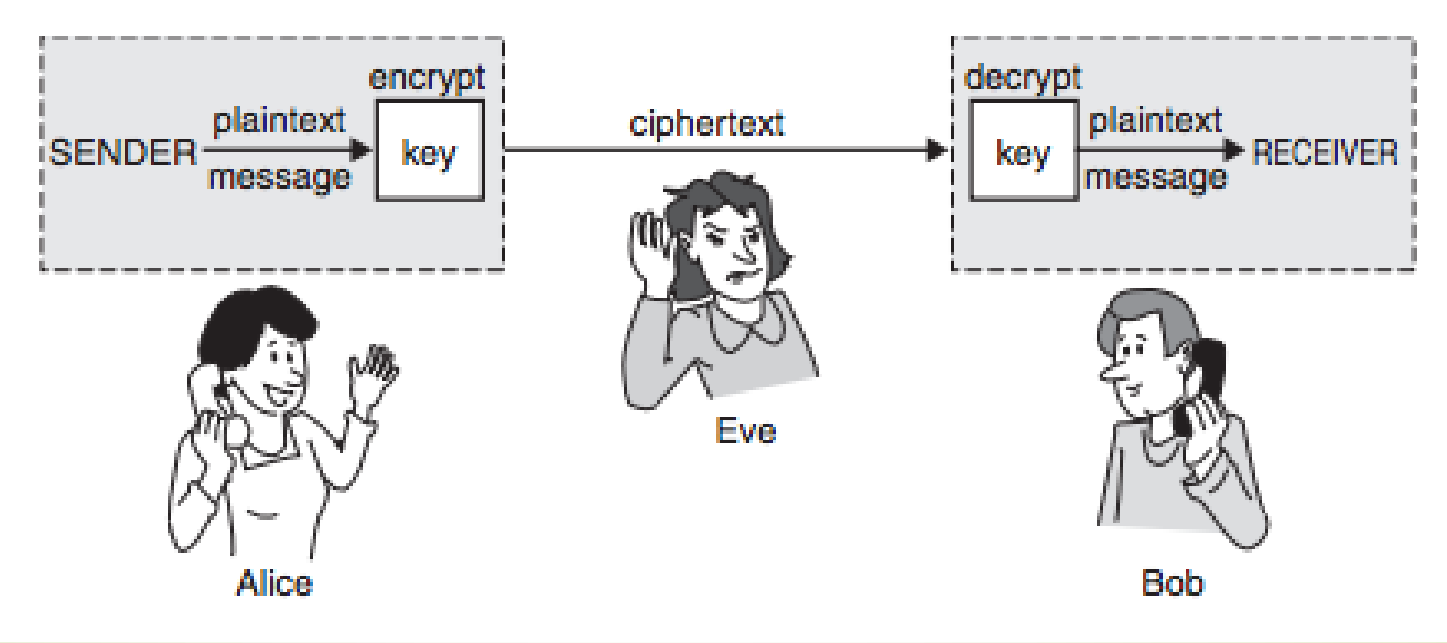
Experimental Evaluation of Time-Memory Trade-Off Attack

Aleksandra Arsić and Aleksandra Zdravković

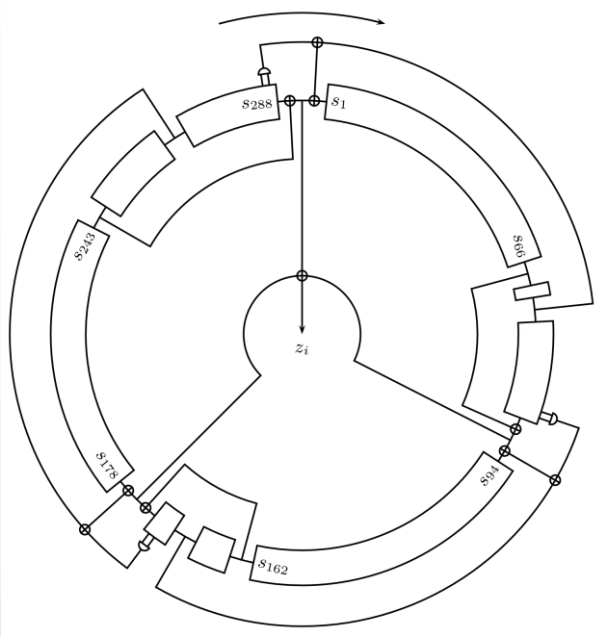
Mathematical Institute SASA, Belgrade, Serbia

