8. Sovlukov, A. S. Determination of liquefied petroleum gas quantity in a reservoir by radiofrequency techniques [Text] / A. S. Sovlukov, V. I. Tereshin // Proceedings of the 20th IEEE Instrumentation Technology Conference (Cat. No. 03CH37412). Vail, CO, USA. — 2003. — Vol. 1. — P. 368–373. doi:10.1109 / imtc.2003.1208182.
9. Sovlukov, A. S. Radiofrequency temperature-independent measurements of the density of liquefied hydrocarbon gases [Text] / A. S. Sovlukov, V. I. Tereshin // Measurement Techniques. — 2008. — Vol. 51, № 7. — P. 791–793. doi:10.1007/s11018-008-9116-z.
10. Совлуков, А. С. Проблемы и опыт разработки методик выполнения измерений для организации коммерческого учета СУГ [Електронный ресурс] / А. С. Совлуков, В. И. Терешин. — Режим доступа: \www/URL: http://www.avk-peterburg.ru/equipments/useful/art-2008-5. — 03.07.2014.

ИССЛЕДОВАНИЕ КОЛИЧЕСТВЕННОГО СОДЕРЖАНИЯ СЖИЖЕННОГО ГАЗА ПУТЕМ ИСПОЛЬЗОВАНИЯ МОДЕЛЬНЫХ ЖИДКОСТНЫХ СИСТЕМ

Предложена методика экспериментальных исследований по выбору модельной жидкостной системы, которая представляет собой соединение близкое к сжиженному нефтяному газу, и определению ее температурной зависимости, которая дает возможность подтвердить адекватность предложенного термометрического метода определения количественного содержания сжиженного нефтяного газа.

Ключевые слова: пропан, бутан, сжиженный нефтяной газ, количественное содержание, модельные жидкостные системы.

Білинський Йосип Йосипович, *доктор технічних наук, професор, завідувач кафедри електроніки, Вінницький національний технічний університет, Україна,* ***e-mail: yosyp.bilynsky@yandex.ru****.*
Книш Богдан Петрович, *аспірант, кафедра електроніки, Вінницький національний технічний університет, Україна,* ***e-mail: tutmos-3@i.ua****.*
Юкиш Марина Йосипівна, *асистент, кафедра електроніки, Вінницький національний технічний університет, Україна,* ***e-mail: yukish@yandex.ua****.*

Билинский Иосиф Иосифович, *доктор технических наук, профессор, заведующий кафедрой электроники, Винницкий национальный технический университет, Украина.*
Кныш Богдан Петрович, *аспирант, кафедра электроники, Винницкий национальный технический университет, Украина.*
Юкиш Марина Иосифовна, *ассистент, кафедра электроники, Винницкий национальный технический университет, Украина.*

Bilynskyy Yosy, *Vinnytsia National Technical University, Ukraine,* ***e-mail: yosyp.bilynsky@yandex.ru****.*
Knysh Bogdan, *Vinnytsia National Technical University, Ukraine,* ***e-mail: tutmos-3@i.ua****.*
Yukysh Maryna, *Vinnytsia National Technical University, Ukraine,* ***e-mail: yukish@yandex.ua***

УДК 003.26.09

Малік О. Р.

ЕМПІРИЧНЕ ДОСЛІДЖЕННЯ ФУНКЦІЇ РОЗПОДІЛУ ЧАСУ СИНХРОНІЗАЦІЇ НЕЙРОННИХ МЕРЕЖ В ПРОТОКОЛІ ОБМІНУ КЛЮЧАМИ

Представлено аналіз особливостей роботи протоколу обміну ключами з використанням взаємного навчання нейронних мереж, розглянуто існуючі атаки на протокол. Емпірично проаналізовано розподіл часу синхронізації нейронних мереж, що дозволило виявити слабкі місця протоколу та зробити висновок стосовно його захищеності.

Ключові слова: *нейронні мережі, взаємне навчання, протокол обміну ключами.*

1. Вступ

Нещодавно було показано, що дві нейронні мережі можуть синхронізуватися взаємним навчанням [1] і [2]. Нейронні мережі отримують на вхід однакове значення та обмінюються своїм виходом. Налаштування вагових коефіцієнтів відповідно до підходящого правила навчання призводить до повної синхронізації за скінченну кількість кроків у випадку дискретних значень. Така синхронізація нейронних мереж є частковим випадком онлайн навчання мереж, причому нейронні мережі починають з вагових коефіцієнтів, які було вибрано випадковим чином. Після цього відповідні вагові коефіцієнти у обох мереж мають однакове значення, навіть, якщо вони будуть оновлені наступним використанням правила навчання [3].

