COSIC
CRYPTOGRAPHY & CYBER SECURITY

Polynomial-Based White-Box AES

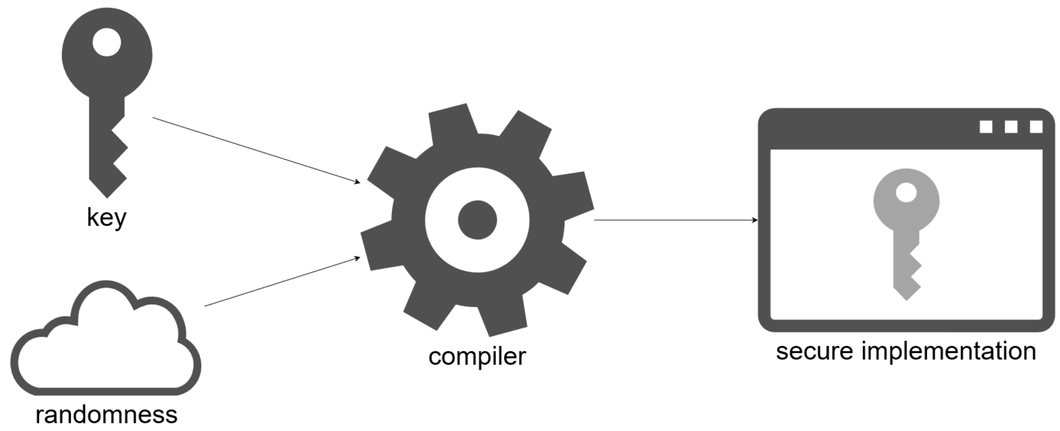
Adrián Ranea and Bart Preneel

Introduction

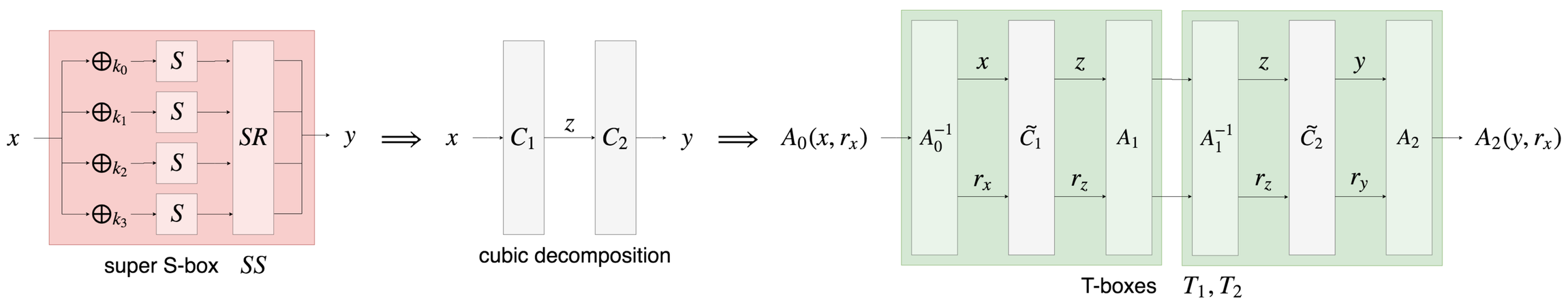
White-box cryptography studies the design of secure software implementations of cryptographic algorithms in the white-box model, where the adversary has full control on the device executing the crypto.

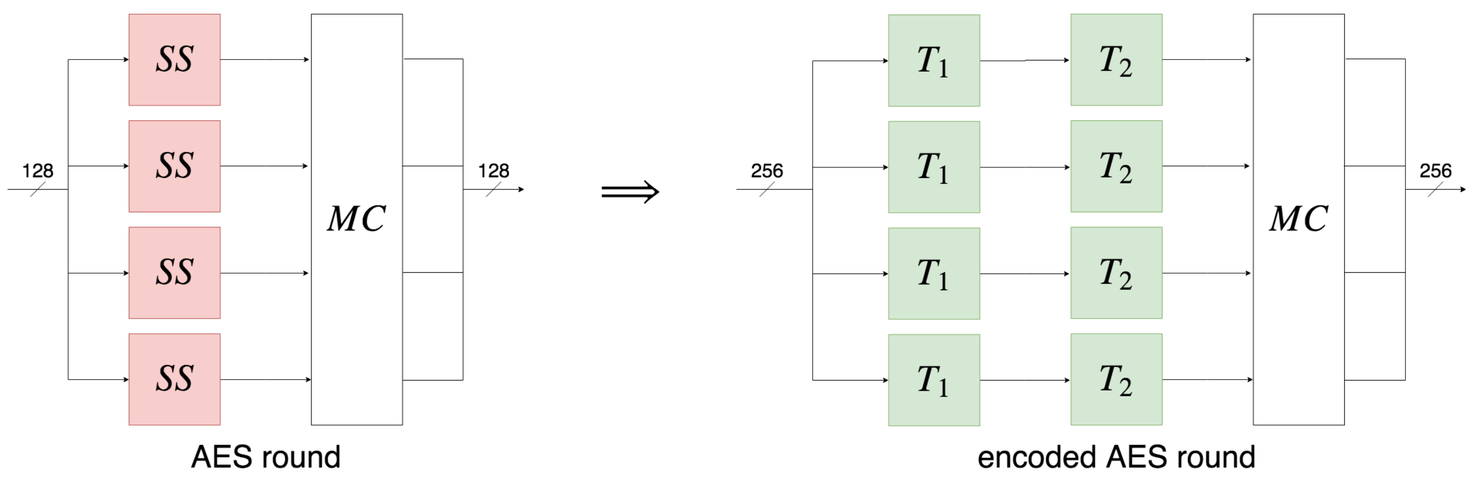
We design a white-box AES compiler, i.e., a systematic and randomized method to compile AES for a fixed-key in such a way that the key cannot be extracted from the binary.

All previous white-box implementations have been broken.



Design





Analysis

T-boxes are implemented by polynomials over GF(2) and their complexity is measured by the number of non-zero monomials.

Since each T-box is a polynomial of 64 variables with algebraic degree 3, the number of non-zero monomials per component is

$$\sum_{i=0}^{3} \binom{64}{i} \approx 2^{15}$$

Several techniques are combined to prevent known white-box attacks:

- External encodings prevent DCA/DFA.
- The unknown middle substitution layer of the T-boxes prevents affine-equivalence-based attacks.
- The structure of the middle substitution layer prevents ASA decomposition attacks.

Conclusion

- We propose a secure white-box AES implementation based on randomized low degree polynomials.
- Our construction can be applied to other ciphers.
- For future work, we are analysing alternatives to external encodings

Bibliography

1. Chow, Stanley, et al. "White-box cryptography and an AES implementation." SAC. Springer, Berlin, Heidelberg, 2002.
2. Billet, Olivier, Henri Gilbert, and Charaf Ech-Chatbi. "Cryptanalysis of a white box AES implementation." SAC. Springer, Berlin, Heidelberg, 2004.
3. Bringer, Julien, Hervé Chabanne, and Emmanuelle Dottax. "White Box Cryptography: Another Attempt." IACR Cryptology ePrint Archive 2006.2006 (2006): 468.
4. Bos, Joppe W., et al. "Differential computation analysis: Hiding your white-box designs is not enough." CHES. Springer, Berlin, Heidelberg, 2016.