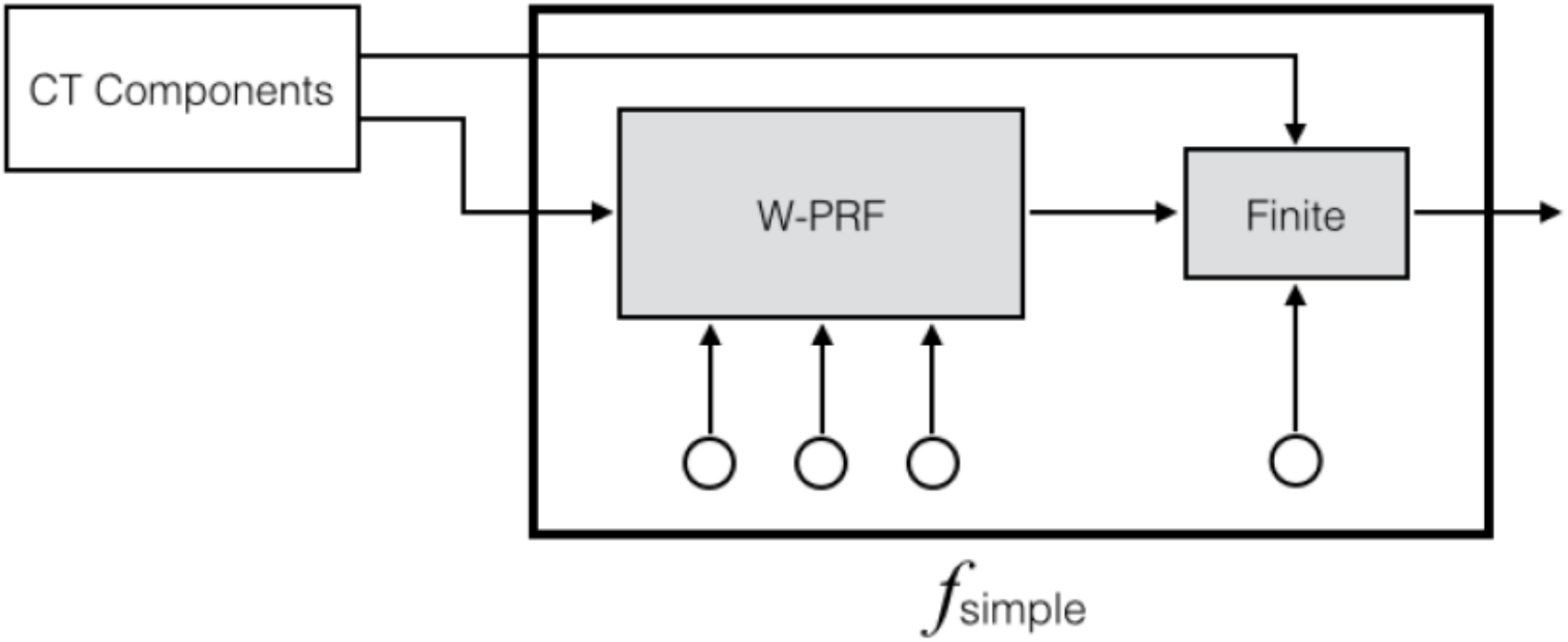
iO from FE for Simple Functions

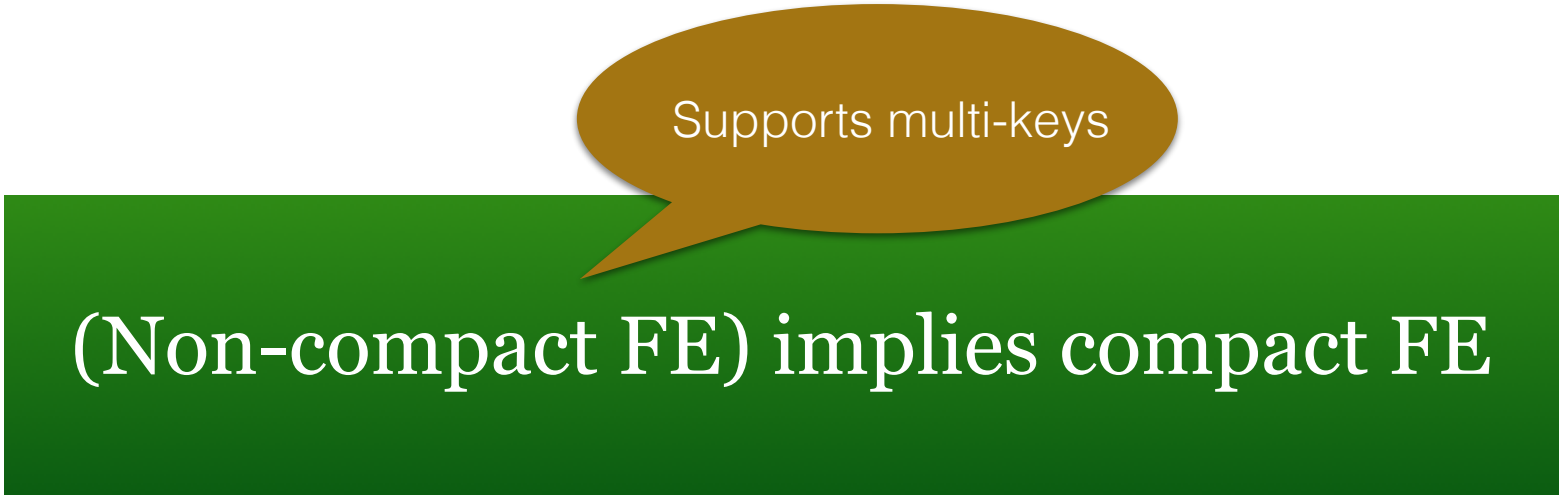
Prabhanjan Ananth Abhishek Jain Amit Sahai

Our result



FE supporting decryption keys for this functionality implies iO for circuits

(Non-compact FE) implies compact FE


Supports multi-keys
(Non-compact FE) implies compact FE

