Provable Security of (Tweakable) Block Ciphers Based on Substitution-Permutation Networks

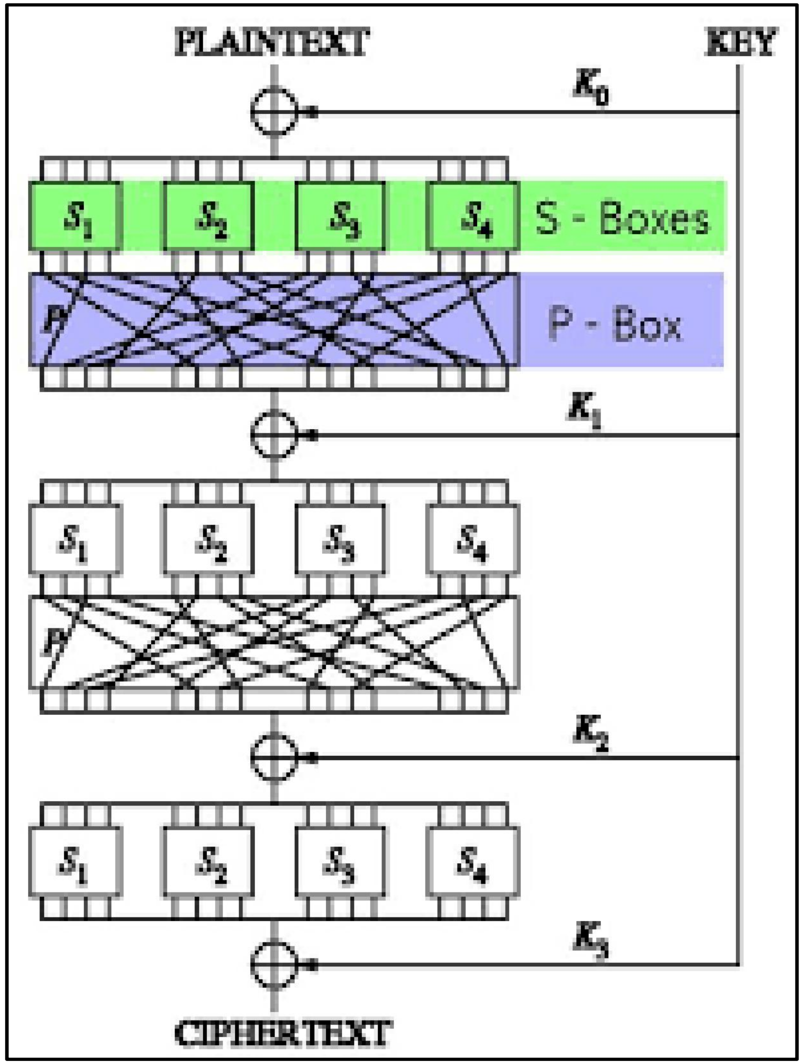
Benoit Cogliati Yevgeniy Dodis Jonathan Katz Jooyoung Lee
John Steinberger Aishwarya Thiruvengadam Zhe Zhang

Block Ciphers

- Building block for many cryptographic constructions
  - Hash functions
  - Encryption schemes
  - Message authentication codes
- Keyed permutations
- Popular Design Paradigms
  - Feistel Networks
  - Substitution-Permutation Networks

Block Ciphers: Designs

- Popular Design Paradigms
  - Feistel Network
    - Eg: DES
  - Substitution-Permutation Network (SPN)
    - Eg: AES



Block Ciphers: Designs

- Popular Design Paradigms
  - Feistel Network
    - Eg: DES
    - Long line of work analyzing provable security of Feistel [LR88, Pat03, Pat04]
    - Security been studied in various security models [Pat10, HR10, HKT11, Tes14, CHKPST16]
  - Substitution-Permutation Network (SPN)
    - Eg: AES
    - In contrast, provable security of SPNs not as well-studied

Related Work

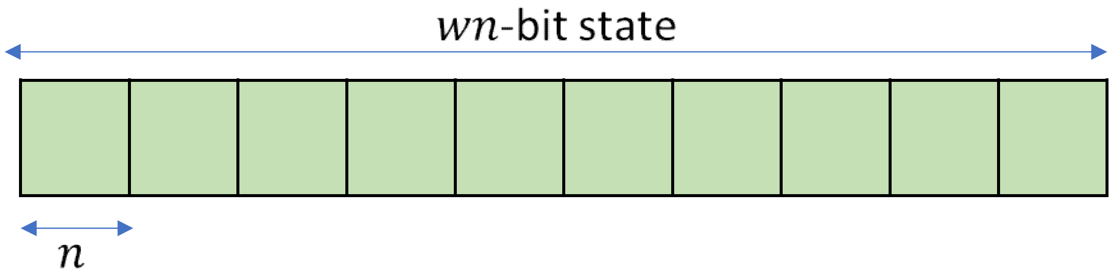
- SPNs with secret S-boxes
  - Naor-Reingold prove security for a non-linear 1-round SPN [NR99], ideas further explored for domain extension [CS06, Hal07]
  - Miles-Viola [MV15]
    - Linear SPNs where S-boxes are random functions (not necessarily invertible)
    - Security against linear/differential attacks for SPNs with concrete S-boxes

Related Work

- SPNs with public S-boxes
  - Dodis et al. [DSSL16] studied indifferentiability of confusion-diffusion networks
    - Can be viewed as unkeyed SPNs
    - Positive results only for $>$5 rounds and weaker security bounds
  - Even-Mansour construction [EM97] – degenerate 1-round linear SPN
    - Security shown against adaptive chosen-plaintext/chosen-ciphertext attacks [EM97]
    - Our positive results imply this as a special case

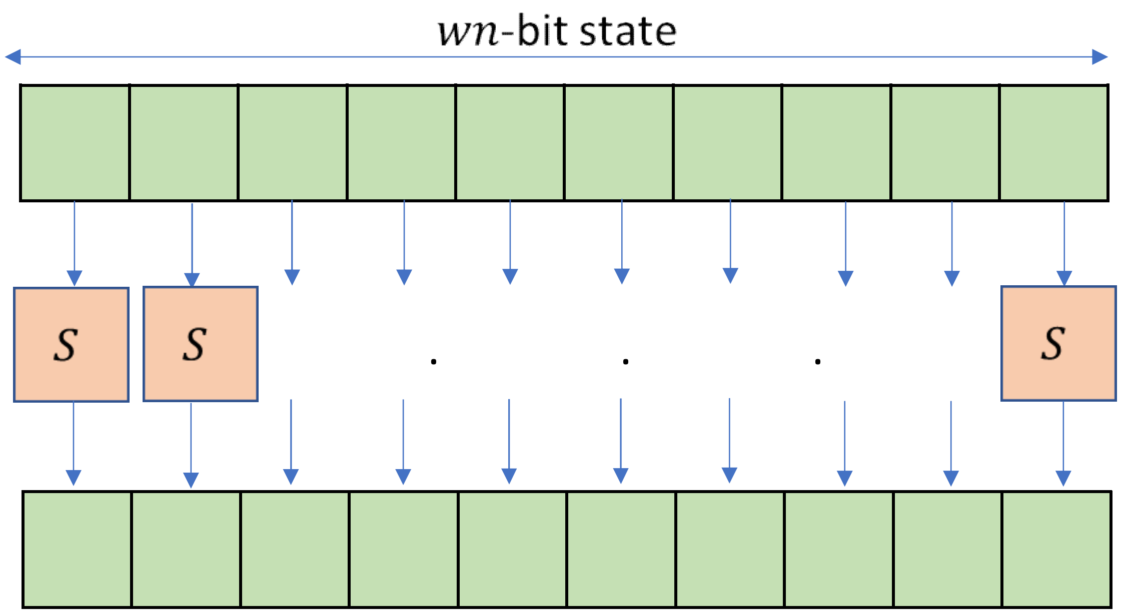
Substitution-Permutation Network (SPN)

