INFORMATION SECURITY

DOI 10.20535/2411-1031.2023.11.2.293748
УДК 004.056

КАТЕРИНА ВОРОБЕЙ,
АНТОН ОЛЕКСІЙЧУК

ФІЛЬТРУВАЛЬНІ ГЕНЕРАТОРИ ГАМИ З ПІДВИЩЕНОЮ СТІЙКІСТЮ ВІДНОСНО АЛГЕБРАЇЧНИХ АТАК

Фільтрувальні генератори гами утворюють один з найвідоміших та найбільш досліджених класів генераторів псевдовипадкових послідовностей, що використовуються для побудови синхронних потокових шифрів. Кожен такий генератор складається з двійкового лінійного регістру зсуву з примітивним поліномом зворотного зв'язку та нелінійної булевої функції ускладнення, до якої висувається низка вимог, пов'язаних з умовою стійкості генератора відносно відомих атак.

Однією з таких вимог є висока алгебраїчна імунність функції ускладнення генератора, яка характеризує його стійкість до сучасних алгебраїчних атак. У певних випадках зазначена вимога є надто обмежувальною з погляду практичності, оскільки підвищує обчислювальну або схемну складність алгоритму генерації гами. Це обумовлює актуальність задачі підвищення стійкості фільтрувальних генераторів гами з фіксованими функціями ускладнення, які мають обмежену (невисоку) алгебраїчну імунність.

У статті пропонується спосіб розв'язання цієї задачі, сутність якого полягає в модифікації функції зворотного зв'язку лінійного регістру зсуву. Проведено дослідження стійкості запропонованих генераторів відносно алгебраїчних атак та показано, що (за певної природної умови) такі генератори є більш стійкими при однаковій довжині початкового стану в порівнянні з традиційними генераторами гами. Запропонований спосіб видається корисним для практичного застосування при побудові перспективних апаратно орієнтованих потокових шифрів.

Ключові слова: кібербезпека, криптографічний захист інформації, потоковий шифр, фільтрувальний генератор гами, алгебраїчна атака, обґрунтування стійкості.

Постановка проблеми. Розглянемо фільтрувальний генератор гами, побудований на основі двійкового лінійного регістру зсуву з примітивним поліномом зворотного зв'язку $f(x) = x^n \oplus c_{n-1}x^{n-1} \oplus \cdots \oplus c_0$ та булевої функції $F : V_n \overset{\text{def}}{=} \{0,1\}^n \to \{0,1\}$. Функціонування генератора відбувається за законом

$$F(uS^i) = \gamma_i,\ i = 1, 2, \ldots, \tag{1}$$

де $u = (u_0, \ldots, u_{n-1}) \in V_n$ – початковий стан генератора, $S = \begin{pmatrix} 0 \ldots 0\ c_0 \\ 1 \ldots\ 0\ c_1 \\ \ldots\ \ldots\ \ldots \\ 0 \ldots\ 1\ c_{n-1} \end{pmatrix}$ – супровідна матриця полінома $f(x)$, γ_i – знак вихідної послідовності генератора в i-му такті (див., наприклад, [1]).

Алгебраїчні атаки на фільтрувальний генератор мають на меті відновлення його початкового стану за відомою вихідною послідовністю шляхом розв'язання системи

рівнянь (1). Загальна схема побудови таких атак полягає у знаходженні систем, що складаються з рівнянь якомога меншого степеня, які є наслідками системи (1), та у розв'язанні отриманих систем-наслідків за допомогою відомих методів [1]-[7]. Часова складність зазначених атак становить порядку $(N_{n,d})^3$ двійкових операцій, де $N_{n,d} = \sum_{i=1}^{d} \binom{n}{i}$, а d є алгебраїчною імунністю функції F, тобто найменшим степенем ненульових рівнянь вигляду $g(x) = 0$, де $g : V_n \to \{0,1\}$, які є наслідками хоча б одного рівняння $F(x) = 0$, $F(x) = 1$ [1], [2], [4].

