New Multiple Encryption for Making Double Encryption Secure Against Meet-in-the-Middle & Related-Key Attacks

Takashi Nishide
Kyushu University

Shinichi Yoshinaga
Kyushu University

Rishi Bhattacharyya
India Statistical Institute

Mridul Nandi
India Statistical Institute

Bimal Roy
India Statistical Institute

Kouichi Sakurai
Kyushu University

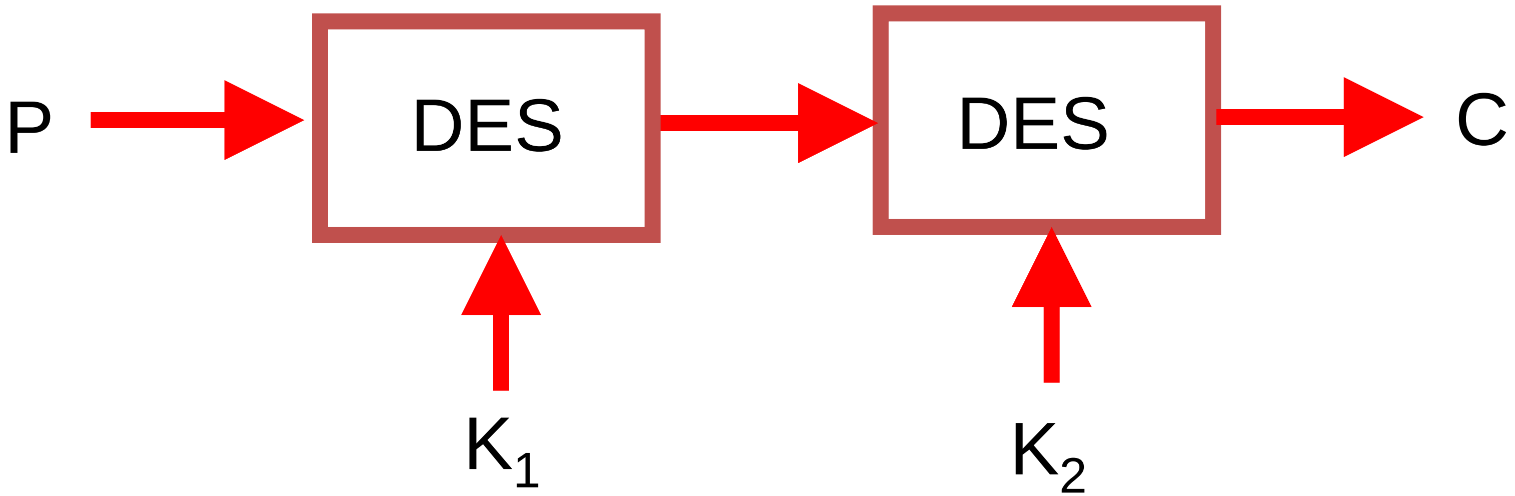
Supported by JAPAN SCIECE AND TECHNOLOGY AGENCY (JST), Strategic Japanese-Indian Cooperative Programme on Multidisciplinary Research Field, which combines Information and Communications Technology with Other Fields, entitled "Analysis of Cryptographic Algorithms and Evaluation on Enhancing Network Security Based on Mathematical Science."

Introduction

- Single DES is not secure anymore because of too short key size
- But exhaustive key search is considered to be an only practical attack on DES
- How about Linear Cryptanalysis by Matsui in 1993?
  - in theory, faster than exhaustive key search
  - but 2^{43} pairs of known plaintext & ciphertext are required and it seems very difficult to do in practice
- Is there an easy & efficient way to increase the key size of block cipher such as DES in general without modifying the original block cipher?
  - Would also be useful for AES when it becomes vulnerable to some attack in the future
- If possible, fast DES hardware implementation can be reused