- Substitution step
  - Split wn-bit state into w n-bit blocks



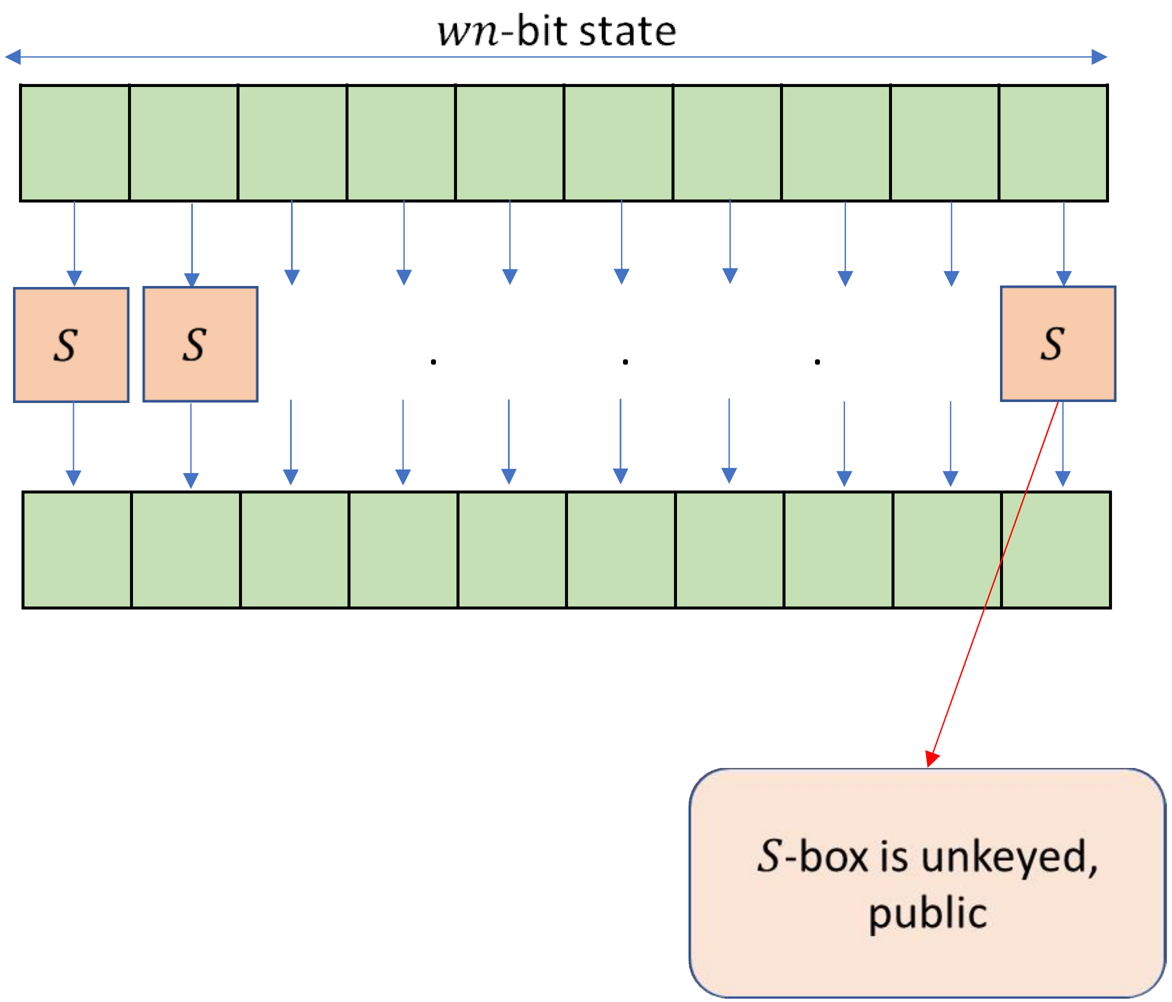
Substitution-Permutation Network (SPN)

- Substitution step
  - Split wn-bit state into w n-bit blocks
  - Compute S-box on each n-bit block
  - S-box: Substitution box is a (cryptographic) permutation from n bits to n bits



Substitution-Permutation Network (SPN)

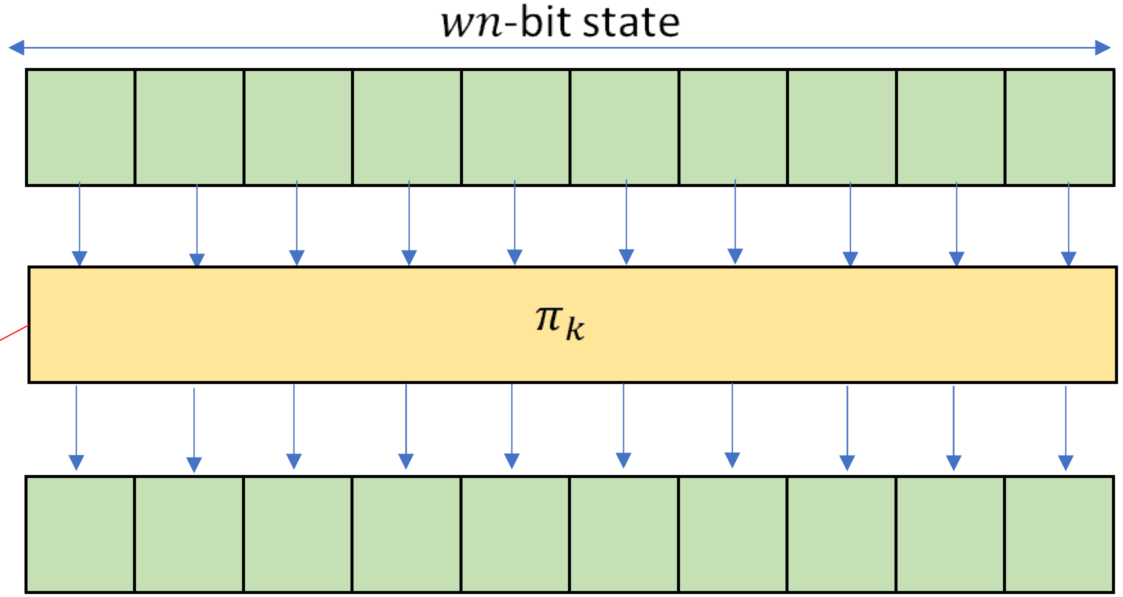
- Substitution step
  - Split wn-bit state into w n-bit blocks
  - Compute S-box on each n-bit block
  - S-box: Substitution box is a (cryptographic) permutation from n bits to n bits



Substitution-Permutation Network (SPN)

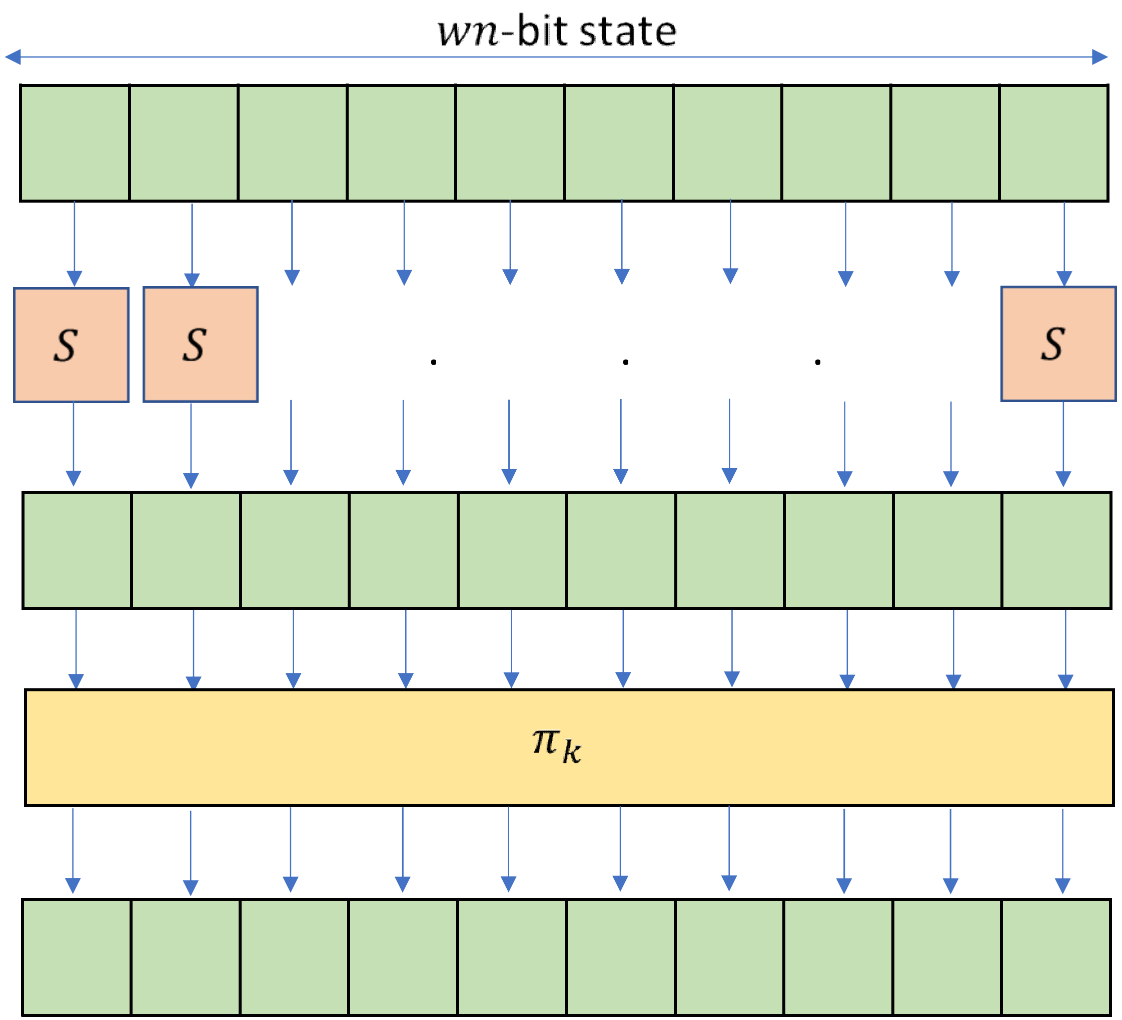
- Substitution step
  - Split wn-bit state into w n-bit blocks
  - Compute S-box on each n-bit block
- Permutation step
  - Apply a non-cryptographic keyed permutation to the wn-bit state

π_k is typically linear. Eg: key-mixing followed by linear transformation



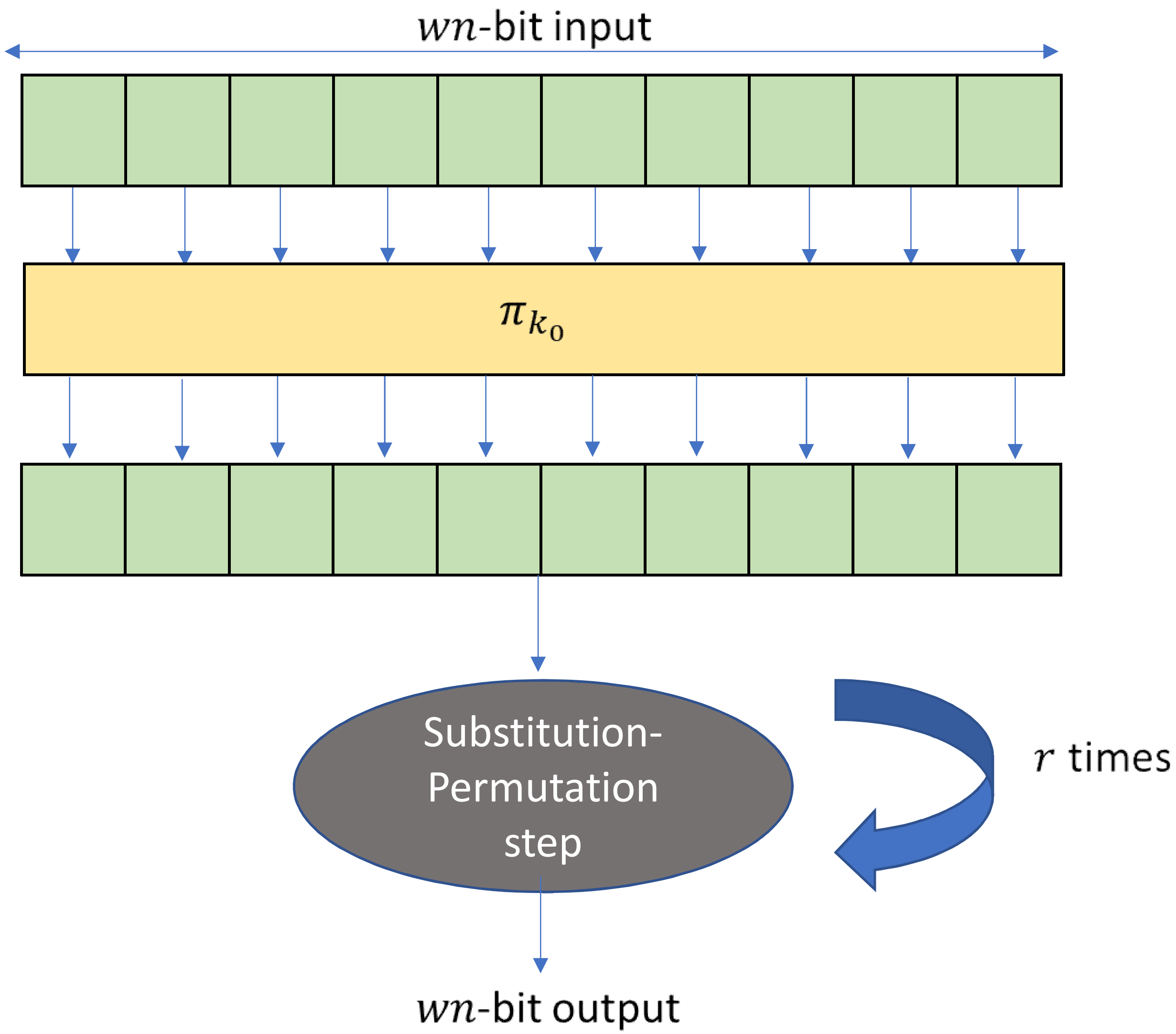
Substitution-Permutation Network (SPN)

- Substitution step
  - Split wn-bit state into w n-bit blocks
  - Compute S-box on each n-bit block
- Permutation step
  - Apply a non-cryptographic keyed permutation to the wn-bit state
- Constitutes a single application of substitution-permutation



Substitution-Permutation Networks

- r-round SPN
  - Round 0 consists of a permutation step
  - Followed by r applications of substitution and permutation steps



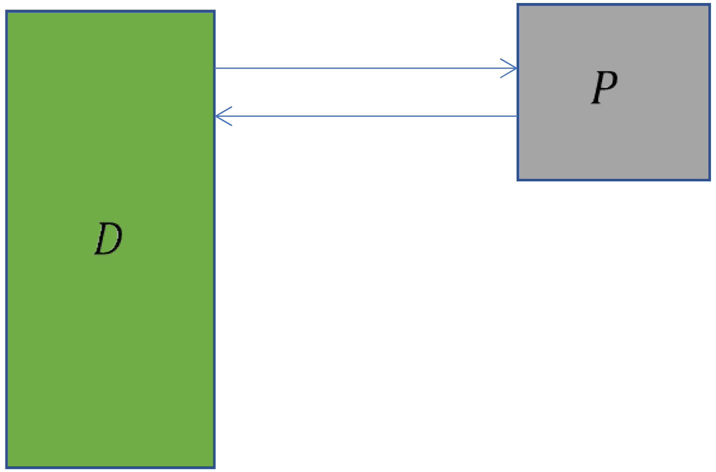
Security of SPNs

- Analyze security as a strong pseudorandom permutation
  - i.e., security against adaptive chosen-plaintext and chosen-ciphertext attacks

- Here, S-boxes modeled as public random permutations
  - Only source of cryptographic hardness

