Designing Secure Hash Functions and Block Ciphers

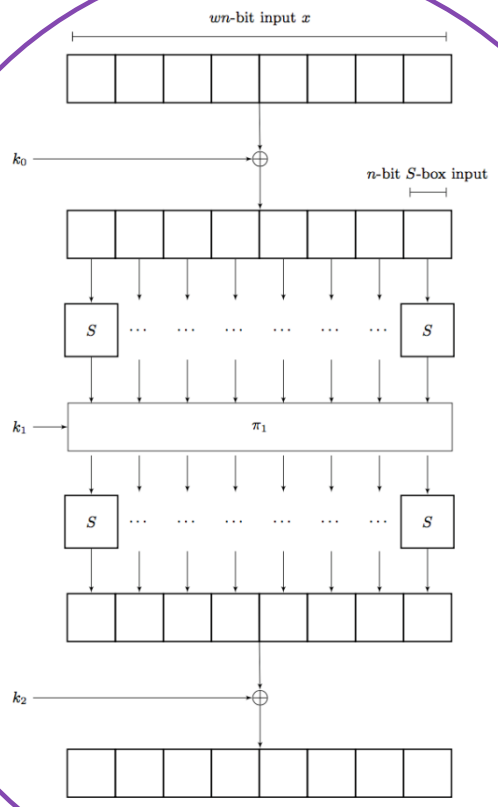
NYU

Challenge:

- Put design of hash functions and block ciphers on solid theoretical foundation
- Counteract potential backdoors in standards

Solution:

- Provide rigorous mathematical security proofs for known and novel designs
- Clearly state assumptions about underlying components



3-round SPN cipher

Scientific Impact:

- Better understanding of security and applicability of hash functions and block ciphers
- Concrete security bounds help in choosing good parameters in practice

Broader Impact:

- Higher trust in standardized hash functions and block ciphers
- Proposed schemes highly practical
- Clean design and analysis suitable for teaching in lectures on cryptography

NSF Trustworthy Computing Grant (#1619158), 9/2016-8/2019. "On the Design of Secure Hash Functions and Block Ciphers." Yevgeniy Dodis, NYU.