Generation of Efficient Bitslice Implementations of Large S-boxes

Presented by:
Augustin Bariant augustin.bariant@inria.fr,
Joint work with:
Matthieu Daumas mdaumas@quarkslab.com,
Adrien Guinet aguinet@quarkslab.com

Quarkslab, France

Abstract. Whitebox cryptography aims at protecting standard cryptographic algorithms that execute in attacker-controlled environments, in which the attacker is able to read a secret key directly from memory. Common implementations mask all data at runtime and operate on masked data by using many small precomputed tables. Practical whiteboxes involve trade-offs between security and execution speed, to limit their footprints and enable applications such as real-time video streaming.

To improve this compromise, we study the use of bitslicing (or bit-parallelism) to implement whiteboxes. Bitslicing is commonly used to write fast constant-time implementations of cryptographic algorithms and relies on the synthesis of boolean circuits implementing the corresponding algorithms. The synthesis of optimal circuits for lookup tables is resource intensive and generally only performed once. In a whitebox context however, a lot of random lookup tables are generated at compile-time, therefore we require the boolean circuit generation to be time efficient.

To begin with, the complexity of the synthesis of optimal size boolean circuits by exhaustive search for a boolean function is double exponential in the number of inputs of the function. The complexity further increases with the number of output bits of the Sbox. Several known algorithms, like the Quine–McCluskey algorithm, improve on the exhaustive search but still remain of double exponential complexity. Ullrich et al. successfully found the optimal bitslice implementation of more than 90% of 4x4 Sboxes up to affine equivalence [1], but the problem of finding optimal bitslice implementations of larger Sboxes remains hard. An efficient bitslice implementation of the AES Sbox was found using its internal structure [2], but this result can not be generalised to other large unstructured Sboxes.

In this talk, we give an introduction to bitslicing and review some well-known circuit-synthesis algorithms. We study the technique of Binary Decision Diagrams to generate efficient circuits in a cheap and adaptable manner. Eventually, we go through different techniques to evaluate the generated circuits and analyse the performances of our algorithm.

This talk will be presented by Augustin Bariant and is a joint work with Matthieu Daumas and Adrien Guinet.

References

1. Markus Ullrich, Christophe De Canniere, Sebastiaan Indesteege, Özgül Küçük, Nicky Mouha, and Bart Preneel. Finding optimal bitsliced implementations of 4× 4-bit s-boxes. In *SKEW 2011 Symmetric Key Encryption Workshop, Copenhagen, Denmark*, pages 16–17, 2011.
2. Robert Könighofer. A fast and cache-timing resistant implementation of the aes. In Tal Malkin, editor, *Topics in Cryptology – CT-RSA 2008*, pages 187–202, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.