Des. Codes Cryptogr. (2011) 58:219
DOI 10.1007/s10623-010-9426-4

ERRATUM

Erratum to: A variant of Digital Signature Algorithm

Dimitrios Poulakis

Published online: 28 August 2010

Erratum to: Des. Codes Cryptogr. (2009) 51:99–104
DOI 10.1007/s10623-008-9246-y

In the above mentioned paper we have described a variant of DSA set in a subgroup of $\mathbb{Z}_n^*$, where $n = pq$ is the product of two large primes which are kept secret. As is pointed out in Mathematical Reviews (MR2480691) there is a flaw in the description since the verifier must know the order of this subgroup in order to compute S_p^{-1} and S_q^{-1} required for the verification procedure.

We can correct this point as follows. The signer computes $S_p^{-1} \bmod \pi_p$ and $S_q^{-1} \bmod \pi_q$ and the signature of a message x is (R, S_p^{-1}, S_q^{-1}) instead of (R, S_p, S_q). The verifier can now perform the verification and the security analysis still stands.

Communicated by P. Wild.

The online version of the original article can be found under doi:10.1007/s10623-008-9246-y.

D. Poulakis (✉)
Department of Mathematics, Aristotle University of Thessaloniki, Thessaloniki 54124, Greece
e-mail: poulakis@math.auth.gr