УДК 621.391:519.2 **DOI:10.30837/rt.2021.1.204.07**

Е.В. КОТУХ, канд. техн. наук, А.В. СЕВЕРИНОВ, канд. техн. наук,
А.В. ВЛАСОВ, канд. техн. наук, А.А. ТЕНИЦКАЯ, Е.А. ЗАРУДНАЯ

НЕКОТОРЫЕ РЕЗУЛЬТАТЫ РАЗРАБОТКИ СХЕМ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ С ИСПОЛЬЗОВАНИЕМ НЕАБЕЛЕВЫХ ГРУПП

Введение

Развитие криптографии с открытым ключом было революционной концепцией, появившейся в двадцатом веке. Первым опубликованным исследованием криптографии с открытым ключом была схема согласования ключей, описанная Диффи и Хеллманом (DH) в 1976 г. Наиболее распространенная криптография с открытым ключом и повседневно используемые схемы (DH, RSA, ElGamal, ECC) зависят от структуры абелевых групп. Их безопасность зависит от вычислительной сложности и неразрешимости некоторых сложных проблем теории чисел. Например, алгоритм RSA зависит от задачи целочисленной факторизации. Алгоритмы Диффи – Хеллмана, Эль-Гамаля и ECC зависят от решения задачи дискретного логарифмирования (DLP). В 1997 г. Шор указал, что существуют алгоритмы с полиномиальным временем для решения факторизации и дискретных логарифмических задач, основанные на абелевых группах в приложении для квантового компьютера [1]. С появлением практических результатов в реализации алгоритмов Шора и Гровера на квантовых компьютерах реализация успешной атаки на упомянутые криптосистемы с открытым ключом становится вопросом времени. Современные результаты в решении задачи построения квантового компьютера достаточной мощности мотивируют разработчиков криптопримитивов к пересмотру существующих подходов и определению наиболее эффективных с точки зрения решения задач постквантовой криптографии. Одним из таких перспективных исследовательских приоритетов является исследование криптосистем на основе неабелевых групп.

Проблемы поиска сопряженности, поиска членства и другие варианты являются сложно решаемыми в теории неабелевых групп и являются основой для построения доказуемо безопасных криптосистем с открытым ключом. Наиболее часто обсуждаемые криптографические неабелевые применения включают группы матриц, группы кос, полупрямые произведения, логарифмические подписи (LS) [2 – 8] и алгебраические ластики (AE). Построение криптосистем на основе решения сложной проблемы слова в алгебре групп было предложено Вагнером и Мадьяриком в [9]. Многие неабелевы протоколы установления ключей на основе групп связаны с протоколом Диффи – Хеллмана (DH).

Цель статьи – обзор основных алгоритмов и свойств неабелевых групповых криптосистем с открытым ключом. Предложенные криптосистемы с открытым ключом на основе неабелевых групп реализуют либо шифрование-дешифрование, либо протоколы согласования ключей. Мы обсудим различные криптографические примитивы, которые используют некоммутативные группы в качестве основы для постквантовых примитивов. Здесь и далее мы будем использовать термин «платформа» для обозначения используемой математической основы в построении криптосистемы. Стандартная модель криптографической схемы с открытым ключом состоит из двух сторон, называемых Алисой и Бобом. Предположим, что Алиса хочет отправить сообщение M Бобу. Общая модель схемы шифрования следующая. Алиса использует алгоритм шифрования f_{k_1} для шифрования сообщения $C = f_{k_1}(M)$, где f_{k_1} – односторонняя функция и является публичной. После получения шифра C Боб использует соответствующий алгоритм дешифрования g_{k_2} для декодирования $g_{k_2}(f_{k_1}(M)) = M$, где g_{k_2} должен быть известен только Бобу. Противник Ева использует

методы дифференциального криптоанализа для проведения успешной атаки на платформу или реализацию.

