WITHIN A FRIEND ZONE: HOW FAR CAN WE PROCEED WITH DATA ENCRYPTION NOT GETTING OUT

VASILY SHISHKIN

I. LAVRIKOV

- TC 26 -

CTCrypt 2018

LET’S MOVE TO

INTRODUCTION

PROBLEMS AND SOLUTIONS

CONCLUSIONS

BC AND EVOLUTION OF TASKS

SIMPLE EXAMPLE[1]

- SIZE OF THE INTERNET DOUBLES EVERY 2 YEARS
- FOR THE BEGINNING OF 2016: APPROX. 7.7 ZETTABYTE
- IN 2020: APPROX. 40 ZETTABYTE
- IN 2020: APPROX. 50 BILLION DEVICES WILL BE CONNECTED TO THE INTERNET

OLD NEW TASKS

- CONFIDENTIALITY,
- INTEGRITY,
- AUTHENTICATION,
- DIFFERENT COMBINATIONS OF TASKS.

SIMPLE SOLUTION: FROM BC TO BC MODES OF OPERATIONS

---

[1] ACCORDING TO http://live-counter.com

BC AND MODES OF OPERATIONS

FROM ATTACKS ON BC TO ATTACKS ON MODES

FROM ATTACKS ON PRIMITIVES TO ATTACKS ON PROTOCOLS

RANGE OF TASKS $\mapsto$

RANGE OF ADVERSARY'S CAPABILITIES $\mapsto$

DIFFERENT ADVERSARIAL MODELS

EXAMPLE OF MODELS

- SIMPLE ANALYSIS,
- DISTINGUISHING ATTACKS,
- CROSS-MODES ATTACKS,
- FAULT ANALYSIS,
- MANY MORE OTHERS, SOME UNDISCOVERED AT THE MOMENT

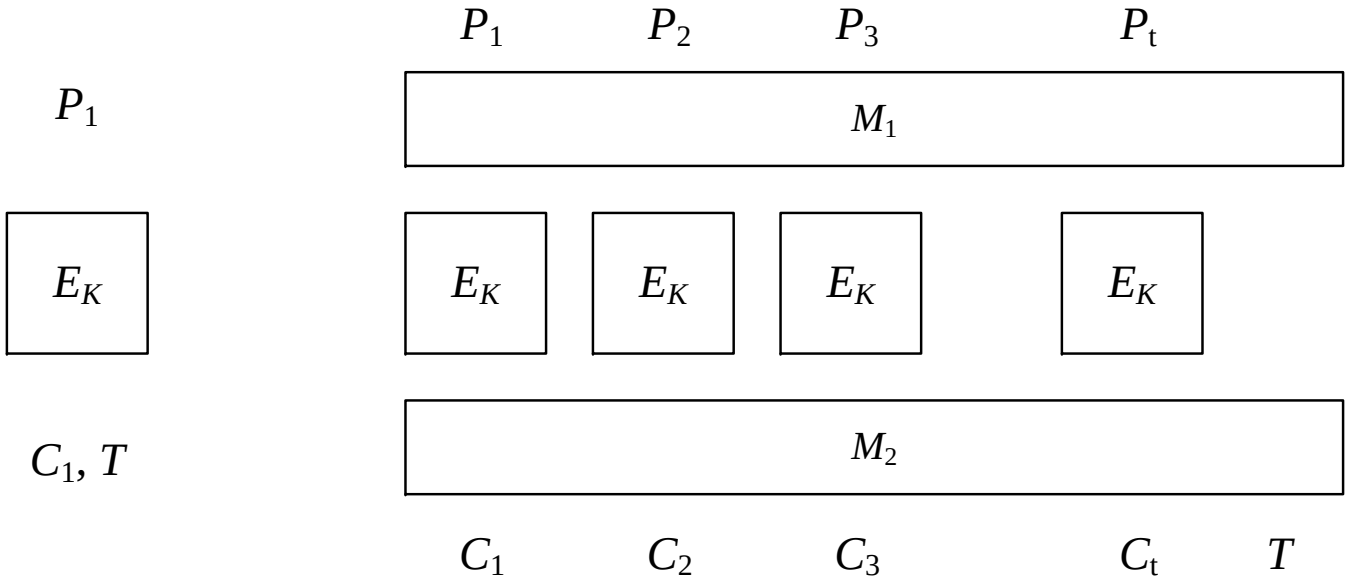
BC IN MODES AND EVOLUTION OF CRYPTANALYSIS

SIMPLE EXAMPLE

SWEET32: THEORETICAL ATTACK ON BC TO PRACTICAL ATTACK ON REAL-LIFE INFORMATIONAL SYSTEMS

CLEAR NEED:

- USE CASES FOR BC AND MODES OF OPERATIONS,
- LIMITATIONS ON USE OF BC AND MODES OF OPERATIONS,
- BASED ON USE CASES LIMITATIONS AND RESTRICTIONS FOR USE OF BC AND MODES OF OPERATIONS.



