STUDIA INFORMATICA 2000
Volume 21 Number 1 (39)

Adam KAPRALSKI
Politechnika Śląska, Instytut Informatyki

NIEMONOTONICZNE MODELE RANKINGOWE

Streszczenie. W pracy przedstawiono metodę budowania silnie nieokreślonych modeli rankingowych dla reprezentowania obiektów kombinatorycznych dowolnego typu. Nieokreśloność modeli uzyskiwana jest poprzez wykładniczo zależną liczbę takich modeli od n i m charakteryzujących rozmiar modeli maksymalnych, tzn. reprezentujących maksymalną liczność zbioru tych obiektów dla danego typu. Ponadto ważnym czynnikiem nieokreśloności modeli jest silna niemonotoniczność rankingu, tzn. porządku generacyjnego poszczególnych obiektów kombinatorycznych reprezentowanego zbioru. Metoda wykorzystuje reprezentacje arbitralnych zbiorów obiektów kombinatorycznych poprzez funkcje wyboru rodzin indeksowych. Stosowane są modele rankingowe tego systemu. Przedstawiono hierarchiczną strukturę modelu rankingowego zapewniającą maksymalną entropię odwzorowania: liczba całkowita (rank) – obiekt kombinatoryczny. Możliwe zastosowania przedstawionej metodologii do kryptografii i dla zapewnienia bezpieczeństwa systemów informatycznych są bardzo szerokie.

NON-MONOTONIC RANKING MODELS

Summary. The paper presents ranking models representing arbitrary sets of combinatorial objects with high entropy of the one-to one mapping that maps a combinatorial object into its rank. The sets of combinatorial objects are represented by the choice functions of indexed families. The number of potential models depends exponentially on fixed n and m characterizing the size of a model. Moreover, the structure of an applied ranking model is hierarchical with unrelieved number of levels. Furthermore, the mapping input ranks into output combinatorial objects is strongly nonmonotonic. The system is strongly resistant against any cryptographic attack. That makes is very suitable tool for any application including cryptography and designing safe data systems.

1. Przedstawienie problemu

Jednym z istotnych zagadnień kryptograficznych jest szyfrowanie i deszyfrowanie struktur reprezentowanych poprzez obiekty kombinatoryczne, takie jak: permutacje, kombinacje, wariacje, podziały, dekompozycje oraz kompozycje. Struktury takie w systemach informatycznych mogą mieć rozmaite przeznaczenie związane z zapewnieniem bezpieczeństwa tych systemów. Istota zastosowań polega na możliwości wykorzystywania licznego zbioru struktur jako kluczy, elektronicznych podpisów itp., tak aby każdy element tego zbioru mógł być wykorzystany najwyżej jednorazowo. Jednorazowe użycie jest warunkiem bądź podstawowego i poprawnego funkcjonowania systemu jak w przypadku elektronicznego podpisu, bądź też jest czynnikiem istotnie zwiększającym odporność systemu na różnego rodzaju ataki, jak w przypadku prywatnego klucza szyfrująco-deszyfrującego. Ograniczenie każdej możliwej struktury do jednorazowego użycia nakłada dość silne wymagania pod adresem systemu produkującego i wykorzystującego takie metody zabezpieczenia. Po pierwsze, zbiór takich możliwych do wyprodukowania struktur musi być bardzo liczny, ale równocześnie musi być zanurzony w jeszcze znacznie większym potencjalnie zbiorze takich struktur. Już sam ten warunek nakłada silne wymagania pod adresem systemu komputerowego implementującego takie rozwiązania, gdyż konieczne jest sensowne znalezienie obiektu należącego do zadanego zbioru oraz sprawdzenie, czy dany obiekt do takiego zbioru należy. Ponadto każdy obiekt należący do zbioru musi być reprezentowany w sposób niejawny, tak aby przechwycenie reprezantacji jakiegoś obiektu nie powodowało jego odtajnienia ani tym bardziej nie powodowało odtajnienia całego systemu. Mówiąc bardziej formalnie, podstawowym wymaganiem pod adresem modelu reprezentującego żądany zbiór obiektów kombinatorycznych jest możliwie największa entropia modelu mierząca nieokreśloność przynależności dowolnego obiektu kombinatorycznego do właściwego zbioru tych obiektów. Gdy znajomość przynależności elementu do modelowanego zbioru nie jest wystarczającym zabezpieczeniem, wtedy możemy dodatkowo zdefiniować liniowy porządek na zbiorze modelowanych obiektów i wymagać, aby autoryzacja dostępu lub możliwość wykorzystania systemu wymagała znajomości tego porządku przynajmniej częściowo, tzn. znany jest następnik lub poprzednik danego obiektu kombinatorycznego. Obiekty kombinatoryczne żądanego zbioru są reprezentowane poprzez ich kody niejawne, wtedy autoryzowany użytkownik systemu musi znać szyfr nie tylko obiektu kombinatorycznego należącego zbioru, ale także musi znać szyfr obiektu kombinatorycznego, który w tym zdefiniowanym porządku liniowym zajmuje określone miejsce. Inaczej mówiąc, zadanie polega na możliwie największej nieokreśloności miejsca obiektu kombinatorycznego we wspomnianym porządku, w którym to

