ISC 2015

On Security of a White-Box Implementation of SHARK

Yang SHI and Hongfei FAN

Tongji University, China

Agenda

- *Part A: WBAC & WBAE*
- Part B: SHARK & white-box SHARK
- Part C: Attack against white-box SHARK

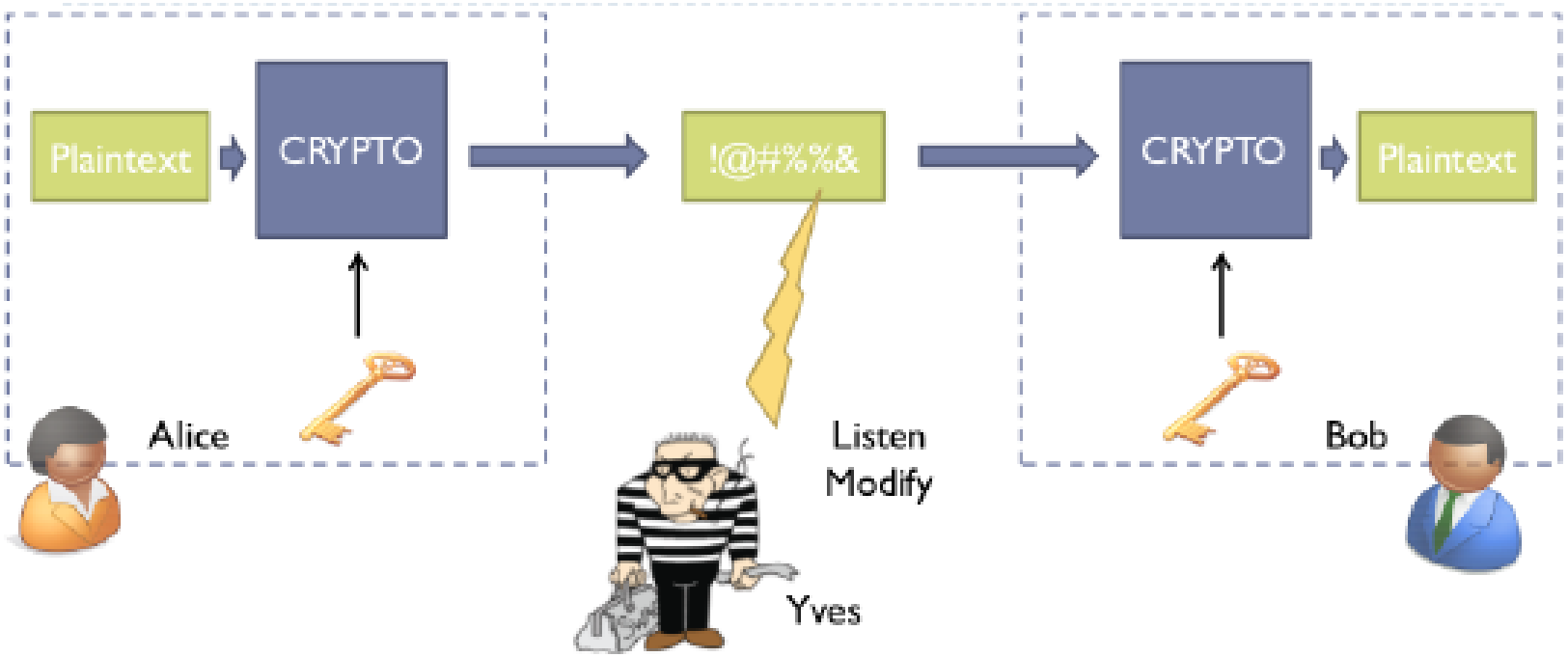
Attack models and contexts

- Black-box
- Grey-box
- White-box
  - White-Box Attack Context (WBAC)
  - White-Box Encryption Algorithm (WBAE)

Black-box attack

Kerckhoffs's principle

- Adversary has knowledge of the algorithm
- The cryptosystem system's security relies on the confidentiality of the key



White-box attack

- Reverse engineering
- Debug
- More...

Adi Shamir and Nicko van Someren. Playing "Hide and Seek" with Stored Keys. In Proceedings of the Third International Conference on Financial Cryptography (FC 1999), volume 1648 of Lecture Notes in Computer Science, Springer-Verlag, 1999, pp. 118–124.

Threats and cryptanalysis techniques

Black-box cryptanalysis

- Oracle: input/output
- Attack:
  - Differential attack
  - Linear attack
  - More...

Side-channel Cryptanalysis

- Oracle: leakage function
- Attack:
  - Time analysis
  - Power analysis
  - Electromagnetic radiation
  - Fault injection
  - More...

White-box cryptanalysis

- Oracle: the implementation
- Attack:
  - Memory inspection
  - CPU call interception
  - Debugging
  - Reverse engineering
  - Code tampering
  - Entropy attack
  - More...

Typical samples of WBAC

- Server/PC for which a hacker has obtained "root" or "admin" privilege
- Malicious host where a mobile agent is running
- Outside wireless sensor network (WSN) node captured by an attacker
- Digital right management (DRM) components in IPTV or cable TV set-top boxes
- Mobile devices captured by an attacker

Heavy-weight WBEAs and analysis

WBEA	Cryptanalysis
White-box DES [4] (Chow et al., 2002)	• Jacob, Boneh and Felten in [21], 2002 • Wyseur, Michiels, Gorissen and Preneel in [22], 2007 • Goubin, Masereel, and Quisquater in [23], 2007
White-box DES [18] (Link and Neumann, 2005)	• Wyseur, Michiels, Gorissen and Preneel in [22], 2007 • Goubin, Masereel, and Quisquater in [23], 2007
White-box AES [3] (Chow et al., 2002)	• Billet, Gilbert and Ech-Chatbi in [24], 2004 • Tolhuizen in [26], 2012 (an improvement of [24]) • Lepoint, Rivain, De Mulder, Roelse and Bart Preneel in [30], 2013 (an improvement of [24])
A generic construction base on [3]	• Michiels, Gorissen and Hollmann in [25], 2008
Perturbated White-Box AES [20] (Bringer et al., 2006)	• De Mulder, Wyseur, and Preneel in [27], 2010
White-box AES [15] (Xiao and Lai, 2009)	• De Mulder, Roelse and Preneel in [28], 2013
White-box AES with dual ciphers [19] (Karroumi, 2011)	• Lepoint, Rivain, De Mulder, Roelse and Preneel in [30], 2013
White-box SHARK [5] (Shi et al., 2013)	• ISC 2015