Multiple Encryption

- Double DES

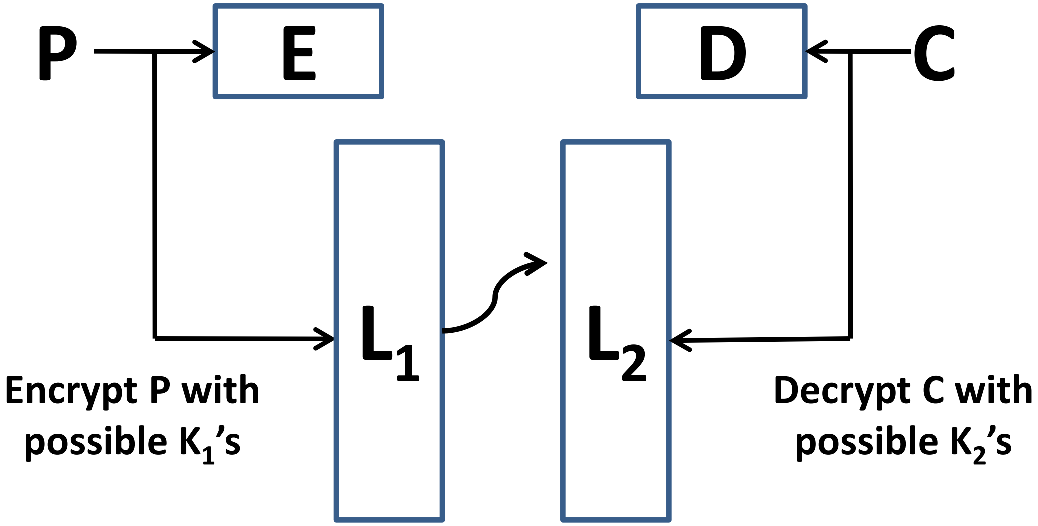


- How much security do we gain?
  - With n-bit K_1 and K_2, ideally, attack complexity should be $O(2^{2*n})$, but there is a meet-in-the-middle attack…

Meet-in-the-middle(MITM) Attack

Attack on double DES

1. Get valid pairs of (P,C),(P’,C’)
2. Compute lists L_1 & L_2 and sort L_1 & L_2
3. Find a match in L_1 & L_2 to determine K_1 ,K_2
4. Check validity of K_1 ,K_2 with (P’,C’)


