Search for Related-key Differential Characteristics in DES-like ciphers

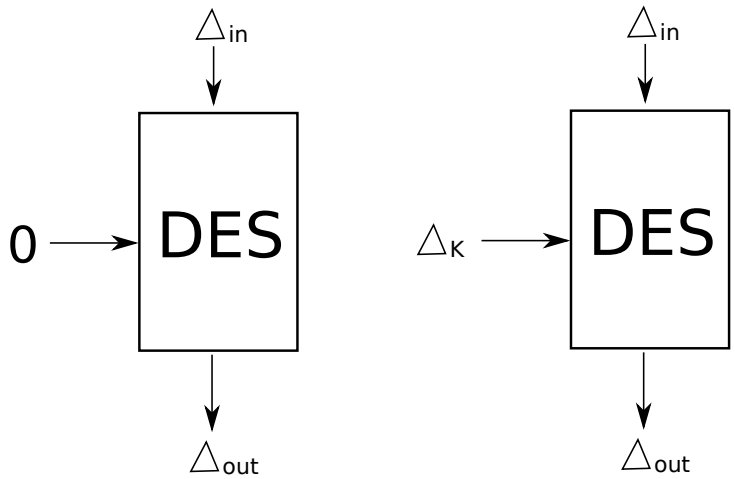
Ivica Nikolić (joint work with Alex Biryukov)

University of Luxembourg, Luxembourg

1 June 2010

Single-Key vs Related-Key in DES

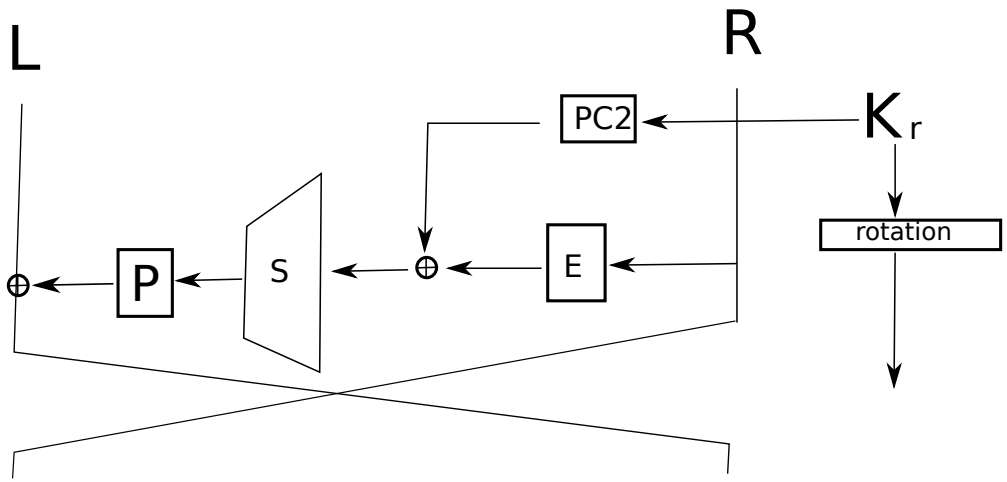
- DES has 64-bit state and 56-bit key
- Single-key diff. brute force $\geq 2^{64}$
- Related-key diff. brute force $\geq 2^{120}$



Description of DES-like Ciphers

- Has 16 rounds
- DES-like $\equiv$ the S-boxes can be any

One round:



Properties

Task: find the best related-key diff. char. Hence:

- Feasible
- Perform a full search

Algorithms

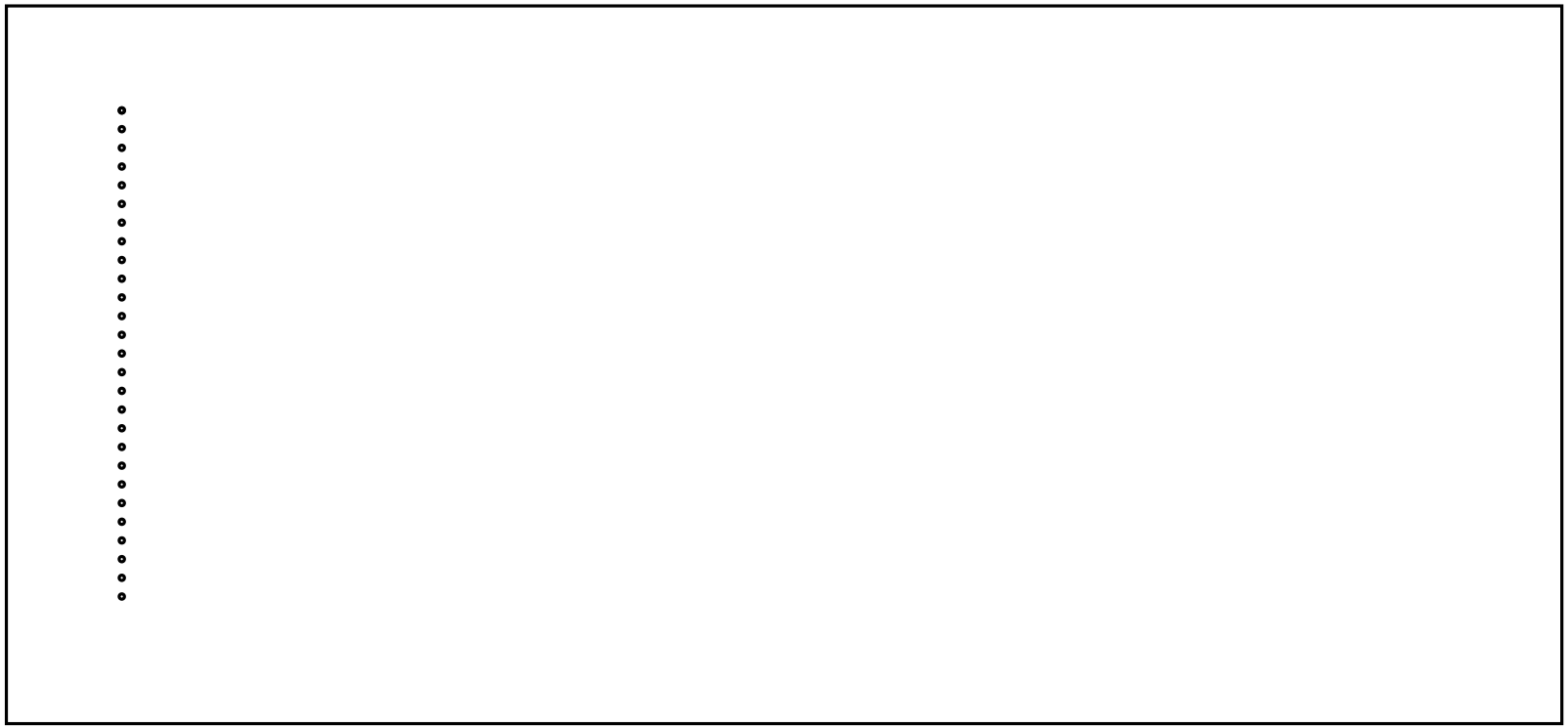
- Dynamic programming (requires memory)
- **Matsui's approach**
- **Split approach**

Matsui's Approach

- Given the probabilities of the best $1, 2, \ldots, r-1$ round characteristics and some r-round characteristic it builds *the* best r-round characteristic.
- Recursive; extend the characteristics only if its prob. $\times$ the prob. of the rest of the rounds is higher then the previous best prob. on all rounds.

