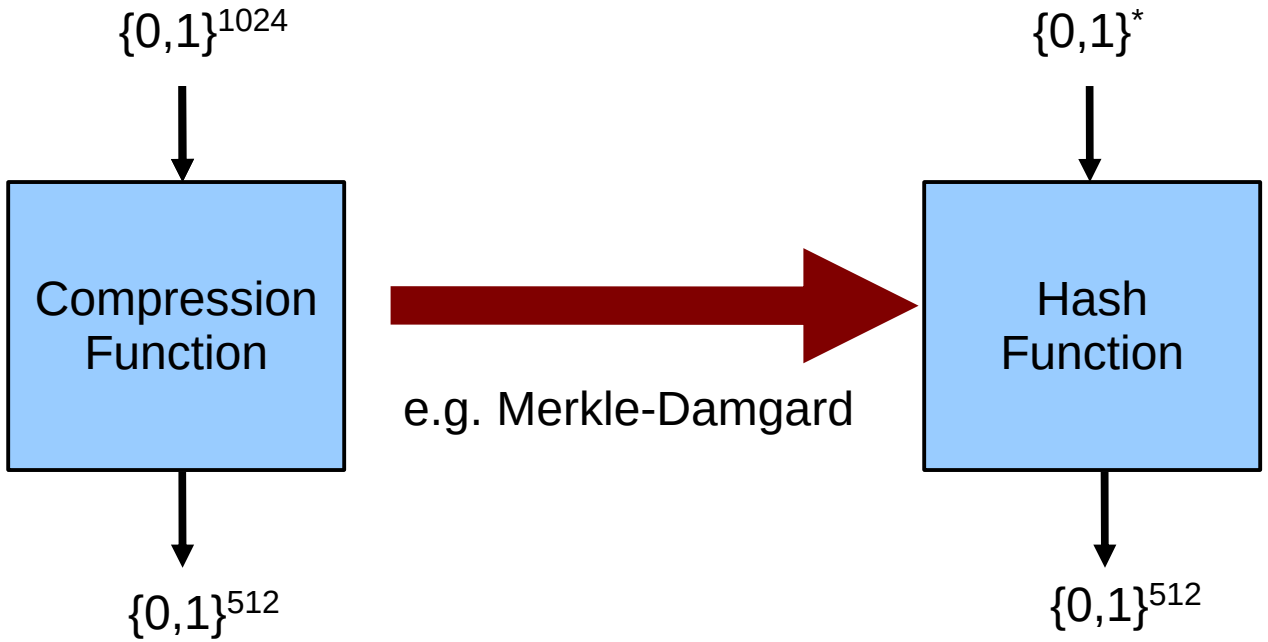
SWIFFTX

Yuriy Arbitman
Gil Dogon
Vadim Lyubashevsky
Daniele Micciancio
Chris Peikert
Alon Rosen

Common Hash Function Design



Compression Function Security → Hash Function Security

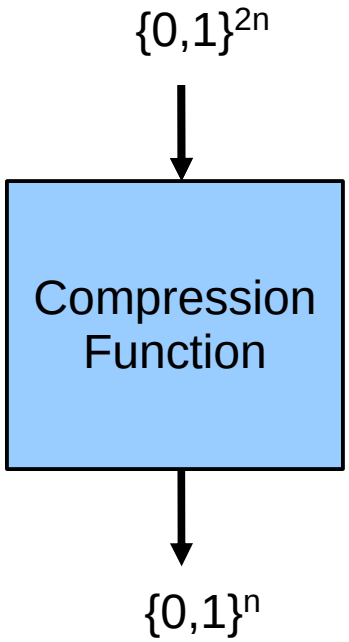
Designing collision-resistant compression functions:

Current goal: “Should resist known attacks”

Why not: “Should resist ALL attacks” ?

