References

[1] Ronald L. Rivest and Adi Shamir. Efficient factoring based on partial information. In *Proceedings of Advances in Cryptology-Eurocrpyt '85*, volume 219 of *LNCS*, pages 31–34. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong, 1986.