КРИПТОГРАФИЧЕСКИЙ МОДУЛЬ ДЛЯ ЛЕГКОВЕСНЫХ БПЛА

Юрченко Е.Д.

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

Лапцевич А.А. – канд. физ.-мат. наук

Аннотация. Исследование посвящено комплексному анализу и проектированию гибридных криптографических структур для беспилотных летательных аппаратов. Интеграция дронов в экосистему Интернета вещей требует принципиально новых подходов к защите данных ввиду жестких ограничений по энергопотреблению. В работе исследуются векторы киберфизических атак, анализируется эффективность стандартов легковесной криптографии и обосновывается необходимость внедрения постквантовых алгоритмов. Основное внимание уделено архитектуре HLCAD++, совмещающей классическую асимметричную криптографию, постквантовые механизмы инкапсуляции и легковесное симметричное шифрование.

Ключевые слова. Беспилотные летательные аппараты, легковесная криптография, постквантовая криптография, HLCAD++, MAVLink, аппаратная защита, кибербезопасность, аутентифицированное шифрование.

Интеграция беспилотных летательных аппаратов (БПЛА) в концепцию Интернета дронов и грядущие сети связи шестого поколения открывает новые возможности для масштабирования автономных операций в логистике, мониторинге критической инфраструктуры и обеспечении безопасности. Однако переход к автономным роевым миссиям, требующим обработки данных в реальном времени, сталкивается с фундаментальным инженерным противоречием. С одной стороны, современные дроны генерируют огромные массивы строго конфиденциальной информации. С другой стороны, подавляющее большинство платформ базируется на вычислительных системах с жестко ограниченными ресурсами оперативной памяти, процессорного времени и емкости аккумуляторных батарей.

Энергетический баланс типичного квадрокоптера выстроен так, что подавляющая часть энергии расходуется на работу винтомоторной группы и удержание аппарата в воздухе. Выполнение ресурсоемких криптографических преобразований на центральном процессоре напрямую сокращает полетное время. Традиционные криптографические алгоритмы создают недопустимые вычислительные задержки в контуре управления полетом, где цикл обратной связи полетного контроллера обычно составляет от 20 до 50 миллисекунд. Следовательно, обеспечение комплексной безопасности требует радикального пересмотра подходов: отказа от программных надстроек общего назначения в пользу специализированных аппаратных криптографических модулей и легковесных алгоритмов.

Архитектура связи БПЛА подвергается непрерывным комбинированным киберфизическим атакам, направленным на деструктивное нарушение конфиденциальности, целостности и доступности телеметрических данных. Актуальные исследования классифицируют векторы этих атак на три категории: атаки на координацию внутри роя, атаки на радиочастотные каналы между дроном и наземной станцией, и атаки на внутренние шины данных самого аппарата. Злоумышленники способны генерировать фиктивные сигналы автоматического зависимого наблюдения-вещания (*ADS-B*), провоцируя ложные срабатывания систем предупреждения столкновений (*TCAS*).

Наиболее распространенными угрозами в радиоканалах остаются атаки типа «человек посередине» и атаки повторного воспроизведения. Перехватив легитимный пакет с командой, атакующий узел может транслировать его в эфир. Для превентивной нейтрализации подобных инцидентов в современные протоколы активно внедряются методы строгой криптографической валидации свежести входящего пакета.

Исторически популярные транспортные протоколы микроавиации, такие как *MAVLink* и *DroneCAN*, разрабатывались без учета механизмов информационной безопасности. Выпуск *MAVLink* 2.0 внедрил механизм криптографической подписи на основе монотонно возрастающего счетчика, однако протокол так и не получил нативной поддержки сквозного симметричного шифрования полезной нагрузки. Телеметрия передается в эфир в виде открытого текста. В ответ на это было разработано расширение *MAVSec*, где наилучшую эффективность показал современный потоковый шифр *ChaCha20*, не требующий выделения дополнительного объема оперативной памяти. Внутренние сети *DroneCAN*, хоть и используют статическое распределение памяти (*DSDL*) для предотвращения фрагментации кучи, также остро нуждаются во внедрении строгих политик контроля доступа на аппаратном уровне шины. Кроме того, технология удаленной идентификации (*Remote ID*) требует криптографического «ослепления» серийных номеров дронов для защиты коммерческой тайны.

