THE FOUR–PART BLOCKS WERE ADDED IN CHORAL PRACTICE BY XSEPES8-2 NETWORK

Jumakulov Abdumannon Kodirjonovich

Kokand University Department of digital technology and mathematics

ABSTRACT The article lists the xsepes8–2 network with two round functions that use the same algorithm in encryption and decryption

Keywords: encryption, algorithm, decryption, round, reflection

ТЎРТТА ҚИСМ БЛОКЛАРИ XOR АМАЛИ БЎЙИЧА ҚЎШИЛГАН XSEPES8–2 ТАРМОҒИ

Жумакулов Абдуманнон Кодиржонович

Қўқон Университети Рақамли технологиялар ва математика кафедраси

АННОТАЦИЯ

Мақолада шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиладиган иккита раунд функцияга эга XSEPES8–2 тармоғи келтирилган

Калит сўзлар: шифрлаш, алгоритм,дешифрлаш, раунд, акслантириш

Ҳозирда Фейстел тармоғига асосланган блокли шифрлаш алгоритмлари кенг қўлланилиб бормоқда. Фейстел тармоғи асосида яратилган блокли шифрлаш алгоритмларига DES, ГОСТ 28147-89 каби блокли шифрлаш алгоритмлари, шунингдек, NIST томонидан эълон қилинган конкурсда қатнашган CAST-256, DFC, E2, LOKI97 каби блокли шифрлаш алгоритмларини олиш мумкин. Бу тармоқнинг асосий афзаллиги шундан иборатки, шифрлаш ва дешифрлашда битта алгоритмдан фойдаланилади, фақат дешифрлашда шифрлаш раунд калитлари тескари тартибда қўлланилади. Бу тармоқ структурасидан фойдаланилган ҳолда бир неча раунд функциядан фойдаланилган ҳолда функционал ва баланслашган функционал Фейстел

тармоқлари ҳам ишлаб чиқилган [1, 3]. Фейстел тармоғининг шифрлаш ва дешифрлаш асклантиришлари қуйидаги формулалар орқали ифода этиш мумкин [1, 3]:

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \end{cases}, i = \overline{1...n} \qquad (1) \qquad \begin{cases} R_{i-1} = L_i \\ L_{i-1} = R_i \oplus F(L_i, K_i) \end{cases}, i = \overline{n...1} \qquad (2)$$