2.1. Матричные группы: схема шифрования Ямамуры

В 1998 г. Ямамурой [10] была предложена ассиметричная схема шифрования на платформе модулярной группы $SL(2,\square)$, которая порождается двумя матрицами $S=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ и $T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, где порядки обоих порождающих $o(S)=4$ и $o(T)=\infty$ и матрица $ST=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ имеет порядок 6. Также группа $SL(2,\square)$, порожденная матрицами S и ST, имеет условия $S^4=(ST)^4=I$ и $(ST)^3=S^2$. Для матрицы $N\in SL(2,\square)$ матрицы $A:=N^{-1}\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}N$ и $B:=N^{-1}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}N$ удовлетворяют условиям $A^6=B^4=I$ и $A^3=B^2$. Таким образом, матрицы A и B порождают $SL(2,\square)$.

Алгоритм генерации ключа имеет следующий вид.

1. Боб выбирает матрицы $V_1:=(BA)^i$ и $V_2:=\left(BA^2\right)^j\in SL(2,\square)$ для некоторых $i,j\in\square$.

2. Боб выбирает матрицы $M\in GL_2(\square)$ и $F_1(X),F_2(X)\in M_{at_2}(\square[X])$ и $a\in\square$ такое, что $F_1(a)=V_1$ и $F_2(a)=V_2$.

3. Боб вычисляет $W_1(X):=M^{-1}F_1(X)M$ и $W_2(X):=M^{-1}F_2(X)M$.

Теперь у Боба есть публичный ключ: $W_1(X),W_2(X)$ и секретный ключ: M,a

Алгоритм шифрования реализуется следующим образом:

Пусть $b_1...b_n\in\{0,1\}^n$ – сообщение, а Алиса шифрует его следующим образом:

$$C(X):=W_2(X)\prod_{i=1}^{n}\left(W_1(X)^{b_i+1}W_2(X)\right)$$

Криптоанализ. Протокол основан на проблеме поиска сопряженности и проблеме корня. Но Р. Стейнвандт [11] указал, что схема шифрования Ямамуры небезопасна. Предположим, что противник Ева перехватила шифр $C(X)$, тогда она может вычислить $D(X):=W_2(X)^{-1}C(X)=\prod_{i=1}^{n}\left(W_1(X)^{b_i+1}W_2(X)\right)$.

Элементы матрицы T $\left(W_1(X)^{b_i+1}W_2(X)\right)^{-1}D(X)$ должны быть полиномами над C. Начиная с первого бита b_1, если хотя бы один из элементов $D_1:=\left(W_1(X)^2W_2(X)\right)^{-1}D(X)$ содержит непостоянный знаменатель, мы можем заключить, что $b_1=0$, а иначе $b_1=1$. Аналогично, если матрица $D_2:=\left(W_1(X)^2W_2(X)\right)^{-1}D(X)$ содержит неполиномиальный элемент, то можно заключить, что $b_2=0$; в противном случае $b_2=1$. Процесс будет продолжаться, пока не будут восстановлены все биты $b_i,i=1,...,n$. Это означает, что открытый текст $b_1...b_n\in\{0,1\}^n$ может быть эффективно восстановлен только из зашифрованного текста $C(X)$ и публичных данных.

2.2. Матричные группы: BMMC/MMMC1/MMMC2.

В 2013 г. С.К. Росошек [12] предложил схему шифрования типа Эль-Гамаля, названную BMMC (базовая матричная модульная криптосистема), с использованием матриц над $\mathbb{Z}_n$. Общая концепция заключается в следующем. Пусть n – большое натуральное число, и пусть $G(\alpha,\beta,\gamma)$ – свободная подгруппа общей линейной группы $GL(2,\mathbb{Z}_n)$, порожденной тремя образующими A,B и C, где $\alpha,\beta,\gamma\in\mathbb{Z}$ с $|\alpha|,|b|,|\gamma|\geq 3$, $A=\begin{pmatrix}1 & 0\\ \alpha & 0\end{pmatrix}$, $B=\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}$ и $C=\begin{pmatrix}1-\gamma & r\\ -\gamma & \gamma+1\end{pmatrix}$. Все предложенные переменные – публичные. Пусть q порядок группы $GL(2,\mathbb{Z}_n)$.

