СЕТИ СВЯЗИ И МУЛЬТИСЕРВИСНЫЕ УСЛУГИ

УДК 004.056, 681.51
DOI: 10.18469/ikt.2025.23.1.01

ИССЛЕДОВАНИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ДЛЯ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Сорокин И.А.
Нижегородский государственный инженерно-экономический университет, Княгинино, РФ
E-mail: ivansorokin@bk.ru

Криптографические методы необходимо использовать для надежного и стабильного обеспечения безопасности систем с целью минимизации риска внешних атак и повышения их эффективности. Беспроводные сенсорные сети (WSN) играют ключевую роль в сборе, мониторинге, обработке и накоплении исходных данных для улучшения работы исполнительных механизмов, микроконтроллеров, встроенных архитектур, IoT-устройств и вычислительных машин, к которым они подключены. В условиях множества потенциальных угроз важно повысить уровень безопасности беспроводных сенсорных сетей, не затрагивая их основную функцию – беспрепятственный сбор и передачу данных на промежуточные устройства. Данная работа направлена на исследование предыдущих и текущих научных исследований в этой области. В результате проведенного исследования в статье будут рассмотрены наиболее подходящие криптографические алгоритмы, которые лучше всего подойдут для обеспечения безопасности беспроводных сенсорных сетей, защиты от угроз и снижения уязвимостей. Это исследование станет основой для будущих работ в данной области, предоставив комплексный и всесторонний взгляд на рассматриваемую тему.

Ключевые слова: *легковесная криптография, рассеивание энергии, потребление энергии, хеширование, открытый ключ, закрытый ключ, беспроводные сенсорные сети, симметричный ключ, криптография, алгоритм, эффективность, распределение ключей, память, временная и пространственная сложность, безопасность*

Постановка задачи

Беспроводные технологии в области связи вместе с энергосберегающими решениями открыли новые перспективы для беспроводных сенсорных сетей (WSN), которые также связаны с развивающимися направлениями, такими как предсказание данных, обучение и анализ. WSN быстро набирают популярность благодаря автоматизации промышленных и производственных процессов, а также развитию технологий MEMS (MicroElectroMechanical Systems) и сенсоров.

Согласно общепринятому определению из Wikipedia, WSN представляют собой пространственно-распределенные автономные сенсоры, которые совместно отслеживают физические или экологические условия, такие как температура, звук, вибрация, давление, движение или загрязнители. Эти небольшие и недорогие устройства могут фиксировать малейшие изменения в окружающей среде, наблюдать их в течение заданного времени, а затем передавать собранные данные на базовую станцию для дальнейшей обработки, проведения вычислений и исследований.

Обработка огромных объемов данных является ключевой функцией WSN. Они играют важную роль в сборе данных в реальном времени, их передаче и дальнейшей обработке. Однако безопасность WSN вызывает серьезные опасения ввиду их уязвимости перед различными видами киберфизических атак. Чаще всего WSN развертываются в сложных климатических условиях для выполнения задач наблюдения в неблагоприятной среде, например, в зонах боевых действий, на ледяных горных вершинах, в густых лесах или на глубине океанов. Это делает их уязвимыми для атак, которые могут нарушить конфиденциальность, целостность и доступность данных.

Кроме того, WSN стали неотъемлемой частью современных технологий, включая медицину, метеорологию, управление чрезвычайными ситуациями, сельское хозяйство, умные дома, экологические проекты, управление дорожным движением и многое другое. Надежная передача данных через WSN необходима для обеспечения точности и достоверности информации. Однако в условиях открытых каналов связи существует угроза модификации данных, их компрометации, подмены, воспроизведения и других атак.

Основной задачей является предотвращение таких атак, защита устройств и поддержание общей целостности системы. Для этого используются протоколы, которые обеспечивают конфиденци-

альность, целостность, доступность, аутентификацию, авторизацию, двустороннюю секретность и невозможность отказа от переданных данных.

Проект направлен на изучение комплексного влияния на основные определяющие параметры WSN: потребление энергии, энергоэффективность и общее время работы сети.

WSN играет жизненно важную роль в мониторинге и записи физических и экологических данных. В свете трагического инцидента с австралийскими лесными пожарами специализированная и эффективная WSN могла бы обеспечить раннее обнаружение и предотвратить катастрофу. Поскольку WSN является устройством с ограниченными ресурсами, проблемы масштабируемости и энергопотребления всегда актуальны. Таким образом, внедрение дополнительных мер безопасности в WSN увеличит вычислительную сложность и энергозатраты. Поэтому необходимо разработать умную и надежную архитектуру корректно функционирующей WSN, которая объединяет в себе две цели: повышение эффективности и усиление безопасности.

Для оптимизации затрат мы будем использовать широкий спектр криптографических техник, включая легковесное шифрование, DES (Data Encryption Standard), AES (Advanced Encryption Standard), и изучать поведение узлов, а также всей сети.

Это исследование позволит получить представление о производительности WSN при различных архитектурах безопасности.

Таким образом, мы сможем найти компромисс между эффективным улучшением функциональности WSN и снижением ее уязвимостей. Мы также изучим влияние SHA-256 (хеширование) и эллиптической криптографии (RSA/Diffie-Hellman) на виртуальный прототип WSN, чтобы проверить их совместимость с относительно низкой вычислительной мощностью и ограниченной памятью WSN.

Кроме того, мы сможем определить наиболее защищенный протокол маршрутизации для нашей WSN-модели, исходя из имеющихся ограничений в дизайне.

В таблице 1 подробно описываются все потенциальные атаки на WSN и приводится их классификация по различным уровням модели TCP/IP. Большинство атак относится к сетевому уровню, поскольку маршрутизация играет важную роль в архитектурном дизайне и функционировании WSN. Ограничения памяти, низкое энергопотребление, истощение энергии и недостаточная вычислительная мощность могут сделать устройство WSN уязвимым для этих разрушительных атак.

Предлагаемые криптографические алгоритмы должны соответствовать требованиям системы. Поскольку атаки происходят на различных уровнях сетевой системы, основанной на модели TCP/IP, алгоритмы должны обеспечивать высокую производительность. Следовательно, в зависимости от характера потенциальных атак разработчик должен применять соответствующий алгоритм.

Большинство атак приходится на сетевой уровень, так как он является наиболее уязвимым из-за своей топологии, основанной на маршру-

Таблица 1. Классификация WSN-атак

Физический уровень	Канальный уровень	Сетевой уровень (Маршрутизация)	Транспортный уровень
Подделка данных	Недобросовестность	Подмена	Десинхронизация
Глушение сигнала	Коллизии	Воспроизведение атак	Атака «затопление»
Внедрение сообщений	Истощение узла	Атака «карстовая воронка»	Подрыв узла
Физическая атака на узел	—	Атака «Черная дыра» Атака «hello»	Компрометация узла
—	—	Замедление червоточины	—
—	—	Атака «Сивиллы»	—
—	—	Бесконечный цикл	—
—	—	Выборочная пересылка	—
—	—	Репликация личности, изменение	—
—	—	Лишение сна, пытки	—
—	—	Подтвержденная подмена	—

тизации и пересылке данных – двух ключевых функций WSN. Поэтому знание возможных атак может помочь в разработке простых мер для стабилизации работы системы.

Эти атаки представляют собой критическую угрозу для работоспособности устройства, так как могут нарушить его полное функционирование.

Для прикладного уровня существуют потенциальные угрозы, такие как атака стимулирования (Stimuli Attack) и внедрение пакетов (Packet Injection), которые не были упомянуты в таблице 1.

Решение

В настоящее время существует множество криптографических методов. Некоторые из них были разработаны еще на заре становления современной криптографической технологии в конце XX века.

Позже многие из этих методов были усовершенствованы и модернизированы, получив новые модификации и оптимизации по сравнению с их предыдущими версиями.

Фундаментальное понимание криптографических методов необходимо для осознания данной проблемы, связанной с повышением уровня безопасности WSN, при этом, не ухудшая ключевые показатели ее производительности.

Все потенциальные криптографические методы должны соответствовать качественным характеристикам защищенной WSN, обеспечивая конфиденциальность, целостность, доступность, аутентификацию данных, их актуальность и невозможность отказа от переданной информации.

Криптография с симметричным ключом, а также методы хеширования обеспечат нашей криптосистеме базовую защиту для бесперебойной передачи данных, восстанавливая и поддерживая свойства целостности и конфиденциальности в среде беспроводной связи.

Данные исследования будут дополнительно рассмотрены далее, где будет обсуждаться гибридизация алгоритмов.

Рисунок 1 демонстрирует различные протоколы безопасности WSN, которые широко используются в настоящее время.

Криптография с открытым ключом является символом аутентификации данных и их доступности, поскольку она предоставляет возможность эффективного распределения и управления ключами, что позволяет сканировать всех участвующих субъектов на наличие вредоносной активности.

Таким образом, любая возможная угроза со стороны противника, как внутри системы, так и от внешнего агента, будет устранена.

Полная блок-схема рабочего процесса представлена на рисунке 2. Она охватывает процедуру проектирования, которой необходимо следовать для проверки всех соответствующих криптогра-

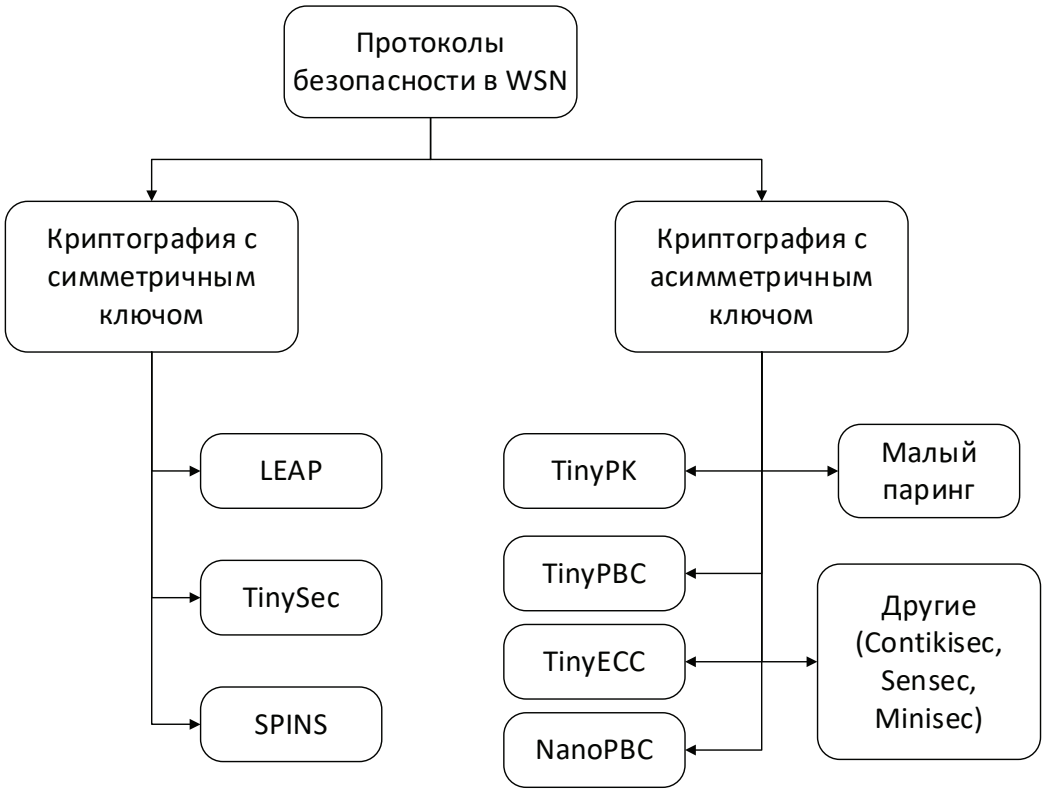

Рисунок 1. Пример протоколов безопасности в WSN

фических алгоритмов на предмет их потенциальной применимости в WSN.

Для тестирования предлагаемых криптографических алгоритмов в нашей модели WSN мы используем платформу симуляции.

Наш проект во многом будет основываться на применении этих алгоритмов, а также традиционных методов, таких как AES, DES, хеширование и MAC. Эти алгоритмы будут внедрены в модель WSN, после чего будет проведен анализ их поведения.

Выбранный нами сетевой симулятор поможет смоделировать виртуальный прототип реалистичной WSN и изучить ее параметры при различных условиях с использованием различных криптографических методов.

Проект охватывает области криптографии и сетевой безопасности, а также затрагивает основные аспекты архитектуры WSN и базового аппаратного обеспечения.

Также в нем рассматриваются принципы работы WSN и ее сетевые функциональные возможности.

В конечном итоге проект даст наглядное представление о влиянии существующих криптографических алгоритмов на WSN.

Одной из основных проблем в области WSN является максимизация общего времени работы сети устройства.

Агрегация данных может значительно снизить энергозатраты системы, что поможет достичь необходимого уровня энергоэффективности.

Агрегация данных определяется как метод сбора и объединения данных.

Агрегация данных является одним из ключевых этапов в обеспечении механизма энергосбережения в WSN.

Этот метод лежит в основе принципов проектирования.

В двух словах, три основные цели процесса агрегации данных заключаются в максимальном увеличении времени жизни сети для всех узлов, повышении энергоэффективности устройства и минимизации потерь мощности системы.

Для агрегации данных можно использовать энергоэффективный и безопасный протокол агрегации данных на основе шаблонов (ESPDA – Energy-Efficient Secure Pattern-based Data Aggregation) [1].

Этот метод позволяет контролировать избыточность в системе, исключая дублирование передаваемых пакетов.

