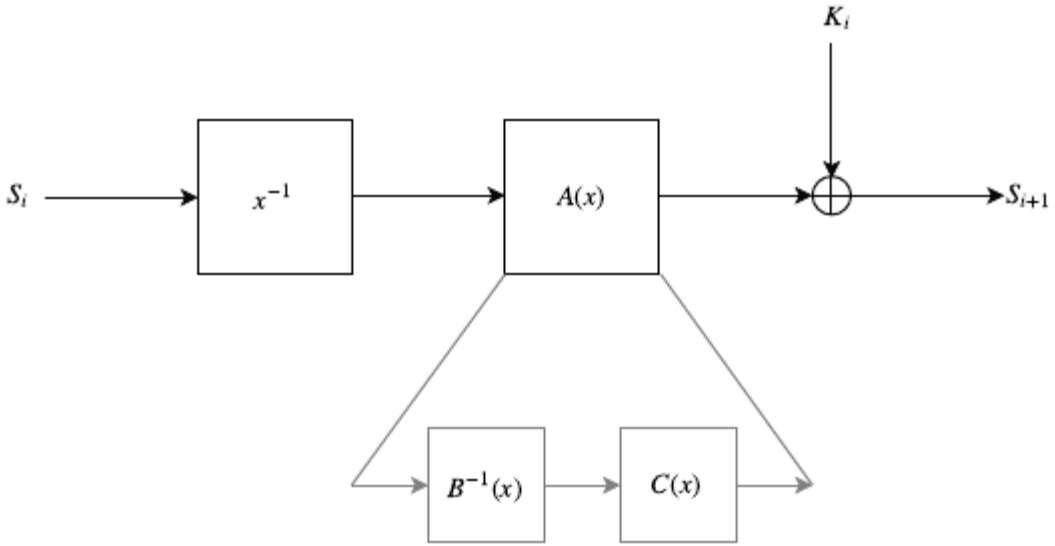
Efficient Symmetric Primitives for Advanced Cryptographic Protocols

(A Marvellous Contribution)


STARKWARE

Jarvis



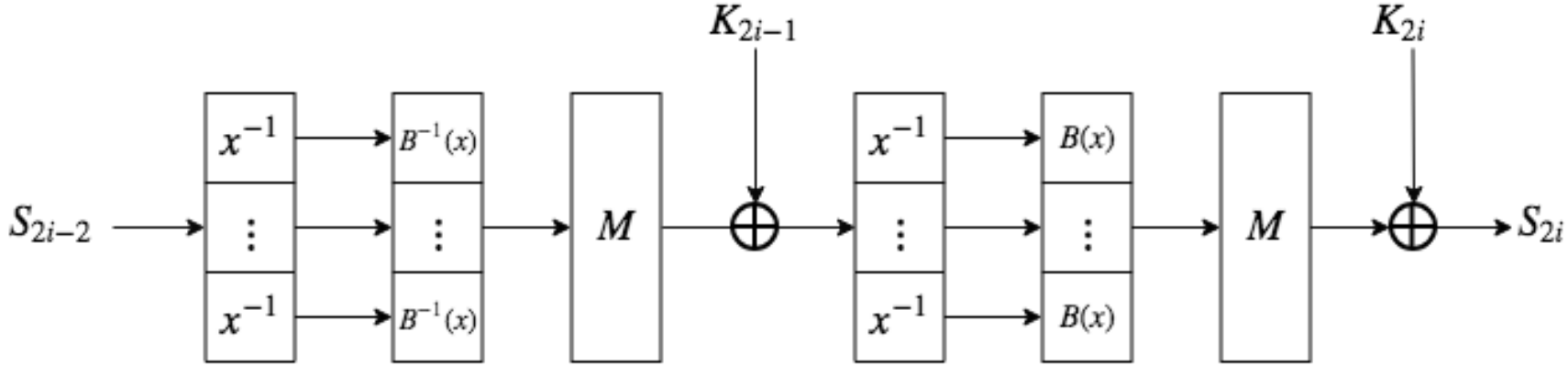
Algebraic cryptanalysis of Jarvis and Friday

