ПРИМЕНЕНИЕ ОБЛЕГЧЁННЫХ КРИПТОАЛГОРИТМОВ ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Анисимова Ю.Н., Савченко А.А.
Власова Г.А. – к.т.н.,доцент

Основные проблемы обеспечения безопасности устройств Интернет вещей обусловлены тем, что существующие методы и средства защиты изначально разрабатывались для персональных компьютеров, и не учитывали особенности и ограничения устройств Интернета вещей. Для защиты таких устройств необходимо применять облегчённые криптографические алгоритмы, эффективность применения которых зависит от специфики устройства и качественного подбора к нему криптоалгоритма.

Интернет вещей (Internet of Things, IoT) – концепция, предполагающая объедение в сеть устройств (вещей), способных взаимодействовать друг с другом на основе встроенных технологий, которые поддерживаются данной сетью. Устройствами (вещами) являются «умные» гаджеты, «умная» техника и другие устройства, которые могут быть использованы в обиходе человека или его дома.

Применение традиционных методов защиты устройств Интернета вещей, таких как шифрование, идентификация/аутентификация и внедрение физических мер обеспечения безопасности, требует их существенного реинжиниринга и адаптации, так как устройства имеют множество ограничений. Интернет вещей, как правило, состоит из портативных устройств с низким электропотреблением, малым форм-фактором и ограниченными возможностями [1].

Основным средством обеспечения информационной безопасности в мире Интернета вещей является так называемая «облегчённая» криптография. К облегчённой криптографии относятся алгоритмы, разрабатываемые специально для устройств с ограниченными или крайне ограниченными вычислительными ресурсами.

Симметричные алгоритмы ввиду своих качеств используются для шифрования видео-данных, где требуются очень производительные системы для шифрования, а также необходима значительная вычислительная мощность для шифрования и декодирования в реальном времени. Стремительное развитие рынка видеонаблюдения показывает, что направлением нового времени является именно IP-видеонаблюдение.

При выборе легковесного криптоалгоритма, реализующего шифрование видео-данных, следует учитывать такие характеристики алгоритма, как длина информационного блока, длина ключа, число раундов (циклов шифрования), влияющие на криптостойкость алгоритма, в данном случае, при шифровании видеоданных, размера ключа в 128 бит и число раундов больше 20 будет достаточно, количество условных логических элементов должно быть в пределе 1000 GE.

Ссылаясь на статью [2], где приведены сравнительные характеристики алгоритмов, и сравнивая по такому параметру, как длина ключа, для обеспечения необходимого уровня криптостойкости подходят алгоритмы LED, Piccolo, PRESENT, TWINE с длиной ключа в 128 бит. Алгоритм LED имеет худшие показатели числа тактов работы, характеристики у Piccolo, PRESENT схожи, однако алгоритм Piccolo имеет преимущество ввиду меньшего количества логических элементов для реализации при таких же показателях длины ключа, числа раундов и числа тактов работы алгоритма.

Ссылаясь на [3], где указаны сравнительные результаты реализации блочных шифров Piccolo-128, TWINE -128, PRESENT-128 на 16-разрядном микропроцессоре RL78 от Renesas Electronics. по параметрам занимаемых ОЗУ, ПЗУ, скорости шифрования и дешифрования, видно, что алгоритмы Piccolo, PRESENT могут быть реализованы с небольшим объемом оперативной памяти, 64 байта оперативной памяти было достаточно во всех категориях. Алгоритм TWINE имеет незначительные программные издержки, что обеспечивает чрезвычайно малый размер кода. С точки зрения скорости, TWINE достиг уровня, аналогичного Piccolo. Для реализации шифрования большого объема данных с IP систем видеонаблюдения с большой скоростью подходит блочный симметричный тип шифрования и реализующий его алгоритм Piccolo-128.

Асимметричная криптография используется в SSL/TLS, которые помогают сделать HTTPS соединение безопасным. К популярным алгоритмам с использованием открытых ключей относятся: RSA, DSA, ECC и PKCS, но все они имеют определенные недостатки, либо сравнительно невысокая скорость работы (напр., алгоритмы на базе эллиптических кривых (ЭК)), либо сравнительно низкая стойкость при сопоставимых

размерах ключей и параметров (схема Диффи-Хеллмана и другие алгоритмы, основанные на дискретном логарифме в поле), либо и то, и другое одновременно (RSA).