Таким образом, агрегация данных является ключевым фактором эффективности WSN и может даже способствовать усилению ее безопасности.

Распределение и управление ключами

Различные характеристики, связанные с эффективными методами распределения ключей в типичной WSN, можно определить следующим образом:

1. Масштабируемость архитектуры.
2. Оптимизация потребления энергии.
3. Снижение потерь мощности.
4. Эффективное использование памяти.
5. Увеличение времени жизни сети.
6. Снижение вычислительных затрат.
7. Поддержание объема данных в допустимых пределах.
8. Обновление и возобновление работы с ключами.
9. Плавный обмен данными.
10. Бесперебойная связь между узлами сети.
11. Усиление защиты от возможных атак.

Основная суть легковесной криптографии заключается в адаптации упрощенной версии стандартных криптографических методов за счет уменьшения размеров входных данных и других параметров с целью снижения энергопотребления в модели WSN.

Кроме того, аппаратная реализация алгоритмов легковесной криптографии будет проще и позволит легче интегрироваться в аппаратную архитектуру WSN.

Легковесная криптография широко применяется в устройствах, имеющих критические ограничения на вычислительную мощность. Важнейшим фактором здесь является компромисс между низким потреблением ресурсов и безопасностью устройства.

Исследователи разработали новые методы эффективного применения поточных и блочных шифров, хеш-функций и других методов шифрования и расшифрования для создания надежного криптографического дизайна.

На рисунке 3 представлена схема баланса проектирования. Разработчикам необходимо корректировать уровень безопасности, размер и стоимость системы, чтобы повысить ее производительность. Таким образом, архитектура должна сбалансированно сочетать последовательные или более оптимизированные параллельные версии.

Количество криптографических раундов должно варьироваться от 8 до 48, а размер ключа должен быть от 80 до 256 бит, чтобы исключить вероятность атак.

Такие оптимизированные легковесные методы позволят устройствам работать быстрее и эффективно сократят общий срок службы WSN. Следовательно, чем меньше времени функционирует WSN, тем ниже будет ее энергопотребление.

Легковесные устройства также имеют значительно более низкую себестоимость производства и занимают меньше места благодаря своей гибкости и возможности компактного размещения на поверхности устройства.

Блочные шифры являются одним из основных методов криптографии, представляя собой упрощенную версию традиционных криптографических методов.