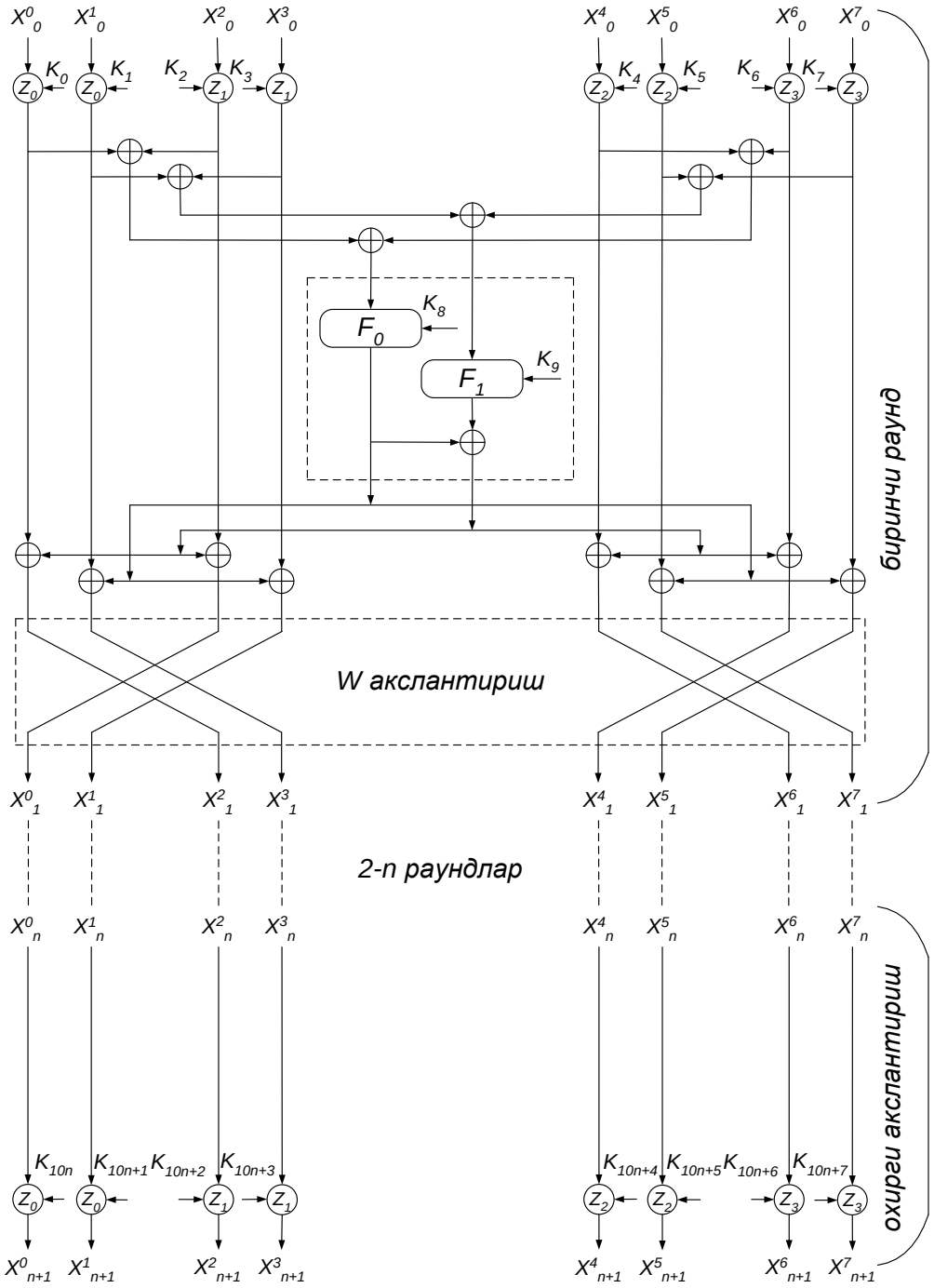
Бу тармоққа асосланган блокли шифрлаш алгоритмлари бардошлиги тармоқ раунд функциясига узвий боғлиқ. Шунингдек, тармоқ F раунд функцияси исталган кўринишда бўлса ҳам, дешифрлашда бу функцияга тескари бўлган F^{-1} функция қуриш ҳожати йўқ, чунки (2) формуладаги R_i ўрнига (1) формуладаги $L_{i-1} \oplus F(R_{i-1}, K_i)$ қийматни қўйсак, $L_{i-1} = R_i \oplus F(L_i, K_i) = L_{i-1} \oplus F(R_{i-1}, K_i) \oplus F(L_i, K_i) = L_{i-1}$ тенглик келиб чиқади [3, 4].

PES [1] блокли шифрлаш алгоритм 1990 йилда яратилган бўлиб, бу алгоритм Лай–Мэсси схемасига асосланган. 1991 йилда муаллифлар бу блокли шифрлаш алгоритмни қайта ишлаб чиқишди ва IDEA [2] деб номлашди. Бу блокли шифрлаш алгоритмларида раунд калитлари қисм блокларга $2^{16}+1$ модул бўйича кўпайтирилади, 2^{16} модул бўйича қўшилади ва МА акслантиришда $2^{16}+1$ модул бўйича кўпайтириш, 2^{16} модул бўйича қўшиш амаллари қўлланилган, яъни амаллар сони чекланган. Лекин бунга қарамасдан, шифрлаш ва дешифрлашда битта алгоритмдан фойдаланилади, шунингдек худди Фейстел тармоғи каби дешифрлашда шифрлаш раунд калитлари тескари тартибда қўлланилади . IDEA NXT блокли шифрлаш алгоритми эса P. Junod, S. Vaudenay томонидан яратилган бўлиб кенгайтирилган Лай–Мэсси схемасига асосланган. Кейинчалик IDEA NXT алгоритми FOX [3] деб атала бошлади.