Security of Compression Functions

- **Cannot** prove anything about a fixed compression function
- **Can** prove something about *families* of compression functions



SWIFFT [LMPR '08]

Finding Collisions in SWIFFT

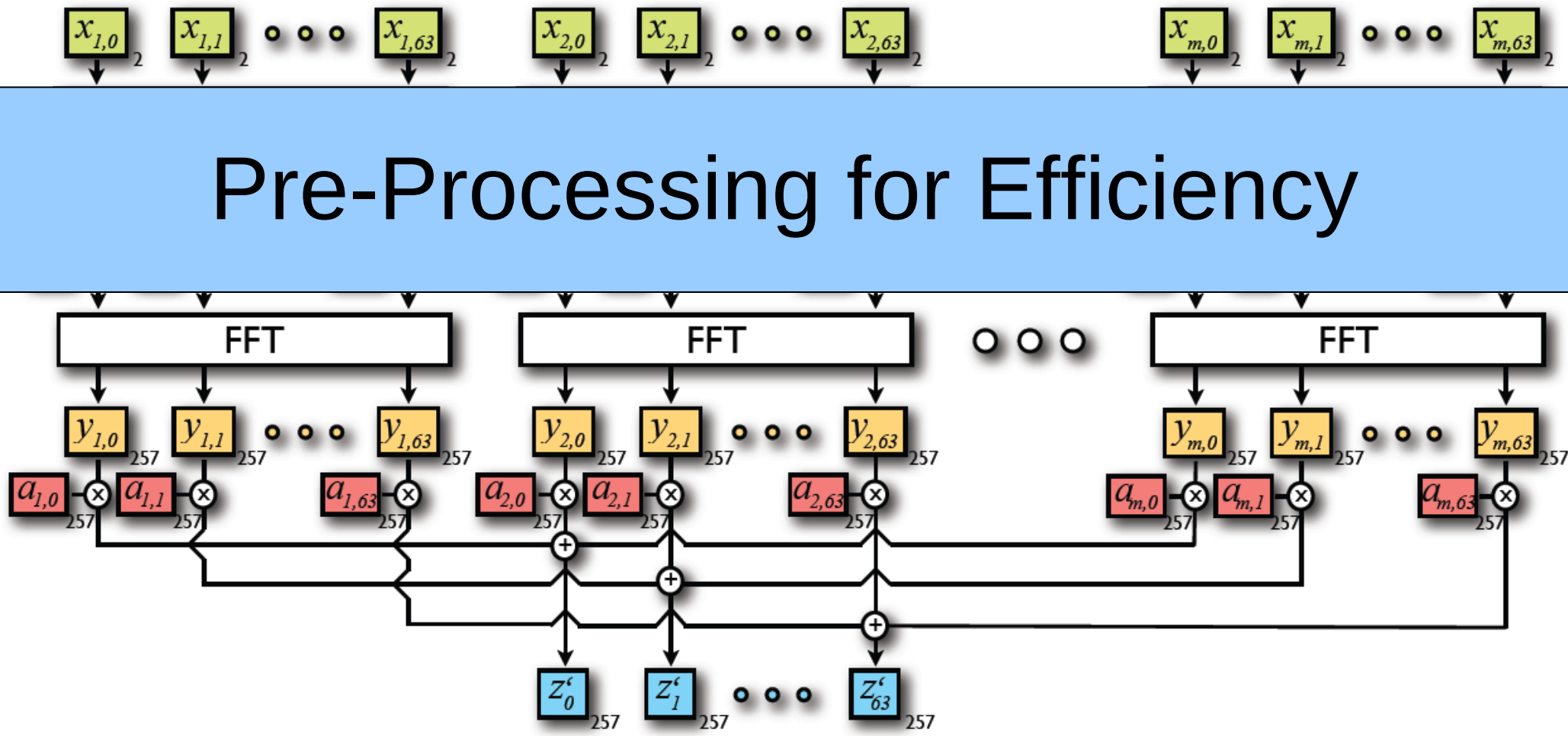
=

Finding Short Vectors in ALL Lattices

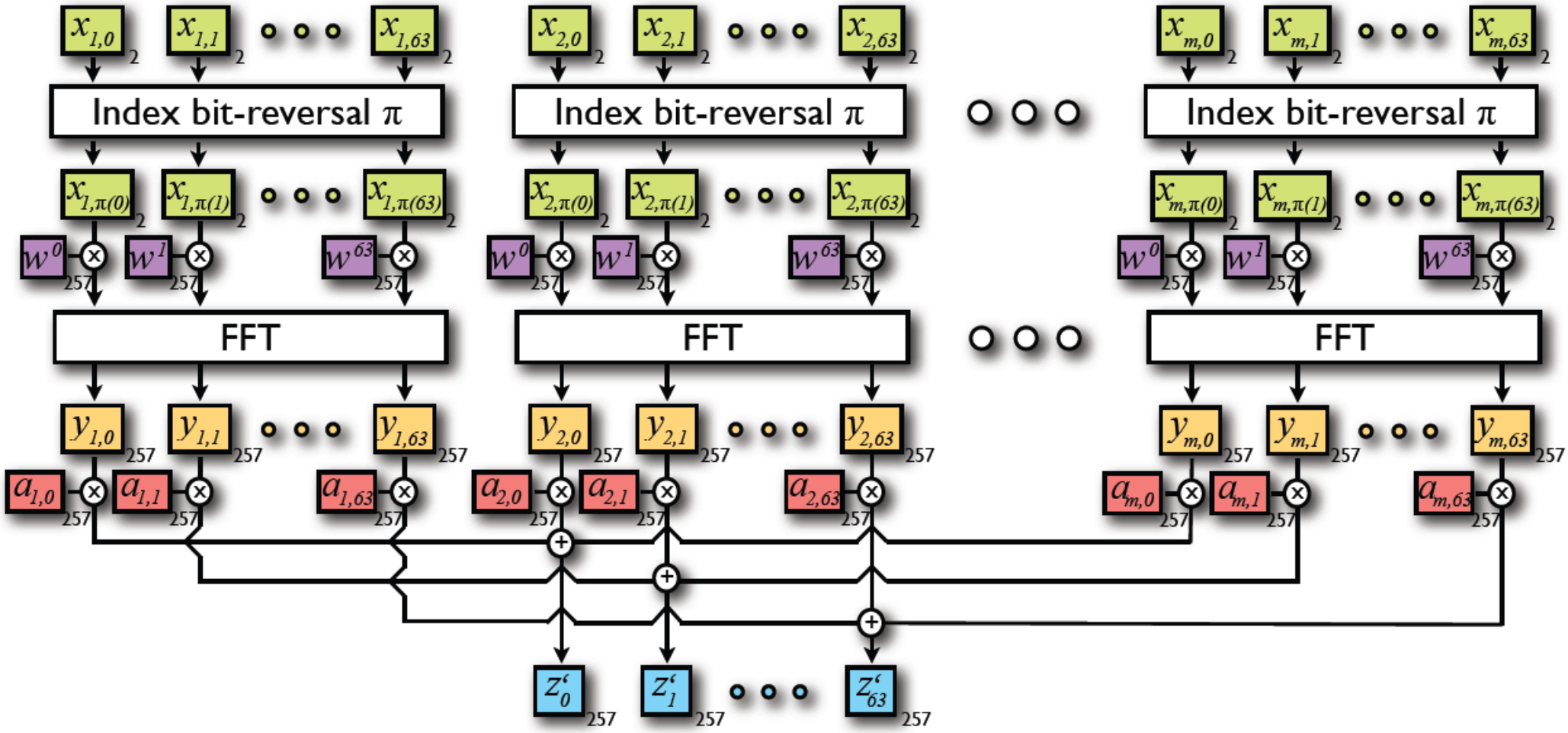
[LM '06, PR '06, LMPR '08]

(Cryptanalysis is still necessary to set the parameters)

SWIFFT [LMPR '08]



SWIFFT [LMPR '08]



