Korea University CIST Center for Information Security Technologies

CRYPTOGRAPHIC ALGORITHM LABORATORY

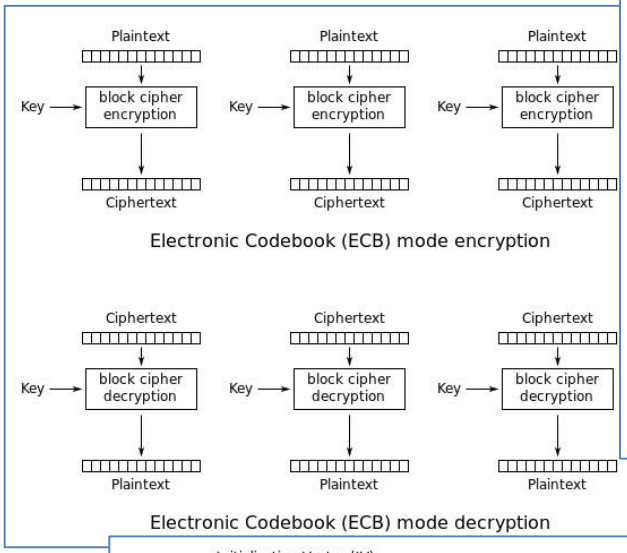
Secure and Efficient Format Preserving Encryption

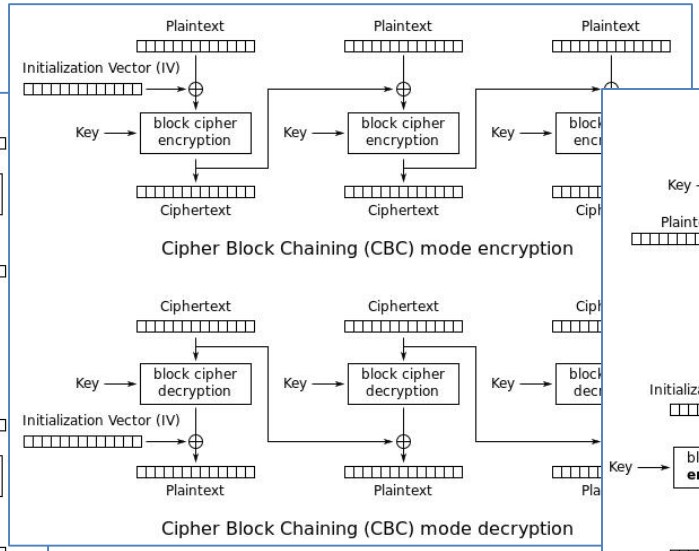
FSE 2014 Rump Session

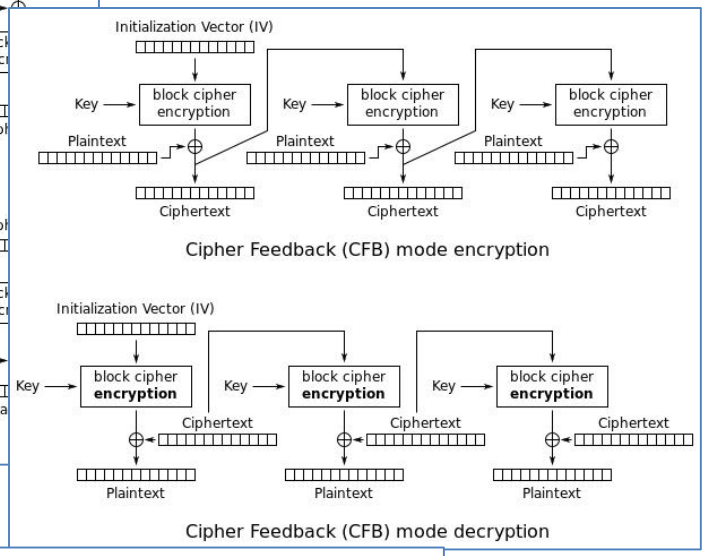
Center for Information Security Technologies (CIST),
Korea University