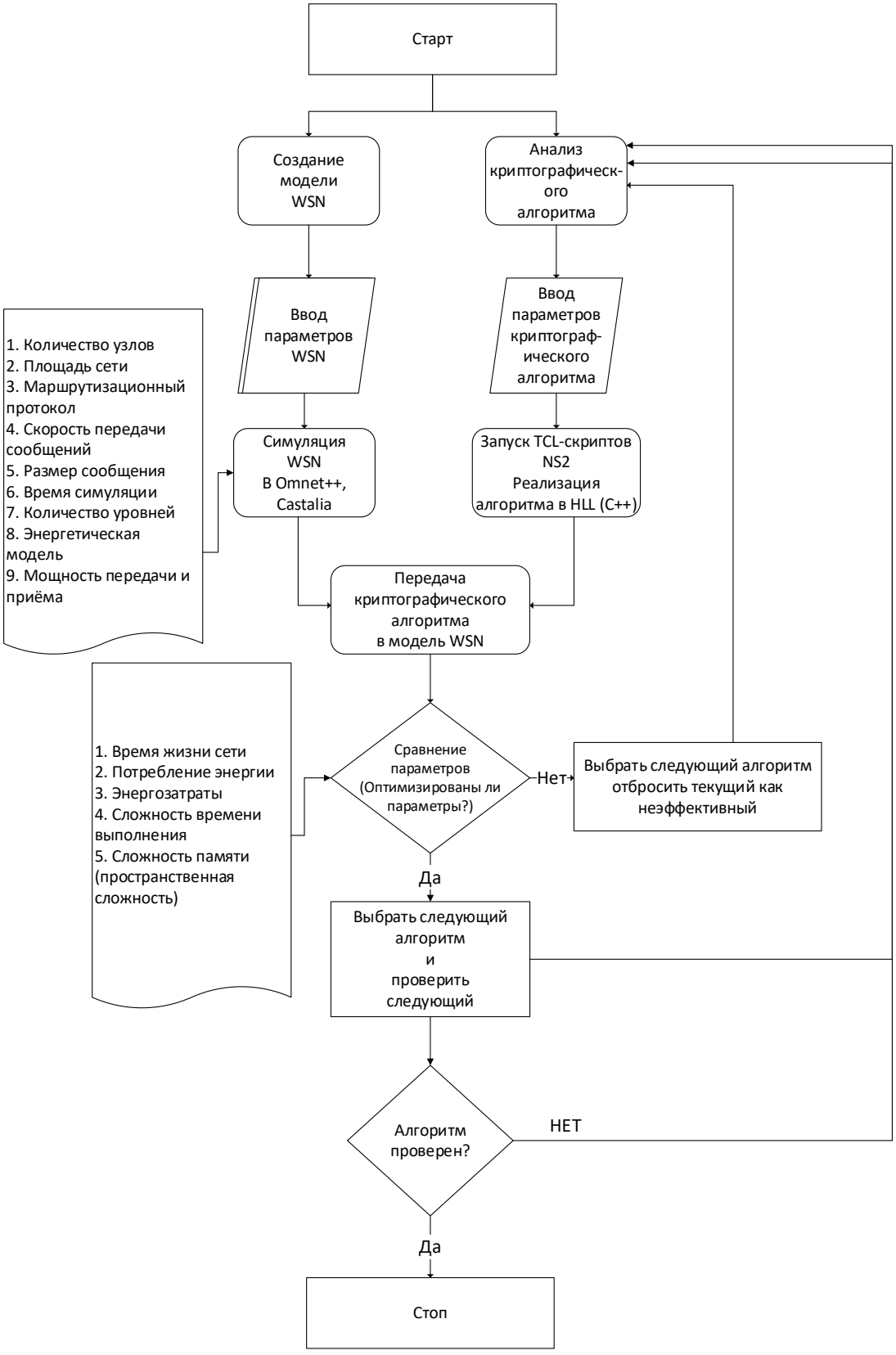

Рисунок 2. Блок-схема всего рабочего процесса

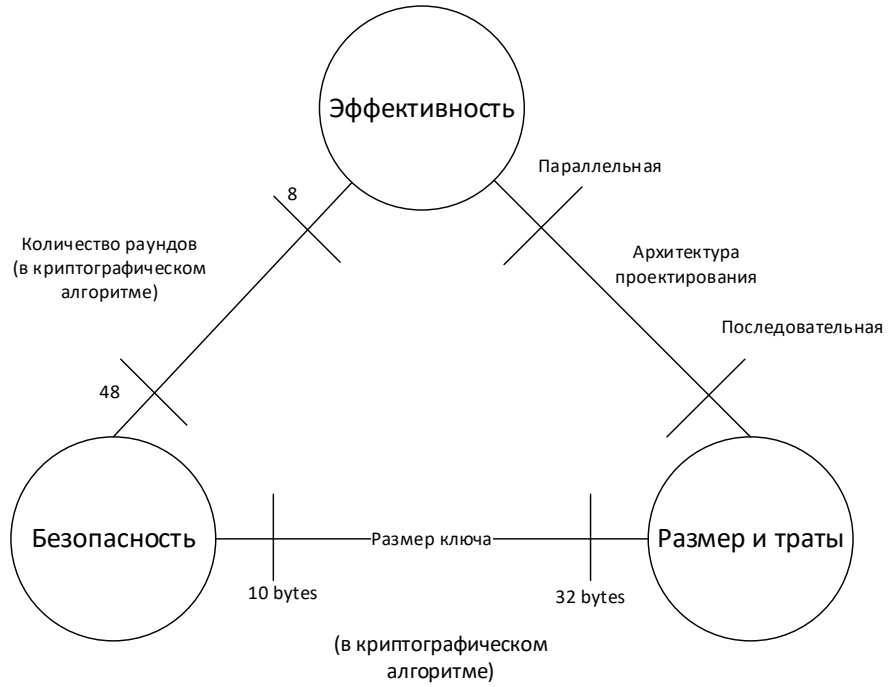

Рисунок 3. Компромисс параметров легковесных криптографических алгоритмов

На рисунке 4 показана классификация легковесных криптографических алгоритмов, которые мы рассматриваем и применяем в нашей работе.

В этом разделе рассматриваются и анализируются различные современные легковесные версии существующих блочных шифров с точки зрения их потенциального применения в WSN (беспроводных сенсорных сетях), а также M3WSN (мобильных мультимедийных беспроводных сенсорных сетях).

AES. AES (Advanced Encryption Standard) принимает на вход блок данных длиной 128 бит и ключ длиной 128 бит, выполняя 10 раундов операций в сети подстановок и перестановок (SPN (Service Principal Name)).

AES также поддерживает ключи длиной 192 и 256 бит. Однако AES сам по себе не обеспечивает достаточный уровень безопасности для WSN.

DESL (Data Encryption Standard Lightweight) и *DESXL (Data Encryption Standard Xor Lightweight)*. Предложенные в [2] алгоритмы представляют собой модификации стандартного симметричного шифра DES.

DESX принимает входной блок длиной 64 бита и ключ длиной 184 бита, выполняя 16 раундов на основе структуры Фейстеля.

DES обладает высоким уровнем безопасности и энергоэффективностью. Благодаря оптимизированному размеру, он широко используется в потоковых шифрах.

PRESENT. Алгоритм PRESENT [3] принимает входной блок размером 64 бита и ключ 128 бит, выполняя 32 раунда итераций.

Первые 32 раунда включают линейную перестановку, нелинейную подстановку и операцию XOR.

Этот алгоритм защищен от атак сдвига и атак, связанных с ключами.

В целом, PRESENT используется для устранения недостатков AES и является более оптимизированной версией AES, особенно в условиях ограниченных ресурсов.

CLEFIA. CLEFIA – это алгоритм, разработанный компанией SONY [4], как улучшенная и более защищенная версия AES.

Этот алгоритм совместим с AES, так как работает с блоками по 128 бит и поддерживает ключи длиной 128, 192 или 256 бит.

Эксперименты показали, что CLEFIA обеспечивает максимальную эффективность при размере ключа 128 бит и 18 раундах на структуре Фейстеля.

Этот алгоритм имеет высокую скорость выполнения и устойчив к дифференциальному и линейному криптоанализу.

CLEFIA демонстрирует лучшую производительность, чем PRESENT, в плане пропускной способности, но PRESENT превосходит CLEFIA по уровню безопасности и использованию памяти.

KATAN. Алгоритм KATAN [5] представляет собой блочный шифр, применяемый для потокового шифрования.

Он поддерживает разные размеры блоков (32, 48, 64 бита) и размер ключа 80 бит, выполняя 256 раундов для шифрования.

Метод потокового шифрования в KATAN основан на загрузке обработанных блоков в пару

регистров сдвига, которые затем используются в качестве регистров обратной связи для нелинейных функций.

HIGHT. HIGHT [6] – алгоритм, который использует блоки по 64 бита и ключ длиной 128 бит, выполняя 32 раунда на структуре Фейстеля.

HIGHT легко реализуется, поддерживает встроенные архитектуры WSN и подходит для ультралегковесных систем.

Однако его производительность уступает традиционным блочным шифрам.

KLEIN. Алгоритм KLEIN [7] использует блоки размером 64 бита и ключи 64, 80 или 96 бит.

Этот метод работает на основе сети подстановок и перестановок (SPN) и выполняет 12, 16 или 20 раундов итераций.

Алгоритм устойчив к дифференциальному криптоанализу, однако остается уязвимым к интегральным атакам.

TWINE. Алгоритм TWINE [8] – блочный шифр с блоками 64 бита и ключами 80 или 128 бит, работающий на структуре Фейстеля типа 2.

На ранних этапах разработки алгоритму не хватало диффузионных свойств, но позже он был усовершенствован в [9] путем изменения структуры Фейстеля.

Обновленная версия защищена от атак «Meet-in-the-Middle» и обеспечивает быстрое шифрование за счет генерации уникальных случайных чисел, предотвращающих атаки сдвига (Slide Attack).

Существует множество других алгоритмов. Все они тщательно изучены и представлены в таблице 2 для удобства сравнительного анализа между различными моделями блочных шифров.

Эти алгоритмы вычислительно не сложны и демонстрируют хорошую производительность в процедурах безопасности WSN.

На основе дополнительных исследований и других статей, связанных с промышленным применением WSN, стало очевидно, что PRESENT, CLEFIA и HIGHT широко используются в работе WSN в контексте блочного шифрования.

PRINT. Авторы работы [10] представили симметричный блочный шифр PRINT, который применяется при печати интегральных схем (Integrated Circuit, IC).

Этот алгоритм использует блоки длиной 48 или 96 бит и ключи длиной 80 или 160 бит, работая на структуре сети подстановок и перестановок (SPN).

PRINT выполняет операцию XOR с раундовым ключом и выполняет 96 операций итераций.

Этот метод устойчив к алгебраическим атакам, атакам на связанные ключи и атакам дифференциального криптоанализа высокого порядка.

Описание параметров блочных шифров

В таблице 2 подробно описываются все алгоритмы с их параметрами, что создает основу для сравнительного анализа и выбора оптимального алгоритма.

SPN (Substitution-Permutation Network) означает сеть подстановок и перестановок.

Из 20 алгоритмов, представленных в таблице 2, более подробно разобраны 8 основных методов.

Экспериментально доказано, что общая энергоэффективность WSN при использовании блочных шифров выше, чем при применении потоковых шифров.

