DZIAŁ NAUKOWY

MATEMATYKA STOSOWANA 7, 2006

Kamil Kulesza (Warszawa)
Paweł Nowosielski (Warszawa)

Kiedy *doskonały* nie jest *idealny*, czyli matematyczne metody dzielenia sekretu

Streszczenie. Praca dotyczy rodziny protokołów kryptograficznych zwanych schematami podziału sekretu. W ramach pracy opisujemy szczegółowo podstawowe schematy podziału sekretu. Następnie prezentujemy uogólnione podejście do zagadnienia podziału sekretu oraz pokazujemy, jak teoria informacji może być wykorzystana do bardziej precyzyjnego opisu przedmiotu pracy. Podajemy też ogólny opis schematów podziału sekretu o rozszerzonych własnościach.

Słowa kluczowe: kryptografia, podział sekretu, bezpieczeństwo informacji.

1. Wstęp. Dzielenie tajemnic (podział sekretu) w swoim pierwszym wcieleniu było rodzajem matematycznej zagadki, swoistym puzzlem. Podstawowe pytanie brzmiało, czy posiadając jakąś tajemnicę (z reguły dla uproszczenia zakładano, że jest to liczba), można podzielić ją pomiędzy kilku graczy, współcześnie zwanych udziałowcami, tak aby jeśli wszyscy będą ze sobą współpracować, mogli oni poznać ową tajemnicę. Dodatkowym wymogiem było, aby żaden z nich samodzielnie nie mógł odkryć tajemnicy. Takie sformułowanie problemu może przywoływać skojarzenia z bajkami i magicznymi sztuczkami, których bohaterowie byli stawiani przed podobnymi zadaniami. Zostawiając jednak w spokoju czarodzieja Merlina i smoki, wypada zauważyć, że włoscy matematycy z czasów średniowiecza i renesansu również lubowali się w tego typu matematycznych szaradach. Była to czysta „sztuka dla sztuki" i pewnie podobnie jak teoria liczb dzielenie tajemnic pozostałoby w obrębie zainteresowania jedynie matematyków (jak w słynnym powiedzeniu Hardy'ego), gdyby nie kryptografia. W tym znaczeniu był to dobry przykład na to, jak zastosowania stymulują badania matematyczne. W rezultacie dzielenie tajemnic (podział sekretu) doczekało się sformalizowanych podstaw i stało się precyzyjnie opisaną dziedziną badawczą.

Mimo to (a może raczej dzięki temu) dzielenie tajemnic jest polem badawczym, gdzie można napotkać interesujące paradoksy oraz różne przeczące codziennej intuicji rezultaty. Np. w przypadku dzielenia tajemnic dwa

pojęcia *doskonałość* i *idealność*, które w języku potocznym są synonimami, mają odmienne i rozłączne znaczenia. Dzielenie sekretów jest jednym z podstawowych prymitywów kryptograficznych i jest używane jako podstawa do bardziej skomplikowanych konstrukcji. Wspomnieliśmy o praktycznych zastosowaniach podziału sekretu; obecnie ich liczba jest duża i ciągle rośnie. Poza zastosowaniami czysto kryptograficznymi, coraz więcej zastosowań pojawia się w wyniku wzrastającej w naszym życiu roli komputerów i technik informacyjnych. Jednak najważniejszym do tej pory zastosowaniem (i jedną z głównych przyczyn rozwoju badań nad schematami podziału sekretu) jest kontrola nad strategiczną i taktyczną bronią nuklearną. W przypadku obu supermocarstw dysponujących taką bronią, jej systemy dowodzenia i kontroli musiały sprostać wielu bardzo ostrym i niejednokrotnie sprzecznym ze sobą wymogom. I tak na przykład: z jednej strony musi istnieć możliwość szybkiego i pewnego użycia takiej broni, z drugiej chcemy mieć tak dużą jak się da pewność, że nie nastąpi nieautoryzowane lub przypadkowe jej użycie. Oczywiście, można mieć jeden tajny kod w rękach zaufanego człowieka (np. przywódcy narodu), tyle że rozwiązanie takie nie spełnia powyższych warunków (co będzie np., jeśli przywódca zwariuje). Dodatkowo, tworzy to sytuację, w której cały system oparty jest na niezawodności pojedynczego elementu, tak więc przeciwnik może go stosunkowo małym kosztem (z punktu widzenia ceny całego systemu) unieruchomić — eliminując przywódcę. Naturalnie narzucającym się rozwiązaniem jest zastosowanie dzielonej kontroli nad systemem, do czego doskonale nadają się schematy podziału sekretu.

W naszej pracy będziemy od czasu do czasu odwoływać się do tego zastosowania dzielenia tajemnic, aby lepiej zilustrować wybrane zagadnienia. Oczywiście działający w praktyce system dowodzenia i kontroli obejmuje znacznie szersze spektrum problemów niż tylko matematyczne aspekty podziału sekretu, warto jednak podkreślić, że prawie cała logika zabezpieczeń systemu (łącznie z procedurami dotyczącymi ludzi) bazuje na podziale sekretu. Zainteresowany czytelnik może znaleźć więcej informacji i doskonały spis bibliografii w książce Rossa Andersona ([2]). Powyżej napisaliśmy, że kontrola nad strategiczną i taktyczną bronią nuklearną jest najważniejszym naszym zdaniem zastosowaniem podziału sekretu w dotychczasowej historii ludzkości i jak każdy widzi, do tej pory system ten okazał się skuteczny. Nie doszło do przypadkowego wybuchu wojny nuklearnej, a autorom było dane napisać ten artykuł.