(Non-compact FE) implies compact FE

- This work + [AJ15,BV15]: Non-compact FE implies iO
- Implication: iO based on GGHZ14 mmap assumptions

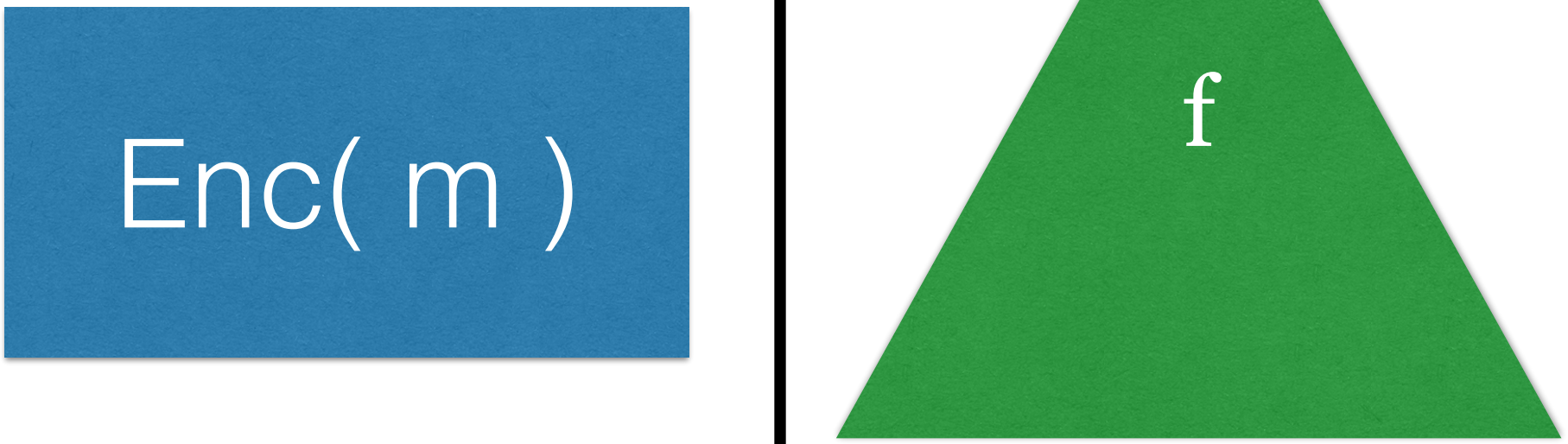
(Non-compact FE) implies compact FE

- This work + [AJ15,BV15]: Non-compact FE implies iO
- Implication: iO based on GGHZ14 mmap assumptions