BC IN MODES VS. ADVERSARIES

TRIVIAL CONCLUSION

EACH CRYPTO MECHANISM COULD BE USED IN SUCH A WAY IT COULD NOT PROVIDE SUFFICIENT[2] LEVEL OF SECURITY

OPPOS.: EACH CRYPTO MECHANISMS COULD BE PROVIDED WITH LIMITATIONS IN A WAY IT WILL PROVIDE SUFFICIENT LEVEL OF SECURITY

[2] FOR SOME USE CASES

LET’S MOVE TO

INTRODUCTION

PROBLEMS AND SOLUTIONS

CONCLUSIONS

OBSERVATION NOTES

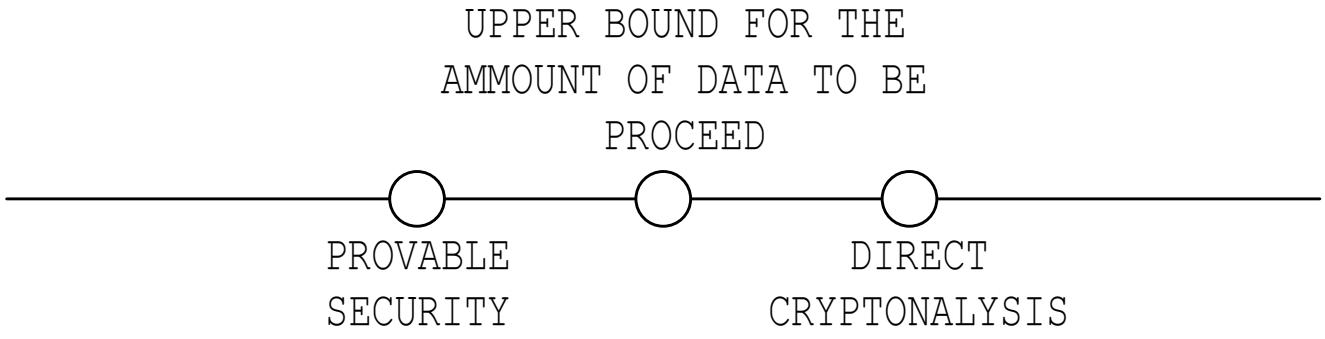
- BROAD STUDY OF MODES OF OPERATIONS,
- PROVABLE SECURITY APPROACH,
- DIRECT CRYPTANALYSIS APPROACH.

DIRECT CRYPTANALYSIS

THIS AMOUNT = ATTACK = UPPER VALUE FOR THE UPPER BOUND

PROVABLE SECURITY

MORE THEN THIS AMOUNT = ATTACK = LOWER VALUE FOR THE UPPER BOUND



DIRECT ANALYSIS

- $P_1, P_2, \ldots, P_u,\ P'_1, P'_2, \ldots, P'_v$ - PLAINTEXT BLOCKS,
- $C_1, C_2, \ldots, C_u,\ C'_1, C'_2, \ldots, C'_v$ - CORRESPONDING CIPHERTEXT BLOCKS.

DIRECT ANALYSIS

- $P_1, P_2, \ldots, P_u,\ P'_1, P'_2, \ldots, P'_v$ - PLAINTEXT BLOCKS,
- $C_1, C_2, \ldots, C_u,\ C'_1, C'_2, \ldots, C'_v$ - CORRESPONDING CIPHERTEXT BLOCKS.

TASK: OBTAIN ADDITIONAL INFORMATION ABOUT UNKNOWN PART OF THE PLAINTEXT WITH PROBABILITY NO LESS THEN π.

SOME OBSERVATIONS:

McGrew, D. Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes.

PROVABLE SECURITY

SOME USEFUL RESULTS:

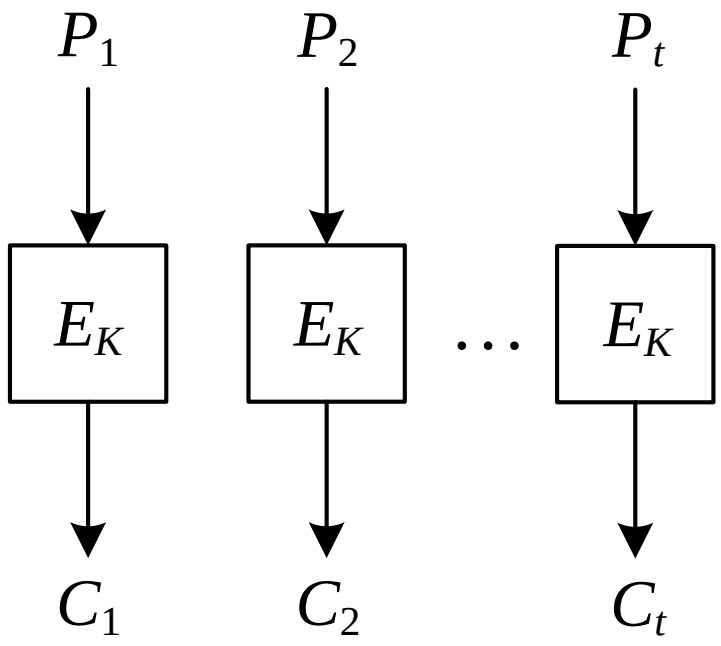

ROGAWAY, P. EVALUATION OF SOME BLOCKCIPHER MODES OF OPERATION.