P
E
D
C
L_1
L_2
Encrypt P with possible K_1’s
Decrypt C with possible K_2’s

$<K_1, E_{K_1}(P)>$ $<K_2, D_{K_2}(C)>$

$O(2^n)$ time complexity with $O(2^n)$ space where K_1,K_2 are n-bit

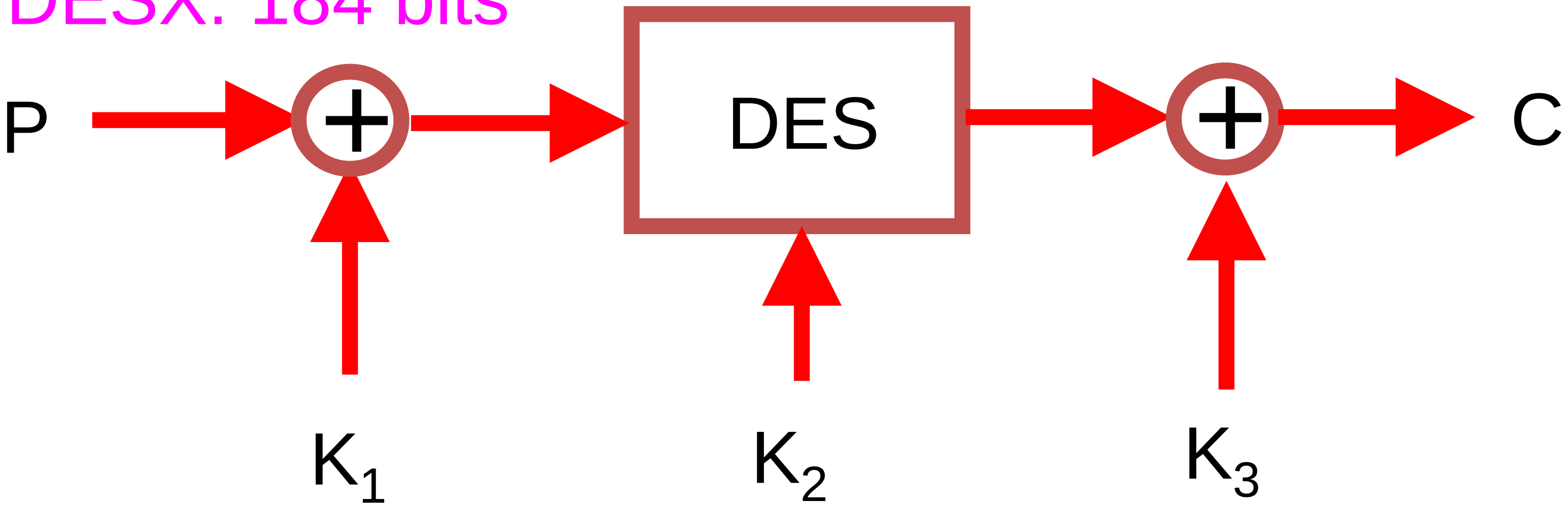
Countermeasure Against MITM Attack

- We should prevent an attacker from computing middle data
- There already exist several DES variants based on multiple encryption
  - DESX
  - Two-key Triple DES
  - DES-EXE
- Our new proposal: DES-XEEX

DESX

- Proposed by Rivest
  - used in the products of RSA Data Security, Inc.
  - Rogaway et al. gave soundness proof [Crypto’96]