obiekt kombinatoryczny jest reprezentowany poprzez jego szyfr. Przyjmijmy założenie upraszczające, że szyfrem dla obiektu kombinatorycznego jest liczba - miejsce obiektu kombinatorycznego w tym porządku. Wtedy znajomość tego szyfru oznacza możliwość wygenerowania zbioru obiektów kombinatorycznych wspomnianego zbioru i odtworzenie ich uporządkowania. Podstawowym porządkiem liniowym obiektów kombinatorycznych jest porządek leksykograficzny. Porządek faktyczny musi być możliwie najbardziej nieokreślony, a zatem musi być możliwie najbardziej różniący się od porządku leksykograficznego. Dla spełnienia tego żądania musimy zapewnić silną niemonotoniczność faktycznie używanego odwzorowania w stosunku do porządku leksykograficznego. Praca poświęcona jest przedstawieniu metody budowy modeli arbitralnych zbiorów obiektów kombinatorycznych oraz sposobów modelowania porządku liniowego dla tych zbiorów obiektów. Porządek liniowy oraz miejsce konkretnego obiektu kombinatorycznego w tym porządku nosi nazwę "ranku" lub "rankingu", zatem zadanie sprowadza się do sposobu budowania i reprezentowania silnie niemonotonicznych i nieokreślonych modeli rankingowych obiektów kombinatorycznych. Przedstawione rozważania są oparte na pracach autora w obszarze generacji i reprezentowania obiektów kombinatorycznych [1], [2], [3].

2. Rozwiązanie tablicowe

Najbardziej oczywistym modelem dla realizacji takiego systemu wybierania i przesyłania niejawnych obiektów kombinatorycznych jest tablica z wydzielonymi polami na jawną reprezentację obiektu kombinatorycznego oraz na jego szyfr. Tablica taka pełni funkcję klucza niejawnego, tzn. tylko użytkownicy upoważnieni do poprawnego odczytania zaszyfrowanej struktury mogą być w jej posiadaniu. Z powodów, o których wspomniano poprzednio, rozmiary takiej tablicy muszą być bardzo duże. Poza tym, stosowanie takiej tablicy w architekturach tradycyjnych wymaga czasu $O(\log(n))$ dla procesu deszyfrowania. Czas szyfrowania również może być $O(\log(n))$, ale tylko w przypadku, gdy posiadamy dodatkową kopię tablicy szyfrów uporządkowaną liniowo względem obiektów kombinatorycznych, w przeciwnym przypadku czas szyfrowania jest $O(n)$. Ogranicza to w istotny sposób możliwość zastosowania tablicy jako podstawowego modelu szyfrowania, deszyfrowania oraz wykorzystania systemu reprezentowania potrzebnych obiektów kombinatorycznych.

