BMGL—Intellectual Property Issues

As far as we have been able to tell, neither the Blum-Micali, nor the Goldreich-Levin construction are covered by patents. The AES algorithm Rijndael is, by written statements from the Rijndael design team (available from NIST’s homepage), free to use.

We, the BMGL submitters, have no patent or IPR claims related to the proposed construction.

On behalf of the submitters
Stockholm, October 2000
Mats Näslund