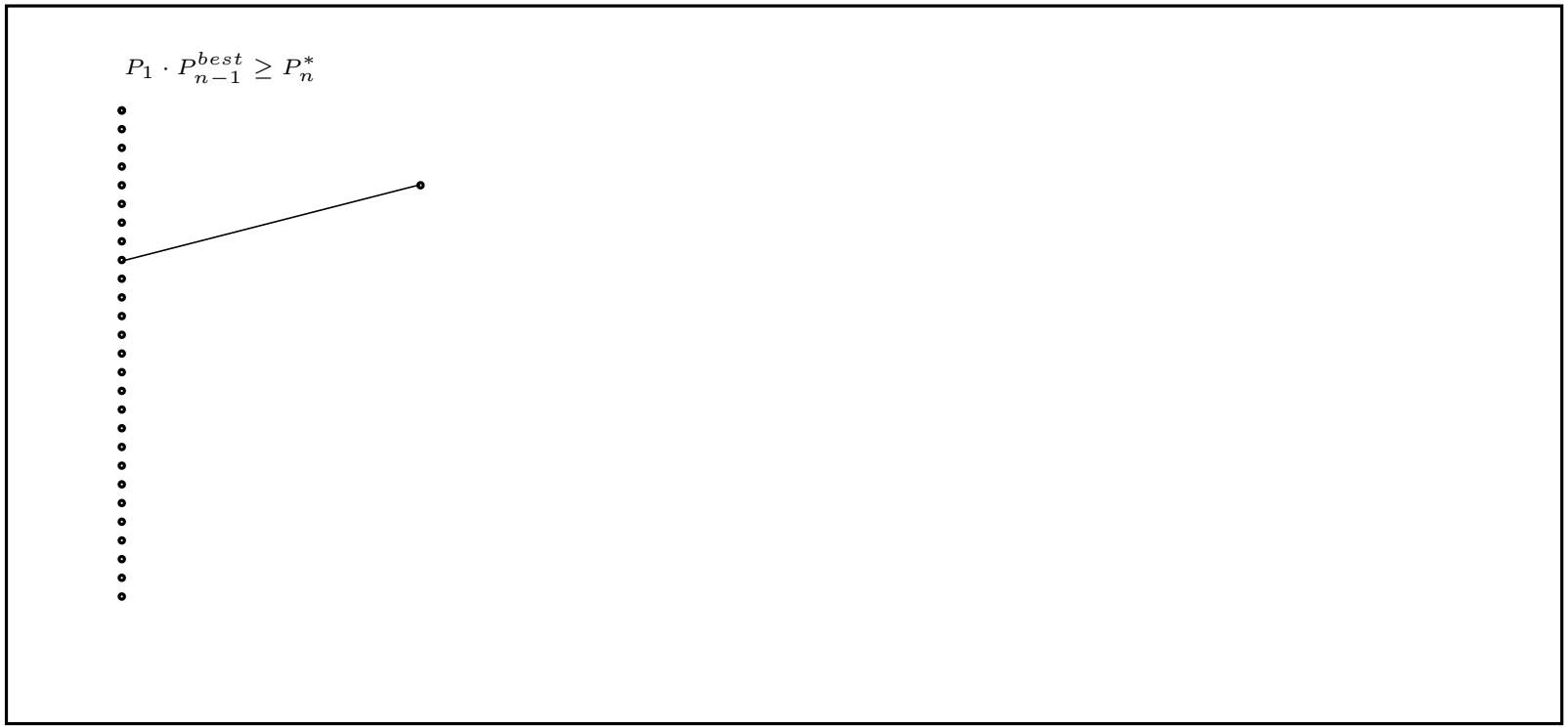
Matsui's Approach

For each $r-1$ round char.: extend for one round, and check if $P_r \cdot P_{n-r}^{best} \geq P_n^*$ (if $P_n > P_n^*$ update P_n^*)



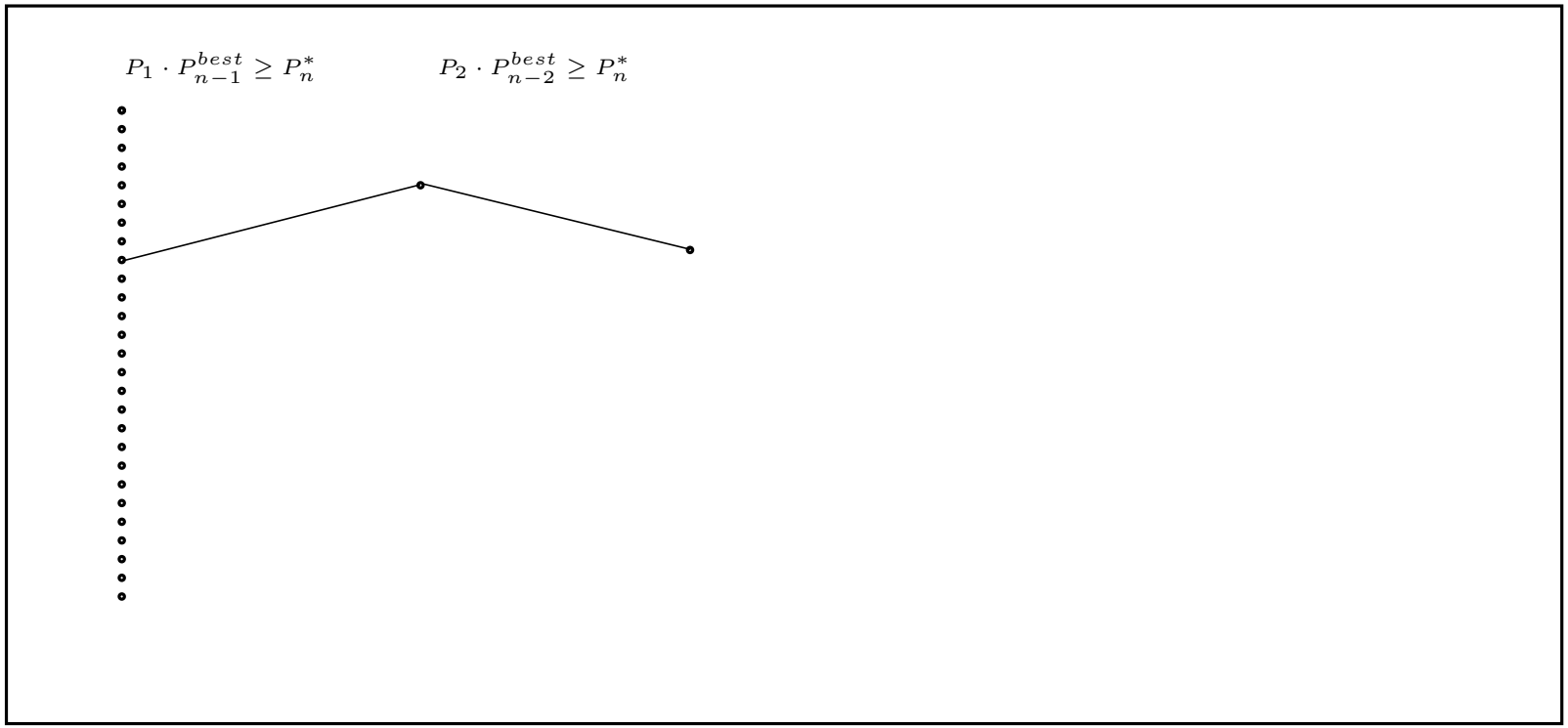
Matsui's Approach

For each $r-1$ round char.: extend for one round, and check if $P_r \cdot P_{n-r}^{best} \geq P_n^*$ (if $P_n > P_n^*$ update P_n^*)



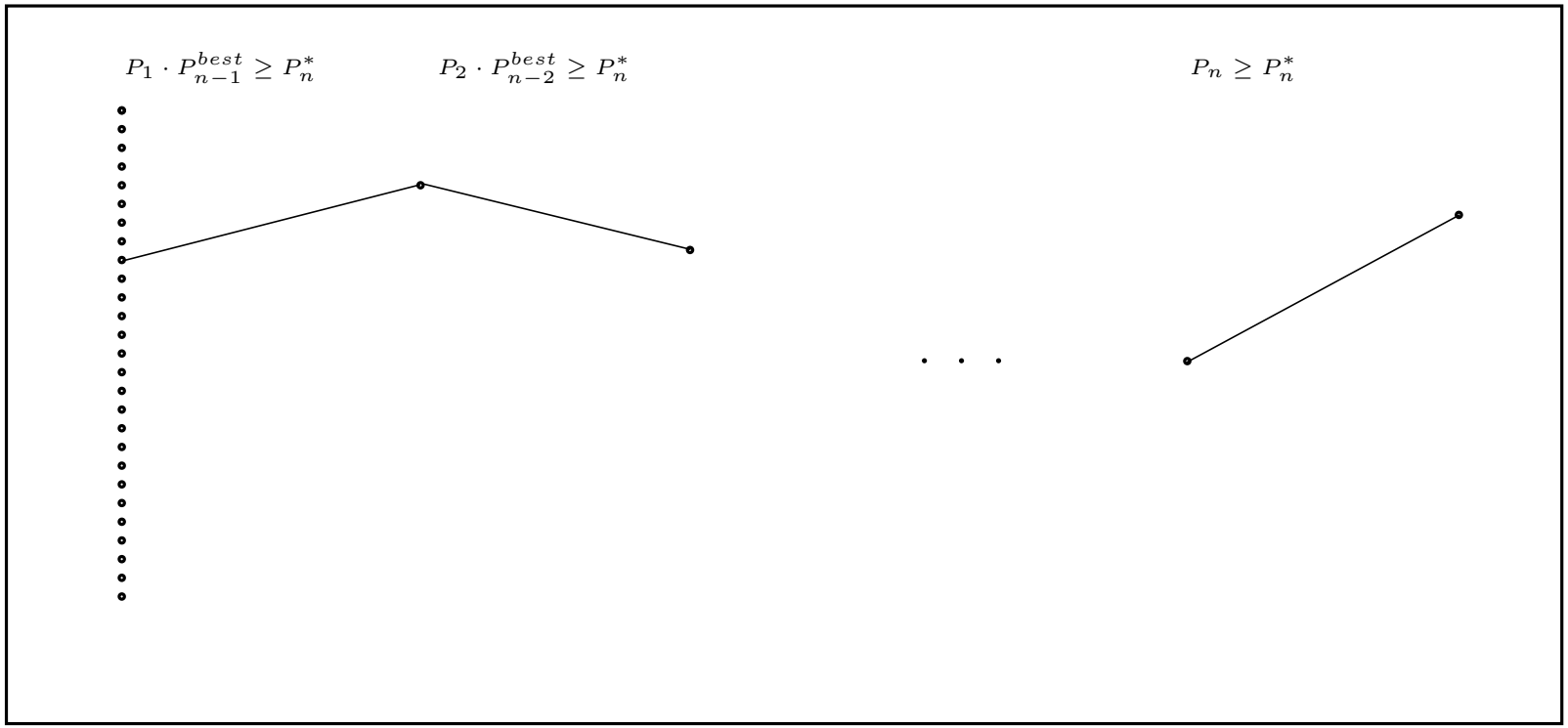
Matsui's Approach

For each $r-1$ round char.: extend for one round, and check if $P_r \cdot P_{n-r}^{best} \geq P_n^*$ (if $P_n > P_n^*$ update P_n^*)



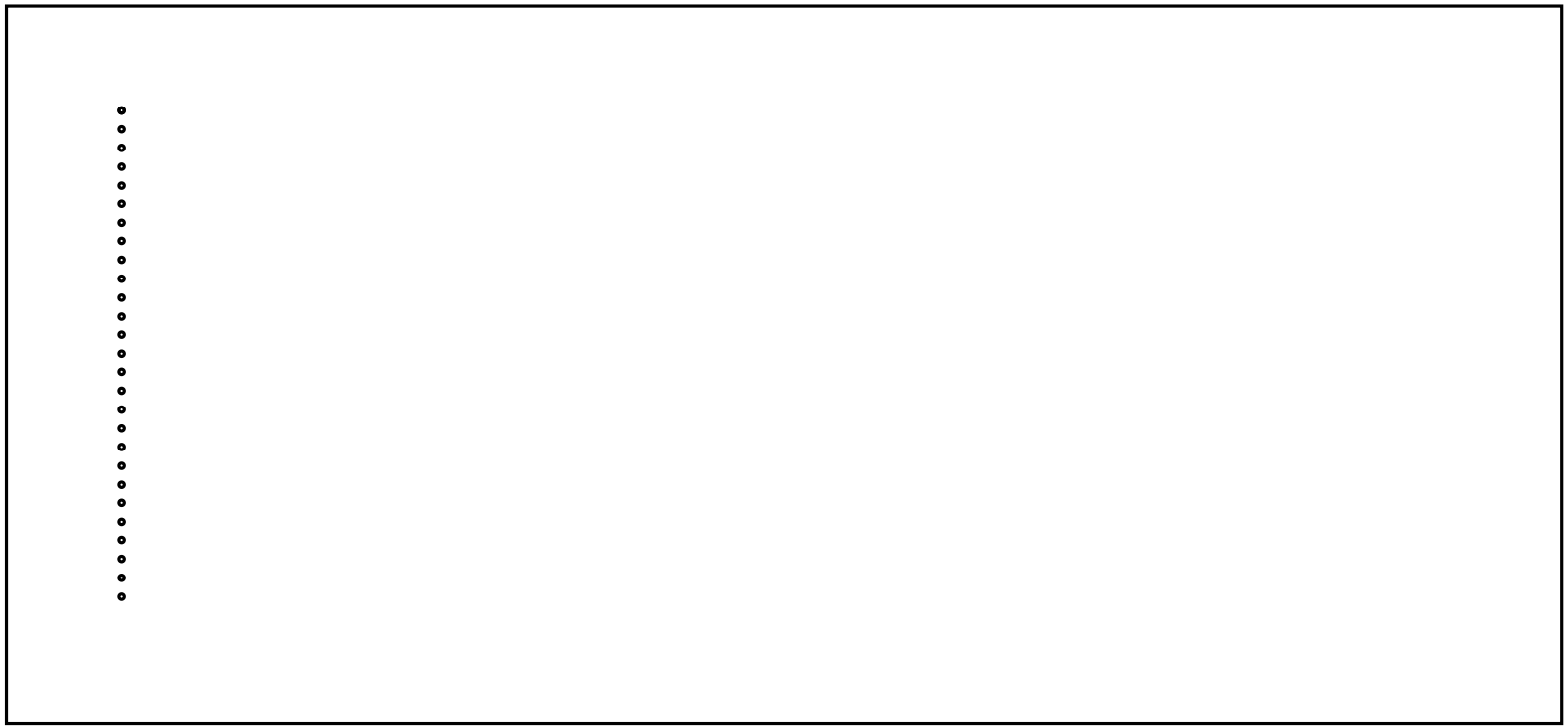
Matsui's Approach

For each $r-1$ round char.: extend for one round, and check if $P_r \cdot P_{n-r}^{best} \geq P_n^*$ (if $P_n > P_n^*$ update P_n^*)