Для забезпечення належної стійкості фільтрувальних генераторів гами необхідно використовувати функції ускладнення, що мають високу алгебраїчну імунність, а також володіють іншими властивостями, які відповідають за стійкість генераторів відносно інших відомих атак. На сьогодні запропоновано чимало конструкцій таких функцій (див. роботу [8] та наведені у ній посилання), проте усі вони виявляють достатньо громіздкими з погляду практичної реалізації. Це обумовлює актуальність задачі побудови фільтрувальних генераторів гами з підвищеною стійкістю за умови фіксації довжині початкового стану та функції ускладнення генератора, яка має обмежену алгебраїчну імунність.

Аналіз останніх досліджень і публікацій. Першу (опубліковану у відкритих джерелах) алгебраїчну атаку на фільтрувальні генератори гами запропоновано в [2] та розвинуто й узагальнено в [4, 7, 9] та інших публікаціях.

Припустимо, що виконується одна з таких умов:

1) існує ненульова функція $g : V_n \to \{0,1\}$ така, що $gF = 0$ і $\deg g < \deg F$;

2) існує ненульова функція $h : V_n \to \{0,1\}$ така, що $h(F \oplus 1) = 0$ і $\deg h < \deg F$.

Тоді у випадку $\gamma_i = 1$ за умови 1) маємо $0 = g(uS^i)F(uS^i) = g(uS^i)$, а у випадку $\gamma_i = 0$ за умови 2) маємо $0 = h(uS^i)F(uS^i) = h(uS^i)$. Отже, за системою рівнянь (1) можна побудувати нову систему, яка складається з рівнянь меншого степеня, що й складає сутність атаки, наведеної в [2].

Для розв'язання отриманої системи рівнянь можна використовувати метод введення нових змінних [1], алгоритми обчислення базисів Грьобнера ідеалів кільця булевих функцій [5], [10], [11] або інші методи. Часова складність зазначених (відомих на сьогодні) методів визначається максимальним степенем нелінійності d рівнянь у системі та становить порядку $(N_{n,d})^3$ двійкових операцій. Таким чином, стійкість фільтрувального генератора гами відносно алгебраїчних атак визначається алгебраїчною імунністю функції F, яка дорівнює найменшому степеню усіх ненульових рівнянь вигляду $g(x) = 0$, де $g : V_n \to \{0,1\}$, що є наслідками одного з рівнянь $F(x) = 0$, $F(x) = 1$ (див., наприклад, [1], [2], [4]).

Наведені результати свого часу стимулювали розвиток методів побудови булевих функцій з великою алгебраїчною імунністю, що володіють також іншими властивостями, необхідними для забезпечення стійкості відповідних генераторів гами відносно сучасних атак. Не дивлячись на певний прогрес у розв'язанні цієї задачі, слід констатувати, що відомі конструкції таких функцій [8], [12], [13] виявляються надто громіздкими з погляду реалізації або задовольняють не усі потрібні для застосувань криптографічні критерії. Добро вивченими та практично прийнятними є функції, що використовуються у сучасних блокових (а також деяких потокових) шифрах [14], проте алгебраїчна імунність таких функцій є надто малою (не перевищує 3) для того, щоб використовувати їх в ролі функцій ускладнення фільтрувальних генераторів гами. Це стимулює пошук способів підвищення стійкості зазначених генераторів відносно алгебраїчних атак без зміни функцій ускладнення.

Метою статті є підвищення стійкості фільтрувальних генераторів гами при фіксованих довжині початкового стану та функції ускладнення, яка має обмежену алгебраїчну імунність.

Виклад основного матеріалу дослідження. Позначимо α корінь полінома $f(x)$ в полі $\mathbf{GF}(2^n)$ (який є примітивним елементом цього поля) та зафіксуємо поліном $v(x) = v_{n-1}x^{n-1} \oplus \cdots \oplus v_0 \in \mathbf{GF}(2)[x]$ такий, що $v(\alpha)$ також є примітивним елементом поля $\mathbf{GF}(2^n)$.

