Методы обеспечения целостности информации на основе вейвлетных преобразований для защиты средств хранения информации

Таранов Сергей Владимирович

Университет ИТМО

План лекции

1. Введение в понятие алгебраических манипуляций (АМ)
2. Использование кодов, обнаруживающих/исправляющих ошибки для защиты от АМ
3. Определение AMD кода
4. Новые конструкции линейных вейвлетных кодов для защиты от АМ
5. Новые конструкции AMD кодов на основе вейвлетных преобразований для защиты от алгебраических манипуляций
6. Области применения

Защита от «алгебраических манипуляций»

- Проблема: Как защитить информацию от ошибок, внедряемых злоумышленником?

- Варианты решения данной проблемы изучаются в криптографии, теории информации и теории кодирования.
  - Какой тип ошибки рассматривается?
  - Какую степень защиты необходимо достичь?
  - Имеется ли возможность использования секретных ключей и псевдослучайных последовательностей?
- Существующие решения: ЦП, MACs, Hash функции, коды, обнаруживающие/исправляющие ошибки.

- **Новые решения:** коды, обнаруживающие искажения (tamper-detection codes); коды, обнаруживающие алгебраические манипуляции (AMD codes); надежные коды (robust codes); коды, ориентированные на безопасность (security-oriented codes).

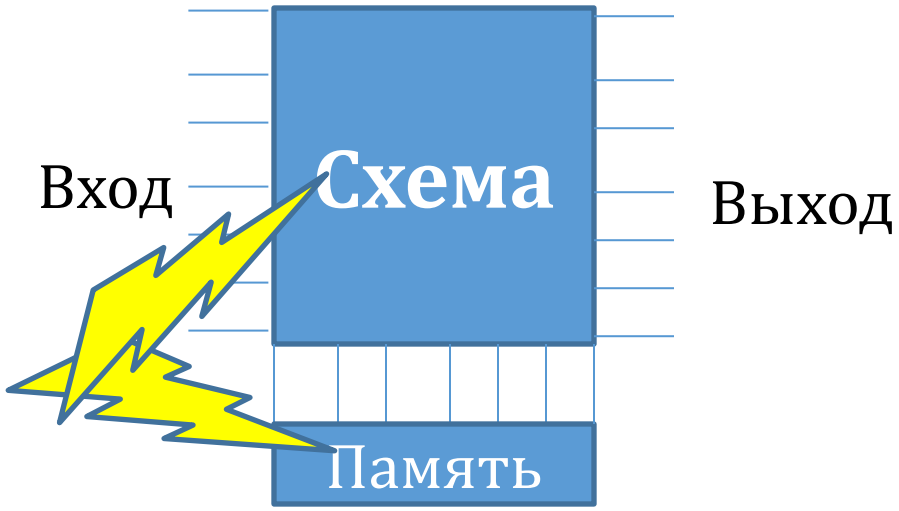
Мотивация: Атаки на аппаратную реализацию устройств

- Реализация криптоалгоритмов для ряда устройств является трудоемкой.
  - Утечка информации по сторонним каналам: Злоумышленник изучает характеристики побочных сигналов, излучаемых устройством.
  - Искажение («алгебраическая манипуляция»): Атакующий может изменить внутреннее состояние устройства и в дальнейшем взаимодействовать с модифицированным устройством.

Мотивация: защита от SCA, направленных на устройства хранения

Внедрение ошибок
в память

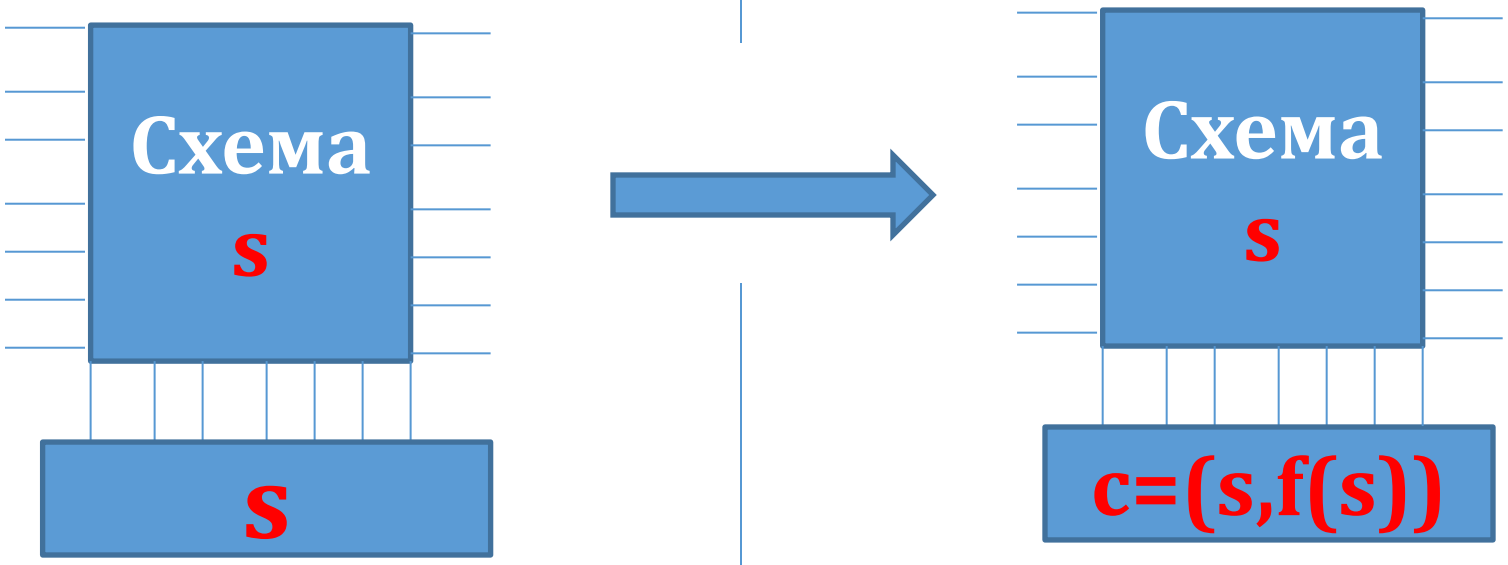
Внедрение ошибок
в память и микросхему



Решение на основе методов помехоустойчивого кодирования

Структура исходной микросхемы (s)

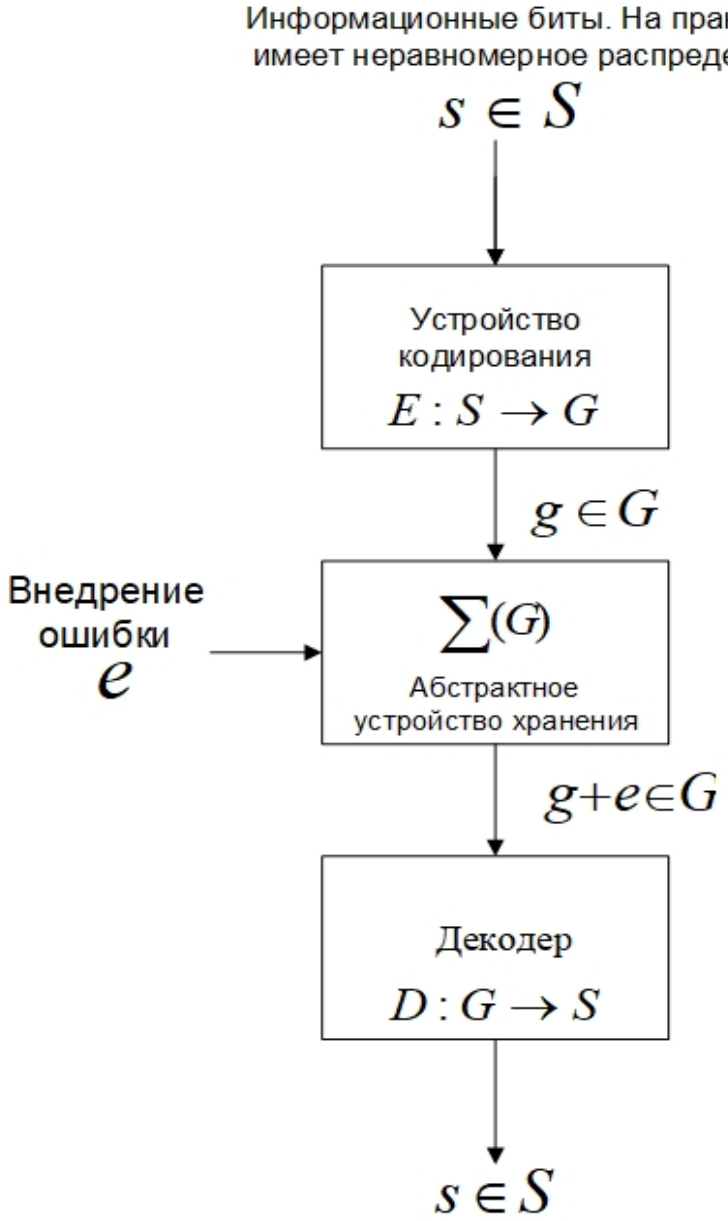
Использование кодирования c=(s, f(s))