3. Proste rozwiązanie rankingowe

Dużą złożoność pamięciową rozwiązania tablicowego przedstawionego powyżej można usunąć, przyjmując tak zwaną rankingową metodę generowania obiektów kombinatorycznych, która może być przedstawiona jak następuje. Klasyczna teoria generowania obiektów kombinatorycznych wprowadza porządek generowania obiektów kombinatorycznych określonego typu. Poprzez typ rozumiemy tutaj określenie pełnego zbioru wyszczególnianych obiektów oraz liczb charakteryzujących te obiekty, np. możemy określić typ jako zbiór wszystkich kombinacji siedmioelementowych ze zbioru dwudziestoelementowego. Jako porządek generowania wszystkich obiektów używany jest porządek leksykograficzny lub znacznie rzadziej porządek antyleksykograficzny. Używane bywają także inne porządki, jednakże są one "łamanymi" porządkami leksykograficznymi, tzn. w dużej liczbie przypadków następnik jest następnikiem w sensie leksykograficznym lub antyleksykograficznym, chociaż dla pewnego podzbioru możliwych przypadków faktyczny następnik nie ma związku z porządkiem leksykograficznym.

Funkcja RANK przyporządkowuje liczbę naturalną do każdego obiektu kombinatorycznego danego typu, zgodną z jego miejscem w tym założonym porządku generacyjnym. Istnieją także algorytmy generacyjne produkujące na wyjściu obiekt kombinatoryczny danego typu, którego wartość ranku jest zadana jako wejście.

Podstawową wadą takiego podejścia jest niska odporność przedstawionego sposobu szyfrowania na brutalny atak, czyniąca taką metodę szyfrowania nieużyteczną w rozwiązaniach praktycznych. Dodatkową wadą klasycznego sposobu generowania obiektów kombinatorycznych poprzez ranking jest duża złożoność czasowa algorytmów produkujących obiekt kombinatoryczny dla danego rankingu. Należy podkreślić, że stosowanie dodatkowego odwzorowania izomorficznego, pozwalającego ukryć faktycznie używany rank na wejściu odpowiedniego algorytmu generacyjnego, nie rozwiązuje bądź problemu dużej złożoności modelu, bądź nie zwiększa wystarczająco odporności metody na brutalny atak. Wyjaśnienie tego faktu jest następujące: Stosowanie jakiegokolwiek odwzorowania izomorficznego definiowanego w postaci wyrażenia algebraicznego nie zwiększa w istotny sposób entropii faktycznego wejścia do algorytmu generacyjnego. Natomiast wykorzystanie tablicy dla zdefiniowania tego odwzorowania nie rozwiązuje problemu dużej złożoności pamięciowej przyjętej metody szyfrowania obiektów kombinatorycznych.

4. Metoda reprezentowania i generowania obiektów poprzez funkcje wyboru rodzin indeksowych

Dowolny typ obiektów kombinatorycznych może być reprezentowany jako funkcja wyboru rodziny indeksowej [1], [2]. Przy czym typ obiektów kombinatorycznych reprezentowanych poprzez zbiory funkcji wyboru jest znacznie szerszy, niż to przyjmuje się w modelu klasycznym. Nierankingowy model reprezentacyjny jest zdefiniowany następująco: $S_U = \langle\langle G_i\rangle, 1 \leq i \leq m, W, \{h\}_{G_i}\rangle$, gdzie $G_i \subseteq U$, U jest dowolnym zbiorem nazywanym uniwersum $|U| = n$, W jest warunkiem, jaki ma spełniać każda funkcja wyboru, $\{h\}_{G_i}$ jest zbiorem funkcji wyboru dla tego modelu. Dla ustalonych n, m oraz W liczba możliwych rodzin indeksowych $\langle G_i\rangle$, $1 \leq i \leq m$, a co za tym idzie liczba zbiorów $\{h\}_{G_i}$ jest określona zależnością wykładniczą. Zakłada się, że model posiada własność Q pozwalającą na generowanie funkcji wyboru w oparciu o algorytmy bez nawrotów. Dla zadanego modelu reprezentacyjnego dany jest generacyjny model nierankingowy zawierajacy procedury FIRST, NEXT, LAST pozwalający generować w porządku leksykograficznym wszystkie funkcje wyboru stosując algorytmy bez nawrotów. Przy czym algorytm FIRST generuje pierwszą w porządku leksykograficznym funkcję wyboru $h \in \{h\}_{G_i}$. Algorytm NEXT bierze jako wejście dowolną funkcję $h \in \{h\}_{G_i}$ i generuje jej leksykograficzny następnik. Natomiast algorytm LAST generuje ostatnią w tym porządku funkcję lub informuje, że dana funkcja jest funkcją ostatnią.

