

io-port 02236201**Jarecki, Stanisław; Saxena, Nitesh****Further simplifications in proactive RSA signatures.**

Kilian, Joe (ed.), Theory of cryptography. Second theory of cryptography conference, TCC 2005, Cambridge, MA, USA, February 10–12, 2005. Proceedings. Berlin: Springer (ISBN 3-540-24573-1/pbk). Lecture Notes in Computer Science 3378, 510-528 (2005).

Summary: We present a new robust proactive (and threshold) RSA signature scheme secure with the optimal threshold of $t < n/2$ corruptions. The new scheme offers a simpler alternative to the best previously known (static) proactive RSA scheme given by *T. Rabin* [Lect. Notes Comput. Sci. 1462, 89–104 (1998; Zbl 0931.94037)], itself a simplification over the previous schemes given by *Y. Frankel* et al. [Lect. Notes Comput. Sci. 1294, 440–454 (1997; Zbl 0882.94020)]. The new scheme is conceptually simple because all the sharing and proactive re-sharing of the RSA secret key is done modulo a prime, while the reconstruction of the RSA signature employs an observation that the secret can be recovered from such sharing using a simple equation over the integers. This equation was first observed and utilized by Luo and Lu in a design of a simple and efficient proactive RSA scheme [<http://citeseer.ist.pou.edu/luo00ubiquitous.html>] which was not proven secure and which, alas, turned out to be completely insecure [ACT 1 Workshop on Security of Ad Hoc and Sensor Networks (SASN), 1–9, October 2004] due to the fact that the aforementioned equation leaks some partial information about the shared secret. Interestingly, this partial information leakage can be proven harmless once the polynomial sharing used by [<http://citeseer.ist.pou.edu/luo00ubiquitous.html>] is replaced by top-level additive sharing with second-level polynomial sharing for back-up. Apart of conceptual simplicity and of new techniques of independent interests, efficiency-wise the new scheme gives a factor of two improvement in speed and share size in the general case, and almost a factor of four improvement for the common RSA public exponents 3, 17, or 65537, over the scheme of [loc. cit.] as analyzed in [loc. cit.]. However, we also present an improved security analysis and a generalization of the [loc. cit.] scheme, which shows that this scheme remains secure for smaller share sizes, leading to the same factor of two or four improvements for that scheme as well.

doi:10.1007/b106171