Encription scenario



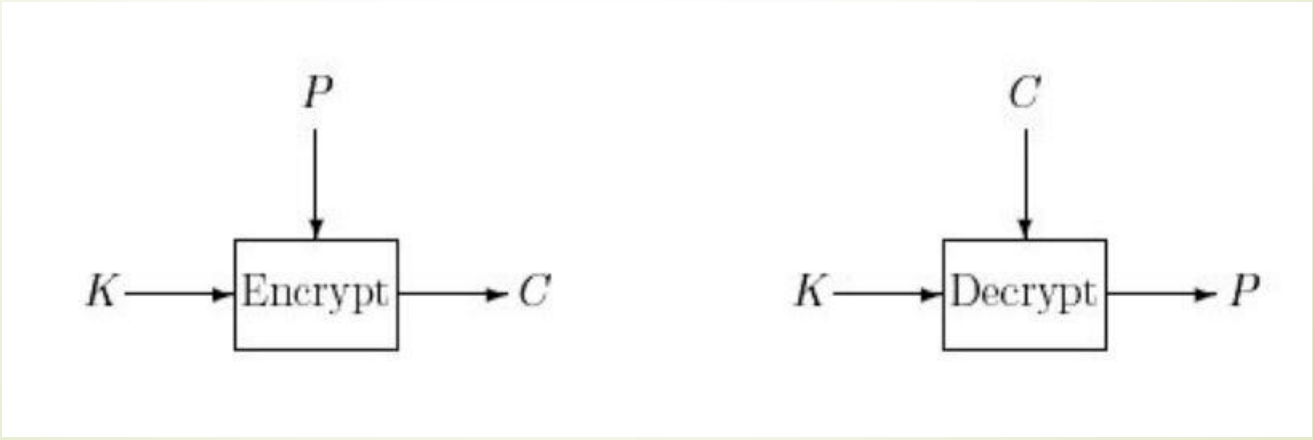
Trivium chiper

- Stream cipher
- Generate keystream
- Uses 80-bit secret key and an 80-bit initial vector (IV)
- Two phases



Nottation

- cipher C = E(P, K)
- where P is plaintext block of size n
- C is ciphertext block of size n
- K is key of size k



Inversion of one-way function?

- f(x)=y, if y is known how to find x?
- There are the following two straightforward approaches for recovering the argument given the corresponding image generated by one-way function where the inversion is a hard problem:
  - (i) exhaustive search over all possible arguments;
  - (ii) employing a code-book with all possible argument-image pairs.

TMTO Attack (Hellman, 1981)

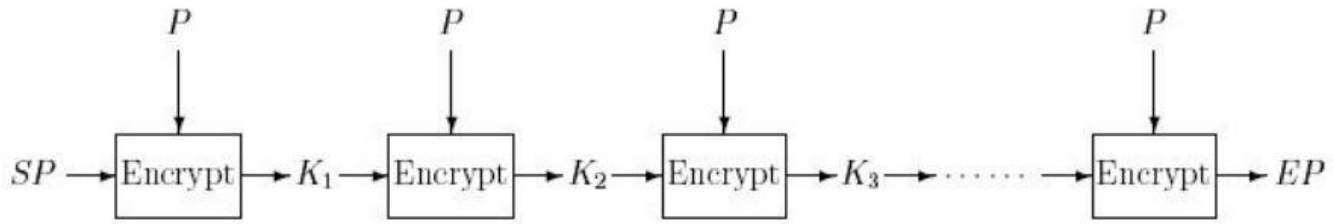
- Compromises the above two extreme approaches

- *Precomputation phase*: For a given plaintext ***P***:
  - *precompute* (ideally all) pairs key-ciphertext {K_i, C_i};
  - *store* only ***some*** of them in the table.

- *Online phase*:
  - perform *some* computations;
  - lookup the table and find the key ***K***.
    - time $T = N^{2/3}$
    - memory $M = N^{2/3}$

Precomputation phase

- Form a m × t matrix that tries to cover the whole search space which is composed of all the possible comibations of key vector as follows:
  - Step 1. Randomly generate m startpoints of the chains, each point is represented like vector of N bits length.
  - Step 2. Make it the next point in the chain which is the output from Trivium function and update the s register with this point.
  - Step 3. Iterate Step (2) t times on each startpoint respectively.
  - Step 4. Store the pairs of startpoints and endpoints (SPj ,EPj), where j = 1, ...,m in the matrix.



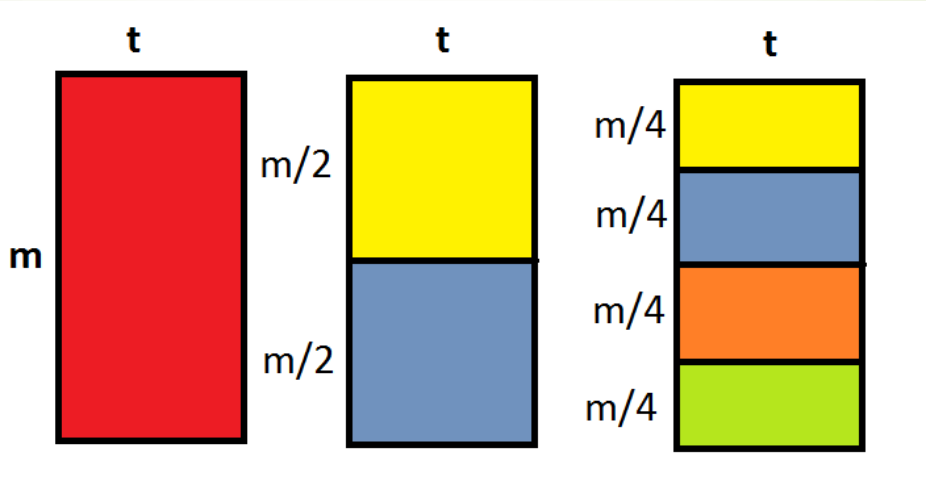
TMTO Issues

- Merging chains
- Cycles in one chain
- Pre-computation is lots of work
- Success is not assured
- There is some repetition rate

- Goal: Try to minimize reppetition rate in precomputing phase, as much as possible.

Rainbow tables

- Several sub-tables
- For each tables generate random vector
- Translating state for coresponding vector
- XOR operation - translation
- Dimension of search space is the same like in case of one table



Experiments and results

Number of tables	Repetiton rate [%]*
1	(57.14, 64.43)
2	(54.71, 61.57)
4	(47.14, 58.90)
8	(35.19, 41.62)

* percent of size of search space

Conclusion:
The larger the table is, the higher is the probability that a new chain has an intersection with previous chains.

Thank you for attention!

aleksandra@mi.sanu.ac.rs

alekzdravkovic@mi.sanu.ac.rs