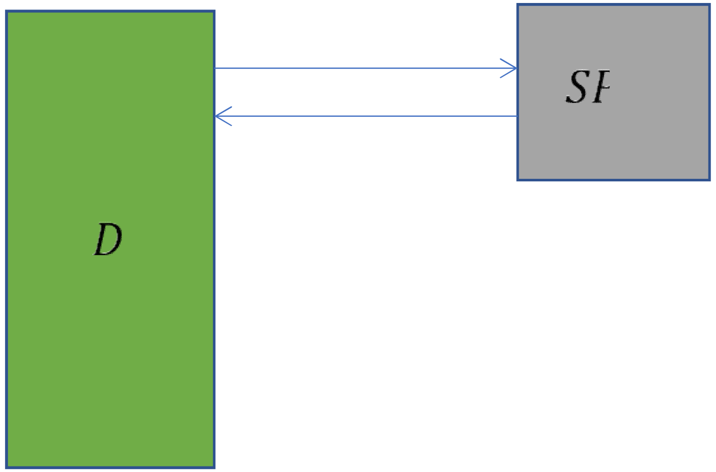
Security of SPNs

- Ideal World



- P – random permutation on wn bits

- Real World

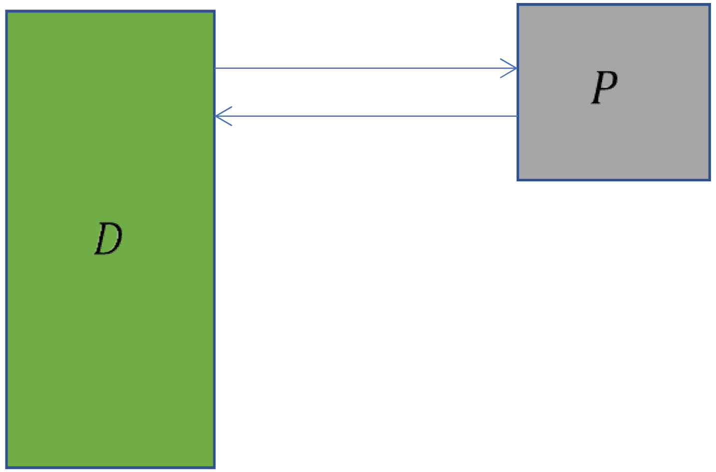


- SPN_k - r-round SPN with key k and S-box S

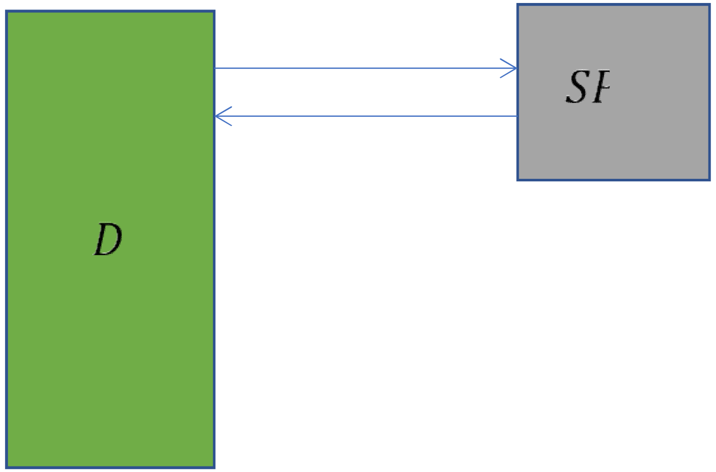
Security of SPNs

S-box is unkeyed, public

- Ideal World



- Real World

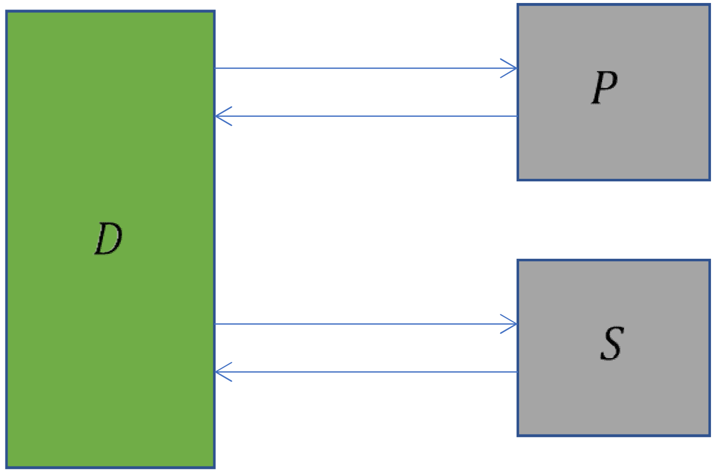


- P – random permutation on wn bits
- SPN_k - r-round SPN with key k and S-box S

Security of SPNs

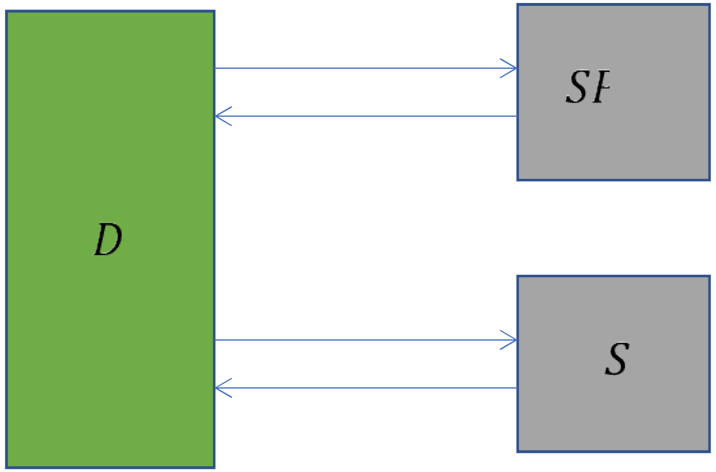
S-box is unkeyed, public

- Ideal World



- P – random permutation on wn bits
- S – random permutation on n bits

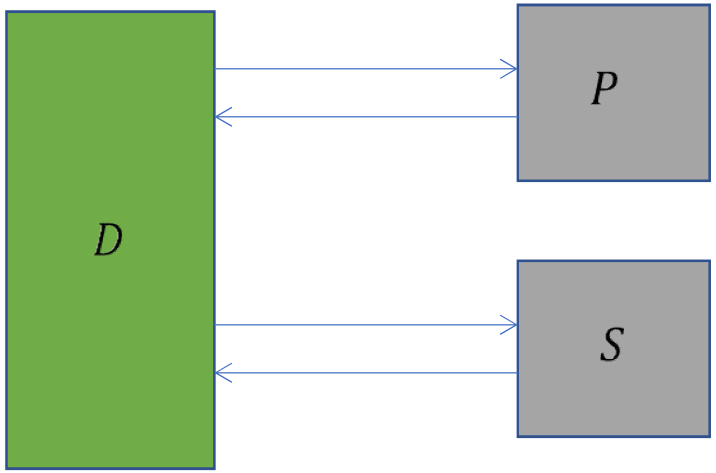
- Real World



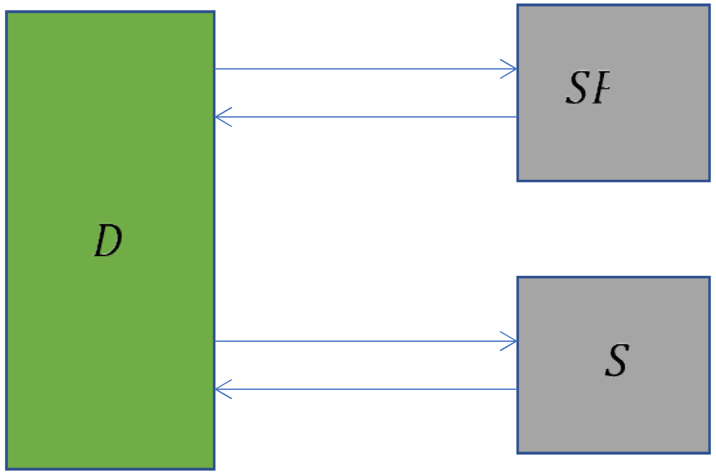
- SPN_k - r-round SPN with key k
- S – random permutation on n bits

Security of SPNs

- Ideal World



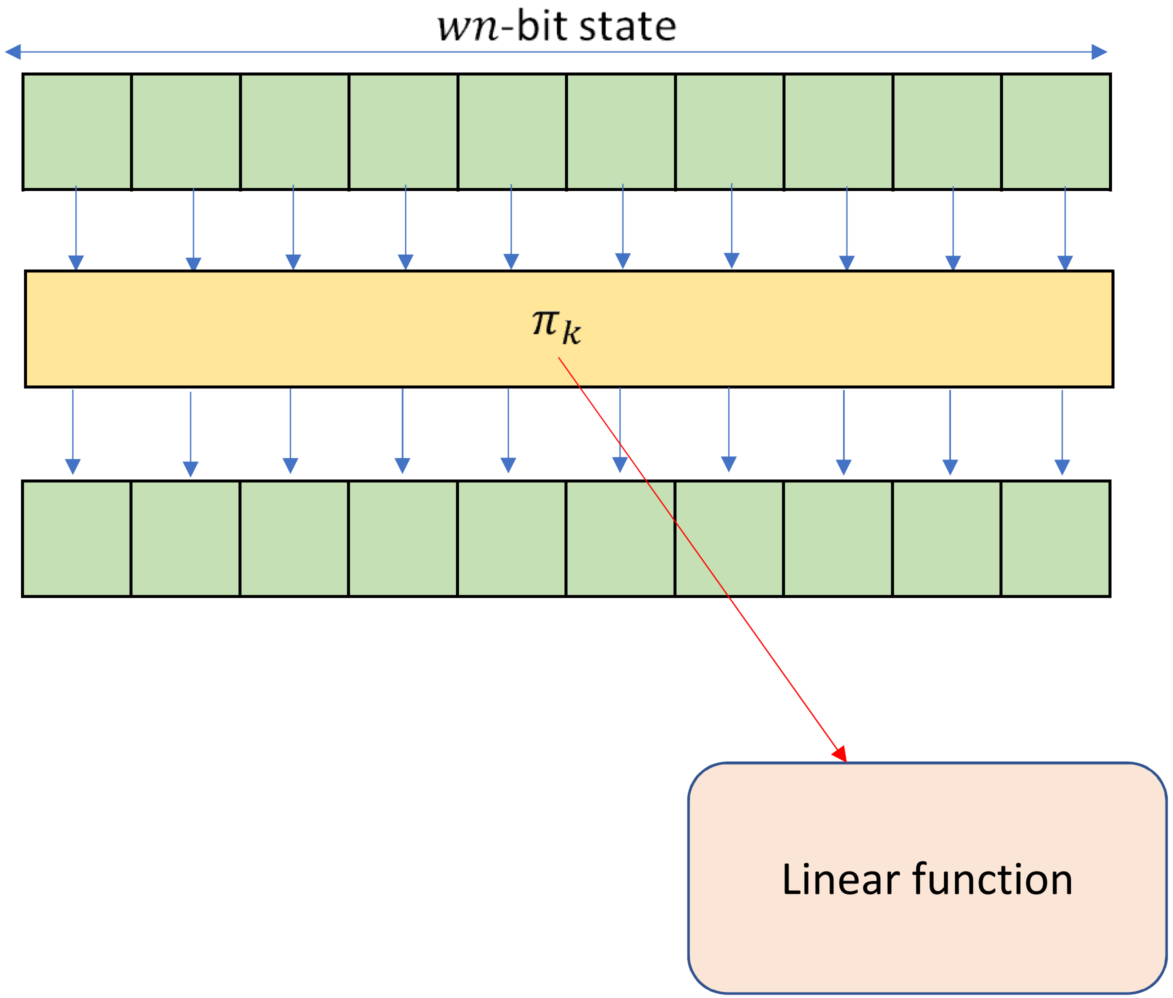
- Real World



D is computationally unbounded but can make only a bounded number of queries to its oracles