BELLARE, M., DESAI, A., JOKIPII, E., AND ROGAWAY, P. A CONCRETE SECURITY TREATMENT OF SYMMETRIC ENCRYPTION.

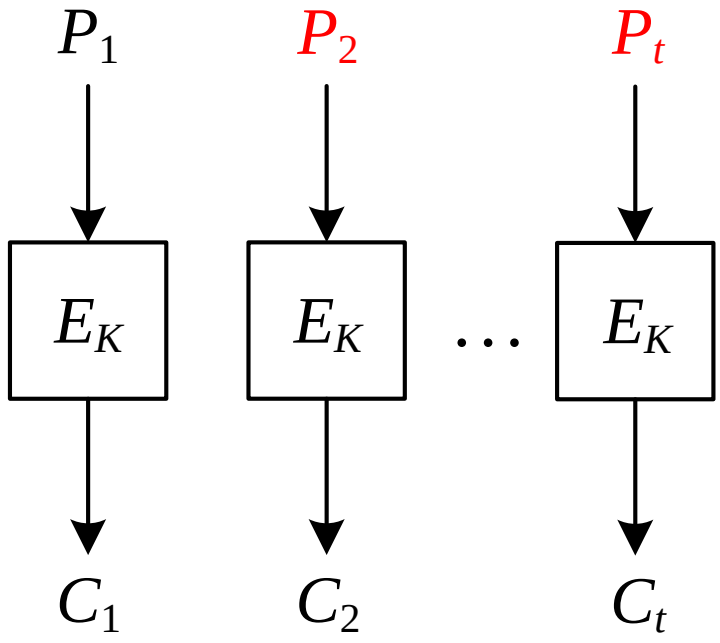

A. ALKASSAR, A. GERALDY, B. PFITZMANN, A.-R. SADEGHI. OPTIMIZED SELF-SYNCHRONIZING MODE OF OPERATION.

- LEFT-OR-RIGHT DISTINGUISHER,
- TIME OF WORK t,
- q QUERIES [OF THE TOTAL LENGTH μ] TO SOME ORACLE,
- BIRTHDAY PARADOX.

