УДК 004.056
DOI: 10.25140/2411-5363-2020-2(20)-210-217

Михайло Шелест, Юлія Ткач, Сергій Семендяй, Марина Синенко, Леся Черниш

ДОСЛІДЖЕННЯ СТІЙКОСТІ АЛГОРИТМУ АВТЕНТИФІКОВАНОГО ШИФРУВАННЯ НА БАЗІ SPONGE-ФУНКЦІЇ

Актуальність теми досліджень. *Автентифіковане шифрування призначено для забезпечення конфіденційності, контролю цілісності та достовірності даних. Альтернативним підходом до побудови спеціальних алгоритмів автентифікованого шифрування є використання конструкцій типу sponge. Конструкції sponge є відносно новими криптографічними примітивами. Дослідження та оцінювання нових рішень у сфері криптографії, зокрема алгоритмів автентифікованого шифрування на базі sponge-функцій, завжди є актуальними у зв'язку з можливим їх застосуванням для задач безпеки сучасного кіберпростору.*

Постановка проблеми. *Перед практичним впровадженні нового методу або засобу криптографічного захисту інформації необхідно проведення його ретельного дослідження, насамперед щодо його стійкості до атак та швидкодії.*

Аналіз останніх досліджень і публікацій. *Вивчення питань автентичного шифрування та sponge-функцій здебільшого вивчався закордонними вченими, зокрема, М. Беллар, Ч. Нампремпре, В. Глігор, П. Донеску, Г. Бертоні, Дж. Даємен, М. Пітерс, Ван Ашче Г., М. Боровський, С. Агієвич, В. Марчук, А. Маслов, В. Семенов. Досліджень вітчизняних учених з цих питань немає.*

Виділення недосліджених частин загальної проблеми. *Нині в роботах вітчизняних та закордонних науковців ще не досліджувалось питання стійкості до атак алгоритму автентифікованого шифрування, на базі sponge-функції Bash-f.*

Постановка завдання. *Дослідити стійкість запропонованого алгоритму автентифікованого шифрування, а саме, отримати оцінки стійкості криптоалгоритму до атак, спрямованих на розшифрування шифртексту (відновлення ключа шифрування), та атак, спрямованих на порушення цілісності (підробки імітовставки).*

Виклад основного матеріалу. *Використання ітераційних конструкцій типу sponge є альтернативним підходом у побудові алгоритмів автентифікованого шифрування. Основними параметрами, за якими оцінюють алгоритм шифрування, зазвичай, є його стійкість до атак, спрямованих на розшифрування шифртексту (відновлення ключа шифрування), та швидкодія процесу шифрування. У випадку з алгоритмом автентифікованого шифрування, додається ще оцінювання його стійкості щодо атак, спрямованих на порушення цілісності (підробки імітовставки). Здебільшого оцінюють стійкість алгоритму як до відомих атак загального призначення, наприклад, tradeoff-атаки, так і до базових атак, що розробляються спеціально під алгоритм.*

Вивчена стійкість алгоритму щодо різних видів tradeoff-атак. Незважаючи на те, що обчислювальна складність tradeoff-атак менше, ніж атаки «брутальної сили», необхідні об'єми пам'яті та кількість префіксів для проведення успішної атаки є достатньо великими. Тому його застосування на практиці є малоймовірним.

Стійкість алгоритму була розглянута відповідно до наступних базових атак: пошук шляхів; знаходження циклів; відновлення стану; внутрішня колізія. Ймовірність успіху базових атак задають оцінки зверху на стійкість sponge-функції, мінімальне число звернень до F для успішної атаки становить $O(2^{c+2})$.

Для режимів алгоритму, що залежить від ключа, розглядаються атаки 'прогнозування гами' та 'підробка імітовставки'. Очікуване число звернень до F склала $O(2^{c/2})$, а при $l \leq c$ атаки взагалі не несуть загрози.

