№5/2026

ADPI
Ilmiy xabarnomasi

«ВНЕДРЕНИЕ ЛЕГКОВЕСНОЙ КРИПТОГРАФИИ В УСТРОЙСТВАХ С ОГРАНИЧЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ МОЩНОСТЬЮ»

Ортиков Муроджон
Андижанской государственный технический институт

Annotatsiya.
Narsalar interneti (IoT), o‘rnatilgan tizimlar va simsiz sensor tarmoqlarining tez sur’atlar bilan rivojlanishi maxfiy ma’lumotlarni qayta ishlaydigan va uzatadigan qurilmalar sonining ko‘payishiga olib keldi. Narsalar interneti qurilmalari ko‘pincha cheklangan hisoblash imkoniyatlari, kichik xotira hajmi va quvvat iste’moliga nisbatan qat’iy talablar bilan tavsiflanadi. Ushbu cheklovlar an’anaviy kriptografik mexanizmlarni qo‘llashni murakkablashtiradi va maxsus xavfsizlik yechimlarini ishlab chiqishni talab etadi [1]. Bunday sharoitda minimal resurslar bilan zarur xavfsizlik darajasini ta’minlaydigan yengil vaznli kriptografiya ayniqsa dolzarb hisoblanadi. Maqolada hisoblash quvvati cheklangan qurilmalarda yengil vaznli kriptografiyani joriy etish xususiyatlari tahlil qilinadi, mavjud algoritmlar, ularning afzalliklari va kamchiliklari ko‘rib chiqiladi, shuningdek, IoT-qurilmalar uchun yechimlarni tanlash bo‘yicha tavsiyalar beriladi.

Kalit so‘zlar:
yengil vaznli kriptografiya, axborot xavfsizligi, narsalar interneti, IoT, o‘rnatilgan tizimlar, mikrokontrollerlar, shifrlash, kriptografik algoritmlar..

Аннотация.
Быстрый рост Интернета вещей (IoT), встроенных систем и беспроводных сенсорных сетей привел к увеличению числа устройств, обрабатывающих и передающих конфиденциальную информацию. Устройства Интернета вещей часто характеризуются ограниченными вычислительными возможностями, малым объемом памяти и жесткими требованиями к энергопотреблению. Эти ограничения усложняют применение традиционных криптографических механизмов и требуют разработки специализированных решений безопасности [1]. В этих условиях особенно актуальна легковесная криптография, обеспечивающая необходимый уровень безопасности при минимальных ресурсах. В статье анализируются особенности внедрения легковесной криптографии в устройствах с ограниченной вычислительной мощностью, рассматриваются существующие алгоритмы, их преимущества и недостатки, а также даются рекомендации по выбору решений для IoT-устройств.

Ключевые слова:
криптографическая защита информации, КЗИ, несанкционированный доступ, НСД, аппаратная безопасность, датчики вскрытия, побочные каналы.

Abstract.
The rapid growth of the Internet of Things (IoT), embedded systems, and wireless sensor networks has led to an increase in the number of devices that process and transmit sensitive information. IoT devices are often characterized by limited computational capabilities, low memory capacity, and stringent power consumption requirements. These constraints complicate the deployment of traditional cryptographic mechanisms and necessitate the development of tailored security solutions [1]. Under these conditions, lightweight cryptography is becoming particularly relevant, as it provides the required level of security while consuming minimal resources. This paper analyzes the specific challenges of implementing lightweight cryptography in resource-constrained devices, reviews existing algorithms along with their advantages and disadvantages, and offers recommendations for selecting security solutions for IoT devices.

Keywords:
lightweight cryptography, information security, Internet of Things, IoT, embedded systems, microcontrollers, encryption, cryptographic algorithms.

Введение. В последние годы, особенно в минувшие десятилетия, количество интеллектуальных устройств, подключенных к Интернету, быстро выросло. Концепция Интернета вещей охватывает миллионы устройств, включая датчики, контроллеры, медицинское оборудование, промышленные системы, транспорт и бытовую

ISSN 2181-4309

электронику. По прогнозам, число IoT-устройств уже достигает десятков миллиардов по всему миру.

