ОТЗЫВ

на автореферат диссертации Высоцкой В.В. на тему: «Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки», представленной на соискание учёной степени кандидата физико-математических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

Диссертация посвящена построению и анализу электронных подписей на кодах. Есть две основные парадигмы построения подписей - "hash & sign" и применение преобразования Фиата-Шамира к протоколу доказательства с нулевым разглашением. В работе исследуются свойства вариаций схемы CFS, построенной на первом подходе (Главы 1-3), и предложена новая схема электронной подписи на основе второго подхода с протоколом идентификации Штерна (Глава 4).

Заметим, что основной недостаток схемы CFS -- медленная генерация подписи, требующая экспоненциального количества операций (в среднем t! операций, где t - вес ошибки). Поэтому схема не применяется на практике и часть диссертационной работы, посвященная вариантам CFS, имеет скорее теоретическую направленность. Более того, диссертационная работа посвящена выбору стойких параметров для разных вариантов схемы CFS и вводит ограничения, которые делают такие схемы ещё менее практичными.

Подписи на основе протокола Штерна (Глава 4) более интересны с практической точки зрения. Основной недостаток подобных схем - большие размеры ключей и подписей. Основной вклад работы - доказательство безопасности схемы в модели EUF-CMA. Практические вопросы оптимизации размеров ключей/подписи не рассматриваются.

В работе присутствуют мелкие ошибки и опечатки:

1. стр. 8 (автореферат), "… $O(2^{28})$ битовых операций вместо $O(2^{256})$" и стр. 10 диссертации.
   - некорректная запись, в О-нотации данные значения равны $O(1)$. Получается, что схему изначально можно было взломать за $O(2^{256})=O(1)$ операций, что неверно.
2. стр. 9 (автореферат):
   - "отказаться от использовать"
   - "разработать новую схемы"

Описанные выше недостатки не умаляют ценности диссертационной работы, так как задача криптоаналитика заключается в поиске схем, подходящих для практического применения и отсечении небезопасных/медленных, что и было выполнено в части по вариациям схемы CFS. А доказательство безопасности схемы подписи, основанной на преобразовании Фиата-Шамира и протоколе Штерна, может использоваться как отправная точка для практических задач.

Учитывая вышеизложенное, считаю, что Высоцкая В.В. заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

к.ф.-м.н., доцент Высшей школы компьютерных наук и искусственного интеллекта Балтийского Федерального университета им. И.Канта

Новоселов Семен Александрович

тел.
236041, г. Калининград, ул. А. Невского 14, корп. 6, каб. 210

Подпись Новоселова С.А. заверяю: