On some exponential sums over Z_m

John Friedlander (frdlndr@math.utoronto.ca)
University of Toronto
Department of Mathematics
Toronto, ON M5S 3G3
Canada

Abstract. We discuss recent joint work with S. Konyagin and I. Shparlinski in which we estimate some exponential sums motivated by cryptographic considerations. The results extend to general modulus m earlier bounds which were developed for moduli of special type.