5. Podstawowe modele rankingowe

Jeżeli zbiór funkcji wyboru $\{h\}_{G_i}$ dla danego modelu nierankingowego jest zbiorem symetrycznym [1], wtedy struktura tego zbioru może być reprezentowana poprzez tablicę D. Algorytmy budowania tablicy D zależą od ogólnych własności podanego modelu rankingowego i zostały przedstawione w [1]. Uzyskana tablica D jest podstawowym komponentem rankingowego modelu reprezentacyjnego. Reprezentacyjny model rankingowy jest zdefiniowany następująco: $S_R = \langle S_U, D, <^h, R(h)\rangle$, gdzie $<^h$ oznacza przyjęty porządek funkcji wyboru, $R(h)$ oznacza rank funkcji h w porządku $<^h$. W oparciu o rankingowy model reprezentacyjny zbudowany jest model generacyjny, którego podstawowym komponentem są algorytmy należące do podsystemu <METHODS>. W generacyjnym modelu rankingowym najważniejszą funkcję spełniają ogólne algorytmy UNRANK i RANK, które są wykorzystywane dla realizacji rankingowej generacji obiektów kombinatorycznych. Algorytm

UNRANK bierze jako wejście liczbę z przedziału $[1, |\{h\}_{G_i}|]$, a zwraca jako wyjście odpowiadającą funkcję wyboru $h \in \{h\}_{G_i}$. Algorytm RANK przeprowadza operację odwrotną, tzn. wejściem jest funkcja wyboru $h \in \{h\}_{G_i}$, natomiast wyjściem jest rank tej funkcji obliczony dla danego modelu. Pozostałe algorytmy rankingowego modelu generacyjnego nie mają dla przeprowadzanych rozważań znaczenia. Istota wykorzystania tej klasy modeli bazuje na następujących ich własnościach:

- dla ustalonej wartości n i m liczba modeli rośnie wykładniczo,
- znajomość funkcji wyboru h oraz odpowiadającego jej rankingu nie pozwala na łatwą identyfikację używanego modelu.

6. Modelowanie rodzin indeksowych dla maksymalizacji entropii $R(h)$

Dla ustalonych wartości n i m oraz dla danego warunku W definiujemy maksymalną rodzinę indeksową jak następuje. Niech $G_i=\{1, 2, ..., n\}$ dla każdego $i \in \{1, 2, ..., m\}$. W oparciu o rodzinę indeksową $<G_i>$, $1 \leq i \leq m$, budujemy reprezentacyjny model nierankingowy $S_U = <<G_i>, 1 \leq i \leq m, W, \{h\}_{G_i}>$. Wtedy maksymalną rodziną indeksową nazywamy rodzinę indeksową $<G_i^{\max}>$, $1 \leq i \leq m$, gdzie $G_i^{\max} \subseteq G_i$, $1 \leq i \leq m$, i taką, że odpowiadający model nierankingowy $S_U^{\max} = <<G_i^{\max}>, 1 \leq i \leq m, W, \{h\}_{G_i}^{\max}>$ jest modelem nienadmiarowym i spełniającym własność Q. Wtedy zachodzi $\{h\}_{G_i} = \{h\}_{G_i}^{\max}$, a zbiór $\{h\}_{G_i}^{\max}$ nazywamy pełnym zbiorem funkcji wyboru. Dla każdej rodziny indeksowej $<G_i'>$, $1 \leq i \leq m$, takiej, że $G_i' \subseteq G_i^{\max}$, budując odpowiadający model S_U' mamy $\{h\}_{G_i}' \subseteq \{h\}_{G_i}$. Przyjmujemy odpowiadające modele rankingowe $S_R^{\max} = <S_U^{\max}, D, <_{\max}^h, R^{\max}(h)>$ oraz $S_R' = <S_U', D', <^h, R'(h)>$. Porządek $<_{\max}^h$ jest porządkiem leksykograficznym.