Алгоритм генерации ключа имеет следующий вид.

Боб выбирает две случайные матрицы P_1 и U в $G(\alpha,\beta,\gamma)$ с условием, что $P_1U\neq UP_1$ и три целых числа k,s,l с условием, что $-q\leq k,s\leq q$ и $2\leq q$

Боб вычисляет $P_2:=U^{-s}P_1^kU^s$ и $P_3:=U^l$.

Таким образом, у Боба есть общий ключ n,P_1,P_2,P_3 и секретный ключ U,k,s.

Алгоритм шифрования.

Пусть сообщение $m\in Mat(2,\mathbb{Z}_n)$ будет матрицей. Алиса выбирает целые числа $r,t\in\mathbb{Z}_n$ и вычисляет шифротекст выражением $(C_1,C_2):=\left(P_3^{-r}P_1^tP_3^r, mP_3^rP_2^{-t}P_3^{-r}\right)$.

Алгоритм дешифрования. Боб вычисляет m, используя секретные ключи k,s, с помощью выражения: $C_2U^{-s}C_1^kU^s=m$

Криптоанализ. Если Ева хочет сломать систему, Ева должна решить задачи преобразования и гибридную задачу, которые сложнее, чем проблема дискретного логарифма в группе той же мощности. BMMC требует трех матричных модульных возведений в степень для генерации ключа. Есть три возведения в степень при шифровании и два возведения в степень при дешифровании. Для ускорения работы алгоритма С.К. Росошек дал две модифицированные схемы, названные MMMC1 и MMMC2 [13]. Обе модифицированные схемы аналогичны, и по этой причине в работе рассмотрена лишь первая.

Алгоритм генерации ключа.

1. Боб вычисляет целое число n, где n может быть либо степенью простого p^r, либо произведением $n=pq$ двух различных простых чисел.

2. Боб определяет две обратимые матрицы $V,W\in GL(2,\mathbb{Z}_n)$, чтобы определить два коммутирующих внутренних автоморфизма α,β кольца $Mat(2,\mathbb{Z}_n):\alpha(D):=V^{-1}DV$ и $\beta(D):=W^{-1}DW$ для всех $D\in Mat(2,\mathbb{Z}_n)$.

3. Боб вычисляет два автоморфизма $\phi:=\alpha^2\beta$ и $\psi:=\alpha\beta^2$.

4. Боб выбирает матрицу $L\in GL(2,\mathbb{Z}_n)$, такую, чтобы $L\notin G$.

5. Боб получает общий ключ $n,\phi(L),\psi(L^{-1})$ и секретный ключ V,W,α,β.

Алгоритм шифрования.

Для реализации шифрования пусть сообщение $m\in Mat(2,\mathbb{Z}_n)$ будет матрицей, тогда:

1. Алиса выбирает $Y\in G$ и определяет внутренний автоморфизм ζ кольца $Mat(2,\mathbb{Z}_n)$ вычисляя $\zeta(D):=Y^{-1}DY$.

2. Алиса вычисляет матрицы $\zeta(\phi(L)),\zeta\left(\psi\left(L^{-1}\right)\right)$ и $m\zeta(\phi(L))$.

3. Алиса вычисляет блок $\gamma \in \square_n$.

4. Алиса вычисляет шифротекст $(C_1, C_2) := \left(\gamma^{-1} \cdot \zeta\left(\psi\left(L^{-1}\right), \gamma \cdot m \cdot \zeta\left(\phi(L)\right)\right)\right)$.

Алгоритм дешифрования.

1. Боб дешифрует сообщение, используя секретный ключ $C_2 \cdot \alpha^{-1}\beta(C_1) = m$.

