Strong security notions for Public Key Cryptographic Primitives

Manuel Bernardo Barbosa
DI/CCTC, Universidade do Minho

December 2010

Context

Fischlin [5] has considered the problem of using public key encryption schemes to build non-malleable commitment schemes. It has been shown that the standard definition of non-malleability is not sufficient for this application and that a stronger variant, referred to as *complete non-malleability*, is required. This security definition allows the adversary to maul the challenge public key, as well as the ciphertext. Put differently, the adversary can output a related ciphertext under a new public key of its choice. Unlike standard non-malleability, it has been shown that completely non-malleable schemes are hard to construct.

Complete non-malleability has recently been shown to be equivalent to *indistinguishability under strong chosen-ciphertext attacks* [2]. This model enhances the adversary's capabilities to forge public keys and ask the decryption oracle to provide decryptions under the corresponding (possibly unknown) secret keys. The authors in [3] formalise *strong plaintext awareness* and *secret key awareness* and show that if such properties are realisable, then they are viable ways to construct strongly chosen-chiphertext secure public-key encryption schemes. Still, it remains an open problem to construct an efficient scheme that achieves these new security notions in the standard model.

Alternative strong security models for public key primitives are being pursued with different motivations. For example, security under related key attacks [1] aims to ensure protection against utilizations of an encryption scheme where several related keys may be used in a protocol. In a different

direction, robust public key encryption [4] aims to thwart attacks that rely on the ability to construct ciphertexts that are valid for different users.

Objectives

One question that naturally arises when so many different security models are being considered is how do these models relate to each other, and whether it is possible to unify them under a single (simpler) definition of security. Furthermore, these new security models pose interesting challenges in terms of constructing new practical schemes that satisfy them. The goal of this proposal is to address these open problems.

References

[1] B. Applebaum, D. Harnik and Y. Ishai. Semantic Security Under Related-Key Attacks and Applications. Cryptology ePrint Archive, Report 2010/544, 2010.

[2] M. Barbosa and P. Farshim. Relations among notions of complete non-malleability: Indistinguishability characterisation and efficient construction without random oracles. ACISP 2010, Lecture Notes in Computer Science, 2010.

[3] M. Barbosa and P. Farshim. Strong Extractors for Public Key Encryption Schemes. ACISP 2010, Lecture Notes in Computer Science, 2010.

[4] M. Abdalla, M. Bellare and G. Neven. Robust Encryption. Cryptology ePrint Archive, Report 2008/440, 2008.

[5] M. Fischlin. Completely non-malleable schemes. In L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, editors, *ICALP*, vol. 3580 of *LNCS*, pp. 779–790. Springer, 2005.