ANOTHER LOOK AT NON-STANDARD DISCRETE LOG AND DIFFIE-HELLMAN PROBLEMS

NEAL KOBLITZ AND ALFRED MENEZES

ABSTRACT. We examine several versions of the one-more-discrete-log and one-more-Diffie-Hellman problems. In attempting to evaluate their intractability, we find conflicting evidence of the relative hardness of the different problems. Much of this evidence comes from natural families of groups associated with curves of genus 2, 3, 4, 5, and 6. This leads to questions about how to interpret reductionist security arguments that rely on these non-standard problems.