Substitution-Permutation Networks and Linear Cryptanalysis

Douglas Wikström
KTH Stockholm
dog@csc.kth.se

January 31

- Substitution-Permutation Networks
- Bias
- Linear Cryptoanalysis

Quote of the Day

The news here is not that DES is insecure, that hardware algorithm-crackers can be built, or that a 56-bit key length is too short. ... The news is how long the government has been denying that these machines were possible. As recently as 8 June 98, Robert Litt, principal associate deputy attorney general at the Department of Justice, denied that it was possible for the FBI to crack DES. ... My comment was that the FBI is either incompetent or lying, or both.

– Bruce Schneier, 1998

Ideal Block Cipher

- For every key a block-cipher with plaintext/ciphertext space $\{0,1\}^n$ is gives a permutation of $\{0,1\}^n$.

  What would be an ideal cipher?

Ideal Block Cipher

- For every key a block-cipher with plaintext/ciphertext space $\{0,1\}^n$ is gives a permutation of $\{0,1\}^n$.

  What would be an ideal cipher?

- The ideal cipher is one where each key gives a **randomly chosen permutation** of $\{0,1\}^n$.

  Why is this not possible?

Ideal Block Cipher

- For every key a block-cipher with plaintext/ciphertext space $\{0,1\}^n$ is gives a permutation of $\{0,1\}^n$.

  What would be an ideal cipher?

- The ideal cipher is one where each key gives a **randomly chosen permutation** of $\{0,1\}^n$.

  Why is this not possible?

- The representation of a single typical function $\{0,1\}^{128} \to \{0,1\}^{128}$ requires $\approx 2^{128}16$ terabytes, and we need 2^{128} of those functions to choose from...

  What should we look for instead?

Something Smaller

Idea. Compose smaller permutations into a large one. Mix the components "thoroughly".

Something Smaller

Idea. Compose smaller permutations into a large one. Mix the components "thoroughly".

Shannon (1948) calls this:

- **Diffusion.** "In the method of diffusion the statistical structure of M which leads to its redundancy is dissipated into long range statistics..."
- **Confusion.** "The method of confusion is to make the relation between the simple statistics of E and the simple description of K a very complex and involved one."

Substitution-Permutation Networks (1/2)

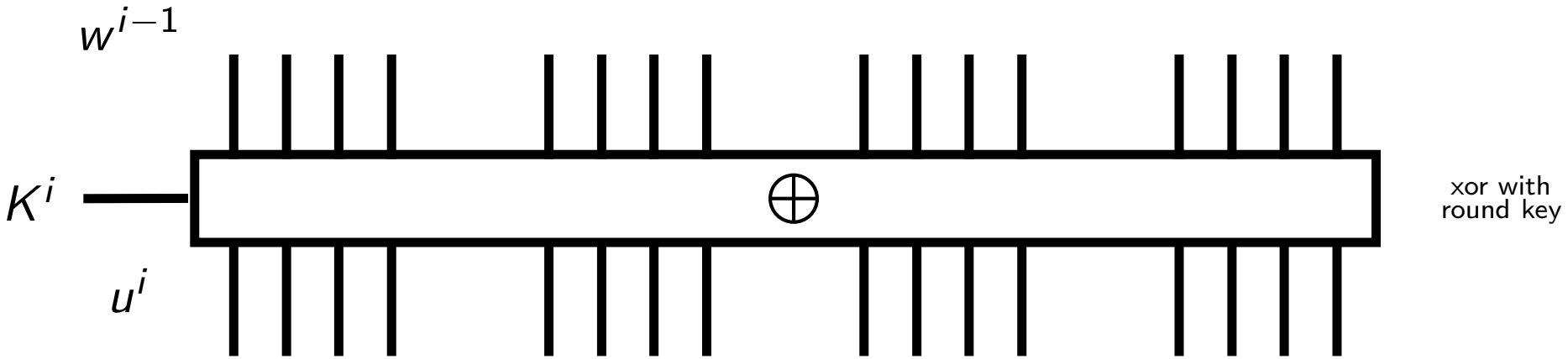
- **Block-size.** We use a block-size of $m \times l$ bits.
- **Key Schedule.** Each round r uses its own round key K^r derived from the key K using a key schedule.
- **Each Round.** In each round we invoke:
  1. **Round Key.** xor with the current round key.
  2. **Substitution.** A permutation π_S acting on $\{0,1\}^l$ on each block of l bits.
  3. **Permutation.** A permutation π_S acting on $\{1,\ldots,lm\}$ to reorder the l-bit blocks.