Agenda

- Part A: WBAC & WBAE
- *Part B: SHARK & white-box SHARK*
- Part C: Attack against white-box SHARK

The block cipher SHARK

- A well-known block cipher
- A 6-round SPN
- Key size: 128 bits
- Block size: 64 bits

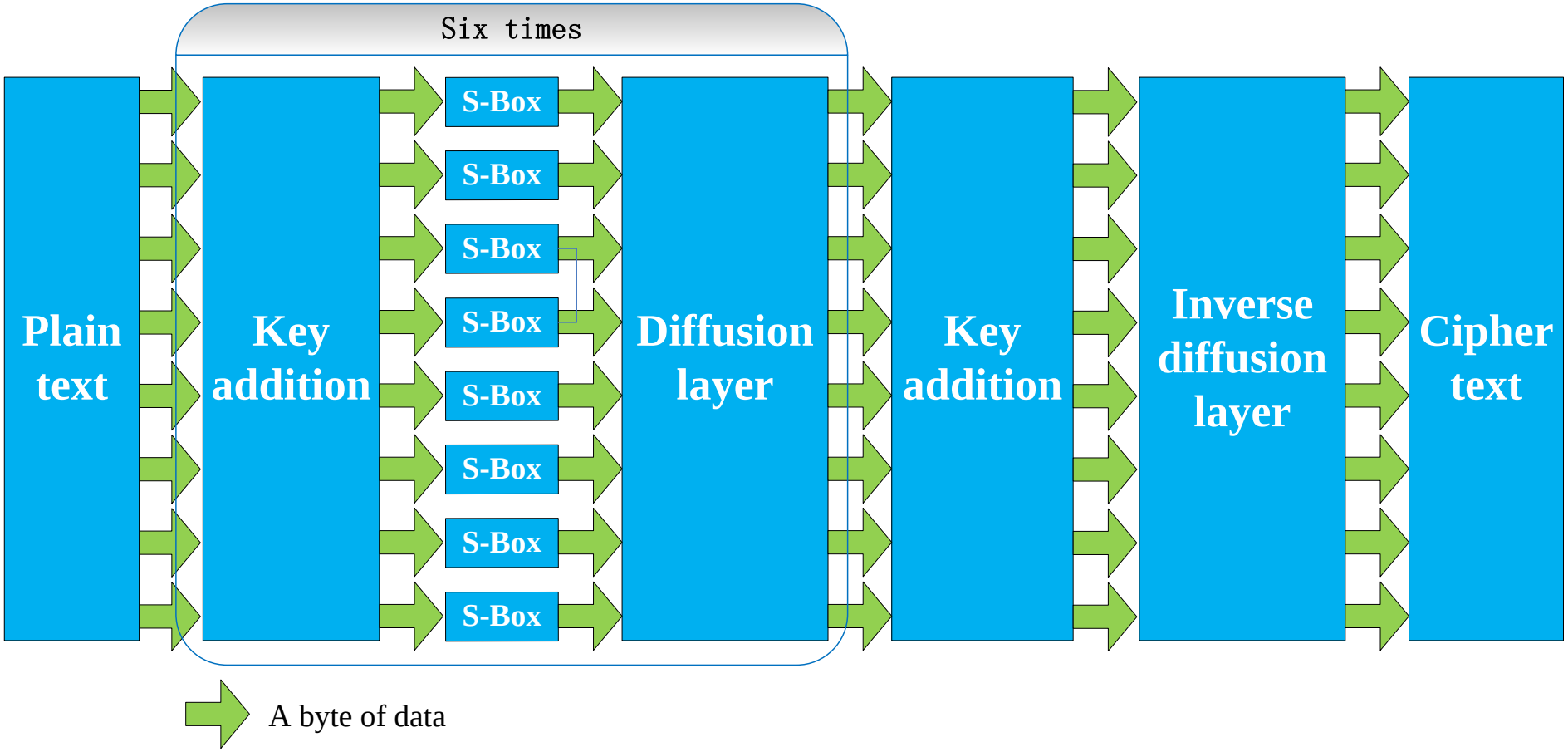
Rijmen, V., Daemen, J., Preneel et al.

The round function

$$SHARK[K] = \lambda^{-1} \circ \left(\bigcirc_{r=1}^{6} \sigma[K^r] \circ \lambda \circ \gamma \right) \circ \sigma\left[K^0\right]$$

- Let $S : GF(2^8) \to GF(2^8), x \mapsto S[x]$ be the mapping of S-Boxes. Then the substitution layer can be defined as $\gamma : GF(2^8)^8 \to GF(2^8)^8$, $\gamma(a) = b \Leftrightarrow b_i = S[a_i]$, $0 \le i \le 7$.
- Let $\lambda : GF(2^8)^8 \to GF(2^8)^8$ denote the linear transformation corresponding to the linear diffusion layer. There exists a matrix H such that $\lambda(a) = b \Leftrightarrow b = a \cdot H$.
- Let K^r be the round key of the r^{th} round and let $\sigma[K^r] : GF(2^8)^8 \to GF(2^8)^8$ be the key exclusive or mapping.