Висновки відповідно до статті. *Отримані результати щодо стійкості алгоритму автентифікованого шифрування як до універсальної tradeoff-атаки, так й до базових атак для конструкцій sponge підтверджують, що він є стійким. Враховуючи отримані раніше оцінки швидкодії реалізації цього алгоритму, можна стверджувати, що даний клас алгоритмів базі sponge-функції Bash-f може бути перспективним для використання при створені захищеного кіберпростору.*

Ключові слова: *автентифікаційне шифрування; sponge-функція; оцінка стійкості криптоалгоритму; tradeoff-атака; базові атаки на конструкції sponge.*

Табл.: 2. Бібл.: 10.

Актуальність теми дослідження. Автентифіковане шифрування (це коли проводиться одночасне виконання функцій шифрування та імітозахисту) призначено для забезпечення конфіденційності, контролю цілісності та достовірності даних [1-2]. Сторони, які мають загальні ключі, можуть організувати не тільки шифрований обмін повідомленнями, але і здійснювати контроль цілісності шляхом додавання імітовставок до повідомлення, що дозволяє переконуватися в прийомі достовірного повідомлення. Автентифіковане шифрування забезпечує певну функціональну гнучкість: ключі можуть оновлюватися в процесі обробки даних; є можливість шифрувати тільки окремі частини повідомлення або чередувати шифровані та відкриті повідомлення; імітовставки можуть бути відсутні або, навпаки, траплятися кілька разів. Переважно алгоритми автентифікованого шифрування будують на базі блочних криптосистем: деякі з них симулюють класичний підхід, виключаючи використання двох ключів, інші – є оригінальними конструкціями.

Альтернативним підходом до побудови алгоритмів автентифікованого шифрування є використання конструкцій типу *sponge* [3-4]. Конструкції *sponge* є відносно новими криптографічними примітивами, які можуть бути використані для побудови різноманітних криптографічних алгоритмів. *Sponge*-функції належать до *LRX*-класу криптографічних перетворень і можуть ефективно за швидкістю реалізуватися на програмованих логічних інтегральних схемах, тому що в них задіяні тільки логічні операції (*L*), циклічні зрушення (*R*) та XOR (*X*), що є цікавим при сучасних швидкостях телекомунікацій.

У роботі [5] білоруськими вченими запропоновано цікаву *sponge*-функцію *Bash-f*. Дослідження та оцінювання нових рішень у сфері криптографії, зокрема алгоритмів автентифікованого шифрування на базі *sponge*-функцій, завжди є актуальними у зв'язку з можливим їх застосуванням для задач безпеки сучасного кіберпростору.

Постановка проблеми. Методи та засоби криптографічного захисту інформації посідають важливе місце в системі забезпечення безпеки кіберпростору. До сучасних засобів криптозахисту висувають певні вимоги, передусім обґрунтовану стійкість та швидкодію, яка відповідає сучасним вимогам. Усі нові рішення у сфері криптографії, що пропонуються для практичного використання, повинні пройти відповідні дослідження.

Аналіз останніх досліджень та публікацій. Значний внесок із розробки теорії автентичного шифрування внесли іноземні вчені М. Беллар, Ч. Нампремпре, В. Глігор, П. Доненску. Питаннями щодо *sponge*-функцій щільно займаються закордонні вчені Г. Бертоні, Дж. Даємен, М. Пітерс, Ван Ашче Г., М. Боровський, С. Агієвич, В. Марчук, А. Маслов, В. Семенов. Досліджень вітчизняних учених із даних питань немає. У роботах Дж. Хонга, П. Саркара, О. Дункелмана, Н. Келлера, А. Бірюкова, А. Шаміра, С. Баббеджа досить повно відображено інформацію щодо універсальних атак на криптоалгоритми.

Виділення недосліджених частин загальної проблеми. На даний час у роботах вітчизняних та зарубіжних вчених не досліджувалось питання стійкості до стандартних атак алгоритму автентифікованого шифрування, на базі *sponge*-функції *Bash-f*.

Мета статті. Метою статті є дослідження стійкості алгоритму автентифікованого шифрування з використанням *sponge*-функції *Bash-f*, а саме, отримання оцінки стійкості криптоалгоритму до атак, спрямованих на розшифрування шифртексту (відновлення ключа шифрування), та атак, спрямованих на порушення цілісності (підробки імітовставки).