PES блокли шифрлаш алгоритми структураси ва кенгайтирилган Лай–Мэсси схемаси фойдаланилган ҳолда алгоритмдаги МА акслантириш ўрнига раунд функция қўллаш орқали шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиладиган тармоқ яратиш мумкин. PES блокли шифрлаш алгоритми структурасидан фойдаланган ҳолда саккизта қисм блок ва тўртта раунд функциядан иборат PES8–4 тармоғи [] мақолада келтирилган. Ушбу мақолада эса PES блокли шифрлаш алгоритми структураси ва кенгайтирилган Лай–

Мэсси схемасидан фойдаланган ҳолда саккизта қисм блок ва иккита раунд функциядан ташкил топган, тўртта қисм блоки XOR амали бўйича қўшилган XSEPES8–2 (subblocks XOR summed extended PES) тармоғи келтирилган.

Тармоқ структураси. Таклиф этилган XSEPES8–2 тармоғида z_0, z_1, z_2, z_3 амаллар сифатида $\otimes$ (mul), $\boxplus$ (add) ва $\oplus$ (xor) амалларини олиш мумкин. Бу ерда $\otimes$ – 32 (16, 8) битли блокларни $2^{32}+1$ $(2^{16}+1, 2^8+1)$ модул бўйича кўпайтириш, $\boxplus$ – 32 (16, 8) битли блокларни 2^{32} $(2^{16}, 2^8)$ модул бўйича қўшиш амали ва $\oplus$ – 32 (16, 8) битли блокларни XOR бўйича қўшиш амали. Тармоқнинг қисм блоклари узунлиги 32 бит бўлганда блок узунлиги 256 бит, 16 бит бўлганда блок узунлиги 128 бит, 8 бит бўлганда блок узунлиги 64 бит бўлган блокли шифрлаш алгоритмлар яратиш мумкин. Тармоқнинг шифрлаш формуласи (3) да, функционал схемаси эса 1–расмда келтирилган.



1–расм. XSEPES8–2 тармоғи функционал схемаси

XSEPES8–2 тармоғида қисм блоклар, $K_{10(i-1)}$, $K_{10(i-1)+1},\ldots,$ $K_{10(i-1)+7}$, $i=\overline{1...n+1}$ раунд калитлар, F_0, F_1 раунд функцияларнинг кириш ва чиқиш битлар узунлиги 32 (16, 8) битга тенг. $K_{10(i-1)+8}$, $K_{10(i-1)+9}$, $i=\overline{1...n}$ раунд калитлари узунлиги эса 32 (16, 8) битга тенг бўлиши шарт эмас.

$$\begin{cases} X_i^0 = (X_{i-1}^2(z_1)K_{10(i-1)+2}) \oplus T_i^0 \oplus T_i^1 \\ X_i^1 = (X_{i-1}^3(z_1)K_{10(i-1)+3}) \oplus T_i^0 \\ X_i^2 = (X_{i-1}^0(z_0)K_{10(i-1)}) \oplus T_i^0 \oplus T_i^1 \\ X_i^3 = (X_{i-1}^1(z_0)K_{10(i-1)+1}) \oplus T_i^0 \\ X_i^4 = (X_{i-1}^6(z_3)K_{10(i-1)+6}) \oplus T_i^0 \oplus T_i^1 \\ X_i^5 = (X_{i-1}^7(z_3)K_{10(i-1)+7}) \oplus T_i^0 \\ X_i^6 = (X_{i-1}^4(z_2)K_{10(i-1)+4}) \oplus T_i^0 \oplus T_i^1 \\ X_i^7 = (X_{i-1}^5(z_2)K_{10(i-1)+5}) \oplus T_i^0 \end{cases}, \ i = \overline{1...n} \tag{3}$$

$$\begin{cases} X_{n+1}^0 = (X_n^0(z_0)K_{10n}) \\ X_{n+1}^1 = (X_n^1(z_0)K_{10n+1}) \\ X_{n+1}^2 = (X_n^2(z_1)K_{10n+2}) \\ X_{n+1}^3 = (X_n^3(z_1)K_{10n+3}) \\ X_{n+1}^4 = (X_n^4(z_2)K_{10n+4}) \\ X_{n+1}^5 = (X_n^5(z_2)K_{10n+5}) \\ X_{n+1}^6 = (X_n^6(z_3)K_{10n+6}) \\ X_{n+1}^7 = (X_n^7(z_3)K_{10n+7}) \end{cases}, \textit{ охирги акслантиришда}$$

бу ерда T_i^0, T_i^1 тармоқ раунд функциялари бўлиб,

$T_i^0 = F_0(((X_{i-1}^0(z_0)K_{10(i-1)}) \oplus (X_{i-1}^2(z_1)K_{10(i-1)+2})) \oplus ((X_{i-1}^4(z_2)K_{10(i-1)+4}) \oplus (X_{i-1}^6(z_3)K_{10(i-1)+6})), K_{10(i-1)+8})$,

$T_i^1 = F_1(((X_{i-1}^1(z_0)K_{10(i-1)+1}) \oplus (X_{i-1}^3(z_1)K_{10(i-1)+3})) \oplus ((X_{i-1}^5(z_2)K_{10(i-1)+5}) \oplus (X_{i-1}^7(z_3)K_{10(i-1)+7})), K_{10(i-1)+9})$

кўринишда тасвирланади.

W акслантиришда ҳар бир раундда X_{i-1}^0 ва X_{i-1}^2, X_{i-1}^1 ва X_{i-1}^3, X_{i-1}^4 ва X_{i-1}^6, X_{i-1}^5 ва X_{i-1}^7 қисм блоклар ўзаро ўрин алмашади. 1–расмда келтирилган тармоқ схемасини 1–вариантдаги тармоқ деб олсак,

– фақат X_{i-1}^0 ва X_{i-1}^2, X_{i-1}^4 ва X_{i-1}^6, $i = \overline{1...n}$ қисм блоклар ўзаро алмашган тармоқни

2–вариантдаги тармоқ,

– қисм блоклар алмашмаган тармоқни 3–вариантдаги тармоқ,

– фақат X_{i-1}^1 ва X_{i-1}^3, X_{i-1}^5 ва X_{i-1}^7, $i = \overline{1...n}$ қисм блоклар ўзаро алмашган тармоқни

4–вариантдаги тармоқ сифатида қабул қилиш мумкин.

2, 3 ва 4–вариантдаги тармоқлар шифрлаш формулалари (3) га ўхшаш, фақат

– 2–вариантдаги тармоқда X_i^1 ва X_i^3, X_i^5 ва X_i^7 қийматлар,

– 3–вариантдаги тармоқда X_i^0 ва X_i^2, X_i^1 ва X_i^3, X_i^4 ва X_i^6, X_i^5 ва X_i^7 қийматлар,

– 4–вариантдаги тармоқда X_i^0 ва X_i^2, X_i^4 ва X_i^6 қийматлар ўзаро ўрин алмашади.

Калитлар генерацияси. $n-$раундли XSEPES8–2 тармоғида ҳар бир раундда 10 та ва охирги акслантиришда 8 та раунд калити иштирок этади, яъни жами раунд калитлари сони $10n+8$ га тенг. Шифрлашда алгоритми K калитидан бирор қоидага кўра $10n+8$ та K_i^c шифрлаш раунд калитлари генерация қилинади. $10n+8$ та K_i^d дешифрлаш раунд калитлари эса шифрлаш раунд калитлари асосида яратилади. Шифрлашда 1–расм ва (3) формуладага K_i ўрнига K_i^c шифрлаш раунд калити, дешифрлашда эса K_i^d дешифрлаш раунд калити қўлланилади, яъни шифрлаш ва дешифрлашда битта тармоқдан фойдаланилади, фақат калитлар жойлашиш тартиби ўзгаради. Барча вариантлардаги *n*–раундли XSEPES8–2 тармоғи биринчи, иккинчи ва *n*–раунд дешифрлаш калитлари шифрлаш раунд калитларига қуйидагича боғланган:

$$\begin{aligned}&(K^d_{10(i-1)},K^d_{10(i-1)+1},K^d_{10(i-1)+2},K^d_{10(i-1)+3},K^d_{10(i-1)+4},K^d_{10(i-1)+5},K^d_{10(i-1)+6},K^d_{10(i-1)+7},K^d_{10(i-1)+8},K^d_{10(i-1)+9})=\\&((K^c_{10(n-i+1)})^{z_0},(K^c_{10(n-i+1)+1})^{z_0},(K^c_{10(n-i+1)+2})^{z_1},(K^c_{10(n-i+1)+3})^{z_1},(K^c_{10(n-i+1)+4})^{z_2},(K^c_{10(n-i+1)+5})^{z_2},\\&(K^c_{10(n-i+1)+6})^{z_3},(K^c_{10(n-i+1)+7})^{z_3},K^c_{10(n-i)+8},K^c_{10(n-i)+9}),i=\overline{1...n}.\end{aligned} \quad (4)$$