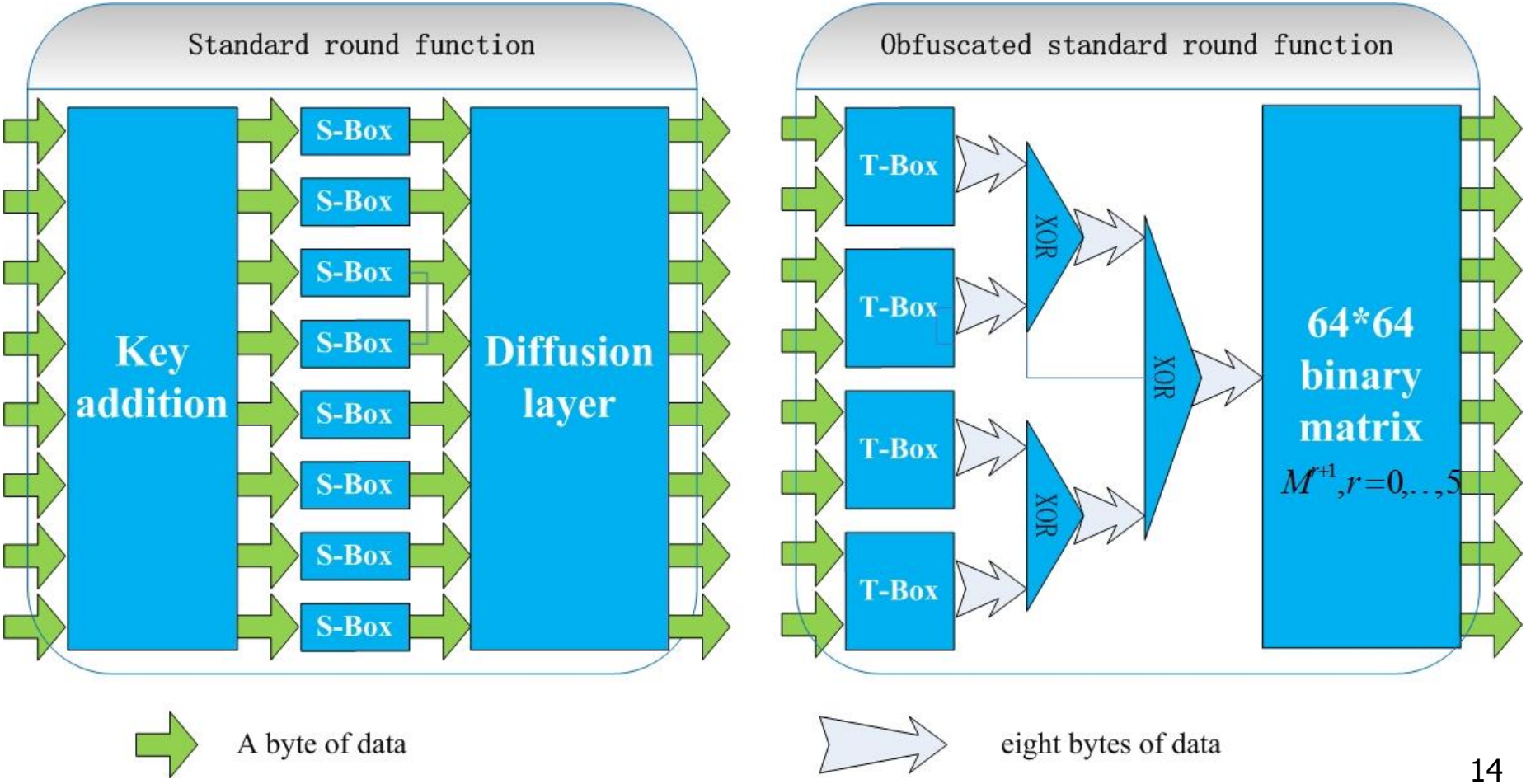
SHARK's flow


Six times
Plain text
Key addition
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
Diffusion layer
Key addition
Inverse diffusion layer
Cipher text
A byte of data

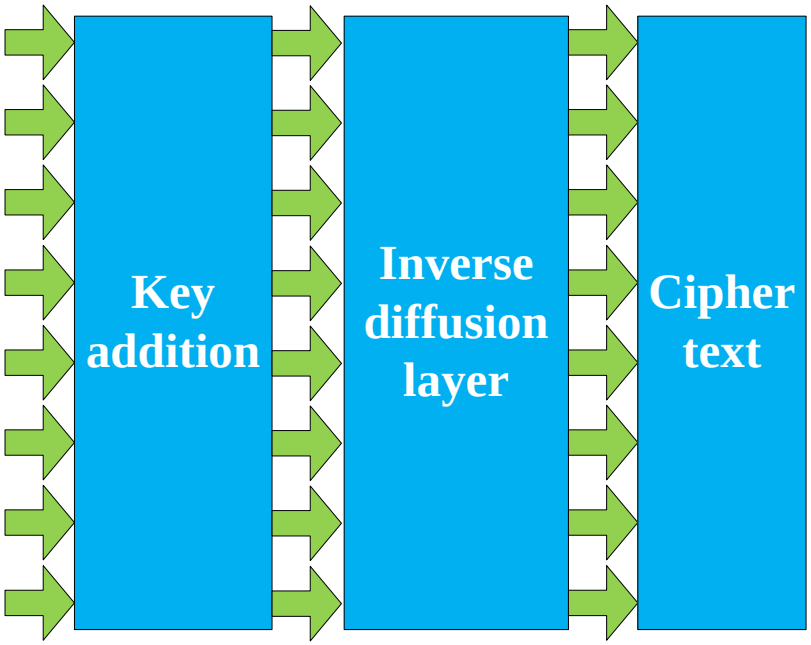
General design strategy

- Combine the three layers together
- Hide keys in lookup tables
- Protect “nake” table with inversable mappings