Применение классических международных стандартов шифрования, таких как передовой стандарт шифрования *AES* с длиной ключа 128 или 256 бит, в контексте маломощных микроконтроллеров сопряжено с неприемлемыми издержками. Энергозатраты на выполнение базовых операций *AES*-128 на типичном микроконтроллере составляют около 1,2 Джоуля. В масштабах

непрерывной трансляции телеметрии с частотой 400 Гц этот показатель становится определяющим фактором сокращения полетного времени.

Революционным решением стала стандартизация Национальным институтом стандартов и технологий (*NIST*) семейства инновационных алгоритмов легковесной криптографии, таких как *ASCON* и *TinyJAMBU*. Алгоритм *ASCON* математически построен на архитектуре «криптографической губки». Важнейшим свойством нового стандарта является его нативная поддержка аутентифицированного шифрования с присоединенными данными (*AEAD*). Этот механизм позволяет за один проход перестановочного алгоритма обеспечивать одновременно скрытие полезной нагрузки и детерминированную генерацию тега криптографической целостности. Энергопотребление легковесных шифров составляет всего около 0,5–0,7 Джоуля, а экстремально малый размер внутреннего состояния *TinyJAMBU* (всего 128 бит) делает его идеальным кандидатом для аппаратной реализации. Сравнительные результаты представлены в таблице 1.

Таблица 1 – Данные об энергоэффективности различных алгоритмов для микроконтроллеров БПЛА

Криптографический алгоритм	Тип алгоритма	Среднее энергопотребление (Дж)	Оценка применимости для встраиваемых систем БПЛА	Защита от квантовых атак
HLCAD++	*AEAD + KEM + ECC*	0.5	Очень высокая	Да
ASCON-128a	Легковесный *AEAD*	0.7	Очень высокая	Нет
AES-128	Традиционный симметричный шифр	1.2	Средняя	Нет
CRYSTALS-Kyber512	Постквантовый инкапсулятор ключей	1.3	Средняя	Да

Стремительный технологический прогресс в области квантовых вычислений формирует угрозу для основ современной асимметричной криптографии. Поскольку жизненный цикл промышленных БПЛА составляет десятилетия, перехваченные зашифрованные данные могут быть сохранены злоумышленниками для гарантированной расшифровки в будущем. Форсированное внедрение алгоритмов постквантовой криптографии становится приоритетной задачей.

Однако попытка прямого внедрения, утвержденного NIST механизма инкапсуляции ключей на основе кристаллических решеток (*CRYSTALS-Kyber512*) сопряжена с инженерными трудностями. Алгоритм генерирует открытый ключ размером около 800 байт. В условиях, когда пропускная способность дальнобойного радиоканала не превышает 250 кбит/с, передача таких ключей создает катастрофические задержки при установлении сеанса связи. Кроме того, вычислительная сложность полиномиального умножения в кольцах требует двукратного расхода энергии аккумулятора по сравнению с классическими протоколами на эллиптических кривых.

Единственным жизнеспособным решением стала разработка гибридных архитектурных парадигм. Наиболее проработанным примером является архитектура гибридного легковесного криптографического алгоритма *HLCAD++* (*Hybrid Lightweight Cryptographic Algorithm for Drones*). Суть подхода заключается в строгом разделении фаз обработки трафика: ресурсоемкая асимметричная криптография используется редко (только при инициализации сессии), а непрерывная передача массивов телеметрии опирается на сверхбыстрое симметричное шифрование.

Архитектура *HLCAD++* интегрирует три криптографических примитива:

1. Классический протокол безопасного обмена на эллиптических кривых (*ECDH*, *Curve25519*), обеспечивающий субмиллисекундную задержку при мгновенном установлении базового уровня безопасности.

2. Постквантовый инкапсулятор ключей (*Kyber512*), добавляющий мощный внешний слой криптографической защиты от атак с применением квантовых компьютеров.

3. Сверхлегковесный симметричный шифр (*TinyJAMBU*-128), аппаратно обрабатывающий потоковые данные с пропускной способностью до 225 Мбит/с.