Pierwszą żądaną własnością modelu S_U' dla jego przydatności dla szyfrowania obiektów kombinatorycznych jest możliwie największa entropia $R(h)$. Miarami entropii $R(h)$ są entropie bezwzględnej odległości ranków oraz entropie względnej odległości ranków.

Entropia względnej odległości ranków jest definiowana następująco:

Niech $R^{\max}(h)$ oznacza ranking funkcji wyboru w modelu $S_U^{\max}$, natomiast $R'(h)$ oznacza ranking funkcji wyboru modelu S_U'. Niech $h_1, h_2 \in \{h\}_{G_i}^{\max}$, natomiast $h_1', h_2' \in \{h\}_{G_i}'$. Ponadto $R^{\max}(h_2) = R^{\max}(h_1) + 1$, natomiast $R'(h_2') = R'(h_1') + 1$.

Względną odległością rankingów $R'(h_2')$ oraz $R'(h_1')$ nazywamy następujące wyrażenie: $\Delta_{|R'|}=|R^{max}(h_2')-R^{max}(h_1')|$, tzn. jest to różnica ranków funkcji h_1' i h_2' w modelu S_U'. Entropia $\Delta_{|R'|}$ jest oznaczana poprzez $E(\Delta_{|R'|})$.

Bezwzględna odległość rankingów $\Delta_{R'}=R^{max}(h_2')-R^{max}(h_1')$ jest liczbą całkowitą dodatnią lub ujemną. Odpowiednio entropia $\Delta_{R'}$ jest oznaczana jako $E(\Delta_{R'})$.

Rozważmy własności rodziny indeksowej $<G_i'>$, $1\leq i\leq m$ dla maksymalizacji $E(\Delta_{|R'|})$. Maksymalizacja $E(\Delta_{|R'|})$ jest warunkowana maksymalizacją entropii rodziny indeksowej $<G_i'>$, $1\leq i\leq m$. Wymaga to takiego ukształtowania rodziny indeksowej, aby zapewnić spełnienie warunku $\sum_{i=1}^{m}|G_i'|\cong\frac{1}{2}\sum_{i=1}^{m}|G_i^{max}|$. Ponadto musimy mieć $|G_i'|\geq|G_{i+1}'|$, a dla $k\cong m/2$ musimy zapewnić $|G_{m-j}'|<<n$, $j=1, 2, ..., k$.

Maksymalizację $E(\Delta_{R'})$ można uzyskać poprzez odpowiednie ukształtowanie relacji $<^h$ liniowo porządkującej zbiór $\{h\}_{G_i}'$. Relacja $<^h$ wyznaczona jest poprzez liniowy porządek zbiorów indeksowych oraz poprzez liniowe uporządkowanie elementów każdego zbioru G_i' W przypadku używania porządku leksykograficznego porządek elementów G_i' jest porządkiem naturalnym wynikającym z uporządkowania liniowego elementów uniwersum U. Natomiast dla modelowanej relacji $<^h$ porządek elementów każdego zbioru G_i' jest budowany indywidualnie, np elementy zbioru $G_i'=\{1, 2, 5, 7\}$ mogą zostać uporządkowane <2, 5, 1, 7> lub w każdy inny sposób.