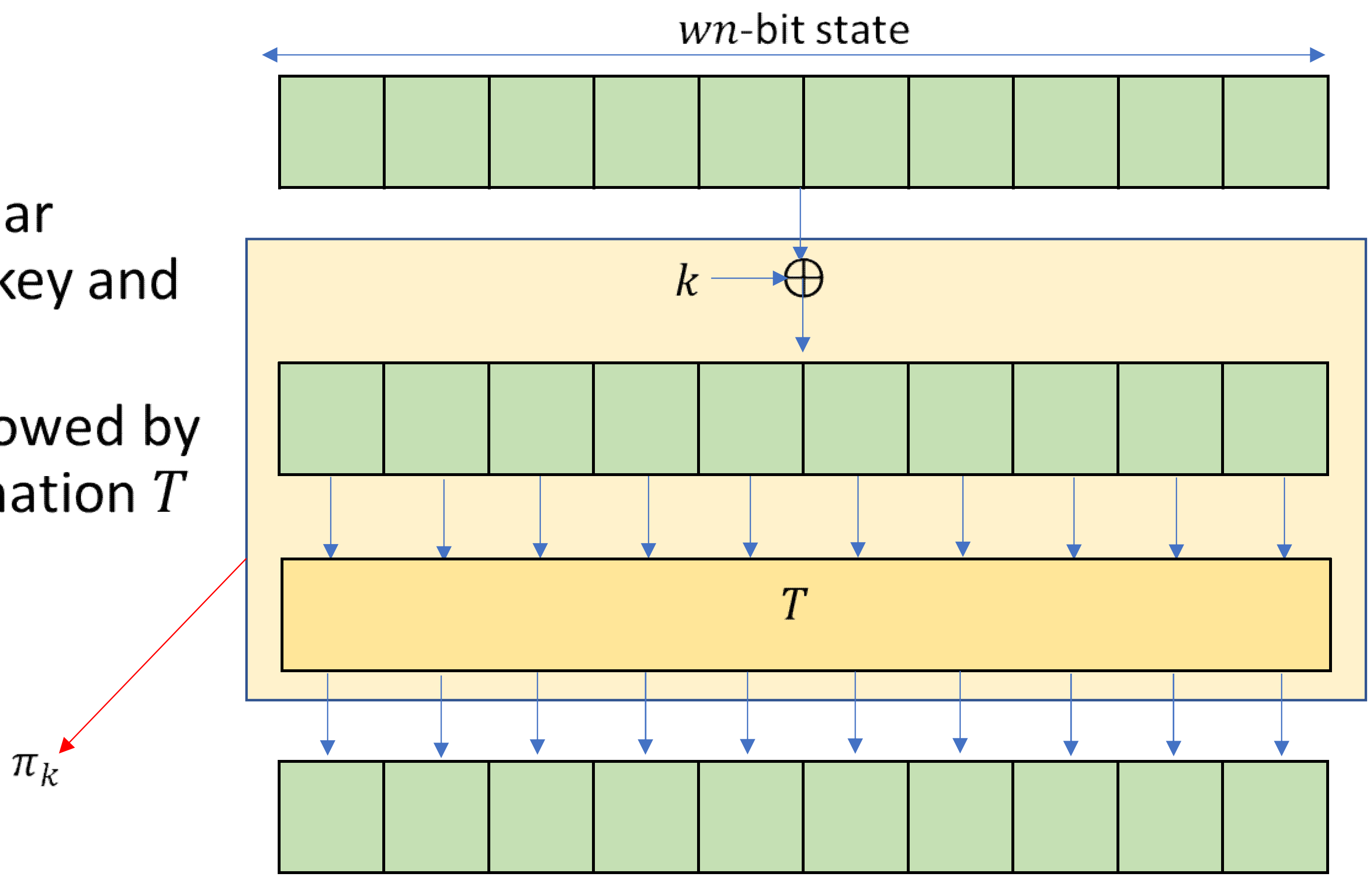
Categorizing SPNs

- Linear SPNs
  - Permutation layer is a linear function of wn-bit round key and state



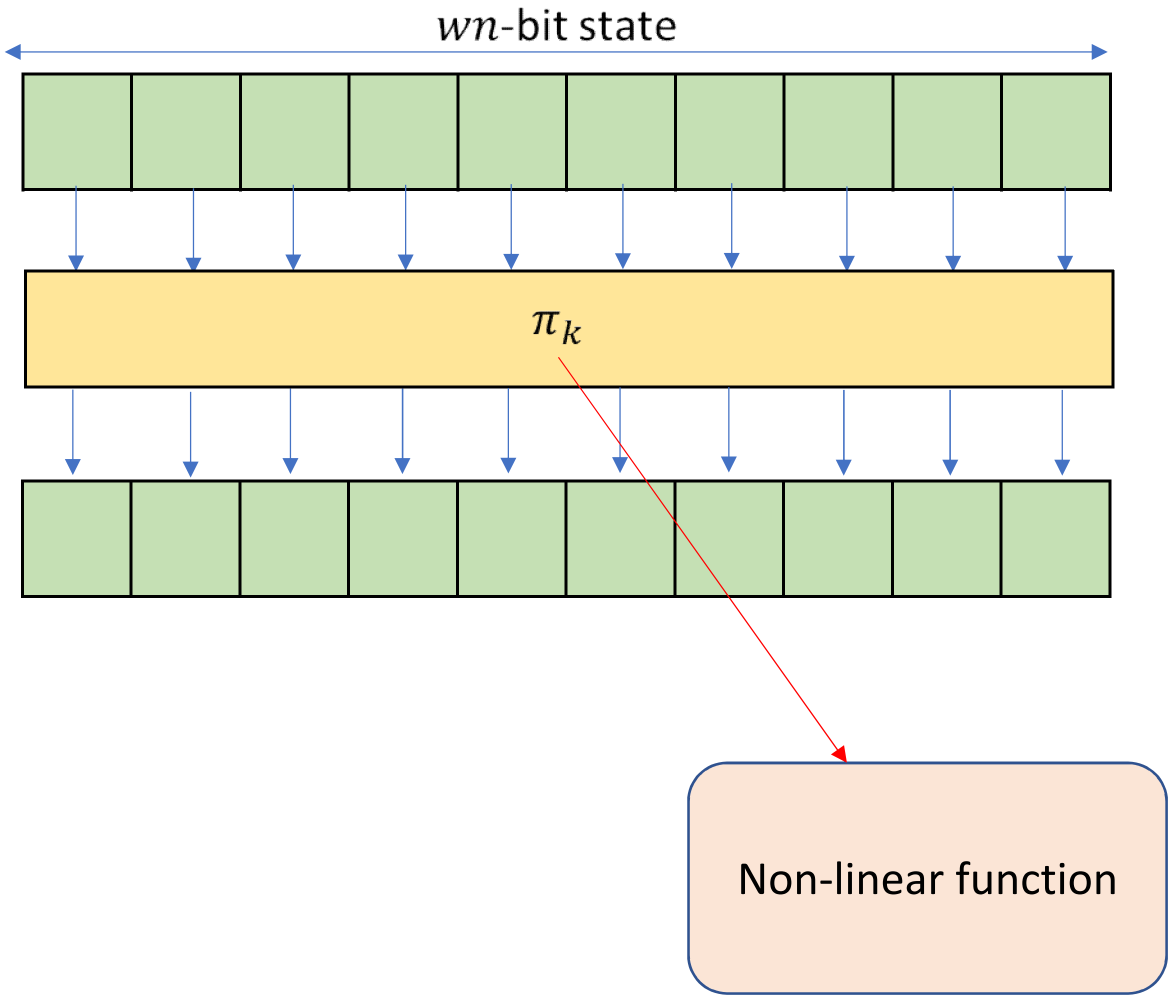
Categorizing SPNs

- Linear SPNs
  - Permutation layer is a linear function of wn-bit round key and state
  - Eg: Simple key-mixing followed by invertible linear transformation T



Categorizing SPNs

- Linear SPNs
  - Permutation layer is a linear function of wn-bit round key and state
  - Eg: Simple key-mixing followed by invertible linear transformation
- Non-linear SPNs
  - If permutation layer is not a linear function



Results: Linear SPNs

- Linear SPNs
  - 2-round insecure (for $w \geq 2$)
    - Application of attack due to Halevi-Rogaway [HR04] for fields of characteristic 2
    - We show an attack that works for fields of general characteristic
  - 3-round linear SPN secure
    - Assuming the keyed permutations satisfy some mild technical requirements (satisfied by matrices with maximal branch number)
    - Proof uses Patarin's H-coefficient technique

Results: Non-linear SPNs

- Non-linear SPNs
  - Even 1-round secure
    - By identifying a combinatorial property that the keyed permutations should satisfy
    - Proof uses Patarin's H-coefficient technique
  - 2-round secure beyond birthday-bound
    - up to $2^{2n/3}$ queries, Independent S-boxes
    - Refined H-coefficient technique [HT16]
  - For $r = 2s$, r-round SPNs secure up to $\ll 2^{\frac{sn}{s+1}}$ queries
    - Show that it can be extended to incorporate tweaks and multi-user security
    - Using coupling technique [MRS09, HR10]

Interpreting our Results

- Provable security of SPN-based block ciphers
  - With public S-boxes
- Domain extension of block ciphers
  - Eg: n = 128 instead of n = 8 -- by using larger domain block cipher with fixed key as S-box
  - First construction of domain extension of block cipher with beyond-birthday security

To allow for public S-box

Interpreting our Results

- Provable security of SPN-based block ciphers
  - With public S-boxes
- Domain extension of block ciphers
  - First construction of domain extension of block cipher with beyond-birthday security

- Implications of small block size
  - Our bounds are weak for SPN-based ciphers such as AES where $n = 8$
  - Need: theory establishing security of building block ciphers from small S-boxes

Results

- Linear SPNs
  - 2-round insecure (for $w \geq 2$)
  - 3-round linear SPN secure
    - Assuming the keyed permutations satisfy some mild technical requirements