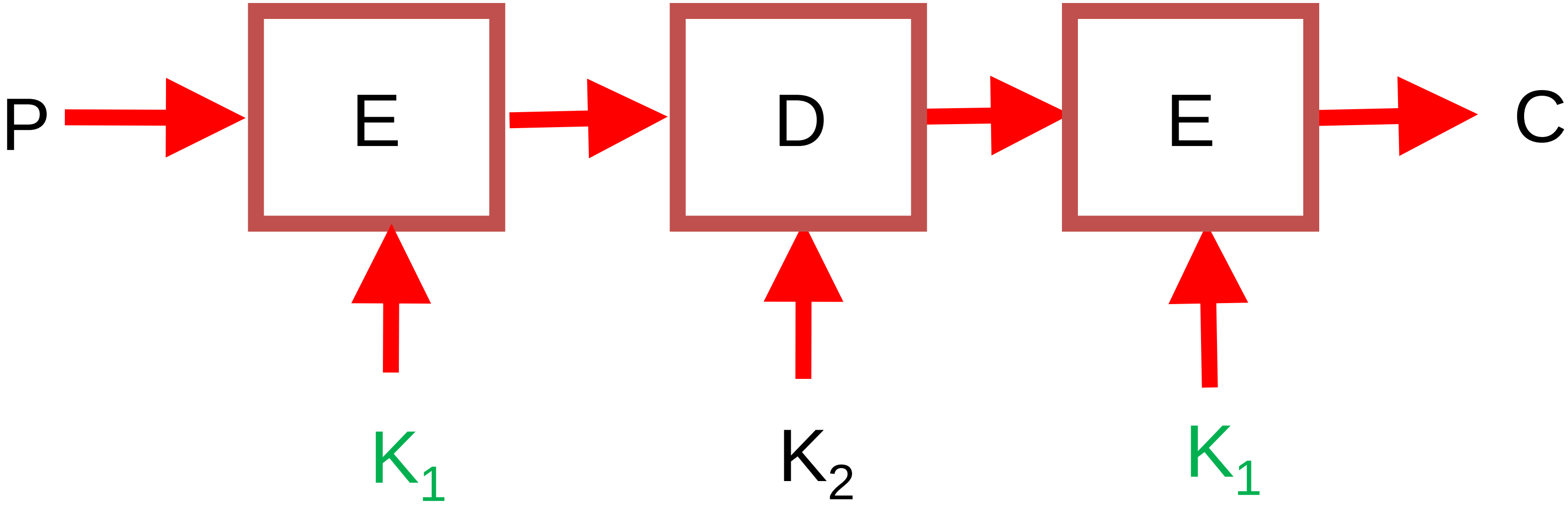
Key size in DESX: 184 bits



- However, another attack called related-key attack [Phan, Shamir’04] exists…

Two-key Triple DES

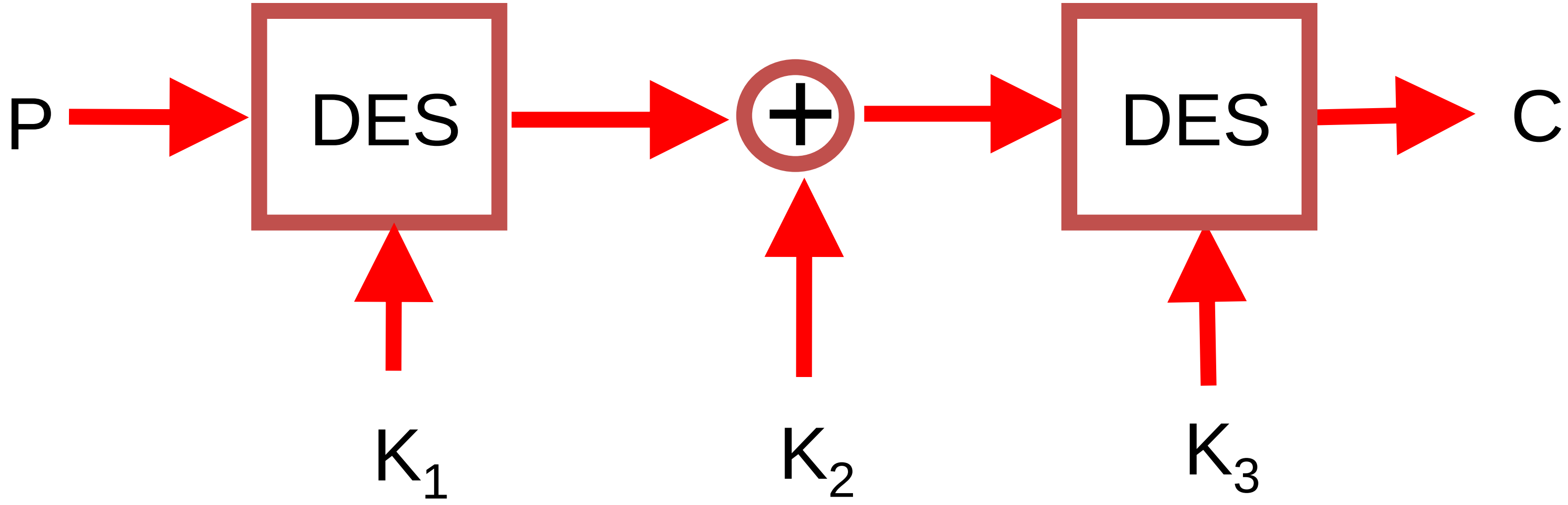
- Proposed by Tuchman in 1979



- There exists a variant of MITM attack faster than exhaustive key search
- Known-plaintext attack [Oorschot, et al ‘90]. So not optimal(only 80-bit(<112)security level).
- 3DES operations and slow performance