ECB



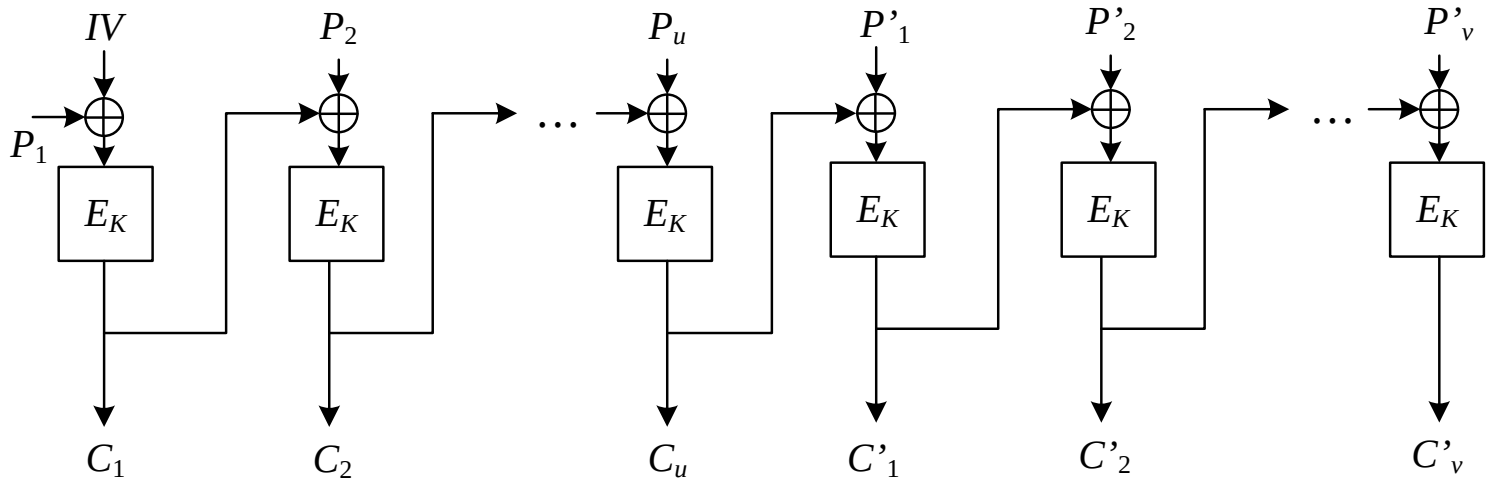
ECB



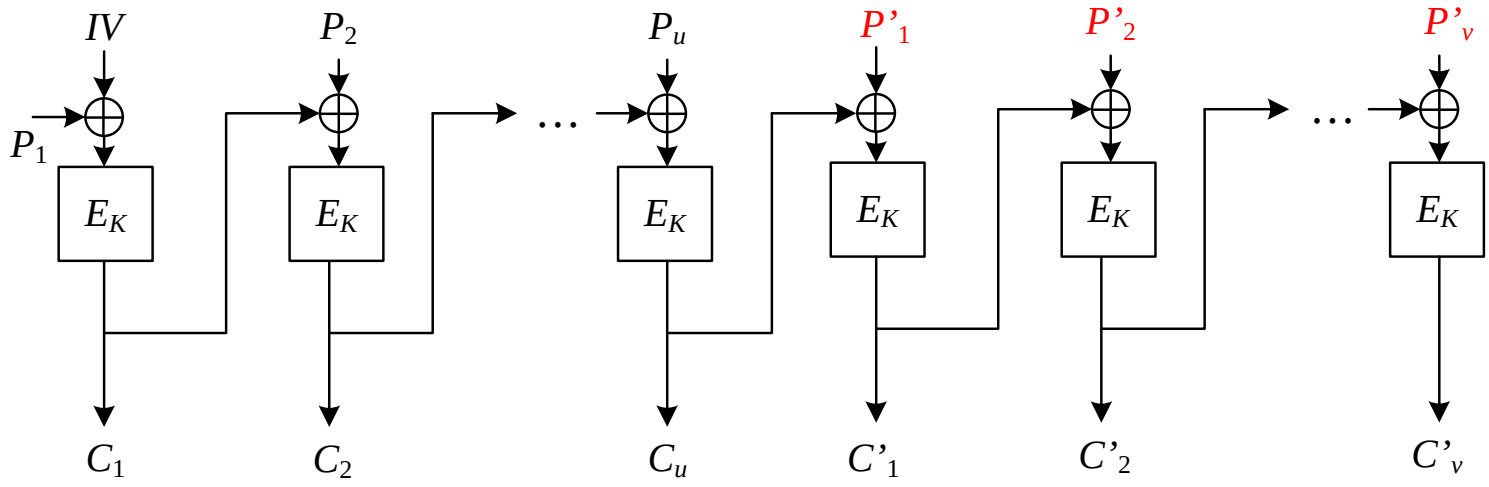
COMPLEXITY OF BRUTEFORCE ATTACK:

FROM 2^{tn} TO $2^n(2^n-1)\dots(2^n-t+1)$.

CBC



CBC



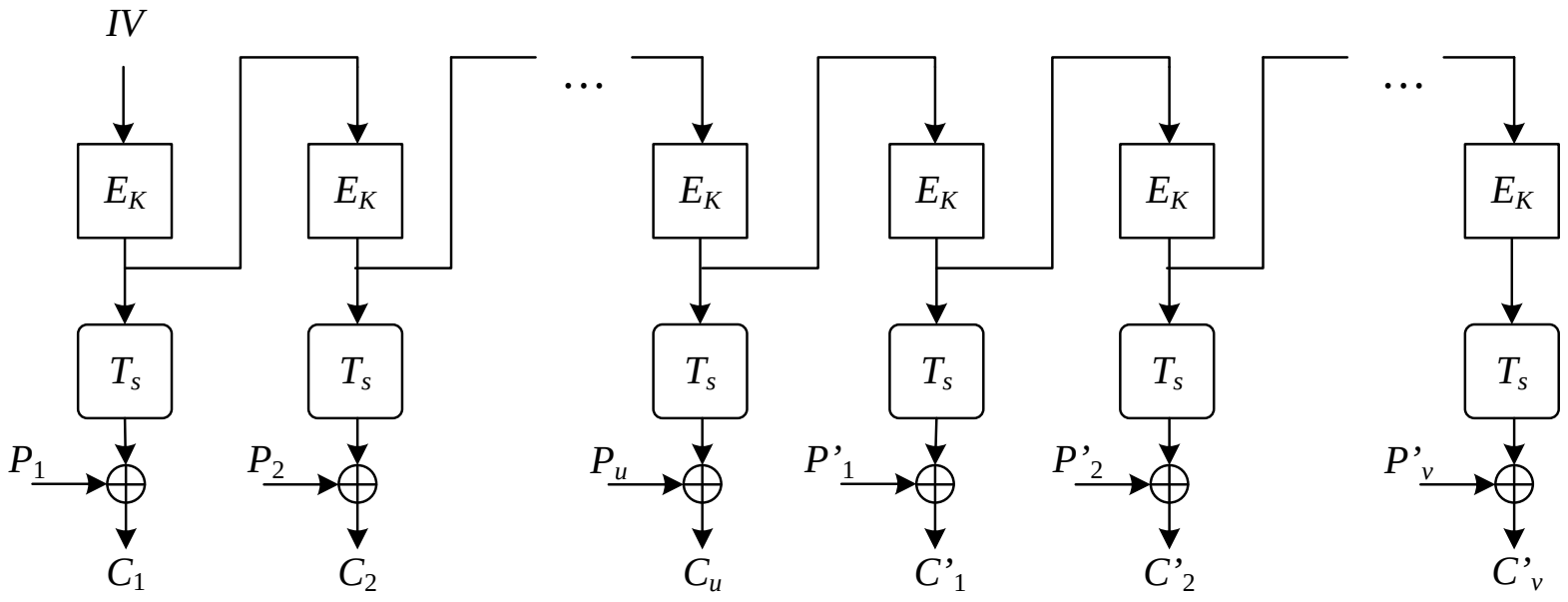
ASSUME $C_i = C'_j$. $P_i = D_K(C_i) \oplus C_{i-1}$, $P'_j = D_K(C'_j) \oplus C'_{j-1}$
THEN