Розглянемо генератор гами, який функціонує за законом

$$F(uv(S)^i) = \gamma_i,\ i = 1, 2, \ldots, \tag{2}$$

де F, u, S, γ_i мають той самий сенс, що і вище, а $v(S) = v_{n-1}S^{n-1} \oplus \cdots \oplus v_0 S^0$. Початковим станом цього генератора є пара двійкових векторів $u = (u_0, \ldots, u_{n-1})$, $v = (v_0, \ldots, v_{n-1})$, причому кількість таких пар дорівнює $(2^n - 1)\varphi(2^n - 1)$, де φ – функція Ойлера (значення якої співпадає з числом примітивних елементів поля $\mathbf{GF}(2^n)$). Зауважимо, що генератор вигляду (1) є окремим випадком генератора (2), коли $v(x) = x$.

Для отримання оцінок стійкості наведеного генератора гами відносно алгебраїчних атак вважатимемо, не обмежуючи загальності, що степінь $\deg F$ функції F дорівнює її алгебраїчній імунності d, причому число d не перевищує $(n-1)/2$. Складність алгебраїчних атак на такий генератор гами становить порядку $(N_{2n,D})^3$ двійкових операцій, де D є максимальним степенем функцій $F(uv(S)^i) = F(uv(S)^i e_1, \ldots, uv(S)^i e_n)$, $i = 1, 2, \ldots$, від $2n$ змінних $u = (u_0, \ldots, u_{n-1})$, $v = (v_0, \ldots, v_{n-1})$, а e_j позначає двійковий вектор довжини n, усі координати якого, за виключенням j-ї, дорівнюють нулю, $j \in \overline{1,n}$.

Позначимо $g_{i,j}(u,v) = uv(S)^i e_j$ та помітимо, що

$$\deg F(uv(S)^i) \le \min\{2n, \max_{1 \le j_1 < \ldots < j_d \le n} \{\deg g_{i,j_1} + \ldots + \deg g_{i,j_d}\}\}, \tag{3}$$

де максимум береться за всіма сполученнями $\{j_1, \ldots, j_d\}$ з n по d.

Припустимо, що для кожного $i = 1, 2, \ldots$ нерівність (3) обертається на рівність. Тоді

$$D = \max_i \min\{2n, \max_{1 \le j_1 < \ldots < j_d \le n} \{\deg g_{i,j_1} + \ldots + \deg g_{i,j_d}\}\}, \tag{4}$$

і для отримання оцінок складності алгебраїчних атак на генератор, що розглядається, достатньо оцінити знизу значення $\deg g_{i,j}$ за всіма $i = 1, 2, \ldots$, $j \in \overline{1,n}$.

Твердження. Справедлива нерівність $\deg g_{i,j} \ge 2$, $i = 1, 2, \ldots$, $j \in \overline{1,n}$. Крім того, для кожного $i < 2^n$, що не є степенем двійки, існує принаймні одне значення j таке, що $\deg g_{i,j} \ge 3$.

Доведення. Помітимо, що $v(S)^i = v_0 S^0 \oplus v_1 S^i \oplus \cdots \oplus v_{n-1} S^{i(n-1)} \oplus w_i(S)$, де $w_i(S)$ є сумою всіх добутків $v_{k_1} v_{k_2} \cdots v_{k_i} S^{k_1 + k_2 + \cdots + k_i}$ таких, що серед чисел $k_1, k_2, \ldots, k_i \in \overline{0, n-1}$ є принаймні два різних. Далі, оскільки S є оборотною матрицею, то $v_k S^{ik} e_j$ є ненульовим стовпцем, причому кожен ненульовий елемент цього стовпця дорівнює v_k, $k \in \overline{0, n-1}$. Але тоді стовпець $(v_0 S^0 \oplus v_1 S^i \oplus \cdots \oplus v_{n-1} S^{i(n-1)}) e_j$ також є ненульовим, і всі його ненульові елементи мають степінь 1. При цьому кожен ненульовий елемент стовпця $w_i(S) e_j$ має степінь не менше ніж 2. Отже, $\deg(v(S)^i e_j) \ge 1$ і $\deg(uv(S)^i e_j) \ge 2$, що й треба було довести.

