1071-94-114 **Dima Grigoriev** and **Vladimir Shpilrain***, Department of Mathematics, The City College of New York, New York, NY 10031. *Cryptography without one-way functions.*

We show that some problems in cryptography can be solved without using one-way functions. The latter are usually regarded as a central concept of cryptography, but the very existence of one-way functions depends on difficult conjectures in complexity theory, most notably on the notorious "$P \neq NP$" conjecture. This is why cryptographic primitives that do not employ one-way functions are often called "unconditionally secure". Here we suggest protocols for secure computation of the sum, product, and some other functions of two or more elements of an arbitrary constructible ring, without using any one-way functions. A new input that we offer here is that, in contrast with other proposals, we conceal "intermediate results" of a computation. For example, when we compute the sum of k numbers, only the final result is known to (one of) the parties; partial sums are not known to anybody. Other applications of our method include voting/rating over insecure channels and a rather elegant and efficient solution of the "two millionaires problem". We also propose a secret sharing scheme where an advantage over Shamir's and other known secret sharing schemes is that nobody, including the dealer, ends up knowing the shares (of the secret) owned by any particular player. (Received February 26, 2011)