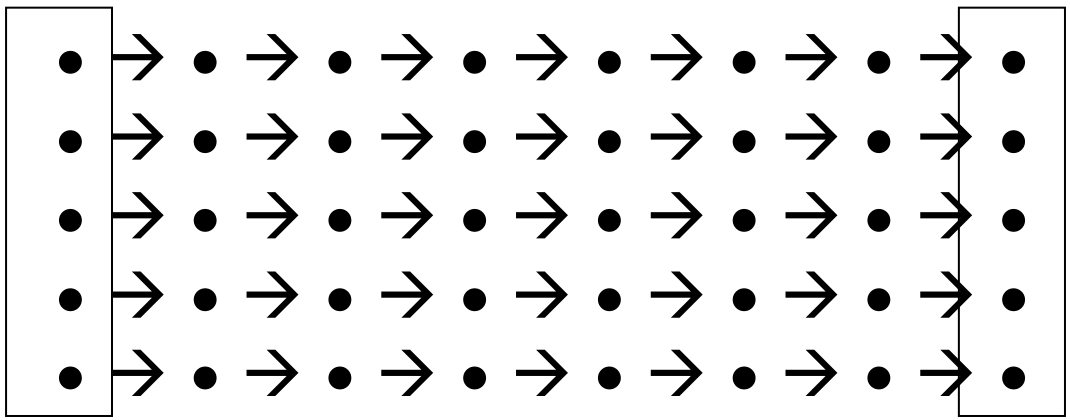
Time Memory Tradeoff Attacks on Streamciphers

– Variations –

Jin Hong and Palash Sarkar

Time Memory Tradeoffs on Streamciphers

- Biryukov & Shamir (Asiacrypt 2000)
- f: state → key stream of state size

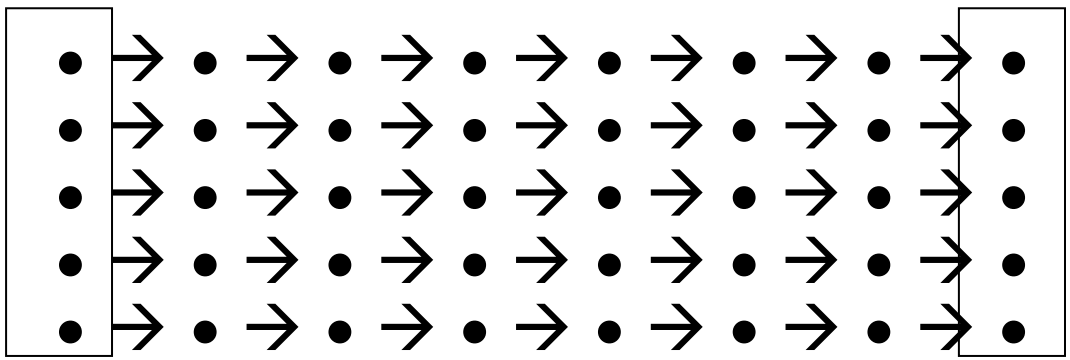


- random start pts
- (start pt, end pt) pairs are stored in a table.

- $T\ M^2\ D^2 = N^2$ and $P = N/D$
- N: search sp size, P: pre-comp time

State vs key

- f: key → key stream of key size



- If f is bijective, a key of appropriate property will be found. This may not be what we want.
- But the situation is different if you know where your key stream started.

State vs key+IV

- Suppose we are given a key stream that we know to be at the beginning

  (IP packets, disk encryption)
- Using the first block of key stream, we may apply the previous argument with

  f: key+IV → key stream of same length
- Always succeeds if IV is XOR'ed into key
- Reduction in pre-comp time possible, if more than one beginning stream is given

Short IVs

- Let us write K for key space size.
- Suppose IV size is 1/3 of key size and we have one block of data, so that

$$N = K^{4/3} \quad \text{and} \quad D = 1$$

- Then $T = M = K^{8/9}$ satisfies

$$T\, M^2\, D^2 = N^2.$$

But, pre-comp time $P = N/D = K^{4/3}$ is greater than K.

- With more data, such (theoretic) attack is possible if IV size is less than key size.
- In particular, this is applicable to SNOW.

Conclusion

- If you believe pre-comp time larger than key exhaustive search time may be allowed in an attack:

- Claims to TMTO resistance should mention key+IV space size, not internal state size.
- IV should be at least the key size.
  (State should be twice the size of key.)
- When combining key and IV into a state, take care so as not to decrease its entropy.
- Do not use IV in a predictable way, or use only a subset. This is equal to using small IV.