Optimal Assymetric Encryption Padding (OAEP): an overview

Victor Glazer

May 10, 2005

1 A Historical Overview

When *chosen-ciphertext security* (or, equivalently, *non-malleability*), now recognized as the "right" notion of security for public-key cryptosytems, was first introduced in [RS92] and [**?**], the "proof-of-concept" cryptosystems presented in both papers were hopelessly inefficient. A practical, efficient public key cryptosystem provably secure against chosen-ciphertext attack under standard hardness assumptions (in this case, the Decisional Deiffie-Hellman assumption) wasn't presented in [CS98]. In the meantime several ad hoc, supposedly chosen-ciphertext secure cryptosystems (which we won't enumerate here) were proposed, some of them later broken.

References

[CS98] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology—CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25. Springer-Verlag, 1998.

[RS92] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology—CRYPTO '92*, pages 433–444. Springer-Verlag, 1992.