Plan dalszej części pracy jest następujący: w następnym rozdziale przedstawimy podstawowe pojęcia i definicje oraz odniesiemy się do kwestii terminologicznych. W kolejnym rozdziale omówimy podstawowe schematy podziału sekretu. Dalej zaprezentujemy wybrane aspekty łączące dzielenie tajemnic i teorię informacji, które stanowią formalne podstawy dziedziny. Takie przygotowanie pozwoli nam w dalszej kolejności zaprezentować rozsze-

rzone schematy podziału sekretu i zarysować podstawowe trudności związane z ich tworzeniem. W ramach podsumowania jeszcze raz nawiążemy do paradoksów związanych z dzieleniem sekretu i pytania, czy sekret zawsze da się wyrazić liczbą.

2. Terminologia i definicje. Uważny czytelnik z pewnością zauważył, że w poprzednim rozdziale wymiennie używano dwóch terminów: *dzielenie tajemnic* i *podział sekretu*. Oba wywodzą się od tego samego angielskiego terminu *secret sharing* i mają to samo znaczenie. W dalszym ciągu pracy będziemy głównie używać terminu podział sekretu, który wydaje się nam bardziej wygodny. W polskich tłumaczeniach literatury przedmiotu można natrafić też na inną terminologię, np. tajne schematy współużytkowania (np. [35]). W naszej pracy przyjmujemy głównie terminologię i definicje za polskim tłumaczeniem książki Pieprzyka i in. [30], czasem korzystamy też z polskich tłumaczeń książek Menezesa i in. ([27]) i Stinsona ([35]).

Schematy podziału sekretu należą do rodziny protokołów kryptograficznych i zostały wymyślone niezależnie przez Adi Shamira ([31]) i George'a Blakleya ([6]). Umożliwiają one podział sekretu na części zwane udziałami, które zostają rozdzielone pomiędzy udziałowców w taki sposób, że tylko pewna grupa (autoryzowany zbiór udziałowców) może odzyskać sekret. Równie istotne jest to, że żaden inny zbiór osób nie może tego zrobić.

Przykładowe zastosowania to:

1. *Transakcje bankowe*. Kiedy klient chce wypłacić z rachunku znaczną kwotę, polecenie wypłaty musi być kontrasygnowane przez dwóch spośród trzech upoważnionych pracowników banku. Tylko po złożeniu przez nich podpisów możliwe jest przygotowanie wypłaty.
2. *Ład korporacyjny*. Aby zarząd firmy podjął ważną (rodzącą skutki prawne) decyzję, musi ona zostać zaakceptowana przez pewną progową liczbę członków zarządu.
3. *Wojsko*. Ważne operacje, np. wystrzelenie pocisku balistycznego, mogą być wykonane jedynie po uprzednim wprowadzeniu tajnego kodu. Dzielona kontrola nad kodem skutkuje dzieloną kontrolą nad ważną operacją.
4. *à la Bond*. Banknot (np. 50 funtów) zostaje przedarty na pół i przekazany dwóm nie znającym się wcześniej agentom (np. z MI6 i KGB). Kiedy agenci ci spotykają się gdzieś w obcym kraju i muszą się jednoznacznie zidentyfikować, każdy wyjmuje swoją część banknotu; jeśli części pasują do siebie, to znaczy, że spotkali się właściwi ludzie.

Powyższe przykłady pozwalają nam wprowadzić dwa podstawowe sposoby wykorzystania dzielenia tajemnic w praktyce:

1. *Dzielona kontrola*, której różne aspekty prezentują przykładowe zastosowania 1, 2, 3.
2. *Uwierzytelnienie*, które w nieco swobodny sposób przedstawia przykładowe zastosowanie „à la Bond". W tym przypadku chodzi o to, że udziałowcy poprzez odtworzenie sekretu potwierdzają swoją tożsamość. Choć kwestia ta nie będzie głównym przedmiotem naszych rozważań, należy zwrócić uwagę na fakt, że problemy właściwego ustalania tożsamości, a więc i uwierzytelniania należą do fundamentalnych we współczesnej inżynierii bezpieczeństwa (por. [2]).

W tym miejscu warto zwrócić uwagę, że sekret nie musi być znany, zanim rozpocznie się procedura jego podziału. Często może to być pewna losowa wartość generowana w trakcie trwania tej procedury. Z punktu widzenia praktycznych zastosowań (szczególnie uwierzytelniania) nie jest bowiem ważna sama wartość sekretu, a fakt jego poprawnego odtworzenia przez udziałowców.

Celem sformalizowania naszych rozważań wprowadzimy następujące oznaczenia:

- $k \in K$ jest sekretem, gdzie K jest przestrzenią sekretu (mówiąc nieformalnie, zbiorem wszystkich możliwych wartości sekretu),
- $s_i \in S$ jest udziałem, gdzie S oznacza przestrzeń udziałów,
- $P_i \in P$ jest udziałowcem sekretu oraz $P = \{P_1, P_2, \ldots, P_n\}$ jest zbiorem wszystkich udziałowców sekretu,
- A jest autoryzowanym zbiorem udziałowców sekretu,
- Γ jest *strukturą dostępu*, czyli zbiorem wszystkich autoryzowanych zbiorów udziałowców sekretu.

Uwagi:

1. W pracy ograniczymy się do rozważania sekretów będących liczbą. W większości praktycznych schematów jest ona liczbą całkowitą lub wektorem, którego składowymi są liczby całkowite. Do tego tematu powrócimy jeszcze w podsumowaniu.
2. Należy zwrócić uwagę na fakt, że w ogólnym przypadku jeden udziałowiec P_i może posiadać więcej niż jeden udział s_i; więcej na ten temat powiemy w podrozdziale 3.2.
3. Dopełnienie zbioru Γ jest czasami zwane *strukturą przeciwnika* (ang. *adversary structure*). Pojęcie to jest ważne, gdyż niektórzy autorzy wolą rozważać podział sekretu w terminach struktury przeciwnika (np. [14]). Logicznym uzasadnieniem takiego spojrzenia jest analizowanie schematów podziału sekretu raczej z punktu widzenia napastnika niż uprawnionego udziałowca, co jest istotne np. w przypadku bezpiecznych obliczeń wielopodmiotowych. W naszej pracy

zajmujemy się jednak matematycznymi podstawami dzielenia sekretu i przyjmujemy optykę struktury dostępu Γ.