Саме цей факт було використано з метою побудови протоколу обміну ключем в роботі [4], що дало поштовх наступним роботам з побудовою більш складних протоколів і криптосистем. Не дивлячись на відсутність достатньо ґрунтовного аналізу стійкості, такі протоколи анонсуються захищеними, навіть в квантовій моделі обчислень [4], опираючись лише на той факт, що їх стійкість не базується на теоретико-числових задачах. З огляду на це, роботи з аналізом захищеності таких протоколів і систем є досить актуальними, оскільки напрям є достатньо новим і може виявитися перспективним, але вкрай необхідним є обґрунтування анонсованих властивостей подібних систем.

2. Аналіз літературних даних і постановка проблеми

TPM (від англ. *tree parity machine*) — це вид багатошарової нейронної мережі прямого поширення, яка складається з одного вихідного нейрону, K прихованих ней-

ронів та KN вхідних нейронів [1]. Загальна структура показана на рис. 1.

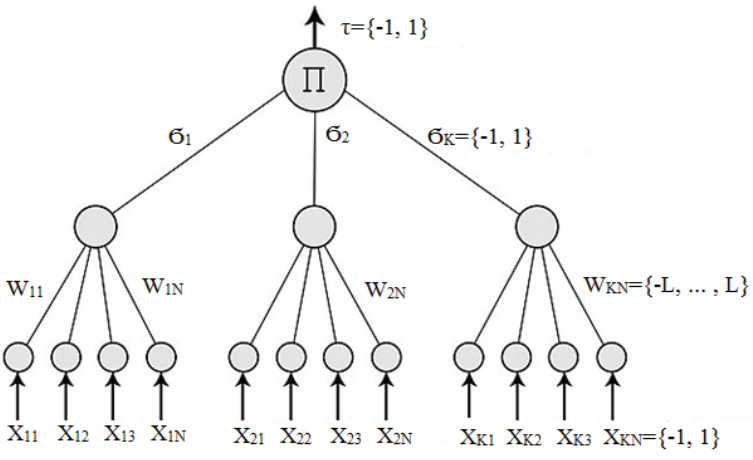

Рис. 1. Структура деревовидної машини парності

Вхідні нейрони приймають лише двійкові значення $x_{ij} \in \{-1,1\}$, де $i = \overline{1,K}$, $j = \overline{1,N}$. Кожен з прихованих нейронів є персептроном з вектором вагових коефіцієнтів w_i, $w_{ij} \in \{-L,..,0,..,+L\}$. Вихідне значення кожного прихованого нейрону i для вхідних значень x_{ij}, $j = \overline{1,N}$, обчислюється як $\sigma_i = \operatorname{sgn}\left(\sum_{j=1}^{N} w_{ij} x_{ij}\right)$. Для того, щоб вихідне x_{ij} значення було двійковим, з множини $\{-1,1\}$, функцію sgn() перевизначають наступним чином:

$$\operatorname{sgn}(x) = \begin{cases} -1, & x \le 0; \\ +1, & x > 0, \end{cases}$$

що відповідає біполярній ступінчастій функції активації. Значення вихідного нейрону, а отже, і вихідне значення всієї мережі на вхідних даних, обчислюється як $\tau = \prod_{i=1}^{K} \sigma_i$.

З наведеного вище слідує, що структура мережі TPM задається трьома параметрами K, N та L, тому на неї можна посилатися як на мережу TPM типу $K-N-L$ [3, 4].