$$P'_j = P_i \oplus C_{i-1} \oplus C'_{j-1}.$$

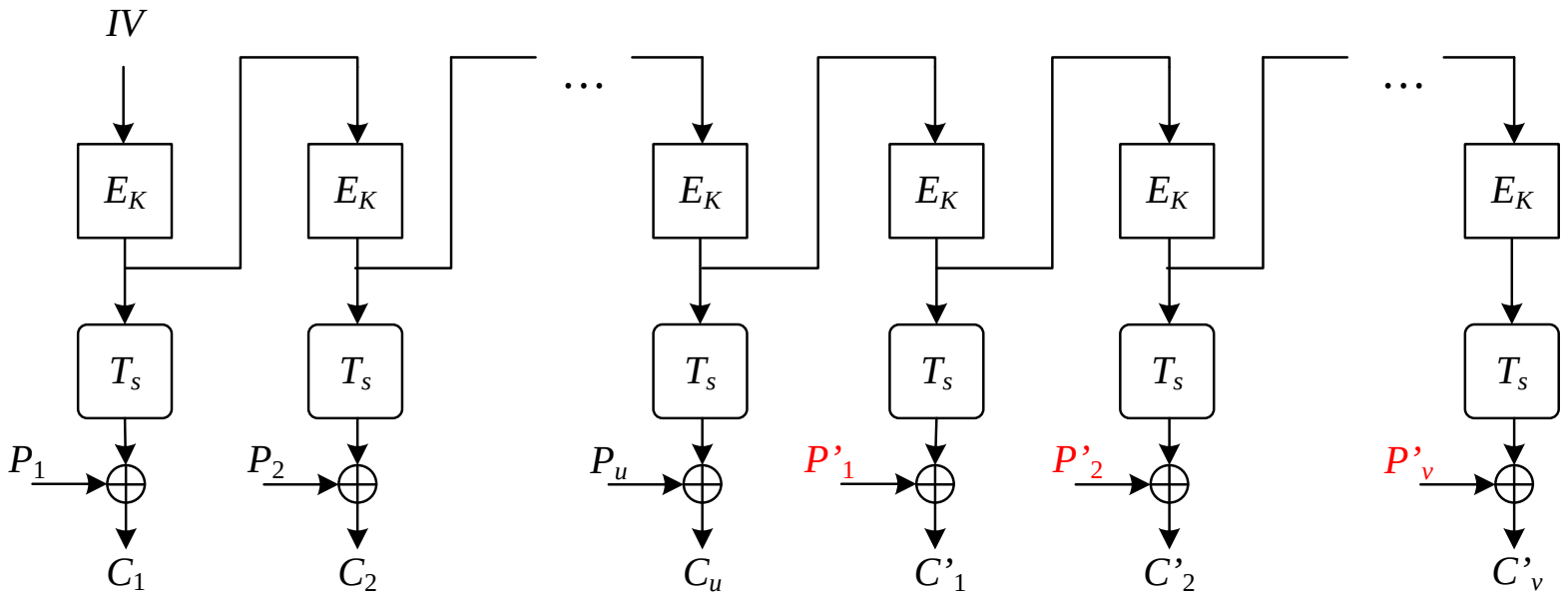
PROVABLE SECURITY PERSPECTIVE:

$$\Delta^{lr}_{\mathrm{CBC}_{\mathcal{F}}}(t, q, \mu) \leq \frac{1}{2^{n-1}} \cdot q^2 + \frac{1}{2^n} \cdot q.$$