Виклад основного матеріалу. Використання ітераційних конструкцій типу sponge є альтернативним підходом у побудові алгоритмів автентифікованого шифрування. В їх основі лежить sponge-функція, яка визначає складне бієктивне перетворення над внутрішнім станом $S\in\{0,1\}^b$ конструкції. У стані S виділяють дві частини $S_r\in\{0,1\}^r$ та $S_c\in\{0,1\}^c$, такі що b=r+c та $S=S_r||S_c$. Підстан S_r може видаватися назовні як частина виходу конструкції, а підстан S_c тримається в секреті і назовні не видається. Різні значення r та c визначають компроміс між швидкістю обробки даних і стійкістю sponge-конструкції: збільшення r з одночасним зменшенням *c* призводить до збільшення швидкості та зниження стійкості.

У роботі [3] для sponge-алгоритмів в припущенні, що ключ K зберігається в таємниці та обирається випадково та ймовірно з множини $\{0,1\}^{|K|}$, визначені такі вимоги безпеки (де A – відкриті дані/заголовок, C – шифртекст, M – відкритий текст, T – імітовставка):

1. *Неможливість відновлення ключа*. Ймовірність находження нападником ключа в будь-якій атаці, в якій він може перевірити *n* ключів, не перевищує $n\cdot 2^{|K|}$.

2. *Неможливість підробки імітовставки*. За умови неможливості відновлення ключа ймовірність успішного визначення нападником імітовставки для будь-якої пари (*A*,*M*) дорівнює $2^{-|T|}$, навіть коли нападнику відомий шифртекст *C*, який відповідає (*A*,*M*), та виходи (C_i, T_i) для адаптивно обираємих їм входів (A_i, M_i), де $(A_i, M_i)\neq(A, M)$.

3. *Неможливість відновлення відкритого тексту*. Для нападника найбільш ефективним методом отримати будь-якої інформації про M (за винятком інформації щодо довжини) по виходу (C, T), відповідному входу (A,M), де A обирається нападником, а M – невідомо, є відновлення ключа, навіть якщо нападнику відомі виходи (C_i, T_i) для адаптивно обираємих їм входів (A_i, M_i), де $A_i \neq A$.

Відзначимо, що вимоги щодо неможливості відновлення відкритого тексту базується на тому, що для фіксованого ключа не повинно бути двох входів (A',M') та (A'',M''), де $A'=A''$ та $M' \neq M''$. Унікальність відкритих даних для того ж самого ключа є критичним з погляду криптографічної стійкості.

Оцінку стійкості будемо проводити в припущені, що базове перетворення $\boldsymbol{F}$ *sponge*-функції *Bash-f* не відрізняється від випадкового.

Основними параметрами, за якими оцінюють алгоритм шифрування, зазвичай, є його стійкість до атак, направлених на розшифрування шифртексту (відновлення ключа шифрування), та швидкодія процесу шифрування. У випадку з алгоритмом автентифікованого шифрування додається ще оцінювання його стійкості щодо атак, направлений на порушення цілісності (підробки імітовставки).

Здебільшого оцінюють стійкість алгоритму як до відомих атак загального призначення (наприклад, повний перебір ключового простору або *tradeoff*-атаки [6-8]), так і до базових атак, що розробляються спеціально під алгоритм.

Умови атаки щодо розшифрування (відновлення ключу шифрування) полягають у тому, що нападник повинен відрізнити випадкову вхідну послідовність від зашифрованого на секретному ключі тексту, при цьому нападник може звертатись як до оракулу розшифрування (на вхід оракула заборонено подавати вхідну послідовність, яку потрібно відрізнити), так і до *sponge*-функції.

Умови атаки щодо порушення цілісності (підробки імітовставки) складаються у тому, що нападник повинен підробити імітовставку заданого вхідного повідомленню, при цьому він може звертатися до оракулу виробки імітовставки (потрібно подавати на вхід вихідне повідомлення) або до *sponge*-функції.

Для оцінювання стійкості автентифікованого шифрування треба довести, що нападник не має суттєвих переваг в умовах проведення певної атаки.

У випадку, коли автентифіковане шифрування використовується для зашифрування відомого відкритого тексту, то воно може розглядатися як поточний алгоритм, який формує гаму по блоках.