План лекции

1. Введение в понятие алгебраических манипуляций (АМ)
2. Использование кодов, обнаруживающих/исправляющих ошибки для защиты от АМ 
3. Определение AMD кода
4. Новые конструкции линейных вейвлетных кодов для защиты от АМ
5. Новые конструкции AMD кодов на основе вейвлетных преобразований для защиты от алгебраических манипуляций
6. Области применения

Модель алгебраических манипуляций



Алгебраические манипуляции не обнаруживаются классическими методами кодирования

Характеристики	Классический подход	Подход с точки зрения безопасности
Тип канала	Передача и хранение данных	Обработка и хранение данных
Характер ошибки	Неантропогенный	Антропогенный
Кратность ошибки	малая кратность	любая кратность
Корреляция между ошибками и данными	Нет	Возможна
Что имеет случайный характер?	Ошибка	Кодовое слово
Что фиксируется?	Кодовое слово	Ошибка
Критерий	Расстояние Хэмминга	Вероятность маскировки ошибки

Вероятность маскировки ошибки

минимизировать $\max_{e \neq 0} Q(e) = \frac{|\{g | g \in C, g+e \in C\}|}{|C|}$

при условии выполнения следующих ***ограничений*** :

1) $e \in GF(q^n), e \neq 0$

2) $\mathrm{s} \in GF\left(q^k\right), \mathrm{g} = (\mathrm{s}, \mathrm{F}(\mathrm{s}))$

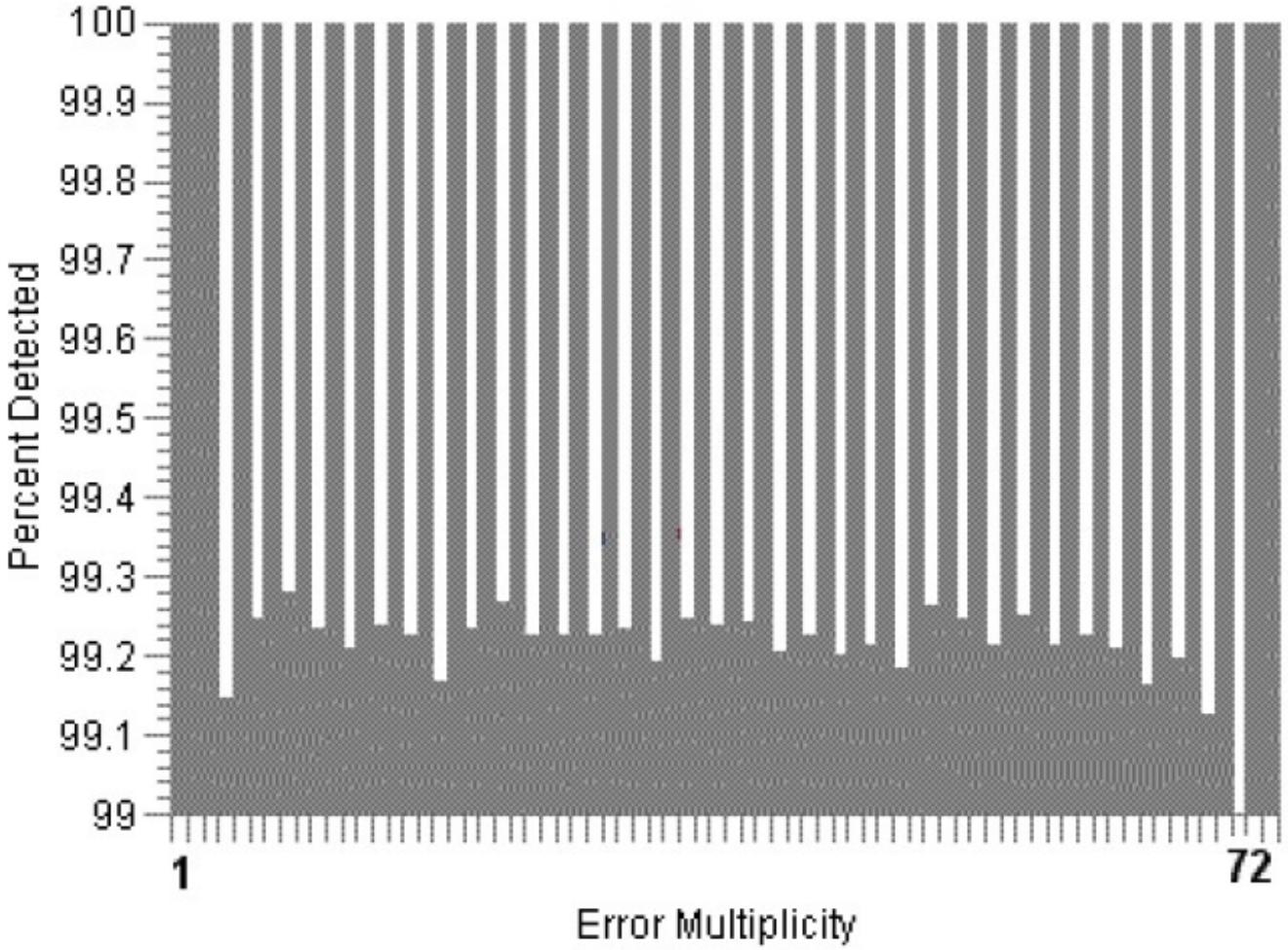
3) Закон распределения входных значений s – может быть неравномерным

4) Равновероятное обнаружение ошибок любой кратности

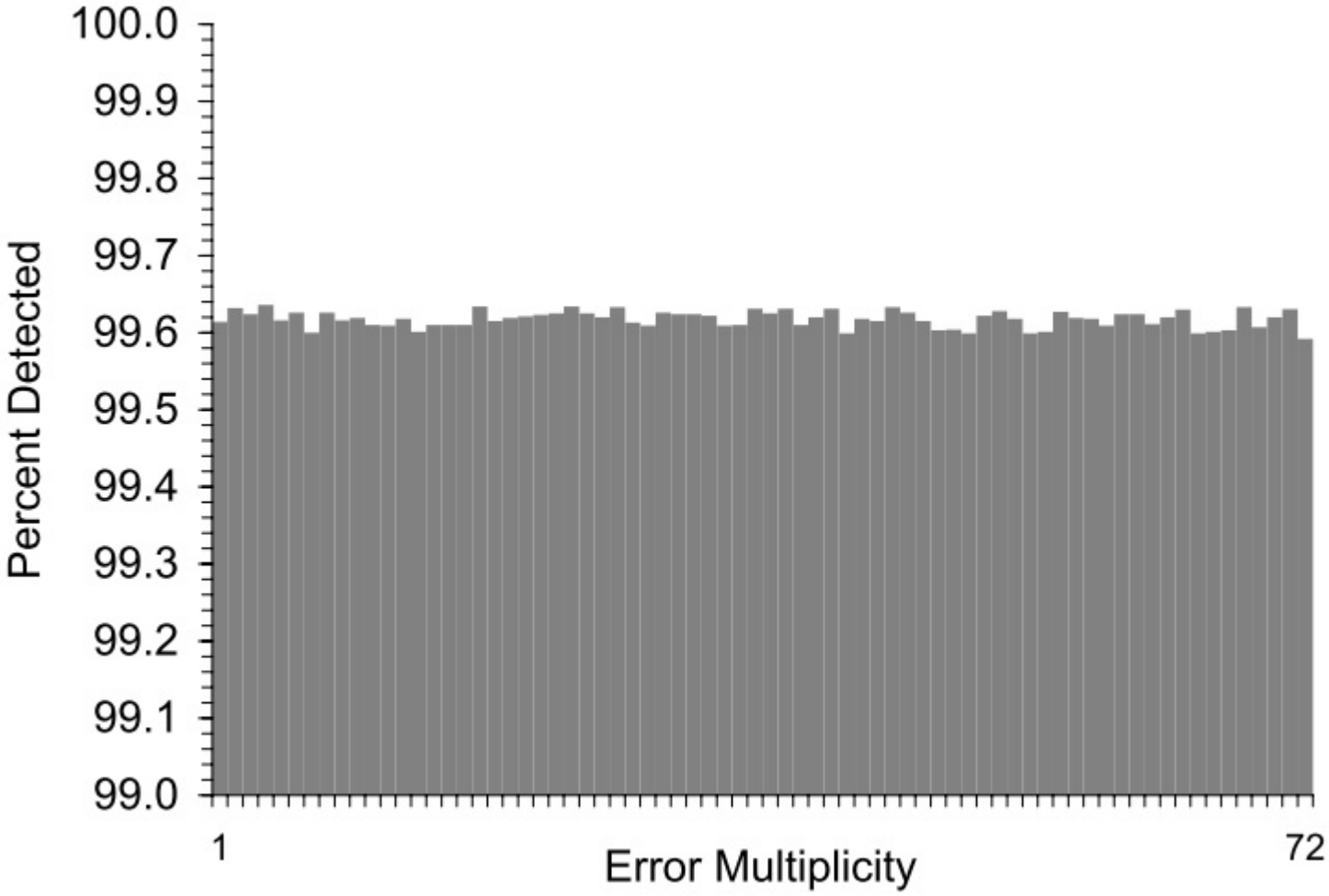
5) Разделяемый, систематический код (избегать модификации информационных символов при возможности)

6) Не использовать ключи и случайные значения в качестве входных параметров

[n=72, M=2^{64}] расширенный код Хэмминга



(n=72, M=2^{64}) надежный квадратичный код



План лекции

1. Введение в понятие алгебраических манипуляций (АМ)
2. Использование кодов, обнаруживающих/исправляющих ошибки для защиты от АМ
3. Определение AMD кода 
4. Новые конструкции линейных вейвлетных кодов для защиты от АМ
5. Новые конструкции AMD кодов на основе вейвлетных преобразований для защиты от алгебраических манипуляций
6. Области применения

Код, обнаруживающий алгебраические манипуляции (AMD код)

Определение (R. Cramer, S. Fehr, and C. Padro. Algebraic manipulation detection codes):

Пусть S будет множеством размера m > 1, G – коммутативной абелевой группой порядка n. Рассмотрим пару функций (E,D), которые представляют собой стохастическую функцию кодирования E : S→G и детерминистскую функцию декодирования D : G → S ∪ {⊥} , такую что D(E(s)) = s с вероятностью 1 для каждого s ∈ S.

Тогда для некоторого ε > 0, AMD код считается ε-надежным, если для каждого s выбранного случайно из S и для каждого δ ∈ G выбранного из G в соответствии с некоторым распределением, которое не зависит от s и E(s), вероятность

$$D(E(s)+\delta) \notin \{s, \perp\}$$ не более ε.

Типы AMD кодов:

1. Линейный код

- Просты в реализации/способны исправлять ошибки
- Обладают множеством необнаруживаемых ошибок
- Неравномерное обнаружение ошибок различной кратности

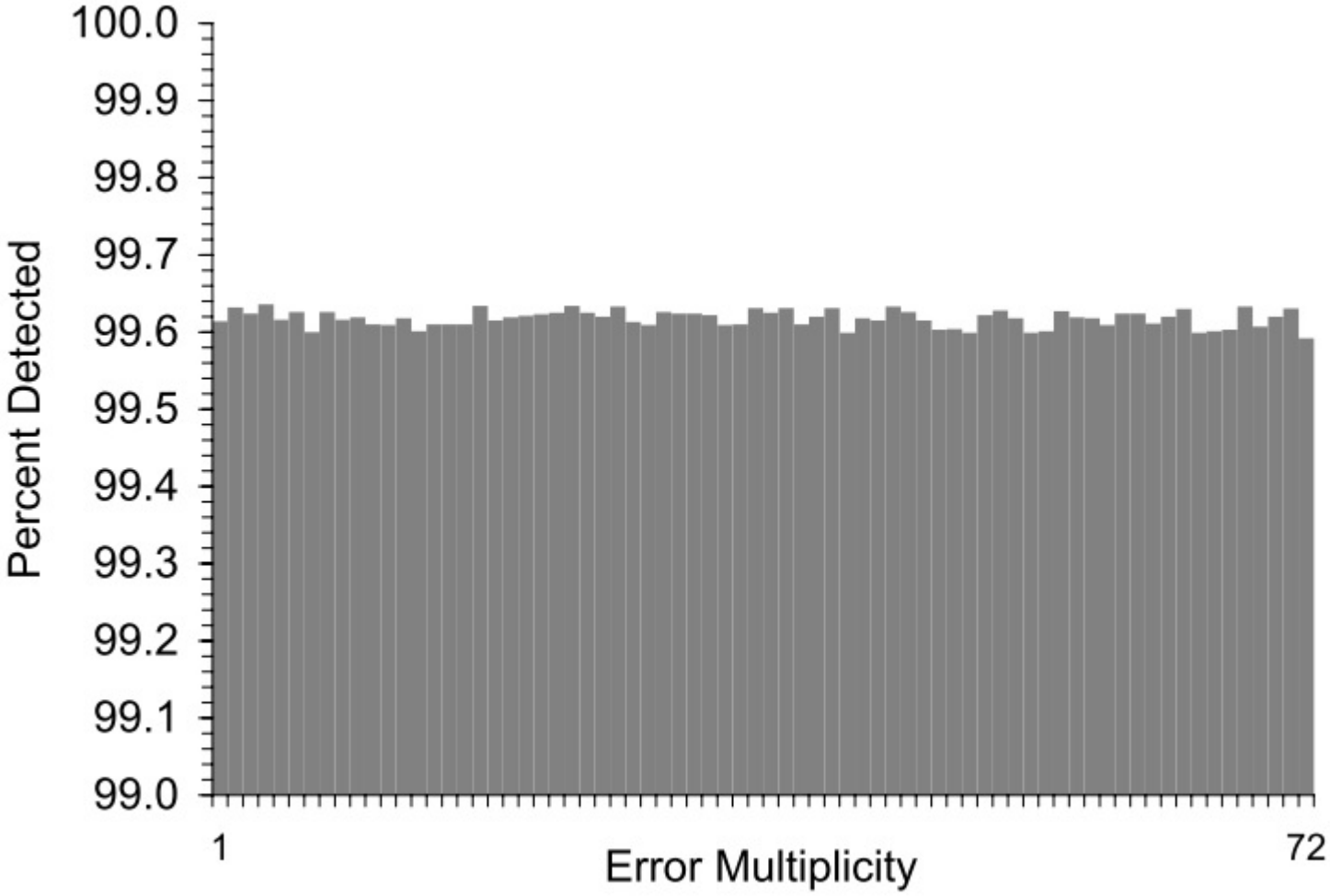
2. AMD код на основе почти совершенно нелинейных функций (APN функций) – x^{-1}, x^3

- Равномерное обнаружения ошибок за исключением тех, которые попадают во множество необнаруживаемых ошибок

3. AMD код на основе совершенно нелинейных функций (PN функций) - xy, xy^{-1}

- Равномерное обнаружения ошибок любой кратности

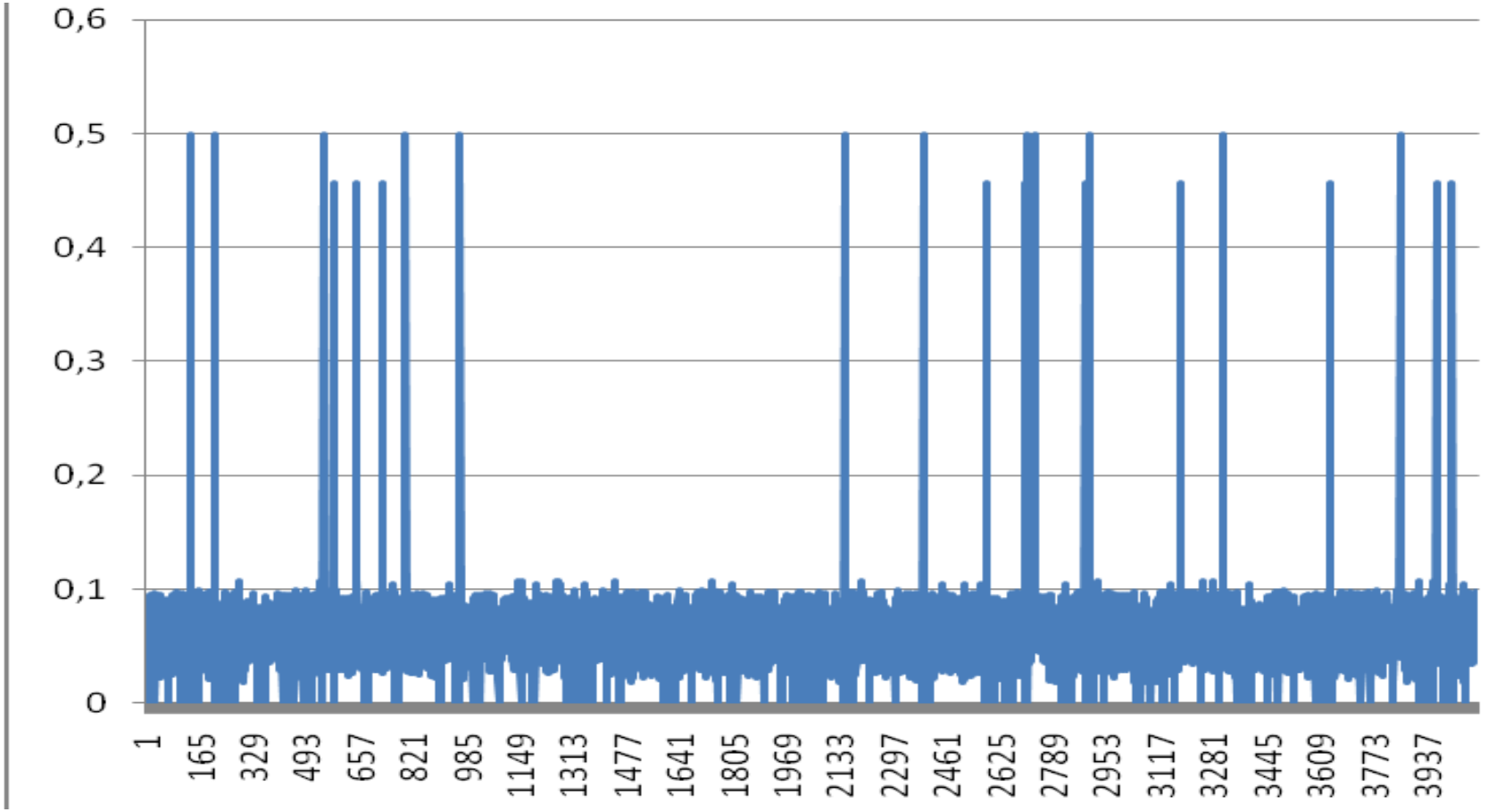
Входные значения s – равномерные!



Чем опасно неравномерное распределение входных значений?

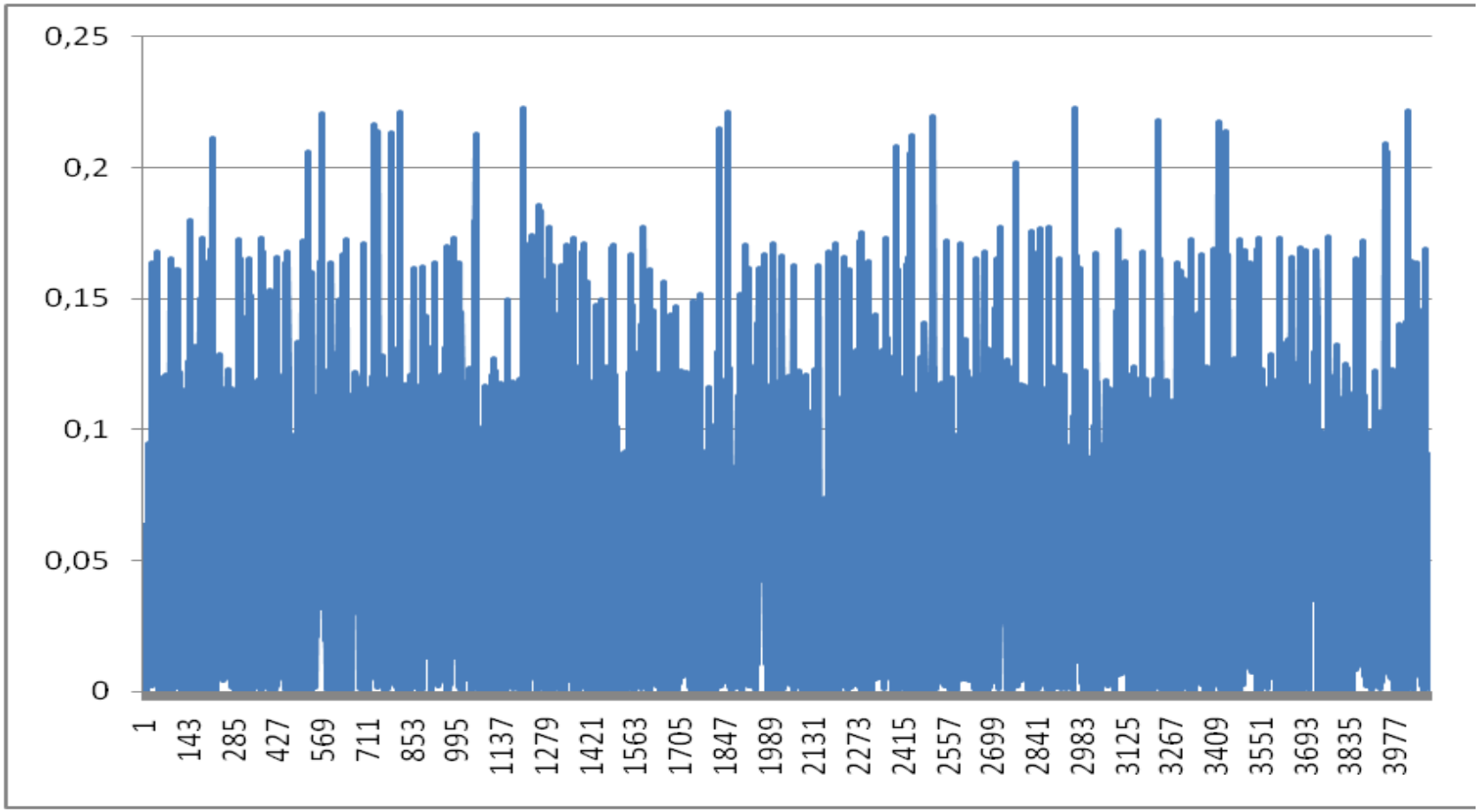
Distribution	$F(x, y) = xy$	$F(x, y) = xy^{-1}$
Uniform distribution	$\max Q(e) = 0.0625$	$\max Q(e) = 0.0625$
Binomial distribution	$\max Q(e) = 0.4987$	$\max Q(e) = 0.2227$
$p_1(c) = \begin{cases} \frac{0.8}{56}, & 51 \le c < 106 \\ \frac{0.2}{200}, & \text{otherwise} \end{cases}$	$\max Q(e) = 0.2285$	$\max Q(e) = 0.1222$
$p_2(c) = \begin{cases} \frac{0.7}{100}, & 101 \le c < 200 \\ \frac{0.3}{156}, & \text{otherwise} \end{cases}$	$\max Q(e) = 0.112$	$\max Q(e) = 0.0917$
$p_3(c) = \begin{cases} \frac{0.1}{150}, & 1 \le c < 150 \\ \frac{0.9}{106}, & \text{otherwise} \end{cases}$	$\max Q(e) = 0.1358$	$\max Q(e) = 0.1045$
$p_4(c) = \begin{cases} \frac{0.9}{30}, & 101 \le c < 130 \\ \frac{0.1}{226}, & \text{otherwise} \end{cases}$	$\max Q(e) = 0.48$	$\max Q(e) = 0.1844$

Распределение вероятности маскировки будет отличаться от теоретических оценок!



Распределение вероятности маскировки ошибок для кода основе PN функции $F(x, y) = xy$

Распределение вероятности маскировки будет отличаться для функций из одних семейств PN функций



Распределение вероятности маскировки ошибок для кода основе PN функции $F(x, y) = xy^{-1}$

План лекции

1. Введение в понятие алгебраических манипуляций (АМ)
2. Использование кодов, обнаруживающих/исправляющих ошибки для защиты от АМ
3. Определение AMD кода
4. Новые конструкции линейных вейвлетных кодов для защиты от АМ 
5. Новые конструкции AMD кодов на основе вейвлетных преобразований для защиты от алгебраических манипуляций
6. Области применения

Новые конструкции AMD кодов

Описание результата	*Новизна*
1. Метод обеспечения целостности на основе вейвлетных линейных кодов и преобразования Грея, позволяющий обеспечивать защиту от атак на основе алгебраических манипуляций, в том числе при неравномерном распределении входных кодовых слов.	До настоящего времени - Вейвлетные линейные коды не применялись для защиты от алгебраических манипуляций; - Не были найдены преобразования для входных значений, при которых линейный вейвлетный код способен противостоять алгебраическим манипуляциям.
2. Метод обеспечения целостности на основе вейвлетных нелинейных кодов, обладающих минимальным порядком дифференциальной равномерности функции кодирования и обеспечивающих защиту от атак на основе алгебраических манипуляций, в том числе при неравномерном распределении входных кодовых слов.	До настоящего времени: - Не существовало метода обеспечения целостности информации, объединяющего вейвлетные и AMD коды; - Не применялись дополнительные механизмы в модели алгебраических манипуляций для скрытия информационной части кодового слова.
3. Практические рекомендации по применению разработанных методов обеспечения целостности для защиты средств хранения информации.	До настоящего времени: - Не существовало схем обнаружения ошибок, использующих вейвлетные преобразования в конечных пространствах, для защиты от алгебраических манипуляций; - Не было исследовано воздействие атак на основе корреляции между входными значениям и внедряемыми ошибками.

Метод обеспечения целостности на основе линейного вейвлетного кода и дополнительного преобразования входных значений

	AMD коды	Предлагаемые методы	Линейные вейвлетные коды
Представители	М. Карповский, Р. Крамер, О. Керен, И. Шумский и др.		Ф. Фекри, Черников и др.
Используемые механизмы	PN и APN функции, дифференциальная равномерность		Теория вейвлетных преобразований в конечных пространствах
Критерии оценки	Вероятность маскировки, множество необнаруживаемых ошибок, скорость кода		Расстояние Хэмминга, скорость кода и др.
Преимущества	Защита устройств, описываемых моделью AM		Эффективная программно-аппаратная реализация
Недостатки	Аппаратно-программная реализация сложнее чем в линейных кодах		Не подходит для случаев, описываемых моделью AM без дополнительных механизмов
Новые свойства предлагаемых методов	1. Дополнительное маскирование информационных символов; 2. Возможно использование при алгебраических манипуляциях совместно с преобразованием входных значений.		

Метод обеспечения целостности на основе линейного вейвлетного кода и дополнительного преобразования входных значений

Порождающая матрица линейного вейвлетного кода

$$G = V^T + aW^T J$$

Проверочная матрица линейного вейвлетного кода

$$H = \overline{V^T} + bJ^T \overline{W^T}$$

Ограничения:

1) $ab = (p-1) \bmod p$, где a,b – это элементы поля GF(q)

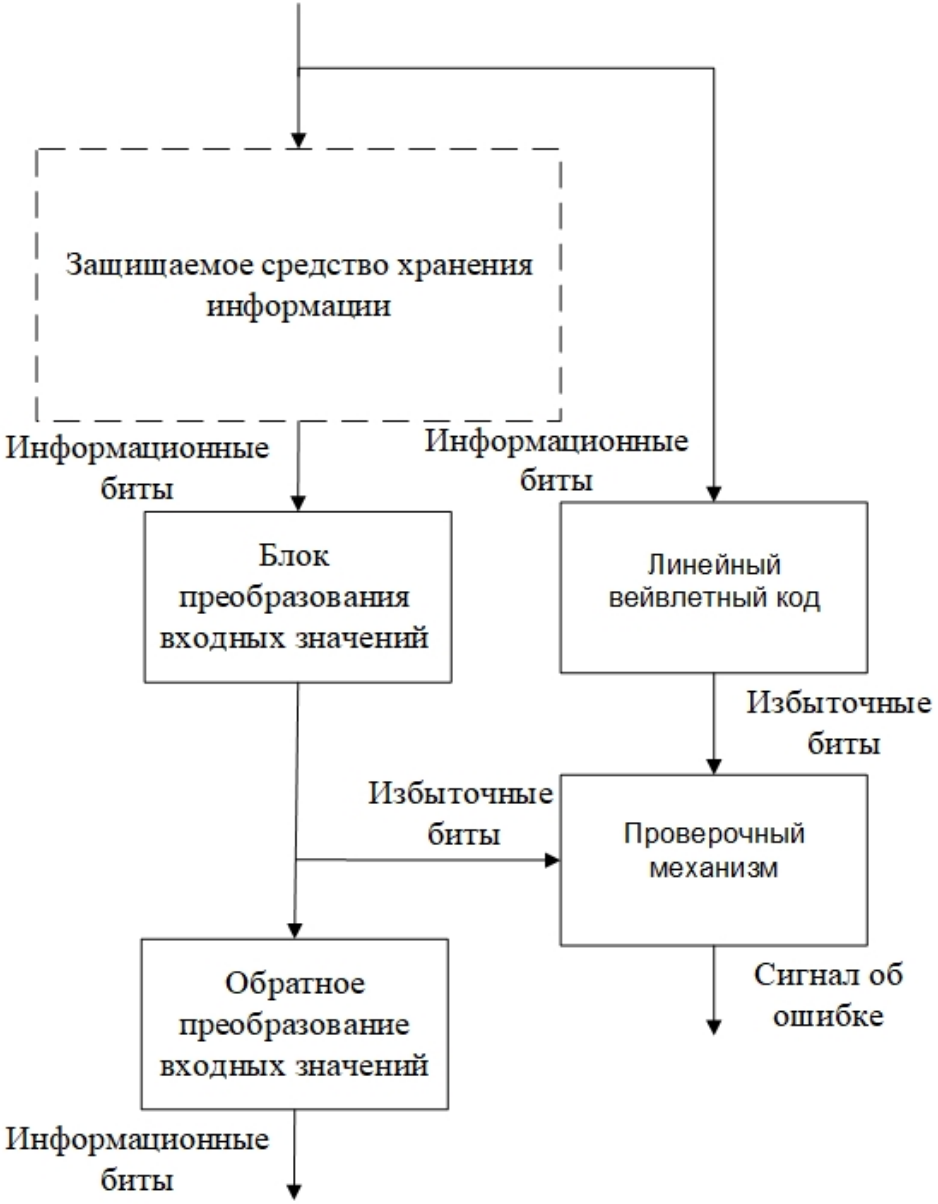
2) Условие биортогональности

$$\begin{cases} \overline{V}V^T = I \\ \overline{W}W^T = I \\ \overline{V}W^T = 0 \\ \overline{W}V^T = 0 \end{cases}$$

3) Условие точного восстановления

$$V^T \overline{V} + W^T \overline{W} = I$$

Обобщенная схема метода обеспечения целостности на основе линейных вейвлетных кодов



Снижение Q(e) за счет преобразования Грея

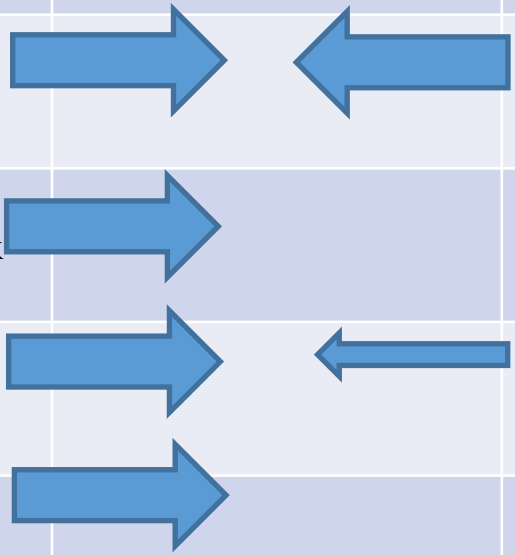
Errors	Integer form of codewords	$Q(e)$	$Q_G(e)$
00000	all vectors	1	1
00001	0	0	0
00010	0, 1, 6, 7, 10, 11, 12, 13	0.5(1-e)	0.5(1-e)
00011	2, 3, 4, 5, 8, 9, 14, 15	0.5(1-e)	0.5(1-e)
00100	0, 2, 4, 6, 8, 10, 12, 14	0.5(1-e)	0.25(1-e)
00101	1, 3, 5, 7, 9, 11, 13, 15	0.5(1-e)	0.75(1-e)
00110	1, 2, 4, 7, 8, 11, 13, 14	0.5(1-e)	0.25(1-e)
00111	0, 3, 5, 6, 9, 10, 12, 15	0.5(1-e)	0.75(1-e)
01000	0, 2, 4, 6, 9, 11, 13, 15	1-e	0.75(1-e)
01001	1, 3, 5, 7, 8, 10, 12, 14	e	0.25(1-e)
01010	1, 2, 4, 7, 9, 10, 12, 15	0.5(1-e)	0.25(1-e)
01011	0, 3, 5, 6, 8, 11, 13, 14	0.5(1-e)	0.75(1-e)
01100	0, 1, 2, 3, 4, 5, 6, 7	0.5(1-e)	0.5(1-e)
01101	8, 9, 10, 11, 12, 13, 14, 15	0.5(1-e)	0.5(1-e)
01110	0, 1, 6, 7, 8, 9, 14, 15	0.5(1-e)	0.5(1-e)
01111	2, 3, 4, 5, 10, 11, 12, 13	0.5(1-e)	0.5(1-e)
10000	0, 2, 5, 7, 8, 10, 13, 15	0.5(1-e)	0.5(1-e)
10001	1, 3, 4, 6, 9, 11, 12, 14	0.5(1-e)	0.5(1-e)
10010	1, 2, 5, 6, 8, 11, 12, 15	0.5(1-e)	0.5(1-e)
10011	0, 3, 4, 7, 9, 10, 13, 14	0.5(1-e)	0.5(1-e)
10100	0, 1, 2, 3, 8, 9, 10, 11	0.5(1-e)	0.5(1-e)
10101	4, 5, 6, 7, 12, 13, 14, 15	0.5(1-e)	0.5(1-e)
10110	0, 1, 4, 5, 10, 11, 14, 15	0.5(1-e)	0.5(1-e)
10111	2, 3, 6, 7, 8, 9, 12, 13	0.5(1-e)	0.5(1-e)
11000	4, 5, 6, 7, 8, 9, 10, 11	0.5(1-e)	0.5(1-e)
11001	0, 1, 2, 3, 12, 13, 14, 15	0.5(1-e)	0.5(1-e)
11010	2, 3, 6, 7, 10, 11, 14, 15	0.5(1-e)	0.5(1-e)
11011	0, 1, 4, 5, 8, 9, 12, 13	0.5(1-e)	0.5(1-e)
11100	1, 3, 4, 6, 8, 10, 13, 15	0.5(1-e)	0.5(1-e)
11101	0, 2, 5, 7, 9, 11, 12, 14	0.5(1-e)	0.5(1-e)
11110	0, 3, 4, 7, 8, 11, 12, 15	0.5(1-e)	0.5(1-e)
11111	1, 2, 5, 6, 9, 10, 13, 14	0.5(1-e)	0.5(1-e)

План лекции

1. Введение в понятие алгебраических манипуляций (АМ)
2. Использование кодов, обнаруживающих/исправляющих ошибки для защиты от АМ
3. Определение AMD кода
4. Новые конструкции линейных вейвлетных кодов для защиты от АМ
5. Новые конструкции AMD кодов на основе вейвлетных преобразований для защиты от алгебраических манипуляций 
6. Области применения

Метод обеспечения целостности на основе нелинейного вейвлетного кода

	AMD коды	Предлагаемые методы	Линейные вейвлетные коды
Представители	М. Карповский, Р. Крамер, О. Керен, И. Шумский и др.		Ф. Фекри, Черников и др.
Используемые механизмы	PN и APN функции, дифференциальная равномерность		Теория вейвлетных преобразований в конечных пространствах
Критерии оценки	Вероятность маскировки, множество необнаруживаемых ошибок, скорость кода		Расстояние Хэмминга, скорость кода и др.
Преимущества	Защита устройств, описываемых моделью AM		Эффективная программно-аппаратная реализация
Недостатки	Аппаратно-программная реализация сложнее чем в линейных кодах		Не подходит случаев, описываемых моделью AM
Новые свойства предлагаемых методов	1. Дополнительное маскирование информационных символов; 2. Дополнительная защита при неравномерном распределении		



Стрелками обозначены наследуемые признаки

Метод обеспечения целостности на основе нелинейного вейвлетного кода

Вейвлетный кубический код. Пусть L линейный вейвлетных код длиной n и количеством избыточных символов r. Код L может быть преобразован в нелинейный систематический код C на основе нелинейной кубической функции:

- путем вычисления куба для вектора избыточных символов r в поле $GF(2^r)$

$$C_L = (x, v) | x \in GF(2^k), v = (Px)^3 \in GF(2^r)$$

Конструкция вейвлетного кода на основе умножения в поле (Вейвлетный AMD код)

Части x и y в кодовом слове

$$(y \in GF(2^{sr}) | x \in GF(2^{sr}) | f(y,x) \in GF(2^r))$$

Представляются как вектора в поле Галуа. Функция кодирования для данной конструкции – это произведение в поле $f(y,x) \in GF(2^r)$

$$f(y,x) = x_1 y_1 \oplus x_2 y_2 \oplus \ldots \oplus x_r y_r$$

Сравнение предлагаемых конструкций вейвлетных кодов и существующих аналогов

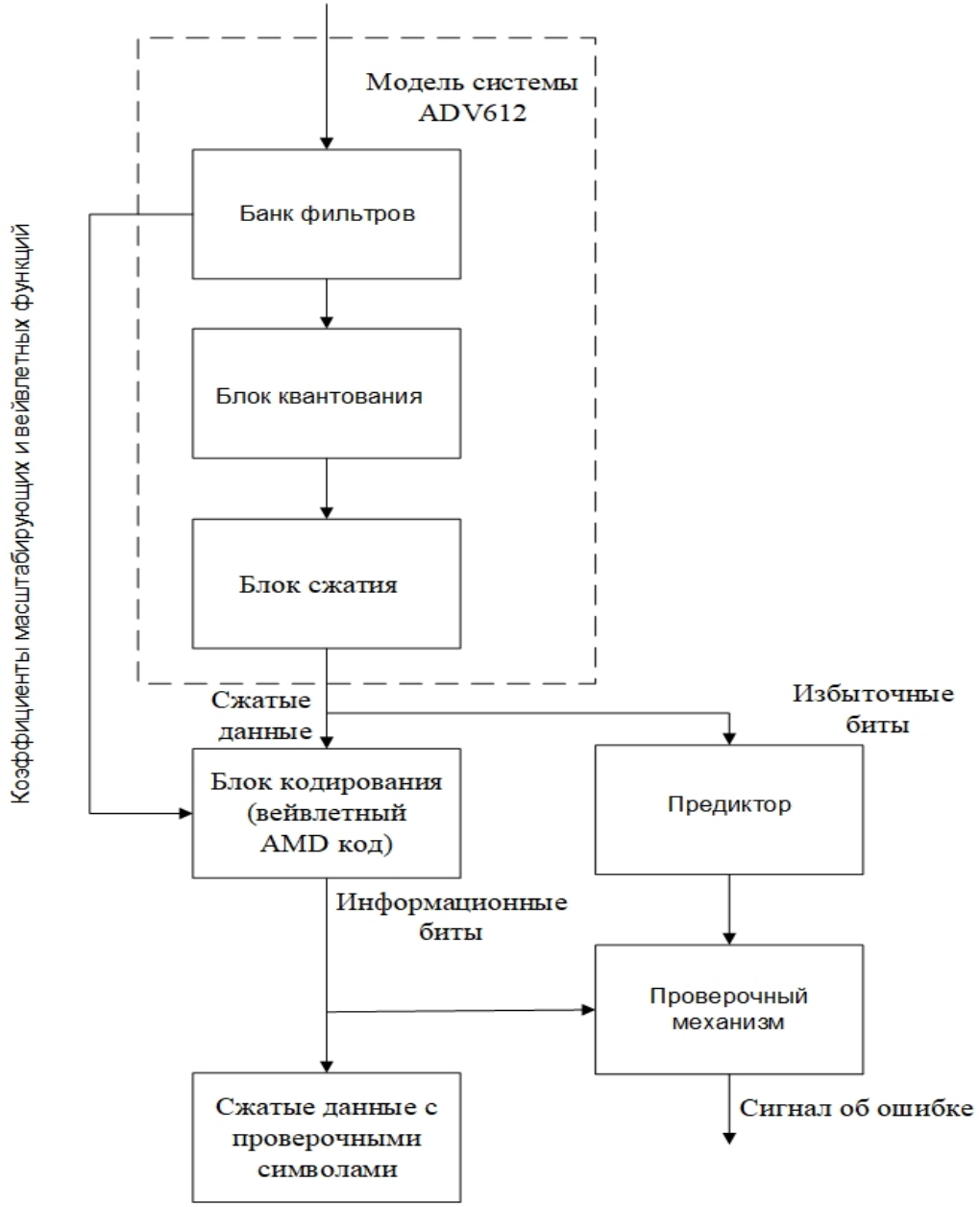
Код	n	k	$R(e)$	max Q(e)
Код на основе мультипликативного обратного	$k+r$	k	2^{k-r}	2^{-r+1} если r четное, иначе 2^{-r+2}
Кубический код	$2k$	k	1	2^{-k+1}
Вейвлетный кубический код	$2k$	k	1	2^{-k+1}
Вейвлетный AMD код	$3r$	$2r$	1	2^{-r}
AMD код (функция Маорана-МакФарланда)	$3r$	$2r$	1	2^{-r}
Линейный код (Код Хемминга)	2^r	$2^r - 1 - r$	2^k	1

где r — количество избыточных символов, k — количество информационных символов, n – длина кода

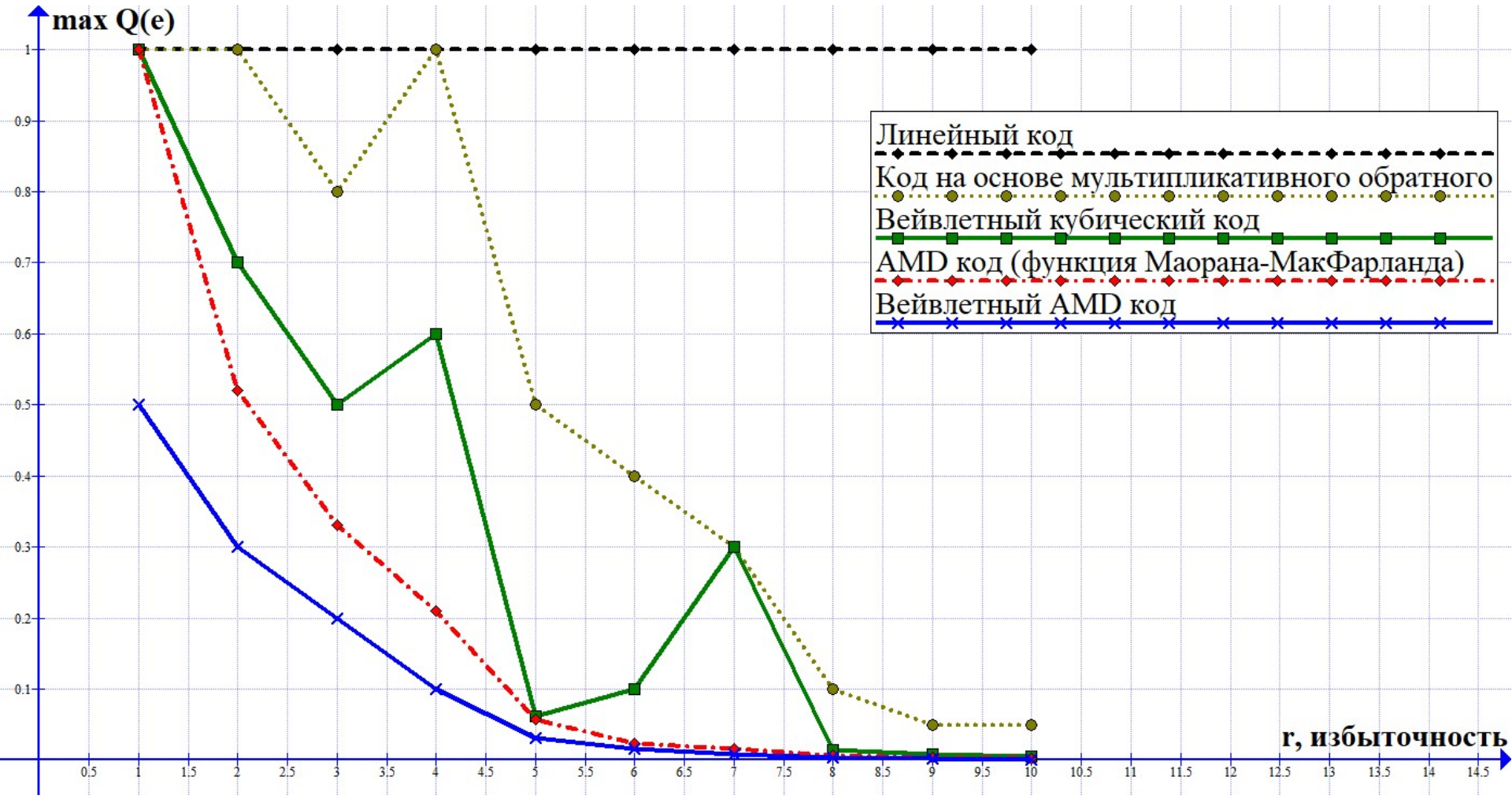
План лекции

1. Введение в понятие алгебраических манипуляций (АМ)
2. Использование кодов, обнаруживающих/исправляющих ошибки для защиты от АМ
3. Определение AMD кода
4. Новые конструкции линейных вейвлетных кодов для защиты от АМ
5. Новые конструкции AMD кодов на основе вейвлетных преобразований для защиты от алгебраических манипуляций
6. Области применения 

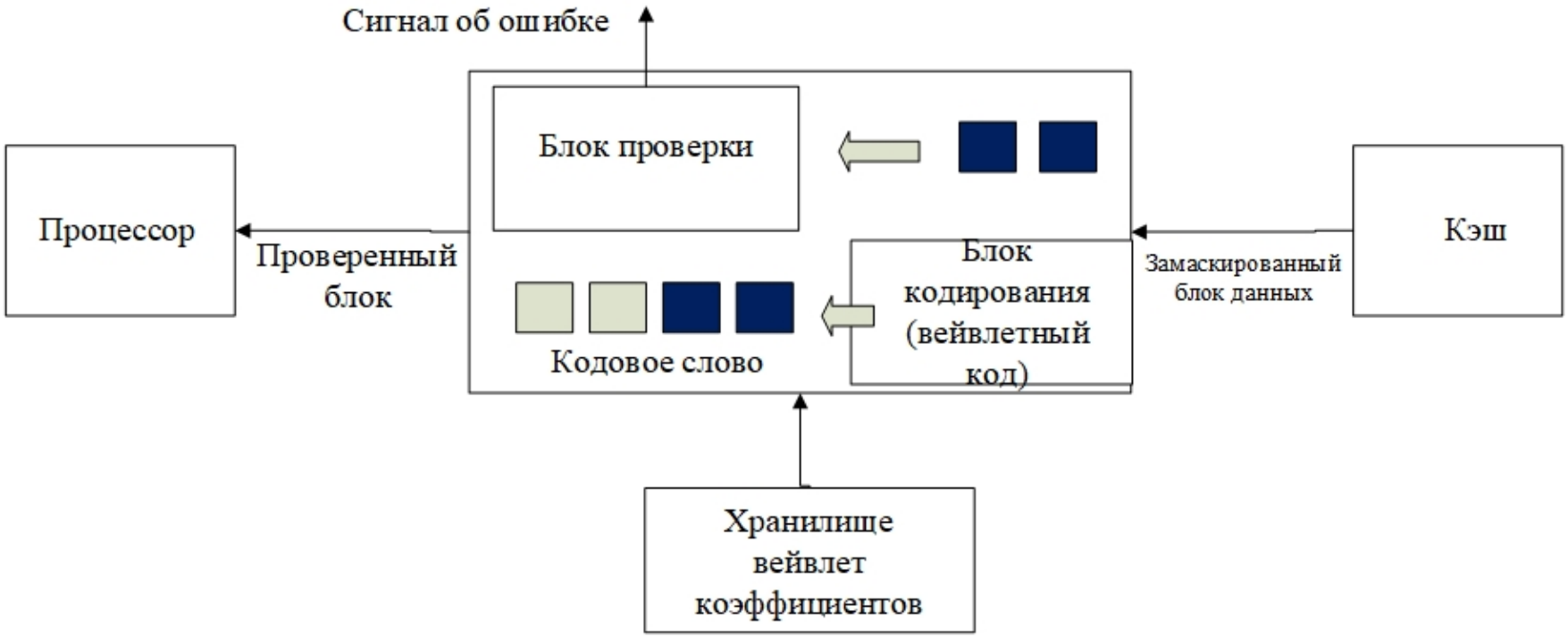
Практические рекомендации по использованию предложенных методов в системе сжатия ADV612