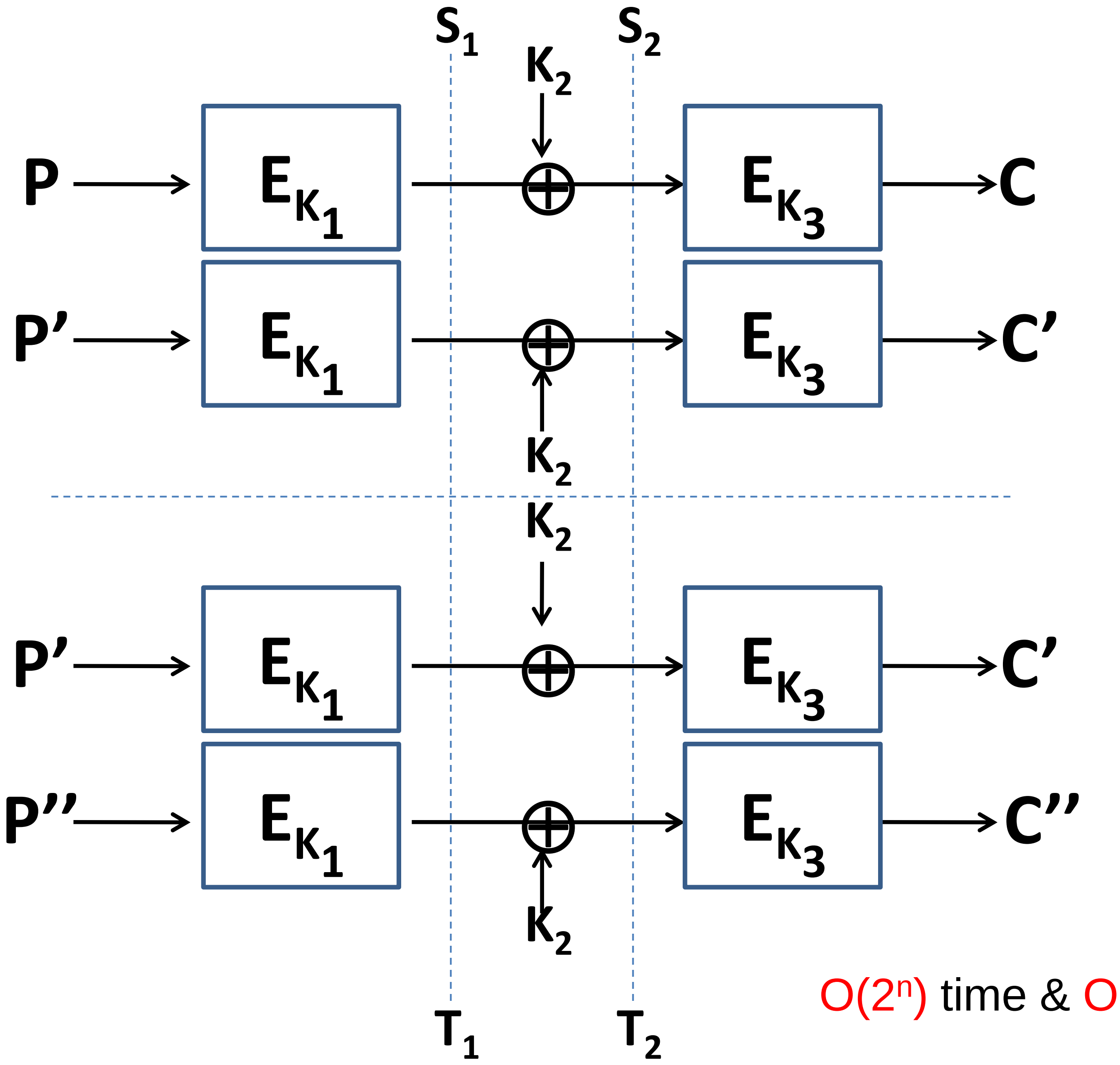
DES-EXE

- Proposed by Kaliski and Robshaw in 1996



- DES-EXE was designed s.t. MITM attack is not applicable
- However, elaborate MITM attack [Choi et al, ICCSA’05] was discovered…

MITM Attack on DES-EXE[Choi et al.]