Pros and Cons of SWIFFT

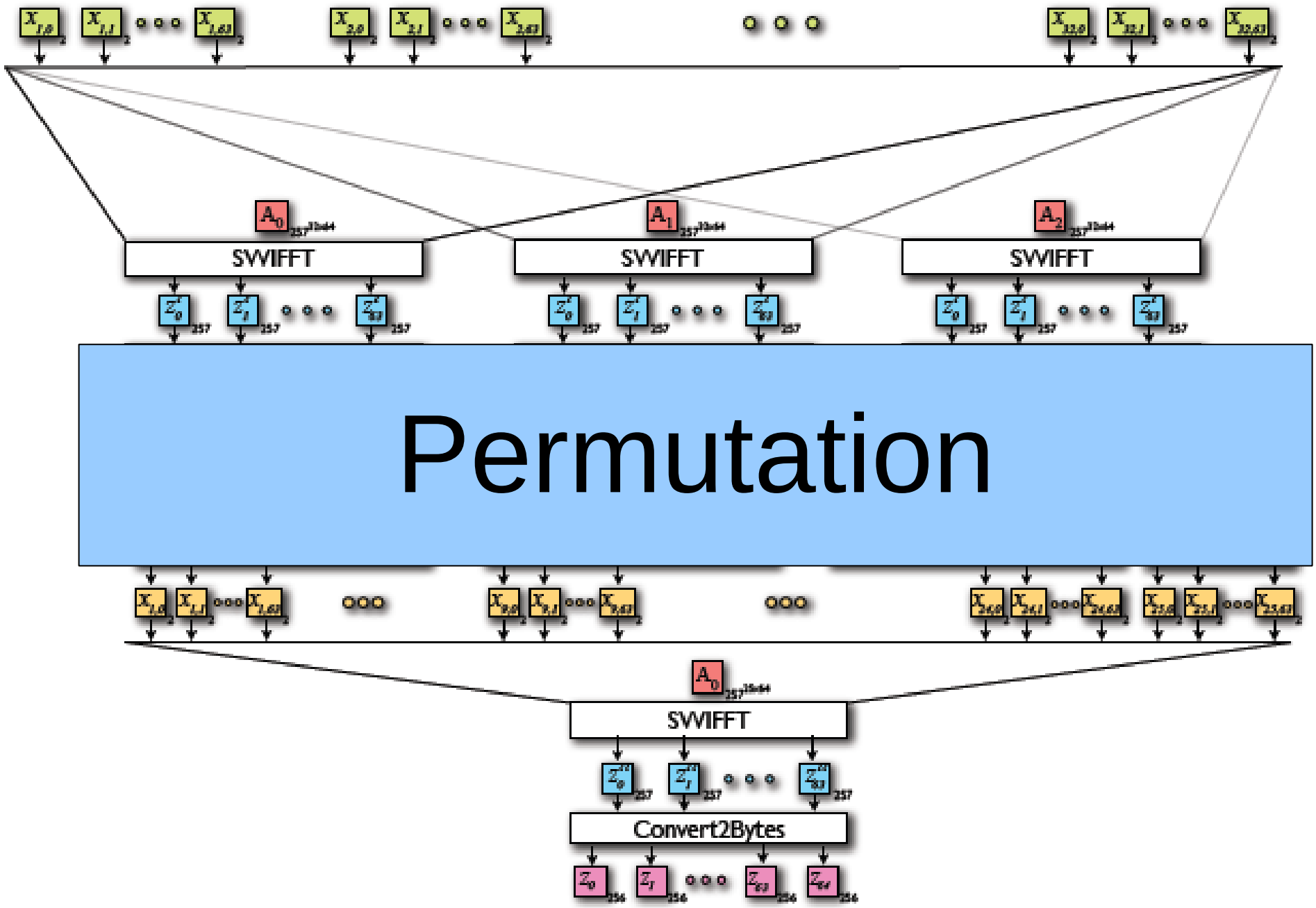
Pros

- Provable Asymptotic Security for Collision-Resistance
- Very Fast
- Parallelizable