Для модифікації вагових коефіцієнтів з метою навчання мережі TPM можна використовувати наступні правила навчання [5]:

— Анти-правило Хебба:

$$w_k^+ = w_k - \tau x_k \theta(\sigma_k \tau)\theta(\tau^A \tau^B).$$

— Правило Хебба:

$$w_k^+ = w_k + \tau x_k \theta(\sigma_k \tau)\theta(\tau^A \tau^B).$$

— Випадкове блукання:

$$w_k^+ = w_k + x_k \theta(\sigma_k \tau)\theta(\tau^A \tau^B).$$

Звичайно, потрібно впевнитись, що правило навчання не виводить вагові коефіцієнти за межу $\{-L,...,L\}$. Якщо вагові коефіцієнти виходять за межу, їх необхідно повернути до найближчої границі $-L$ або L. Це реалізується за допомогою функції $g(w)$:

$$g(w) = \begin{cases} \operatorname{sgn}(w)L, & |w| > L; \\ w, & \text{інакше.} \end{cases}$$

Під синхронізацією двох мереж будемо розуміти повне співпадання їх вагових коефіцієнтів.

В роботах [2–5] було показано можливість побудови криптографічного протоколу обміну ключами, який дістав назву ККК, використовуючи нейронні мережі саме такого спеціального виду — деревовидні машини парності. Для побудови протоколу обміну ключами кожен з абонентів A і B ініціалізує свою мережу TPM, вибравши випадкові значення вагових коефіцієнтів. Структура обох TPM має бути однаковою, тобто мають співпадати значення K, L та N, які можуть бути публічно відомими. Також має бути вибране спільне правило навчання мереж TPM.

Протокол обміну ключами ККК:

1. Згенерувати випадковим чином вектор вхідних даних x необхідного розміру.
2. Кожен з абонентів обчислює значення прихованих нейронів своєї мережі для вхідного вектору x.
3. Кожен з абонентів обчислює вихідне значення своєї мережі для вхідного вектору x, τ^A та τ^B відповідно, та передає це значення іншій стороні.
4. Якщо $\tau^A = \tau^B$, то кожен з абонентів застосовує правило навчання до своєї мережі.
5. Якщо мережі не синхронізовано, повернутися на крок 1.

Таким чином, для кожної ітерації, спочатку генерується випадковим чином вхідний вектор x (однією із сторін, або третьою стороною). Кожна із сторін обчислює вихідні значення прихованих нейронів та загальне вихідне значення своєї мережі для вхідного вектору x, τ^A та τ^B відповідно. Сторони обмінюються значеннями вихідних бітів τ^A і τ^B. Якщо вихідні біти різні, тобто $\tau^A \neq \tau^B$, то нічого не змінюється і генерується наступний вектор вхідних даних x. Якщо ж $\tau^A = \tau^B$, то кожен з абонентів застосовує правило навчання до своєї мережі TPM (але лише до тих прихованих нейронів, вихідне значення яких збігається із загальним вихідним значенням мережі), внаслідок чого зміняться її вагові коефіцієнти, і лише після цього генерується новий вектор вхідних даних для наступного кроку синхронізації [6].

Після певної кількості кроків мережі TPM обох абонентів будуть повністю синхронізовані [2–5], тобто їх мережі матимуть абсолютно однакові значення векторів вагових коефіцієнтів w^A та w^B. Саме це спільне значення можна використовувати як сформований ключ [1]. В оригінальній роботі [2] для навчання використовувалося анти-правило Хебба у випадку різних вихідних результатів мереж, що призводило до синхронізації векторів вагових коефіцієнтів, але з різними знаками. Але як було згодом показано в [7], що застосування правила Хебба є простішим і приводить до того ж результату. Моделювання показує, що навіть велика мережа потребує тільки скінченну кількість обміну бітами, близько 400 у випадку для $N = 100$, $L = 3$ [7].

Треба також відзначити, що процес повторюється доки вагові коефіцієнти абонентів A і B не будуть мати однакові значення $w^A = w^B$. Подальше застосування правила навчання не може зруйнувати синхронізацію, оскільки зміна вагових коефіцієнтів залежить тільки від вхідних значень та значення вагових коефіцієнтів, які є ідентичними у нейронних мереж абонентів A та B після синхронізації. Цей момент є досить нечітким, оскільки з протоколу не зовсім зрозуміло, коли саме настане синхронізація, або як порівняти вагові коефіцієнти, щоб впевнитися, що вони однакові у обох абонентів.

