Automated Proofs for Encryption Modes. *

Martin Gagné[2], Pascal Lafourcade[1], Yassine Lakhnech[1], and Rei Safavi-Naini[2]

[1] Université Grenoble 1, CNRS,VERIMAG, FRANCE
[2] Department of Computer Science, University of Calgary, Canada

A block cipher algorithm (e.g. AES, Blowfish, DES, Serpent and Twofish) is a symmetric key algorithm that takes a fixed size input message block and produces a fixed size output block. A mode of operation is a method of using a block cipher on an arbitrary length message. Important modes of operation are Electronic Code Book ECB, Cipher Block Chaining (CBC), Cipher FeedBack mode (CFB), Output FeedBack (OFB), and Counter mode (CTR). Modes of operations have different applications and provide different levels of security and efficiency. An important question when a mode of operation is used for encryption is the level of security that the mode provides, assuming the underlying block cipher is secure. The answer to this question is not straightforward. For example if one uses the naive ECB mode with a "secure" block cipher, then the encryption scheme obtained is not even IND-CPA secure. Another example is using (CTR) mode with Initial Vectors (IV) that instead of randomly selected, is obtained by incrementing it by one for each consecutive message.

The main contribution of this paper is to propose a compositional Hoare logic for proving IND-CPA-security of modes of operation for symmetric key block ciphers. We first notice that most of modes use a small set of operations such as xor, concatenation, and selection of random values. This allows us to introduce a simple programming language to specify encryption modes and an assertion language that allows to state invariants and axioms and rules to establish such invariants. The assertion language consists of few atomic predicates. Transforming the Hoare logic into an (incomplete) automated verification procedure is quite standard. Indeed, we can interpret the logic as a set of rules that tell us how to propagate the invariants backwards. We were able to automatically verify IND-CPA security of several encryption modes including (CBC), (CFB), (CTR) and (OFB).

* This work was supported by ANR SeSur SCALP, SFINCS and AVOTE.