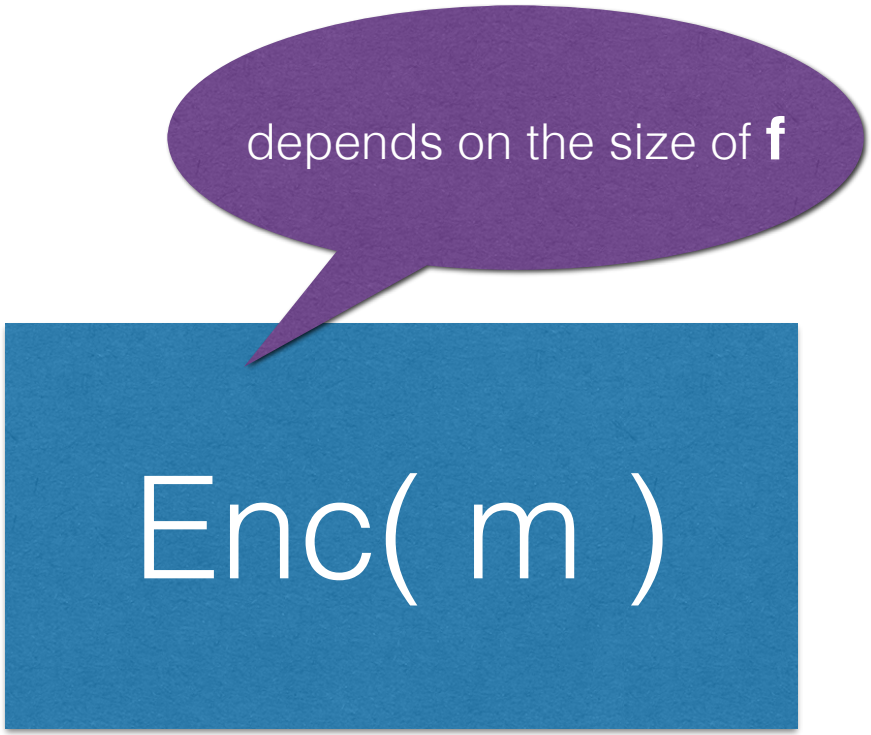
Also observed by Bitansky-Vaikuntanathan'15