Стороння нейронна мережа може навчатись на прикладах, що беруть участь у протоколі, тобто вхідних і вихідних значеннях, що генеруються в процесі синхронізації. Оскільки ця нейронна мережа не може впливати на результати роботи мереж абонентів A та B, вона вважається «студентською» мережею [8]. Якби в протоколі використовувалися персептрони, які є більш простими нейронними мережами, неможливо знайти істотної різниці між кількістю кроків необхідних для синхронізації, та кількістю кроків, необхідних для навчання. В той час як у деревовидних машин парності можна спостерігати цікаве явище: дві нейронні мережі синхронізуються набагато швидше, ніж третя мережа, яка тільки підслуховує їх. Цю різниця між однонаправленою та двонаправленою взаємодією і було використано для вирішення задачі обміну ключами. Для цього абоненти A і B синхронізують свої деревовидні машини парності, причому вони генерують їх спільний ключ швидше ніж атакуюча сторона здатна знайти його шляхом навчання іншої нейронної мережі. Як наслідок, різниця між синхронізацією та навчанням має велике значення для забезпечення безпеки протоколу нейронного обміну ключами [2]. Треба відзначити, що за таких умов використовується лише пасивна модель зловмисника.

З огляду на представлений в роботах [2–5] новий протокол обміну ключами актуальною є задача перевірки його захищеності. Зокрема, з точки зору зловмисника цікавим є момент визначення синхронізації мереж абонентів, який не досить чітко описано в протоколі. **Метою даної роботи** є дослідження функції розподілу часу синхронізації мереж TPM різних K-N-L типів. Для досягнення поставленої мети необхідно було промоделювати роботу протоколу обміну ключами, використовуючи достатньо велику кількість TPM мереж різних K-N-L типів, щоб оцінити максимальне та середнє значення часу синхронізації мереж і спробувати використати особливості функції розподілу часу синхронізації мереж для виявлення слабких місць протоколу.

3. Існуючі стратегії атак на протокол обміну ключами

Спочатку опишемо існуючі стратегії атак на протокол, щоб показати важливість визначення моменту синхронізації мереж для захищеності абонентів.

Абоненти A і B використовують TPM з однаковою структурою, а параметри K, L та N є відкритими значеннями. Кожна нейронна мережа починає роботу з випадково вибраних вагових коефіцієнтів, значення яких тримаються у секреті. В процесі синхронізації, який описаний раніше, тільки вхідні вектори та спільні вихідні передаються по відкритому каналу. Тому кожен учасник знає тільки своє внутрішнє представлення $(\sigma_1,\sigma_2,\ldots,\sigma_k)$ власної TPM (значення прихованих нейронів для поточного вектору вхідних даних). Утримання цієї інформації в секреті має важливе значення для протоколу обміну ключами. Після досягнення повної синхронізації A і B використовують вагові вектори як спільний секретний ключ.

Основна проблема зловмисника E полягає в тому, що внутрішнє представлення $(\sigma_1,\sigma_2,\ldots,\sigma_k)$ деревоподібних машин парності абонентів A і B є для нього невідомими. Оскільки зміна вагових коефіцієнтів залежить від σ_i для успішної атаки важливо вгадати стан прихованих нейронів. На даний момент основні стратегії атак на протокол ККК представлено в роботах [7] і [9].

Генетична стратегія атаки.

Генетична стратегія полягає в тому, що зловмисник ініціалізує собі великий набір нейронних мереж TPM з аналогічною структурою, що і у двох абонентів протоколу. І далі вони навчаються за тими ж вхідними значеннями, що і мережі абонентів A та B. На кожному етапі приблизно половина мереж має на виході +1, а інша половина — вихідне значення, що дорівнює −1. Атака починається з однією мережею з довільно вибраними ваговими коефіцієнтами. Сукупність мереж розвивається відповідно з трьома сценаріями:

1. A і B мають різні виходи, $O^A \neq O^B$, і не змінюють свої показники, тоді всі мережі атакуючої сторони залишаються без змін.

2. A і B мають рівні виходи, $O^A = O^B$, а загальне число атакуючих мереж менше, ніж деяка межа M. У цьому випадку існує 4 можливих комбінації значень прихованих нейронів, узгоджених з кінцевим виходом.

3. A і B мають рівні виходи $O^A = O^B$, але загальне число емульованих мереж більше M. Атакуюча сторона обчислює виходи всіх мереж, прибирає неуспішні мережі, чий вихід відмінний від O^A, а також оновлює вагові коефіцієнти в успішних мережах шляхом використання стандартного правила навчання.

Відразу після цього A і B синхронізуються, а атакуюча сторона використовує цей факт для перевірки того, яка з мереж має такі ж вагові коефіцієнти.

Дана атака була успішно застосована до різних варіантів схеми ККК, використовуючи різні параметри в якості різноманітних правил для відновлення вагових коефіцієнтів і обчислення виходу. Атака є особливо ефективною для випадків, в яких вона має невелику локальну лінійну швидкість [9, 10].

Геометрична стратегія атаки.

Геометрична атака базується на тому, що зловмисник будує одну нейронну мережу E з такою ж структурою, що у абонентів A і B, та ініціалізує випадковим чином її вагові коефіцієнти. На кожному етапі вона об'єднує E з тим же входом, що і обидві сторони, а також відновлює вагові коефіцієнти відповідно до таких правил:

1. A і B мають різні виходи, $O^A \neq O^B$, тоді атакуюча сторона не оновлює свою мережу E.

2. A і B мають рівні виходи, $O^A = O^B$, і $O^E = O^B$, тоді атакуюча сторона оновлює мережу E, використовуючи звичайне правило навчання.

3. A і B мають рівні виходи, $O^A = O^B$, і $O^E \neq O^B$, тоді атакуюча сторона знаходить таке значення $i \in \{1,\ldots,K\}$, що мінімізує значення $\sum_{j=0}^{N} w_{ij}^E \cdot x_{ij}$. Атакуюча сторона

інвертує прихований нейрон O_i^E і оновлює мережу E, приймаючи нові приховані біти та вихід O^A.

Мережа зловмисника навчається набагато повільніше, ніж сторони A і B синхронізуються. Тому зловмисник може визначити ключ з дуже малою ймовірністю. Різні зловмисники починають з довільно вибраних станів та поводять себе незалежно, таким чином, велика сукупність атакуючих сторін має велику ймовірність успіху. Дана атака була випробувана зі 100 довільними початковими станами та було встановлено, що хоча б один з них був синхронізований з мережею A, швидше ніж мережа B з ймовірністю 90 %.

Ймовірнісна стратегія атаки.

Навчання нейронної мережі можна розглядати як випадкове блукання в обмеженому багатовимірному просторі. Передбачити позицію точки після декількох кроків такого блукання, як правило, простіше ніж вгадати її початкове положення. Найпростіший варіант зробити це — представити кожну координату окремо, а також задати функцію розподілу на відрізку $\{-L,...,L\}$, яка буде оновлюватися на кожному кроці. Перешкодою цьому методу є той факт, що зловмисник не знає, до яких саме прихованих нейронів мереж абонентів застосовувалося правило навчання. Але це можна обійти, використовуючи методи динамічного програмування та відповідні умовні ймовірності.

Треба відзначити, що наведені сценарії атак гарантовано діють для невеликих нейронних мереж, але на практиці рідко коли використовуються мережі із значеннями параметрів $N<100$, $K<100$ та $L<10$.

4. Емпіричне дослідження функції розподілу часу синхронізації нейронних мереж

Останній крок протоколу ККК викликає багато питань, оскільки чітко не визначено, як абоненти можуть дізнатися, що їх нейронні мережі було вже синхронізовано, а більша кількість ітерацій не порушить синхронізації, але надасть зловмиснику набагато більше інформації. Проаналізуємо емпірично необхідну кількість ітерацій (часу) для синхронізації мереж абонентів протоколу ККК. Зробимо декілька дослідів, зафіксувавши значення $N=16$ і K, та спробуємо дослідити залежність функції розподілу часу синхронізації, змінюючи лише значення L з набору {1, 2, 3, 4, 5, 10, 20, 25}, виконуючи синхронізацію згідно протоколу ККК. Для одного фіксованого значення L будемо повторювати цей тест 1000 разів, щоб визначити, максимальну необхідну кількість ітерацій та середнє значення. Потім зафіксуємо пари значень L, N та L, K і проведемо аналогічний дослід. Отримані результати наведено в табл. 1–5.

Наведені результати показують, що залежність часу від параметра L має чітко виражений квадратичний характер, тобто залежить від L^2. Більш того різниця між максимальним та середнім значенням в проведеному тесті зберігається і є досить суттєвою.