Tradeoff-атака відноситься до ефективних універсальних атак на алгоритми поточного шифрування [9]. Ця атака використовується для обернення односторонньої функції, тобто для визначання невідомого прообразу по відомому образу. Такі односторонні функції відображають внутрішній стан чи ключ та сінхропосилку алгоритму у вихідну послідовність, яка називається префіксом [6]. Довжина потрібного префіксу залежить від класу атаки. Якщо атака направлена на відновлення внутрішнього стану, то довжина префіксу повинна дорівнювати сумі довжин ключа та сінхропосилки. Префікси, що використовуються в атаці, можуть відповідати тому самому ключу чи різним ключам.

Атака складається з двох етапів [7]:

1) етап попередніх обчислень, на якому у відповідності до алгоритму створюються певні таблиці;

2) етап реального часу (етап пошуку рішення), на якому відстежуються вихідні префікси та відновлює внутрішній стан чи ключ по таблицях, що створені на першому етапі.

Tradeoff-атака характеризується наступними параметрами [8]:

– N – потужність множини внутрішніх станів та ключів (потужність простору пошуку);

– P – обчислювальна складність етапу попередніх обчислень;

– M – розмір пам’яті, необхідний для зберігання попередньо обчислених таблиць;

– T – обчислювальна складність етапу реального часу;

– D – кількість префіксів, необхідних для проведення атаки;

– π – імовірність успіху атаки.

Для того, щоб атака була успішною, параметри повинні відповідати визначеному рівнянню компромісу, яке залежить від класу атаки. Зазвичай розглядають рішення для рівняння компромісу з ймовірністю успіху атаки $\pi = 0{,}63$.

Проведемо аналіз стійкості алгоритму автентифікованого шифрування до найбільш ефективних *tradeoff*-атак.

Метою атаки є визначення таємного ключа $K \in \{0,1\}^l$, де $l \in \{128,256\}$ – рівень стійкості. Будем рахувати, що проводиться атака на алгоритм шифрування при відомому відкритому тексті (тобто при відомій гамі). У такому випадку нападнику буде невідома тільки частина $S[1571\text{-}2l\ldots) \in \{0,1\}^{2l-8}$ внутрішнього стану $S \in \{0,1\}^{1563}$. У випадку успішного відновлені значення внутрішнього стану S у деякий момент часу t, легко можна отримати значення внутрішнього стану, який мав місце одразу ж після загрузки ключа та сінхропосилки, а також безпосередньо сам ключ.

У роботі [9] розглянуто *BG*-атаку, основану на парадоксі днів народження та направлену на відновлення початкового стану. Рівняння компромісу *BG*-атаки має вид: $TM=N$, де $M=D$, $P=M=N/D$, N – потужність множини станів. Одним з можливих рішень рівняння є $T=M=D=P=N^{1/2}$.

У роботі [10] запропонована модифікація класичної *tradeoff*-атаки (позначимо її як *BS*-атака). Дана атака направлена на відновлення початкового стану алгоритму. Рівняння компромісу *BS*-атаки має вид: $T \cdot M^2 \cdot D^2 = N^2$, де $P=N/D$, $1 \le D^2 \le T$, N – потужність множини ключів. Одним з можливих рішень для даного рівняння є

$$T=M=N^{1/2},\ D=N^{1/4},\ P=N^{3/4}.$$

Атаки *BG* та *BS* направлені на відновлення внутрішнього стану. У випадку, коли сума довжин ключа та сінхропосилки менше ніж розмір внутрішнього стану, застосовуються більш ефективні модифікації таких атак. Наприклад, у роботі [6] запропоновано модифікації атак *BG* та *BS*, що направлені на відновлення ключа по префіксам, отриманих на одному ключі, но на різних сінхропосилках (дані атаки позначимо через *HBG* и *HBS*, відповідно). При довжини ключа k, довжині сінхропосилки v та потужності множини ключів N рішеннями для даних модифікацій є:

– $(P, D, M, T) = (N^{1/2}, N^{1/2}, N^{1/2}, N^{1/2})$, де $P = 2^{(k+v)/2} < 2^k$ для $k > v$;

– $(P, D, M, T) = (N^{2/3}, N^{1/3}, N^{1/3}, N^{2/3})$, де $P = 2^{(k+v)/3} < 2^k$ для $k > 2v$;

– $(P, D, M, T) = (N^{3/4}, N^{1/4}, N^{1/2}, N^{1/2})$, де $P = 2^{(k+v)/4} < 2^k$ для $k > 3v$.