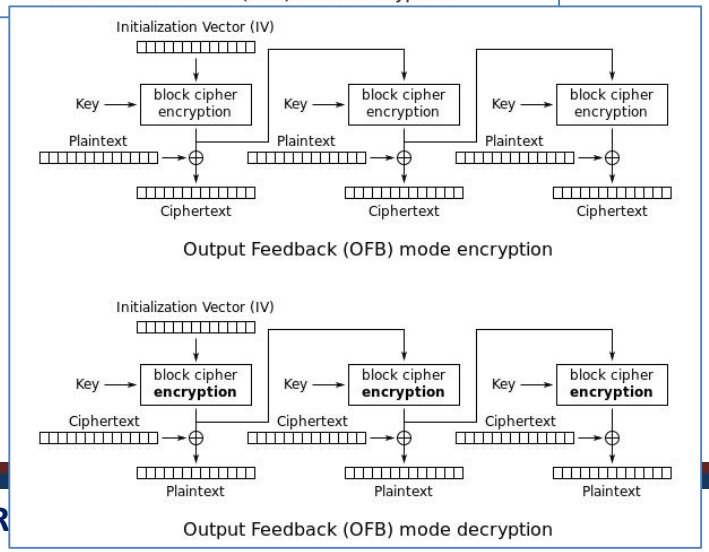
HyungChul Kang

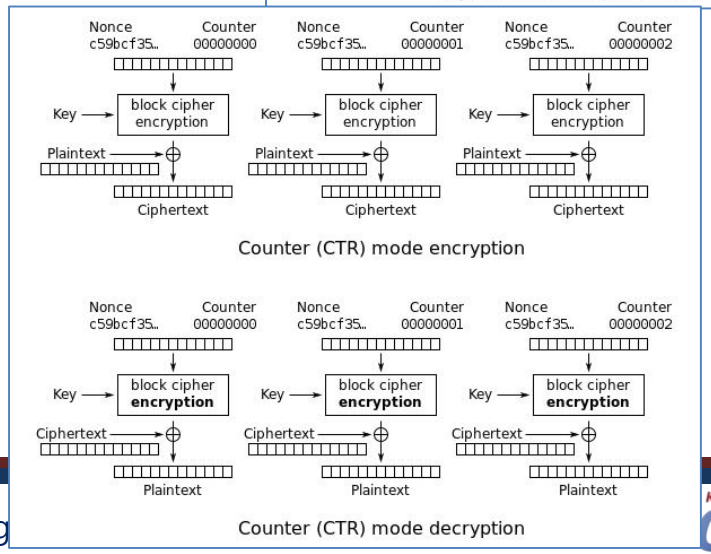
Mode of Operation