Криптоанализ. Безопасность схемы основана на проблеме поиска сопряженности "случайной соли". Для заданных матриц A, B в $Mat(2, \square_n)$ необходимо найти обратимую матрицу $X \in GL(2, \square_n)$ и целое число $0 < \gamma < n$, такое что $X^{-1}AX = \gamma B$. Если целое число γ в алгоритме шифрования удаляется, то система небезопасна. Это связано с тем, что обычная задача поиска сопряженности на общей линейной группе $GL(2, \square_n)$ не является сложной. Уравнение $C_1 = Y^{-1}\psi(L^{-1})Y$ может быть преобразовано в систему четырех линейных уравнений с четырьмя неизвестными. С другой стороны, автор [13] утверждал, что “соль” γ может быть найдена только при атаке грубой силы, и для больших n эта проблема становится неразрешимой.

2.3. Схемы на основе группы кос

Впервые группы кос были явно введены Э. Артиным [14]. Существует несколько способов представления кос, но наиболее распространенным является использование генераторов Артина и основной косы [14]. Группы кос (Артина), обозначаемые как B_n , представляют собой группы кос на n нитях, определяемые следующим представлением

$$B_n := < \sigma_1, ...\sigma_{n-1} \mid \sigma_i\sigma_{i+1} = \sigma_{i+1}\sigma_i, \sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i, 1 \le i \le n-1 > .$$

Это неабелевы апериодические группы. Группы кос Артина казались хорошим кандидатом в качестве группы платформ для криптографических приложений благодаря эффективным прикладным вычислениям. В начале XXI века были предложены некоторые криптосистемы с открытым ключом на основе групп кос. Пионерские работы по криптографии на основе групп кос включают схему Аншеля – Аншеля – Голдфельда (AAG) [15] в 1999 г. и Ко–Ли (название для этой схемы составлено из фамилии первого и последнего авторов) [17] в 2000 г. Безопасность наиболее предлагаемых криптографических схем группы кос основывается на задаче поиска сопряженности или ее различных версиях, например на проблеме поиска членства. К сожалению, проблема поиска сопряженности на линейных группах несложна, и группы кос являются линейными группами [16]. Хотя наиболее предлагаемые криптографические схемы на основе групп кос уязвимы для нескольких анонсированных методов атаки [18], исследования групп кос для криптографии не уменьшились. Помимо проблемы поиска сопряженности существуют и другие сложные проблемы в группах кос, которые не были изучены экстенсивно. Поэтому мы рассматриваем работы Ко–Ли, AAG и соответствующие атаки, основанные на линейных представлениях групп кос. Алгоритмы применимы не только к группам кос, но и к любым неабелевым группам.

Схема Ко–Ли.

Пусть LB_k и RB_{n-k} будут коммутирующими подгруппами группы кос B_n , где $0 < k < n$ состоит из кос, сделанных путем заплетения k левых прядей и заплетения $n-k$ правых прядей из n прядей соответственно. Для любых $a \in LB_k$ и $b \in RB_{n-k}$ выполняется правило коммутативности: $ab = ba$.

Схема согласования ключей представлена в [17]: Алгоритм построен по подобию DH.

Общий ключ: группы кос B_n, LB_k, RB_{n-k} и коса $x \in B_n$.

1. Алиса выбирает случайную секретную косу $a \in LB_k$ и посылает Бобу $y_1 := axa^{-1}$.

2. Боб выбирает случайную секретную косу $b \in RB_{n-k}$ и посылает Алисе $y_2 := bxb^{-1}$.

3. Алиса получает y_2 и вычисляет общий ключ $K = ay_2a^{-1}$.

4. Боб получает y_1 и вычисляет общий ключ $K = by_1b^{-1}$.

Схема шифрования представлена в работе [18]:

Публичный ключ Боба x, y , где $x \in B_n, y := axa^{-1}$ и функция хеширования $H : B_n \to \{0,1\}^l$. Секретный ключ Боба: $a \in LB_k$

Шифрование реализуется следующим образом. Пусть $m \in \{0,1\}^l$ исходный текст сообщения.