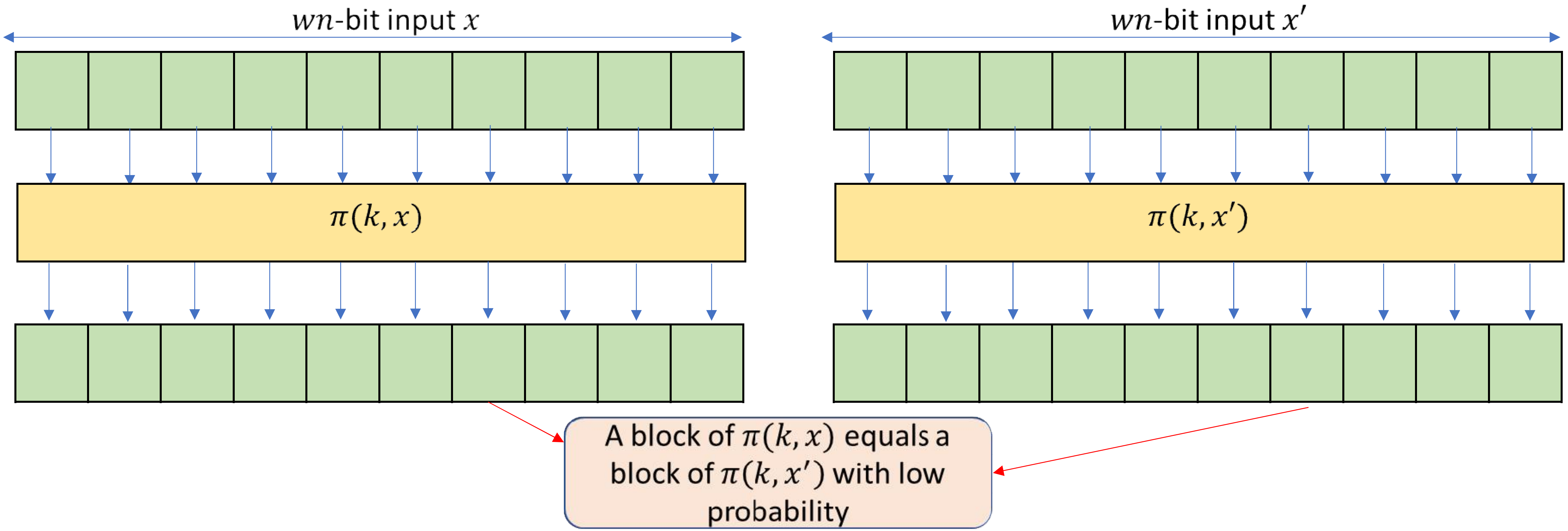
- Non-linear SPNs
  - Even 1-round secure
    - Identify a combinatorial property on the keyed permutations
  - 2-round secure beyond birthday-bound
    - up to $2^{2n/3}$ queries, independent S-boxes
  - r-round SPNs secure up to $\ll 2^{\frac{sn}{s+1}}$ queries for $r = 2s$

Constructing Non-linear SPNs

- Tool: Blockwise-universal Permutations
- Def: A permutation π taking key k and wn-bit input x

Constructing Non-linear SPNs: Blockwise Universal Permutations

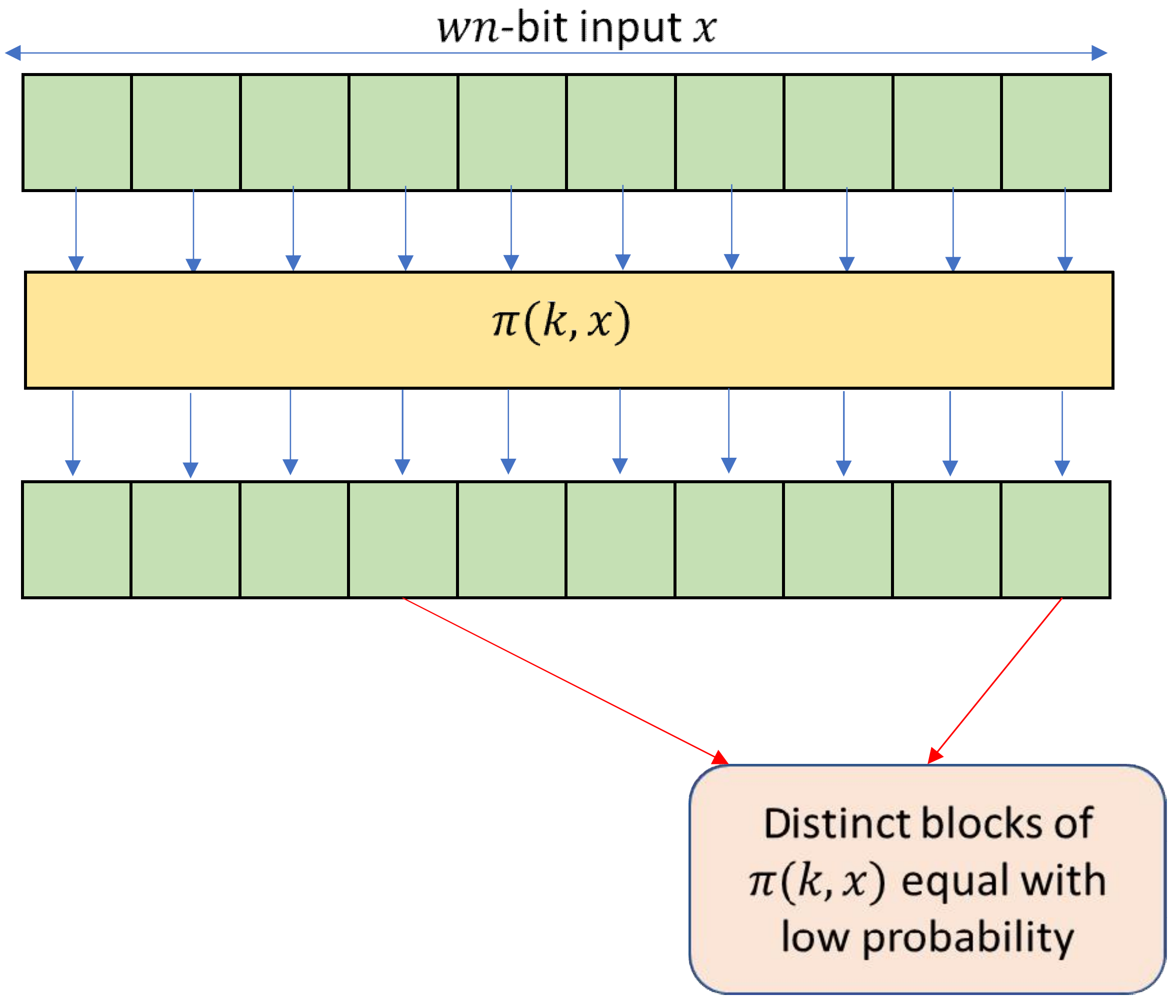
- A keyed permutation π is blockwise-universal if
  1) For any distinct x, x', the probability over uniform key k that a block of $\pi(k, x)$ is equal to a block of $\pi(k, x')$ is low



Constructing Non-linear SPNs: Blockwise Universal Permutations

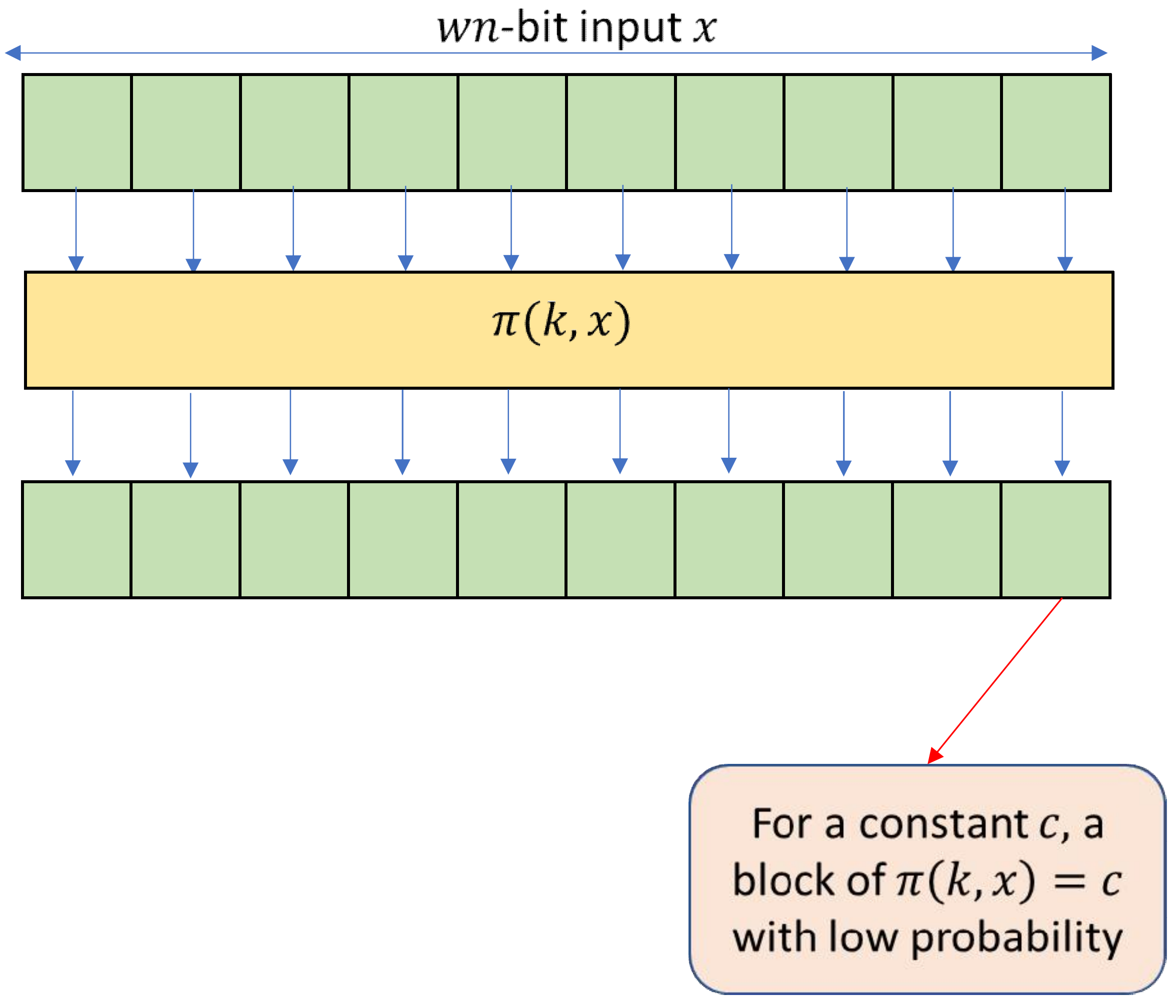
- A keyed permutation π is blockwise-universal if