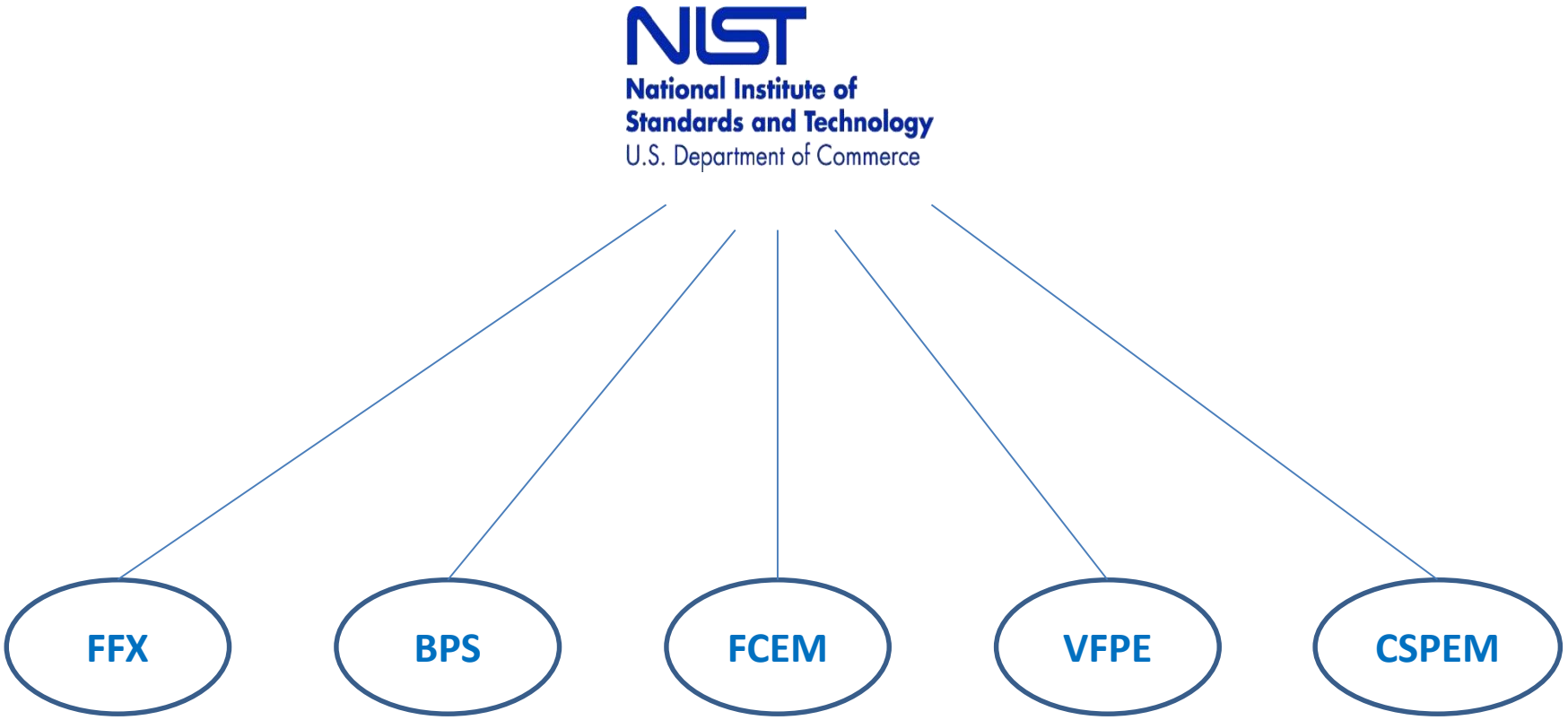




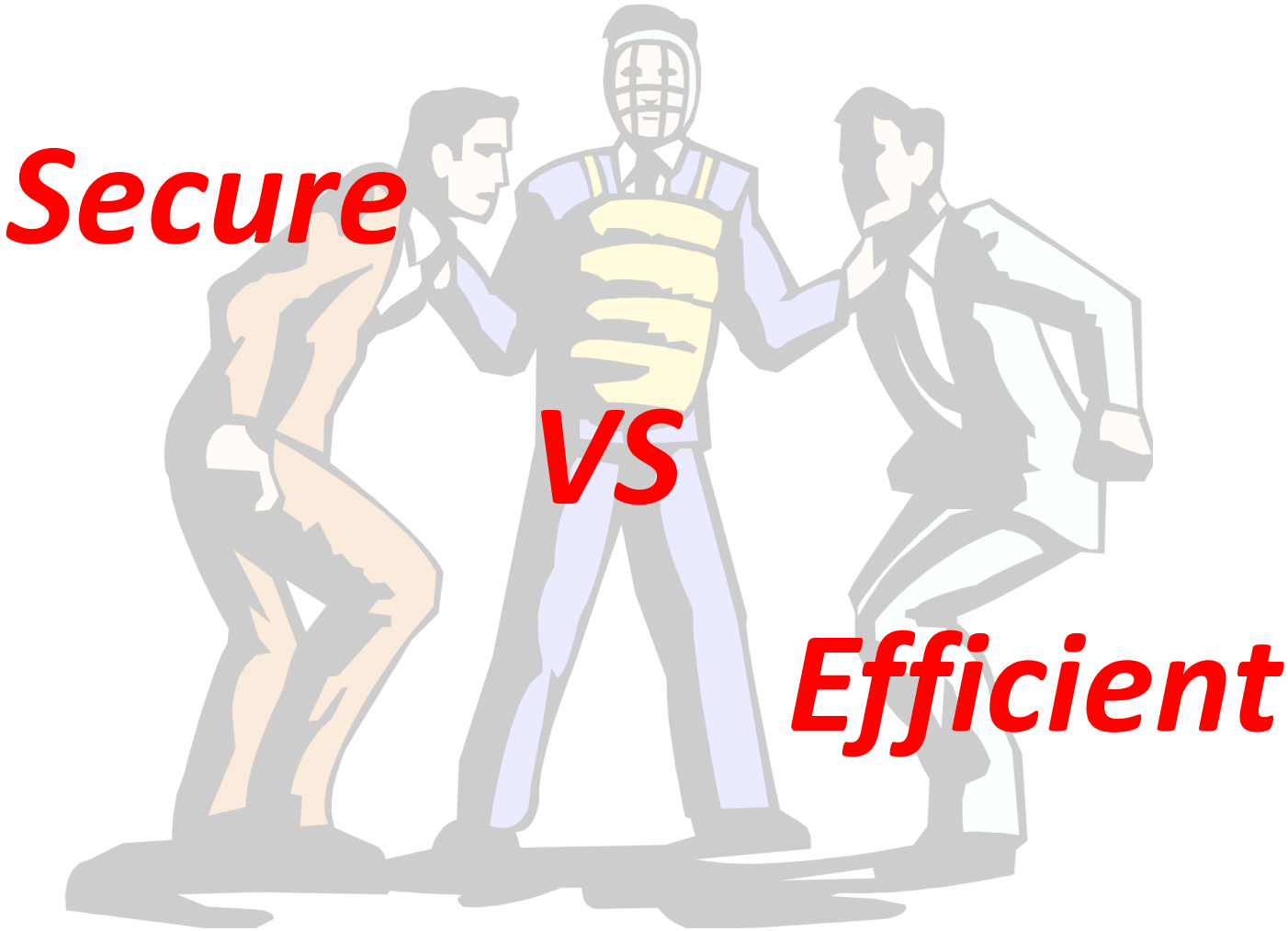




Format Preserving Encryption



Secure? Efficient?

