A Trivial Attack on McOE-X

Florian Mendel, Vincent Rijmen, Elmar Tischhauser

The Construction

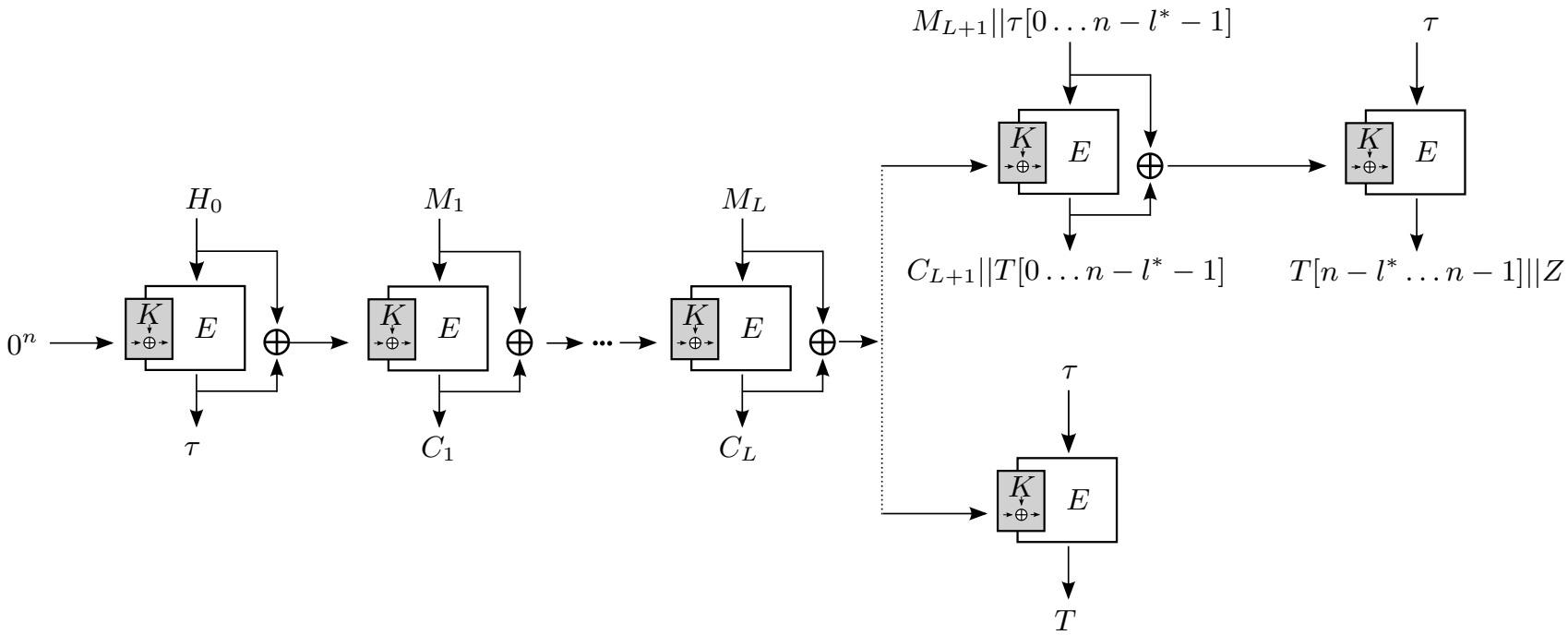

Figure: Structure of McOE-X.

The Attack

1. Choose an arbitrary value a.

The Attack

1. Choose an arbitrary value a.
2. For ℓ values k compute $b = E(k, a)$ and save the pair (b, k) in a list L.

The Attack

1. Choose an arbitrary value a.
2. For ℓ values k compute $b = E(k, a)$ and save the pair (b, k) in a list L.
3. Choose an arbitrary x and set $M_1 = x$ and $M_2 = a$ such that $m = x \| a$ and ask for the ciphertext/tag pair (c, T) with $c = C_1 \| C_2$.

The Attack

1. Choose an arbitrary value a.
2. For ℓ values k compute $b = E(k, a)$ and save the pair (b, k) in a list L.
3. Choose an arbitrary x and set $M_1 = x$ and $M_2 = a$ such that $m = x \| a$ and ask for the ciphertext/tag pair (c, T) with $c = C_1 \| C_2$.
4. Check if C_2 is in the list L to get K.

The Attack

1. Choose an arbitrary value a.
2. For ℓ values k compute $b = E(k, a)$ and save the pair (b, k) in a list L.
3. Choose an arbitrary x and set $M_1 = x$ and $M_2 = a$ such that $m = x \| a$ and ask for the ciphertext/tag pair (c, T) with $c = C_1 \| C_2$.
4. Check if C_2 is in the list L to get K.
   - If C_2 is in the list L then a candidate for the key is found. Compute $K = k \oplus M_1 \oplus C_1$,

The Attack

1. Choose an arbitrary value a.
2. For ℓ values k compute $b = E(k, a)$ and save the pair (b, k) in a list L.
3. Choose an arbitrary x and set $M_1 = x$ and $M_2 = a$ such that $m = x \| a$ and ask for the ciphertext/tag pair (c, T) with $c = C_1 \| C_2$.
4. Check if C_2 is in the list L to get K.
   - If C_2 is in the list L then a candidate for the key is found. Compute $K = k \oplus M_1 \oplus C_1$,
   - Else go back to step 3.

The Attack

1. Choose an arbitrary value a.
2. For ℓ values k compute $b = E(k, a)$ and save the pair (b, k) in a list L.
3. Choose an arbitrary x and set $M_1 = x$ and $M_2 = a$ such that $m = x \| a$ and ask for the ciphertext/tag pair (c, T) with $c = C_1 \| C_2$.
4. Check if C_2 is in the list L to get K.
   - If C_2 is in the list L then a candidate for the key is found. Compute $K = k \oplus M_1 \oplus C_1$,
   - Else go back to step 3.

After repeating steps 3-4 about $2^n/\ell$ times one expects to find the correct key with complexity of about $2^n/\ell + \ell$.

Discussion

- Attack is applicable whenever known values are xored (combined) with the key input

Discussion

- Attack is applicable whenever known values are xored (combined) with the key input
- How to fix McOE-X?

Discussion

- Attack is applicable whenever known values are xored (combined) with the key input
- How to fix McOE-X?
  - Increase the keysize

Discussion

- Attack is applicable whenever known values are xored (combined) with the key input
- How to fix McOE-X?
  - Increase the keysize
  - Use a tweakable block cipher :-)

Discussion

- Attack is applicable whenever known values are xored (combined) with the key input
- How to fix McOE-X?
  - Increase the keysize
  - Use a tweakable block cipher :-)

Thank you for your attention!