В целом, ключевыми параметрами блочного шифра, которые играют решающую роль в энергопотреблении WSN, являются:

A. Выбор вектора инициализации.

B. Количество раундов итераций.

C. Размер ключа и длина блока.

D. Выбор и настройка ключа.

Поскольку потоковые шифры редко используются в работе WSN, в данной области существует ограниченное количество исследований, представленных в таблице 3. В частности, ссылки [2] и [8] касаются работ, посвященных хаотическим потоковым шифрам.

В [2] авторы разработали защищенную криптосистему, которая гарантирует возможность безопасного шифрования данных между всеми узлами WSN.

Кроме того, этот метод оптимизирует потребление энергии и снижает стоимость устройства, а также обеспечивает защиту от атак «человек посередине» (MITM (Man-in-the-Middle)) и атак воспроизведения (Replay Attacks).

В [8] представлена разработка потокового шифра eLoBa, который снижает накладные расходы на передачу данных и демонстрирует устойчивость к алгебраическим атакам.

Этот метод исключает вероятность модификации данных и их подделки со стороны вредоносных внешних агентов.

MD5, SHA1 и RIPEMD – это одни из самых известных криптографических хеш-алгоритмов, которые обеспечивают надежность механизмов подписи сообщений.

Однако хеш-функции подвержены значительным накладным расходам, а шифрование как таковое не является их основной задачей. Это особенно заметно в методах, таких как Message Authentication Code (MAC) и других алгоритмах хеширования, основанных на случайных ключах.

Таблица 2. Табличное представление блочных шифров

Название шифра	Структура	Длина блока	Размер ключа	Количество раундов
LED	SPN	64	128	32/48
AES-128	SPN	128	128	10
PRESENT	SPN	64	80,128	31
NOEKEON	SPN	128	128	16
MCRRYPTON	SPN	64	96,128	12
PRINCE	SPN	64	128	12
PRINT	SPN	48,96	80,160	96
KLEIN	SPN	64	80,96	12/16/20
BSPN	FESITEL	64	64	8
CLEFIA	FESITEL	128	128	18
DESXL	FESITEL	64	184	16
SKIPJACK	FESITEL	64	80	32
LBLOCK	FESITEL	64	80	32
HIGHT	FESITEL	64	128	32
PICCOLO	FESITEL	64	80,128	25/31
SEA	FESITEL	96	96	Variable
TWINE	FESITEL	64	80/128	36
TEA & XTEA	FESITEL	64	128	64
KATAN & KTANTAN	FESITEL	32	64/80	254
MIBS		64	80/128	32
IDEA	LAI-MASSEY	64	128	8,5

Таблица 3. Табличное представление потоковых шифров

Потоковый шифр	Размер ключевого потока (байт)	Количество циклов
Sosemanuk	80	8559
Trivium	80	80
Salsa	64	17812
Grain	80	80
RC4	1	311

Основная цель хеширования в криптосистемах – обеспечение целостности данных.

В [9] авторы разработали легковесную однонаправленную хеш-функцию, устойчивую к атакам на прообраз и коллизии, не использующую ключевую структуру.

Этот метод позволяет снизить накладные расходы для алгоритмов MD5 и SHA1. Однако этот подход не был экспериментально протестирован в WSN, поскольку в нем отсутствует механизм аутентификации сообщений и поддержка работы в реальном времени.

Поскольку MAC использует ключевую структуру, его применение не считается оптимальным для WSN.

В работе [10] автор разработал аналогичный алгоритм, как в [9], также основанный на однонаправленном хешировании, но с улучшенными характеристиками накладных расходов.

В исследованиях [3] и [4] авторы использовали MAC-ориентированную криптосистему, которая:

1. Обеспечивает аутентификацию данных и целостность сообщений.

2. Защищает от атак воспроизведения (Replay Attacks).

HMAC (Hash-based Message Authentication Code) – это еще одна передовая техника, в которой размер ключа определяет уровень безопасности криптосистемы [11].

Метод HMAC также использовался в [8], где применяется генератор псевдослучайных чисел и ключ.

Этот подход поддерживает аутентификацию данных и обеспечивает конфиденциальность информации на каждом узле WSN, предотвращая несанкционированный доступ соседних узлов и внешних злоумышленников.

Поскольку WSN требует надежного механизма защиты, комбинация методов симметричного и асимметричного шифрования позволяет обеспечить высокий уровень безопасности, сочетая эффективность криптографии с открытым ключом и простоту проектирования криптографии с закрытым ключом.

В [9] предложена трехуровневая схема обеспечения безопасности, охватывающая:

– конфиденциальность (Elliptic Curve Cryptography (ECC) и Advanced Encryption Standard (AES));

– целостность (с использованием Message Digest-5 (MD5));

– аутентификацию (XOR-DUAL RSA).

С точки зрения размера шифрованного текста, энергопотребления WSN, времени шифрования и расшифрования, этот гибридный алгоритм превосходит существующие решения.

Таким образом, данный метод уменьшает вычислительную нагрузку на узлы и снижает общие энергозатраты.

Преимущества и недостатки гибридного подхода изложены ниже.

Хотя криптография с симметричным ключом более эффективна по затратам и вычислительным ресурсам, ее недостаток заключается в необходимости безопасного обмена секретным ключом между сторонами.

С другой стороны, криптография с асимметричным ключом решает эту проблему за счет эффективного распределения ключей, но имеет высокую вычислительную сложность.

Поэтому гибридное решение является оптимальным выбором, поскольку сочетает лучшие стороны обоих подходов.

Использование двух типов ключей дает полный контроль над пространством ключей, что обеспечивает стойкость к атакам методом полного перебора (brute-force).

Таким образом, гибридные методы находят широкое применение в криптосистемах для шифрования изображений, делая их практически неуязвимыми.

Фазы работы гибридного алгоритма

На первом этапе обеспечивается конфиденциальность и защита информации за счет комбинации ECC и AES.

На втором этапе реализуются доступность данных и аутентификация пользователей с помощью XOR-DUAL-RSA.

Для обеспечения целостности системы применяется хеширование MD5, которое выполняет функцию цифровой подписи сообщений.

Другие гибридные решения

В [10] предложен гибридный алгоритм, основанный на последовательном шифровании AES и ECC.

Он обеспечивает базовую защиту в беспроводных сетях автономных сенсорных узлов.

Однако у этого метода повышенное время выполнения, что может замедлять работу системы.

В [6] исследована комбинация DES и RSA (Rivest, Shamir и Adleman) для решения задач блочного шифрования и распределения ключей.

Однако безопасность этой схемы оказалась слабой, особенно при малых размерах ключей.

В результате этот метод более уязвим для криптоанализа и медленнее, чем чистая симметричная криптография.

В [12] разработана гибридизация алгоритмов ECC и RC4.