Слияние энтропии, независимо полученной от классического и квантового алгоритмов, осуществляется с использованием функции деривации ключа (*HKDF*) с полным соблюдением математического разделения доменов. Амортизированная энергетическая стоимость такого обмена ключами становится приемлемой: суммарный объем передаваемого полезного груза для установки защищенной сессии составляет всего около 1,5 килобайт. Для предотвращения избыточного расхода энергии в *HLCAD++* применяется интеллектуальный планировщик перешифрования, который

инициирует ротацию ключей не по таймеру, а при критических событиях: переполнении 96-битного счетчика nonce, фиксации высокого уровня потери пакетов или исчерпании бюджета подделок.

Реализация сложных криптографических механизмов исключительно программным способом внутри операционной системы реального времени (*ОСРВ*) признается стратегической уязвимостью. Наличие хотя бы одной уязвимости переполнения буфера в полетном стеке позволяет злоумышленнику прочитать оперативную память и извлечь корневые ключи. Для предотвращения подобных сценариев применяются передовые подходы строгой аппаратной изоляции: доверенные среды исполнения (*TEE*) и аппаратные криптографические модули (*HSM*).

Технология *TEE* аппаратно, на уровне кремниевого кристалла (например, *ARM TrustZone*), делит процессорное время, память и системные шины на защищенную и обычную зоны. Исследователи разработали специализированные среды (такие как *FC-TEE*), позволяющие перенести все криптографические операции в изолированную зону. Обычный системный процесс отправляет данные исключительно через строго контролируемый вызов безопасного монитора. Многоуровневый иерархический планировщик в *FC-TEE* позволяет выполнять криптографию в фоне с накладными расходами всего около 2,7% процессорного времени, не нарушая жестких ограничений контура управления.

В ситуациях, когда полетный контроллер не поддерживает *TEE*, применяется обязательная интеграция внешних автономных криптопроцессоров (*HSM*), таких как ATECC608B или *OPTIGA Trust* M. Эти чипы подключаются по стандартным шинам (*I2C*/*SPI*) и содержат аппаратные генераторы истинно случайных чисел на основе квантового теплового шума, ускорители эллиптической криптографии и глубоко защищенные ячейки энергонезависимой памяти. Извлечь секретные данные практически невозможно благодаря наличию активных датчиков вскрытия.

Обеспечение беспрецедентного уровня информационной безопасности БПЛА невозможно с использованием традиционных криптографических стандартов, вступающих в прямое противоречие с требованиями контуров управления полетом и емкостью бортовых аккумуляторов. Разрешение этого конфликта заключается в полном переходе на стандартизированные алгоритмы легковесной криптографии (*ASCON*, *TinyJAMBU*) для высокоскоростной передачи потоковых данных. Для защиты долговременных секретов от квантовых угроз в условиях узкополосных каналов связи оптимальным решением является использование гибридных многоуровневых фреймворков (*HLCAD++*). Фундаментом всей системы безопасности выступает обязательная аппаратная изоляция криптографических вычислений, реализуемая посредством доверенных сред исполнения (*TEE*) или автономных криптопроцессоров (*HSM*), что гарантирует надежность выполнения автономных миссий в условиях интенсивного кибернетического противодействия.

Список использованных источников:

1. Security Requirements for Cryptographic Modules, 2019. – 11 с

2. Department of Defense Test Method Standard: Environmental Engineering Considerations and Laboratory Tests, 2008. 804 с

3. Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions, 2024. 36 с

4. Zhaxygulova, D. Secure and Energy-Aware Cryptographic Framework for IoT-Enabled UAV Systems / D. Zhaxygulova [et al.] // Symmetry. – 2025. – Vol. 17, No. 11. – P. 1987.

UDC

CRYPTOGRAPHIC MODULE FOR LIGHTWEIGHT UAVS

Yurchenko E.D.

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Laptsevish A.A. – Candidate of Physical and Mathematical Sciences

Abstract. This study focuses on the comprehensive analysis and design of hybrid cryptographic structures for unmanned aerial vehicles. Integrating drones into the Internet of Things ecosystem necessitates fundamentally new approaches to data protection due to stringent power consumption constraints. The paper investigates cyber-physical attack vectors, analyzes the efficiency of lightweight cryptography standards, and substantiates the need for implementing post-quantum algorithms. Primary attention is devoted to the HLCAD++ architecture, which combines classical asymmetric cryptography, post-quantum encapsulation mechanisms, and lightweight symmetric encryption.

Keywords: Unmanned aerial vehicles, lightweight cryptography, post-quantum cryptography, HLCAD++, MAVLink, hardware security, cybersecurity, authenticated encryption.