УДК 004.057.4

**DOI:** 10.31673/2412-9070.2020.023438

**В. М. ЧЕРЕВИК**, канд. техн. наук, доцент;
**А. В. ГЛУЩУК**, аспірант,
Державний університет телекомунікацій, Київ

# ЗАХИСТ ІНФОРМАЦІЇ ПІД ЧАС ПЕРЕДАВАННЯ ПАКЕТІВ ДАНИХ ПО РАДІОКАНАЛУ Wi-Fi НА БАЗІ ПРОТОКОЛУ HTTP/3

***Обґрунтовано виконання послідовності операцій щодо захисту інформації в мережах на базі протоколу HTTP/3 з урахуванням стійкості захисту даних під час передавання по радіоканалу Wi-Fi. Зазначено, що основою практично стійкого криптографічного захисту пакетів інформації є використання абонентами мережі шифрів з одноразовим ключем (шифрів Вернама), які від пакета до пакета підлягають зміні. Для захисту інформації, використовуючи сеансові ключі парою абонентів (відправник інформації – отримувач інформації), доцільно застосовувати алгоритми асиметричного криптозахисту. З метою комплексного захисту даних у радіомережах інформація підлягає захисту на інформаційному рівні, на рівні формування сигнальникових конструкцій та на енергетичному рівні.***

**Ключові слова:** протокол; радіоканал; HTTP/3; Wi-Fi; HTTP-over-QUIC; MAC-адреса; AES; криптостійкість; криптографія; алгоритм; гаміювання масивів.

## *ВСТУП*

Широке застосування радіомереж у промисловості, на транспорті в телемедичних системах, в інформаційних системах безпеки руху транспортних засобів, відеомоніторингу та дистанційного моніторингу станів віддалених об'єктів вимагає від розробників інформаційних систем забезпечення конфіденційного та крипостійкого передавання даних у радіоканалі. Як правило, діапазони робочих смуг радіочастот поширених технологій побудови радіомереж (ZigBee, Wi-Fi, WiMax тощо) відомі багатьом користувачам, тому існує висока ймовірність доступу несанкціонованих абонентів радіомереж до масивів даних, що передаються в пакетах інформації, а також існує висока ймовірність підміни даних та імітації роботи санкціонованих абонентів мережі несанкціонованими користувачами. Сьогодні в радіомережах на базі протоколу HTTP/3 для захисту інформації чималого поширення дістали потокові методи шифрування даних [1-4], забезпечується комплекс заходів з автентифікації і авторизації абонентів мережі та захисту трафіку даних у процесі передавання по Wi-Fi радіоканалах навіть під час завад із поєднанням **MAC** (*Media Access Control*)-фільтрації з шифруванням **WPA** (*Wi-Fi Protecting Access*) та використанням міжмережних екранів. Сучасні інтелектуальні радіомодулі провідних комп'ютерних та мікроелектронних фірм світу для захисту даних в ISM-діапазоні радіочастот (**ISM** — *industrial, scientific, medical*: 433 МГц, 868 МГц, 902…928 МГц (для США), 2,4 ГГц) використовують 128-бітне AES-шифрування (**AES** — *Advanced Encryption Standard*). Було запропоновано новий метод захисту даних у комп'ютерних мережах на базі протоколу HTTP/3 [5], згідно з яким первинні масиви даних, що підлягають передаванню, не шифруються, а замість них передаються ознаки шифрованих даних. При цьому шифрування даних ґрунтується на заміні байтів первинного файла байтами спеціально організованого файла ключа.

Невирішеними проблемами захисту даних у сенсорних, локальних та локально регіональних радіомережах є організація передавання пакетів даних між віддаленими абонентами з урахуванням досягнення практичної стійкості криптографічного захисту інформації, яка б максимально відповідала вимогам теоретичної стійкості криптосистеми.

***Метою статті*** є розроблення та обґрунтування послідовності операцій щодо захисту інформації в радіомережах на базі протоколу HTTP/3 з урахуванням досягнення теоретичної стійкості захисту даних абонентами мережі під час передавання цих даних по Wi-Fi. При цьому виконання елементарних операцій захисту даних поєднується з оптимізацією процесів стиску даних та компактного кодування пакетів інформації, що передаються в каналах зв'язку з шумами. Таким чином, залежно від продуктивності абонентських процесорних засобів та наявного часу оброблення і кодування даних у місцях зародження інформаційних потоків абонентами радіомереж здійснюється ефективне кодування та передавання компактних, крипостійких та завадостійких інформаційних пакетів (ІП).