ECC (Elliptic-curve cryptography, криптография на эллиптических кривых) применяется для эффективного распределения ключей и оптимизации памяти.

RC4 (потоковый шифр) используется для ускорения процессов шифрования и расшифрования.

Хотя этот метод снижает энергопотребление и повышает пропускную способность, его уровень безопасности остается под вопросом.

Таким образом, гибридные криптографические алгоритмы позволяют компенсировать недостатки отдельных методов, однако каждый вариант имеет свои особенности, которые необходимо учитывать при выборе оптимального решения.

В работе [8] авторы предложили трехэтапную гибридную методику, направленную на минимизацию времени выполнения.

На первом этапе применяется алгоритм AES, после чего на втором этапе используется DES.

После прохождения этих двух последовательных раундов, обеспечивающих базовую безопасность, в финальном этапе применяется модифицированная версия алгоритма RSA (mRSA, Modified Rivest–Shamir–Adleman).

Последний этап отвечает за упрощенное распределение ключей.

Благодаря распределенному выполнению шифрования на трех этапах, обеспечивается параллельная обработка, что позволяет достичь лучших результатов по сравнению с каждым из алгоритмов, используемым отдельно.

Методы асимметричного ключа также являются неотъемлемой частью различных технологий, используемых в моделях WSN.

По сравнению с технологиями закрытого ключа, эти алгоритмы обеспечивают лучшую модель для защиты конфиденциальности и аутентификации информации.

Схемы распределения ключей и методы цифровой подписи являются отличительными признаками этих алгоритмов.

Tiny-PK – это легковесная версия криптосистемы RSA, которая требует аутентификации цифрового сертификата, основанного на протоколе

согласования ключей Диффи-Хеллмана (Diffie-Hellman).

Благодаря своему относительно небольшому размеру, криптография на эллиптических кривых (ECC) часто используется в WSN-приложениях.

Схема распределения ключей этого метода вычислительно легковесная и обладает высокой эффективностью.

Четкий анализ компромисса между методами RSA и ECC в криптографии с открытым ключом представлен в работе [7].

ECC превосходит RSA (Rivest, Shamir и Adleman) в плане меньшей сложности памяти.

Время, затрачиваемое на процессы шифрования и расшифрования при фиксированном размере ключа, меньше у ECC, чем у RSA.

Даже более оптимизированные версии RSA, такие как та, что использует Китайскую теорему об остатках (Chinese Remainder Theorem), уступают ECC.

Размер ключа 60/224/256 бит для ECC обеспечивает тот же уровень безопасности, что и ключи RSA размером 1024/2048/3072 бит.

Широко известный Multi Prime RSA, как еще одна версия алгоритма, демонстрирует худшую временную и операционную эффективность по сравнению с ECC.

Авторы [7] также описали преимущества ECC перед RSA и другими симметричными методами шифрования, которые используются в настоящее время.

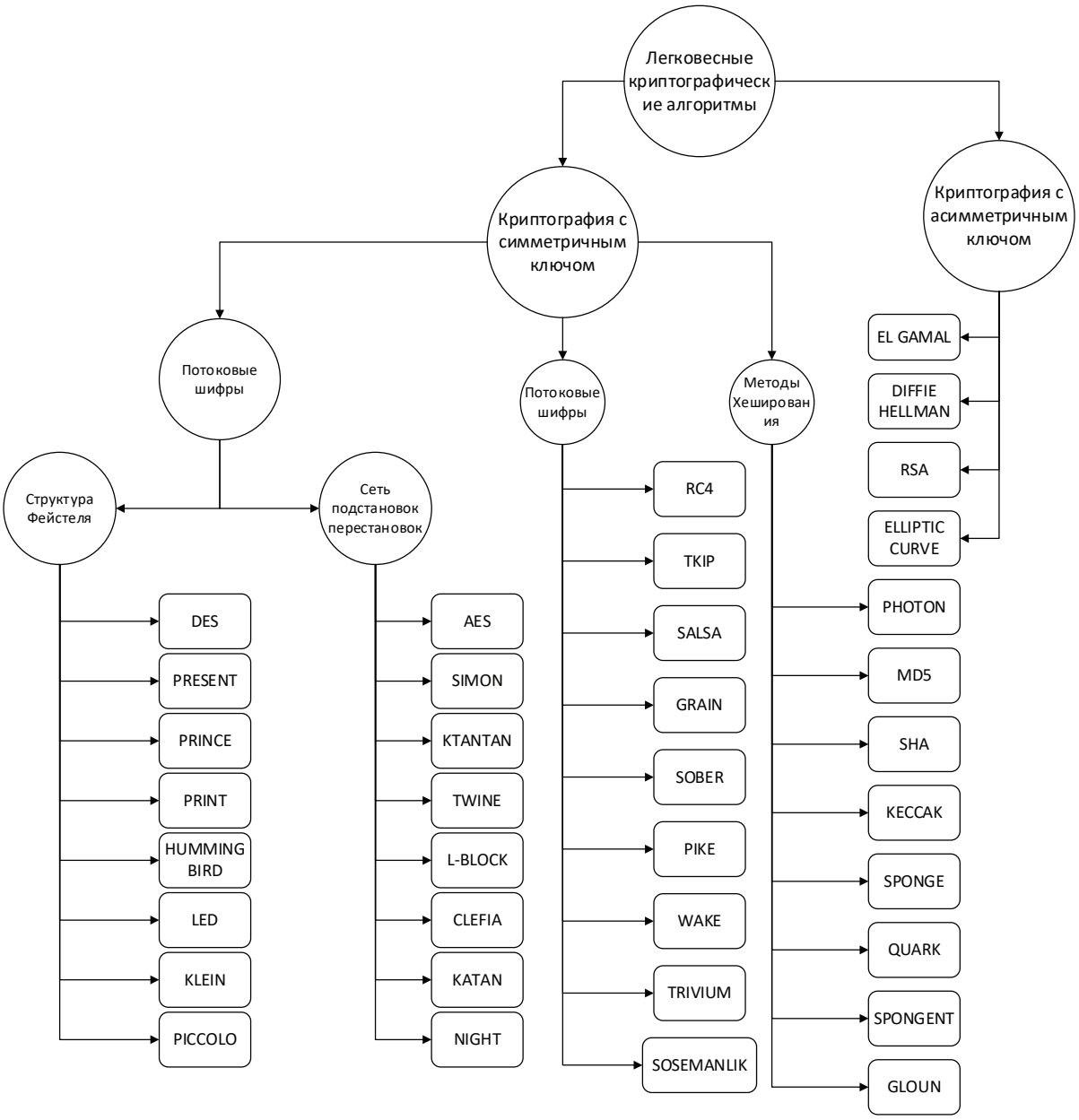

Рисунок 4. Классификация легковесных криптографических алгоритмов

Основная идея заключается в улучшении моделей с использованием модифицированных координатных техник и эластичных окон для предотвращения атак анализа мощности (SPA, Special Power Analysis).