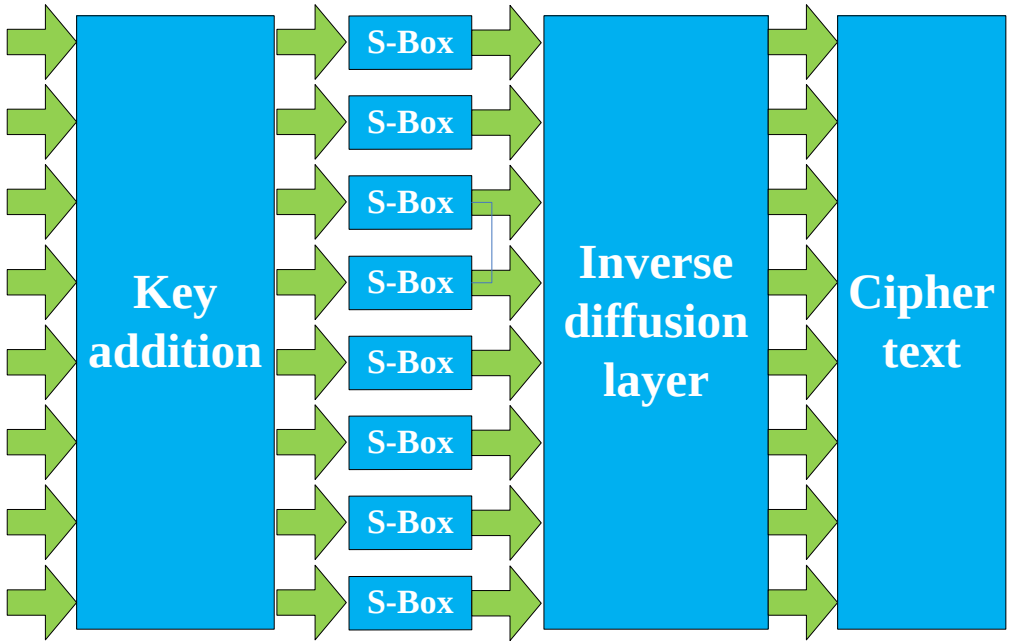
Flow of white-box SHARK



Modification on SHARK's last round

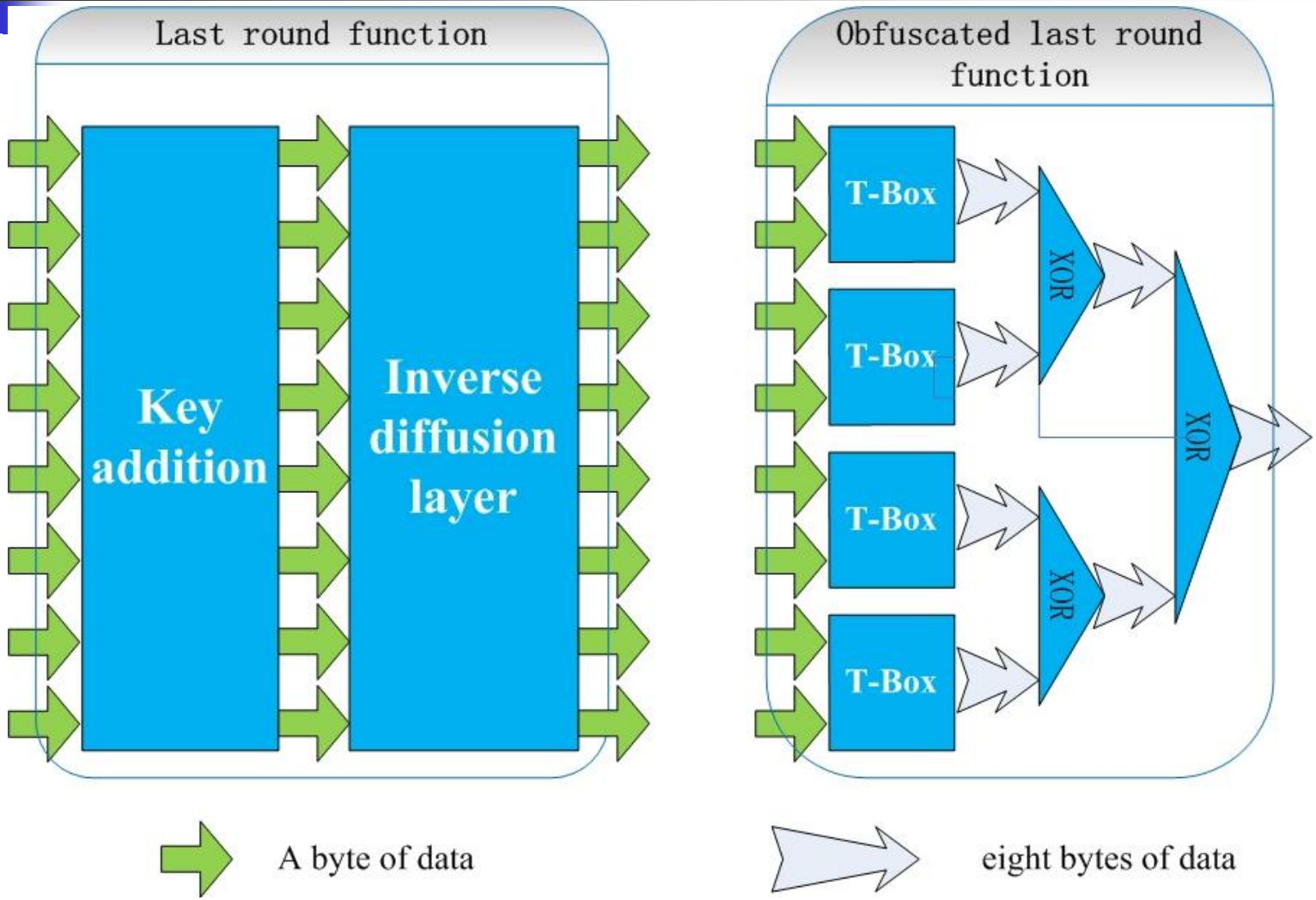


(a) The last round of SHARK



(b) The modified last round of SHARK

Dataflow in Round 6



Hiding the key in T-Boxes

- Each T-Box is implemented as a 16-bit to 64-bit lookup table

$$r = 0,\ldots,5; i = 0,\ldots,3:$$

$$\rho_W[r,i,K](x) = \left(\left(S \| S\right)_{\Delta r} \left(\left(L_i^{(r)}(x) \right) \oplus \left(\Delta_r \left(k_{2i}^{(r)} \left\| k_{2i+1}^{(r)} \right. \right) \right) \right) P_i^{(r)} \right)$$

$$r = 6; i = 0,\ldots,3:$$

$$\rho_W[6,i,K](x) = \left(\left(L_i^{(6)}(x) \right) \oplus \left(\Delta_6 \left(k_{2i}^{(6)} \left\| k_{2i+1}^{(6)} \right. \right) \right) P_i^{(6)} \right)$$