## *ОСНОВНА ЧАСТИНА*

### *Обґрунтування доцільності виконання комплексу операцій абонентами мережі для надійного захисту ІП*

Основна проблема захисту інформації в комп'ютерних мережах із протоколом HTTP/3 полягає

в поширенні абонентських секретних ключів. В ідеальному випадку абонент повинен мати такий секретний ключ (довге число), який не має бути відомим іншим абонентам. Водночас процес передавання інформації передбачає, що пара абонентів (відправник інформації – отримувач інформації) має володіти інформацією щодо поточних секретних ключів, використовуваних для шифрування/дешифрування інформаційних кадрів (ІК) пакетів даних. Основою практичної стійкості абонентських секретних ключів (СК) є теоретичні викладки К. Шеннона [6], згідно з якими в системах передавання інформації по мережі Wi-Fi необхідно, щоб поточний СК використовувався тільки один раз (тобто після шифрування і передавання бітів поточного ІК даний СК має бути замінено на інший), при цьому первинні дані ІК до шифрування { } і $X$, $i = 1,n$, $n$ — кількість бітів ІК, та шифрограма { } і $Y$ мають бути статистично незалежними для всіх можливих послідовностей бітів масивів { } і $X$ і { } і $Y$.

Із робіт Шеннона випливає, що в теоретично стійких секретних системах СК за обсягом не повинні бути меншими, ніж обсяг первинного тексту { } і $X$ та шифрограми { } і $Y$. На практиці прикладом такого шифру є шифр Вернама (шифр з одноразовим ключем), причому захист інформації ґрунтується на виконанні операції додавання за модулем 2 над відповідними бітами двох послідовностей [4; 5]: послідовності бітів первинного масиву даних $i\ n\ X\ x,\ldots,x,\ldots,x$ і послідовності випадкових бітів поточного СК $i\ n\ K\ k,\ldots,k,\ldots,k$. У результаті виконання операцій додавання за модулем 2 дістаємо криптограму $i\ n\ Y\ y,\ldots,\ y,\ldots y$, для якої справедливий вираз $Y = X \oplus K$, де $1\ 1\ 1\ y = x \oplus k,\ldots,i\ y = i\ i = x \oplus k,\ldots,\ n\ n\ n\ y = x \oplus k$, а $X \oplus 0 = X$, $X \oplus X = 0$. Істотною вимогою у процесі виконання операцій шифрування даних з одноразовим ключем є дотримання вимоги, щоб при виконанні кожної наступної операції шифрування (додавання за модулем 2) використовувався інший, незалежно згенерований СК. Відповідно для $j$-ї операції шифрування парою абонентів, що беруть участь у передаванні/прийманні ІП, генерується поточна послідовність випадкових бітів $j\ j\ i\ j\ n\ j\ K\ k\ k\ k + + + = ,\ldots, ,\ldots,1$.

Таким чином, базовими операціями захисту масивів даних ІП є використання абонентами мережі операцій генерації довготривалих псевдовипадкових послідовностей (ПВП), гаміювання відповідних масивів даних, формування перевірних кодів (ПерК) ІК пакетів даних та перемішування бітів ІК та бітів ПерК [4; 8], які було внесено до стандарту нового протоколу HTTP/3. Величина ступеня захисту інформації $zP$ пропорційна до величин масивів даних, що підлягають гаміюванню, тобто $[m]zP \cong \max 2$, де $m$ — мінімально необхідна довжина поточної ПВП, яка використовується для надійного захисту інформації ($m \geq 2048$ біт). Залежно від наявного часу оброблення та кодування даних по Wi-Fi на частоті 2,4 ГГц операцію гаміювання можливо виконувати одноразово, наприклад після виконання операцій стиснення даних без втрат та формування перевірних кодів або кодів, що виправляють помилки. Багаторазове виконання операцій гаміювання даних підвищує ступінь захисту інформації спотворенням (на основі виконання відповідних операцій гаміювання даних) первинних масивів даних до стиснення, у процесі стиснення даних без втрат (за рахунок реалізації оперативних алгоритмів стиснення-захисту двійкової інформації), після виконання операції перемішування компактних даних ІК із перевірним кодом (кодом, що виправляє помилки) та реалізації кінцевої операції гаміювання.

