Отзыв официального оппонента

на диссертационную работу Алексеева Максима Олеговича «Методы нелинейного кодирования для повышения достоверности обработки информации», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.01 «Системный анализ, управление и обработка информации (технические системы)»

1 Актуальность темы диссертации

Широкое распространение банковских карт, электронных пропусков, удостоверений, доверенных вычислительных систем и других устройств, призванных обеспечивать защищенные обработку и хранение информации, требует создания методов выявления попыток несанкционированного доступа к данным. С другой стороны, продолжающееся снижение норм технологического процесса повышает уязвимость вычислительных устройств к действию внешних помех, в т.ч. ионизирующего излучения. Для предотвращения случайного искажения информации запоминающие устройства должны быть способны исправлять случайные ошибки. Обе эти задачи могут быть решены с помощью кодов, обнаруживающих или исправляющих алгебраические манипуляции. Диссертация М.О. Алексеева посвящена именно этой, весьма активно исследуемой в настоящее время, проблеме. Таким образом, актуальность темы диссертации не вызывает сомнений.

2 Краткий обзор содержания диссертации

Диссертация состоит из пяти глав и приложения.

В первой главе описана модель канала с алгебраическими манипуляциями и представлены различные сценарии, в которых она может быть применима, в т.ч. воздействие ионизирующего излучения, линейные схемы разделения секрета с мошенниками, различные методы воздействия на защищенные вычислительные устройства. Следует отметить, что далее в диссертации используется только модель канала с алгебраическими манипуляциями, в то время как приведенная в главе информация о различных физических и технических предпосылках их возникновения остается невостребованной.

Во второй главе приведен обзор различных методов повышения помехоустойчивости вычислительных систем. Автор отмечает, что отсутствуют гарантии оптимальности существующих кодов, обнаруживающих алгебраические манипуляции, а также методов их декодирования.

В третьей главе представлена нижняя граница длины систематического R-равномерно надежного кода и показано, что существуют коды, лежащие на этой границе. Автор отмечает, что параметры существующих надежных кодов расходятся с этой границей. В главе также приведена новая нижняя граница обнаруживающей способности AMD кода на базе кода Рида-Маллера, и отмечено, что в некоторых случаях она оказывается выше теоретической границы для AMD-кодов.

В четвертой главе представлена новая конструкция обобщенных систематических надежных кодов, приведены оценки вероятности необнаружения сильных манипуляций. Приведены способы модификации этого кода, позволяющие обеспечивать исправление ошибок кратности 1 и обнаружение ошибок кратности 2. Предложен также метод исправления повторяющихся ошибок. Представлена схема гибридного кодека, обнаруживающего алгебраические манипуляции, который способен обеспечить заданный уровень обнаружения искажений для различных блоков устройства, что позволяет снизить требуемые аппаратные затраты. Представлено также сравнение

предложенных кодов с конструкциями на основе обобщенных кодов Рида-Маллера , линейных кодов и умножения в поле.

Кроме того, представлена конструкция надежного кода на основе экспоненциальной функции, а также ряд модификаций AMD кода, позволяющие гибко выбирать его длину.

Представленные подходы позволяют повысить вероятность обнаружения искажений, а также снизить сложность реализации.

В пятой главе представлены предложения по использованию предлагаемых кодов для защиты от искажений, возникающих в бортовых вычислительных системах космических аппаратов под воздействием ионизирующего излучения, а также архитектуры шифра AES от вычислительных ошибок.

В приложении приведен обзор методов атаки на защищенные вычислительные системы с помощью сторонних каналов сбора информации.

3 Научная новизна и основные результаты исследования

Из приведенного анализа диссертации следует, что представленная работа содержит ряд новых результатов, являющихся заметным вкладом в теорию и практику помехоустойчивого кодирования:

- Конструкция обобщенных систематических надежных кодов и ее модификации с увеличенным минимальным расстоянием.
- Конструкция надежного кода на основе экспоненциальной функции.
- Граница обнаруживающей способности AMD-кода на базе кода Рида-Маллера.
- Граница длины систематического R-равномерно надежного кода.

4 Достоверность и обоснованность основных результатов исследования

Для всех утверждений в работе представлено их строгое доказательство с использованием аппарата алгебры и комбинаторики. Достоверность результатов диссертационной работы подтверждается сопоставлением с опубликованными результатами других исследователей.

5 Теоретическая значимость

Полученные в работе границы могут быть использованы для оценки оптимальности как существующих, так и новых кодовых конструкций. Предложенные в работе кодовые конструкции являются заметным вкладом в теорию кодов, обнаруживающих алгебраические манипуляциию.