В статье [4] приведены сравнения размеров ключей для Number Theorists aRe Us (NTRU) с эквивалентными размерами ключей для систем, основанных на проблемах факторизации целых чисел и дискретного логарифма в группе точек эллиптических кривых. Сравнения показывают, что NTRU имеет все необходимые условия для обеспечения наивысшего уровня стойкости и по этому показателю не отстает от конкурентов.

В [4] приводятся сравнительные результаты измерений скорости NTRU, ЭК и RSA.

NTRU имеет высокую скорость выполнения операций зашифрования/расшифрования. По заявлениям компании Security Innovation, занимающейся разработкой NTRU, данный алгоритм до двухсот раз быстрее, чем алгоритмы на эллиптических кривых и RSA, и при этом его реализация гораздо меньше (около 8 Кб).

Ниже в таблице 1 приводится сравнение алгоритмов NTRU, RSA и ECC-NIST-224. Скорость работы данных алгоритмов была замерена как на ЦПУ, так и на графических процессорах с использованием технологии распараллеливания CUDA от Nvidia. Алгоритмы NTRU, RSA и ECC-NIST-224 представлены в [5].

Таблица 1 – Сравнение скорости реализаций NTRU, RSA и ЭК для ЦПУ и ГПУ

Алгоритм	Языки платформа	Параметры алгоритма	Зашифр/с	Расшифр/с	Бит/опер.
NTRU	Intel Core2 Extreme @ 3.00GHz	(N, q, p) = (1171, 2048, 3) (k = 256)	95	95	1756
	CUDA, GTX280 (1 операция)		571	546	
	CUDA, GTX280		$24*10^3$	$24*10^3$	
RSA	CUDA, Nvidia 8800 GTS	2048 bit (k = 112)	-	104	2048
	Intel Core2 @ 1.83GHz		$6,65*10^3$	168	
ЭК	CUDA, Nvidia 8800 GTS	ECC-NIST-224 (k = 112)	-	$1,41*10^3$	

	Intel Core2 @ 1.83 GHz (ECDSA)			1,86** 10^3	

Можно сделать вывод о высоком уровне стойкости NTRU, который не уступает стойкости алгоритмов на базе эллиптических кривых. Но в связи с новизной и малой распространенностью NTRU необходимо проводить дополнительные исследования на предмет возможных закладок и критических уязвимостей, которые могут быть использованы для разработки эффективных атак. В результате анализа быстродействия NTRU было установлено, что его скорость работы гораздо выше, чем у RSA и ЭК.

Применение облегчённых криптоалгоритмов позволяет обеспечить защиту устройств Интернета вещей с ограниченными вычислительными ресурсами. Микропроцессор на основе асимметричной криптографии могут использоваться в любых гаджетах, где не требуется высокая пропускная способность интернет трафика, например, в гаджетах «умного» дома. Выбор алгоритма для реализации основывается на таких сравнительных характеристиках, как требуемое количество условных логических элементов, занимаемой ОЗУ, ПЗУ, скорости шифрования, скорости дешифрования. Результаты сравнения скорости реализации асимметричных легковесных криптографических алгоритмов показали, что наилучшими параметрами обладает алгоритм NTRU. Результаты сравнения основных параметров реализации симметричных легковесных криптографических алгоритмов показали, что алгоритм Piccolo-128 имеет преимущества и подходит для реализации шифрования большого объема данных с IP-систем видеонаблюдения.

Список использованных источников:

1. Полегенько А. М. Особенности защиты информации в интернете вещей [Текст] / А. М. Полегенько // International Journal of Open Information Technologies. – 2018. - № 6. – С. 41-44.

2 .Жуков А. Е. Легковесная криптография. часть 1 [Текст] / А. Е. Жуков // Вопросы кибербезопасности. – 2015. - № 4. – С. 31-36.

3. Cryptographic Technology Guideline (Lightweight Cryptography) [Текст]: Lightweight Cryptography Working Group / Kazumaro Aoki, Tetsu Iwata, Kazuto Ogawa и др. – Cryptrec, 2017. – С. 39-44.

4. Jens Hermans, Frederik Vercauteren, Bart Preneel. Speed records for NTRU. Department of Electrical Engineering, University of Leuven Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium.

5. Speed records for NTRU [Электронный ресурс]. – Режим доступа: https://homes.esat.kuleuven.be/~fvercaut/papers/ntru_gpu.pdf.