OFB



OFB



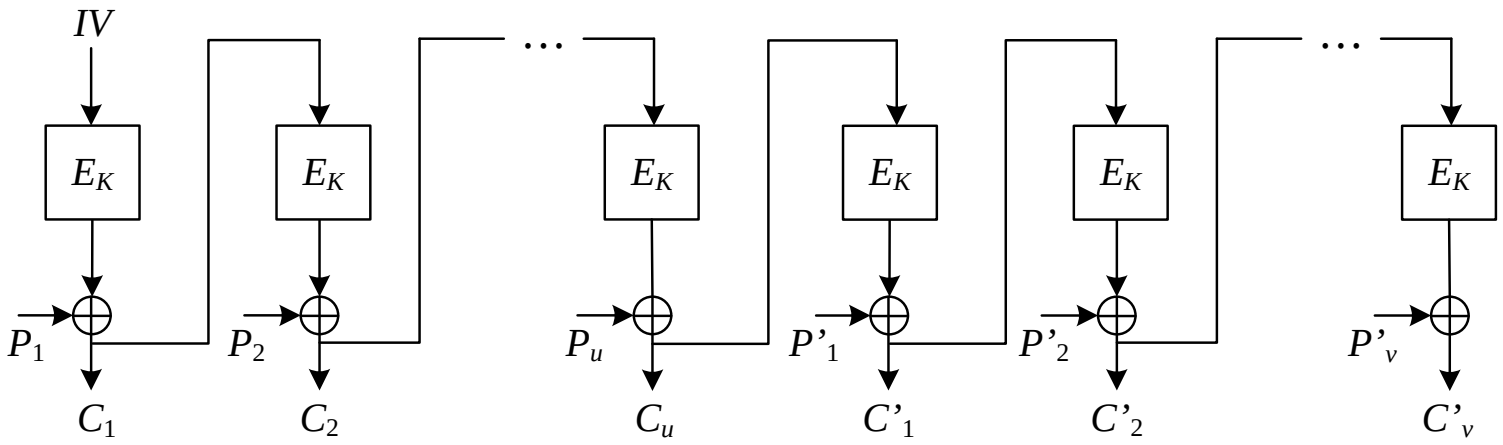
$P_i = E_K^i(a) \oplus C_i,\ \ P'_j = E_K^{j+u}(a) \oplus C'_j,$ THEN IT IS POSSIBLE THAT $E_K^i(a) = E_K^{j+u}(a)$ AND

$$P'_j = P_i \oplus C_i \oplus C'_j.$$

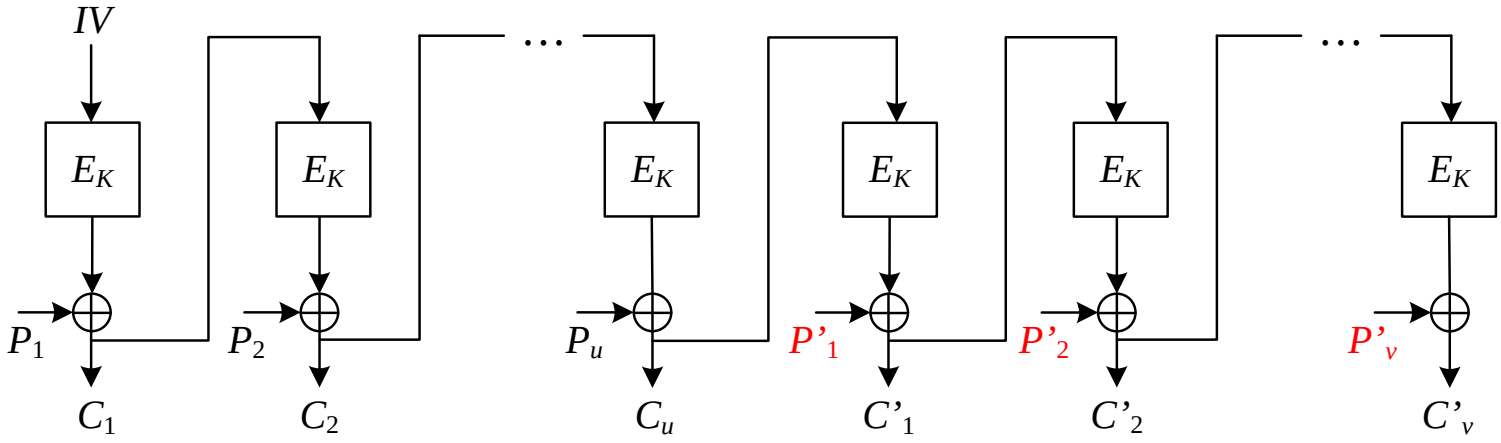
PROVABLE SECURITY PERSPECTIVE:

$$\Delta^{lr}_{\mathtt{OFB}_{\mathcal{F}}}(t, q, \mu) \leq \frac{1}{2^{n-1}} \cdot q^2 + \frac{1}{2^n} \cdot q.$$

CFB



CFB



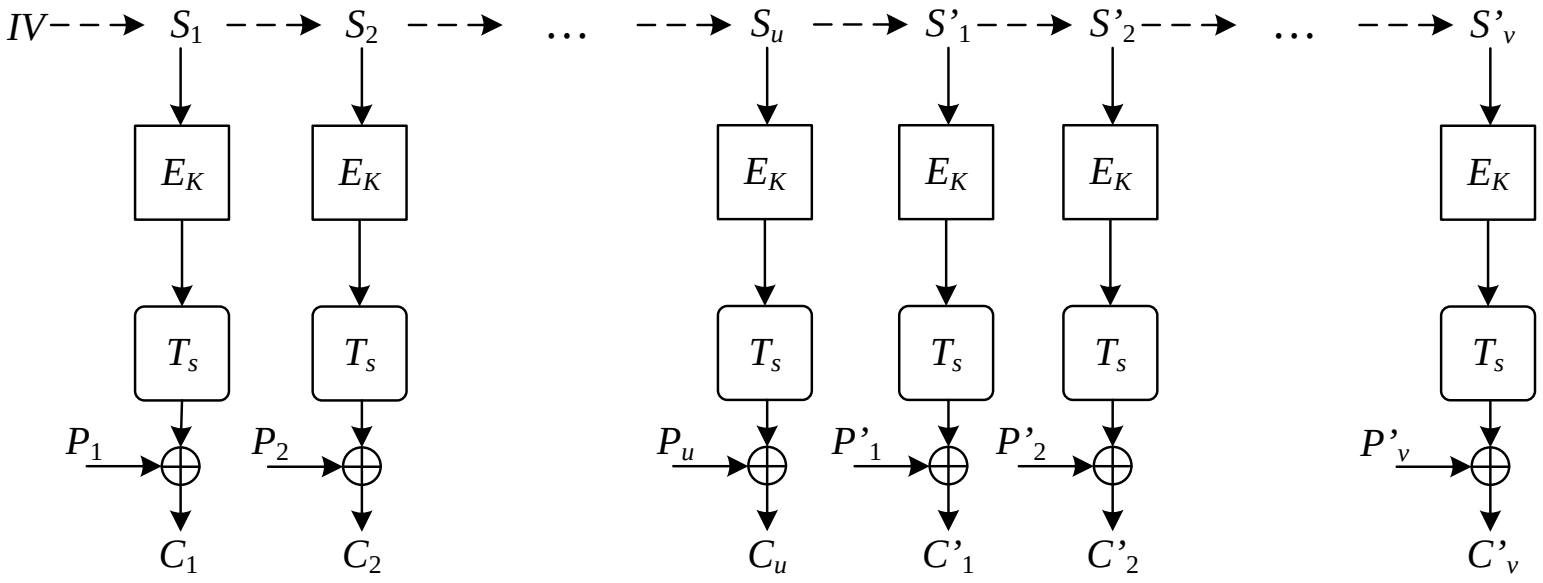
ASSUME C_{i-1} AND C'_{j-1}. $P_i = E_K(C_{i-1}) \oplus C_i$, $P'_j = E_K(C'_{j-1}) \oplus C'_j$ THEN