Метод TINY-ECC представляет собой легковесный механизм, который обеспечивает схему цифровой подписи, протокол согласования ключей и операцию шифрования с открытым ключом.

Однако он также имеет недостаток в виде низкой масштабируемости.

Недостатки, связанные с их потенциальным применением в WSN, создают предпосылки для более широкого использования ECC (таблица 4).

Таблица 4. Проблемы нескольких криптографических алгоритмов с открытым ключом

Название алгоритма криптографии с открытым ключом	Проблема в применении WSN
Chor-Rivest Knapsack	Подмножество суммы
Digital Signature Algorithm [DSA]	Высокая временная сложность
RSA	Сложность памяти
Mc Eliece	Декодирование линейных кодов
El Gamal	Диффи-Хеллман
Blum Goldwasser	Сложность пространства
Rabin	Факторизация целых чисел

Это обеспечит более высокую степень актуальности данных, подлинность узлов, целостность информации и конфиденциальность в архитектуре встроенных систем.

Однако, с дальнейшим развитием квантовой криптографии, алгоритмы криптографии с открытым ключом сталкиваются с большими вызовами ввиду существования новейших исследований в области квантовых вычислений, в частности алгоритма Шора (Shor's algorithm).

Существует множество других криптографических методов, которые здесь не рассматриваются.

Эта область постоянно развивается, поэтому возможно появление новых методов и технологий.

До этого раздела мы представили всесторонний обзор преимуществ и недостатков существующих алгоритмов.

Ниже приведен краткий обзор полезности этих алгоритмов в контексте их применения в WSN.

Рисунок 5 показывает круговую диаграмму, отражающую процентное соотношение использования этих алгоритмов в современных архитектурах безопасности WSN.

Выводы

В этой работе рассмотрены потенциальные алгоритмические методы, которые могут быть использованы для повышения уровня безопасности беспроводных сенсорных сетей.

Результаты исследования позволяют утверждать, что методы криптографии с закрытым ключом, а также методы хеширования широко применяются в WSN.

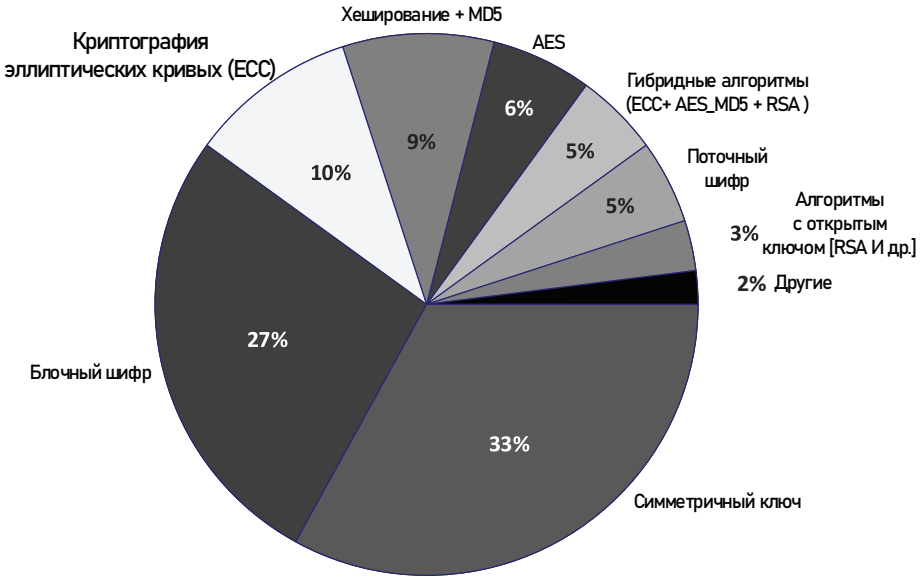

Рисунок 5. Круговая диаграмма, отображающая применение легких криптоалгоритмов в WSN

В этой работе мы рассмотрели передовые достижения в области криптографии и сетевой безопасности.

Она охватывает многочисленные алгоритмы, предназначенные для реализации в WSN, с целью снижения вероятности различных видов атак.

Мы подробно рассмотрели различные виды атак, которые представляют угрозу и могут потенциально нарушить основную цель развертывания WSN.

Во всех предыдущих разделах мы методично описали синтез всех возможных криптографических систем и алгоритмов, которые обеспечат максимальную безопасность WSN.

Гипотетически возможно построить криптосистему, обладающую всеми необходимыми характеристиками для поддержки конфигурации WSN.

Однако на данный момент пока еще не существует полной и динамичной системы, которая могла бы обеспечить стопроцентную защиту криптосистемы WSN.

Проект направлен на достижение статистического сравнения эффективности WSN при использовании различных криптографических алгоритмов.

Это позволит получить четкое и всестороннее представление о таких дополнительных аспектах WSN, как управление ключами и их распределение, а также происхождение данных при использовании оптимального алгоритма.

Дополнительные исследования и моделирование приведут к получению четкого представления о методах работы криптографических алгоритмов в WSN.

В ближайшем будущем планируется написать TCL-скрипты в NS2 и запустить существующие алгоритмы на смоделированной WSN, чтобы получить более конкретное подтверждение нашей идеи.

В качестве подготовки мы изучили несколько научных работ по моделированию, в которых проводились аналогичные эксперименты и были сделаны соответствующие выводы.

В скором времени мы разработаем собственную симуляцию и запустим соответствующие скрипты для проверки алгоритмов.

На данный момент параметры WSN уже разработаны в виде черновых записей.

Мы наметили методологии для систематизации наших наблюдений и формирования конкретного вывода.

Основным результатом и ключевым выводом данного исследования является превосходство алгоритмов криптографии с закрытым ключом над их асимметричными аналогами с открытым ключом.

Наряду с различными легковесными методами хеширования, эти техники доказали свою надежность и обеспечивают достаточный уровень безопасности для решения возникающих проблем.

Они являются наиболее подходящими для использования в WSN.

Среди методов криптографии с открытым ключом ECC демонстрирует наибольшую эффективность в плане меньшей сложности памяти, повышенной скорости работы и лучшей безопасности по сравнению с другими методами.

Таким образом, основным выводом является использование техники криптографии с симметричным ключом и гибридизация метода хеширования для оптимизации атрибута аутентификации системы. В критически важных случаях достаточно будет использовать только первый метод.

