Критические замечания по разделу, озаглавленному "Нанотехнологии в криптоанализе"

А. Э. Растегин
кафедра теоретической физики, Иркутский государственный университет
бульвар Гагарина 20, Иркутск 664003, Россия
e-mail: rast@api.isu.ru

Раздел, озаглавленный "Нанотехнологии в криптоанализе", содержит множество вводящих в заблуждение и несостоятельных утверждений. В этой связи необходимо отметить следующее.

1. Название раздела "Нанотехнологии в криптоанализе" не соответствует его содержанию. Фактически, в данном разделе просто упоминается о квантовом алгоритме факторизации целых чисел. Поэтому адекватным названием было бы "Перспективы использования квантовых компьютеров в криптоанализе" или что-то аналогичное. Кроме того, на сегодня даже с экспериментальной точки зрения разработки в сфере нанотехнологий и имеющиеся попытки реализации квантовых вычислений практически мало связаны друг с другом. Заглавие "Нанотехнологии в криптоанализе" для раздела о квантовых вычислениях указывает на полную некомпетентность автора (авторов) как в области нанотехнологий, так и в вопросах квантовых вычислений.

2. В контексте тематики раздела, предложение "С помощью квантового компьютера можно проводить вычисления, не реализуемые на сегодняшних (классических) компьютерах" является безграмотным и неадекватным. Принимая такое заявление, мы вынуждены будем считать, что на сегодняшних компьютерах невозможно факторизовать целые числа. В действительности же речь должна идти о том, что для некоторых задач известны квантовые алгоритмы, работающие экспоненциально быстро по сравнению с имеющимися алгоритмами для классических компьютеров. Для факторизации целых чисел разработано множество нетривиальных алгоритмов, например: ρ-метод Полларда и $(p-1)$-метод Полларда, метод квадратичного решета (QS) и метод решета числового поля (NFS). Значительный прогресс в развитии методов факторизации для обычных компьютеров можно проиллюстрировать таким фактом. Вслед за созданием криптосистемы RSA некоторые специалисты прогнозировали, что факторизация тестового числа RSA129 "займет" 40 квадрильонов лет. На самом деле число RSA129 было разложено на множители методом QS в 1994 г. Хотя все известные "классические" алгоритмы факторизации экспоненциальны либо субэкспоненциальны, они могут вполне успешно использоваться на практике.

3. Среди квантовых алгоритмов, не только алгоритм Шора потенциально важен с точки зрения применений в криптоанализе. Например, вскоре после открытия алгоритма Гровера один из ведущих экспертов по криптографии, Жиль Брассард, показал, как использовать данный алгоритм для эффективной атаки на симметричные криптосистемы, подобные DES. В отношении алгоритма Шора нужно отметить, что его улучшенная версия разлагает n-битовое число (где $n = \lfloor \log N \rfloor + 1$) за время $O\big(n^2 \log n \log\log n\big)$, вместо указанного в тексте $O\big(n^3\big)$.

4. Заявление о том, что "алгоритм Шора чрезвычайно прост и довольствуется гораздо более скромным аппаратным обеспечением", свидетельствует об абсолютном непонимании существа дела. Не углубляясь в описание весьма и весьма нетривиального алгоритма Шора, сделаем лишь одно принципиальное замечание. Всякое реальное устройство работает с ошибками и подвержено воздействию шума. Для квантовых компьютеров эти проблемы качественно иного уровня сложности, чем в случае обычных компьютеров. Действительно, лежащие в основе "квантового параллелизма" нелокальные корреляции чрезвычайно чувствительны к внешнему воздействию. Теоретически, разработаны и продолжают разрабатываться определенные методы проведения отказоустойчивых квантовых вычислений. Но это сопряжено с довольно существенным расширением и даже изменением исходной квантовой схемы, реализующей тот или иной алгоритм. Так или иначе, мнение об "аппаратном обеспечении" конкретного вычисления может быть со-

ставлено только после того, как будут практически реализованы и опробованы квантовые схемы, содержащие реально значимое количество кубитов.

5. Влияние квантовых технологий на криптографию не исчерпывается перспективой использования пока еще не созданных квантовых компьютеров в криптоанализе. Уже в восмидесятых годах прошлого века было показано, что "запутанные" квантовые состояния можно использовать для распределения секретного ключа в реальном времени. Фактически, первая схема BB84 квантовой критографии основана на еще более ранних, тогда не опубликованных, идеях Виснера (высказанных почти одновременно с разработкой системы RSA, сформулированной в статье 1978 г.). В настоящее время квантовая криптография является реально работающей технологией, а квантовые криптосистемы — коммерческим продуктом. К слову, значительная доля работ в этой области контролируется военными и спецслужбами, так что информация о конкретных системах не публикуется. Вот неполный список основных коммерческих квантовых криптосистем и компаний-разработчиков: the system Clavis^2 by id Quantique, web-link http://www.idquantique.com; the systems QPN-8505 and Q-Box by MagiQ Technologies, web-link http://www.magiqtech.com.

Перечисленные выше факты хорошо известны специалистам, но, очевидно, станут сюрпризом для автора (или авторов) указанного псевдонаучного текста.