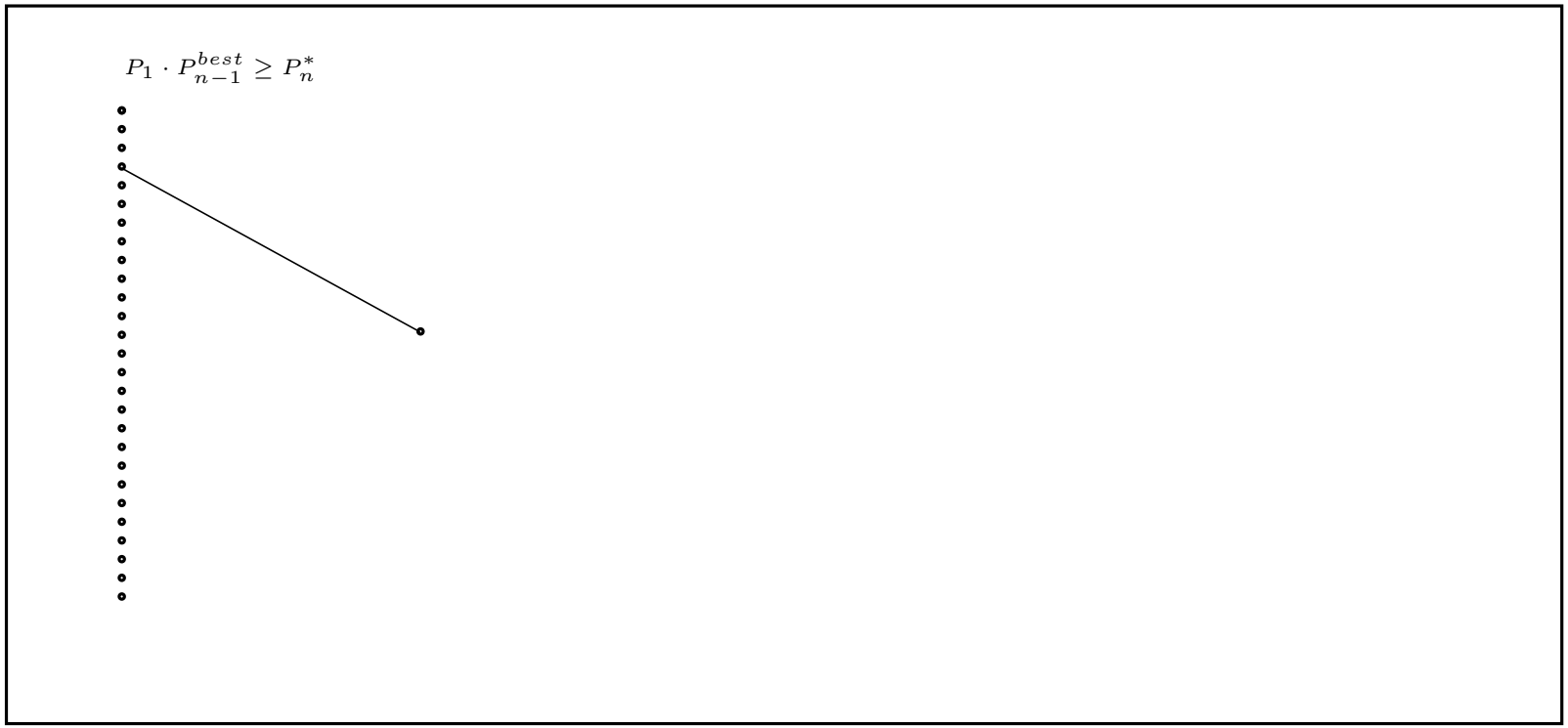
Matsui's Approach

For each $r-1$ round char.: extend for one round, and check if $P_r \cdot P_{n-r}^{best} \geq P_n^*$ (if $P_n > P_n^*$ update P_n^*)



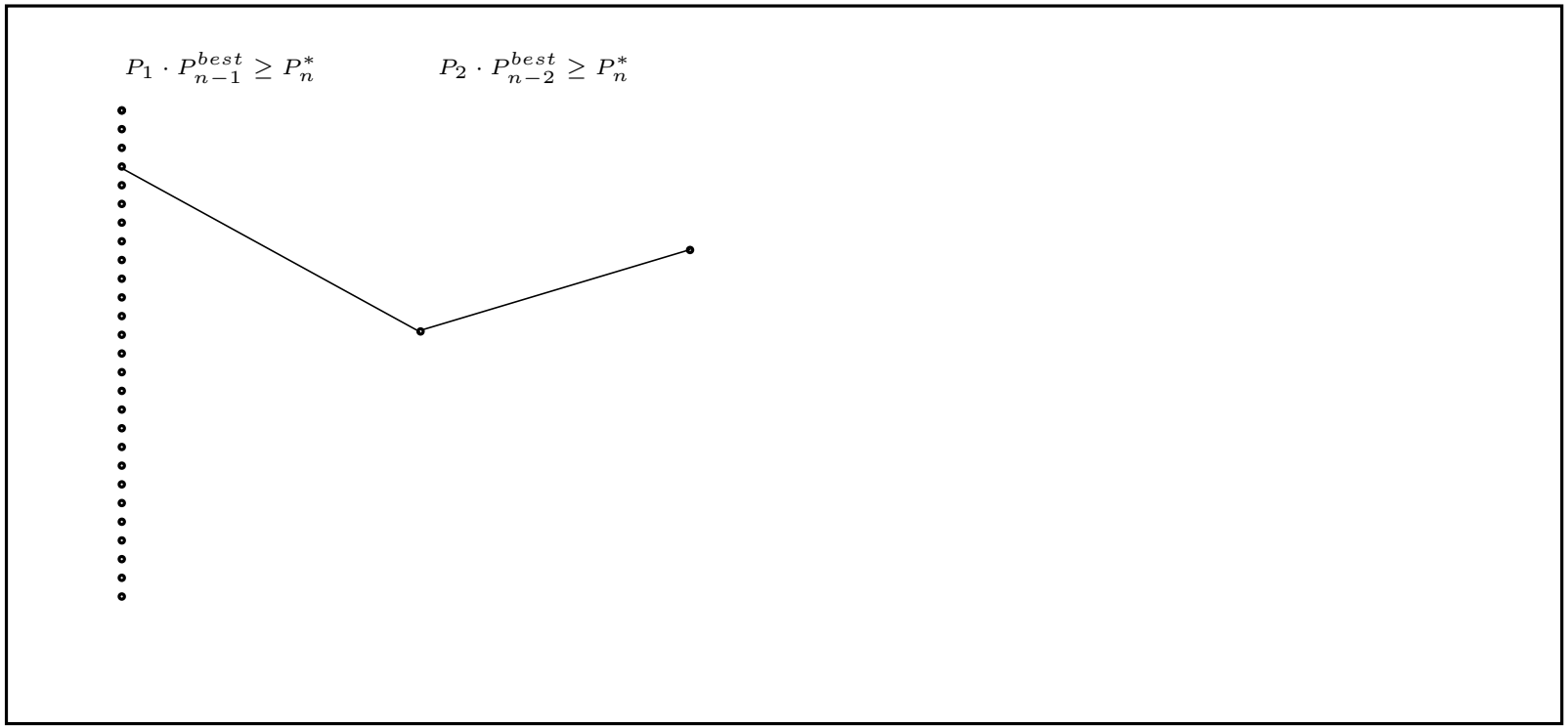
Matsui's Approach

For each $r-1$ round char.: extend for one round, and check if $P_r \cdot P_{n-r}^{best} \geq P_n^*$ (if $P_n > P_n^*$ update P_n^*)