1. Алиса выбирает случайную косу $b \in RB_{n-k}$.

2. Алиса вычисляет шифротекст (c, d) , где $c = bxb^{-1}$, $d = H\left(byb^{-1}\right) \oplus m$.

Алгоритм дешифрования. Дешифрование реализуется следующим образом. Боб использует простой ключ α для восстановления сообщения $m = H\left(aca^{-1}\right) \oplus d$.

Криптоанализ. Безопасность обеих этих схем основана на проблеме поиска сопряженности на группах кос. Чтобы сломать обе схемы, Еве достаточно решить проблему сопряженности кос Диффи – Хеллмана. Предлагаемый алгоритм решения задачи DH с косой примерно описывается следующим образом. Предположим, что Ева может найти такую матрицу A, что $\mathrm{K}(y_1)A = A\mathrm{K}(y_1)$ и $\mathrm{K}(\sigma_i)A = A\mathrm{K}(\sigma_i)$ для всех порождающих $\sigma_i \in LB_k$. Тогда $A\mathrm{K}(y_2)A^{-1} = A\mathrm{K}(b)\mathrm{K}(x)\mathrm{K}(b)^{-1}A^{-1} = \mathrm{K}(b)\mathrm{K}(y_1)\mathrm{K}(b)^{-1} = \mathrm{K}(K)$. Обратите внимание, что представление Лоуренса – Краммера является точным и можно эффективно найти образ $\mathrm{K}(g)$ для любого $g \in B_n$. Более того, можно эффективно восстановить $\mathrm{K} \in B_n$ из его образа $\mathrm{K}(K)$, используя алгоритм инверсии Чеона – Джуна [19].

Схема AAG

В отличие от Ко-Ли схемы схема согласования ключей AAG не требует коммутирующих подгрупп [15]. Пусть G – публичная неабелева группа и $a_1,...,a_k,b_1,...b_m \in G$ – публичные векторы. Тогда схема шифрования AAG имеет вид:

1. Алиса выбирает случайный секрет $x = x(a_1,...,a_k) \in G$ как слово в $a_1,...,a_k$.

2. Алиса посылает $b_1^x,...,b_m^x$ Бобу.

3. Боб выбирает случайный секрет $y = y(b_1,...,b_m) \in G$ как слово в $b_1,...b_m$.

4. Боб посылает $a_1^x,...,a_m^x$ Алисе.

5. Алиса вычисляет $x\left(a_1^y,...,a_k^y\right) = x^y = y^{-1}xy$ и $x^{-1}(y^{-1}xy) = K$.

6. Боб вычисляет $y\left(b_1^x,...,b_m^x\right) = y^x = x^{-1}yx$ и $\left(y^{-1}(x^{-1}yx)\right)^{-1} = K$.

Криптоанализ. В работе [16] группы кос выбраны в качестве платформы для схемы. Безопасность схемы AAG основана на проблеме множественного поиска сопряженности, которую иначе называют проблемой поиска членства. Однако для того чтобы Ева извлекла общий ключ K из общедоступной информации, достаточно решить задачу коммутатора обмена ключей, которая иначе называется проблемой AAG, за полиномиальное время. Использование метода Чеона и Джуна [19], для уменьшения проблемы коммутатора обмена ключами в матричных группах над полями.

Схема Штикеля.

В 2003 г. Э. Штикель представил алгоритмы подобные решению Диффи – Хелманна [20, 21], основанные на неабелевых группах. Алгоритмы реализуют согласование ключей,

аутентификацию и цифровую подпись. Пусть G – конечная неабелева группа и пусть $a,b \in G$ с условием $ab \neq ba$ и $o(a) = N, o(b) = M > 1$

Схема согласования ключей Штикеля.

1. Алиса выбирает два случайных натуральных числа $n < N, m < M$ и посылает Бобу $u := a^n b^m$.

2. Боб выбирает два случайных натуральных числа $r < N, s < M$ и посылает Алисе $v := a^r b^s$.