Substitution-Permutation Networks (2/2)

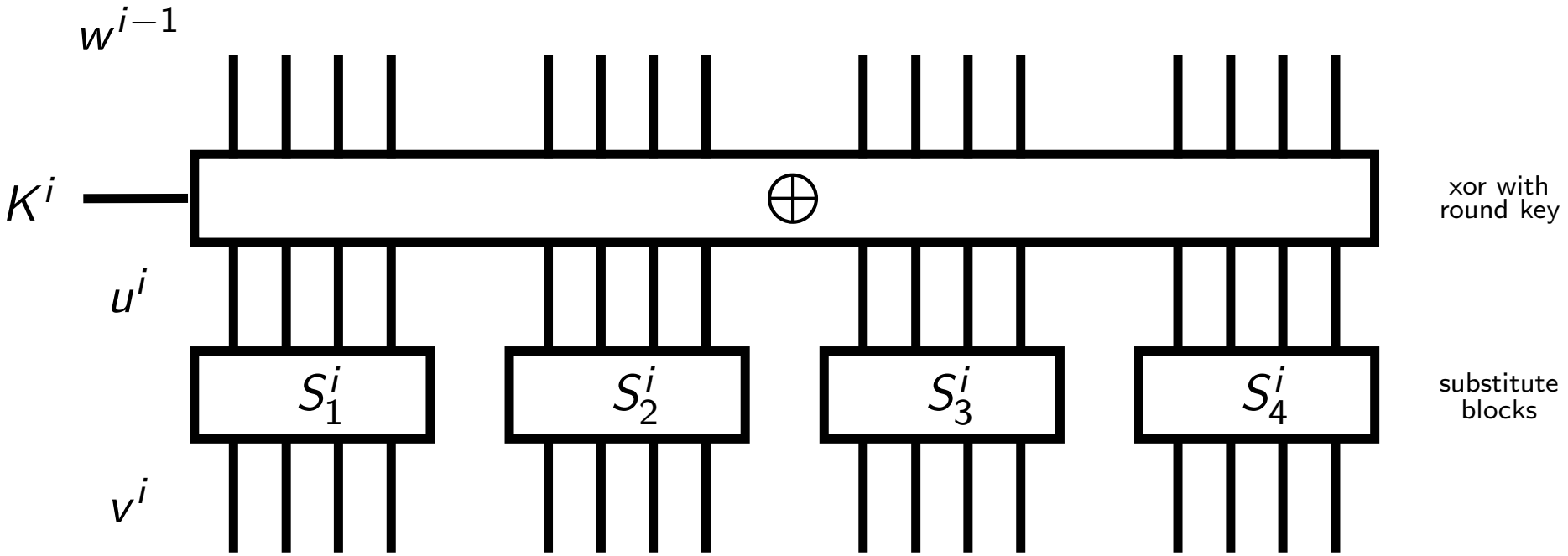
w^{i-1}