Припустимо зараз, що i не є степенем двійки, і для кожного $j \in \overline{1,n}$ виконується рівність $\deg g_{i,j} = 2$. Тоді з наведених вище міркувань випливає, що $w_i(S) = 0$. Отже, має місце

рівність $v(S)^i = v_0 S^0 \oplus v_1 S^i \oplus \cdots \oplus v_{n-1} S^{i(n-1)}$ матричних поліномів від булевих змінних $v_0,...,v_{n-1}$. Звідси випливає, що для будь-яких фіксованих значень $v_0,...,v_{n-1},v'_0,...,v'_{n-1} \in \mathbf{GF}(2)$ справедливі рівності

$$\begin{aligned}((v_0 \oplus v'_0)S^0 \oplus (v_1 \oplus v'_1)S^1 \oplus \cdots \oplus (v_{n-1} \oplus v'_{n-1})S^{(n-1)})^i = \\ = (v_0 \oplus v'_0)S^0 \oplus (v_1 \oplus v'_1)S^i \oplus \cdots \oplus (v_{n-1} \oplus v'_{n-1})S^{(n-1)i} = \\ = (v_0 S^0 \oplus v_1 S^1 \oplus \cdots \oplus v_{n-1} S^{(n-1)})^i \oplus (v'_0 S^0 \oplus v'_1 S^1 \oplus \cdots \oplus v'_{n-1} S^{(n-1)})^i,\end{aligned} \quad (5)$$

які, у свою чергу, тягнуть за собою тотожність

$$(x \oplus y)^i = x^i \oplus y^i,\ x, y \in \mathbf{GF}(2^n) \quad (6)$$

Дійсно, оскільки S є супровідною матрицею примітивного полінома $f(x)$ з коренем α, то формула (5) еквівалентна рівності

$$\begin{aligned}((v_0 \oplus v'_0)\alpha^0 \oplus (v_1 \oplus v'_1)\alpha^1 \oplus \cdots \oplus (v_{n-1} \oplus v'_{n-1})\alpha^{(n-1)})^i = \\ = (v_0 \alpha^0 \oplus v_1 \alpha^1 \oplus \cdots \oplus v_{n-1} \alpha^{(n-1)})^i \oplus (v'_0 \alpha^0 \oplus v'_1 \alpha^1 \oplus \cdots \oplus v'_{n-1} \alpha^{(n-1)})^i,\end{aligned}$$

що має місце для будь-яких $v_0,...,v_{n-1},v'_0,...,v'_{n-1} \in \mathbf{GF}(2)$. Але елементи $1, \alpha,..., \alpha^{n-1}$ утворюють базис поля $\mathbf{GF}(2^n)$ над полем $\mathbf{GF}(2)$, звідки й випливає тотожність (6).

Вважаючи в (6) $y = 1$, отримаємо, що поліном $(x \oplus 1)^i \oplus x^i \oplus 1$ визначає нульову функцію над полем $\mathbf{GF}(2^n)$. Проте, якщо $i < 2^n$ не є степенем двійки, то це неможливо на підставі теорем Лукаса (див., наприклад, [15]).

Таким чином, твердження повністю доведено

Як наслідок, отримаємо, що за умови (4) складність алгебраїчних атак на генератор гами (2) становить порядку $T_2 = (N_{2n,D})^3$ двійкових операцій, де D є не менше за $2(d-1)+3 = 2d+1$, d – алгебраїчна імунність функції F. При цьому складність зазначених атак на фільтрувальний генератор (1) з такою ж довжиною початкового стану (тобто $2n$) та функцією ускладнення, яка має ту ж саму алгебраїчну імунність d, становить порядку $T_1 = (N_{2n,d})^3$ двійкових операцій.

