Об эквивалентности задачи RSA и факторизации

Игорь Туфанов, группа 246, осенний семестр 2008

Задачей RSA называют задачу расшифровки сообщения, закодированного с помощью RSA, открытый ключ считается известным. Вопрос об эквивалентности задачи RSA и задачи факторизации (разложения числа на простые множители) остается открытым и по сей день.

Соображения в пользу эквивалентности

Вопрос об эквивалентности этих задач возникает в связи с очевидным фактом — из существования эффективного алгоритма факторизации следует существование эффективного алгоритма решения задачи RSA. Достаточно разложить число N из открытого ключа на простые множители p, q и отсюда найти $\phi(N)$, по которому для экспоненты шифрования e легко вычисляется экспонента дешифрования d (например, с помощью расширенного алгоритма Евклида). Здесь считается, что операции возведения в степень и нахождения d так же эффективны.

Кроме того, доказано, что и задача RSA, и задача факторизации принадлежат одному классу временной сложности. Каждая из них одновременно NP и $co-NP$. Доказательство этого факта заключается в постороении соответствующих недетерминированных машин Тьюринга.

Соображения против эквивалентности

Боней (Boneh) и Венкатесан (Venkatesan) показали, что для RSA с маленькой экспонентой (то есть с ключем шифрования e меньше фиксированной константы) решение задачи RSA проще, чем решение задачи факторизации. Ими показано, что в этих случаях существование оракула для решения RSA не влечет к существованию оракула для факторизации. После выхода их статьи в 1998 году математики стали склоняться к мнению о том, что эти две задачи не эквивалентны, и задача RSA проще, то есть ее решение не приблизит нас к решению задачи факторизации.

Список источников

- "Криптография" , Н. Смарт, 2005
- "Breaking RSA may not be equivalent to factoring" , D. Boneh, R. Venkatesan, Lecture Notes in Computer Science 1403, Advances in Cryptology - EUROCRYPT'98, p59-71
- "Recent Advances in RSA Cryptography" , S. Katzenbeisser, 2001