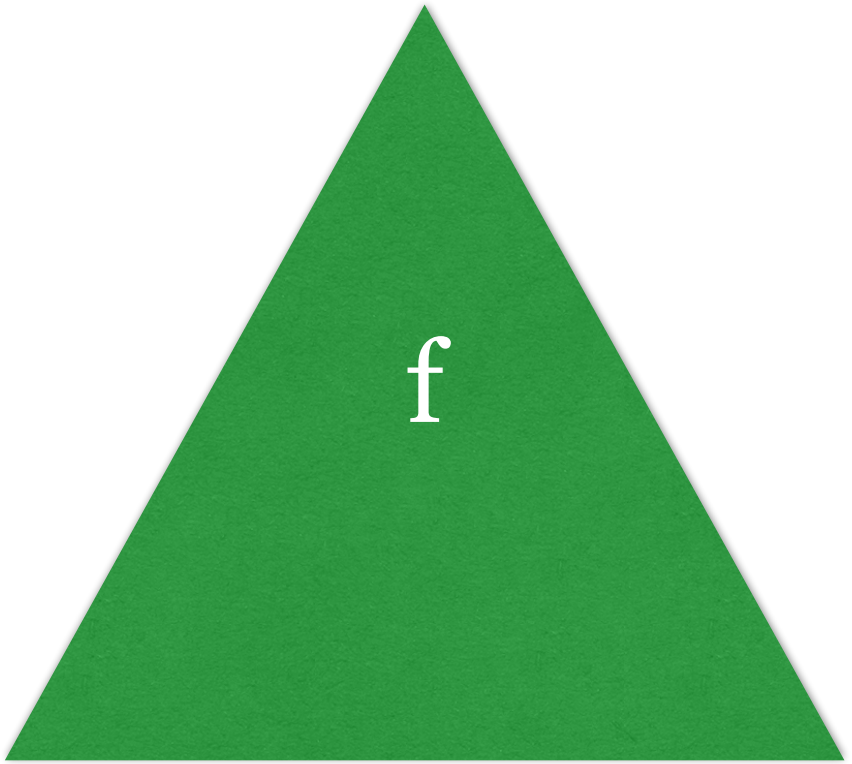
Main Idea

Non Compact FE



Non Compact FE

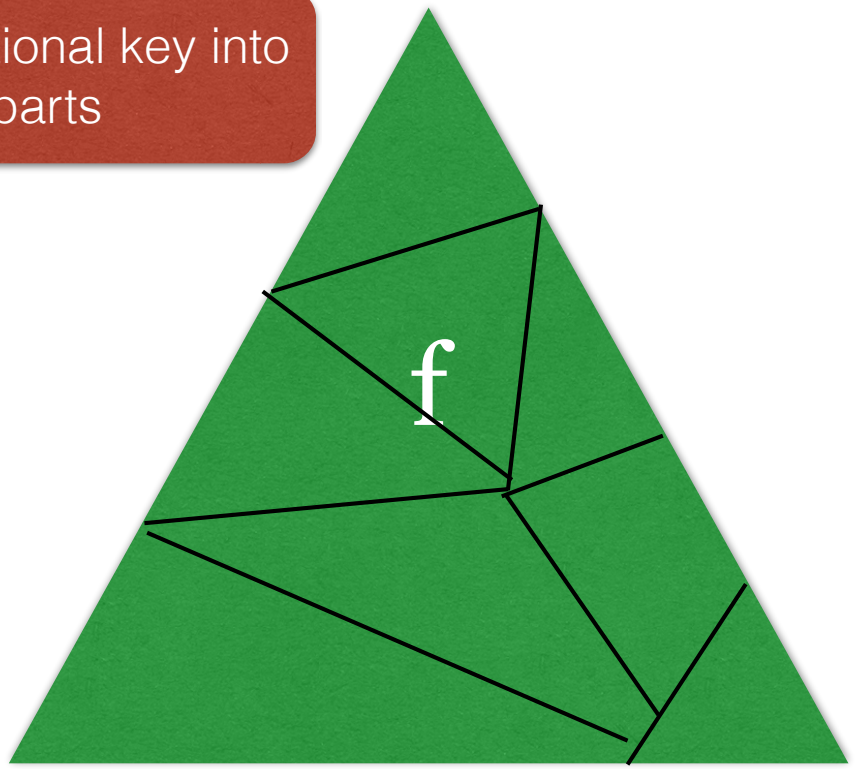




