7. Madeline Gonzarlez Mun˜iz, Rainer Steinwandt: Security of signature schemes in the presence of key-dependent messages. In Tatra Mt. Math. Publ. 47 (2010), 15–29.

In the paper problems and risks for classical systems in the field of cryptographic protection of information in connection with the development of quantum computing are formulated. Problems the need to finding new solutions are grounded. The paper includes analysis of requirements of two major organizations NIST and ETSI. There are security models for cryptographic primitives offered in terms of post quantum cryptography.

Key words: *post quantum cryptography, requirements for crypto algorithms in post quantum period, NIST requirements, ETSI requirements, security models for post quantum cryptography.*

Одержано 15.02.2017

УДК 519.1:004

І. А. Ревенчук, канд. техн. наук, доцент

Харківський національний університет радіоелектроніки, м. Харків

МАТЕМАТИЧНА МОДЕЛЬ АГРЕГАЦІЇ ДАНИХ В СОЦІАЛЬНИХ МЕДІА

В роботі представлена математична модель агрегації даних соціальних мереж за допомогою узагальнення графа, що може в подальшому використовуватися в галузі інтернет маркетингу і створення необхідних пакетів даних для користувача соціальних мереж.

Ключові слова: *агрегація даних, соціальні мережі, платформи агрегації, узагальнення графу, медіа данні.*

Вступ. Акаунти у соціальних мережах мають мільйони користувачів, і кожен середній користувач має профіль у більш ніж одній з цих мереж. Деякі дані з профілю користувача соціальної мережі є конфіденційними, а деякі — відкритими. Існує величезна кількість загальнодоступних даних, які можуть бути об'єднані і використані для створення профілю користувача, а також визначення способу комунікації з ним.

Агрегація даних на основі веб-платформи включає агрегування загальнодоступних даних про людину з веб-сайтів соціальних мереж.

Інтерес представляють такі функціональні можливості: пошук, побудова профілю з агрегованими даними користувача, якого шукають;список контактів або взаємодій користувача в мережі; галузь наукових інтересів; індивідуальний маркетинг.

Аналіз методів агрегації даних, як концепція може бути розширена до формування змісту профілю користувача соціальної мережі. Відомос-

ті про профіль можуть бути інтегровані практично з усіма постачальниками соціальних мереж. Більше інтеграції дають кращі результати. Також це може бути інтегровано з пошуковою системою, яка має можливість кластеризації результатів за допомогою ключових слів на основі параметрів і інтересів користувачів соціальної мережі тощо. Дані, витягнуті з профайлів користувачів соціальної мережі можуть бути використані в пошукових системах, а також для побудови більш значущих профілів користувачів інших соціальних мереж з урахуванням характеру людини, кола знайомих, його інтересів і переваг.

Графи це потужний інструмент для моделювання даних в різних галузях. Вузли в графах, як правило, представляють собою реальні об'єкти світу і ребра вказують на відносини між об'єктами. Приклади змодельованих даних у вигляді графів включають у себе соціальні мережі, біологічні мережі тощо. Часто вузли мають атрибути пов'язані з ними.

На рис. 1, а, показано вузол, який представляє студента з атрибутами: стать і відділ. Крім того, граф може містити безліч різних типів відносин, таких як друзі і однокласники відносин, показаних на рис. 1, а.

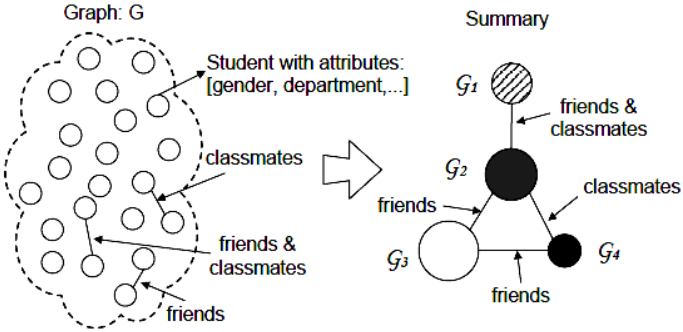

Рис. 1. *Узагальнення графа G за допомогою агрегації*

В багатьох випадках графи дуже великі, з тисячами або навіть мільйони вузлів і ребер. В результаті майже неможливо зрозуміти інформацію, закодовану в великих графах за допомогою простого візуального огляду. Таким чином, ефективні методи узагальнення графа необхідні, щоб допомогти користувачам отримати і зрозуміти основну інформацію.