White-box SHARK's encryption process

Algorithm $SHARK_W[K]$ $(on\ \ input\ \ x)$:

(1) $i \leftarrow 0$

(2) $(x_0, x_1, x_2, x_3) \leftarrow x$

(3) $j \leftarrow 0$

(4) $y_j \leftarrow TBox_{i,j}(x_j)$ // *Lookup in a TBox*

(5) $j \leftarrow j+1$

(6) *if* $(j < 4)$ *goto*(4); *else goto*(7)

(7) $x \leftarrow y_0 \oplus y_1 \oplus y_2 \oplus y_3$

(8) *if* $(i < 7)$ *goto*(9); *else goto*(11)

(9) $x \leftarrow x \cdot M_i$

(10) $i \leftarrow i+1$; *goto*(2)

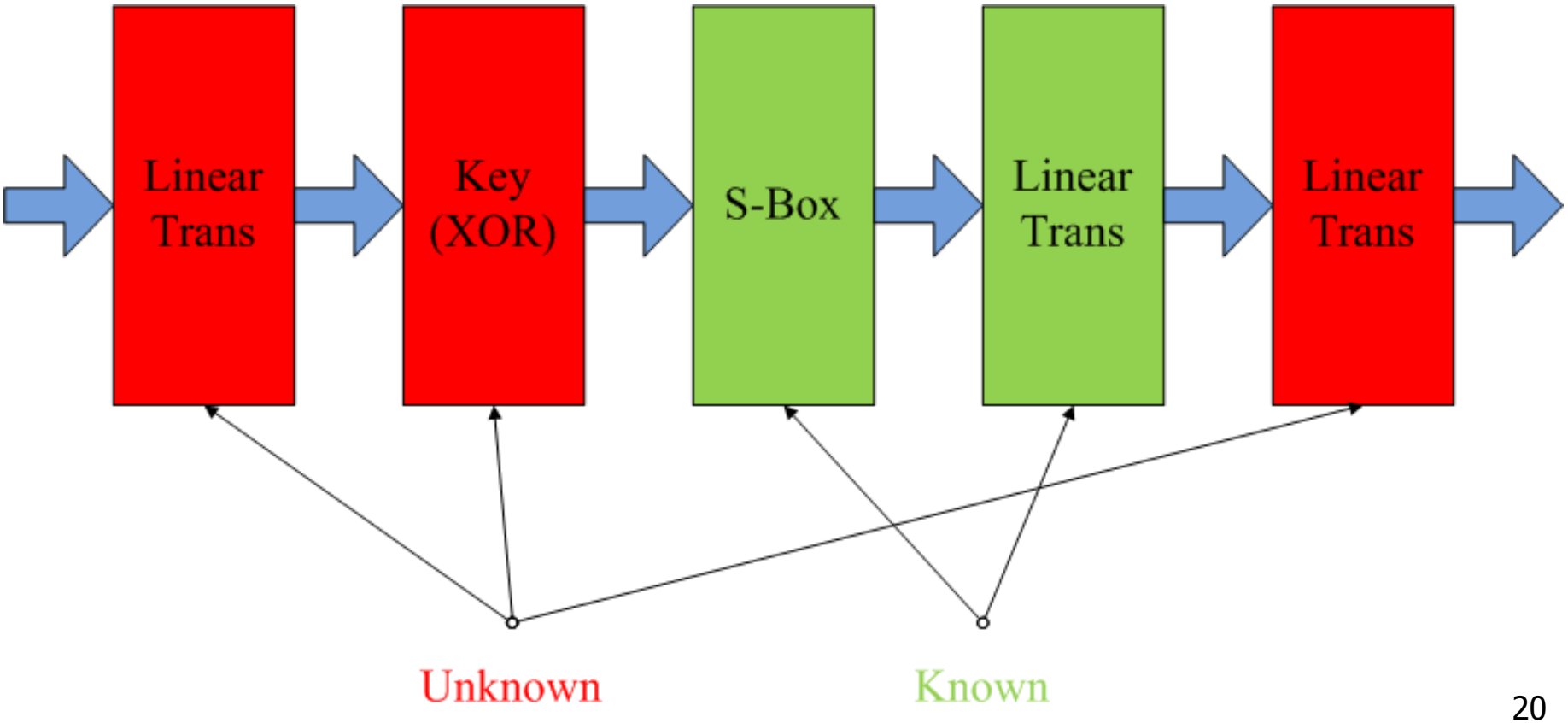
(11) *output* x

Agenda

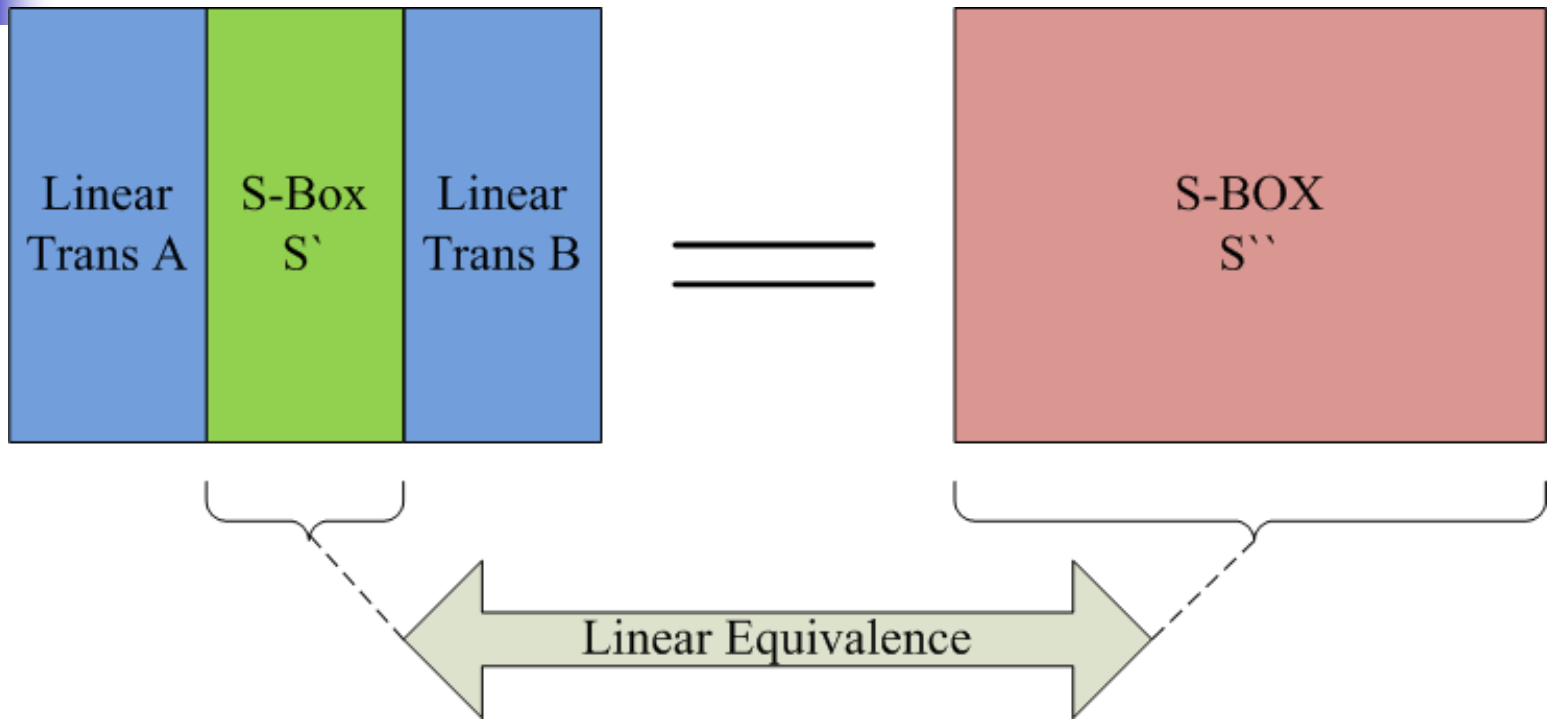
- Part A: WBAC & WBAE
- Part B: SHARK & white-box SHARK
- *Part C: Attack against white-box SHARK*

Theoretical analysis of T-Boxes

- Theorem 1:

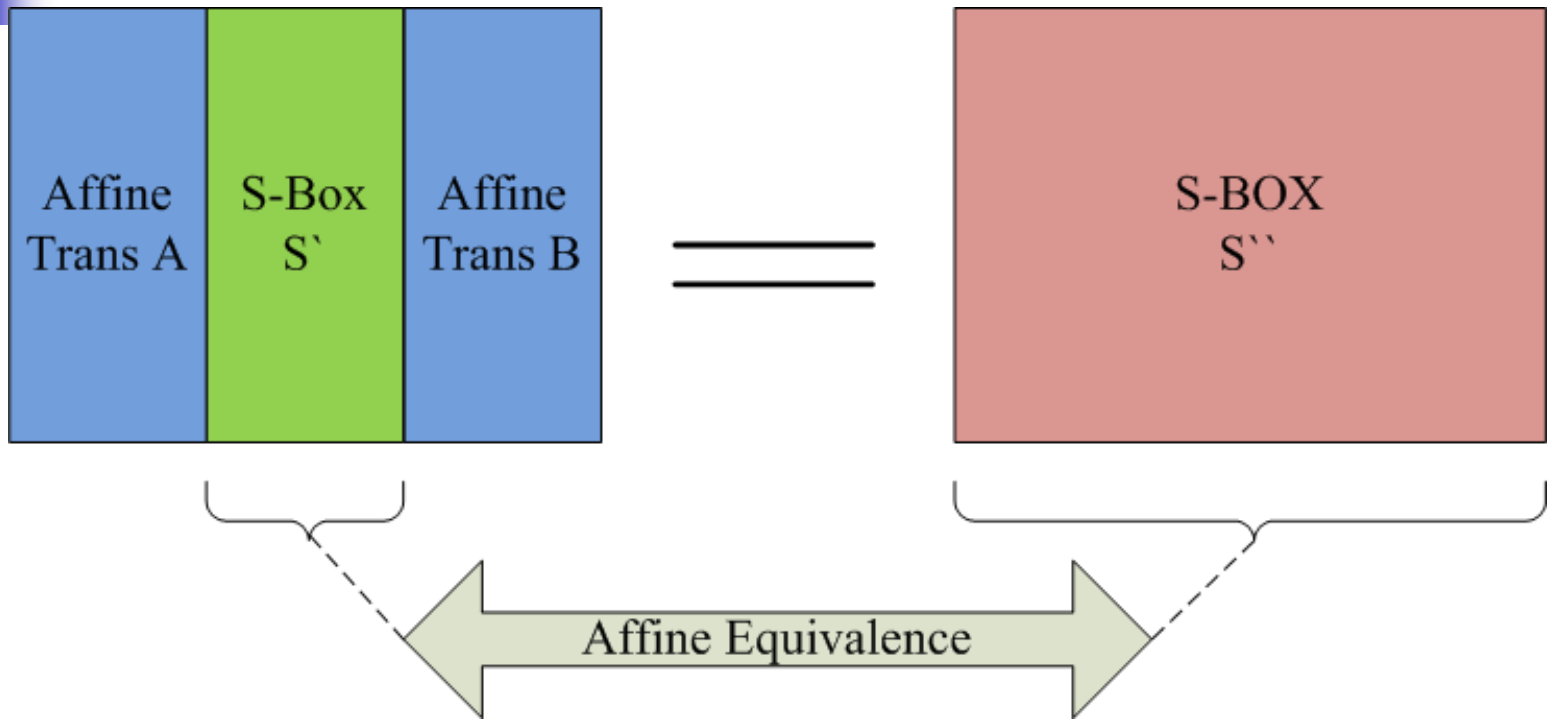


LE problem and solution



- $O(n^3 2^n)$, 2^{28} when n=16

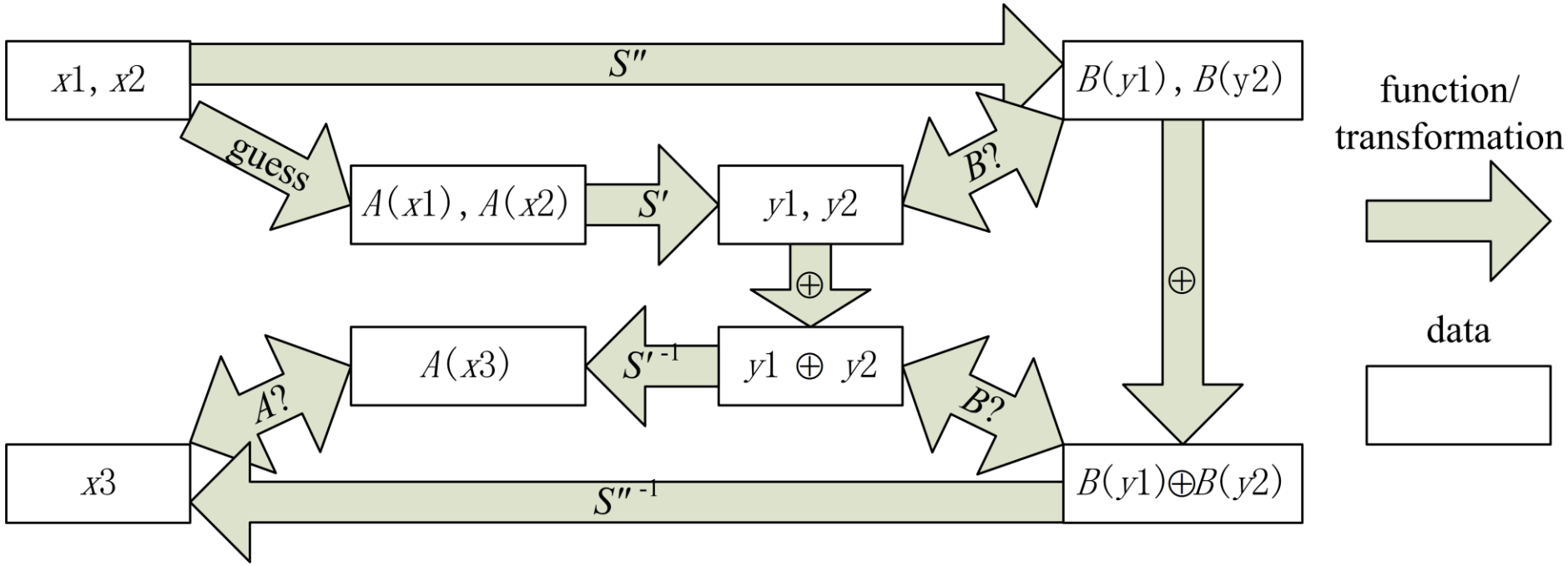
AE problem and solution



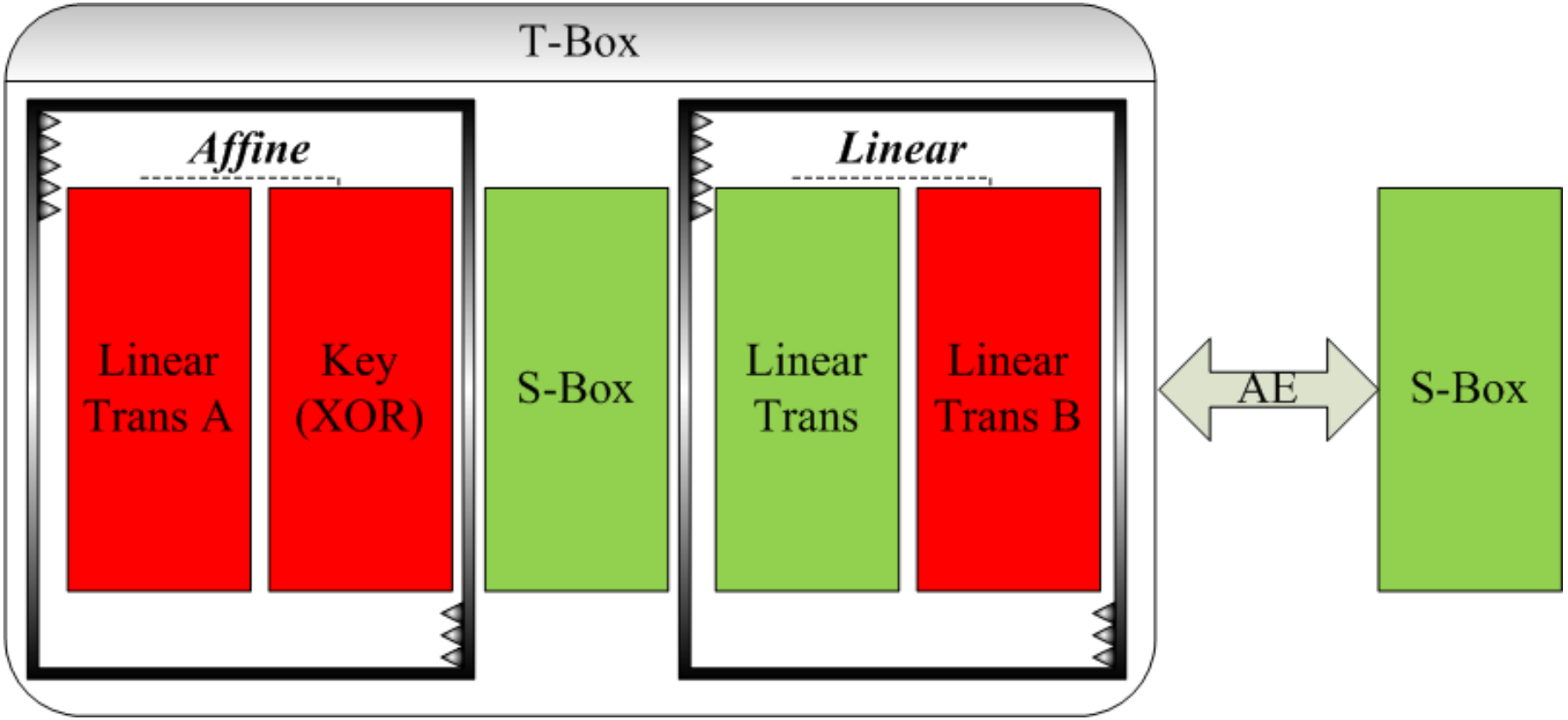
- $O(n^3 2^{2n})$, 2^{44} when n=16

Extended LE

- Executing LE over all possible guesses
- Gaussian elimination (n^3) for each possible pair of initial guesses (2^{2n}): $n^3 * 2^{2n}$