K^i

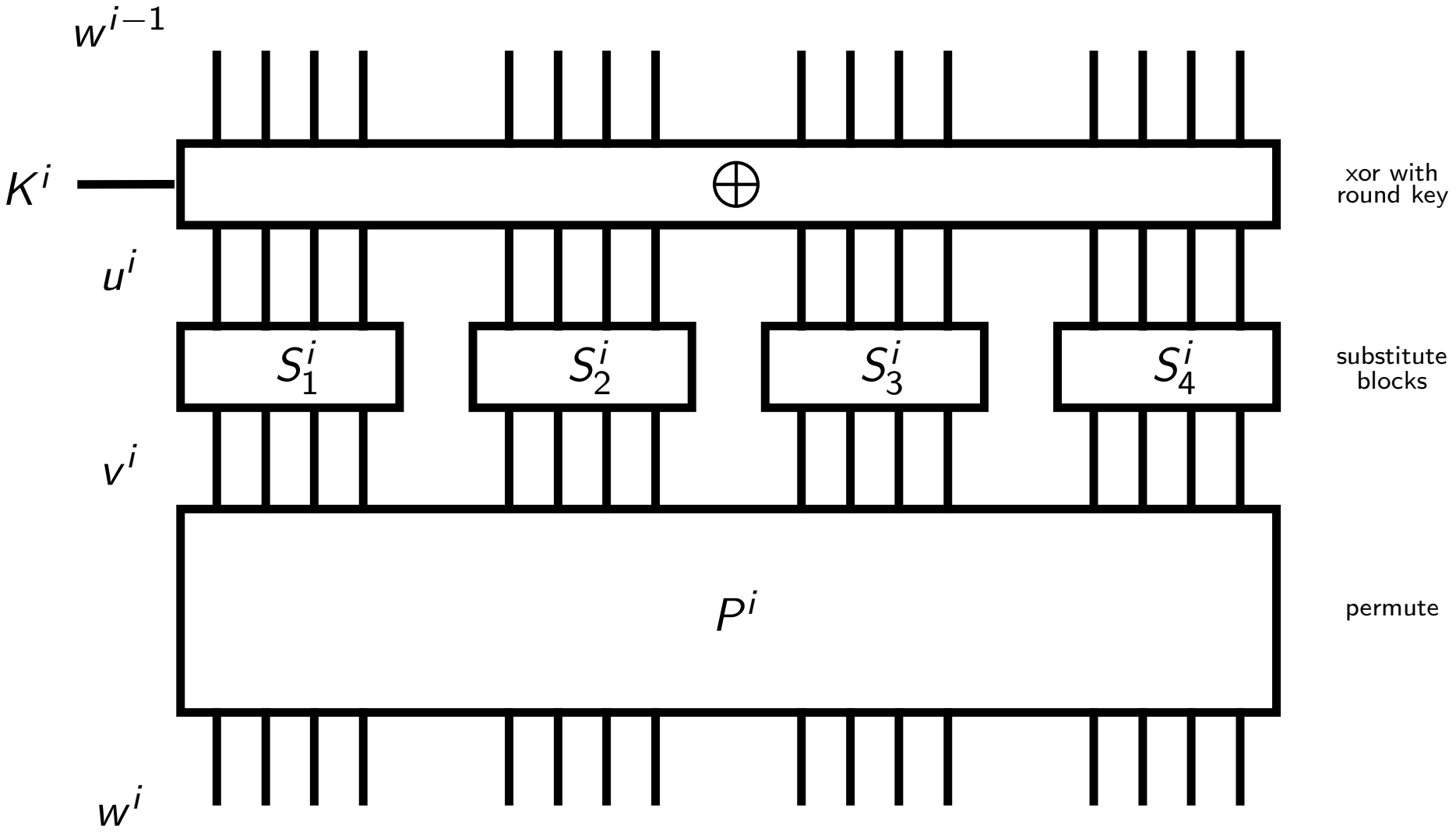
Substitution-Permutation Networks (2/2)