Definicja 2.1. Struktura dostępu Γ jest *monotoniczna*, gdy dla dowolnych zbiorów A i B takich, że $A \subseteq B$, jeśli $A \in \Gamma$, to $B \in \Gamma$.

Definicja 2.2. Zbiór $A \in \Gamma$ jest *minimalny*, gdy żaden jego podzbiór właściwy nie należy do Γ.

Definicja 2.3. Zbiór wszystkich minimalnych zbiorów $A \in \Gamma$ nazywamy *bazą struktury dostępu* i oznaczamy Γ_0.

W pracy [4] wykazano, że każda rozsądnie realizowalna struktura dostępu musi być monotoniczna. Więcej informacji na temat struktur dostępu podamy w podrozdziale 3.2. Teraz natomiast, operując wprowadzonymi pojęciami, formalnie opiszemy podział sekretu.

Definicja 2.4. *Schemat podziału sekretu* składa się z dwóch algorytmów:

1. *Algorytmu rozprowadzającego*, który przypisuje każdemu udziałowcowi P_i co najmniej jeden udział s_i;
2. *Algorytmu łączącego*, który mając odpowiednie udziały sekretu, oblicza sekret k.

3. Podstawowe schematy podziału sekretu. Najprostszy schemat podziału sekretu to taki, kiedy wszyscy udziałowcy potrzebni są do tego, aby odtworzyć sekret. Taki schemat podziału z licznych powodów nie jest jednak satysfakcjonujący. Posługując się naszym przykładem kontroli nad bronią nuklearną, na moment wyobraźmy sobie schemat, kiedy istnieją trzy części sekretu, np. w rękach prezydenta, ministra obrony i szefa sztabu generalnego. Tak więc aktywowanie arsenału nuklearnego wymaga zgodnej decyzji wszystkich trzech udziałowców. O ile można sobie wyobrazić, że taka decyzja jest możliwa, o tyle celem zablokowania systemu wystarczy, że przeciwnik wyeliminuje jednego (dowolnie wybranego) udziałowca. Jeśli którykolwiek z udziałów nie będzie dostępny, niemożliwe z definicji będzie odtworzenie sekretu i w rezultacie cały arsenał nuklearny będzie bezużyteczny, a kraj bezbronny. Tak więc rozwiązanie to jest nawet bardziej zawodne niż kontrola pojedynczej osoby i w oczywisty sposób słabsze. Aby zaradzić tym niedogodnościom, stworzono klasę schematów podziału sekretu z progiem.

3.1. *Progowe schematy podziału sekretu.* Podziały sekretu z progiem umożliwiają odzyskanie sekretu k, gdy t spośród wszystkich n udziałowców współpracuje ($t \leq n$). Takie schematy nazywamy *schematami progowymi* (t, n), gdzie liczba t jest zwana progiem. Bardziej precyzyjnie, progowy schemat podziału sekretu (t, n) jest schematem, w którym Γ_0 zawiera wszystkie zbiory $A \in \Gamma$ takie, że $|A| = t$.

Szczególnym przypadkiem tej klasy schematów podziału sekretu jest sytuacja, kiedy próg jest równy liczbie udziałowców. Choć jak napisano powyżej, takie rozwiązanie jest niesatysfakcjonujące w praktyce, warto się z nim zapoznać ze względu na prostotę jego konstrukcji i zalety teoretyczne. Dodatkowo, po pewnej modyfikacji może ono służyć jako podstawa do realizacji uogólnionych schematów podziału sekretu.

Schemat (t, t) KGH. Schemat został zaproponowany przez Karnina, Greena i Hellmana w [20]; od ich nazwisk pochodzi nazwa. Schemat KGH wymaga, aby wszyscy udziałowcy sekretu współpracowali w celu jego odzyskania. Dlatego jest to schemat podziału sekretu (t, t).

Przygotowanie. Dla sekretu k ustalmy pewne p takie, że $p > k$.

Algorytm rozprowadzający

1. Wybieramy losowo $t-1$ udziałów $s_1, s_2, \ldots, s_{t-1} \in \mathbb{Z}_p$.
2. Obliczamy $s_t = \sum_{i=1}^{t-1} s_i \pmod p$.
3. Wysyłamy udziały do udziałowców sekretu za pomocą bezpiecznego kanału komunikacji.

Algorytm łączący. Gdy udziałowcy zdecydują się odzyskać sekret, obliczają następującą sumę:

$$k = \sum_{i=1}^{t} s_i \pmod p.$$

Ponieważ t udziałowców jest potrzebnych, aby odzyskać tajemnicę, dodanie $t-1$ (lub mniej) udziałów nie ujawni żadnej informacji o sekrecie.

Modyfikacje KGH umożliwiają podział sekretu k, który jest η-elementowym wektorem $X_\eta = (x_1, x_2, \ldots, x_\eta)$. Wybieramy dowolne $p > \max\{x_1, x_2, \ldots, x_\eta\}$. Każdemu z t udziałowców przydzielamy wektor $X_\eta^{(j)}$, $j = 1, \ldots, t$, o elementach z $\mathbb{Z}_p$. Aby odzyskać sekret, należy wykonać algorytm łączący dla każdej ze składowych wektora, przy czym możliwe jest równoległe wykonywanie operacji dla wszystkich składowych. Dla $p = 2$ metoda KGH działa tak jak bitowa różnica symetryczna ($\oplus$) na η-bitowych liczbach.

Przykład 3.1. Rozważmy modyfikacje schematu KGH nad $\mathbb{Z}_2$. Niech $s_1 = 01101$, $s_2 = 11011$, $s_3 = 00100$. Wtedy $k = s_1 \oplus s_2 \oplus s_3 = 10010$.