Більшість існуючих методів узагальнення графа використовують прості статистичні дані для опису характеристик графа. Користувачам потрібен більш керований і інтуїтивний метод для узагальнення графів. Метод узагальнення має дозволити користувачам вільно вибирати атрибути і відносини, що представляють інтерес, а потім використовувати ці функції, щоб виробляти невеликі і інформативні резюме. Крім того, користувачі повинні мати можливість контролю-

вати дозвіл одержуваних зведень і «drill-down» (деталізація) або «roll-up» («згортання») інформації, так само як і методи агрегування OLAP в традиційних системах баз даних.

Пропонується модель узагальнення графа (МУГ) на основі угрупування вузлів на атрибутах і парних відносин, це дає короткий граф вхідного графа за допомогою угрупування вузлів на основі вибраних користувачем атрибутів вузлів і зв'язків.

На рис. 1 схематично показана ідея роботи МУГ. На рис. 1, а представлений граф про студентів (з атрибутами: gender — стать, department — відділ і т. д.) і відносини (classmates — однокласників і friends — друзів) між ними. Слід зазначити, що лише деякі з ребер показані на рис. 1, а. На основі обраних користувачем атрибутів: gender — стать і department — відділ та відносин серед classmates — однокласників і friends — друзів, операція МУГ виробляє короткий граф, показаний на рис. 1, б. Це резюме містить чотири групи студентів і відносини між цими групами. Студенти в кожній групі мають однакову стать і знаходяться в тому ж відділі, і вони ставляться до студентів, що належать одному і тому ж набору відносин груп з друзями та однокласниками. Наприклад, на рис. 1, б, кожен студент в групі G_1 має принаймні одного однокласника в групі G_2. Це компактне узагальнення розкриває основні характеристики про вузли та їх відносин у вихідному графі.

Формально позначимо граф G, як , де V є безліч вузлів, і $\Upsilon = \{E_1, E_2, ..., E_r\}$ безліч типів ребер, з кожним $E_i \subseteq V \times V$, що становить безліч ребер певного типу.

Вузли в графі є набір атрибутів, пов'язаних з ними, який позначається як $\Lambda = \{a_1, a_2, ..., a_t\}$. Кожен вузол має значення для кожного атрибута. Ці атрибути використовуються для опису особливостей об'єктів, які представляють вузли. Наприклад, на рис. 1, а, вузол, який представляє Студент може мати атрибути, які представляють стать студента і відділ.

Різні типи ребер у графі відповідають різним типам відносин між вузлами, такими як друзі та однокласник. Два вузли можуть бути з'єднані різними типами ребер, наприклад, два студенти можуть бути однокласниками і друзями одночасно.

Для простоти викладу ми позначатимемо множину вершин графа G, як $V(G)$, набір атрибутів, як $\Lambda(G)$, фактичне значення атрибута a_i. Для вузла v як $a_i.(v)$, безліч типів ребер, таких як $\Upsilon(G)$, а безліч ребер типу Ei як $Ei(G)$. Крім того, ми позначатимемо потужність множини S як $|S|$.

Операція *узагальнення графа на основі угрупування вузлів* (УГОУВ) на атрибутах і парних відносин виробляє короткий граф

через однорідне угрупування вузлів вхідного графа, заснований на обраних користувачем атрибутах вузла і зв'язках. Формально визначимо цю операцію.

Для того, щоб почати формальне визначення операції УГОУВ, спочатку визначимо поняття вузла-угрупування.