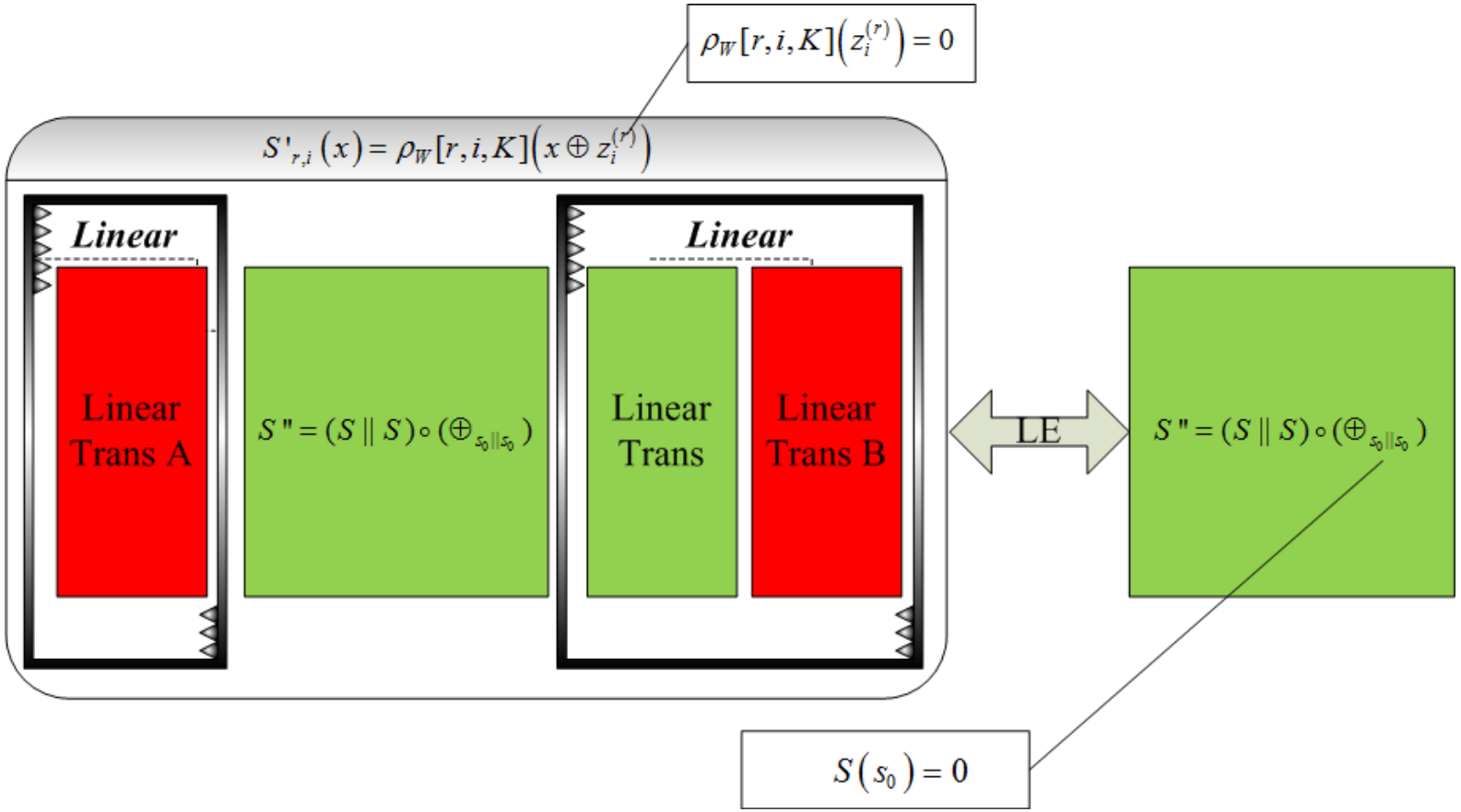


Intuitive attack



Improved attack

- Theorem 2: enabling LE analysis



Workflow of the whole attack

Generate all possible linear transformations from lookup tables of round 0,1,6 by using the ELE Algorithm.

↓

Find real-used linear transformations of round 0 and 1 by checking the compatibility of them.

↓

Search the rounds keys of round 0 and 1 from related lookup tables.

↓

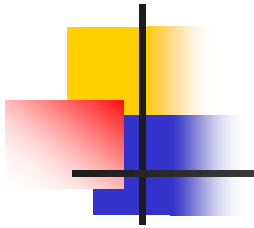
Calculate the cipher key from the first two round keys according to the key scheduling algorithm of SHARK.

↓

Find real-used linear transformations of round 6 by checking the compatibility of the output of standard SHARK and white-box SHARK.

Future work

- Implement the attack
- Improve the attack
- Design a more secure white-box SHARK against various known attacks



Thank You