Przykład

Dana jest rodzina indeksowa $G_1'=\{1, 2, 5, 6\}$, $G_2'=\{3, 7\}$, $G_3'=\{8\}$, wskazać relację $<^h$ porządkującą odmienną od naturalnego porządku leksykograficznego zbiór rosnących funkcji wyboru $\{h\}_{G_i}'$

Rozwiązanie

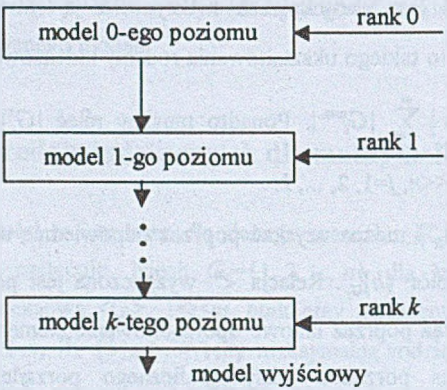
Naturalny porządek rosnących funkcji wyboru jest następujący:

<1, 3, 8>; <1, 7, 8>; <2, 3, 8>; <2, 7, 8>; <5, 7, 8>; <6, 7, 8>, gdzie <1, 3, 8> reprezentuje funkcję $h(1)=1$; $h(2)=3$; $h(3)=8$.

Dla modelowania relacji $<^h$ przyjmujemy uporządkowanie zbiorów indeksowanych jak następuje: $G_1'=$ <5, 1, 6, 2>; $G_2'=$<7, 3>; $G_3'=$<8>. Przedstawiona relacja $<^h$ porządkuje następująco zbiór funkcji wyboru <5, 7, 8>; <1, 7, 8>; <1, 3, 8>, <6, 7, 8>; <6, 3, 7>; <2, 7, 8>; <2, 3, 8>.

Zauważmy, że w porządku leksykograficznym funkcja h_2: $h_2(1)=1$, $h_2(2)=7$, $h_2(3)=8$ poprzedza funkcję h_1: $h_1(1)=5$, $h_1(2)=7$, $h_1(3)=8$, natomiast dla skonstruowanej relacji $\prec'$ sytuacja jest odwrotna. Mamy także $R'(h_2)=2$; $R'(h_1)=1$.

7. Modele hierarchiczne



Rys. 1. Hierarchiczne modele rankingowe
Fig. 1. Hierarchical ranking models

Celem dalszego zwiększenia entropii używanego modelu rankingowego jest hierarchia niejawnych modeli rankingowych. Hierarchię niejawnych modeli rankingowych przedstawia rys. 1. Każdy k-ty model rankingowy bierze jako wejście k-ty rank oraz obiekt kombinatoryczny będący wyjściem z modelu $k-1$ oraz buduje na tej podstawie model k-ty. Wyjściem z modelu k-tego jest żądany obiekt kombinatoryczny. Dla $k=2$ entropia modelu 2-giego poziomu jest zwykle wystarczająco duża, aby proces tworzenia modeli wyższego poziomu uznać za niecelowy.

Typ funkcji wyboru dla ostatniego poziomu omawianej hierarchii wynika z zapotrzebowania. Natomiast dla poziomów poprzedzających najkorzystniejszy jest model zapewniający możliwie największą liczbę funkcji wyboru przy ustalonej strukturze rodziny indeksowej. Dlatego najlepszym rozwiązaniem dla modeli pośrednich jest zastosowanie bijekcji wyboru.

8. Struktura danych

Podstawową strukturą danych wejściowych dla budowy k-tego modelu rankingowego jest tablica $A[n \times m]$, której elementy są zmiennymi boolowskimi. Elementy tablicy A stanowią dane wejściowe dla budowy rodziny indeksowej $<G_i^k>$, $1 \leq i \leq m$, dla każdego poziomu modelu rankingowego z wyjątkiem poziomu zerowego. Tablica ta jest zatem podstawowym kluczem prywatnym i jest podzielona na dwie podtablice $A_1[n \times m_1]$ oraz $A_2[n \times m_2]$, gdzie $m_1+m_2=m$. Im większe n oraz m, tym większa entropia k-tego modelu rankingowego. Tablica A_1 powinna mieć liczbę elementów równych TRUE w przybliżeniu równą liczbie elementów równych FALSE, natomiast liczba elementów tablicy A_2 powinna być znacznie mniejsza w granicach pomiędzy m_1 a $d \cdot m_1$, gdzie d=1 lub d=2, lub d=3. Każda kolumna i każdy z wierszy tablicy A powinny mieć co najmniej jeden element równy TRUE.

