J. Cryptology (2004) 17: 233
DOI: 10.1007/s00145-004-1704-8

Journal of
CRYPTOLOGY

© 2004 International Association for Cryptologic Research

Preface

Arjen K. Lenstra
Lucent Technologies, Room 2T-504,
600 Mountain Avenue, P.O. Box 636,
Murray Hill, NJ 07974-0636, U.S.A.
akl@lucent.com

It is well known that the discrete logarithm problem in the group of a supersingular elliptic curve over a finite field can be solved in subexponential time. This result, often referred to as the MOV embedding and dating back to at least 1993, is based on the Weil pairing. Despite this early cryptanalytic success, it was not until recently that the more general cryptologic applicability of pairings was widely recognized. These days, the bilinear map that the pairing gives rise to is regarded as one of the basic tools that are at any cryptographer's disposal—with no need to understand or fully appreciate its mathematical intricacies. Using pairings has become a mainstream cryptologic activity.

This issue of the *Journal of Cryptology* collects four of the most recent papers in the new wave of cryptologic interest in pairings. The papers by Antoine Joux, Eric Verheul, Dan Boneh, Ben Lynn, and Hovav Shacham, and Paulo Barreto, Ben Lynn, and Michael Scott are final versions of papers that appeared in various conference proceedings. Furthermore, Victor Miller was invited to contribute an introductory paper describing his 1985 algorithm for the efficient calculation of the Weil pairing. Although generally regarded as one of the "classical" results in this area, it has not appeared before.

The timely cooperation of all authors and reviewers for this special issue is gratefully acknowledged.