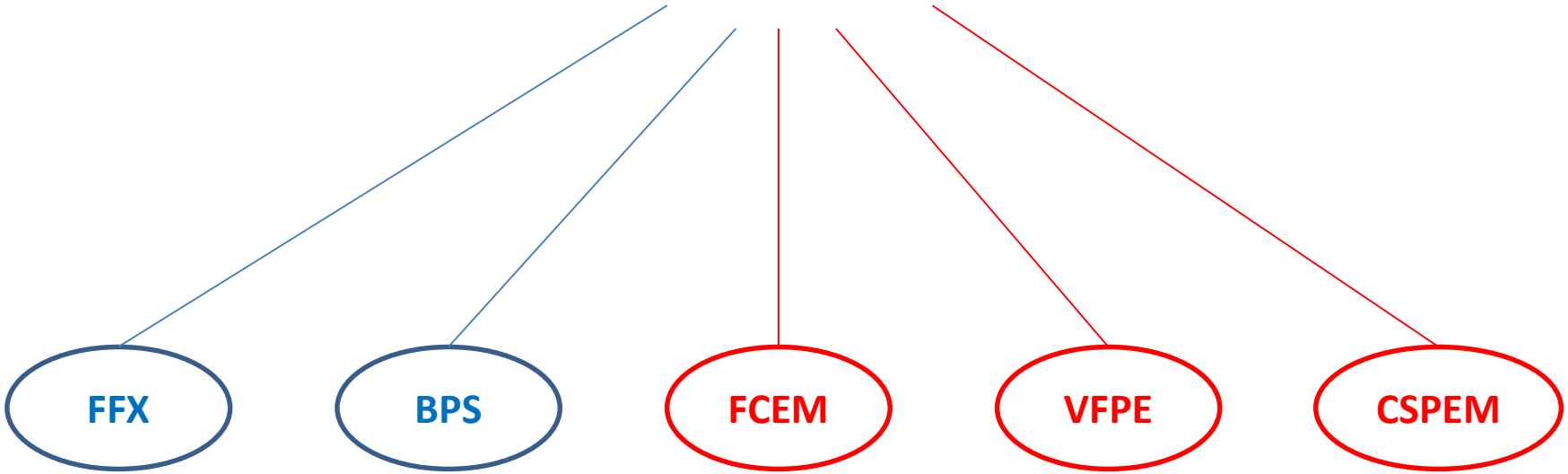


Secure? Efficient?

Efficient?

Secure?

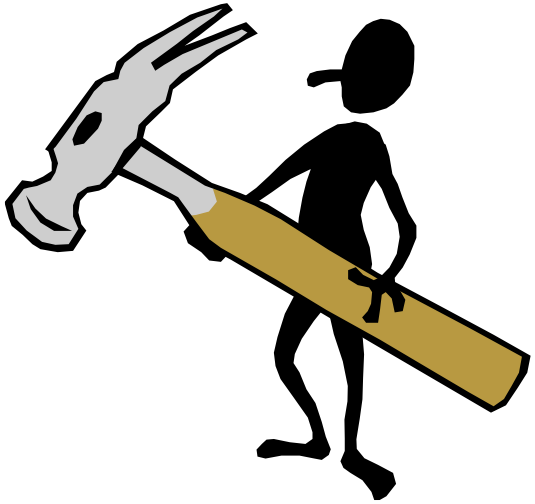
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



Make Efficiently

FFX

BPS

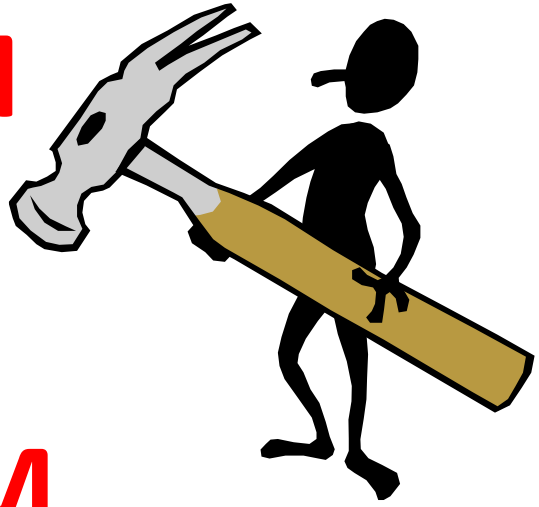


Make Securely

FCEM

VFPE

CSPEM



Thank you.

kanghc@korea.ac.kr