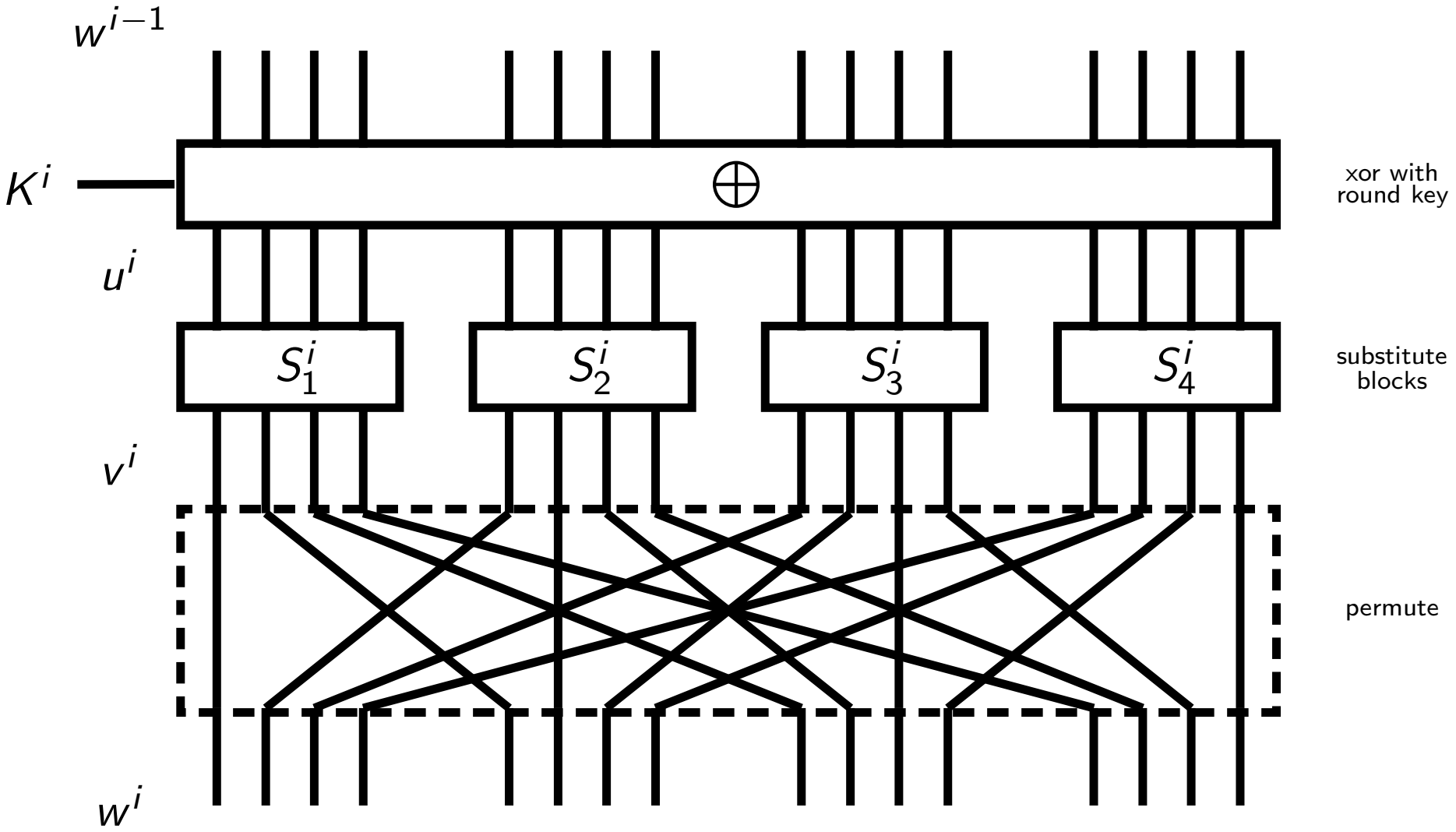
Substitution-Permutation Networks (2/2)