В табл. 1 наведені значення параметрів T_1, T_2 для $n = 256$ та низки значень d. Як видно з таблиці, складність алгебраїчних атак на генератор гами вигляду (2) є у $2^{79} \div 2^{391}$ разів вище в порівнянні зі складністю цих складністю на фільтрувальний генератор гами (1).

Таблиця 1 – порівняння складності алгебраїчних атак на генератори гами

d	$\log T_1$	$\log T_2$
3	73.24	151.98
4	94.23	187.36
5	114.24	220.88
6	133.45	252.84
20	355.32	606.72
30	483.40	797.32
40	596.13	955.45
50	697.16	1088.15

Висновки. У статті запропоновано спосіб підвищення стійкості фільтрувальних генераторів гами відносно відомих алгебраїчних атак, сутність якого полягає в модифікації функції зворотного зв'язку лінійного регістру зсуву генератора. Показано, що за певної природної умови (див. формулу (4)), складність алгебраїчних атак на запропоновані генератори гами зростає у $2^{79} \div 2^{391}$ разів у порівнянні зі складністю цих атак на традиційні фільтрувальні генератори (див. табл. 1).

Недоліком запропонованого способу є уповільнення процедури гамоутворення при її програмній реалізації (не більше ніж в n разів; див. формули (1), (2)), проте цього можна уникнути, використовуючи апаратну реалізацію запропонованих генераторів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] T. W. Cusick, and P. Stanica, *Cryptographic Boolean Functions and Applications*. San Diego, California, USA: Academic Press is an imprint of Elsevier, 2009.

[2] N. Courtois, and W. Meier, "Algebraic attacks on stream ciphers with linear feedback", *in Proc. Advanced in Cryptology – EUROCRYPT 2003*, Springer Verlag, pp. 345-359, 2003. [Online]. Available: https://www.researchgate.net/publication/221348082_Algebraic_Attacks_on_Stream_Ciphers_with_Linear_Feedback. Accessed on: Sep. 12, 2023.

[3] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, "Efficient algorithms for solving overdefined systems of multivariate polinomial equations", *in Proc. Advanced in Cryptology – EUROCRYPT 2000*, Springer Verlag, pp. 392-407, 2000. [Online]. Available: https://www.researchgate.net/publication/221347926_Efficient_Algorithms_for_Solving_Overdefined_Systems_of_Multivariate_Polynomial_Equations. Accessed on: Sep. 12, 2023. doi: https://doi.org/10.1007/3-540-45539-6_27.

[4] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback", *in Proc. Advanced in Cryptology – EUROCRYPT 2003*, Springer Verlag, pp. 177-194, 2003. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-45146-4_11. Accessed on: Sep. 04, 2023.

[5] L. Bettale, J.-C. Faugere, and L. Perret, "Hybrid approach for solving multivariate systems over finite fields", *J. Math. Crypt.*, vol. 3, pp. 177-197, 2009. doi: https://doi.org/10.1515/JMC.2009.009.

[6] A. S. Meluzov, "On construction of efficient algorithms for solving systems of polynomial Boolean equations by testing a part of variables", *Diskretnaya Matematika*, vol. 23, pp. 66-79, 2011. doi: https://doi.org/10.4213/dm1162.

[7] F. Armknecht, "Improving fast algebraic attacks" *in Proc. Fast Software Encryption – FSE'04, Proceedings*, Springer-Verlag, pp. 65-82, 2004. [Online]. Available: https://www.researchgate.net/publication/220942492_Improving_Fast_Algebraic_Attacks. Accessed on: Sep. 04, 2023. doi: https://doi.org/10.1007/978-3-540-25937-4_5.

[8] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, LAGA, University of Paris 8, France, 2007.

[9] F. Armknecht, "On the existence of low-degree equatios for algebraic attacks", *Theoretische Informatik*. [Online]. Available: https://eprint.iacr.org/2004/185.pdf. Accessed on: Sep. 16, 2023.

[10] J.-C. Faugere, "A new efficient algorithm for computing Groebner bases (F4)", *Journal of Pure and Applied Algebra*, vol. 139, pp. 61-88, 1999.

