Getting a Few Things Right and Many Things Wrong

Neal Koblitz

Department of Mathematics
University of Washington
Seattle, Washington 98195-4350, Seattle, USA
koblitz@math.washington.edu

Abstract. The history of cryptography from ancient times to the present is full of tales of blunders and oversights, typically occurring when an over-confident encryptor is outwitted by a patient and clever cryptanalyst. In contrast, mathematics (if properly peer-reviewed) is perfect. There is never error, because by definition one cannot prove a theorem if it is false. So in order to remove the contingent and subjective elements from cryptography there have been concerted efforts in recent years to transform the field into a branch of mathematics, or at least a branch of the exact sciences. In my view, this hope is misguided, because in its essence cryptography is as much an art as a science.

I will start by describing a setting (taken from a recent paper written with Alfred Menezes and Ann Hibner Koblitz) in which the conventional wisdom about parameter selection might (or might not) be wrong. Then I will illustrate the pitfalls of working in cryptography by giving a (far from exhaustive) survey of the many misjudgments I have made and erroneous beliefs I have had over the course of 25 years working in this field. I will then describe a few of the embarrassing moments in the history of "provable security", which is the name of an ambitious program that aims to transform cryptography into a science.

G. Gong and K.C. Gupta (Eds.): INDOCRYPT 2010, LNCS 6498, p. 1, 2010.