$$P'_j = P_i \oplus C_i \oplus C'_j,$$

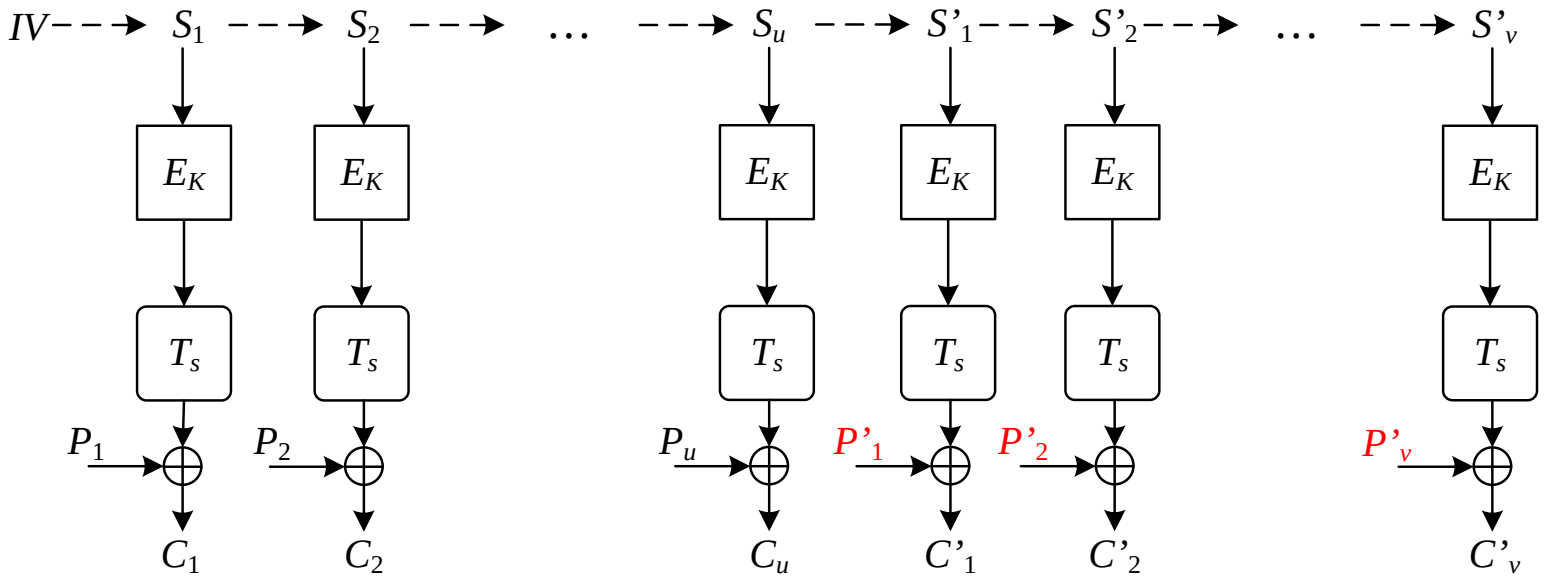
PROVABLE SECURITY PERSPECTIVE:

$$\Delta^{lr}_{\mathrm{CFB}_{\mathcal{F}}}(t, q, \mu) \leq \frac{q^2}{2^n} + \frac{q(q-1)}{2^{n+1}}.$$

CTR



CTR



All values $P_i \oplus C_i$ and $P' \oplus C'_j$ are pairwise distinct. Then unknown plaintext block can 't belong to the set $M = \{P_i \oplus C_i \oplus C'_j \mid i \in \overline{1,u},\ j \in \overline{1,v}\}$.

Provable security perspective:

$$\Delta^{lr}_{\mathrm{CTR\$}_{\mathcal{F}}}(t,q,\mu) \le \frac{q^2}{2^n} + \frac{\mu(q-1)}{n \cdot 2^n}, \quad \Delta^{lr}_{\mathrm{CTRC}_{\mathcal{F}}}(t,q,\mu) \le \frac{q^2}{2^n}.$$

SUMMARY

TABLE: UPPER BOUNDS FOR ACCEPTABLE AMOUNT OF DATA TO BE PROCESSED.

MODE OF OPERATION	MARGIN 1	MARGIN 2
ECB	1	-
CTR	$2^{\frac{n}{2}+1}\sqrt{\ln(\pi 2^n)}$	$\sqrt{\varepsilon}\cdot 2^{\frac{n}{2}}$
OFB	$2^{\frac{n}{2}}\sqrt{\ln\left(\frac{1}{1-\pi}\right)}$	$\sqrt{\varepsilon}\cdot 2^{\frac{n-1}{2}}$
CBC	$2^{\frac{n}{2}+1}\sqrt{\ln\left(\frac{1}{1-\pi}\right)}$	$\sqrt{\varepsilon}\cdot 2^{\frac{n-1}{2}}$
CFB	$2^{\frac{n}{2}+1}\sqrt{\ln\left(\frac{1}{1-\pi}\right)}$	$\sqrt{\varepsilon}\cdot \frac{1}{\sqrt{3}}2^{\frac{n+1}{2}}$

LET’S MOVE TO

INTRODUCTION

PROBLEMS AND SOLUTIONS

CONCLUSIONS

CONCLUSIONS

- DIFFERENT TASKS - DIFFERENT MODES,
- DIFFERENT TASKS - DIFFERENT ADVERSARIES,
- LIMITATION AND RESTRICTIONS COULD BE PROVIDED,
- MAXIMUM ACCEPTABLE AMOUNT OF BLOCKS TO BE PROCESSED WITHOUT KEY CHANGE ARE GIVEN,
- BOUNDARIES PRESENTED ARE VERY CLOSE, SO, AMOUNT OF DATA CAN BE SET.
- NOT UNIVERSAL RESTRICTIONS, JUST THE MOST WEAK ONES.

THANK YOU FOR YOUR ATTENTION!

ANY QUESTIONS?

FEEL FREE TO CONTACT US ON ANY MATTER AT

SHISHKIN_VA@TC26.RU
LAVRIKOV_IV@TC26.RU