Агарда z_0, z_1, z_2, z_3 амаллари сифатида $\otimes$ амал қўлланилса, $K=K^{-1}$, $\boxplus$ амал қўлланилса, $K=-K$ ва $\oplus$ амал қўлланилса, $K=K$, бу ерда $K^{-1}-K$ сонига $2^{32}+1$ $(2^{16}+1,2^8+1)$ модул бўйича тескари қиймат, $-K-K$ сонига 2^{32} $(2^{16},2^8)$ модул бўйича қарама–қарши қиймат. 32 битли сонлар учун $K\otimes K^{-1}=1\bmod(2^{32}+1)$, 16 битли сонлар учун $K\otimes K^{-1}=1\bmod(2^{16}+1)$, 8 битли сонлар учун $K\otimes K^{-1}=1\bmod(2^8+1)$ ва $-K\boxplus K=0$, $K\oplus K=0$.

Охирги акслантириш дешифрлаш раунд калитлари эса шифрлаш раунд калитларига қуйидагича боғланган:

$$(K_{10n}^d, K_{10n+1}^d, K_{10n+2}^d, K_{10n+3}^d, K_{10n+4}^d, K_{10n+5}^d, K_{10n+6}^d, K_{10n+7}^d) = ((K_0^c)^{z_0}, (K_1^c)^{z_0}, (K_2^c)^{z_1}, (K_3^c)^{z_1}, (K_4^c)^{z_2}, (K_5^c)^{z_2}, (K_6^c)^{z_3}, (K_7^c)^{z_3}). \quad (5)$$

Олинган натижалар. Тадқиқот натижасида саккизта қисм блок ва иккита раунд функциядан ташкил топган XSEPES8–2 тармоғи яратилди. PES8–4 тармоғида иккита қисм блок XOR бўйича қўшилиб, ҳосил бўлган қиймат раунд функцияга кирувчи қиймат сифатида қабул қилинса, XSEPES8–2 тармоғида эса тўртта қисм блок XOR бўйича қўшилиб, ҳосил бўлган қиймат раунд функцияга кирувчи қиймат сифатида қабул қилинади. Шунингдек, XSEPES8–2 тармоғида шифрлаш ва дешифрлашда битта алгоритмдан фойдаланилади ва z_0, z_1, z_2, z_3 алгебраик амаллари ўзгарувчан.

Хулоса. Таклиф этилган XSEPES8–2 тармоғининг раунд функцияси сифатида блокли шифрлаш алгоритмларида кенг қўлланиладиган акслантиришларни, шунингдек, бир томонли, яъни тескариси мавжуд бўлмаган акслантиришларни ҳам олиш мумкин. z_0, z_1, z_2, z_3 амаллари сифатида add, mul, xor амалларини (z_0, z_0, z_1, z_1, z_2, z_2, z_3, z_3) кўринишда $3^4 = 81$ усулда танлаш мумкин, яъни барча мумкин бўлган вариантлари 81 га тенг. Шунингдек, қисм блоклари алмашишига боғлиқ ҳолда тўртта варианти мавжуд. Амалларни саксон бир усулда ва вариантларни тўрт усулда танлаш орқали F_0, F_1 раунд функциялари ўзгармас бўлган XSEPES8–2 тармоғига асосланган 324 та блокли шифрлаш алгоритмлари қуриш мумкин. Бу тармоғи асосида яратилган блокли шифрлаш алгоритмларда шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиш ҳисобига аппарат ва дастурий–аппарат воситалари ишлаб чиқиш қулайлик туғдиради, яъни битта қурилма ёки дастурдан шифрлаш ва дешифрлашда фойдаланилади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Lai X., Massey J.L. A proposal for a new block encryption standard. Advances in Cryptology – Proc. Eurocrypt’90, LNCS 473, Springer–Verlag, 1991, pp. 389–404.

2. Lai X., Massey J.L. On the design and security of block cipher. ETH series in information processing, v.1, Konstanz: Hartung–Gorre Verlag, 1992.
3. Junod, P., Vaudenay, S.. FOX: a new family of block ciphers. In 11th Selected Areas in Cryptography (SAC) Workshop, LNCS 3357, pages 114–129. Springer–Verlag.
4. http://ru.wikipedia.org/wiki/AES_(конкурс)