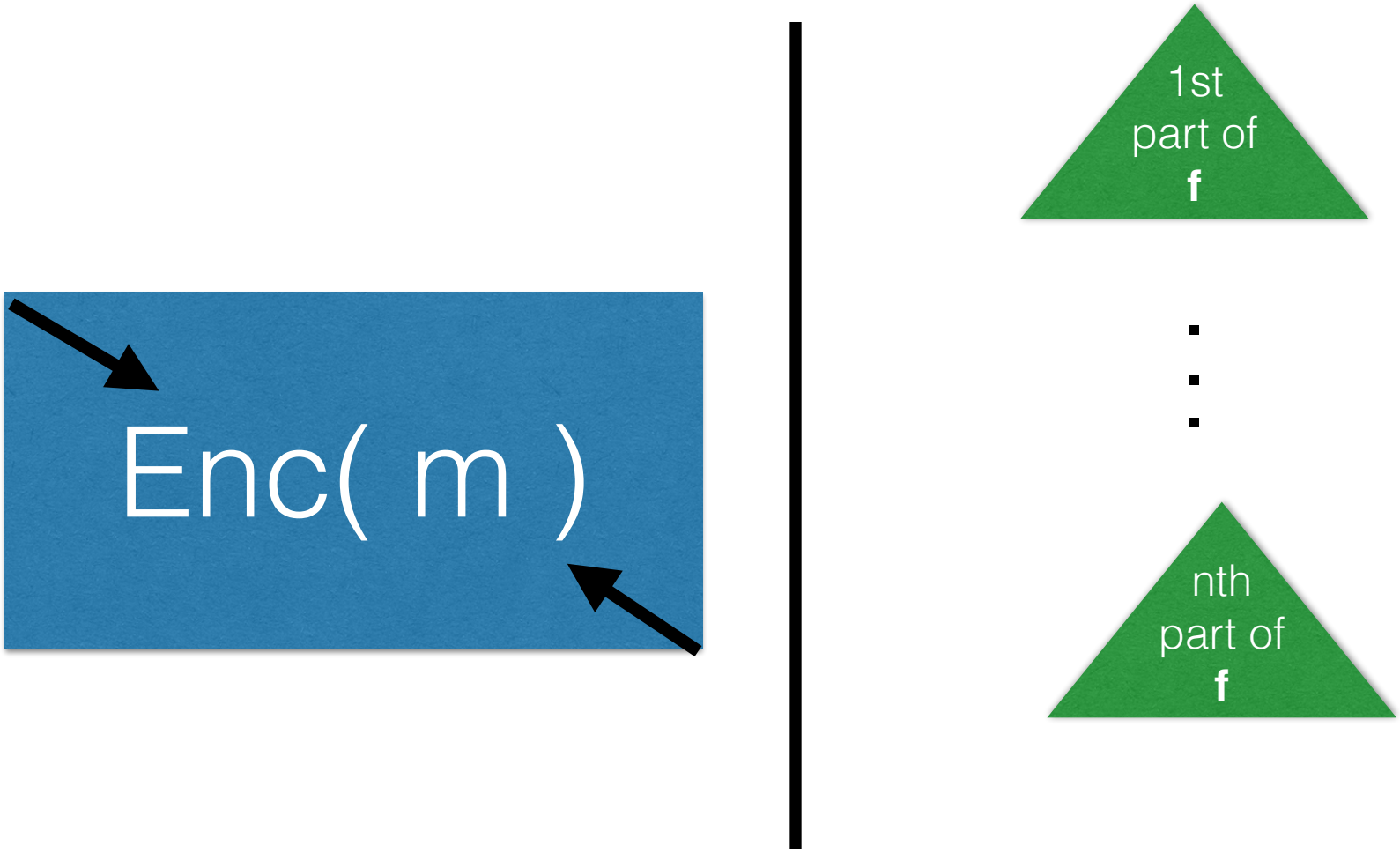
Non Compact FE

Break the functional key into many parts

Enc(m)