Крок 1. Вузол — угрупування графа G $\Phi = \{\varsigma_1, \varsigma_2, \ldots, \varsigma_k\}$ називається вузлом-угрупуванням G, тоді і тільки тоді, коли:

$$\forall \varsigma_i \in \Phi,\ \varsigma_i V(G) \text{ and } \varsigma_i \neq 0,\ \bigcup \varsigma_i \in \varsigma_i = V(G)$$

для $\forall \varsigma_i, \varsigma_i \in (i \neq j),\ \varsigma_i \bigcap \varsigma_j = 0$.

Інтуїтивно зрозуміло, що вузол-угрупування розділяє вузли в графі на непересічні підмножини. Кожна підмножина ς_i називається групою. Коли немає ніякої двозначності, ми просто називаємо угрупування вузлом-угрупуванням. Для цього угрупування Φ з G, група, який належить вузол v і позначається як Φ(v). Крім того, визначимо розмір угрупування, як кількість груп, які вона містить.

Далі визначаємо часткове відношення до порядку на безлічі всіх груп графа.

Крок 2. Домінування зв'язків. Для графа G, угрупування Φ домінує угрупування Φ', позначається $\Phi' \leq \Phi$ тоді і тільки тоді, коли $\forall \varsigma_i' \in \Phi', \exists \varsigma_i \in \Phi$, де $\varsigma_i' \subseteq \varsigma_i$. Легко бачити, що ставлення домінування рефлексивно, анти-симетрично і транзитивно, отже, є відношенням часткового порядку. Далі визначимо особливий вид угрупування на основі набору обраних користувачем атрибутів.

Крок 3. Атрибути сумісності угрупування.

Для набору атрибутів $A \subseteq \Lambda(G)$ угрупування Φ сумісні з атрибутами A чи просто A-сумісні, якщо він задовольняє наступним чином: $\forall u, v \in V$, якщо $\Phi(u) = \Phi(v)$ тоді $\forall a_i \in A$, $a_i(u) = a_i(v)$.

Якщо угрупування Φ сумісне з A, просто позначимо його як Φ_A. У кожній групі A-сумісного угрупування, кожен вузол має точно такі ж значення для набору атрибутів A.

Не може бути більше одного сумісного угрупування з A. Фактично тривіальне угрупування, в якій кожен вузол це група завжди сумісна з будь-яким набором атрибутів.

Крок 4. Доведемо, що серед усіх A-сумісних груп графа, існує глобальний максимум угрупування по відношенню до домінантності відносини.У безлічі всіх A-сумісних груп графа G, позначається як S_A, $\exists \Phi_A \in S_A$, $\forall \Phi_A \in S_A$, $\forall \Phi'_A \in S_A$, $\Phi'_A \leq \Phi_A$.

Припустимо, що не існує глобального максимуму A-сумісного угрупування, але більше, ніж одного максимального угрупування.

Тоді для будь-яких двох таких максимальних угрупувань Φ_1 і Φ_2, побудуємо нове A-сумісне угрупування Φ_3 таким чином, що $\Phi_1 \le \Phi_3$ і $\Phi_2 \le \Phi_3$, що суперечить припущенню, що суперечить припущенню, що Φ_1 і Φ_2 є максимальним сумісним угрупуванням.

Припустимо: $\Phi_1 = \{\varsigma_1^1, \varsigma_2^1, ..., \varsigma_s^1\}$ і $\Phi_2 = \{\varsigma_1^2, \varsigma_2^2, \ldots, \varsigma_t^2\}$.

Побудуємо двочастковий граф $\Phi_1 \bigcup \Phi_2$, як показано на рис. 2.