  2) the probability over uniform key k of two distinct blocks of $\pi(k, x)$ being equal is low



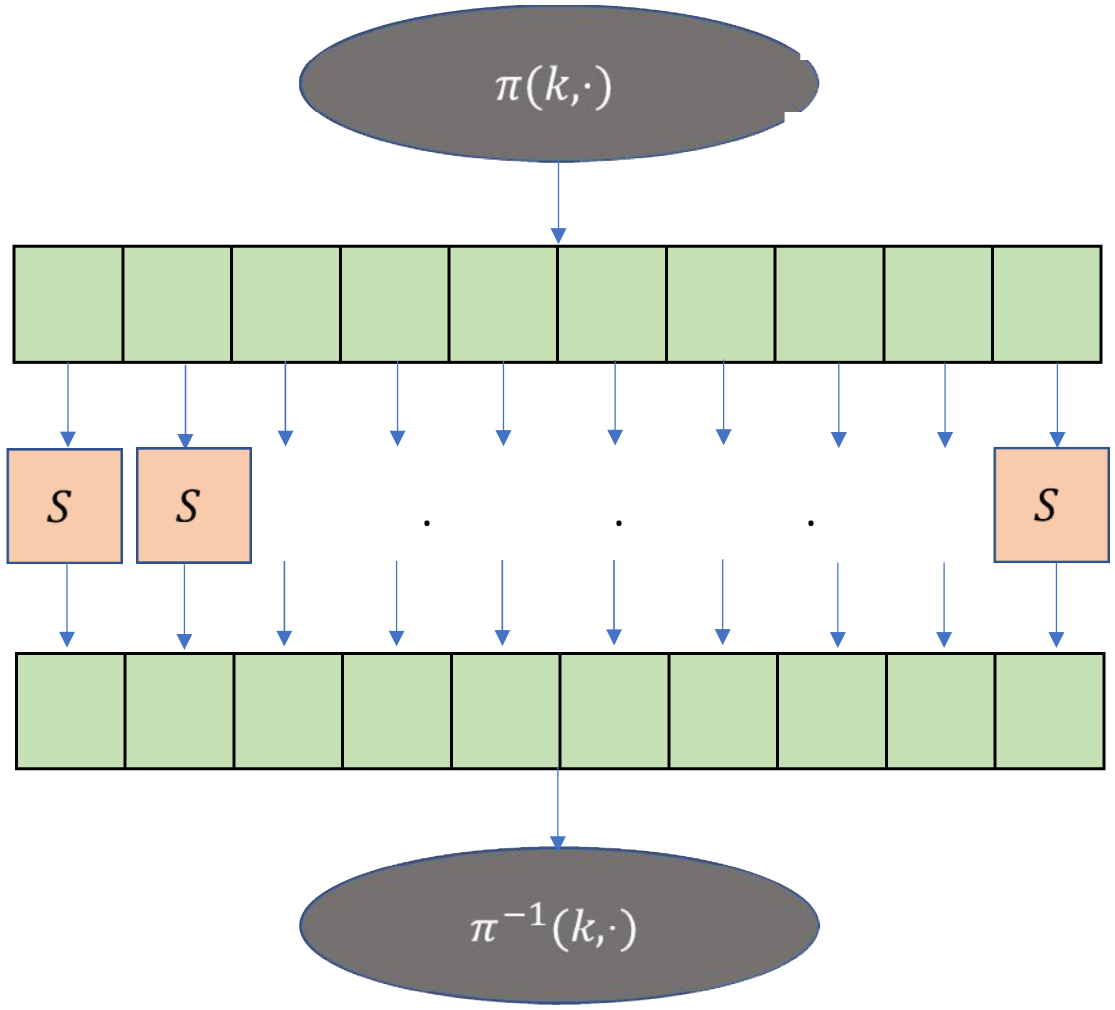
Constructing Non-linear SPNs: Blockwise Universal Permutations

- A keyed permutation π is blockwise-universal if
  3) the probability over a uniform key k that a block of $\pi(k,x) = c$ for a constant c is low
- Related notion considered earlier [HR04, Hal07, NR99]
  - Didn't require this condition
  - Arises due to public S-box



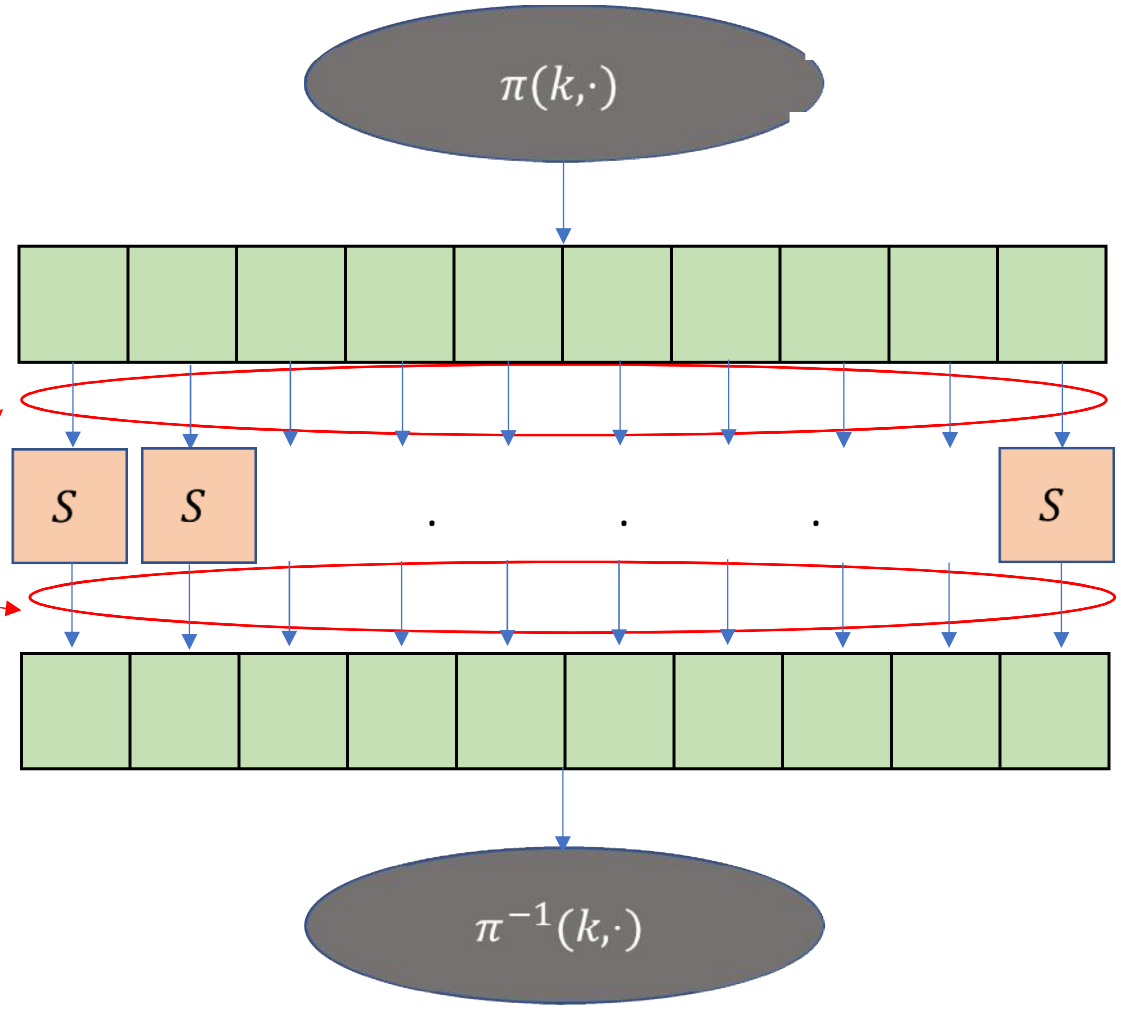
Non-linear SPNs via Blockwise Universal Permutations

- Let π be a keyed permutation that is blockwise-universal
- Theorem: This 1-round non-linear SPN is secure up to the birthday bound
  - Even when same key k is used for π and π^{-1}



Non-linear SPNs via Blockwise Universal Permutations

- Let π be a keyed permutation that is blockwise-universal
- Theorem: This 1-round non-linear SPN is secure up to the birthday bound
- Intuition: Blockwise universality ensures that
  - Inputs to S-box on construction queries are distinct whp
  - D's queries to S and inputs to S-box on construction queries are distinct whp