Перші два рішення відповідають *HBG*-атаці, а третє – *BS*-атаці.

У роботі [7] описана модифікація *BS*-атаки (назвемо її *DK*-атака), яка спрямована на відновлення ключа по префіксах, отриманих на різних ключах та однаковій сінхропосилці. Рівняння компромісу для такого виду атаки є

$$T \cdot M^2 \cdot D^2 = N^2,$$

де $1 \le D^2 \le T$, $P=N/D$, N - потужність множини ключів. Одними з можливих рішень для цього рівняння є:

– $(P, D, M, T) = (N^{2/3}, N^{1/3}, N^{1/3}, N^{2/3})$;

– $(P, D, M, T) = (N^{3/4}, N^{1/4}, N^{1/2}, N^{1/2})$.

У табл. 1-2 наведено характеристики деяких *tradeoff*-атак відносно досліджуваного алгоритму для рівня стійкості $l = 128$ та $l = 256$. Для *HBG*-атаки довжина сінхропосилки $v = l/2$.

Таблиця 1

Характеристики tradeoff-атак для рівня стійкості l=128.

Атака	*N*	*T*	*M*	*D*	*P*
BG	2^{248}	2^{124}	2^{124}	2^{124}	2^{124}
BS	2^{248}	2^{124}	2^{124}	2^{62}	2^{186}
HBG	2^{192}	2^{96}	2^{96}	2^{96}	2^{96}
DK	$\mathbf{2^{128}}$	$\mathbf{2^{85.3}}$	$\mathbf{2^{42.7}}$	$\mathbf{2^{42.7}}$	$\mathbf{2^{85.3}}$

Таблиця 2

Характеристики tradeoff-атак для рівня стійкості l=256.

Атака	*N*	*T*	*M*	*D*	*P*
BG	2^{504}	2^{252}	2^{252}	2^{252}	2^{252}
BS	2^{504}	2^{252}	2^{252}	2^{126}	2^{378}
HBG	2^{384}	2^{192}	2^{192}	2^{192}	2^{192}
DK	$\mathbf{2^{256}}$	$\mathbf{2^{170.7}}$	$\mathbf{2^{85.3}}$	$\mathbf{2^{85.3}}$	$\mathbf{2^{170.7}}$

З наведених даних видно, що найкращі характеристики має *DK*-атака. Незважаючи на те, що обчислювальна складність *DK*-атаки менше, ніж атаки «брутальної сили», необхідні об'єми пам'яті та кількість префіксів для проведення успішної атаки є достатньо великими. Тому його застосування на практиці є малоймовірним.

Тепер розглянемо стійкість алгоритму по відношенню до базових атак.

У роботі [3] досліджено стійкість *sponge*-функції щодо базових атак, в яких апріорі немає ніяких припущень щодо можливих атаках на функцію $\boldsymbol{F}$.

У досліджені передбачалось, що нападник може виконати не більше, ніж β звернень до $\boldsymbol{F}$ (у т.ч. до $\boldsymbol{F}^{-1}$, якщо $\boldsymbol{F}$ є бієкцією). Стійкість алгоритму була розглянута відповідно до таких базових атак:

− *Пошук шляхів*. Необхідно знайти такий рядок, який після фази 'вбирання' алгоритму отримує заданий внутрішній стан. Ймовірність успіху атаки становила $\beta^2/2^{c+2}$, якщо $\boldsymbol{F}$ – бієкція.

− *Знаходження циклів*. Проводиться пошук циклів у вихідних послідовностях при коректних вхідних даних. Ймовірність успіху атаки складала $\beta^2/2^{c+r+1}$, якщо $\boldsymbol{F}$ – не бієкція.

− *Відновлення стану*. Для заданого рядка Z проводиться відновлення відповідного стану S. Ймовірність успішної атаки склала $\beta/2^c$.