Вочевидь без знання абонентських СК несанкціонованим користувачам мережі HTTP/3 невідомі масиви даних до стиснення і після стиснення даних, а також кінцевий масив даних після завадостійкого кодування. Фактично, на інформаційному рівні реалізується ідея К. Шеннона, згідно з якою проблему створення стійкого СК, що не піддається розшифруванню, можна вирішити побудовою такого шифру, розкриття якого було б еквівалентне розв'язанню надскладної задачі.

Слід зазначити, що елементарні операції захисту інформації на абонентських системах радіоме-реж із протоколом HTTP/3 є відомими, проте невідомою є комбінація виконання елементарних операцій під час формування поточних кодів ПВП. Для збереження конфіденційності інформації про абонентські СК доцільно застосувати алгоритми захисту даних, побудованих на основі асиметричної криптографії з використанням закритих та відкритих абонентських ключів, які (закриті ключі) періодично змінюються центром розповсюдження ключів. Із метою реалізації крипостійкого та прихованого передавання інформації в шумах радіоканалу Wi-Fi мережі невідомими для сторонніх абонентів мають бути методи формування сигналів, що підлягають передаванню, а також структура цих сигналів [7; 8]. Тому захист даних абонентами радіомережі здійснюється на різних рівнях: на інформаційному рівні, на рівні формування сигнально-кодових конструкцій, що передаються на модулятор радіопередавача, на енергетичному рівні.

### *Реалізація оперативного захисту сигналів, зображень, відеоданих та масивів даних на абонентських системах радіомереж, які використовують технологію HTTP-over-QUIC*

Побудова інформаційно-ефективних радіомереж широкого застосування ґрунтується на реалізації в місцях зародження інформації методів

та алгоритмів багатофункціонального оброблення і кодування даних (сигналів, відеосигналів, масивів даних) з урахуванням мінімізації вихідних потоків крипостійких та завадостійких ІП. За теоретичну основу для побудови інформаційно-ефективних радіомереж на базі HTTP/3 із технологією HTTP-over-QUIC було взято теорему К. Шеннона про те, що за відповідних способів кодування та модуляції коефіцієнт пропускної здатності каналу зв'язку $\eta = R/C$ може бути дуже близьким до одиниці ($\eta \to 1$), де $R$ — швидкість передавання інформації, біт/с, у разі двійкового методу кодування; $C$ — пропускна здатність каналу зв'язку (теоретична максимальна швидкість передавання інформації). На практиці коефіцієнт $\eta \to 1$ за постійного підтримання швидкості передавання інформації $\max R \to R$ в умовах зміни відношення сигнал/шум у каналі зв'язку у великих межах. Відповідно основою побудови інформаційно-ефективних радіомереж із використанням HTTP/3 є формування абонентами мережі компактних (із мінімальною тривалістю), крипостійких та завадостійких пакетів даних [9].

У процесі кодування сигналів, які характеризуються мінімальними і максимальними значеннями амплітудних і частотних параметрів відповідно $\min X$ і $\max X$ та $\min f$ і $\max f$, доцільно виявляти та компактно кодувати найбільш інформативні (істотні) відліки, до яких належать екстремуми та точки перегину обвідної (точки зміни опуклості кривої). Для компактного кодування істотних відліків сигналу опосередковано визначається вхідне відношення сигнал/шум в околі істотних відліків [С/Ш]вх та середня крутість сигналу [4]. Отримані додаткові параметри відліків сигналів дають можливість вибрати (закодувати) оптимальну частоту Wi-Fi мережі під час дискретизації сигналу $f$ та кількість бітів $q$ для кодування відліків сигналів. Компактне кодування істотних відліків здійснюється з контрольованими втратами, тобто на чистих від шумів ділянках істотні відліки кодуються більш точно на противагу відлікам на зашумлених ділянках.