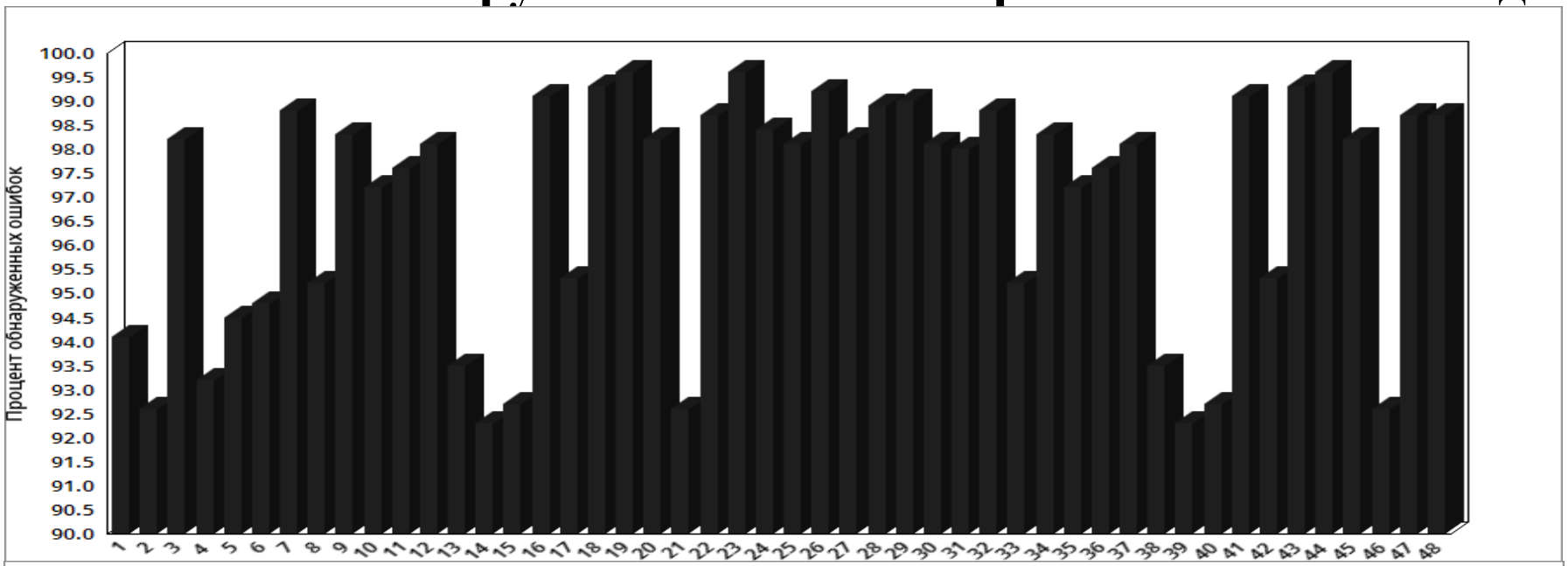
Неравномерное распределение входных кодовых слов, задаваемое кусочной функцией

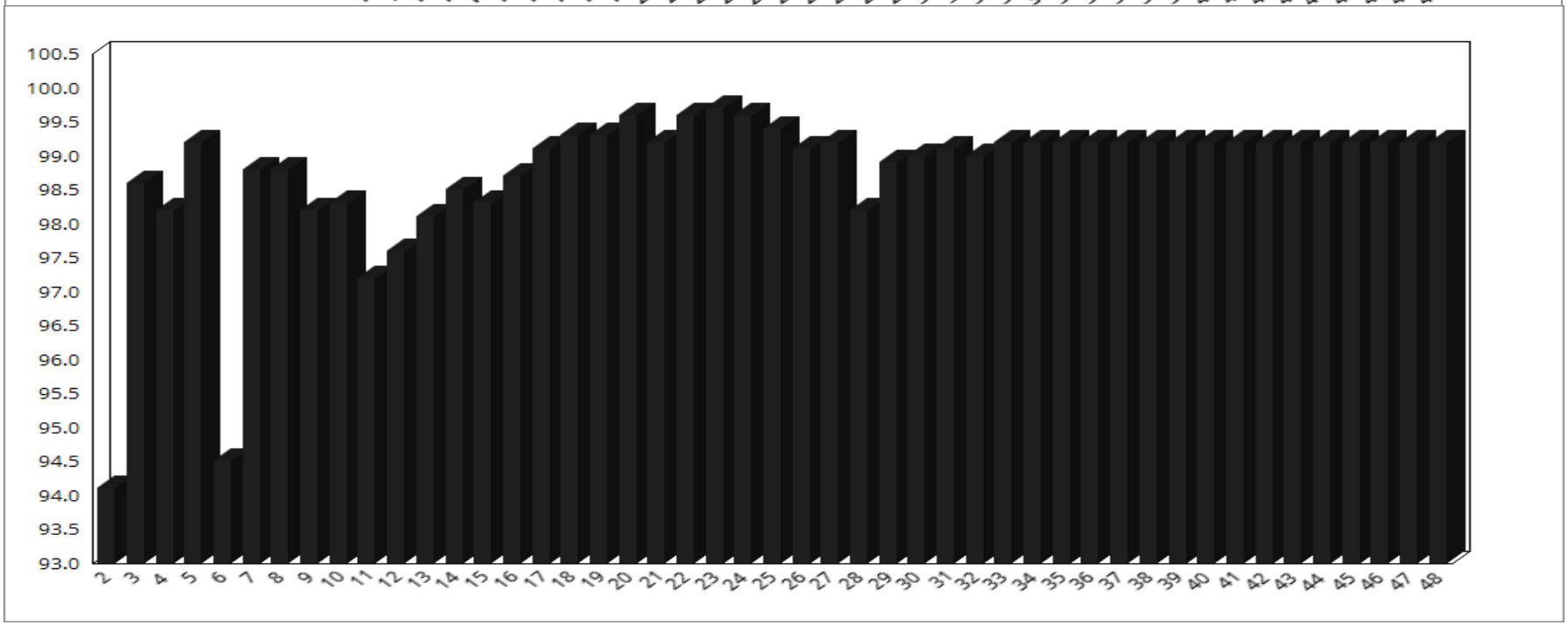


Практические рекомендации по использованию предложенных методов для защиты кэш памяти



Статистика обнаруженных ошибок при атаке на AMD код





Другие области применения AMD кодов

- Защита каналов со случайной структурой;
- Безопасность линейных частей криптографических устройств;
- Построение схем разделения секрета;
- Безопасность многоуровневой NAND флеш памяти;

Заключение

1. Рассмотрено понятие алгебраических манипуляций (АМ)
2. Показаны недостатки и преимущества от использование кодов, обнаруживающих/исправляющих ошибки для защиты от АМ
3. Дано определение AMD кода
4. Представлены новые конструкции линейных вейвлетных кодов для защиты от АМ
5. Представлены новые конструкции AMD кодов на основе вейвлетных преобразований для защиты от алгебраических манипуляций

Спасибо за внимание!