УДК 004.056.55

ШИФРУВАННЯ ДАНИХ В АУДІОСИГНАЛАХ

П. В. Римар, К. О. Якубич

Існують два класи систем зв'язку: цифрові і аналогові. Цифровий сигнал – це сигнал, що має кінцеве число дискретних рівнів. Аналогові сигнали є безперервними. Типовим прикладом такого сигналу є мовний сигнал, який передається по звичайному телефону. Інформацію, передану аналоговими сигналами, також необхідно захищати, в тому числі і криптографічними методами.

Одним із таких методів захисту інформації в аудіо-сигналах є скремблювання звуку. Це шифрування потоку даних, в результаті якої він виглядає як потік випадкових бітів. Послідовність вхідних бітів шифрується за допомогою згенерованої послідовності шифруючих бітів, де імовірність появи одиниці або нуля однакова. Під час шифрування зберігається можливість дешифрувати послідовність.

Аудіо-скремблер – програмний або апаратний пристрій, що виконує скремблювання. Основною відмінністю аудіо-скремблерів від інших пристроїв, що виконують шифрування звукових сигналів, є те, що аудіо-скремблери можуть шифрувати безперервний аналоговий сигнал, не піддаючи його оцифруванню.

При скремблюванні аудіо-сигнал може бути перетворений за трьома параметрами: амплітудою, частотою та часом. Можливі перешкоди в каналах зв'язку впливають, в першу чергу, на амплітуду сигналу, в зв'язку з чим амплітудні перетворення застосовуються рідко. Частіше використовуються перетворення в частотній та часовій областях, а також їх комбінаціях.

Основні методи скремблювання звукових сигналів:

Частотні перетворення:

– Частотна інверсія сигналу (перетворення спектра сигналу за допомогою гетеродина і фільтра).

– Розбиття смуги частот мовного сигналу на кілька діапазонів і частотна інверсія спектра в кожному відносно середньої частоти діапазоні.

– Розбиття смуги частоти мовного сигналу на кілька діапазонів і їх частотні перестановки.

Часові перетворення

– Інверсія за часом сегментів мови.

– Часові перестановки сегментів мовного сигналу.

Комбіновані методи.

При частотній інверсії перетворення спектра мовного сигналу еквівалентно повороту частотної смуги сигналу навколо деякої середньої частоти Fи - частоти інверсії.

Декілька більш складний у порівнянні з частотною інверсії спосіб перетворення сигналу забезпечує скремблер з розбивкою смуги мовного сигналу на діапазони з частотною інверсією сигналу в кожному діапазоні (смугасто-зсувний інвертор). Зазвичай використовується розбиття смуги на 2 діапазони.

Смугові скремблери використовують спосіб розбиття смуги мовного сигналу на кілька діапазонів з частотними перестановками цих діапазонів. Смуговий скремблер може бути реалізований на основі швидкого перетворення Фур'є (ШПФ) [3]. В такому скремблері на передавальній стороні проводиться пряме ШПФ, частотна перестановка смуг, а потім – зворотне ШПФ. На приймальній стороні здійснюються аналогічні перетворення зі зворотною частотною перестановкою смуг. У скремблерах з ШПФ можливо досягти високого ступеня захисту інформації за рахунок збільшення кількості перемішуючих смуг, однак на практиці цей метод скремблювання в рухомому

радіозв'язку застосовується рідко в зв'язку зі складнощами технічної реалізації. Крім цього, скремблери з ШПФ вносять в канал зв'язку тимчасову затримку.

Найпростішим видом часового перетворення є часова інверсія, при якій вихідний сигнал ділиться на послідовність часових сегментів і кожен з них передається інверсно в часі – з кінця до початку.

У скремблері з часовими перестановками мовний сигнал ділиться на часові кадри, кожен з яких в свою чергу поділяється на сегменти, а потім сегменти мовного сигналу піддаються перестановці.

Для подальшого підвищення ступеня закриття мовлення використовується комбінація часового і частотного скремблювання. В такому скремблері після аналого-цифрового перетворення спектр цифрованого мовного сигналу розбивається на частотно-часові елементи, які потім перемішуються на частотно-часовій площині відповідно до одного з криптографічних елементів і підсумовуються, не виходячи за межі частотного діапазону вихідного сигналу.

Отже, скремблювання підвищує надійність синхронізації пристроїв, підключених до лінії зв'язку (забезпечує надійне виділення тактової частоти безпосередньо з прийнятого сигналу), зменшує рівень перешкод, випромінюваних на сусідні лінії багатожильного кабелю, та захищає інформацію, що передається, від несанкціонованого доступу.

Література

1. Журнал «Схемотехника». 2004, N12. С. 25–27.
2. Конахович Г. Ф., Климчук В. П., Паук С. М. Защита информации в телекоммуникационных системах. К.: «МК-Пресс», 2005. 288 с.
3. Нуссбаумер Г. Быстрое преобразование Фурье и алгоритмы вычисления сверток. М.: Радио и связь, 1985.

УДК 004.01

ЧОМУ БЛОКЧЕЙН – ЦЕ ЦІННО

А. І. Катаєва, К. В. Захарова

Застереження: Стаття несе ознайомчу мету, а не фінансову пораду.

03 січня 2009 року в 20:15 (GMT +2) невідомий створив перший (нульовий) блок першої в світі криптовалюти у розмірі 50 монет, вартістю $0.00 [1]. Станом на 18 квітня 2021 року 17:50 (GMT +3) цей блок коштував би $2,782,134.50. Через 12 років після запуску до обігу блокчейну, сьогодні вже створено більше 9 тис. різноманітних криптовалют, з загальною капіталізацією у розмірі більше 2-ох трильйонів доларів [2].

Як випадковий набір чисел може бути переведений на реальні, чималі, кошти? Відповідь полягає в унікальності проекту.

Що таке «блокчейн»?

Все, що потрапляє в блокчейн, навіки там і залишається.

«Блок-Чейн» (з англ. «Block» – блок, «Chain» – ланцюг) – збірна назва впорядкованих транзакцій (блоків), що зв'язані хешами (ланцюгами). Оскільки кількість платежів та переводів невпинно збільшується, збільшується і кількість блоків, так зародилася інтернет-система у вигляді хеш-дерева.

Кожен блок є цілком захищеним від підробки та будь-яких змін. Блок містить у собі наступну інформацію:

1. Хеш – унікальний ідентифікатор блока;