Separation Results on the "One-More" Computational Problems

Emmanuel Bresson[1], Jean Monnerat[2,⋆], and Damien Vergnaud[3]

[1] DCSSI Crypto Lab, Paris, France
[2] Department of Computer Science & Engineering, University of California San Diego, USA
[3] École Normale Supérieure – C.N.R.S. – I.N.R.I.A.
45 rue d'Ulm, 75230 Paris CEDEX 05, France

Abstract. In 2001, Bellare, Namprempre, Pointcheval and Semanko introduced the notion of *"one-more" computational problems*. Since their introduction, these problems have found numerous applications in cryptography. For instance, Bellare *et al.* showed how they lead to a proof of security for Chaum's RSA-based blind signature scheme in the random oracle model.

In this paper, we provide separation results for the computational hierarchy of a large class of algebraic "one-more" computational problems (*e.g.* the one-more discrete logarithm problem, the one-more RSA problem and the one-more static Computational Diffie-Hellman problem in a bilinear setting). We also give some cryptographic implications of these results and, in particular, we prove that it is very unlikely, that one will ever be able to prove the unforgeability of Chaum's RSA-based blind signature scheme under the sole RSA assumption.

Keywords: "One-more" problems, Black-box reductions, Random self-reducible problems, Algebraic algorithms.

1 Introduction

BACKGROUND. In cryptography, a one-way function f is a function that can be computed by some algorithm in polynomial time (with respect to the input size) but such that no probabilistic polynomial-time algorithm can compute a preimage of $f(x)$ with a non-negligible probability, when x is chosen uniformly at random in the domain of f. At the very beginning of the century, it has been observed that there seems little hope of proving the security of many cryptographic constructions based only on the "standard" one-wayness assumption of the used primitive. The security of some schemes seems to rely on different, and probably stronger, properties of the underlying one-way function. Cryptographers have therefore suggested that one should formulate explicit new computational problems to prove the security of these protocols. For instance, Okamoto and Pointcheval [14] introduced in 2001 a novel class of computational problems, the *gap problems*, which find a nice and rich practical instantiation with the Diffie-Hellman problems. They used the gap Diffie-Hellman problem for solving a more than 10-year old open security problem: the unforgeability of Chaum-van Antwerpen undeniable signature scheme [11].

⋆ Supported by a fellowship of the Swiss National Science Foundation, PBEL2–116915.

T. Malkin (Ed.): CT-RSA 2008, LNCS 4964, pp. 71–87, 2008.

In 2001, Bellare, Namprempre, Pointcheval and Semanko [2] introduced the notion of *one-more one-way function*. A function is one-more one-way if it can be computed by some algorithm in polynomial time (in the input size) but for which there exists no probabilistic polynomial-time algorithm $\mathcal{A}$ with non-negligible probability to win the following game:

- $\mathcal{A}$ gets the description of f as input and has access to two oracles;
- an *inversion* oracle that given y in f's codomain returns x in f's domain such that $f(x) = y$;
- a *challenge* oracle that, each time it is invoked (it takes no inputs), returns a random challenge point from f's codomain;
- $\mathcal{A}$ wins the game if it succeeds in inverting all n points output by the challenge oracle using strictly less than n queries to the inversion oracle.

Bellare *et al.* showed how these problems lead to a proof of security for Chaum's RSA-based blind signature scheme [10] in the random oracle model.

The approach consisting in introducing new computational problems to study the security of cryptosystems is not completely satisfactory since the proof of security often relies on an extremely strong assumption which is hard to validate. Nevertheless, it is better to have such a security argument than nothing since as mentioned in [2]: "*These problems can then be studied, to see how they relate to other problems and to what extent we can believe in them as assumptions.*" The purpose of this paper is to study the hierarchy of the computational difficulty of the "one-more" problems of Bellare *et al.* and its cryptographic implications. In particular, we prove that it is very unlikely, that one will ever be able to prove the unforgeability of Chaum's RSA-based blind signature scheme under the sole RSA assumption.

RELATED WORK. Since the one-more-inversion problems were introduced in [2], they have found numerous other applications in cryptography.

- Bellare and Palacio [4] proved in 2002 that Guillou-Quisquater and Schnorr identification schemes [12,17] are secure against impersonation under active (and concurrent) attack under the assumption that the *one-more* RSA *problem* and the *one-more discrete logarithm problem* are intractable (respectively).
- Bellare and Neven [3] proved the security of an RSA based transitive signature scheme suggested by Micali and Rivest in 2002 [13] under the assumption of the hardness of the one-more RSA problem.
- Bellare and Sandhu had used the same problem to prove the security of some two-party RSA-based signature protocols [5].
- In [6], Boldyreva proposed a new blind signature scheme – based on Boneh-Lynn-Shacham signature [7] – which is very similar to the RSA blind signature protocol. She introduced a new computational problem: the *one-more static Computational Diffie-Hellman problem* (see also [9]) and proved the security (in the random oracle model) of her scheme assuming the intractability of this problem.
- Paillier and Vergnaud [15] provided evidence that the security of Schnorr signatures [17] cannot be equivalent to the discrete log problem in the standard model. They proposed a method of converting a reduction of the unforgeability of this signature scheme to the discrete logarithm problem into an algorithm solving the