Литература

1. Лебедева Д.Ю. Пути оптимизации энергопотребления в беспроводных сенсорных сетях // Язык в сфере профессиональной коммуникации: материалы международной научно-практической конференции преподавателей, аспирантов и студентов. Екатеринбург: ООО «Издательский Дом «Ажур», 2021. С. 495–499.
2. New lightweight DES variants / G. Leander [et al.] // Fast Software Encryption (FSE 2007). Lecture Notes in Computer Science. 2007. Vol. 4593. P. 196–210. DOI: 10.1007/978-3-540-74619-5_13
3. PRESENT: An ultra-lightweight block cipher / A. Bogdanov [et al.] // Cryptographic Hardware and Embedded Systems (CHES 2007). Lecture Notes in Computer Science. 2007. Vol. 4727. P. 450–466. DOI: 10.1007/978-3-540-74735-2_31
4. Ищукова Е.А., Куликов А.В. Исследование алгоритмов анализа шифра CLEFIA // Современные наукоемкие технологии. 2019. № 12-2. С. 287–292.
5. Ищукова Е.А., Толоманенко Е.А. Анализ алгоритмов шифрования малоресурсной криптографии в контексте интернета вещей // Современные наукоемкие технологии. 2019. № 3-2. С. 182–186.
6. Вычислительно асимметричные преобразования и схемы из обратимых элементов / А.Е. Жуков [и др.] // Вопросы кибербезопасности. 2015. № 2 (10). С. 49–55.
7. Жуков А.Е. Легковесная криптография. Часть 2 // Вопросы кибербезопасности. 2015. № 2 (10). С. 2–10.

8. Жуков А.Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. 2015. № 1 (9). С. 26–43.
9. Пестунов А.И., Перов А.А., Пестунова Т.М. О некоторых направлениях научных исследований в области криптоанализа симметричных алгоритмов // Вестник НГУЭУ. 2016. № 3. С. 280–298.
10. Бабенко Л.К., Ищукова Е.А. Анализ симметричных криптосистем // Известия ЮФУ. Технические науки. 2012. № 12 (137). С. 136–147.
11. Чиликов А.А. Атака методом анализа сбоев на алгоритмы выработки имитовставок HMAC и NMAC // Математика и математическое моделирование. 2020. № 4. С. 65–92.
12. Исследование реализации механизмов инкапсуляции ключей постквантовых криптографических методов / А.В. Власенко [и др.] // Прикаспийский журнал: управление и высокие технологии. 2019. № 4 (48). С. 121–127.

Дата поступления 24.01.2025
Дата принятия 24.02.2025

Сорокин Иван Александрович, к.т.н., доцент кафедры инфокоммуникационных технологий и систем связи Нижегородского государственного инженерно-экономического университета. 606340, Российская Федерация, г. Княгинино, ул. Октябрьская, 22 а. Тел. +7 960 191-11-01. E-mail: ivansorokin@bk.ru

UDC 004.056, 681.51
DOI: 10.18469/ikt.2025.23.1.01

RESEARCH OF CRYPTOGRAPHIC ALGORITHMS FOR WIRELESS SENSOR NETWORKS

Sorokin I.A.
Nizhny Novgorod State University of Engineering and Economics, Knyaginino, Russian Federation
E-mail: ivansorokin@bk.ru

Cryptographic techniques are essential for reliable and stable provision of system security in order to minimize the risk of external attacks and improve its efficiency. Wireless sensor networks play a key role in collecting, monitoring, processing and accumulating raw data in order to improve the operation of actuators, microcontrollers, embedded architectures, IoT devices and computing machines to which they are connected. In the presence of many potential threats, it is important to enhance the security of wireless sensor networks without affecting their primary function – seamless collection and transmission of data to intermediate devices. This work aims to examine the previous and current scientific research in this area. As a result of the conducted research, the article will consider the most suitable cryptographic algorithms that are best suited to ensure wireless sensor networks security, protect against threats and reduce vulnerabilities. This study will form the basis for future work in this area, providing a comprehensive and in-depth view on the topic considered.

Keywords: *lightweight cryptography, energy dissipation, energy consumption, hashing, public key, private key, wireless sensor networks, symmetric key, cryptography, algorithm, efficiency, key distribution, memory, time and space complexity, security*

Sorokin Ivan Aleksandrovich, Nizhny Novgorod State University of Engineering and Economics, 22a, Oktyabrskaya Street, Knyaginino, 606340, Russian Federation; Associate Professor of Infocommunication Technologies Department, PhD in Technical Sciences. Tel. +7 960 191-11-01. E-mail: ivansorokin@bk.ru

References

1. Lebedeva D.Yu. Ways to optimize the energy consumption in wireless sensor networks. *Yazik v sfere professionalnoi kommunikatsii: materiali mezhdunarodnoi nauchno-prakticheskoi konferentsii prepodavatelei, aspirantov i studentov*. Ekaterinburg: OOO «Izdatel'skiy Dom «Azhur», 2021, pp. 495–499. (In Russ.)

2. Leander G. et al. New lightweight DES variants. *Fast Software Encryption (FSE 2007). Lecture Notes in Computer Science*, 2007, vol. 4593, pp. 196–210. DOI: 10.1007/978-3-540-74619-5_13
3. Bogdanov A. et al. PRESENT: An ultra-lightweight block cipher. *Cryptographic Hardware and Embedded Systems* (*CHES 2007*). *Lecture Notes in Computer Science*, 2007, vol. 4727, pp. 450–466. DOI: 10.1007/978-3-540-74735-2_31
4. Ishchukova E.A., Kulikov A.V. Research of CLEFIA cipher analysis algorithms. *Sovremennye naukoemkie tekhnologii,* 2019, no. 12-2, pp. 287–292. (In Russ.)
5. Ishchukova E.A., Tolomanenko E.A. Analysis of the algorithms for encryption of lightweight cryptography in the context of the internet of things. *Sovremennye naukoemkie tekhnologii,* 2019, no. 3-2, pp. 182–186. (In Russ.)
6. Zhukov A.E. et al. Computationally asymmetric transformations and reversible logic circuits. *Voprosy kiberbezopasnosti,* 2015, no. 2 (10), pp 49–55. (In Russ.)
7. Zhukov A.E. Lightweight cryptography. Part 2. *Voprosy kiberbezopasnosti,* 2015, no. 2 (10), pp. 2–10. (In Russ.)
8. Zhukov A.E. Lightweight cryptography. Part 1. *Voprosy kiberbezopasnosti,* 2015, no. 1 (9), pp. 26–43. (In Russ.)
9. Pestunov A.I., Perov A.A., Pestunova T.M. On some scientific problems in cryptanalysis of symmetric algorithms. *Vestnik NGUEU,* 2016, no. 3, pp. 280–298. (In Russ.)
10. Babenko L.K., Ishchukova E.A. Analysis of symmetric cryptosystems. *Izvestiya YuFU. Tekhnicheskie nauki,* 2012, no. 12 (137), pp. 136–147. (In Russ.)
11. Chilikov A.A. Fault attack on message authentication codes HMAC and NMAC. *Matematika i matematicheskoe modelirovanie,* 2020, no. 4, pp. 65–92. *(In Russ.)*
12. Vlasenko A.V. et al. Research of key encapsulation mechanisms based on postquantum cryptographic algorithms. *Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii,* 2019, no. 4 (48), pp. 121–127. *(In Russ.)*

Received 24.01.2025
Accepted 24.02.2025