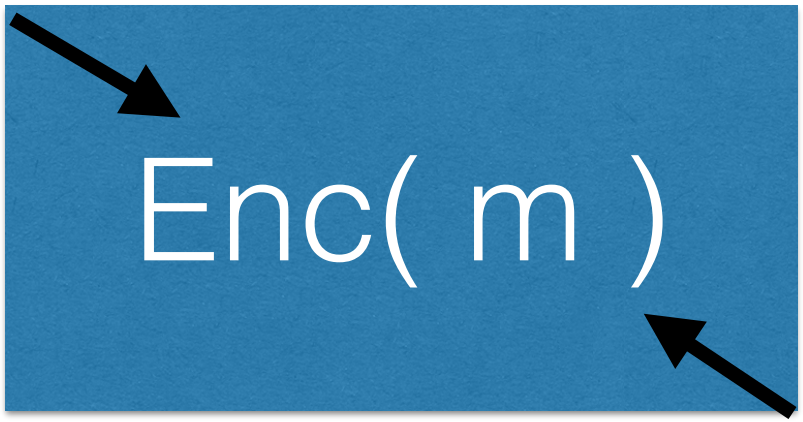


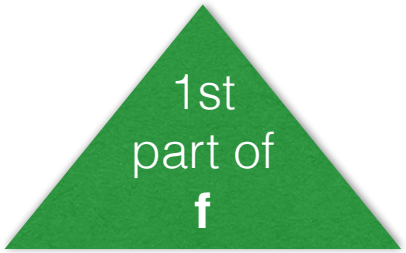
Non Compact FE

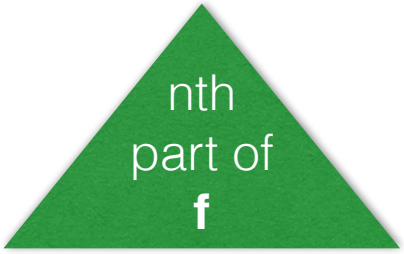


Non Compact FE

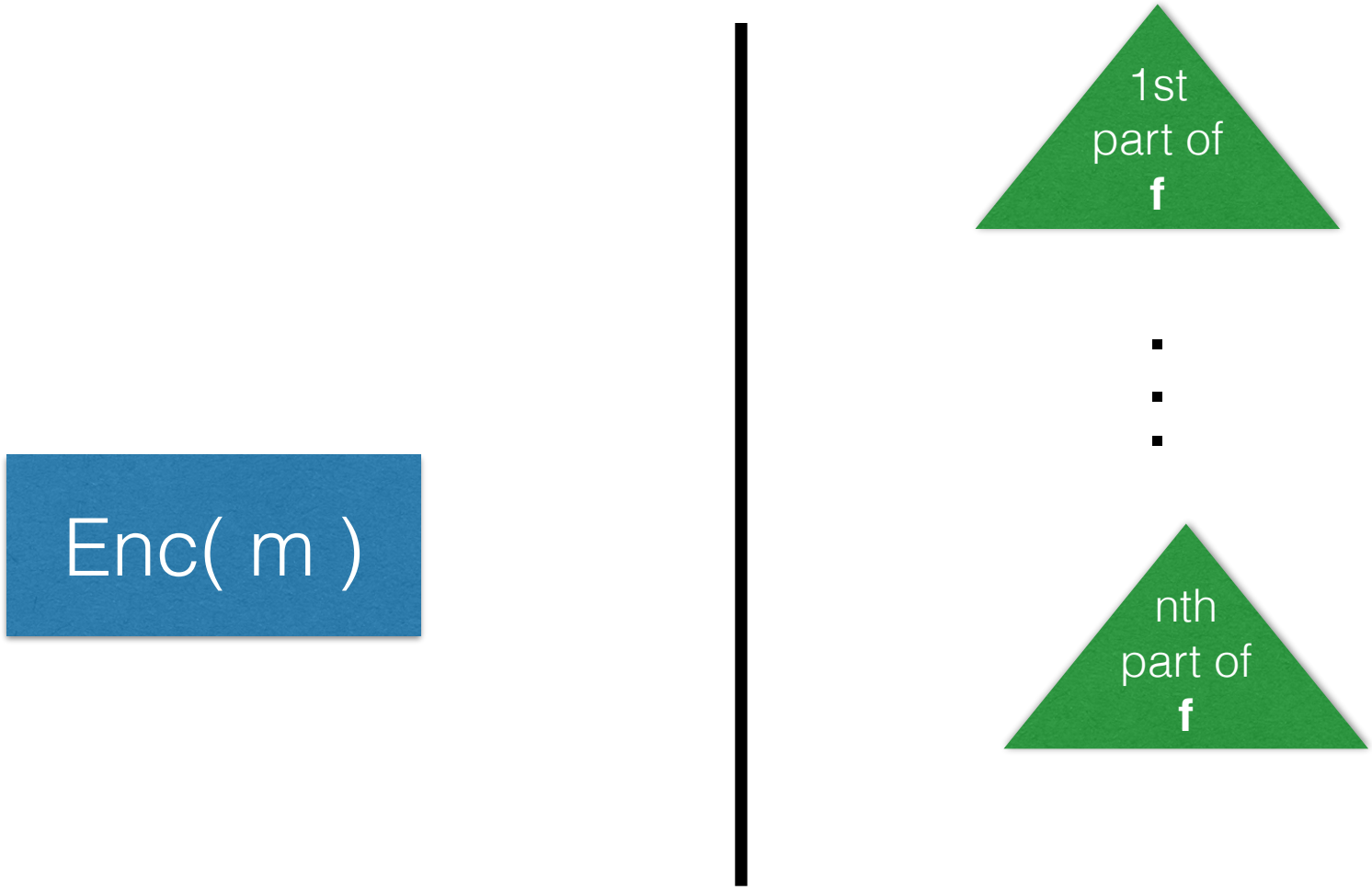