Martin R. Albrecht, Carlos Cid, Dmitry Khovratovich, Lorenzo Grassi, Christian Rechberger

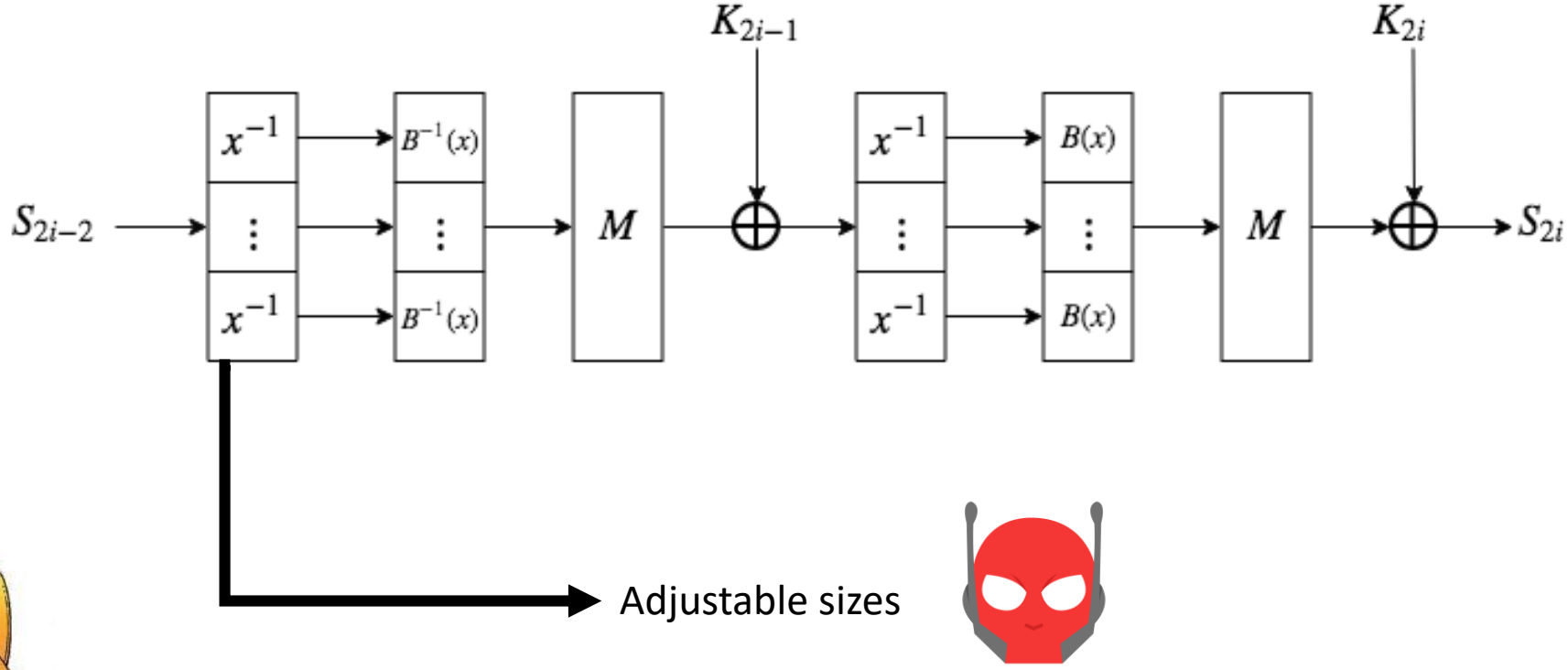
Royal Holloway University of London, Evernym Inc., ABDK Consulting, TU Graz