− *Зв'язування виходу.* Для заданого рядка Z проводиться пошук такого стану S, який видає відповідний вихід. При цьому не гарантується, що такий стан існує. Ймовірність успішної атаки склала $\beta/2^{|Z|-r}$.

− *Внутрішня колізія.* Проводиться пошук таких двох рядків, що в результаті завершення етапу «вбирання» отримується однаковий внутрішній стан (зовнішні стани можуть відрізнятися). Ймовірність успіху атаки склала $\beta^2/2^{c+1}$.

Вразливість *sponge*-функції до таких атак обумовлена тим, що стан кінцевий, тому атаки не спроможні до випадкового оракулу. Ймовірність успіху базових атак задають оцінки зверху на стійкість *sponge*-функції. Мінімальне число β звернень до $\boldsymbol{F}$ для однієї успішної атаки становить $O(2^{c+2})$.

Для режимів, що залежить від ключа, розглядаються наступні атаки.

− *Прогнозування гами.* Після завершення успішної атаки по відновленню поточного стану по відомій частині вихідної гами прогнозується інша частина гами. Очікуване число звернень до $\boldsymbol{F}$ склала $2^{c/2}$, а при $l \leq c$ атака взагалі не несе загрози.

− *Підробка імітовставки*. Після успішного проведення атаки по відновленню поточного стану може бути проведена підробка імітовставки для нового повідомлення при спостереженні наборів пар «повідомлення+імітовставка» – «імітовставка». Очікуване число звернень до $\boldsymbol{F}$ становила $2^{r+c-n}/(m+1)$, де m – число спостережних повідомлень, а

n – довжина імітовставки. При $l \leq c - log_2(m)$ атака не становить загрози. При $m=2^{c/2}$ отримано оцінку $c \geq 2l$. Інший спосіб підробки імітовставки полягає в пошуку внутрішньої колізії ключової sponge-функції. Очікуване число спостережних блоків становить $2^{c/2}$. Після визначення внутрішньої колізії імітовставки можуть бути легко подроблені.

Висновки відповідно до статті. Отримані результати щодо стійкості досліджуваного алгоритму автентифікованого шифрування як до універсальної *tradeoff*-атаки, так й до базових атак для конструкцій *sponge* підтверджують, що він є стійким. Враховуючи отримані раніше оцінки швидкодії реалізації цього алгоритму [10], можна стверджувати, що цей клас алгоритмів базі *sponge*-функції $\boldsymbol{F}$ може бути перспективним для використання при створені захищеного кіберпростору.

Список використаних джерел

1. Bellare M., Namprempre Ch. Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm. *ASIACRYPT 2000, LNCS 1976*. 2000. P. 531–545.

2. Gligor V., Donescu P. Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes. *Matsui M. (Eds.) Fast Software Encryption. FSE 2001. LNCS 2355*. Springer, Berlin, Heidelberg, 2001. P. 92–108.

3. Bertoni G., Daemen J., Peeters M., Van Assche G. (2011). Cryptographic sponge functions. Retrieved from http://sponge.noekeon.org/CSF-0.1.pdf.

4. Borowski M. The sponge construction as a source of secure cryptographic primitives. *Military Communication Conference*, France, 2013.

5. Agievich S., Marchuk V., Maslau A., Semenov V (2016). Bash-f: another LRX sponge function. *Proceedings of the 5th Workshop on Current Trends in Cryptology*, Russia (pp. 184–205).

6. Hong J. Sarcar P. New Application of Time Memory Data Tradeoffs. *Advances in Cryptology, Asiacrypt 2005*, LNCS 3788. Springer-Verlag, 2005. P. 353–372.

7. Dunkelman O., Keller N. Treatment of the initial value in Time-Memory-Data Tradeoffs attacks on stream ciphers. *Information Processing Letters*. 2008. Vol. 107(5). P. 133-137.

8. Biryukov A., Shamir A. Cryptanalytic Time-Memory Data Tradeoffs for Stream Ciphers. *Advances in Cryptology, proceedings of ASIACRYPT 2000*, LNCS 1976. Springer-Verlag, 2000, P. 1–13.

9. Babbage S. Improved exhaustive search attacks on stream ciphers. *European Convention Security and Detection, IEE Conference publication* No. 408, IEE, 1995, P. 161–166.

10. Бакрі М., Гері Л. Ч. Віяй, Юрченко А. В., Ткач Ю. М., Шелест М. Є. Реалізація стандарту шифрування SES для забезпечення безпеки цифрової інфраструктури. *Безпека ресурсів інформаційних систем* : тези доп. учасників І Міжнар. наук.-практ. конф. (м. Чернігів 16-17 квітня 2020 р.). Чернігів : Вид-во ЧНТУ, 2020. С. 30–31.

References

1. Bellare, M., Namprempre, Ch. (2000). Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm. *ASIACRYPT 2000*, LNCS 1976, pp. 531–545 [in English].

2. Gligor, V., Donescu, P. (2001). Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes. In *Matsui M. (Eds.) Fast Software Encryption. FSE 2001. LNCS 2355*. (pp. 92–108). Springer, Berlin, Heidelberg [in English].

3. Bertoni, G., Daemen, J., Peeters, M., Van Assche G. (2011). Cryptographic sponge functions. Retrieved from http://sponge.noekeon.org/CSF-0.1.pdf [in English].

4. Borowski, M. (2013).The sponge construction as a source of secure cryptographic primitives. *Military Communication Conference*. France [in English].

5. Agievich, S., Marchuk, V., Maslau, A., Semenov, V. (2016). Bash-f: another LRX sponge function. *Proceedings of the 5th Workshop on Current Trends in Cryptology*, Russia (pp. 184–205) [in English].

6. Hong, J. Sarcar, P. (2005). New Application of Time Memory Data Tradeoffs. *Advances in Cryptology. Asiacrypt 2005, LNCS 3788* (pp. 353–372). Springer-Verlag [in English].

7. Dunkelman, O., Keller, N. (2008). Treatment of the initial value in Time-Memory-Data Tradeoffs attacks on stream ciphers. *Information Processing Letters*, 107(5), 133-137 [in English].

8. Biryukov A., Shamir A. Cryptanalytic Time-Memory Data Tradeoffs for Stream Ciphers. *Advances in Cryptology, proceedings of ASIACRYPT 2000, LNCS 1976* (pp. 1-13). Springer-Verlag, 2000 [in English].

9. Babbage, S. (1995). Improved exhaustive search attacks on stream ciphers. *European Convention Security and Detection, IEE Conference publication* No. 408, IEE, 161-166 [in English].

10. Bakri, M., Heri, L. Ch. Viiai, Yurchenko, A. V., Tkach, Yu. M., Shelest, M. Ie. (2020). Realizatsiia standartu shyfruvannia SES dlia zabezpechennia bezpeky tsyfrovoi infrastruktury [Realization of the SES encryption standard for secure digital security infrastructure]. *Bezpeka resursiv informatsiinykh system : I Mizhnar. nauk.-prakt. konf. – Security of information systems resources: I International. scientific-practical conf. (Chernihiv, April 16-17, 2020).* Chernihiv [in Ukraine].

UDC 004.056

Mikhailo Shelest, Yuliia Tkach, Sergiy Semendyay, Marina Sinenko, Lesya Chernish

STUDY OF THE STRENGTH OF AN AUTHENTIFIED ENCRYPTION ALGORITHM BASED ON SPONGE FUNCTION

Urgency of the research. *In recent years, the direction of "cryptography of substitutions" has been formed in theoretical cryptography, which studies fixed substitutions of large dimensions as crypto-primitives. So-called sponge functions can be used in the implementation of this class of primitives.*

Target setting. *One of the approaches to building authenticated encryption algorithms is to use sponge functions. In some countries (for example, in the Republic of Belarus and Malaysia) the development of national standards for cryptographic protection of information using authenticated encryption algorithms based on the sponge function Bash-f is being completed. In this regard, there is some interest in the study of this algorithm, especially to assess its resistance to attacks and evaluate its speed.*