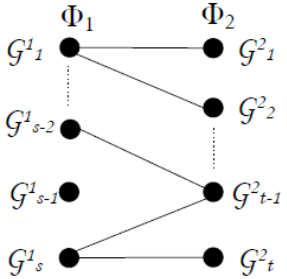

Рис. 2. *Двочастковий граф Ф3*

Вузли в двочастковому графі є групи Φ_1 і Φ_2. І є ребро між $\varsigma_i^1 \in \Phi_1$ і $\varsigma_j^2 \in \Phi_2$ тоді і тільки тоді, коли $\varsigma_i^1 \bigcap \varsigma_j^2 \neq 0$. Після побудови двочасткового графу, розкладаємо цей граф на компоненти зв'язності C_1, C_2, ..., C_m.

Для кожного підключеного компонента C_k, ми об'єднаємо групи всередині цього компонента $\bigcup(C_k)$. Тепер ми можемо побудувати нове угрупування $\Phi_3 = \{\bigcup(C_1), \bigcup(C_2), \ldots., \bigcup(C_m)\}$. Легко бачити, що $\Phi_1 \le \Phi_3$ і $\Phi_2 \le \Phi_3$.

Φ_3 сумісний з A. З визначення A-сумісних угрупувань, якщо $\varsigma_i^1 \bigcap \varsigma_j^2 \neq 0$ вузли в $\varsigma_i^1 \bigcup \varsigma_j^2$ всі мають однакові значення атрибутів.

Таким чином, існує глобальний максимум A-сумісного угрупування.

Позначимо цей глобальний максимум A-сумісне угрупування $\Phi_A^{\max}$, що також A-сумісне угрупування з мінімальною кількістю елементів. Насправді, якщо розглядати кожен вузол в графі як запис даних, а потім $\Phi_A^{\max}$ дуже схожий в результаті з групової операцією для цих записів даних на атрибути, які є в системах реляційних баз даних.

A-сумісні угрупування облікового запису є тільки для атрибутів вузла. Проте, вузли не тільки атрибути, а й беруть участь у парних відносинах, представлених ребрами. Далі розглянемо відносини за угрупуванням вузлів.

Для угрупування Ф позначимо сусіда-групи вузла v в E_i як *NeighborGroups* Ф, $E_i(v) = \{ \Phi(u) | (u,v) \in E_i \}$.

Визначимо угрупування, сумісні з обома атрибутами вузла і відносин.

Крок 5. Атрибути і відносини сумісність угрупування. Для набору атрибутів $A \subseteq \Lambda(G)$ і набір типів відносин $R \subseteq \Upsilon(G)$, угрупування Ф сумісний з атрибутами A і відносини типів R або просто (A, R) сумісний, якщо він задовольняє: Ф – A-сумісний,

$$\forall\, u, v \in V(G), \text{ якщо } \Phi(u) = \Phi(v), \text{ потім } \forall E_i \in R,$$

$$\textit{NeighborGroups}\ \Phi, E_i(u) = \textit{NeighborGroups}\ \Phi, E_i(v).$$

Якщо угрупування Ф сумісне з A і R, також будемо позначати його як $\Phi_{(A, R)}$. У кожній групі (A, R) групування сумісне, всі вузли є однорідними з точки зору як атрибути A і відносини в R. Іншими словами, кожен вузол всередині групи має точно такі ж значення для атрибутів A, і знаходиться поруч з вузлами в тому ж наборі груп для всіх відносин в R.

Як приклад, припустимо, що рис. 1, б це угрупування сумісний з атрибутами стать і відділ, і відносини однокласник і друг. Потім, наприклад, кожен студент (вузол) в групі ς_2, має ту ж саму стать і відділ значень атрибутів, і є одним деяким студентом(ами) в ς_3, однокласник деякого студента(ів) в ς_4, і один до деякого студента(ів), а також однокласником до деякий студент(и) в ς_1.