[11] J.-C. Faugere, "A new efficient algorithm for computing Groebner bases without reduction to zero (F_5)", *ISSAC 2002*, ACM Press, pp. 75-83, 2002. [Online]. Available: https://dl.acm.org/doi/10.1145/780506.780516. Accessed on: Sep. 14, 2023. doi: https://doi.org/10.1145/780506.780516.

[12] D. K. Dalai, K. C. Gupta, and S. Maitra, "Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity", *in Proc. Fast Software Encryption – FSE'05, Proceedings*, Springer-Verlag, pp. 98-111, 2005. [Online]. Available: https://dl.acm.org/doi/10.1007/11502760_7. Accessed on: Sep. 16, 2023. doi: https://doi.org/10.1007/11502760_7.

[13] D. K. Dalai, S. Maitra, and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible algebraic immunity", *Designs, Codes and Cryptography*, vol. 40, pp. 41-58, 2006. [Online]. Available: https://eprint.iacr.org/2005/449.pdf. Accessed on: Jul. 17, 2023.

[14] I. Gorbenko, A. Kuznetsov, Yu. Gorbenko, A. Alekseychuk, and V. Timchenko, "Strumok Keystream Generator", *in Proc. 20018 IEEE 9th International Conference on De-pendable Systems, Services and Technologies (DESSERT)*, Kyiv, 2018, pp. 292-299. [Online]. Available:

https://ieeexplore.ieee.org/document/8409147. Accessed on: Sep. 19, 2023. doi: https://doi.org/10.1109/DESSERT.2018.8409147.

[15] E. Berlekamp, *Algebraic Coding Theory*. London, UK: World Scientific Publishing Company, 2015.

Стаття надійшла до редакції 15.11.2023.

REFERENCES

[1] T. W. Cusick, and P. Stanica, *Cryptographic Boolean Functions and Applications*. San Diego, California, USA: Academic Press is an imprint of Elsevier, 2009.

[2] N. Courtois, and W. Meier, "Algebraic attacks on stream ciphers with linear feedback", *in Proc. Advanced in Cryptology – EUROCRYPT 2003*, Springer Verlag, pp. 345-359, 2003. [Online]. Available: https://www.researchgate.net/publication/221348082_Algebraic_Attacks_on_Stream_Ciphers_with_Linear_Feedback. Accessed on: Sep. 12, 2023.

[3] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, "Efficient algorithms for solving overdefined systems of multivariate polinomial equations", *in Proc. Advanced in Cryptology – EUROCRYPT 2000*, Springer Verlag, pp. 392-407, 2000. [Online]. Available: https://www.researchgate.net/publication/221347926_Efficient_Algorithms_for_Solving_Overdefined_Systems_of_Multivariate_Polynomial_Equations. Accessed on: Sep. 12, 2023. doi: https://doi.org/10.1007/3-540-45539-6_27.

[4] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback", *in Proc. Advanced in Cryptology – EUROCRYPT 2003*, Springer Verlag, pp. 177-194, 2003. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-45146-4_11. Accessed on: Sep. 04, 2023.

[5] L. Bettale, J.-C. Faugere, and L. Perret, "Hybrid approach for solving multivariate systems over finite fields", *J. Math. Crypt.*, vol. 3, pp. 177-197, 2009. doi: https://doi.org/10.1515/JMC.2009.009.

[6] A. S. Meluzov, "On construction of efficient algorithms for solving systems of polynomial Boolean equations by testing a part of variables", *Diskretnaya Matematika*, vol. 23, pp. 66-79, 2011. doi: https://doi.org/10.4213/dm1162.

[7] F. Armknecht, "Improving fast algebraic attacks" *in Proc. Fast Software Encryption – FSE'04, Proceedings*, Springer-Verlag, pp. 65-82, 2004. [Online]. Available: https://www.researchgate.net/publication/220942492_Improving_Fast_Algebraic_Attacks. Accessed on: Sep. 04, 2023. doi: https://doi.org/10.1007/978-3-540-25937-4_5.