December 18th, 2018

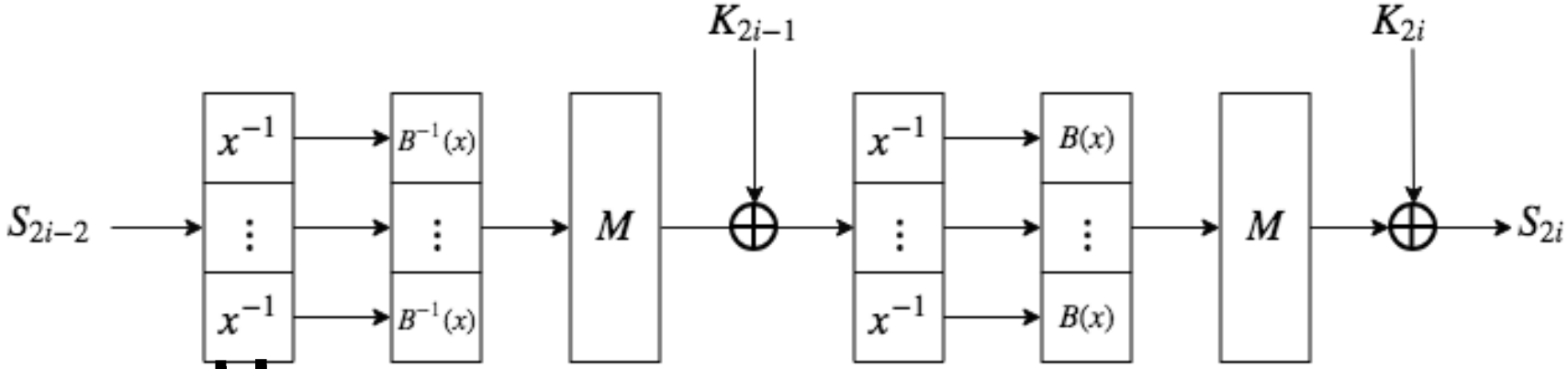
Vision



Vision



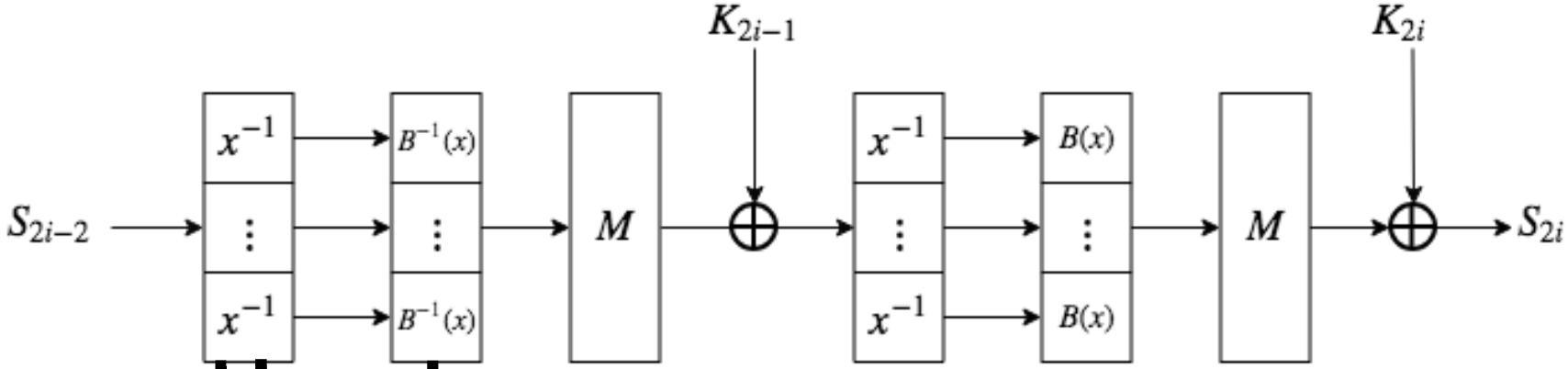
Vision



Adjustable sizes