Interesującą własnością KGH jest to, że gdy pewien, ustalony zbiór wektorów zostanie wyłączony z przestrzeni sekretu, metoda pozostaje w dalszym ciągu bezpieczna. Ponownie, mając $t-1$ (lub mniej) udziałów, nie można ujawnić żadnej informacji o tajemnicy. KGH z wyłączonym zbiorem wektorów jest oznaczany przez KGHe. Naturalnie dla jednakowej długości wektorów, moc przestrzeni sekretu jest mniejsza w przypadku KGHe niż KGH.

Jak można było zaobserwować powyżej, schemat KGH jest konstrukcją prostą i elegancką. Pora jednak przejść do progowych schematów podziału sekretu, które działają dla $t \leq n$. Poniżej przedstawimy trzy schematy tego typu. Nawiązując do naszego przykładu, stwierdzamy, że zgodnie z dostępnymi informacjami schemat progowy typu $(2, 3)$ jest używany przez Rosję do kontroli strategicznej broni nuklearnej, a udziałowcami sekretu w tym przypadku są prezydent, szef sztabu generalnego i ministerstwo obrony (zob. [2]).

Schemat Shamira (t, n). Schemat ten został zaproponowany przez Adi Shamira w [31]. Jest to model schematu progowego (t, n). Schemat ten był pierwszym znanym schematem progowym o dobrych własnościach teoretycznych i jest najczęściej stosowany w praktyce, szczególnie do ochrony kluczy kryptograficznych.

Przygotowanie. Dla sekretu k:

1. Wybieramy n różnych, niezerowych elementów z $\mathbb{Z}_p$, gdzie $p > n$ jest liczbą pierwszą.
2. Oznaczmy powyższe elementy przez x_i, $1 \leq i \leq n$, i rozdzielamy je do odpowiednich udziałowców sekretu P_i (te wartości mogą być udostępnione publicznie).

W schemacie Shamira powyższe punkty są zwykle wykonane przez algorytm rozprowadzający.

Algorytm rozprowadzający. Jeśli nie zaznaczono inaczej, obliczenia są przeprowadzane w $\mathbb{Z}_p$.

1. Losowo wybieramy $t-1$ liczb $a_1, a_2, \ldots, a_{t-1}$.
2. Dla każdego $1 \leq i \leq n$ obliczamy $s_i = a(x_i)$, gdzie $a(x) = k + \sum_{j=1}^{t-1} a_j x^j \bmod p$.
3. Wysyłamy udziały do udziałowców sekretu, używając bezpiecznego kanału komunikacji.

Jak widać, dla zadanego sekretu k algorytm rozprowadzający k tworzy losowy wielomian $f(x)$ stopnia co najwyżej $t-1$. Wartość sekretu jest równa wyrazowi wolnemu wielomianu $f(x)$.

Algorytm łączący. Gdy t udziałowców (dla uproszczenia przyjmijmy $P_1, P_2, \ldots, P_t$) zdecyduje się odzyskać sekret, mogą otrzymać k:

a. rozwiązując układ t równań liniowych

$$\begin{cases} s_1 = k + a_1 x_1 + a_2 x_1^2 + \ldots + a_{t-1} x_1^{t-1} \bmod p, \\ s_2 = k + a_1 x_2 + a_2 x_2^2 + \ldots + a_{t-1} x_2^{t-1} \bmod p, \\ \quad \ldots \\ s_t = k + a_1 x_t + a_2 x_t^2 + \ldots + a_{t-1} x_t^{t-1} \bmod p; \end{cases}$$

b. przy użyciu wielomianu interpolacyjnego Lagrange'a

$$h(x) = \sum_{i=1}^{t} s_i \prod_{j=1, i\neq j}^{t} \frac{x_j}{x_i - x_j} \bmod p$$

obliczając k, które jest równe $h(0)$.

Przykład 3.2. Rozważmy schemat Shamira $(3, 6)$ nad $\mathbb{Z}_{11}$. Niech $x_i = i$ dla $i = 1, \ldots, 6$ oraz $f(x) = 7 + 2x + x^2$. Wtedy

$$s_1 = f(1) = 10,\ s_2 = f(2) = 4,\ s_3 = f(3) = 0,\ s_4 = f(4) = 9,$$
$$s_5 = f(5) = 9,\ s_6 = f(6) = 0.$$

Udziałowcy P_1, P_3, P_6 łączą swe udziały (odpowiednio s_1, s_3, s_6). Odzyskanie sekretu sprowadza się do rozwiązania układu równań

$$\begin{cases} 10 = a_0 + a_1 + a_2 \bmod 11, \\ 0 = a_0 + 3a_1 + 9a_2 \bmod 11, \\ 0 = a_0 + 6a_1 + 3a_2 \bmod 11. \end{cases}$$

Powyższy układ ma jednoznaczne rozwiązanie $a_2 = 1$, $a_1 = 2$, $a_0 = k = 7$.

Modularny schemat progowy (t, n) AB. Schemat został przedstawiony przez Asmutha i Blooma w [3] i stąd bierze się jego nazwa. Wykorzystuje on chińskie twierdzenie o resztach.

Twierdzenie 3.1 (chińskie twierdzenie o resztach). *Niech $n_1, n_2, \ldots, n_k$ będą dodatnimi liczbami całkowitymi, parami względnie pierwszymi. Dla dowolnych dodatnich liczb całkowitych $a_1, a_2, \ldots, a_k$ układ kongruencji*

$$\begin{cases} a \equiv a_1 \bmod n_1, \\ a \equiv a_2 \bmod n_2, \\ \quad \ldots \\ a \equiv a_k \bmod n_k \end{cases}$$

ma jednoznaczne rozwiązanie modulo $n = n_1 \cdot n_2 \cdot \ldots \cdot n_k$.

Mimo że modularny schemat AB jest oparty na innym problemie, posiada on taką samą teoretyczną własność informacji co schemat Shamira (por. rozdział 4).