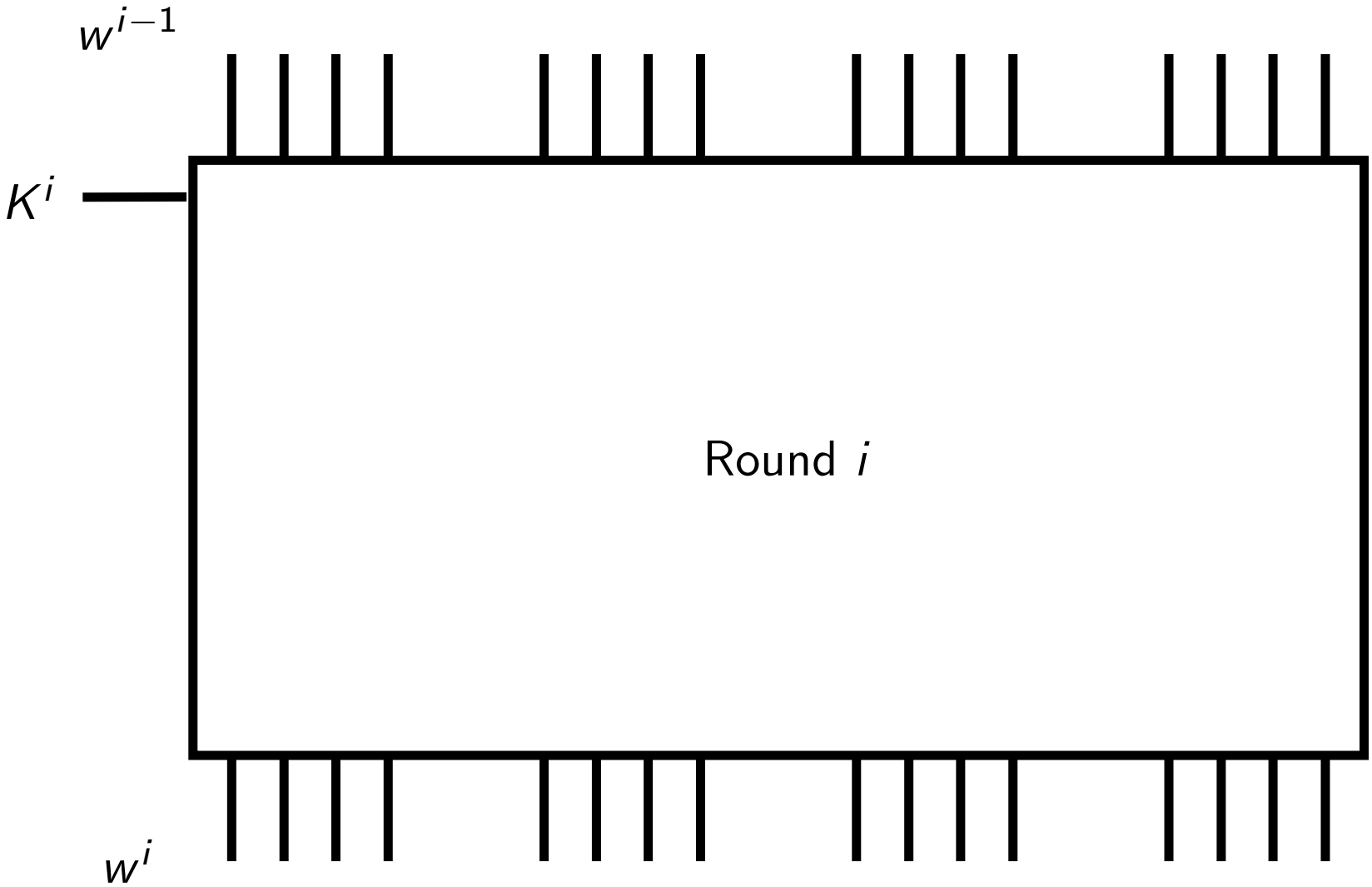
Substitution-Permutation Networks (2/2)



Substitution-Permutation Networks (2/2)



Substitution-Permutation Networks (2/2)



Bias

Definition. The bias $\epsilon(X)$ of a binary random variable X is defined by

$$\epsilon(X) = \Pr[X = 0] - \frac{1}{2} \ .$$

Measures the distance of the expected value of X from $1/2$.

Piling-Up Lemma

Lemma. Let $X_1, \ldots, X_k$ be independent binary random variables and let $\epsilon_i = \epsilon(X_i)$. Then

$$\epsilon\left(\bigoplus_i X_i\right) = 2^{k-1}\prod_i \epsilon_i \ .$$

Proof.

$$\begin{aligned}\sum_{\oplus x_i=1}\prod_i\left(\frac{1}{2}+(-1)^{x_i}\epsilon_i\right) &= \sum_{\oplus x_i=1}\left(2^{-k}+(-1)^k\prod_i\epsilon_i\right)\\ &\quad+\sum_j\sum_{\oplus x_i=1} f_j(x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_k)\\ &= \frac{1}{2}+(-1)^k 2^{k-1}\prod_i\epsilon_i \ .\end{aligned}$$

Application

- Given a random system we can find the bias of **some** binary random variables by exhaustive search.
- Then we can **heuristically** compute the bias of **any** linear combination modulo 2 of these variables **assuming independence**.
- Unless the bias is extreme, we can only consider small k.

Idea

Idea.

1. Find biased linear combinations of the input and output of the S-boxes.

2. Combine these using Pile-Up Lemma to a single biased variable expressed in terms of a small number of input, output, and key bits.