ciphertext shrinks



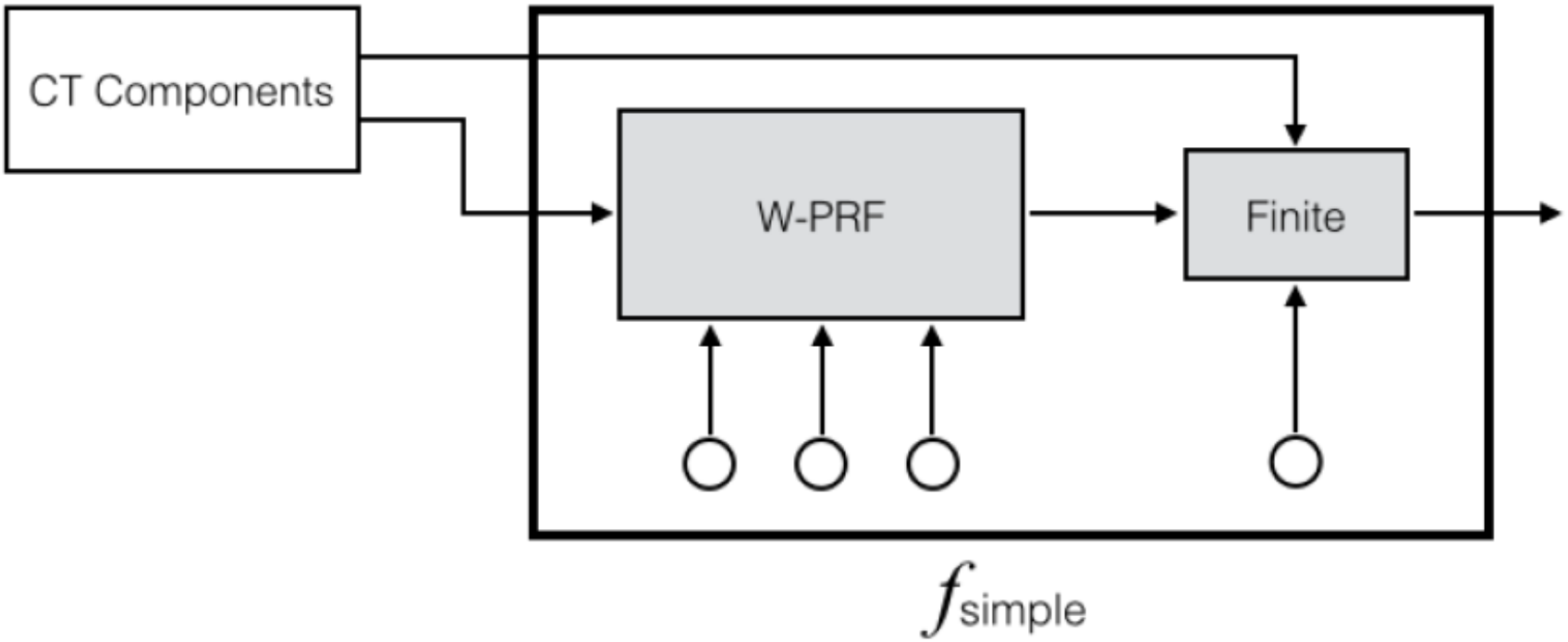




Resulting scheme: Compact FE !!



- Showed: FE for f_{simple} implies iO for all functions



- link: http://eprint.iacr.org/2015/730.pdf