Przygotowanie. Dla sekretu k:

1. Wybieramy i podajemy do publicznej wiadomości p_i dla $i = 0, 1, \ldots, n$ takie, że
   (a) p_i są liczbami pierwszymi lub parami względnie pierwszymi,
   (b) $k < p_0 < p_1 < \ldots < p_n$.
2. Wybieramy losowo liczbę naturalną s taką, że $0 < s < \prod_{i=1}^{t} p_i$. Sekret k należy do $\mathbb{Z}_{p_0}$ i $k \equiv s \bmod p_0$.

W schemacie AB przygotowanie jest zwykle przeprowadzone w algorytmie rozprowadzającym.

Algorytm rozprowadzający

1. Obliczamy $s_i \equiv s \bmod p_i$.
2. Rozdzielamy udziały do udziałowców sekretu poprzez bezpieczny kanał komunikacyjny.

Algorytm łączący. Gdy t udziałowców (z udziałami $s_{i_1}, \ldots, s_{i_t}$) decyduje się na odzyskanie sekretu, musi zostać rozwiązany następujący układ kongruencji:

$$\begin{cases} s_{i_1} = s \bmod p_{i_1}, \\ \quad \ldots \\ s_{i_t} = s \bmod p_{i_t}. \end{cases}$$

Układ ma jednoznaczne rozwiązanie $0 < s < \prod_{i=1}^{t} p_i$ na mocy chińskiego twierdzenia o resztach. Schemat może zostać zmodyfikowany tak, aby zamiast liczb całkowitych używał wielomianów nad $\mathbb{Z}_{2^n}$ $(GF(2^n))$.

Przykład 3.3. Rozważmy modularny schemat progowy $(2, 4)$ AB. Przyjmijmy $p_0 = 11$, $p_1 = 13$, $p_2 = 17$, $p_3 = 19$, $p_4 = 23$. Liczba $s = 117$ z $\mathbb{Z}_{13\times 17} = \mathbb{Z}_{221}$ jest wybrana losowo. W wyniku tego losowania ustalony zostaje też sekret $k = 117 \pmod{11} = 7$ (oczywiście znając wcześniej sekret, można też postąpić na odwrót: obliczyć s na podstawie p_0). Wtedy $s_1 = 117 \pmod{13} = 0$, $\quad s_2 = 117 \pmod{17} = 15$, $\quad s_3 = 117 \pmod{19} = 3$, $s_4 = 117 \pmod{23} = 2$. Przypuśćmy, że udziałowcy P_2, P_4 chcą odzyskać sekret. Rozwiązują układ kongruencji

$$\begin{cases} 15 = s \bmod 17, \\ 2 = s \bmod 23, \end{cases}$$

skąd $s = 117$ oraz $k = 117 \pmod{11} = 7$.

Schemat progowy (t, n) *Blakleya.* Interesująca konstrukcja została przedstawiona przez Blakleya w [6]. Obecnie raczej nie jest praktycznie wykorzystywana, jednak ze względów historycznych przedstawimy pokrótce jej główny pomysł (Blakley wraz z Shamirem był jednym z twórców schematów podziału sekretu).

Przygotowanie. Schemat wykorzystuje (t-wymiarową) przestrzeń rzutową $PG(t, q)$ nad $\mathbb{Z}_q$. Sekret k jest punktem $p \in PG(t, q)$.

Algorytm rozprowadzający. Każdy z udziałowców posiada $(t-1)$-wymiarową podprzestrzeń przestrzeni $PG(t, q)$, która zawiera p.

Algorytm łączący. Mając t podprzestrzeni (udziałów sekretu), znajdujemy ich punkt przecięcia p.

3.2. *Ogólny podział sekretu.* Praktyczne zastosowania często wymagają, aby tylko pewien, specyficzny podzbiór udziałowców był w stanie odzyskać sekret. Rozważmy sytuację, w której rozkaz odpalenia taktycznej rakiety balistycznej musi być wydany przez dwóch generałów, lub przez generała

i dwóch pułkowników. Jest oczywiste, że progowe schematy podziału sekretu nie będą tutaj użyteczne; potrzebujemy czegoś bardziej ogólnego. Ogólny podział sekretu po raz pierwszy został opisany przez Ito, Saito i Nishizeki w [23]. Aby wprowadzić strukturę dostępu o wymaganych właściwościach, użyto konstrukcji tablicy kumulacyjnej (patrz [23] i [30]). Jest ona binarną macierzą określającą relacje między udziałami a udziałowcami. Przy podstawowym podziale sekretu każdy udziałowiec ma przypisany pojedynczy udział, natomiast w zastosowaniach tablicy kumulacyjnej ta relacja jest modyfikowana, pozwalając udziałowcowi posiadać wiele udziałów i używać ich w zależności od potrzeb. Aby najlepiej zobrazować tablice kumulacyjne, rozważmy dwa przykłady poniżej.

Przykład 3.4. Weźmy $P = \{P_1, P_2, P_3, P_4\}$ i $\Gamma = \{\{P_1, P_2\}, \{P_3, P_4\}\}$. Odpowiednia tablica kumulacyjna przedstawia się następująco:

$P \setminus S$	s_1	s_2	s_3	s_4
P_1	1	1	0	0
P_2	0	0	1	1
P_3	1	0	1	0
P_4	0	1	0	1

Przykład 3.5. Weźmy $P = \{P_1, P_2, P_3, P_4\}$ i $\Gamma = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}\}$. Odpowiednia tablica kumulacyjna to:

$P \setminus S$	s_1	s_2	s_3
P_1	1	0	1
P_2	0	1	1
P_3	1	1	0
P_4	0	1	0

Interesującą obserwacją jest fakt, że w powyższym przykładzie, pomimo znacznie bardziej skomplikowanej struktury dostępu niż w przykładzie 3.4, wynikowa tablica kumulacyjna jest prostsza, gdyż potrzebuje tylko trzech udziałów s_i.

