Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет
Харківський національний економічний університет
Об'єднаний інститут проблем інформатики НАН Білорусі
Азербайджанська державна нафтова академія
Бєлгородський державний університет, Росія
Гірничо-металургійна академія AGH, Польща
Новий університет Лісабона, Португалія
Університет ЛІОН 2 ім. Люм'єра, Франція
Інститут інженерів з електротехніки та електроніки (IEEE), Українська секція

Тези доповідей Тертьої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації»

м. Вінниця, Україна
20-22 квітня 2011 року

Тезисы докладов Третьей Международной научно-практической конференции «Методы и средства кодирования, защиты и сжатия информации»

г. Винница, Украина
20-22 апреля 2011 года

ВНТУ 2011

УДК 004+681.3+621.3
М54

Відповідальний редактор В. А. Лужецький

Матеріали статей опубліковані в авторській редакції

Методи та засоби кодування, захисту й ущільнення
М54 інформації. Тези доповідей Третьої Міжнародної науково-практичної конференції. м. Вінниця, 20-22 квітня 2011 року. – Вінниця: ВНТУ, 2011. – 231 с.
ISBN 978-966-641-406-2

Збірка містить матеріали доповідей третьої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за п'ятьма основними напрямками: методи та засоби кодування інформації; методи та засоби криптографічного захисту інформації; інформаційна безпека комп'ютерних систем; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації.

УДК 004+681.3+621.3

ISBN 978-966-641-406-2

УДК 621.391

ПРО ОДНУ ТАБЛИЧНУ МОДЕЛЬ ПЕРЕТВОРЕННЯ ДАНИХ

В. А. Лужецький, д.т.н., професор[1];
О. Ю. Романенко, провідний інженер[2]
[1]Вінницький національний технічний університет
[2]Вінницьке підприємство високовольтних електричних мереж

Узагальненою моделлю перетворення даних є модель, що описується як відображення елементів множини M в елементи цієї або іншої множини. З даною моделлю пов'язане поняття функції. Існують різні форми представлення функцій: аналітична, графічна, таблична та ін.. На практиці використовують таку форму представлення функції, яка є зручнішою для розв'язання конкретної задачі. Наприклад, бінарна операція групи часто описується відповідною таблицею Келі.

Якщо поставити задачу описати k різних за змістом бінарних операцій на елементами однієї множини, то буде потрібно скласти k різних таблиць Келі й при розв'язанні конкретної задачі використовувати їх у певній послідовності. Для спрощення такої задачі автори пропонують нову табличну модель перетворення даних.

Нехай дані $\mathbf{D}$ і $\mathbf{G}$, елементами яких є числа, що належать множині цілих додатних чисел $\mathbf{A} = \{0,1,...,(m-1)\}$, представлені в вигляді кортежів $\mathbf{D} = \langle d_1 \| d_2 \| ... \| d_n \rangle$ і $\mathbf{G} = \langle g_1 \| g_2 \| ... \| g_n \rangle$. Результатом виконання певної послідовності різних бінарних операцій над $\mathbf{D}$ і $\mathbf{G}$ буде кортеж $\mathbf{C} = \langle c_1 \| c_2 \| ... \| c_n \rangle$.

Для спільного опису виконуваних операцій та одержуваних результатів складається таблиця за таким правилом. У комірку, що знаходиться на перетині стовпця з номером i ($i = 1,2,...,n$) та рядка з номером g_i, записується елемент d_i. Інші елементи i-го стовпця є елементами певної перестановки чисел множини **A**, в який елемент у позиції g_i є елементом d_i.

Наприклад, для даних $\mathbf{G} = \langle 2 \| 0 \| (m-1) \| ... \| 1 \rangle$ маємо таку таблицю:

	g_1=2	g_2=0	g_3=m-1	…	g_n=1
0	p_{10}	d_2	p_{30}	…	p_{n0}
1	p_{11}	p_{21}	p_{31}	…	d_n
2	d_1	p_{22}	p_{32}	…	p_{n2}
…	…	…	…	…	…
m-1	$p_{1(m-1)}$	$p_{2(m-1)}$	d_3	…	$p_{n(m-1)}$

Результат перетворення формується шляхом вибору за певним правилом одного елемента з кожного стовпця.

Наприклад, у разі вибору елементів тільки одного рядка з номером 1 результат перетворення має вигляд $\mathbf{C} = \langle p_{11} \| p_{21} \| p_{31} \| ... \| d_n \rangle$ або при виборі з різних рядків - $\mathbf{C} = \langle p_{10} \| p_{21} \| d_3 \| ... \| p_{n2} \rangle$.

Запропонована таблична модель може бути використана для опису нових алгоритмів шифрування з секретним ключем та хешування даних. При шифруванні даних **D** одна складова секретного ключа використовується для формування за певним правилом даних **G**, друга складова визначає правила перестановок у стовбцях, а третя – правило вибору по одному елементу з кожного стовпця при формуванні результату шифрування.