Smashes Differential and Linear Attacks

Vision

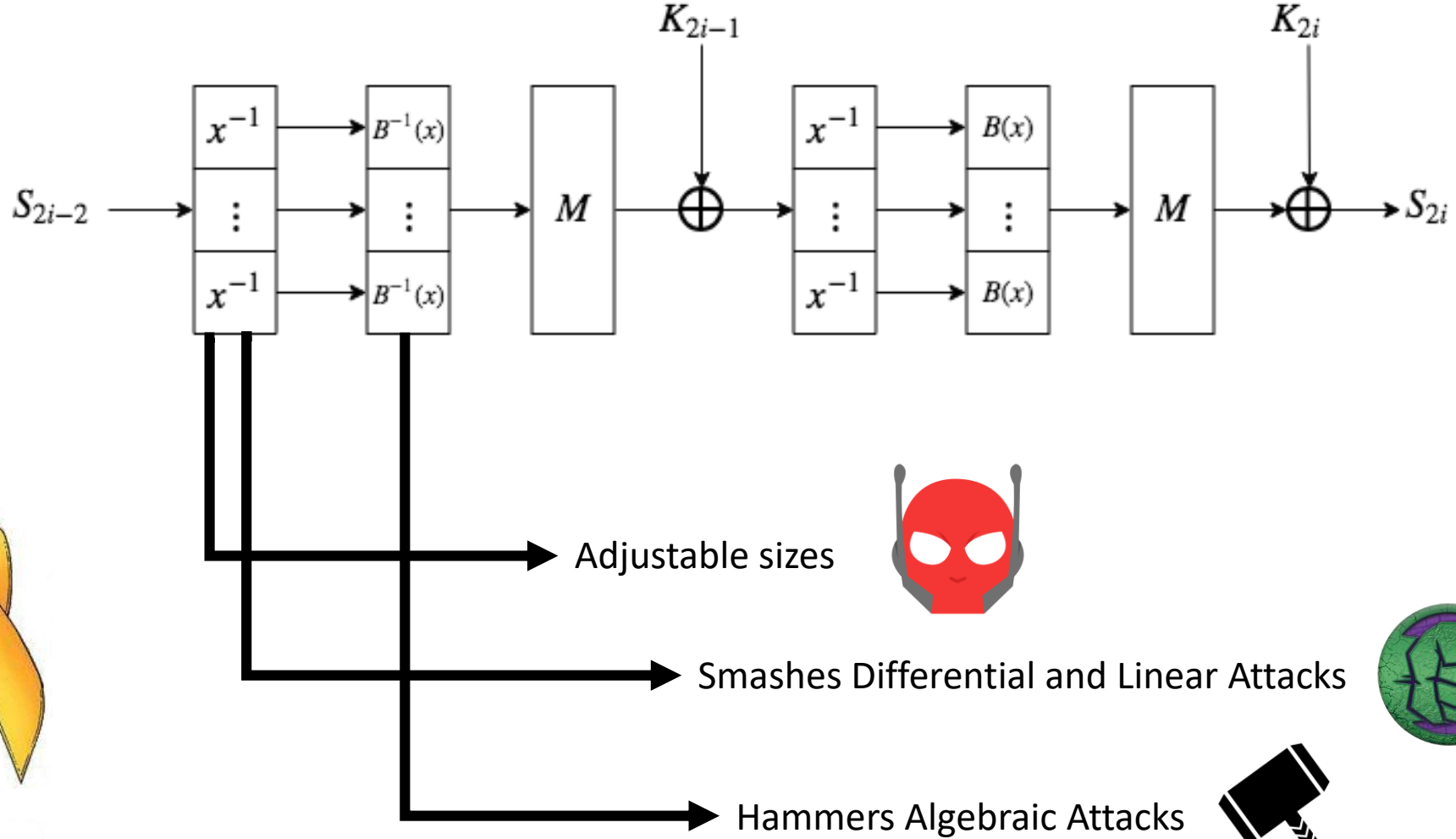


Adjustable sizes

Smashes Differential and Linear Attacks

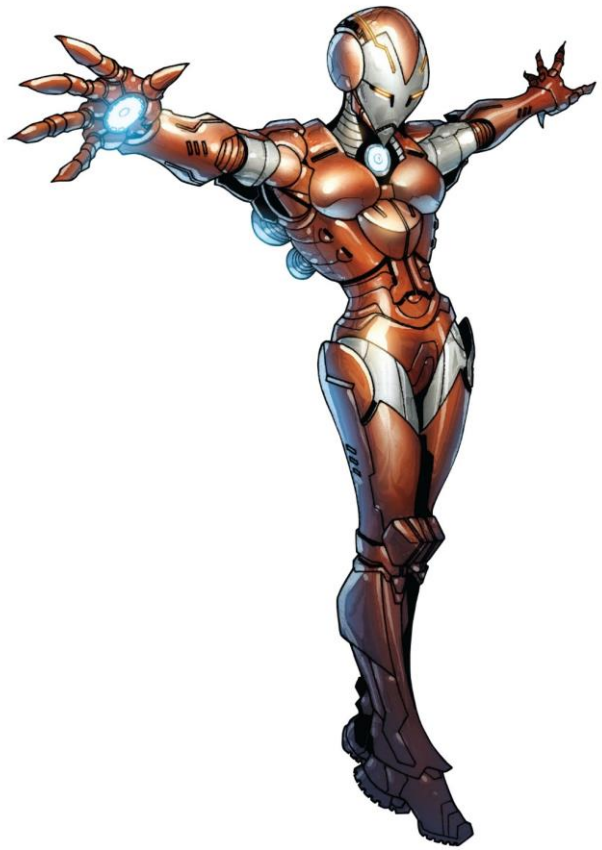