Łącząc tablice kumulacyjne z metodą KGH, dostajemy realizację schematu ogólnego podziału sekretu (np. [30]). Podobny efekt można uzyskać w konstrukcji Benaloha–Leichtera (patrz [4]). Problemem tych dwóch konstrukcji jest to, że mimo wykazywania dobrych parametrów bezpieczeństwa, często wymagają przypisania więcej niż jednego udziału do udziałowca sekretu. Z punktu widzenia teorii informacji nie jest to dobre rozwiązanie (zobacz też rozdział 4). Tego problemu często daje się uniknąć, stosując schemat zaproponowany przez Brickella w [11].

Schemat Brickella. Metoda Brickella jest uogólnieniem schematu Shamira z wykorzystaniem t-wymiarowej przestrzeni wektorowej $\mathbb{Z}_p^t$.

Obserwacja. W schemacie Shamira wielomian $f(x) = a_0 + a_1 x + \ldots + a_{t-1}x^{t-1}$ nad $\mathbb{Z}_p$ daje udział sekretu w postaci

$$s_i = f(x_i) = a_0 + a_1 x_i + \ldots + a_{t-1}x_i^{t-1}$$

lub odpowiednio

$$s_i = (a_0, a_1, \ldots, a_{t-1}) \cdot (1, x_i, \ldots, x_i^{t-1}) = \overline{a} \cdot \overline{x}_i.$$

Innymi słowy, s_i jest iloczynem skalarnym dwóch wektorów. Ta obserwacja leży u podstaw uogólnienia schematu Shamira przez Brickella.

Przygotowanie. Rozważmy t-wymiarową przestrzeń wektorową $\mathbb{Z}_p^t$, gdzie p jest liczbą pierwszą. Niech $\tau\colon P \to \mathbb{Z}_p^t$ będzie funkcją przypisującą udziałowcowi $P_i \in P$ publiczny wektor x_i w ten sposób, że

$$\forall_{A\in\Gamma}(1, 0, \ldots, 0) = b_1\overline{x}_1 + b_2\overline{x}_2 + \ldots + b_t\overline{x}_t$$

dla pewnego $\overline{b} = (b_1, b_2, \ldots, b_t) \in \mathbb{Z}_p^t$. Wektor $(1, 0, \ldots, 0)$ nie może być przedstawiony jako kombinacja liniowa wektorów $\overline{x}_i$, gdy odpowiadający im podzbiór udziałowców $B \notin \Gamma$.

Algorytm rozprowadzający

1. Ustalamy $\mathbb{Z}_p^t$, τ i wszystkie publiczne wektory $x_i = \tau(P_i)$.
2. Wybieramy losowo $t-1$ elementów z $\mathbb{Z}_p$, oznaczanych przez $a_2, \ldots, a_t$.
3. Obliczamy $\overline{a} = (a_1, a_2, \ldots, a_t)$ taki, że $k = (1, 0, \ldots, 0) \cdot \overline{a} = a_1$.
4. Poprzez bezpieczny kanał komunikacji przesyłamy każdemu udziałowcowi P_i jego udział $s_i = \overline{a} \cdot \overline{x}_i$.

Algorytm łączący. Gdy t udziałowców (dla uproszczenia przyjmijmy $P_1, P_2, \ldots, P_t$), tworzących autoryzowany zbiór udziałowców A, zdecyduje się odzyskać sekret, ich publiczne wektory dają się zsumować do $(1, 0, \ldots, 0)$. Innymi słowy, istnieją współczynniki $b_i \in \mathbb{Z}_p$ takie, że

$$(1, 0, \ldots, 0) = \sum_{i:\, P_i \in A} b_i \overline{x}_i.$$

Mnożąc obie strony przez $\overline{a}$, dostajemy

$$\overline{a} \cdot (1, 0, \ldots, 0) = \sum_{i:\, P_i \in A} b_i \overline{a} \cdot \overline{x}_i,$$

$$k = \sum_{i:\, P_i \in A} b_i s_i.$$

Przykład 3.6. Rozważmy następujący schemat Brickella:

$$\Gamma = \{\{P_1, P_2, P_3\}, \{P_1, P_4\}\},$$

$$\overline{x}_1 = (0, 1, 1),\ \overline{x}_2 = (0, 1, 0),\ \overline{x}_3 = (0, 1, 1),\ \overline{x}_4 = (-1, -1, -1).$$

Najpierw sprawdzimy, czy za pomocą kombinacji liniowej publicznych wektorów, należących do dowolnego minimalnego zbioru autoryzowanego, można otrzymać wektor $(1,0,0)$.

a. $A = \{P_1, P_2, P_3\}$; wtedy $(1,0,0) = \overline{x}_2 + \overline{x}_3 - \overline{x}_1 = (0,1,0) + (1,0,1) - (0,1,1)$;
b. $A = \{P_1, P_4\}$; wtedy $(1,0,0) = -\overline{x}_4 - \overline{x}_1 = (1,1,1) - (0,1,1)$.

Dodatkowo żadna kombinacja liniowa publicznych wektorów z B, gdzie $B \notin \Gamma$, nie da wektora $(1,0,0)$.