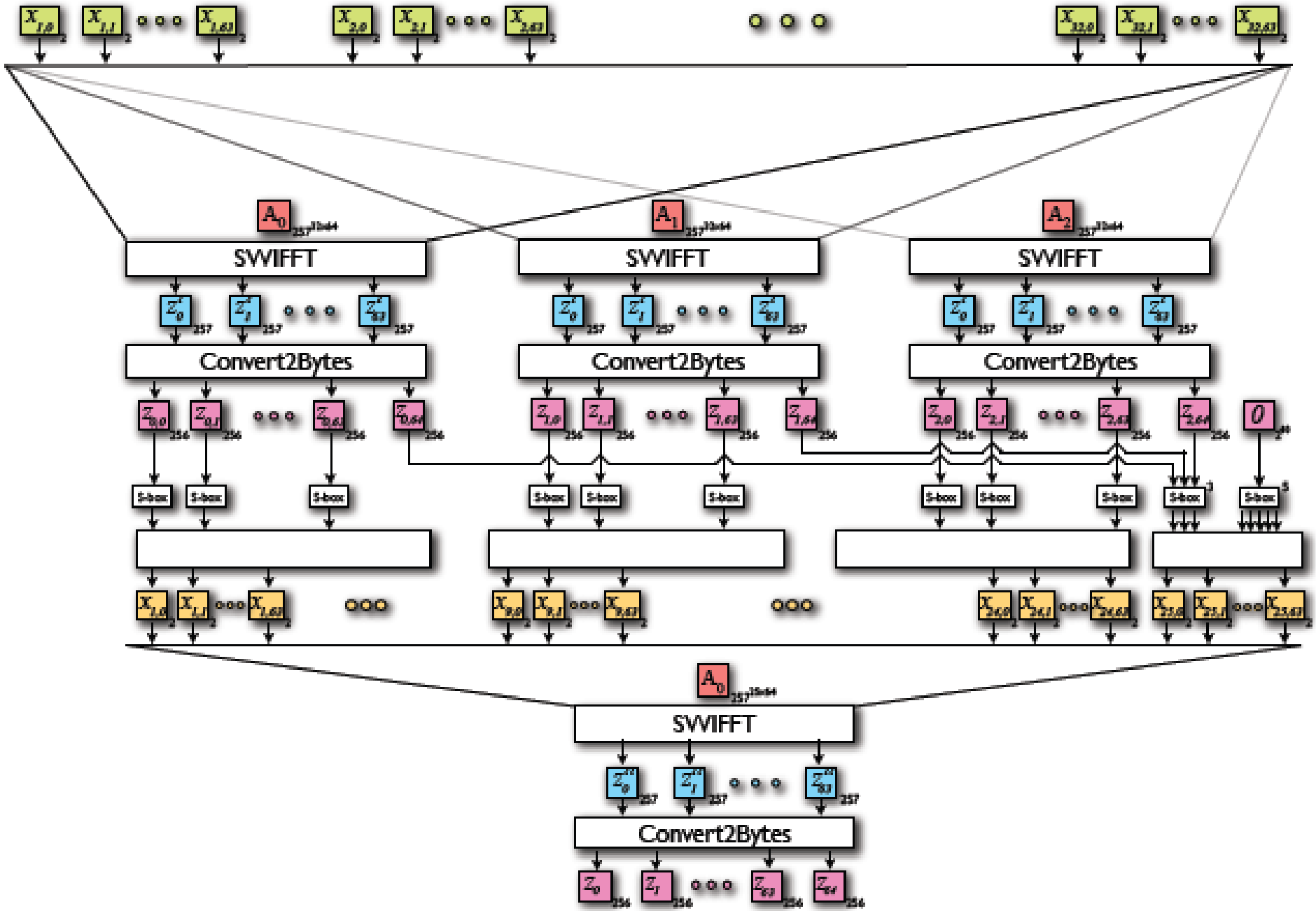
Cons

- Linear
- 512 bit output only gives 100 bit security
- Large footprint

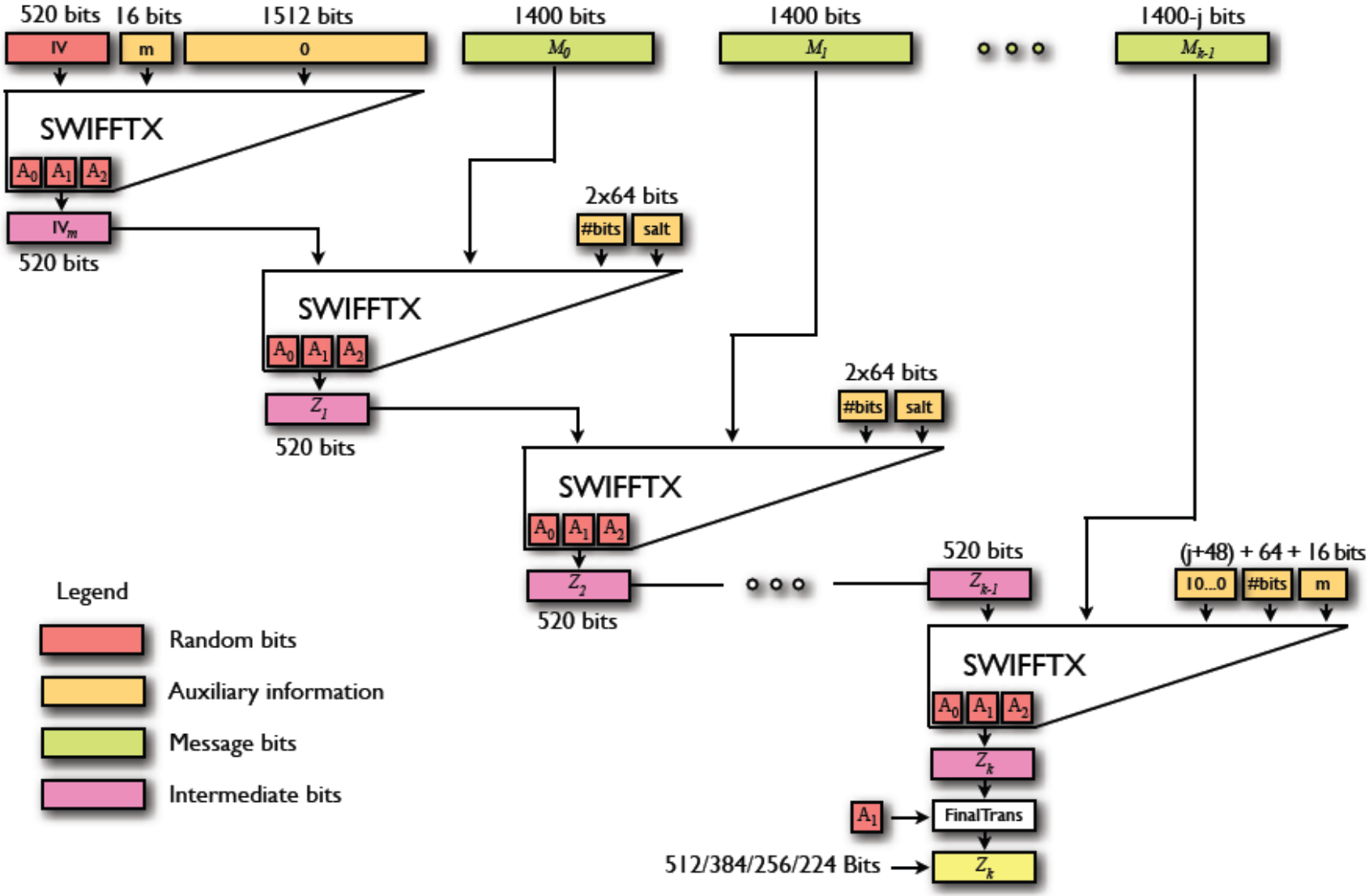
SWIFFTX Compression Function



SWIFFTX Compression Function



Use HAIFA (BD '07) as a Mode of Operation



Pros and Cons of SWIFFTX

Pros

- Provable Asymptotic Security for Collision-Resistance
- ~~Very~~ Fast

  (60 cycles/byte)
- Parallelizable

Cons

- ~~Linear~~
- ~~512 bit output only gives 100 bit security~~
- Large footprint