Hammers Algebraic Attacks

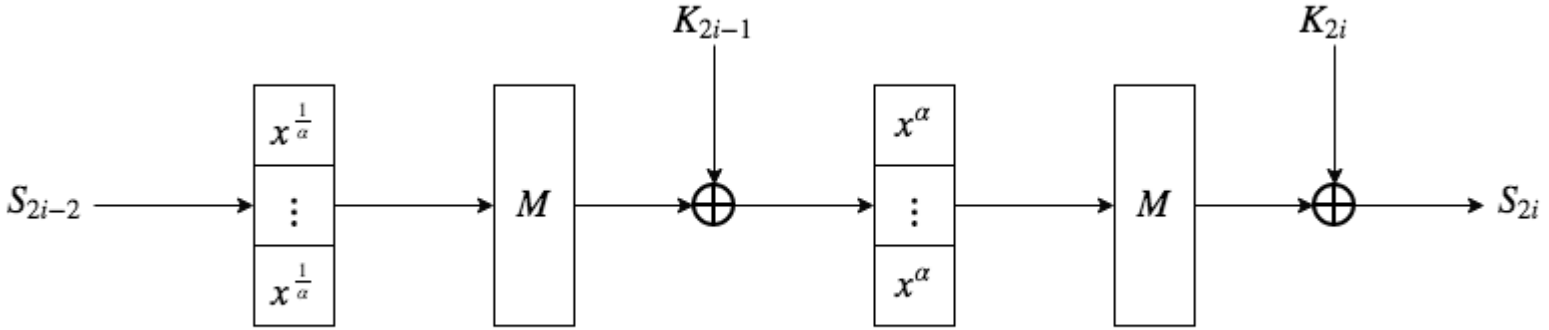
Vision



Generally STARK Friendly

Rescue





Now also in the prime field flavor


Thank You!