Actual scientific researches and issues analysis. *In modern research, a significant place is occupied by the problems of cryptographic protection of information. In the works of scientists widely various issues regarding the protection of information, including cryptographic are described, but the question of the stability of the algorithm of authenticated encryption based on the sponge function remains unexplored.*

Uninvestigated parts of general matters defining. *At present, the work of domestic and foreign scientists has not studied the issue of resistance to standard attacks of the algorithm of authenticated encryption, based on the proposed by Belarusian scientists sponge-function Bash-f.*

The research objective. *Investigate the resistance to standard attacks of the authenticated encryption algorithm, based on the sponge function Bash-f proposed by Belarusian scientists.*

The statement of basic materials. *The use of iterative constructions such as sponge is an alternative approach in the construction of authenticated encryption algorithms. The main parameters by which the encryption algorithm is evaluated are usually its resistance to attacks aimed at decrypting the ciphertext (recovery of the encryption key), and the speed of the encryption process. In the case of the authenticated encryption algorithm, an assessment of its resistance to attacks is added, aimed at violating the integrity (forgery of imitations). As a rule, the stability of the algorithm is evaluated both to known general-purpose attacks, such as tradeoff-attacks, and to basic attacks developed specifically for the algorithm.*

The stability of the algorithm for different types of tradeoff-attacks is studied. Although the computational complexity of tradeoff attacks is less than brute force attacks, the amount of memory required and the number of prefixes for a successful attack is large enough. Therefore, its application in practice is unlikely.

The stability of the algorithm was considered in accordance with the following basic attacks: search for ways; finding cycles; recovery; internal collision. The probability of success of basic attacks is determined by estimates from above on the stability of the sponge function, the minimum number of calls to F for a successful attack is $O(2^{c+2})$.

For key-dependent algorithm modes, 'gamma prediction' and 'fake imitation' attacks are considered. The expected number of appeals to F was $O(2^{c/2})$*, and at* $l \leq c$ *attacks do not pose a threat at all.*

Conclusions. *The results obtained on the resilience of the investigated algorithm of authenticated encryption to both universal tradeoff-attack and basic attacks for sponge constructs confirm that it is stable. Given the previously obtained estimates of the speed of implementation of this algorithm, it can be argued that this class of algorithms based on the sponge function F may be promising for use in creating a secure cyberspace.*

Keywords: *authentication encryption; sponge-function; cryptographic algorithm stability assessment; tradeoff-attack; basic attacks on sponge constructs.*

Table: 2. References: 10.

Шелест Михайло Євгенович – доктор технічних наук, професор, професор кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Shelest Mykhailo– Doctor of Technical Science, Professor, Professor of Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: mishel3141@gmail.com
ORCID: https:// orcid.org/0000-0003-1090-0371
SCOPUS Author ID: 57211429755

Ткач Юлія Миколаївна – доктор педагогічних наук, доцент, завкафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Tkach Yuliia – Doctor of Pedagogical Science, Associate Professor, Head of Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology (95 Shevchenko str., 14035 Chernihiv, Ukraine).
E-mail: tkachym79@gmail.com

ORCID: https:// orcid.org/0000-0002-8565-0525
SCOPUS Author ID: 57193026076

Семендяй Сергій Матвійович – завідувач лабораторії кібербезпеки, аспирант, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Semendiai Serhii – Head of the cybersecurity laboratory, PhD Student, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: sovnarcom@ukr.net
ORCID: http://orcid.org/0000-0002-7751-5956

Синенко Марина Анатоліївна – кандидат фізико-математичних наук, доцент, доцент кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Synenko Maryna – PhD in Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Cybernetic Protection and Mathematical Modeling, Chernigiv National University of Technology (95 Shevchenko str., 14035 Chernigov, Ukraine).
E-mail: mara.a.snnk@gmail.com
ORCID: http://orcid.org/0000-0002-8961-533X
Scopus ID: 6504542623
ResearcherID: V- 1813-2017

Черниш Леся Григоріївна – кандидат технічних наук, доцент, доцент кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Chernysh Lesia – PhD in Technical science, Associate Professor, Associate Professor of Department of Cybersecurity and Mathematical Simulation, , Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: lg4@ukr.net
ORCID: http://orcid.org/0000-0001-7446-1684