У разі кодування відеоданих необхідно зважати на особливості вихідних потоків сучасних відеосенсорів, які чимало залежать від формату відеокадру, прийнятої схеми кольорового відеокодування, топології побудови світлофільтрів відеосенсора та формату вихідних даних. У разі використання відеосенсорів із поширеною RGBG-топологією розміщення піксельних світлофільтрів матриці зображення розміром $M \times N$ ($M$ — кількість пікселів у рядку, $N$ — кількість пікселів у стовпчику (кількість рядків)), вихідні відеодані передаються процесорним пристроям від кадру до кадру. При цьому коди відповідних пікселів рядок за рядком по паралельній шині передаються на входи процесора. Із метою якісного відбиття відео-даних для кожного пікселя необхідно визначати три складові $R$-, $G$-, $B$-відліки, де $R$, $G$ і $B$ — коди відповідно червоного, зеленого і синього відліків. Таким чином, формуються $R$-, $G$- і B-сигнали, компактне кодування яких нічим не відрізняється від кодування аналогового сигналу (пошук істотних відліків та компактне кодування службових та інформативних бітів). Після аналізу та визначення амплітудно-часових характеристик істотних відліків на інтервалі вибірки відповідного сигналу, наприклад поточного рядка або групи рядків матриці $M \times N$, здійснюється компактне кодування даних із урахуванням наявності загальної службової інформації, службової інформації і компактних даних істотних і неістотних відліків відповідних рядків чи групи рядків поточного кадру. Для досягнення заданого коефіцієнта стиснення відеоданих із збереженням максимальної точності параметрів істотних відліків здійснюється рейтингове або порогове відсіювання найбільш інформативних істотних відліків відеосигналів. Подальшим резервом стиснення відеоданих є компактне кодування змін між групою сусідніх відеокадрів.

Здобуті компактні масиви даних із контрольованими втратами відліків сигналів (відеосигналів) підлягають подальшому стисненню на основі оперативного та адаптивного способу стиснення бітових масивів даних. У процесі стиснення масивів без втрат ефективно реалізується захист інформації з урахуванням відповідних кодів згенерованої ПВП. Як правило, будь-який масив двійкових даних характеризується нерівномірним розподілом $n$-бітових послідовностей, де $n = 3,4,5,6,\ldots$ . Здійснивши кодування первинних масивів даних з використанням відповідних шифрів із багаторазовим підставленням, можна істотно спотворити вміст масивів даних. При цьому істинний обсяг вихідного зашифрованого масиву даних буде меншим за первинний масив даних. Тому таку комплексну операцію можна назвати операцією «стиснення-захисту» даних. За рахунок гамію вання даних можливо змінювати характеристики розподілу $n$-бітових послідовностей, а поєднання операцій гамію вання та багаторазового підставлення двійкових послідовностей дає можливість надійно захистити масиви даних, що підлягають нагромадженню та передаванню по каналах зв'язку.

Для формування довготривалих ПВП доцільно використати генератори $M$-послідовностей із надвеликими утворювальними поліномами, наприклад $X\,163 + X\,7 + X\,6 + X\,3 + 1$ [10], а також $X\,41 + X\,20 + 1$, $X\,41 + X\,3 + 1$ [11]. Із метою генерації криптостійких ПВП кожний абонент використовує таблицю кодових ключів генерації бітів ПВП. На початку кожного циклу генерації дов-

готривалих ПВП, для підвищення її криптостійкості, випадковим чином змінюють послідовність слідування табличних номерів кодових ключів генерації елементарних ПВП. Використовуючи циклічно задану кількість бітів абонентського СК (поточного СК), гаміюємо біти кожного табличного номера кодового ключа з поточними бітами СК. Отже, утворюється додаткова таблиця кодових ключів із псевдовипадковим розміщенням номерів кодових ключів. Із додаткової таблиці беремо два сусідніх кодових ключа, генеруємо їх, утворивши поточний фрагмент елементарної ПВП, яка, у свою чергу, гаміюється з бітами ПВП, згенерованої на основі використання одного з надвеликих кодових ключів. Для уникнення довготривалих однотипних бітових послідовностей у вихідному потоці ПВП (довгих послідовностей нульових чи одиничних бітів) після обчислення допустимої величини однотипних бітів (цю величину можна змінювати в заданих межах випадковим чином) доцільно інвертувати наступний однотипний біт.

Таким чином, кожний абонент мережі має закритий секретний ключ, який невідомий іншим абонентам, а також володіє базою даних кодових ключів для генерації ПВП. За необхідності передавання пакетів даних *j*-му абонентові мережі *i*-й абонент направляє *j*-му абоненту коротке повідомлення і після отримання підтвердження від *j*-го абонента, направляє останньому сеансовий ключ (випадкове число), зашифрований засобами асиметричної криптографії. Після цього здійснюється передавання ІП, зашифрованих сеансовим ключем.

