Cryptanalysis vs. Provable Security

Phong Q. Nguyen

INRIA, France and Tsinghua University, China
http://www.di.ens.fr/~pnguyen/

Abstract. In 2004, Koblitz and Menezes started [2] a series of papers questioning the methodology and impact of provable security. We take another look, by comparing cryptanalysis results and provable security results on a variety of topics. We argue that security is complex, and that there is much to gain from better interaction between cryptanalysis and provable security.

Security evaluations of cryptographic schemes or protocols used to be exclusively based on cryptanalysis. A cryptosystem was deemed secure if no efficient attack was known. This traditional approach has obvious limitations: if there is no attack today, it does not imply that there will not be an attack tomorrow, as the history of cryptography has shown repeatedly. Nevertheless, cryptographic key sizes and parameters are still routinely selected based on the state-of-the-art in cryptanalysis.

The field of provable security was developed to provide a new kind of insurance. Its goal is to mathematically prove security properties: a typical provable security result states that a cryptographic scheme A is secure in the security model B, provided that a set C of assumptions hold. Here, an element of C could be a computational assumption – *e.g.* factoring is hard, or a security assumption on a given primitive or protocol – *e.g.* AES is a pseudo-random permutation. That such kinds of statements can be proved is fascinating, and represents a major achievement of theoretical cryptography. Yet, this approach also has well-known limitations, see for instance [2,1,4,5]. In particular, there are provably-secure cryptosystems which were later shown to be insecure, in practice and/or in theory, for various reasons.

These limitations do not mean that one should/could ignore cryptanalysis or provable security. On the contrary, it serves as a reminder that cryptographic security is complex, and that if one is interested in actual security, one should gather as much information as possible, from both cryptanalysis and provable security, without ignoring one or the other. We illustrate this point with several examples from the past thirty years.

We argue that there are a lot of similarities between cryptology and physics. Both use a lot of mathematics, but neither is part of mathematics. Physics aims at discovering the laws of nature and understanding how the physical world works, but we can never know for sure if our theories are correct: we can only tell if our theories are consistent with state-of-the-art experiments. We invent theoretical models to capture reality better and better, but this might be a

C.-K. Wu, M. Yung, and D. Lin (Eds.): Inscrypt 2011, LNCS 7537, pp. 22–23, 2012.
© Springer-Verlag Berlin Heidelberg 2012

never-ending work in progress: even if we find the right theory of everything in theoretical physics, we will never know for sure if it is the right one. Similarly, cryptology aims at achieving security, but in some sense, we never know if something is really secure in the real world, especially in the long term. We keep refining our security models, *e.g.* to take into account side-channel attacks. At best, we can say that something is theoretically secure within a certain security model, or that something seems to be secure in practice for now.

Finally, we argue that there is much to gain from better interaction/dialogue between cryptanalysis and provable security. A security proof can help cryptanalysts to identify weak points: for instance, if the security model or the assumption seems to be unreasonable in practice, this could be the starting point for an attack. Reciprocally, cryptanalysis can help provable security by playing a rôle similar to experiments in physics.

References

1. Chatterjee, S., Menezes, A., Sarkar, P.: Another Look at Tightness. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 293–319. Springer, Heidelberg (2012)
2. Koblitz, N., Menezes, A.: Another look at "provable security". IACR Cryptology ePrint Archive, 2004:152 (2004); Published in [3], All papers available at `http://anotherlook.ca/`, the most recent ones being [1,4]
3. Koblitz, N., Menezes, A.: Another look at "provable security". J. Cryptology 20(1), 3–37 (2007)
4. Koblitz, N., Menezes, A.: Another look at HMAC. IACR Cryptology ePrint Archive, 2012:74 (2012)
5. Leurent, G., Nguyen, P.Q.: How Risky Is the Random-Oracle Model? In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 445–464. Springer, Heidelberg (2009)