Niech $\overline{a} = (18,7,3)$ nad $\mathbb{Z}_{11}$, czyli $k = 8 = (1,0,0) \cdot \overline{a}$. Udziałami sekretu są:

$$\begin{aligned} s_1 &= \overline{a} \cdot \overline{x}_1 = (8,7,3) \cdot (0,1,1) = 10, \\ s_2 &= \overline{a} \cdot \overline{x}_2 = (8,7,3) \cdot (0,1,0) = 7, \\ s_3 &= \overline{a} \cdot \overline{x}_3 = (8,7,3) \cdot (1,0,1) = 11 \equiv 0 \bmod 11, \\ s_4 &= \overline{a} \cdot \overline{x}_4 = (8,7,3) \cdot (-1,-1,-1) = -7 \equiv 4 \bmod 11. \end{aligned}$$

Dla $A = \{P_1, P_2, P_3\}$ mamy

$$\begin{aligned} (1,0,0) &= \overline{x}_2 + \overline{x}_3 - \overline{x}_1, \\ (1,0,0) \cdot \overline{a} &= (\overline{x}_2 + \overline{x}_3 - \overline{x}_1) \cdot \overline{a} = s_2 + s_3 - s_1, \\ s_2 + s_3 - s_1 &= 7 + 0 - 10 = -3 \equiv 8 \bmod 11. \end{aligned}$$

Schemat Brickella wydaje się być dobrym rozwiązaniem dla ogólnej struktury dostępu. Niestety może on być zastosowany tylko do części struktur dostępu. Istnieją struktury dostępu, których zrealizowanie jest niemożliwe w ramach schematu Brickella (por. [30], [35]). Z kolei tablice kumulacyjne i konstrukcja Benaloha–Leichtera mogą zostać zastosowane we wszystkich strukturach dostępu, ale optymalne zaprojektowanie relacji jest raczej sztuką niż ścisłą nauką (patrz [30]). Mimo wszystko możliwe jest otrzymanie teoretycznych wyników, opisujących ograniczenia możliwych konstrukcji; rozważania na ten temat wykraczają jednak poza ramy niniejszej pracy. Czytelnika zainteresowanego powyższymi zagadnieniami odsyłamy do [30] i [35].

4. Dzielenie tajemnic a teoria informacji. Teoria informacji dostarcza wielu użytecznych narzędzi do jakościowego opisu własności schematów podziału sekretu. Jej precyzyjny język pozwala również na sformułowanie pewnych paradoksów związanych z tą dziedziną. Zanim jednak przejdziemy do tych zagadnień, warto poświęcić kilka linijek pojęciu entropii, tak jak rozumiemy je w kryptografii. W tym znaczeniu entropia została wprowadzona przez Shannona w jego fundamentalnej pracy *Communication theory of secrecy systems* ([32]) i zwykle pojawia się w odniesieniu do źródła informacji. W kryptografii entropię uważa sie za miarę losowości sekwencji bitów. Dla pewnej zmiennej losowej X o rozkładzie prawdopodobieństwa $p(X)$, jej en-

tropia może być rozumiana jako matematyczna miara ilości informacji (lub niejednoznaczności) otrzymanej z obserwacji. Dobrze zostało to ujęte w następującym cytacie: *Przypuśćmy, że mamy zmienną losową X przyjmującą wiele wartości zgodnie z rozkładem prawdopodobieństwa $p(X)$. Jakiej informacji dostarcza zdarzenie zachodzące zgodnie z rozkładem $p(X)$? Równoważnie, jeśli zdarzenie (jeszcze) nie zaszło, jak ocenić niepewność co do jego wyniku? Taką wielkość nazywa się entropią zmiennej losowej X i oznacza symbolem $H(X)$* ([35], str. 52). Dysponując pojęciem entropii, możemy definiować różne własności schematów podziału sekretu. Korzystając z tych własności, podamy kilka twierdzeń dotyczących poszczególnych schematów. Ich dowody zostaną pominięte; zainteresowany czytelnik może znaleźć część z nich w pracach [30], [35].

Definicja 4.1. Niech X będzie zmienną losową reprezentującą przypisanie udziałów do zbioru udziałowców P. Schemat podziału sekretu ze strukturą dostępu Γ jest *doskonały*, jeśli

$$H(k|X) = \begin{cases} H(k), & X \notin \Gamma, \\ 0, & X \in \Gamma. \end{cases}$$

Twierdzenie 4.1. *Schemat (t, t) KGH jest doskonały.*

Wniosek 4.1. *Tablice kumulacyjne i konstrukcja Benaloha–Leichtera są doskonałe (ponieważ KGH jest doskonały).*

Następny wynik jest dość zaskakujący. Upłynęło kilka lat, zanim został odkryty.

Twierdzenie 4.2. *Schemat Shamira (t, n) z losowym wielomianem $f(x)$ stopnia $t - 1$ nie jest doskonały.*

Dowód twierdzenia 4.2 pociąga za sobą następujący wniosek.

Wniosek 4.2. *Schemat Shamira (t, n) z losowym wielomianem $f(x)$ stopnia co najwyżej $t - 1$ jest doskonały.*

Tak więc w schemacie Shamira własność doskonałości może być zachowana, jeśli nie podaje się informacji o użytym stopniu wielomianu.

Twierdzenie 4.3. *Modularny schemat (t, n) AB jest doskonały.*

Własność doskonałości podziału sekretu jest przyczyną interesującego paradoksu. W życiu codziennym jesteśmy przyzwyczajeni do sytuacji, gdy im więcej mamy części danego obiektu/przedmiotu, tym więcej informacji o nim posiadamy. W przypadku schematu, który jest doskonały, fakt posiadania dowolnej liczby udziałów sekretu, które nie stanowią zbioru autoryzowanego, ma tę samą wartość informacyjną. Innymi słowy, w doskonałym schemacie typu (t, n), z punktu widzenia wartości informacji, którą

posiadamy, nie ma różnicy, czy mamy zero czy $t-1$ udziałów. W obu przypadkach naszą najlepszą strategią odtworzenia sekretu może być jedynie odgadywanie, w dodatku z tym samym prawdopodobieństwem sukcesu. Paradoksalne i sprzeczne z codziennym doświadczeniem jest to, że zbierając kolejne udziały, nie zyskujemy żadnej dodatkowej informacji.

Definicja 4.2. *Współczynnikiem informacji* dla $P_i \in P$ nazywamy liczbę

$$\rho_i = \frac{\log_2 |K|}{\log_2 |S_i|},$$

gdzie S_i oznacza zbiór możliwych udziałów, jakie udziałowiec P_i może otrzymać.