Альтернативний спосіб вирішення проблеми обміну ключами між абонентами радіомережі на базі протоколу HTTP/3 без використання засобів асиметричної криптографії полягає у такому: центр розподілу ключів генерує сеансовий ключ для передавання поточних пакетів, а далі доставляє по Wi-Fi мережі сеансовий ключ, зашифрований за допомогою секретних ключів кожного з двох абонентів. Після дешифрування повідомлення про сеансовий ключ абоненти використовують його під час передавання ІП до наступної зміни сеансового ключа.

### *Висновки*

**1.** У процесі передавання пакетів інформації в радіомережах на базі протоколу HTTP/3 із урахуванням досягнення практичної стійкості криптографічного захисту інформації, яка б максимально відповідала вимогам теоретичної стійкості криптосистеми, необхідно кожний інформаційний кадр поточного пакета шифрувати своїм секретним шифром. Відповідно шифри від пакета до пакета мають бути різні, при цьому первинні дані поточного інформаційного кадру та його шифрограма мають бути статистично незалежними масивами даних, оскільки передавання здійснюється по мережі Wi-Fi.

Основою практично стійкого криптографічного захисту пакетів інформації є використання абонентами мережі шифрів з одноразовим ключем (шифрів Вернама).

**2.** Базовими операціями захисту пакетів є генерація абонентами довготривалих псевдовипадкових послідовностей, гаміювання відповідних масивів даних, формування перевірних кодів або кодів, що виправляють помилки, та перемішування бітів інформаційного кадру та перевірних бітів. Для збереження конфіденційності інформації про абонентські секретні ключі доцільно використати алгоритми захисту даних (для передавання сеансових ключів), побудованих на основі асиметричної криптографії.

**3.** Із метою реалізації криптостійкого та прихованого передавання інформації в шумах радіоканалу Wi-Fi мережі невідомими для сторонніх абонентів мають бути методи формування сигналів, що підлягають передаванню, а також структура цих сигналів. Відповідно захист даних абонентами радіомережі на базі HTTP/3 має бути на різних рівнях: інформаційному, рівні формування сигнально-кодових конструкцій, енергетичному рівні.

**4.** Для побудови інформаційно-ефективних радіомереж завдяки мінімізації абонентами вихідних потоків криптостійких та завадостійких пакетів доцільно на кожній абонентській системі мережі реалізувати стиснення-захист масивів даних на основі оперативного та адаптивного способу стиснення бітових послідовностей. Для цього доцільно поєднати операції гаміювання та багаторазового підстановлення двійкових послідовностей.

**5.** Для формування довготривалих криптостійких псевдовипадкових послідовностей доцільно абонентами мережі використовувати базу даних кодових ключів для генерації ПВП, серед яких є ключі генераторів, наприклад *M*-послідовностей з надвеликими утворювальними поліномами. При цьому під час формування абонентами результуючої ПВП забезпечуються умови псевдовипадкового використання відповідних кодових ключів. Альтернативний спосіб вирішення проблем шифрування/дешифрування даних ІП (без використання засобів асиметричної криптографії) полягає в передаванні та використанні абонентами сеансового ключа, зашифрованого відповідними абонентськими ключами.

### *Список використаної літератури*

*1.* ***Столлингс В.*** *Основы защиты сетей на базе протокола HTTP/3: приложения и стандарты. Москва: Издательский дом «Вильямс», 2015. 429 с.*

*2. **Шахнович И. В.** Современные технологии беспроводной связи, 2-е изд. Москва: Техносфера, 2010. 288 с.*

*3. **Зубов А.** Совершенные шифры. Москва: Гелиос АРВ, 2012. 160 с.*

*4. **Шевчук Б. М., Задірака В. К., Фраєр С. В.** Ефективні методи фільтрації-стиску та захисту інформації в комп'ютерних мережах тривалого моніторингу станів об'єктів // Штучний інтелект. 2016. № 3. С. 804–815.*

*5. **Алишов Н. И., Марченко В. А., Оруджева С. Г.** Косвенная стеганография как новый способ защиты компьютерных данных // Комп'ютерні засоби, мережі та системи. 2010. № 8. С. 105–112.*

