Safely Doubling Your Blockcipher for a Post-Quantum World

Ritam Bhaumik, André Chailloux, Paul Frixons, María Naya-Plasencia
INRIA Paris

Frisiacrypt 2022
Terschelling, Frisia
27 September 2022

Motivation

The Problem

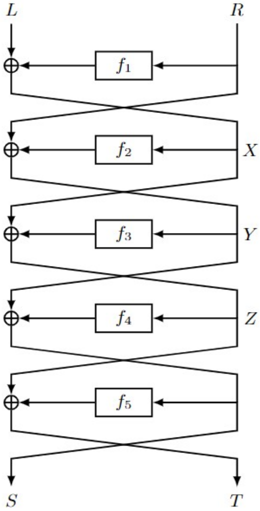
Goal

- Generic quantum-safe technique to *double* a block-cipher
- Use blockcipher with n-bit key, n-bit state
- Come up with a *wider* cipher
- Target state size: 2n bits
- Target key size: at least 2n bits

Desired Security

- n-bit security against classical and quantum attacks
- a provable guarantee that the security doesn't collapse against a quantum attack

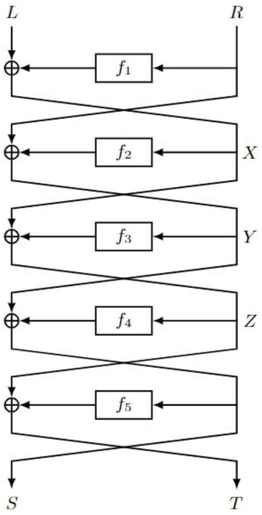
Possible Candidate: LR5



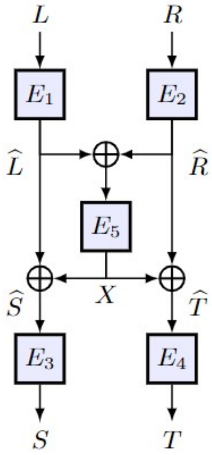
Problems with LR5

No attacks found (yet), but...

- Too many XORs
- Possibly susceptible to quantum attacks
- (Attack already found for LR4)
- In any case very difficult to prove post-quantum security



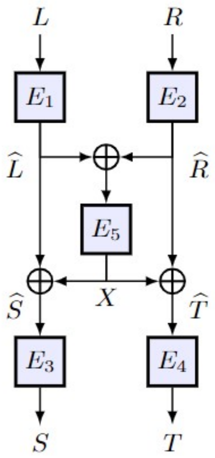
Possible Candidate: (two-block) EME



Things to like about EME

Advantages of EME

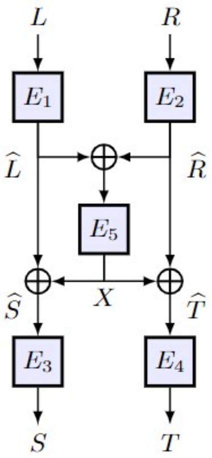
- More parallelisable than LR5
- Looks less susceptible to quantum attacks
- The ECB layers remove periods
- Every branch passes through at least two blockcipher calls



However...

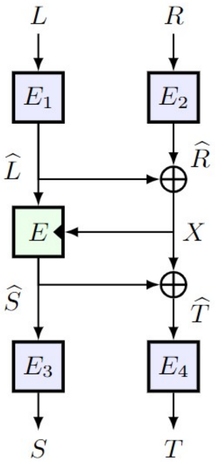
New Attack on EME!

- Use BHT to obtain collision on S
- Use Grover to recover key of E_2:
  - Guess the key of E_2
  - Use Simon to recover period and then the state
- Can be extended to any linear mixing of $\widehat{L}$ and $\widehat{R}$



Introducing QuEME

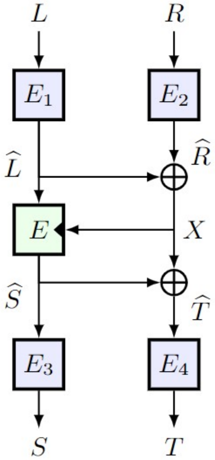
Our Proposal: QuEME



Why QuEME?

Advantages of QuEME

- Retains parallelisability of EME
- Middle layer prevents the EME-like attack
- Provably secure against classical and quantum adversaries



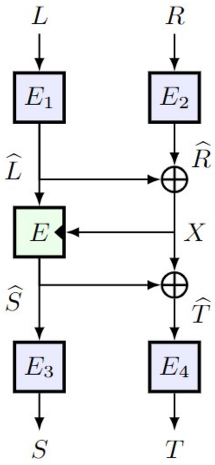
Security Results

Classical Security Proofs

- Up to $2n/3$ bits using direct counting
- Up to n bits using Mirror Theory
- Matching distinguisher of n bits

Quantum Security

- Can be shown up to $n/6$ bits using existing techniques
- We suspect actual security to be higher
- No better attack than classical found



Mirror Theory

Setup

- q equations $X_i \oplus Y_j = \delta_{ij}$ over n-bit numbers
- $X_1, \ldots, X_a$ distinct, $Y_1, \ldots, Y_b$ distinct
- Find lower bound on number of solutions

Conjectural Bounds

- From literature: $(2^n)_a (2^n)_b / 2^{nq}$
- We conjecture a tighter bound:
  - Form graph of equations with X's, Y's as vertices
  - Component sizes: $a_1, \ldots, a_r$ for X's, $b_1, \ldots, b_r$ for Y's
  - Tighter bound: $[2^{na_1}(2^n - a_1)^{a_2} \ldots][2^{nb_1}(2^n - b_1)^{b_2} \ldots]/2^{nq}$

Numerical Evidence for Mirror Theory

Conjectured bound (from last slide)

$$\frac{[2^{na_1}(2^n - a_1)^{a_2}(2^n - a_1 - a_2)^{a_3}\dots][2^{nb_1}(2^n - b_1)^{b_2}\dots]}{2^{nq}}$$

Simulations for small values of n

- Exact simulation for $n = 5$
- Close approximation for $n = 8$
- Slightly worse approximation up to $n = 11$
- All results seem to support the conjectured bound

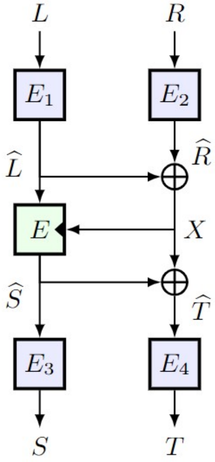
Instantiating QuEME

Key Scheduling

- Use a $2n$-bit key $k_1||k_2$
- Input layer: $E_1 = E(k_1, \cdot)$, $E_2 = E(k_2, \cdot)$
- Output layer: $E_3 = E(k_1 \oplus k_2, \cdot)$, $E_4 = E(k_1 \oplus (k_2 \lll 1), \cdot)$

With Round-Reduced AES

- Using E with r rounds of AES
- Found attack for $r = 3$
- Our guess: $r = 7$ should be enough
- $r \geq 4$: no attacks found yet, cryptanalytic attempts invited!



Open Problems

Things to do

- Find attacks on round-reduced instantiations of QuEME
- Find a better quantum proof for QuEME
- Explore other ways to instantiate QuEME (e.g., fewer rounds in the middle layer)
- Design better algorithms to simulate Mirror Theory for higher values of n
- (Even better) Prove the tighter version of Mirror Theory!

Thank you for your attention!