Automated Proofs for Asymmetric Encryption. ⋆

Judicaël Courant, Marion Daubignard, Cristian Ene, Yassine Lakhnech, and Pascal Lafourcade

Université Grenoble 1, CNRS,Verimag
firstname.last@imag.fr

We present an automated proof method for analyzing generic asymmetric encryption schemes in the random oracle model (ROM). Generic encryption schemes aim at transforming schemes with weak security properties, such as one-wayness, into schemes with stronger security properties, especially security against chosen ciphertext attacks. Examples of generic encryption schemes are [?,?,?,?,?,?,?,?]. The paper contains two main contributions. The first one is a compositional Hoare logic for proving IND-CPA-security. That is, we introduce a simple programming language (to specify encryption algorithms that use one-way functions and hash functions) and an assertion language that allows to state invariants and axioms and rules to establish such invariants. Compositionality of the Hoare logic means that the reasoning follows the structure of the program that specifies the encryption oracle. The assertion language consists of three atomic predicates. The first predicate allows us to express that the value of a variable is indistinguishable from a random value even when given the values of a set of variables. The second predicate allows us to state that it is computationally infeasible to compute the value of a variable given the values of a set of variables. Finally, the third predicate allows us to state that the value of a variable has not been submitted to a hash function.

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 have done this for our logic resulting in a verification procedure implemented in less than 250 lines of CAML. We have been able to automatically verify IND-CPA security of several schemes among which [?,?,?]. Our Hoare logic is incomplete for two main reasons. First, the reader should notice that IND-CPA security is an observational equivalence-based property, while with our Hoare logic we establish invariants. Nevertheless, as shown in one of our propositions, we can use our Hoare logic to prove IND-CPA security at the price of completeness. That is, we prove a stronger property than IND-CPA. The second reason, which we think is less important, is that for efficiency reasons some axioms are stronger that needed.

The second contribution of the paper presents a simple criterion for plaintext awareness (PA). Plaintext awareness has been introduced by Bellare and Rogaway in [?]. It has then been refined in [?] such that if an encryption scheme is PA and IND-CPA then it is IND-CCA. Intuitively, PA ensures that an adversary cannot generate a valid cipher without knowing the plaintext, and hence, the decryption oracle is useless for the adversary. The definition of PA is complex

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

and proofs of PA are also often quite complex. In this paper, we present a simple syntactic criterion that implies plaintext awareness. Roughly speaking the criterion states that cipher should contain as a sub-string the hash of the plaintext and the random seed. This criterion applies for many schemes such as [?,?,?] and easy to check. Although (or maybe because) the criterion is simple, the proof of its correctness is complex.

Putting together these two contributions, we get a proof method for IND-CCA security, that applies for instance to the constructions in [?,?,?].

An important feature of our method is that it is not based on a global reasoning and global program transformation as it is the case for the game-based approach [?,?]. Indeed, both approaches can be considered complementary as the Hoare logic-based one can be considered as aiming at characterizing, by means of predicates, the set of contexts in which the game transformations can be applied safely.

References

1. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *CRYPTO'98*, pages 26–45, 1998.
2. M. Bellare and P. Rogaway. Optimal asymmetric encryption. In *EUROCRYPT'04*, volume 950 of *LNCS*, pages 92–111, 1994.
3. M. Bellare and P. Rogaway. Code-based game-playing proofs and the security of triple encryption. Cryptology ePrint Archive, Report 2004/331, 2004.
4. Mihir Bellare and Phillip Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In *CCS'93*, pages 62–73, 1993.
5. I. Damgard. Towards practical public key systems secure against chosen ciphertext attacks. In *CRYPTO'91*, pages 445–456, 1992.
6. T. Okamoto and D. Pointcheval. React: Rapid enhanced-security asymmetric cryptosystem transform. In *CT-RSA'01*, pages 159–175, 2001.
7. D. Pointcheval. Chosen-ciphertext security for any one-way cryptosystem. In *PKC'00*, pages 129–146, 2000.
8. V. Shoup. Oaep reconsidered. *J. Cryptology*, 15(4):223–249, 2002.
9. V. Shoup. Sequences of games: a tool for taming complexity in security proofs, 2004. URL: `http://eprint.iacr.org/2004/332`.
10. D. Soldera, J. Seberry, and C. Qu. The analysis of zheng-seberry scheme. In *ACISP*, volume 2384 of *LNCS*, pages 159–168, 2002.
11. Y. Zheng and J. Seberry. Immunizing public key cryptosystems against chosen ciphertext attacks. *J. on Selected Areas in Communications*, 11(5):715–724, 1993.