Drugą strukturą wejściową jest lista porządków PA elementów każdej kolumny tablicy A, może być ona zadana jako lista m- rekordów, gdzie każdy i-ty rekord zawiera uporządkowaną listę elementów i-tej kolumny.

Kolejnym elementem struktury danych są dwa modele rankingowe zerowego poziomu $S_R^{0w}=<<G_i^0, 1 \leq i \leq m_1, W, \{h^{0w}\}_{G_i}^0>, <^{h^{0w}}, D^{0w}, R(h^{0w})>$ oraz $S_R^{0w}=<<G_i^0, m_1+1 \leq i \leq m_1, W, \{h^{0n}\}_{G_i}^0>, <^{h^{0n}}, D^{0n}, R(h^{0n})>$, gdzie wszystkie elementy tych modeli z wyjątkiem zbiorów $\{h^{0w}\}_{G_i}^0$ i $\{h^{0n}\}_{G_i}^0$, które są niejawne, lecz mogą być wygenerowane, są dodatkowymi elementami klucza prywatnego. Model S_R^{0w} jest wykorzystywany do produkcji wartości funkcji $h^0(i)$ dla $i \in \{1, 2, ..., m_1\}$, natomiast model S_R^{0n} jest wykorzystywany do produkcji wartości funkcji $h^0(i)$ dla $i \in \{m_1+1, ..., m\}$.

Rank 0 jest szyfrem pozwalającym utworzyć model 1-szego poziomu. Ponieważ dla danej rodziny indeksowej liczba bijekcji jest największa, wobec tego warunek W powinien reprezentować bijekcje. Funkcja wyboru produkowana jako wyjście 0-go poziomu jest reprezentowana w tablicy jednowymiarowej IA^0, kolejne elementy tej tablicy $IA^0[i]$, $1 \leq i \leq m$, reprezentują wartości funkcji $h^0(i)$.

9. Budowa j-tego modelu rankingowego

Jak wspomniano poprzednio, tablica IA^j, $0 \leq j \leq k$-1 reprezentuje bijekcję dla dziedziny $\{1, 2, ..., m\}$ i przeciwdziedziny $\{1, 2, ..., n\}$, $n>m$. Transformuje ona kolumnowo tablicę

A^{j-1} do tablicy A^j w ten sposób, że każda i-ta kolumna tablicy A^{j-1} staje się kolumną i-tą tablicy A^j. Tablica A^j jest wykorzystywana do utworzenia rodziny indeksowej $<G_i^j>$, $1 \leq i \leq m$, w ten sposób, że każda i-ta kolumna tablicy A^j odpowiada zbiorowi indeksowemu G_i^j. Jeżeli $A^j[q, i]$=TRUE, to element q należy do G_i^j, gdy $A^j[q, i]$=FALSE, wtedy element $q \notin G_i^j$. Rodzina indeksowa $<G_i^j>$, $1 \leq i \leq m$, utworzona według przedstawionego sposobu, musi zostać zredukowana oraz należy zapewnić spełnialność własności Q stosując w tym celu metodę redukcji oraz zapewniania spełnialności tej własności przedstawioną w [2]. Kolejnym elementem tworzenia modelu jest budowa tablicy D^j w oparciu o metodologię przedstawioną w cytowanej pracy. Relacja częściowego porządku $<^{h^j}$ jest budowana na podstawie listy PA z uwzględnieniem elementów faktycznie należących do każdego zbioru indeksowego G_i^j rodziny $<G_i^j>$, $1 \leq i \leq m$. Utworzenie modelu rankingowego S_R^j i podanie ranku j pozwala wygenerować funkcje wyboru tego poziomu w oparciu o procedurę RANK reprezentowaną poprzez tablicę IA^{j+1}. Tablica IA^k utworzona w ostatnim kroku reprezentuje żądany obiekt kombinatoryczny.