3. The correct key preserves this bias, whereas the wrong key destroys it.

4. Known plaintext attack. Large number of plaintext-ciphertext pairs give samples from our variable.

5. Guess the key-bits with the largest bias!

Linear Approximation of S-boxes

Let X and Y be the input and output of an S-box, i.e.

$$Y = \pi_S(X) \ .$$

We consider the bias of linear combinations of the form

$$a \cdot X \oplus b \cdot Y = \left(\bigoplus_i a_i X \right) \oplus \left(\bigoplus_i b_i Y \right) \ .$$

Linear Approximation Example From Stinson (1/2)

- Let $N_L(a, b)$ be the number of zero-outcomes of $a \cdot X \oplus b \cdot Y$.
- The bias is then

$$\epsilon(a \cdot X \oplus b \cdot Y) = \frac{N_L(a, b) - 8}{16} \quad ,$$

since there are four bits in X, and Y is determined by X.

Linear Approximation Table Example From Stinson (2/2)

$N_L(a,b)$		b														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
a	0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	1	8	8	6	6	8	8	6	14	10	10	8	8	10	10	8	8
	2	8	8	6	6	8	8	6	6	8	8	10	10	8	8	2	10
	3	8	8	8	8	8	8	8	8	10	2	6	6	10	10	6	6
	4	8	10	8	6	6	4	6	8	8	6	8	10	10	4	10	8
	5	8	6	6	8	6	8	12	10	6	8	4	10	8	6	6	8
	6	8	10	6	12	10	8	8	10	8	6	10	12	6	8	8	6
	7	8	6	8	10	10	4	10	8	6	8	10	8	12	10	8	10
	8	8	8	8	8	8	8	8	8	6	10	10	6	10	6	6	2
	9	8	8	6	6	8	8	6	6	4	8	6	10	8	12	10	6
	A	8	12	6	10	4	8	10	6	10	10	8	8	10	10	8	8
	B	8	12	8	4	12	8	12	8	8	8	8	8	8	8	8	8
	C	8	6	12	6	6	8	10	8	10	8	10	12	8	10	8	6
	D	8	10	10	8	6	12	8	10	4	6	10	8	10	8	8	10
	E	8	10	10	8	6	4	8	10	6	8	8	6	4	10	6	8
	F	8	6	4	6	6	8	10	8	8	6	12	6	6	8	10	8

Linear Cryptanalysis (1/2)

- **Approximation of S-boxes.** Find variables

$$a \cdot U^i_{[t,t+4]} \oplus b \cdot V^i_{[t,t+4]} = a \cdot (W^{i-1}_{[t,t+4]} \oplus K^i_{[t,t+4]}) \oplus b \cdot V^i_{[t,t+4]}$$

with large bias.

- **Preservation of Bias.** Note that the bias is preserved if we condition on $K^i_{[t,t+4]} = k^i_{[t,t+4]}$.
- **Cancellation of Bias.** On the other hand

$$a \cdot (W^{i-1}_{[t,t+4]} \oplus \tilde{k}^i_{[t,t+4]}) \oplus b \cdot V^i_{[t,t+4]}$$

with $\tilde{k}^i_{[t,t+4]} \neq k^i_{[t,t+4]}$ has (probably) small bias.

Linear Cryptanalysis (1/2)

- **Approximation of S-boxes.** Find variables

  $$a \cdot U^i_{[t,t+4]} \oplus b \cdot V^i_{[t,t+4]} = a \cdot (W^{i-1}_{[t,t+4]} \oplus K^i_{[t,t+4]}) \oplus b \cdot V^i_{[t,t+4]}$$

  with large bias.

- **Preservation of Bias.** Note that the bias is preserved if we condition on $K^i_{[t,t+4]} = k^i_{[t,t+4]}$.

- **Cancellation of Bias.** On the other hand

  $$a \cdot (W^{i-1}_{[t,t+4]} \oplus \tilde{k}^i_{[t,t+4]}) \oplus b \cdot V^i_{[t,t+4]}$$

  with $\tilde{k}^i_{[t,t+4]} \neq k^i_{[t,t+4]}$ has (probably) small bias.

Samples of $W^{i-1}_{[t,t+4]}$ and $V^i_{[t,t+4]}$ let us identify $k^i_{[t,t+4]}$!

Linear Cryptanalysis (2/2)

Additional Steps.

1. **Find Trails.** Combine biased variables to cancel out all intermediate variables, i.e., a small number of input-, output-, and key-bits should remain.

2. **Bias.** Compute the resulting bias using the Pile-Up lemma.

3. **Identify Key Bits.** The preservation/cancelation of bias works the same as for a single S-box. Identify key bits using plaintext-ciphertext pairs!