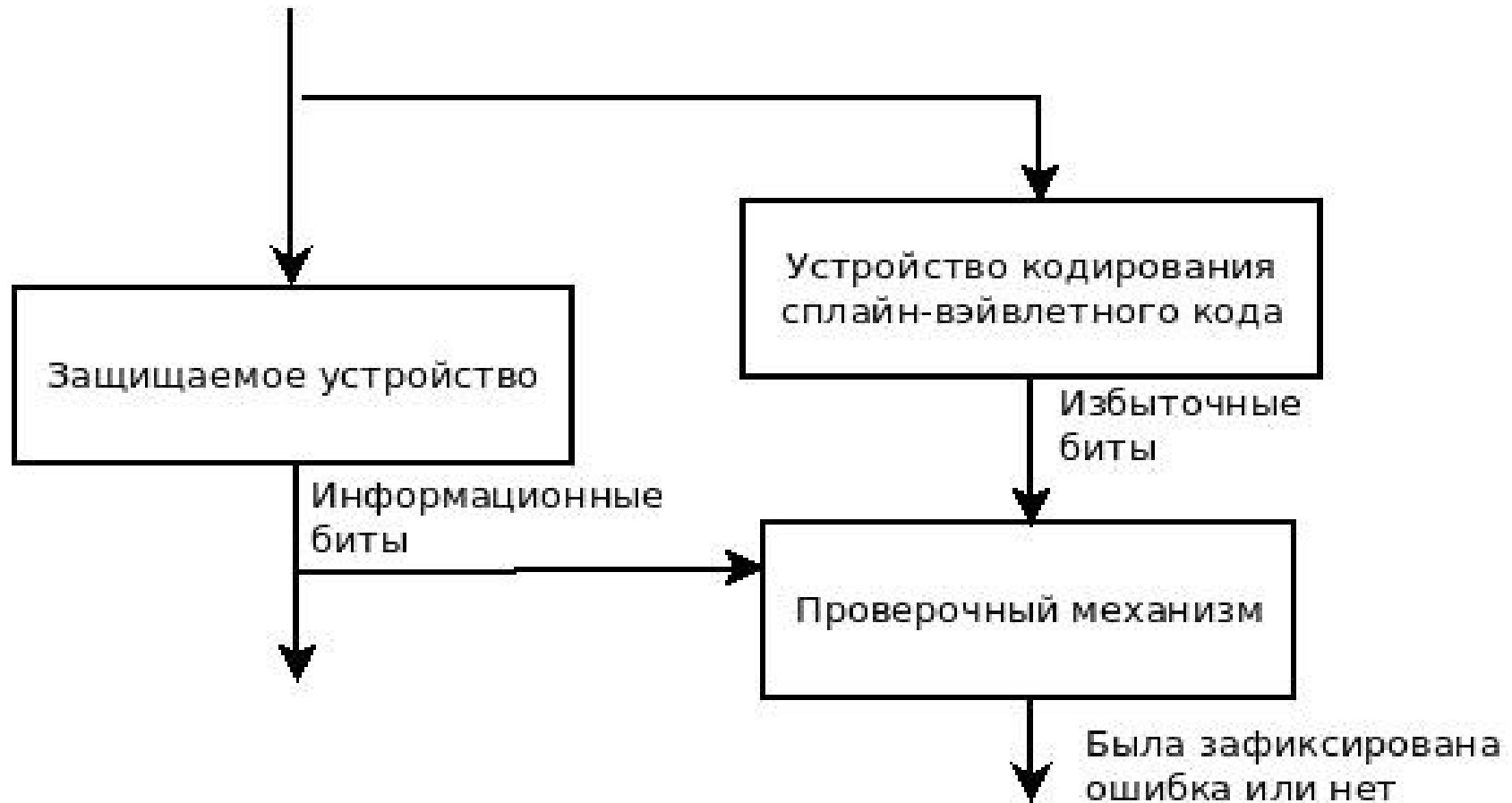


ITMO UNIVERSITY

Надежные коды на основе вэйвлетных разложений

Saint Petersburg
2015

Надежный код



Надежный код предусматривает возможность внедрения злоумышленником ошибки любой кратности и в любой участок системы. Данный класс помехоустойчивых кодов обеспечивает защиту против всех возможных ошибок.

Сравнение разработанной конструкции с другими классами помехоустойчивых кодов

Коды	Max Q(e) — максимум вероятности маскировки ошибки	Количество необнаруживаемых ошибок	Скорость кодирования информации при обработке помехоустойчивым кодом блока данных размером 64 Кб	
(64, 32) - линейный код на основе вэйвлетов (Faramarz Fekri)	1	2^{32}	1, 12 сек	
(64,32) надежный код на основе совершенно нелинейных функций (Mark Karpovski)	2^{-31}	0	3, 59 сек	
(64, 32) - надежный сплайн-вэйвлетный код	2^{-31}	0	В системе с вэйвлетными преобразованиями	2, 33 сек
			В системе без вэйвлетных преобразований	3, 47 сек

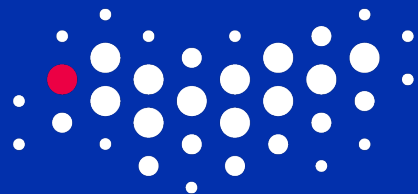
Характеристики надежности в случае неравномерного распределения кодовых слов

Коды	Характер распределения кодовых слов	Максимум вероятности маскировки ошибки без использования преобразования Грея	Максимум вероятности маскировки ошибки с использованием преобразования Грея
(64,32) надежный код на основе совершенно нелинейных функций (Mark Karpovski)	Равномерное распределение	0, 571	0,571
	Неравномерное распределение	0, 758	0, 692
(64, 32) - надежный сплайн-вэйвлетный код	Равномерное распределение	0, 571	0,571
	Неравномерное распределение	0, 711	0, 643

Чем ближе максимум вероятности маскировки ошибки к единице, тем сложнее обнаружить ошибку с помощью надежного кода.

Результаты:

1. Разработанный на основе сплайн-вэйвлетного преобразования второго порядка помехоустойчивых код является надежным кодом, поэтому он позволяет обеспечить высокий уровень защиты против атак внедрения ошибок, по сравнению с линейными кодами.
2. Если система, которую планируется улучшать с помощью надежных помехоустойчивых кодов, уже использует вэйвлетные преобразования, то разработанные коды могут существенно сократить время кодирования за счет повторного использования задействованных в системе коэффициентов масштабирующих функций вейвлетных преобразований.
3. По сравнению с надежными кодами (Mark Karrovski), разработанные сплайн-вэйвлетные коды дают больший выигрыш при применении преобразования Грея. К тому же даже без использования преобразования Грея, сплайн-вэйвлетные коды меньше подвержены тенденции снижения характеристик надежности при неравномерном распределении кодовых слов, свойственной всем надежным кодам.



ITMO UNIVERSITY

Спасибо за внимание!

Санкт-Петербург
2015