10. Ocena odporności na ataki

Jakikolwiek atak przeprowadzany celem odtajnienia przedstawionego tutaj modelu hierarchicznego wymaga znajomości szyfrów i odpowiadających im obiektów kombinatorycznych k-tego poziomu. Z natury swojej zbiory obiektów kombinatorycznych reprezentowanych poprzez funkcję wyboru niepełnych rodzin indeksowych są bardzo liczne, wobec tego odporność na brutalny atak zależna jest od wielkości liczb n i m, które praktycznie nie są ograniczone. Monotoniczność modelu rankingowego mogłaby umożliwiać atak pełzający polegający na ograniczaniu podzbiorów obiektów kombinatorycznych reprezentowanych poprzez większe oraz mniejsze ranki od ranków znanych i odpowiadających znanym obiektom kombinatorycznym. Niemonotoniczność modelu rankingowego czyni takie działania bardzo trudnymi do przeprowadzenia, przy czym trudność jest tym większa, im większa jest entropia $E(\Delta_{R'})$. W oczywisty sposób zwiększenie liczby poziomów hierarchicznego modelu rankingowego zwiększa entropie $E(\Delta_{R'})$ oraz $E(\Delta_{|R'|})$. Liczba przesyłanych ranków może być dowolna z przedziału [1, k], wtedy jedna lub więcej liczb przesłanych może być traktowana jako rank jednego lub kilku poziomów. Oznacza to możliwość utajnienia podstawowej struktury, a nie tylko parametrów stosowanego hierar-

chicznego modelu rankingowego. Należy podkreślić, że algorytmy obliczania parametrów poszczególnych modeli oraz obliczania produkowanych obiektów kombinatorycznych mają złożoność asymptotyczną co najwyżej $O(n.m)$ przy niewielkiej złożoności czasowej, zatem proponowany sposób budowy niemonotonicznych modeli rankingowych jest w pełni przydatny dla szyfrowania obiektów kombinatorycznych.

LITERATURA

1. Kapralski A.: Modeling and Generation of Arbitrary sets of Combinatorial Objects and their Sequential and Parallel Generation. (praca złożona w redakcji ZN Pol. Śl.).
2. Kapralski A.: New Methods for the Generation of Permutations, Combinations and other Combinatorial Objects in Parallel. *JPDC*, Vol.17, No 4, 315-326, April, 1993.
3. Kapralski A.: Representation and Parallel Generation of Number and Set Partitions.
4. Decompositions, Compositions and Related Combinatorial Objects Technical Report Nr 94-1-038, University of Aizu, July, 1994.

Recenzent: Dr inż. Andrzej Białas

Wpłynęło do Redakcji 3 kwietnia 2000 r.

Abstract

The presented in this paper methodology for making non-monotonic and highly entropic mappings of an integer (representing rank) into a combinatorial object is valid from theoretical point of view and can be widely applied in different branches of designing safe computer systems. The methodology is basing on the theory of representing any set of combinatorial objects by unranking S_U and ranking S_R models [1],[2],[3]. The basic components of unranking models are the indexed families, requirements W that are to be satisfied by these indexed families and the sets of choice functions of these indexed families that each choice function represents a combinatorial object of an arbitrary set. If the sets of combinatorial objects are symmetric, then their structure can be represented by the tables D. The tables D can be effectively evaluated and assembled with a given linear order on the sets of choice functions make the fundamental data for efficient ranking generation algorithms. Treating a rank as a

code of a combinatorial object and keeping the model unrelieved, we can make cryptographic systems very resistant against any attack. This resistance can be even increased designing hierarchical representation models. We can hide the number of levels of the hierarchical model and also all componential models can also be hidden. The methodology for making the ranking system non-monotonic is an additional and valid factor for keeping the model resistant against cryptoanalisis. That makes the presented models as very suitable tools for any application including cryptography and designing safe data systems.