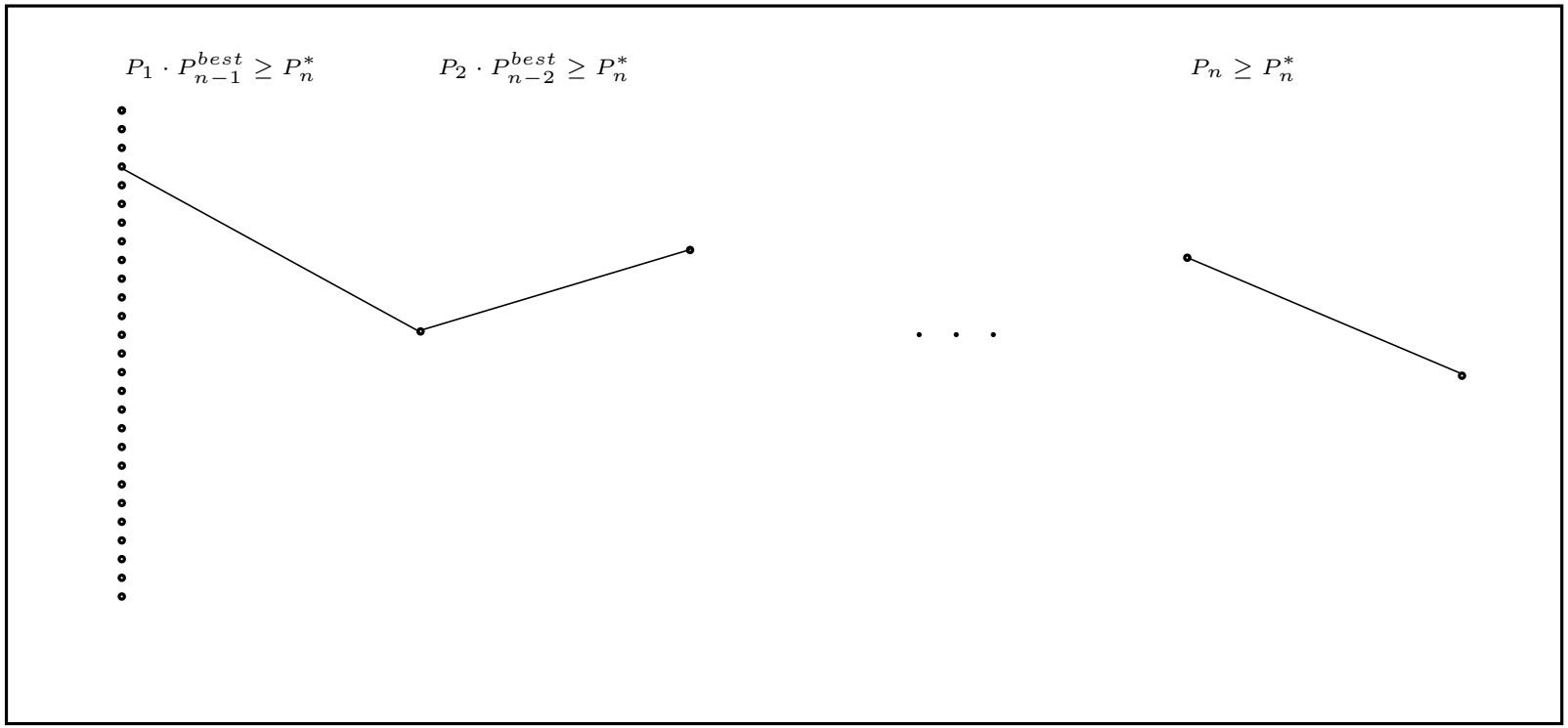
Matsui's Approach

For each $r-1$ round char.: extend for one round, and check if $P_r \cdot P_{n-r}^{best} \geq P_n^*$ (if $P_n > P_n^*$ update P_n^*)



Matsui's Approach

For each $r-1$ round char.: extend for one round, and check if $P_r \cdot P_{n-r}^{best} \geq P_n^*$ (if $P_n > P_n^*$ update P_n^*)



The Split Approach

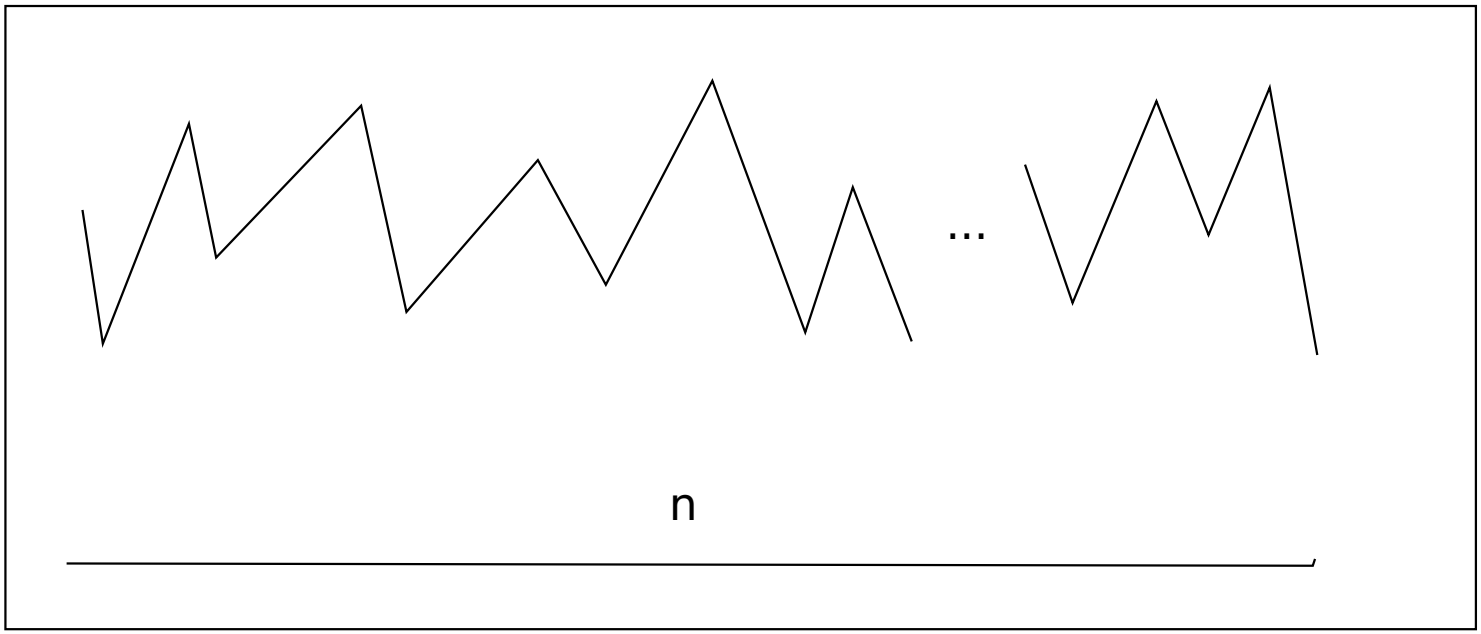
Divide and conquer + inside out approach

Fact: *If exists char. on n rounds with P_n, then exists sub char. on n/k consecutive rounds with $\geq \sqrt[k]{P_n}$*

The split can be combined with Matsui's approach

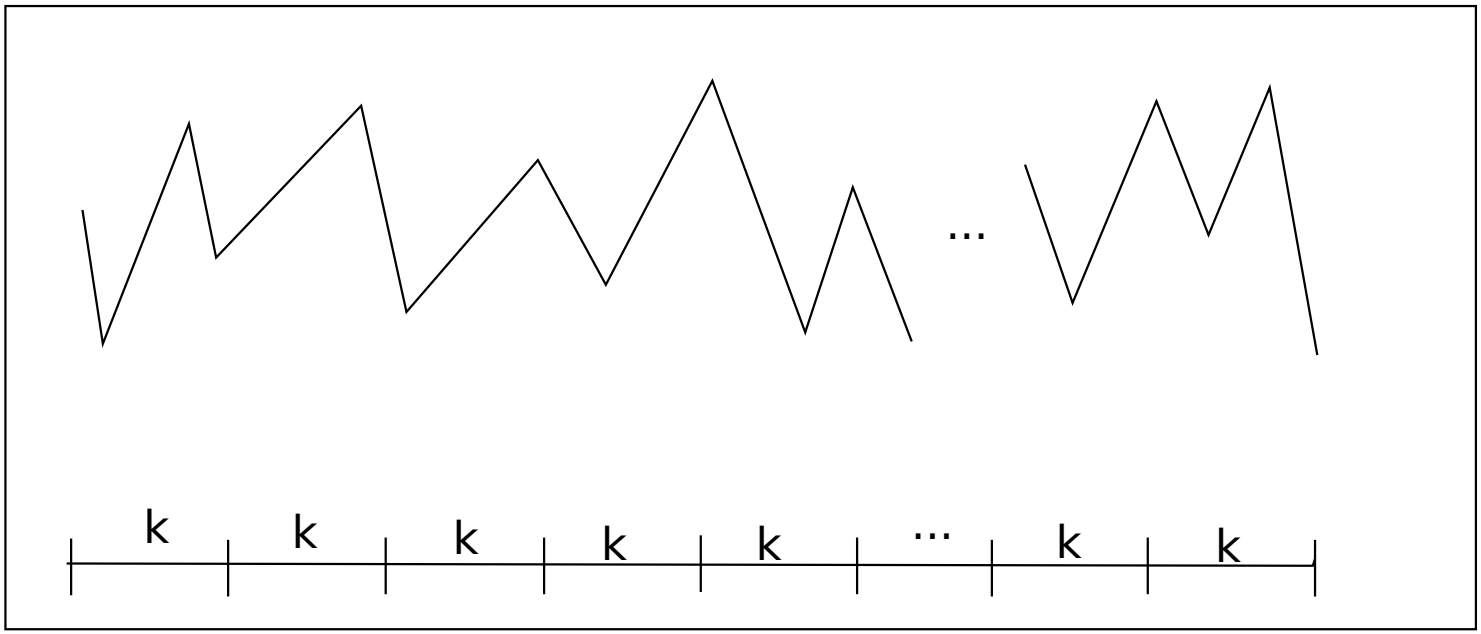
The Split Approach

Characteristic on n rounds with P_n



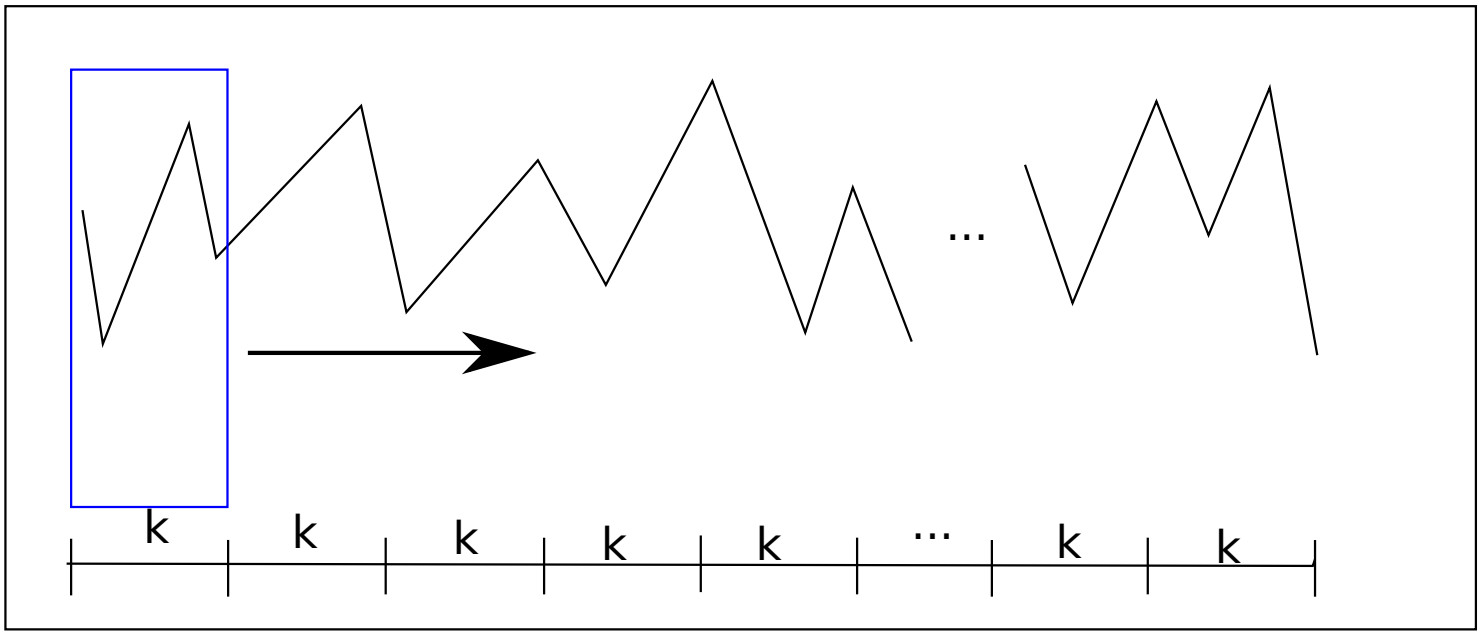
The Split Approach

Divide n rounds into $\frac{n}{k}$ k rounds



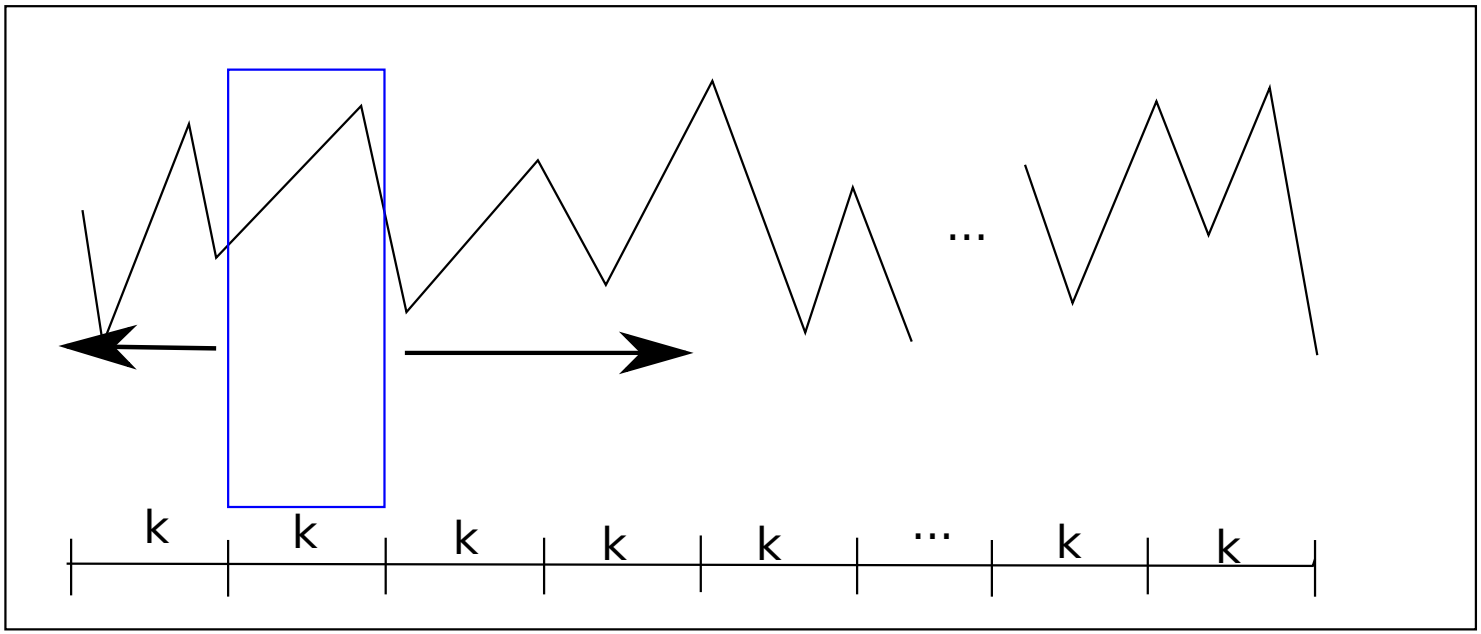
The Split Approach

Assume the char. on first k rounds is $\geq \sqrt[k]{P_n}$. Extend to n



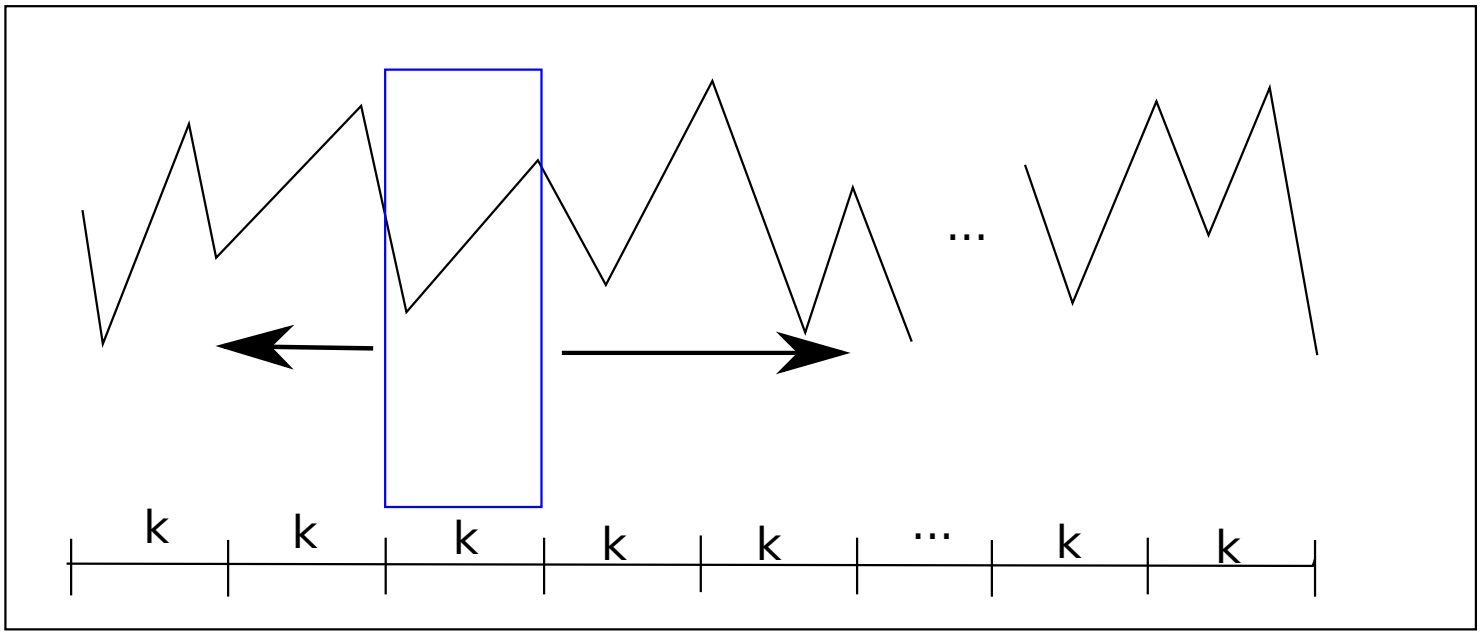
The Split Approach

Assume the char. on second k rounds is $\geq \sqrt[k]{P_n}$. Extend to n



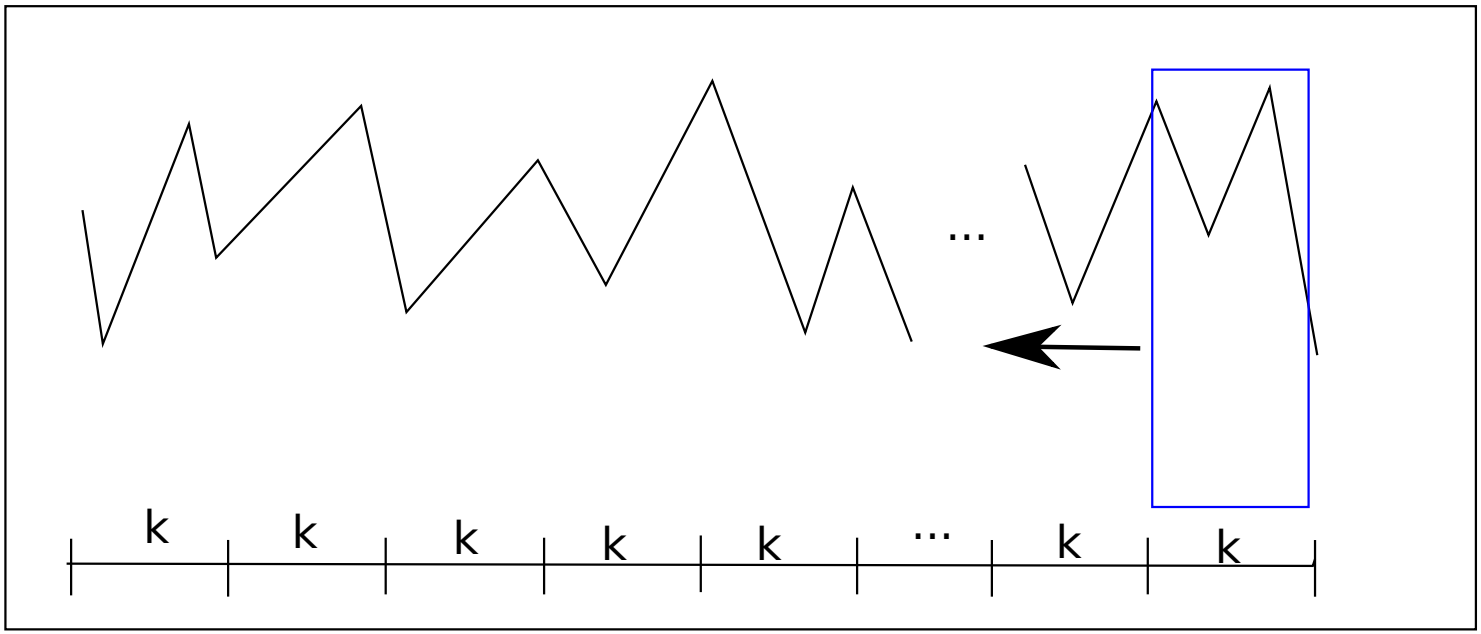
The Split Approach

Assume the char. on third k rounds is $\geq \sqrt[k]{P_n}$. Extend to n



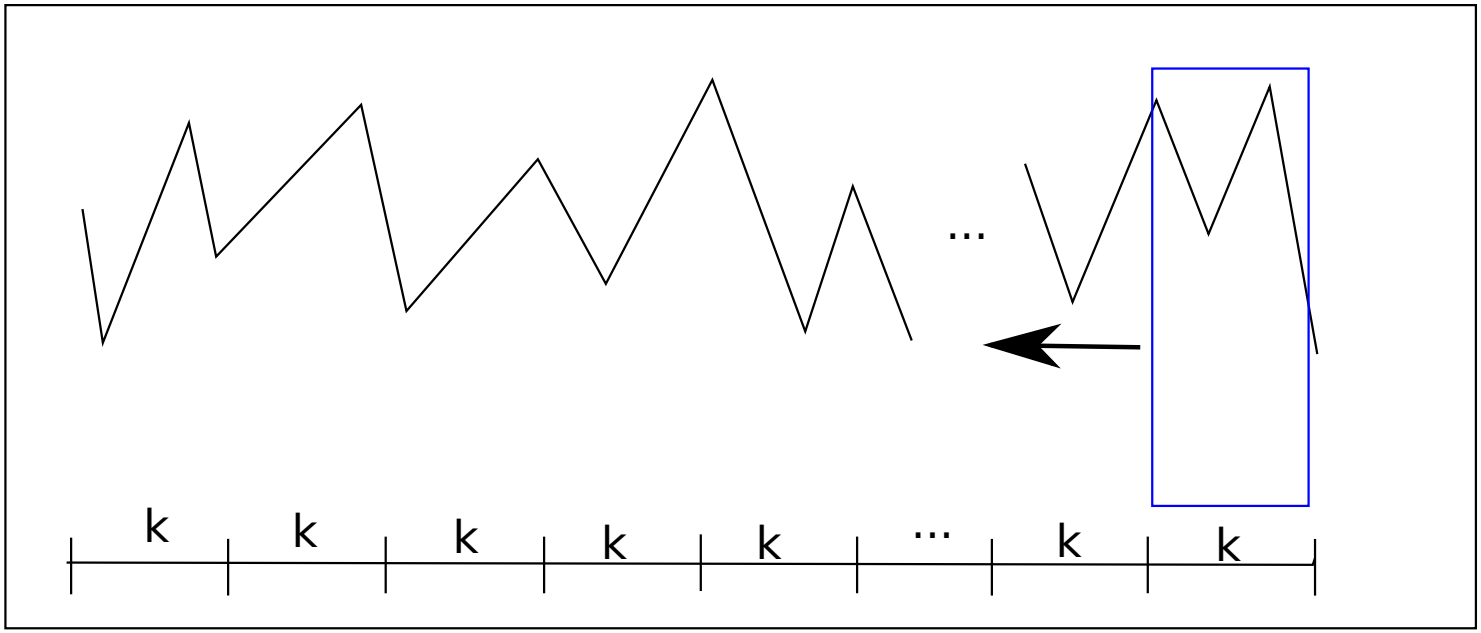
The Split Approach

Assume the char. on last k rounds is $\geq \sqrt[k]{P_n}$. Extend to n



The Split Approach

The best of all iterations, is the the best on n rounds



Starting Difference

- There are 2^{120} starting differences
- Matsui's and the split provide bounds on probabilities of the first k rounds

Instead of brute forcing input diff., brute force the input-output diffs. for the S-boxes

Each input-output diff. adds to the total probability of a round

Starting Difference

Single key (Matsui's approach in DES)

If input-output diffs. to S-boxes in 2 rounds are fixed, then input and output diffs. are fixed.

Starting Difference

Single key (Matsui's approach in DES)

If input-output diffs. to S-boxes in 2 rounds are fixed, then input and output diffs. are fixed.

Related key

If input-output diffs. to S-boxes in 3 rounds are fixed, then input and output diffs. are fixed **as well as 2^8 possible values of diff. in the key**.

Algorithm

1. Fix input-output diffs. to S-boxes in 3 consecutive rounds. Matsui's/split approach provide bounds on probability => no need to try all possible diffs.
2. Obtain the input difference and the output difference.
3. If Matsui's approach then extend this 3-round char. forward to n rounds; if split extend backwards and forwards.

DES

rounds	Single-key	Related-key	Method used
4	$2^{-9.6}$	$2^{-4.61}$	RK Matsui'
5	$2^{-13.21}$	$2^{-7.83}$	RK Matsui'
6	$2^{-19.94}$	$2^{-12.92}$	RK Matsui'
7	$2^{-23.60}$	$2^{-20.38}$	Split
8	$2^{-30.48}$	$2^{-29.75} \leq \overline{P_8} < 2^{-22}$	Limited Matsui'
9	$2^{-31.48}$	$2^{-31.48}$	Split + Matsui'
10	$2^{-38.35}$	$\leq \overline{P_9}$	