Отже, це показує, що визначення моменту синхронізації або його обмеження є досить вузьким місцем протоколу ККК і вимагає чіткої специфікації. З одного боку, для криптографічного протоколу обміну ключем досить незвичним є факт невдалого застосування, коли в результаті сторони мають різні значення, якщо встановити межу кількості ітерацій на недостатньо великому рівні. З іншого боку, якщо гарантувати вдале застосування протоколу, тобто встановити межу гарантовано більшу ніж можлива максимальна кількість для синхронізації, це дасть змогу зловмиснику отримати більше інформації для проведення атаки, використовуючи одну із відомих стратегій атак.

Таблиця 1

Кількість ітерацій для синхронізації TPM з параметрами $N = 16$ та $K = 2$

K	N	L	max	average
2	16	1	32	17
2	16	2	512	74
2	16	3	2592	201
2	16	4	8192	359
2	16	5	20000	551
2	16	10	320000	2536
2	16	15	1620000	5006
2	16	20	5120000	32639
2	16	25	12500000	69819

Таблиця 2

Кількість ітерацій для синхронізації TPM з параметрами $N = 16$ та $K = 3$

K	N	L	max	average
3	16	1	48	10
3	16	2	768	167
3	16	3	3888	173
3	16	4	12288	280
3	16	5	30000	628
3	16	10	480000	2459
3	16	15	2430000	9854
3	16	20	7680000	16735
3	16	25	18750000	22094

Таблиця 3

Кількість ітерацій для синхронізації TPM з параметрами $N = 16$ та $K = 5$

K	N	L	max	average
5	16	1	80	35
5	16	2	1280	258
5	16	3	6480	524
5	16	5	50000	1272
5	16	10	800000	56095
5	16	15	4050000	778481
5	16	20	12800000	5579338
5	16	25	31250000	9120973

Таблиця 4

Кількість ітерацій для синхронізації для TPM з параметрами $N = 16$ та $L = 3$

K	N	L	average	max
3	16	3	623	3888
4	16	3	133	5184
5	16	3	673	6480
10	16	3	1014	12960
15	16	3	2583	19440
20	16	3	1827	25920
25	16	3	2424	32400
30	16	3	3595	38880
40	16	3	7942	51840
50	16	3	5483	64800
60	16	3	6096	77760

Таблиця 5

Кількість ітерацій для синхронізації для TPM з параметрами $K = 3$ та $L = 3$

K	N	L	average	max
3	5	3	174	1215
3	10	3	194	2430
3	20	3	379	4860
3	30	3	227	7290
3	40	3	293	9720
3	50	3	433	12150
3	60	3	302	14580
3	70	3	240	17010
3	80	3	215	19440
3	90	3	179	21870
3	100	3	252	24300

Також було емпірично перевірено розподіл можливих значень ключа після проведення протоколу ККК. Авжеж, це значення залежить від вибраних абонентами вагових коефіцієнтів та вхідних векторів, але попередній аналіз показав, що за правил навчання Хебба та анти-Хебба, отримане значення має далеко не рівномірний розподіл, а результуючі значення вагових коефіцієнтів з набагато більшою ймовірністю будуть близькі до $\pm L$.

Отже, даний напрямок хоча і є досить перспективним з точки зору нових ідей та швидкості реалізації, але вимагає досконального аналізу та специфікації, щоб можна було говорити про конкретні оцінки стійкості.

5. Висновки

В даній роботі було розглянуто протокол обміну ключами ККК з використанням властивості взаємного навчання нейронних мереж, зокрема, деревовидних машин парності. Описано існуючі стратегії та варіанти атак на цей протокол.

Було проведено емпіричне дослідження необхідної кількості ітерацій протоколу (часу) для синхронізації TPM мереж різних K-N-L типів. Отримано оцінки максимального та середнього значення часу синхронізації нейронних мереж з вибраними параметрами. Не зважаючи на те, що дослідження було емпіричним, що моделювало роботу протоколу із мережами з випадково вибраними ваговими коефіцієнтами, і значення параметрів K, N та L було досить обмеженим, проведені дослідження впевнено показали квадратичну залежність часу синхронізації мереж від параметра L, а також продемонстрували суттєву різницю між максимальним часом синхронізації мереж та середнім значенням для фіксованих значень параметрів K, N та L. Ця знайдена особливість функції розподілу часу синхронізації TPM мереж може бути використана зловмисником для проведення атаки на ключ, використовуючи одну із відомих стратегій атак, що вказує на вразливість протоколу ККК обміну ключами.