$<K_1, S_1, T_1>$ where

$S_1 = E_{K_1}(P) \oplus E_{K_1}(P')$

$T_1 = E_{K_1}(P') \oplus E_{K_1}(P'')$

$<K_3, S_2, T_2>$ where

$S_2 = D_{K_3}(C) \oplus D_{K_3}(C')$

$T_2 = D_{K_3}(C') \oplus D_{K_3}(C'')$

Find

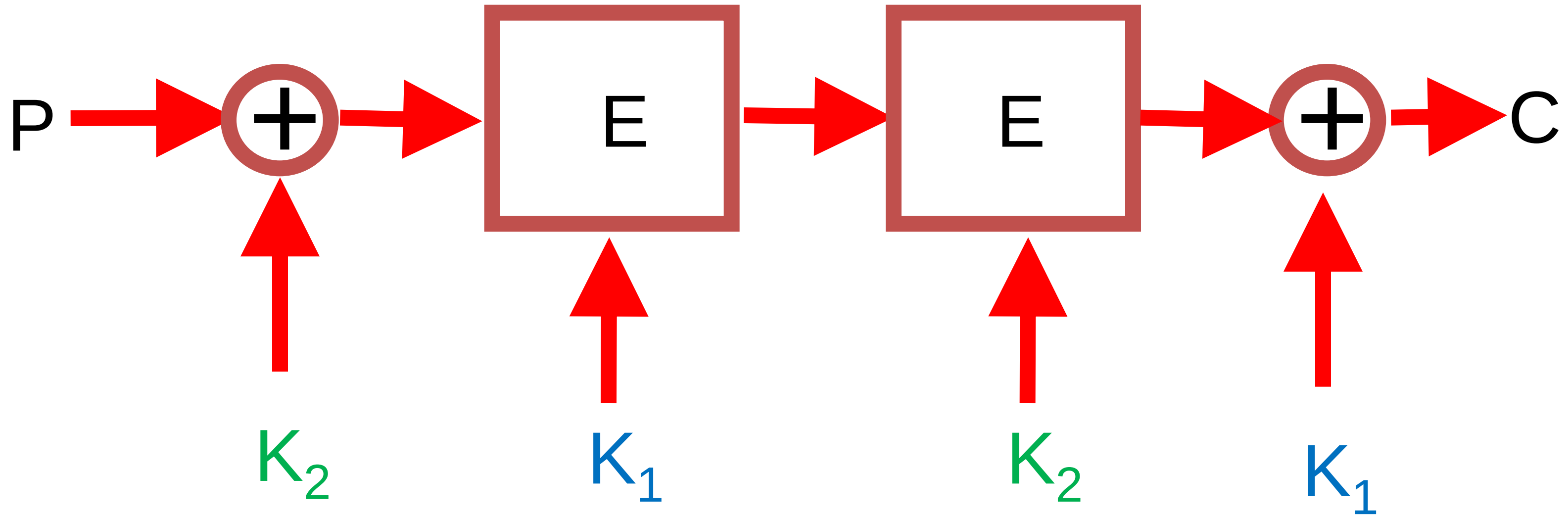
$<K_1, S_1, T_1>$

$<K_3, S_2, T_2>$

s.t. $S_1=S_2$ & $T_1=T_2$

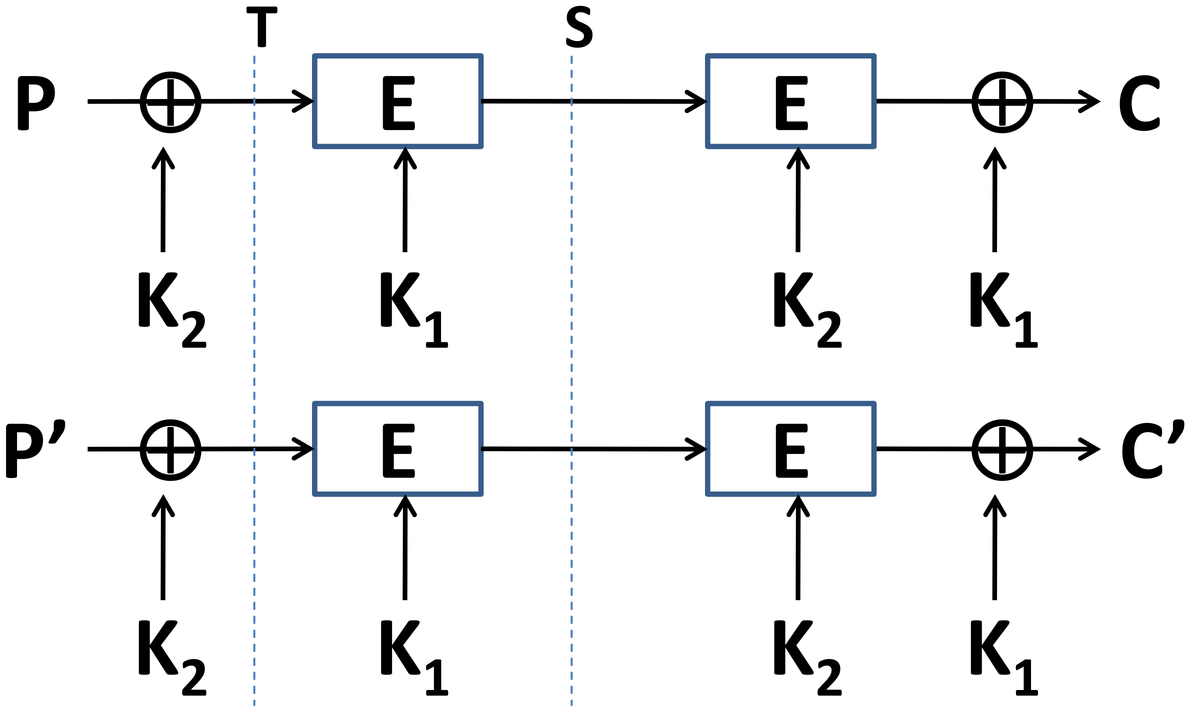
$O(2^n)$ time & $O(2^n)$ space

Proposal: DES-XEEX



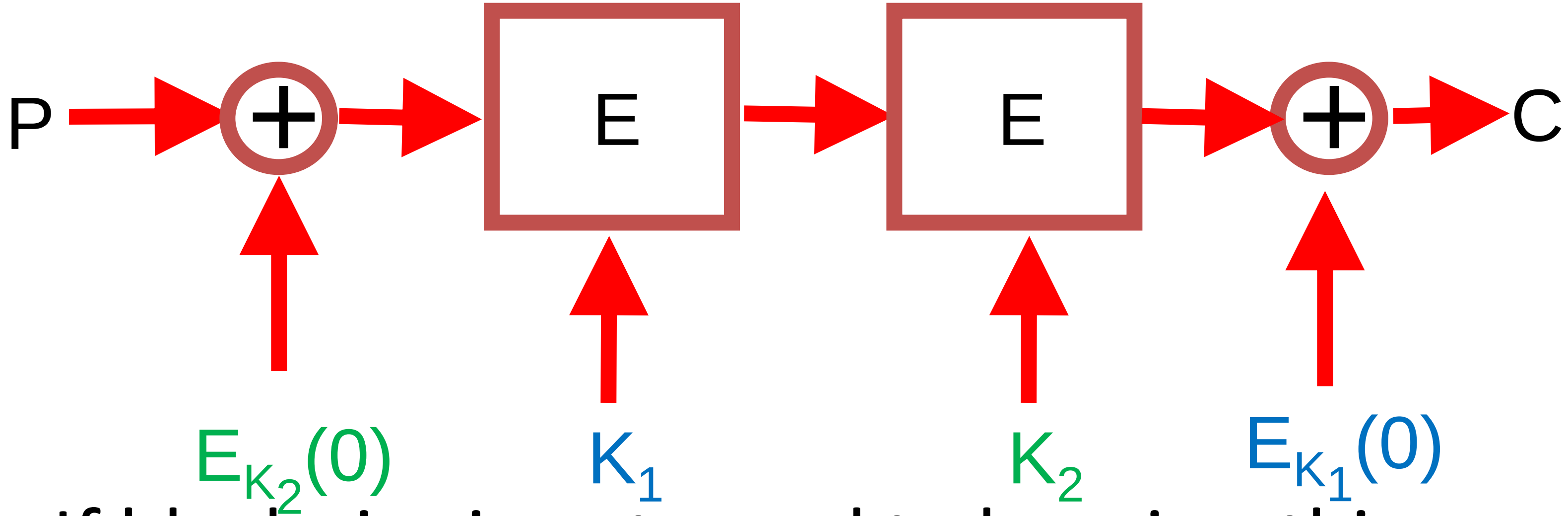
- MITM attack/Related-key attack on DES-EXE will not work
- Seems that no attack faster than exhaustive key search exists
  - Heuristic analysis given in the paper
- Detailed security analysis is still underway…

MITM Attack on DES-XEEX?



- Intuitively, to compute middle data at S, both K_1 & K_2 must be specified, so $O(2^{2n})$ space will be needed
- Also the attack time complexity will be $O(2^{2n})$

Variant of DES-XEEX



- If block size is not equal to key size, this variant is useful
  - $E_{K_2}(0)$ & $E_{K_1}(0)$ can be pre-computed
- Also can erase DES complementation property
  - $\overline{DES_K(P)} = DES_{\overline{K}}(\overline{P})$
  - $DES_{\overline{K_2}}\left(DES_{\overline{K_1}}\left(P \oplus DES_{\overline{K_2}}(0)\right)\right) \oplus DES_{\overline{K_1}}(0) =$ $DES_{K_2}\left(DES_{K_1}\left(P \oplus DES_{K_2}(\bar{0})\right)\right) \oplus DES_{K_1}(\bar{0})$

Summary

- We considered a multiple encryption scheme secure against
  - MITM attack
  - Related-key attack
  - Known-plaintext attack
- Existing DES variants are vulnerable to these attacks
- We gave one new construction which we call DES-XEEX and its variant
  - Generic and applicable to any block cipher

Thank you for you attention!