Non-linear SPNs via Blockwise Universal Permutations

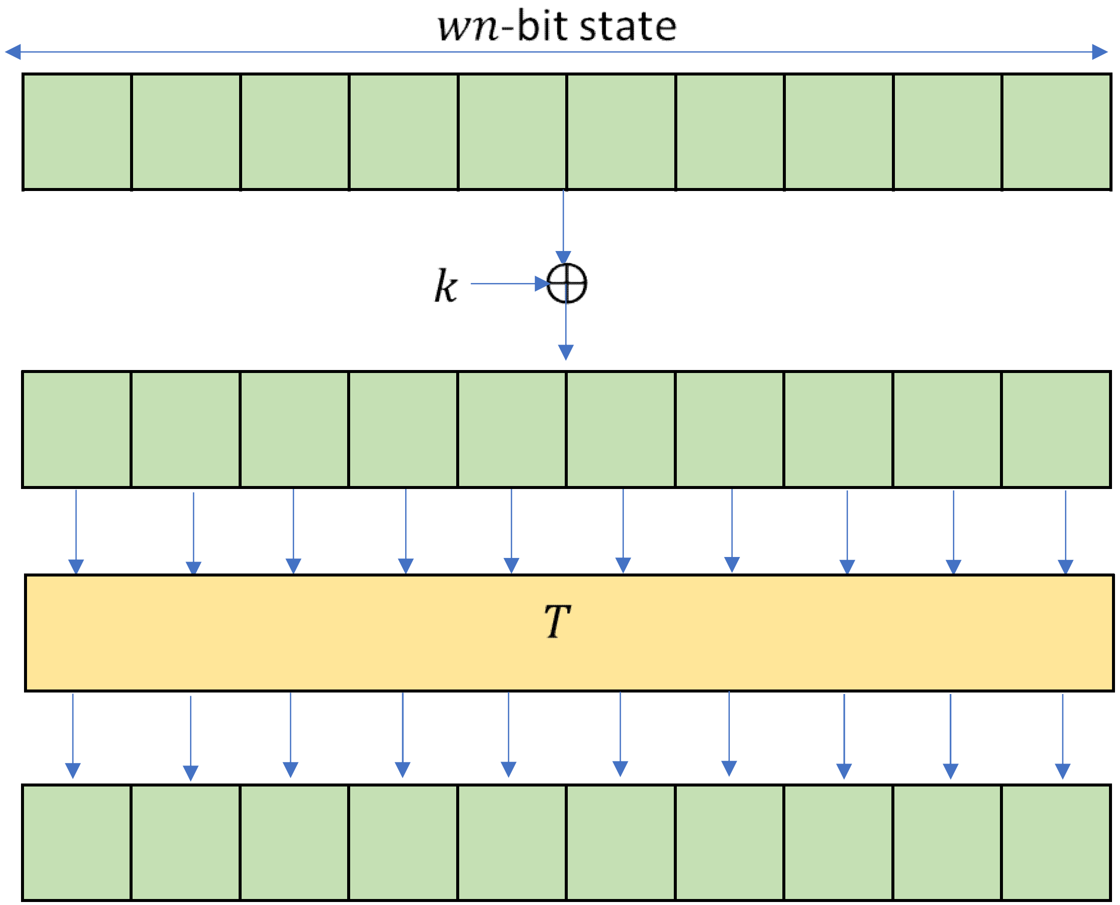
- Instantiating Blockwise Universal Permutations for 1-round non-linear SPN
  - Construction with n-bit keys but high degree
  - Construction with longer keys but low degree (3)

Results

- Linear SPNs
  - 2-round insecure (for $w \geq 2$)
  - 3-round linear SPN secure
    - Assuming the keyed permutations satisfy some mild technical requirements
- Non-linear SPNs
  - Even 1-round secure
    - Identify a combinatorial property on the keyed permutations
  - 2-round secure beyond birthday-bound
    - up to $2^{2n/3}$ queries, independent S-boxes
  - r-round SPNs secure up to $\ll 2^{\frac{sn}{s+1}}$ queries for $r = 2s$

Security of 3-round linear SPN

- Linear SPNs
  - Permutation layer is a linear function of wn-bit round key and state
  - Eg: Simple key-mixing followed by invertible linear transformation T



Security of 3-round Linear SPNs

- Informally, the first and last round of a 3-round linear SPN can be considered to be a blockwise universal permutation

- Intuition doesn't translate formally as the S-boxes are public
  - Needs a dedicated proof

Results

- Linear SPNs
  - 2-round insecure (for $w \geq 2$)
  - 3-round linear SPN secure
    - Assuming the keyed permutations satisfy some mild technical requirements
- Non-linear SPNs
  - Even 1-round secure
    - Identify a combinatorial property on the keyed permutations
  - 2-round secure beyond birthday-bound
    - up to $2^{2n/3}$ queries, independent S-boxes
  - r-round SPNs secure up to $\ll 2^{\frac{sn}{s+1}}$ queries for $r = 2s$

Takeaway

- Provable security of SPN-based block ciphers
  - With public S-boxes
- Domain extension of block ciphers
  - First construction of domain extension of block cipher with beyond-birthday security

Thank You

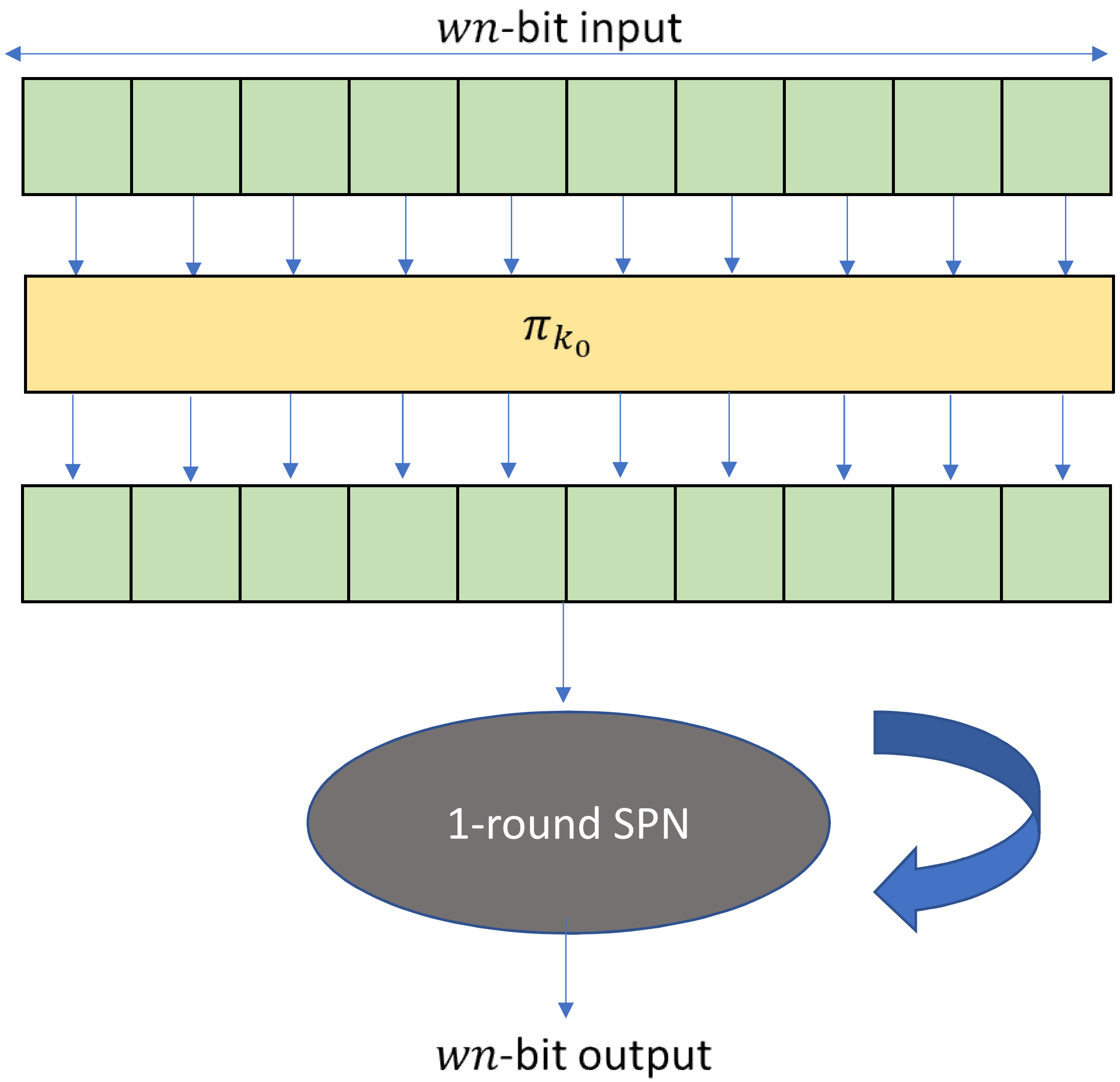
Constructing Non-linear SPNs

- Tool: Blockwise-universal Permutations
- A keyed permutation π is blockwise-universal if
  - (1) For any distinct x, x', the probability that a block of $\pi(k, x)$ is equal to a block of $\pi(k, x')$ is low
  - (2) the probability of two distinct blocks of $\pi(k, x)$ being equal is low
  - (3) the probability that a block of $\pi(k, x) = c$ for a constant c is low

- Related notion considered earlier [HR04, Hal07, NR99]
  - Didn't require third condition – arises due to public S-box

SPNs: Applications

- Block ciphers (via SPNs)
  - Eg: AES
  - Typically, have small S-boxes
    - AES uses 8-bit S-box
- Domain Extension to obtain wide block ciphers
  - Larger domain block cipher with fixed key as S-box
  - Or larger dedicated permutation as S-box



Constructing Non-linear SPNs: Blockwise Universal Permutations

- A keyed permutation π is blockwise-universal if
  1) For any distinct x, x', the probability over uniform key k that a block of $\pi(k, x)$ is equal to a block of $\pi(k, x')$ is low