11	$2^{-39.35}$	$2^{-39.35}$ if $\overline{P_8} = 2^{-29.75}$	RK Matsui'
12	$2^{-46.22}$	$2^{-46.22}$	Split + Matsui'
13	$2^{-47.22}$	$2^{-47.22}$	Split + Matsui'
14	$2^{-54.09}$	$\leq \overline{P_{13}}$	
15	$2^{-55.09}$	$2^{-55.09}$	RK Matsui'
16	$2^{-61.97}$	$\leq \overline{P_{15}}$	

DESL

Round	Probability
4	$2^{-4.67}$
5	$2^{-7.24}$
6	$2^{-12.09}$
7	$2^{-19.95}$
8	$\leq \overline{P_7}$
9	$< 2^{-30}$
10	$< 2^{-31}$
11	$\leq \overline{P_{10}}$
12	$< 2^{-40}$
13	$< 2^{-41}$
14	$\leq \overline{P_{13}}$
15	$< 2^{-50}$
16	$< 2^{-51}$

s2DES

rounds	Single-key	Related-key
4	$2^{-6.8}$	$2^{-5.19}$
5	$2^{-9.22}$	$2^{-8.0}$
6	$2^{-14.35}$	$2^{-12.61}$
7	$2^{-17.03}$	$2^{-17.03}$
8	$2^{-21.96}$	$2^{-21.96}$
9	$2^{-22.71}$	$2^{-22.71}$
10	$2^{-27.35}$	$2^{-27.35}$
11	$2^{-28.39}$	$2^{-28.39}$
12	$2^{-34.07}$	$2^{-34.07}$
13	$2^{-34.07}$	$2^{-34.07}$
14	$2^{-39.75}$	$2^{-39.75}$
15	$2^{-39.75}$	$2^{-39.75}$
16	$2^{-45.42}$	$2^{-45.42}$

Conclusions

- On higher rounds no better RK char. in DES
- Key schedule has no notable weakness
- Algorithms can be used for finding RK char. with high prob. ($\geq 2^{-20}$) in any bit-oriented cipher with linear key schedule