Одновременно с расширением сферы применения IoT возрастают требования к защите передаваемых и хранимых данных. Многие устройства обрабатывают персональную информацию пользователей, технологические параметры производственных процессов или критически важные данные инфраструктуры. Несанкционированный доступ к таким данным может привести к финансовым потерям, нарушению конфиденциальности и сбоям в работе систем.

Традиционные криптографические алгоритмы, такие как AES, RSA и ECC, обеспечивают высокий уровень защиты информации, однако их использование в устройствах с ограниченными вычислительными ресурсами зачастую сопровождается значительными затратами памяти, процессорного времени и энергии. В связи с этим возникает необходимость разработки и внедрения специальных криптографических механизмов, ориентированных на ресурсно-ограниченные устройства.

Целью настоящего исследования является анализ возможностей внедрения легковесной криптографии в устройствах с ограниченной вычислительной мощностью и оценка ее эффективности для обеспечения информационной безопасности современных IoT-систем.

Устройства с ограниченными вычислительными ресурсами

Под устройствами с ограниченными вычислительными ресурсами понимаются электронные устройства, обладающие ограниченными возможностями обработки данных, небольшим объемом оперативной памяти и низким энергопотреблением.

К данной категории относятся:

- микроконтроллеры;
- RFID-метки;
- беспроводные сенсорные узлы;
- интеллектуальные счетчики;
- медицинские импланты;
- носимые устройства;
- системы промышленного мониторинга;
- устройства Интернета вещей.

Типичный микроконтроллер может содержать всего несколько килобайт оперативной памяти и работать на частоте в десятки мегагерц. Многие устройства функционируют от батарей и должны сохранять работоспособность в течение нескольких лет без обслуживания.

Основными ограничениями таких устройств являются:

- ограниченный объем памяти;
- низкая производительность процессора;
- малое энергопотребление;
- ограниченная пропускная способность каналов связи;

ISSN 2181-4309

• невысокая стоимость аппаратной реализации.

Перечисленные факторы существенно ограничивают возможность применения традиционных криптографических решений и требуют использования специализированных алгоритмов.

Проблемы внедрения традиционной криптографии

Традиционные алгоритмы криптографической защиты создавались преимущественно для персональных компьютеров и серверных систем, обладающих значительными вычислительными ресурсами.

Алгоритм RSA обеспечивает надежную асимметричную защиту данных, однако требует выполнения сложных математических операций над большими числами. В результате процесс шифрования и дешифрования может занимать значительное время на маломощных микроконтроллерах.

Несмотря на высокую эффективность алгоритма AES, его реализация также требует определенного объема памяти и вычислительных ресурсов. Для ряда устройств это может приводить к увеличению времени отклика системы и повышенному энергопотреблению.

Использование криптографии в ресурсно-ограниченных системах сопровождается следующими проблемами:

• снижение производительности устройства;
• увеличение времени передачи данных;
• рост энергопотребления;
• увеличение стоимости аппаратной реализации;
• сокращение срока службы автономных источников питания.

Таким образом, применение классических криптографических алгоритмов не всегда является оптимальным решением для устройств Интернета вещей.

Концепция легковесной криптографии

Легковесная криптография предназначена для обеспечения криптографической защиты в системах с ограниченными ресурсами, где важным критерием является баланс между уровнем безопасности, производительностью и потреблением энергии [2].

Основными требованиями к легковесным алгоритмам являются:

• низкое потребление энергии;
• минимальное использование памяти;
• высокая скорость обработки данных;
• устойчивость к современным криптоаналитическим атакам;
• возможность аппаратной и программной реализации.

Главной особенностью легковесной криптографии является поиск оптимального баланса между безопасностью и производительностью.

При разработке подобных алгоритмов особое внимание уделяется сокращению количества математических операций, уменьшению размеров таблиц подстановок и оптимизации структуры раундовых преобразований.

В отличие от традиционной криптографии, где приоритетом выступает максимальная стойкость независимо от ресурсов системы, легковесная криптография ориентирована на обеспечение достаточного уровня защиты при минимальных вычислительных затратах.

Современные алгоритмы легковесной криптографии

В последние годы разработано множество алгоритмов, предназначенных для использования в ограниченных вычислительных средах.

PRESENT

Алгоритм PRESENT был разработан как компактный блочный шифр для применения в системах с ограниченными аппаратными ресурсами. Авторы алгоритма ориентировались на минимизацию площади аппаратной реализации при сохранении достаточного уровня криптографической стойкости [3]. Алгоритм использует размер блока 64 бита и ключ длиной 80 либо 128 бит.

Преимуществами алгоритма являются:

- компактная реализация;
- низкое энергопотребление;
- высокая скорость работы на микроконтроллерах.

Недостатком является относительно небольшой размер блока по сравнению с современными стандартами.

GIFT

Алгоритм GIFT разработан как усовершенствование ряда существующих легковесных шифров. Он обеспечивает высокую производительность и устойчивость к современным методам криптоанализа.

Преимуществами являются:

- низкие требования к памяти;
- высокая эффективность аппаратной реализации;
- хорошие показатели безопасности.

SIMON и SPECK

Данные алгоритмы были разработаны для использования в ограниченных вычислительных средах.

SIMON ориентирован преимущественно на аппаратную реализацию, тогда как SPECK демонстрирует высокую эффективность при программной реализации.

Основными достоинствами являются:

- высокая скорость работы;
- простая архитектура;
- небольшие требования к ресурсам.

Ascon

Алгоритм Ascon представляет собой семейство криптографических алгоритмов с аутентифицированным шифрованием, разработанное для эффективной реализации в устройствах с ограниченными ресурсами. В 2023 году Ascon был выбран Национальным

ISSN 2181-4309

институтом стандартов и технологий США (NIST) в качестве основы стандарта легковесной криптографии [4].

Алгоритм обеспечивает:

- конфиденциальность данных;
- контроль целостности сообщений;
- защиту от подделки информации;
- эффективную работу на микроконтроллерах.

Благодаря сочетанию безопасности и производительности данный алгоритм рассматривается как один из наиболее перспективных стандартов для IoT-систем.

Практические аспекты внедрения легковесной криптографии

Процесс внедрения легковесной криптографии включает несколько этапов.

На первом этапе проводится анализ характеристик устройства:

- объем памяти;
- частота процессора;
- энергопотребление;
- объем передаваемых данных.

На втором этапе осуществляется выбор криптографического алгоритма.

Для датчиков с минимальными ресурсами целесообразно использование сверхкомпактных алгоритмов. Для более производительных устройств возможно применение современных схем аутентифицированного шифрования.

На третьем этапе выполняется организация управления ключами.

Наиболее распространенными подходами являются:

- предварительная загрузка ключей;
- генерация ключей на устройстве;
- использование инфраструктуры открытых ключей;
- применение протоколов обмена ключами.

После настройки системы проводится тестирование производительности и устойчивости к атакам.

Особое внимание уделяется защите от:

- атак повторного воспроизведения;
- подделки сообщений;
- атак по сторонним каналам;
- физического вмешательства в устройство.

Оценка эффективности применения легковесной криптографии

Использование легковесных алгоритмов позволяет существенно сократить вычислительные затраты.

Практические исследования показывают, что по сравнению с традиционными криптографическими механизмами возможно добиться:

- уменьшения потребления памяти;
- сокращения времени выполнения операций;

ISSN 2181-4309

• снижения энергозатрат;

• увеличения времени автономной работы устройств.

Для IoT-систем данный фактор имеет критическое значение, поскольку многие устройства функционируют без обслуживания в течение длительного времени.

Кроме того, снижение вычислительной нагрузки позволяет использовать более дешевые микроконтроллеры без ухудшения уровня защищенности системы.

Следовательно, внедрение легковесной криптографии обеспечивает не только повышение безопасности, но и снижение общей стоимости эксплуатации распределенных IoT-инфраструктур. Анализ показал, что алгоритмы семейства SIMON и SPECK демонстрируют высокую скорость выполнения операций на микроконтроллерах. Однако алгоритм Ascon обеспечивает не только шифрование данных, но и аутентифицированное шифрование, что существенно повышает уровень защиты информации.

Алгоритм	**Размер ключа (бит)**	**Размер блока (бит)**	**Производительность**	**Требования к памяти**	**Уровень безопасности**
PRESENT	80/128	64	Средняя	Очень низкие	Высокий
GIFT	128	64	Высокая	Низкие	Высокий
SIMON	64–256	32–128	Высокая	Низкие	Высокий
SPECK	64–256	32–128	Очень высокая	Низкие	Высокий
Ascon	128	320 (состояние)	Высокая	Низкие	Очень высокий

Проведенное исследование показывает, что использование традиционных алгоритмов криптографической защиты в устройствах Интернета вещей не всегда является эффективным вследствие ограниченности вычислительных ресурсов.

Легковесные алгоритмы позволяют существенно уменьшить нагрузку на процессор и сократить объем используемой памяти. Особенно важным преимуществом является снижение энергопотребления, что критически важно для автономных устройств, работающих от аккумуляторов или батарей.

Среди рассмотренных решений наиболее перспективным представляется алгоритм Ascon, который сочетает высокий уровень криптографической стойкости с низкими требованиями к аппаратным ресурсам.

Полученные результаты подтверждают возможность широкого внедрения легковесной криптографии в интеллектуальных датчиках, медицинских устройствах, промышленных контроллерах и других компонентах Интернета вещей.

Перспективы развития

Современные тенденции развития информационной безопасности свидетельствуют о дальнейшем росте популярности легковесной криптографии.

Основными направлениями развития являются:

• создание новых алгоритмов;

• совершенствование методов защиты от атак по сторонним каналам;
• интеграция криптографии в аппаратное обеспечение микроконтроллеров;
• разработка стандартов безопасности для IoT;
• адаптация криптографических механизмов к постквантовой эпохе.

Особый интерес представляет разработка гибридных решений, сочетающих легковесную криптографию и методы искусственного интеллекта для обнаружения аномалий и кибератак.

В ближайшие годы ожидается расширение применения легковесной криптографии в промышленном Интернете вещей, интеллектуальных транспортных системах, телемедицине и концепции умного города.

Заключение

Внедрение криптографических механизмов в устройствах с ограниченной вычислительной мощностью является одной из ключевых задач современной информационной безопасности. Ограниченные ресурсы встроенных систем не позволяют эффективно использовать многие традиционные алгоритмы шифрования, что обусловило развитие направления легковесной криптографии.

Проведенный анализ показал, что современные легковесные алгоритмы способны обеспечивать необходимый уровень защиты при минимальных затратах памяти, вычислительной мощности и энергии. Наиболее перспективными решениями являются PRESENT, GIFT, SIMON, SPECK и Ascon, демонстрирующие высокую эффективность в устройствах Интернета вещей.

Использование легковесной криптографии позволяет повысить безопасность IoT-инфраструктур, увеличить срок автономной работы устройств и снизить стоимость их эксплуатации. В дальнейшем развитие данного направления будет играть важную роль в обеспечении надежной защиты данных в условиях стремительного роста числа подключенных устройств.

Список литературы:

1. Stankovic J. A. Research Directions for the Internet of Things. IEEE Internet of Things Journal. 2014. Vol. 1, No. 1. P. 3–9. DOI: 10.1109/JIOT.2014.2312291.
2. Beaulieu R., Shors D., Smith J. et al. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. URL: https://eprint.iacr.org/2013/404
3. Bogdanov A., Knudsen L. R., Leander G., Paar C., Poschmann A., Robshaw M., Seurin Y., Vikkelsoe C. PRESENT: An Ultra-Lightweight Block Cipher. In: Cryptographic Hardware and Embedded Systems – CHES 2007. Lecture Notes in Computer Science, vol. 4727. Springer, 2007. P. 450–466. DOI: 10.1007/978-3-540-74735-2_31
4. National Institute of Standards and Technology. Ascon-Based Lightweight Cryptography Standards for Constrained Devices. NIST Special Publication 800-232. Gaithersburg: NIST, 2025.