[8] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, LAGA, University of Paris 8, France, 2007.

[9] F. Armknecht, "On the existence of low-degree equatios for algebraic attacks", *Theoretische Informatik*. [Online]. Available: https://eprint.iacr.org/2004/185.pdf. Accessed on: Sep. 16, 2023.

[10] J.-C. Faugere, "A new efficient algorithm for computing Groebner bases (F4)", *Journal of Pure and Applied Algebra*, vol. 139, pp. 61-88, 1999.

[11] J.-C. Faugere, "A new efficient algorithm for computing Groebner bases without reduction to zero (F_5)", *ISSAC 2002*, ACM Press, pp. 75-83, 2002. [Online]. Available: https://dl.acm.org/doi/10.1145/780506.780516. Accessed on: Sep. 14, 2023. doi: https://doi.org/10.1145/780506.780516.

[12] D. K. Dalai, K. C. Gupta, and S. Maitra, "Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity", *in Proc. Fast Software Encryption – FSE'05, Proceedings*, Springer-Verlag, pp. 98-111, 2005. [Online]. Available: https://dl.acm.org/doi/10.1007/11502760_7. Accessed on: Sep. 16, 2023. doi: https://doi.org/10.1007/11502760_7.

[13] D. K. Dalai, S. Maitra, and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible algebraic immunity", *Designs, Codes and Cryptography*, vol. 40, pp. 41-58, 2006. [Online]. Available: https://eprint.iacr.org/2005/449.pdf. Accessed on: Jul. 17, 2023.

[14] I. Gorbenko, A. Kuznetsov, Yu. Gorbenko, A. Alekseychuk, and V. Timchenko, “Strumok Keystream Generator”, *in Proc. 20018 IEEE 9th International Conference on De-pendable Systems, Services and Technologies (DESSERT)*, Kyiv, 2018, pp. 292-299. [Online]. Available: https://ieeexplore.ieee.org/document/8409147. Accessed on: Sep. 19, 2023. doi: https://doi.org/10.1109/DESSERT.2018.8409147.

[15] E. Berlekamp, *Algebraic Coding Theory*. London, UK: World Scientific Publishing Company, 2015.

KATERYNA VOROBEI,
ANTON ALEKSEYCHUK

FILTER GENERATORS WITH INCREASED RESISTANCE AGAINST ALGEBRAIC ATTACKS

Filter generators form one of the best known and most studied classes of key stream generators used in synchronous stream ciphers. Each such generator consists of a binary linear shift register with a primitive feedback polynomial and a nonlinear Boolean function, which has a number of requirements related to the condition of generator security against known attacks.

One such requirement is the high algebraic immunity of the generator's filter function; this parameter characterises security filter generator against modern algebraic attacks. In certain cases, this requirement is too restrictive in sense of practicality, as it increases the computational or circuit complexity of the key stream generation algorithm. This makes the actuality of increasing the resistance of filter generators with fixed filter functions, that have limited (low) algebraic immunity.

The paper proposes to solve this problem by modifying the feedback function of the linear shift register. the security of the proposed generators against algebraic attacks is investigated and is shown that (under certain natural conditions) such generators are more secure at the same initial state length as compared to traditional filter generators. The proposed solution seems to be useful for practical application in advanced hardware-oriented stream ciphers design.

Keywords: cybersecurity, cryptographic protection of information, stream cipher, filter generator, algebraic attack, security justification.

Воробей Катерина Іллівна, аспірант кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна, ORCID 0009-0007-4523-0626, katerinabuturlakina@gmail.com.

Олексійчук Антон Миколайович, доктор технічних наук, професор, професор кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна, ORCID 0000-0003-4385-4631, alex-dtn@ukr.net.

Vorobei Kateryna, postgraduate student at the state information resources academic department, Institute of special communication and information protection of the National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.

Alekseychuk Anton, doctor of technicai science, professor, professor at the state information resources academic department, Institute of special communication and information protection of the National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.