З огляду на угрупування $\Phi_{(A, R)}$, можна зробити висновок, відносини між групами з відносин між вузлами в R. Для кожного типу ребра $E_i \in R$, визначимо відповідну групу відносин як

$$E_i(G, \Phi_{(A, R)}) = \{(\varsigma_i, \varsigma_j) | \varsigma_i, \varsigma_i \in \Phi_{(A, R)} \text{ і } \exists\, u \in \varsigma_i,\ v \in \varsigma_j \ s.t.\ (u, v) \in E_i\}.$$

Насправді, за визначенням з (A, R), сумісними з угрупуваннями, якщо є один вузол група примикає до деякого вузла(ів) в іншій групі, а потім кожен вузол в першій групі примикає до деякого вузла(ів) в другій.

Аналогічно атрибути сумісних груп, не може бути більше одного угрупування сумісного з заданими атрибутами і відносинами. Угрупування, в якому кожен вузол утворює групу завжди сумісні з будь-якими заданими атрибутами і відносинами.

Крок 6. Серед всіх (A, R) сумісними з угрупуваннями існує глобальний максимум угрупування щодо домінантності відносини.

У безлічі всіх (A, R) сумісних угрупувань графа G, позначається

$$S_{(A,R)}, \exists \Phi_{(A,R)} \in S_{(A,R)}, \forall \Phi'_{(A,R)} \in S_{(A,R)}, \Phi'_{(A,R)} \le \Phi_{(A,R)}.$$

Отже операція УГОУВ приймає як вхідний даний граф G, набір атрибутів $A \subseteq \Lambda(G)$, і набір ребер $R \subseteq \Upsilon(G)$ і отримується сумарний узагальнюючий граф G_{total}, де:

$$V\left(G_{total}\right) = \Phi^{\max}_{(A,R)} \text{ і } \Upsilon\left(G_{total}\right) = \{E_i(G, \Phi^{\max}_{(A,R)}) \mid E_i \in R\}.$$

Таким чином, зрозуміло, що операція УГОУВ виробляє узагальнений граф вхідного графа на основі вибраних користувачем атрибу-

тів і зв'язків. Вузли цього короткого графа відповідають групам в максимумі (A, R), сумісні з угрупуваннями. А ребра цього короткого графа є групові відносини виведені з вузла відносин в R.

Висновки. Представлена операція агрегації УГОУВ заснована на угрупування графа. Цей метод дозволяє користувачам вільно вибирати атрибути вузлів і відносини, які становлять інтерес, і виробляють угрупування на основі певних функцій.

В рамках майбутньої роботи можна запропонувати організувати розробку формальної моделі графа даних і мови запитів, що дозволяє включення до УГОУВ, поряд з цілим рядом інших додаткових поширених і корисних методів графа відповідності.

Список використаних джерел:

1. Newman M. E. J. [Text]. The structure and function of complex networks. SIAM Review. 2003. P.167–256.
2. Leskovec J., Faloutsos C. [Text]. Sampling from large graphs. Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2006. C. 631–636.
3. Koby Crammer, OferDekel, Joseph Keshet, Shai Shalev-Shwartz, Yoram Singer. [Text]. Online Passive-Aggressive Algorithms. JMLR, 7(Mar): P. 551–585. 2006.

The mathematical model of data aggregation via social networks generalization graph was presented, that can be used in the field of internet marketing and create the necessary packet data for users of social networks.

Key words: *data aggregation, social network platform aggregation, generalization graph, media data.*

Одержано 16.02.2017

УДК 621.3.06

М. Ю. Родінко, аспірантка

ПАТ «Інститут інформаційних технологій», м. Харків

МАЛОРЕСУРСНИЙ СИМЕТРИЧНИЙ БЛОКОВИЙ ШИФР «КИПАРИС» — СУТНІСТЬ ТА ОСНОВНІ ВЛАСТИВОСТІ

Наведений опис та результати аналізу основних властивостей перспективного малоресурсного симетричного блокового шифру «Кипарис».

Ключові слова: *симетричний блоковий шифр, малоресурсна криптографія, мережа Фейстеля.*

Вступ. У зв’язку із поширенням Інтернету речей, до криптографічних алгоритмів, у тому числі й симетричних, висуваються нові вимоги. Такі блокові шифри, як «Калина» (ДСТУ 7624-2014 [1]), AES