6 Практическая ценность работы

Предложенные в работе методы могут быть использованы при разработке доверенных вычислительных систем, а также компонентов оборудования, предназначенных для использования в условиях наличия ионизирующего излучения.

7 Полнота опубликования научных результатов

Результаты диссертационной работы отражены в 12 публикациях, в т.ч. представлен доклад на одной из профильных международных конференций по теории кодирования «Workshop on Coding and Cryptography». Автореферат правильно и в достаточной мере отражает содержание диссертации.

8 Замечания по работе

Тем не менее, необходимо выделить следующие недостатки диссертационной работы:

1. В работе отсутствует сравнение предлагаемых кодов и конструкции, предложенной в работе Sh. Ge, Zh. Wang, M. Karpovsky, P. Luo. Reliable and Secure Memories Based on Algebraic Manipulation Detection Codes and Robust Error Correction. In Proceedings Of DEPEND 2013.
2. Неясно, почему в формуле (3.2), задающей нижнюю границу вероятности ошибки, фигурирует знак ≥, хотя в предшествующих формулах было ≤.
3. Неясно, почему там же используется граница Синглтона, а не, например, Грайсмера.
4. На стр. 65 автор утверждает, что сложность предлагаемого алгоритма существенно уступает аналогам. Вместе с тем, предлагаемый метод использует операцию нахождения обратного элемента в конечном поле. Для больших значений r это может быть весьма трудоемкой операцией.
5. В тексте присутствуют опечатки и неудачные выражения. Например:
   - стр. 39: код не имеет необнаруживаемых ошибок
   - Стр. 45: b≤b-3

9 Заключение

Диссертация Алексеева М.О. «Методы нелинейного кодирования для повышения достоверности обработки информации» является законченной научно-квалификационной работой, выполненной автором на высоком уровне. Работа базируется на достаточном числе исходных данных, примеров и расчетов. По каждой главе и работе в целом сделаны четкие выводы.

Диссертационная работа удовлетворяет критериям п. 9 «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства РФ от 24.09.2013 г. № 842 по специальности 05.13.01 – «Системный анализ, управление и обработка информации (технические системы)», а ее автор Алексеев Максим Олегович заслуживает присвоения ей ученой степени кандидата технических наук по специальности 05.13.01 «Системный анализ, управление и обработка информации (технические системы)».

07.09.2015

Официальный оппонент

Доцент кафедры «Распределенные вычисления и компьютерные сети»

ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого»

К.т.н., доц. Трифонов Петр Владимирович

Подпись П.В. Трифонова
УДОСТОВЕРЯЮ
Ведущий специалист
по кадрам
«7» 09 2015 г.

Сведения о составителе отзыва:
Трифонов Петр Владимирович
Доцент кафедры «Распределенные вычисления и компьютерные сети»
ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого»
Кандидат технических наук, доцент
e-mail: petert@dcn.icc.spbstu.ru
194021, Санкт-Петербург, ул. Политехническая, д. 21

1. В работе отсутствует сравнение предлагаемых кодов и конструкции, предложенной в работе Sh. Ge, Zh. Wang, M. Karpovsky, P. Luo. Reliable and Secure Memories Based on Algebraic Manipulation Detection Codes and Robust Error Correction. In Proceedings Of DEPEND 2013.
2. Неясно, почему в формуле (3.2), задающей нижнюю границу вероятности ошибки, фигурирует знак ≥, хотя в предшествующих формулах было ≤.
3. Неясно, почему там же используется граница Синглтона, а не, например, Грайсмера.
4. На стр. 65 автор утверждает, что сложность предлагаемого алгоритма существенно уступает аналогам. Вместе с тем, предлагаемый метод использует операцию нахождения обратного элемента в конечном поле. Для больших значений r это может быть весьма трудоемкой операцией.
5. В тексте присутствуют опечатки и неудачные выражения. Например:
   - стр. 39: код не имеет необнаруживаемых ошибок
   - Стр. 45: b≤b-3

9 Заключение

Диссертация Алексеева М.О. «Методы нелинейного кодирования для повышения достоверности обработки информации» является законченной научно-квалификационной работой, выполненной автором на высоком уровне. Работа базируется на достаточном числе исходных данных, примеров и расчетов. По каждой главе и работе в целом сделаны четкие выводы.

Диссертационная работа удовлетворяет критериям п. 9 «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства РФ от 24.09.2013 г. № 842 по специальности 05.13.01 – «Системный анализ, управление и обработка информации (технические системы)», а ее автор Алексеев Максим Олегович заслуживает присвоения ей ученой степени кандидата технических наук по специальности 05.13.01 «Системный анализ, управление и обработка информации (технические системы)».

07.09.2015

Официальный оппонент

Доцент кафедры «Распределенные вычисления и компьютерные сети»

ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого»