and Instruments for Information Sharing and Decision-Making against Biological Threats and Pandemics», проведенной 30 ноября — 8 декабря 2008 г. в Милане, Италия [3], и используется в политике междисциплинарной сети информационного обмена [4]. Перспективным представляется дальнейшее совершенствование модели для решения задачи оптимизации распределения средств, направляемых на межведомственное и международное сотрудничество. Обсуждается возможность применения данных техник расчетов для анализа цепей миграции радионуклидов в экосистемах.

СПИСОК ЛИТЕРАТУРЫ:

1. http://www.cs.cmu.edu/~pkeyani/publications/peerpressure.pdf.
2. http://www.pitt.edu/~super1/disasters/disasters.htm.
3. http://www.pitt.edu/~super1/BH/Milan5.html.
4. *Trufanov A., Caruso A., Dmitrienko N., Galindo F., Guidotti M., Gursky E., Kolesnikov S., Laporte R., Linkov F., Ranghieri M., Rossodivita A., Shubnikov E.* Information — Sharing Networks for Global Emergency Medical Services // Abstr. of Scientific and Invited Papers: 16th World Congress for Disaster and Emergency Medicine. Prehosp Disast Med 2009. 24(2). S. 81.

Ю. В. Гель, А. Г. Ростовцев

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ В ГРУППЕ КЛАССОВ ИЗОГЕННЫХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Безопасность существующих криптосистем с открытым ключом базируется на двух обобщенных задачах: дискретное логарифмирование в группе вычислимого порядка (на этой задаче основывается криптосистема Эль-Гамаля, а также стандарт электронной цифровой подписи ГОСТ Р 34.10-2001) и определение порядка и структуры конечной группы (например, задача разложения на множители, на которой основана безопасность криптосистемы RSA).

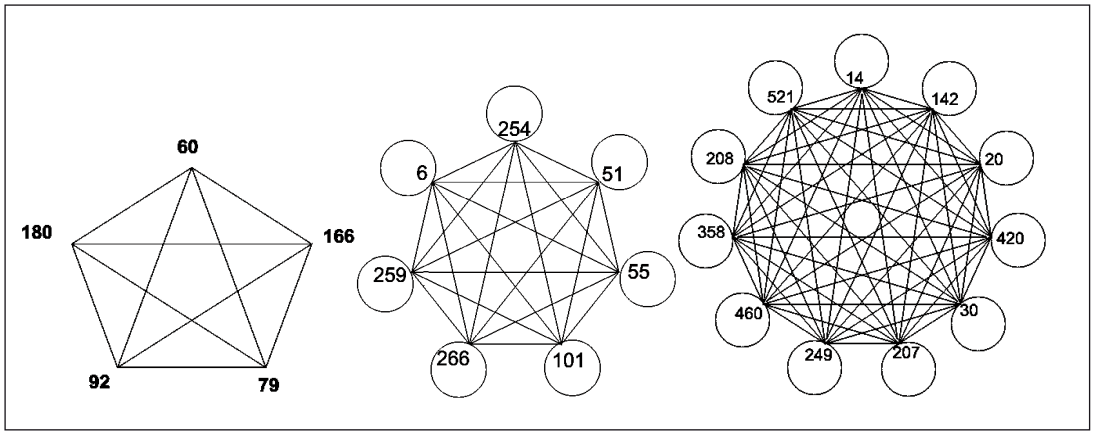
Новый тип вычислительных машин, использующий квантово-механические взаимодействия, может преодолеть многие ограничения для обычных компьютеров. Существуют задачи, которые могут быть решены на квантовом компьютере принципиально быстрее, чем на классическом. Например, разложить число на простые множители или вычислить дискретный логарифм в циклической группе можно с полиномиальной сложностью алгоритмом Шора. Это ставит под угрозу безопасность большинства криптосистем с открытым ключом. В настоящее время компания D-Wave Systems разработала модель квантового компьютера на сверхпроводящих торах разрядностью 512 q-битов.

Таким образом, нужна новая задача, стойкая по отношению к квантовому компьютеру. Один из возможных вариантов решения — использование задачи поиска изогении между эллиптическими кривыми.

Изогения эллиптических кривых — бирациональный гомоморфизм, мощность ядра которого над алгебраически замкнутым полем равна степени изогении. Изогения между эллиптическими кривыми существует тогда и только тогда, когда эти кривые имеют одинаковое число точек, т. е. их инварианты являются корнями одного и того же полинома Гильберта, задающего поле классов мнимого квадратичного порядка для дискриминанта эндоморфизма Фробениуса.

У кривых над полем F_ρ с одинаковым числом точек значение следа эндоморфизма Фробениуса совпадает. Кривые, связанные изогенией простой нечетной степени l, образуют циклы. Группа классов изогений и группа классов идеалов мнимых квадратичных порядков изоморфны, норме идеала соответствует степень изогении. Если число классов велико, то этот изоморфизм не вычислим ни в одну сторону ни на обычном, ни на квантовом компьютере. Сложность описания группы изогенных кривых экспоненциально зависит от размера дискриминанта эндоморфизма Фробениуса и, следовательно, от размера характеристики поля. Элемент группы действует как перестановка на множестве j-инвариантов, при этом описание такой перестановки требует перечисления инвариантов всех изогенных кривых.

Звездой изогенных эллиптических кривых называется граф, состоящий из простого числа изогенных эллиптических кривых, связанных изогениями простых степеней Элксиса. На рисунке представлены примеры звезд с числом классом 5, 7 и 11 соответственно. В вершинах указаны j-инварианты эллиптических кривых.



Путь на звезде определяется как совокупность направленных изогений. Пути обладают свойством коммутативности, что позволяет строить на звезде криптографические примитивы. Направление пути определяется степенью полинома, задающего ядро изогении.

Протокол электронной цифровой подписи базируется на протоколе Шнорра. Ключом подписи является секретный путь. Ключ проверки — j-инвариант эллиптической кривой. Вместо точек эллиптической кривой используются j-инварианты изогенных кривых из группы классов, а вместо сложения точек используется отображение j-инвариантов с помощью изогений малых простых степеней l, для которых дискриминант эндоморфизма Фробениуса является квадратичным вычетом по модулю степени изогении.

Для обеспечения стойкости число классов должно быть простым числом или должно иметь большой простой делитель.