3. Алиса вычисляет общий ключ $K = a^n v b^m$.

4. Боб вычисляет общий ключ $K = a^r u b^s$.

Криптоанализ. Предположим, что Ева хочет взломать систему и перехватила значения u и v. Чтобы получить секретный общий ключ K, Еве не нужно находить пару целых чисел (n,m) или (r,s), а необходимо решить задачу поиска декомпозиции, которую можно описать следующим образом. Для рекурсивно представленной группы G две рекурсивно порожденные подгруппы $A, B \in G$ и два элемента $u, w \in G$. Необходимо найти два элемента $x \in A$ и $y \in B$ такие, чтобы $x \cdot w \cdot y = u$, если существует хотя бы одна такая пара элементов. Предположим, что Ева может найти пару $x, y \in G$, которая удовлетворяет системе уравнений

$$\begin{cases} xa = ax \\ yb = by \\ u = xwy \end{cases}$$

Тогда Ева может воспользоваться перехваченным у Боба значением v , чтобы вычислить

$$xvy = xa^r wb^s y = a^r xwyb^s = a^r ub^s = K$$

Предлагаемые платформы: в статье [21] было предложено использовать общую линейную группу $GL_k(\mathrm{F}_{2^t})$ как базовую группу G. Тогда указанная выше система из трех уравнений, включая нелинейное уравнение, может быть приведена к системе из трех уравнений:

$$\begin{cases} x^{-1}a = ax^{-1} \\ yb = by \\ xu = wy \end{cases}$$

Это делает протокол уязвимым для атак с использованием линейной алгебры. Автор статьи [22] предложил полугруппы с большим количеством необратимых элементов. В этом случае атака, использующая линейную алгебру, неэффективна. В то же время, анализ уязвимости к другим атакам не проводился. В связи с этим пока не доказано, делает ли протокол уязвимым использование полугруппы с большим количеством необратимых элементов в качестве основы.

Заключение

Существуют новаторские идеи по предложению криптографии с открытым ключом на основе неабелевых групп, хотя большинство криптографических систем кажутся уязвимыми с точки зрения безопасности. Например, задача поиска сопряженности на линейных группах, используемых в упомянутых протоколах (матричных группах и группах кос), кажется несложной. Тем не менее, они по-прежнему имеют подтвержденную безопасность. Некоторые из этих систем имеют модификации со все еще достаточным уровнем безопасности. С другой стороны, эффективность и безопасность криптографической системы зависят не только от конструкции алгоритма, но и от выбора платформы. Продолжение исследования

неабелевых групп в качестве платформы для постквантовой криптосистемы рассматривается как перспективное.

Список литературы:

1. Shor P. Polynomial-time algorithms for prime factorization and discrete logarithm problems // SIAM Journal on Computing, vol. 26, pp. 1484-1509, 1997.
2. Magliveras S. S. A cryptosystem from logarithmic signatures of finite groups // Proceedings of the 29th Midwest Symposium on Circuits and Systems, pp. 972–975. Elsevier Publishing, Amsterdam, The Netherlands, 1986.
3. Svaba P. and T. van Trung. Public key cryptosystem MST3 cryptanalysis and realizationт // Journal of Mathematical Cryptology, vol.4, no.3, pp.271–315, 2010.
4. Magliveras S. S., Svaba P, van Trung T, et al. On the security of a realization of cryptosystem MST3 // Tatra Mt Math Publ, 2008, 41: 1–13
5 T. van Trung. Construction of strongly aperiodic logarithmic signatures // J. Math. Cryptol., vol. 12, no. 1, pp. 23-35, 2018.
6. Khalimov G., Kotukh Y., Khalimova S. MST3 cryptosystem based on the automorphism group of the hermitian function field' // IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 – Proceedings, 2019, pp. 865 – 868.
7. Khalimov G., Kotukh Y., Khalimova S. MST3 cryptosystem based on a generalized Suzuki 2 – Groups // CEUR Workshop Proceedings, 2020, 2711, pp. 1–15.
8. Khalimov G., Kotukh Y., Khalimova S. Encryption scheme based on the automorphism group of the Ree function field // 2020 7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020, 2020, 9340192.
9. Wagner N. R., Magyarik M. R. A public key cryptosystem based on the word problem // Advances in Cryptology (CRYPTO'84). Lecture Notes in Computer Science, vol. 196, pp. 19-36, 1985.
10. Yamamura A. Public-key cryptosystems using the modular group // 1st Internationa Workshop on Practice and Theory in Public Key Cryptography (PKC'98), Lecture Notes in Computer Science, vol. 1431, pp. 203-216, 1998.
11. Steinwandt R. Loopholes in two public key cryptosystems using the modular group // Lecture Notes in Computer Science, vol. 1992, pp. 180-189, 2002.
12. Rososhek S. K. New practical algebraic public-key cryptosystem and Some related algebraic and computational aspects // Applied Mathematics, vol. 4, no, 7, pp. 1043-1049, 2013.
13. Rososhek S. K. Modified matrix modular cryptosystems // Britsh Journal of Mathematics & Computer Science, vol. 5, no. 5, pp. 613-636, 2015.
14. Artin E. Theory of braids // Annal of Mathematics, vol. 48, pp. 101-126, 1947. International Journal of Network Security, Vol.20, No.2, PP.278-290, Mar. 2018 (DOI: 10.6633/IJNS.201803.20(2).09) 289.
15. Anshel I., Anshel M., Goldfeld D., Lemieux S. Key agreement, the algebraic eraserTM, and lightweight cryptography // Contemporary Mathematics, vol. 418, pp. 1-34, 2006.
16. Anshel I., Anshel M., Goldfeld D. An algebraic method for public-key cryptography // Mathematics Research Letter, vol. 6, pp. 287-291, 1999.
17. Ko K. H., Choi D. H., Cho M. S., Lee S. J. New Signature Scheme using Conjugacy Problem, 2002. (http://eprint.iacr.org/2002/168)
18. Ko K. H., Lee S. J., Cheon J. H., Han J. W., Kang J. S., Park C. New public key cryptosystem using braid groups // Advances in Cryptology (CRYPTO'00), pp. 166-184, 2000.
19. Cheon J., Jun B. A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem // Advances in Cryptography (CRYPTO'03), Lecture Notes in Computer Science, vol. 2729, pp. 212-224, 2003.
20. Stickel E. A New Public-Key. Cryptosystem in Non-Abelian Groups, 2003. (https: //www.semanticscholar.org)
21. Stickel E. A new method for exchanging secret keys // Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05), pp. 426-430, 2005.
22. Shpilrain V. Cryptanalysis of stickel's key exchange scheme // Lecture Notes in Computer Science, vol. 5010, pp. 283-288, 2008.

Поступила в редколлегию 03.02.2021

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, кафедра комп'ютерних наук, Сумський державний університет, Україна; ORCID: https://orcid.org/0000-0003-4997-620X; e-mail: yevgenkotukh@gmail.com

Сєвєрінов Олександр Васильович – канд. техн. наук, доцент, кафедра Безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Україна; ORCID: https://orcid.org/0000-0002-6327-6405; e-mail: oleksandr.sievierinov@nure.ua

Власов Андрій Володимирович – канд. техн. наук, ст. дослідник, ст. викладач, кафедра Безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Україна; ORCID: https://orcid.org/0000-0003-2599-8834; e-mail: andrii.vlasov@nure.ua

Теницька Альона Олексіївна – студентка, факультет електроніки та інформаційних технологій, Сумський державний університет, Україна; ORCID: https://orcid.org/0000-0002-2526-8842; e-mail: tenickajaalena@gmail.com

Зарудна Катерина Олександрівна – студентка, факультет електроніки та інформаційних технологій, Сумський державний університет, Україна; ORCID: https://orcid.org/0000-0002-0653-3030; e-mail: zarudnayakatyaa@gmail.com