Також було зроблено емпіричний аналіз функції розподілу часу синхронізації мереж в протоколі ККК за умов різних правил навчання, що показало далеко не рівномірний розподіл вихідного значення ключа, що також не є хорошою ознакою з точки зору захищеності протоколу. Але для побудови конкретної атаки необхідним є більш детальне вивчення особливостей функції розподілу часу синхронізації TPM мереж.

Література

1. Kanter, I. The theory of neural networks and cryptography [Text] / I. Kanter, W. Kinzel // The Physics of Communication — Proceedings of the XXII Solvay Conference on Physics. — 2003. — P. 631–644. doi:10.1142/9789812704634_0044.
2. Volkmer, M. Tree Parity Machine Rekeying Architectures [Text] / M. Volkmer, S. Wallner // IEEE Transactions on Computers. — 2005. — Vol. 54(4). — P. 421–427. doi:10.1109/TC.2005.70.
3. Mislovaty, R. Security of Neural Cryptography [Text] / R. Mislovaty, E. Klein, I. Kanter, W. Kinzel // Proceedings of the 2004 11th IEEE International Conference on Electronics, Circuits and Systems (ICECS). — 2004. — P. 219–221. doi:10.1109/ICECS.2004.1399654.
4. Kanter, I. Secure exchange of information by synchronization of neural networks [Text] / I. Kanter, W. Kinzel, E. Kanter // Europhysics Letters. — 2002. — Vol. 57(1). — P. 141–147. doi:10.1209/epl/i2002-00552-9.
5. Dolecki, M. Distribution of the Tree Parity Machine Synchronization Time [Text] / M. Dolecki, R. Kozera // Advances in Science and Technology Research Journal. — 2013. — Vol. 7(18). — P. 20–27. doi:10.5604/20804075.1049490.
6. Rosen-Zvi, M. Mutual learning in a tree parity machine and its application to cryptography [Text] / M. Rosen-Zvi, E. Klein, W. Kinzel, I. Kanter // Physical Review E. — 2002. — Vol. 66(6). — 066135. doi:10.1103/PhysRevE.66.066135.
7. Klimov, A. Analysis of neural cryptography [Text] / A. Klimov, A. Mityagin, A. Shamir // Advances in Cryptology — Proceedings of ASIACRYPT 2002. — Springer Science + Business Media, 2002. — P. 288–298. doi:10.1007/3-540-36178-2_18.
8. Klein, E. Synchronization of neural networks by mutual learning and its application to cryptography [Text] / E. Klein, R. Mislovaty, I. Kanter, A. Ruttor, W. Kinzel // Advances in Neural Information Processing Systems. — 2005. — Vol. 17. — P. 689–696.
9. Shacham, L. N. Cooperating Attackers in Neural Cyptography [Text] / L. N. Shacham, E. Klein, R. Mislovaty, I. Kanter, W. Kinzel // Physical Review E. — 2004. — Vol. 69. — 066137. doi:10.1103/PhysRevE.69.066137.
10. Ruttor, A. Genetic Attack on Neural Cryptography [Text] / A. Ruttor, W. Kinzel, R. Naeh, I. Kanter // Physical Review E. — 2006. — Vol. 73. — 036121. doi:10.1103/PhysRevE.73.036121.

ЭМПИРИЧЕСКОЕ ИССЛЕДОВАНИЕ ФУНКЦИИ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ СИНХРОНИЗАЦИИ НЕЙРОННЫХ СЕТЕЙ В ПРОТОКОЛЕ ОБМЕНА КЛЮЧАМИ

Представлен анализ особенностей работы протокола обмена ключами с использованием взаимного обучения нейронных сетей, рассмотрены существующие атаки на протокол. Эмпирически проанализировано распределение времени синхронизации нейронных сетей, что позволило выявить слабые места протокола и сделать вывод о его защищенности.

Ключевые слова: нейронные сети, взаимное обучение, протокол обмена ключами.