*6. **Шеннон К.** Теория связи в секретных системах. Работы по теории информации и кибернетике. Москва: Изд. иностр. лит., 1963. С. 333–369.*

*7. **Шевчук Б. М., Фраєр С. В.** Защита информации в компьютерных мониторинговых сетях на основе протокола HTTP/3, используя аскирования сжатых данных и передачи псевдослучайных шумоподобных пакетов информации // Компьютерная математика. 2016. № 1. С. 80–87.*

*8. **Урядников Ю. Ф., Аджемов С. С.** Сверхширокополосная связь. Теория и применение. Москва: СОЛОН-Пресс, 2015. 368 с.*

*9. **Шевчук Б. М.** Моделі та методи обробки, кодування і передачі інформації для побудови інформаційно-ефективних комп'ютерних мереж // Комп'ютерні засоби, мережі та системи. 2009. № 8. С. 81–89.*

*10. **ДСТУ 4145 – 2002.** Державний стандарт України. Інформаційні технології: Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.*

*11. **Новые алгоритмы** формирования и обработки сигналов в системах подвижной связи / А. М. Шлома, М. Г. Бакулин, В. Б. Крейнделин, А. П. Шумов; под ред. А.М. Шломы. Москва: Горячая линия-Телеком, 2008. 344 с.*

*В. М. Черевик, А. В. Глущук*

**ЗАЩИТА ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ПАКЕТОВ ДАННЫХ ПО РАДИОКАНАЛУ Wi-Fi НА БАЗЕ ПРОТОКОЛА HTTP/3**

*Обосновано выполнение последовательности операций по защите информации в сетях на базе протокола HTTP/3 с учетом устойчивости защиты данных при передаче по радиоканалу Wi-Fi. Отмечено, что основой практически устойчивой криптографической защиты пакетов информации является использование абонентами сети шифров с одноразовым ключом (шифров Вернама), которые от пакета к пакету подлежат изменению. Для защиты информации используются сеансовые ключи парой абонентов (отправитель информации – получатель информации) целесообразно использовать алгоритмы асимметричной криптозащиты. С целью комплексной защиты данных в радиосетях информация подлежит защите на информационном уровне, на уровне формирования сигнальных конструкций и на энергетическом уровне.*

**Ключевые слова:** протокол; радиоканал; HTTP/3; Wi-Fi; HTTP-over-QUIC; MAC-адрес; AES; криптостойкость; криптография; алгоритм; гаммирование массивов.

*V. M. Cherevik, A. V. Glushchuk*

**INFORMATION SECURITY IN THE TRANSMISSION OF DATA PACKETS OVER THE Wi-Fi CHANNEL ON THE BASIS OF THE HTTP/3 PROTOCOL**

*The article substantiates implementation of sequence of operations for protection of information in networks based on the HTTP/3 protocol, taking into account the sustainability of data protection during transmission over Wi-Fi radio. It is noted that the basis of a practically stable cryptographic protection of information packets is the use of a network of ciphers with a one-time key (Vernam ciphers) by subscribers. These ciphers are subject to change from package to package. To protect information, the session keys are used by a couple of subscribers (the sender of information is the recipient of information) it is advisable to use asymmetric cryptographic algorithms. For the purpose of comprehensive data protection in radio networks, information is subject to protection at the information level, at the level of formation of signal structures and at the energy level. When transmitting packets of information in radio networks based on HTTP/3 protocol, taking into account the achievement of practical stability of cryptographic protection of information, which would maximally meet the requirements of theoretical stability of the cryptosystem, each information frame of the current packet must be encrypted with its own secret cipher. Accordingly, the ciphers must be different from packet to packet, with the primary data of the current information frame and its cipher text must be statistically independent data sets since the transmission is via Wi-Fi. The basis of virtually stable cryptographic protection of information packets is the use of subscribers of a network of ciphers with a one-time key (Vernam ciphers). Basic packet protection operations are the generation of long-term pseudorandom sequences by subscribers, gamification of relevant data arrays, generation of error-correcting codes or codes, and mixing of information frame bits and validation bits.*

**Keywords:** protocol; radio channel; HTTP/3; Wi-Fi; HTTP-over-QUIC; MAC-address; AES; cryptographic strength; cryptography; algorithm; gammating of arrays.