Малік Олена Романівна, *кафедра математичних методів захисту інформації, Національний технічний університет України «Київський політехнічний інститут», Україна,* ***e-mail: aqua_venera@bigmir.net****.*

Малик Елена Романовна, *кафедра математических методов защиты информации, Национальный технический университет Украины «Киевский политехнический институт», Украина.*

Malik Olena, *National Technical University of Ukraine «Kyiv Polytechnic Institute», Ukraine,* ***e-mail: aqua_venera@bigmir.net***

УДК 666.9.035

Флейшер Г. Ю.,
Токарчук В. В.,
Василькевич О. І.,
Свідерський В. А.

ВПЛИВ СПИРТІВ ЯК ДОБАВОК-ПРИСКОРЮВАЧІВ ТВЕРДНЕННЯ НА ВЛАСТИВОСТІ ЦЕМЕНТУ

Досліджено вплив спиртів з різною просторовою структурою та з різною кількістю гідроксильних груп на фізико-механічні властивості цементу, головним чином на міцність, в тому числі ранню (1 доба). Виявлено найбільш ефективні з точки зору прискорення набору міцності добавки спиртів. Досліджено вплив спиртів як компонентів комплексної добавки (у поєднанні із суперпластифікатором) на міцнісні характерики цементу.

Ключові слова: *гідратація, добавка-прискорювач, комплексна добавка, спирт, суперпластифікатор, міцність на стиск, строки тужавіння.*

1. Вступ

В будівельному виробництві досить часто виникає потреба в інтенсифікації процесів тверднення цементного тіста в бетонних і розчинових сумішах, які застосовуються при бетонуванні або виготовленні бетонних та залізобетонних конструкцій, з метою максимального підвищення міцності на стиск бетону чи розчинової суміші, компенсації зниження міцності при введенні підвищених кількостей пластифікуючих добавок і в кінцевому результаті — економії клінкерних цементів. З цією метою застосовуються добавки-прискорювачі тверднення [1].

Добавки-прискорювачі викликають сьогодні особливу зацікавленість з точки зору поєднання їх з високо ефективними пластифікуючими добавками. Адже, застосовувані суперпластифікатори (на основі лігносульфонатів та полікарбоксилатів) проявляють ефективність при досить високих концентраціях, за яких суттєво гальмується розвиток міності, особливо в ранні строки тверднення. Тому, вводячі до складу суперпластифікаторів різні добавки-прискорювачі, можна усунути негативний вплив пластифікуючих добавок на міцність.

2. Аналіз лутературних даних та постановка проблеми

Сучасна класифікація передбачає поділ добавок-прискорювачів на прискорювачі процесів тужавіння та прискорювачі процесів тверднення [2]. Окремо виділяють добавки, які збільшують міцність.

Згідно визначень, наведених в [3] добавки, що прискорюють тужавлення — це речовини, що скорочують час початку переходу суміші від в'язкотекучого до твердого стану, а прискорювачі тверднення — добавки, що прискорюють розвиток ранньої міцності, впливаючи або не впливаючи на строки тужавлення. Перші повинні забезпечувати початок тужавлення розчинової суміші 30 хв або більше при 20 °С, а при 5 °С — 60 % або менше від часу початку тужавлення контрольної суміші. Додатково прописані вимоги щодо набору міцності бетону з такими добавками [3].

Добавки, що прискорюють тверднення за 1 добу при 20 °С повинні забезпечувати міцність основного складу 120 % або вище від міцності контрольного складу. За 28 діб міцність основного складу повинна дорівнювати 90 % або вище міцності контрольного складу.

Вимоги до добавок, які збільшують міцність наступні: за 28 діб міцність основного складу повинна бути 120 % або вище міцності контрольного складу.

Роль прискорювачів полягає в активізації процесів гідратації цементу, яка сприяє прискореному утворенню гелю. В результаті енергійних реакцій обміну прискореними темпами виділяється в розчин вільне вапно і таким чином підвищується розчинність силікатних складових цементу, що призводить до утворення гелів гідроксидів металів та кальцію. Одночасно з цим прискорюється коагуляція утвореного колоїдного розчину, яка сприяє зближенню частинок цементу та частинок гідратних новоутворень [1].

Існує багато прискорювачів тужавіння і тверднення цементів та виробів на їх основі, а також декілька