Definicja 4.3. *Współczynnikiem informacji* schematu nazywamy

$$\rho = \min_{i=1,\ldots,n} \rho_i.$$

Definicja 4.4. Schemat podziału sekretu jest *idealny*, jeśli $\rho = 1$.

Nieformalnie mówiąc, powyższa definicja stwierdza, że długość udziału sekretu (w bitach) powinna być równa długości samego sekretu. Niektórzy autorzy (np. [35], [11]) używają bardziej restrykcyjnej definicji, opisując własność idealności przez doskonałe schematy podziału sekretu.

Twierdzenie 4.4. *Następujące schematy podziału sekretu są idealne:*

a. *KGH* (t, t),
b. *Shamira* (t, n),
c. *Modularny* (t, n) *AB,*
d. *Brickella,*

pod warunkiem stosowania z odpowiednią konstrukcją struktury dostępu.

W tym miejscu czytelnik wie już, że w przeciwieństwie do języka potocznego doskonałość i idealność są różnymi własnościami podziału sekretu. Pierwsza z nich mierzy, na ile dany schemat jest bezpieczny, a druga — czy jest odpowiednio ekonomiczny z punktu widzenia informacji, którą należy przechowywać. Idealność ma też daleko idące konsekwencje praktyczne, gdyż w przypadku większych systemów (np. medyczne bazy danych) wielkość udziałów sekretu ma duże znaczenie. Aby to sobie uzmysłowić, wystarczy zauważyć, że nawet w idealnym schemacie podziału sekretu sumaryczna ilość informacji, którą należy przechowywać, rośnie liniowo wraz z liczbą udziałowców.

Twierdzenie 4.5 (o współczynniku informacji). *W każdym doskonałym schemacie podziału sekretu używającym struktury dostępu* Γ*, współczynnik informacji* ρ *jest nie większy od* 1.

Definicja 4.5. Dla każdego doskonałego schematu podziału sekretu używającego Γ, niech ρ^* oznacza maksymalny współczynnik informacji.

Oczywiście dowolny schemat, określony jak w definicji, spełnia $\rho \leq \rho^*$. Na pierwsze rzut oka może się więc wydawać, że powyższa definicja jest trywialna. Należy jednak zwrócić uwagę na fakt, że o ile własność doskonałości zależy od samego schematu podziału sekretu, o tyle idealność zależy od struktury dostępu Γ oraz sposobu, w jaki struktura ta jest realizowana w danym schemacie. Jak napisaliśmy w zakończeniu podrozdziału 3.2, realizacja struktur dostępu jest bardziej sztuką niż ścisłą nauką. Można bez większego trudu wskazać dwie poprawne realizacje struktury dostępu, używające tego samego doskonałego schematu podziału sekretu, które będą się charakteryzować różnymi współczynnikami informacji ρ. Również taka sama struktura dostępu realizowana za pomocą różnych doskonałych schematów podziału sekretu może mieć różne wartości współczynnika informacji ρ. Wystarczy rozważyć struktury dostępu zrealizowane za pomocą schematu KGH w przykładach 3.4 i 3.5 i ich możliwą realizację za pomocą schematu Brickella. Po raz kolejny odsyłamy czytelnika zainteresowanego powyższymi zagadnieniami do książek [30] i [35].

5. Rozszerzone schematy podziału sekretu. Podstawowe schematy podziału sekretu dają się z reguły dobrze opisywać i analizować narzędziami teorii informacji. Niestety ich własności są niewystarczające przy tworzeniu systemów w praktyce i muszą być rozszerzone o kolejne funkcjonalności. W tym rozdziale naszkicujemy kilka najbardziej popularnych możliwości rozszerzeń. Zgodnie z terminologią z prac [27] i [33] możliwości te nazywamy *rozszerzonymi własnościami* (ang. *extended capabilities*). Należy jednak wspomnieć, że schematy o rozszerzonych własnościach, jeśli chodzi o funkcjonalność, częściowo pokrywają się z innymi bardziej zaawansowanymi konstrukcjami, jak bezpieczne obliczenia wielostronne (por. [14]) i *group oriented cryptography* (kryptografia grupowa, zob. [30]). Granica między tymi konstrukcjami nie jest dokładnie ustalona, aby więc uniknąć sporu terminologicznego, przyjęliśmy, że rozszerzone własności należą do schematów podziału sekretu, natomiast ich bardziej złożone realizacje z reguły przypisywane są bardziej zaawansowanym konstrukcjom.

Proaktywne dzielenie sekretu (PDS). Proaktywne dzielenie sekretu jest używane w przypadku sekretów o długim czasie życia (por. [21]). Sama ich natura może uniemożliwiać ich zmianę, np. można rozważać dokumenty prawne lub sekrety przemysłowe. PDS umożliwia okresowe odnawianie udziałów przy zachowaniu tego samego sekretu. Wymóg okresowości odnawiania wynika również z założenia, że kiedy udziałowiec sekretu został „spalony" (np. włamano się na jeden z serwerów odpowiedzialnych za roz-

proszone zarządzanie kluczami kryptograficznymi), historia wszystkich jego działań z przeszłości jest dostępna dla przeciwnika (zob. [14]). Dodatkowo należy też zapewnić:

- sposób odzyskiwania (lub ponownego obliczenia) udziałów, które zaginęły lub uległy uszkodzeniu,
- metody dołączania nowych udziałowców i usuwania starych.

Ponieważ każdy czytelnik obdarzony odrobiną wyobraźni jest w stanie zauważyć liczne korzyści ze stosowania PDS w naszym stałym przykładzie dotyczącym broni nuklearnej, więc bez zbędnej zwłoki przejdziemy dalej.

Podział sekretu z weryfikacją (PSW). Przedstawione w poprzednich rozdziałach schematy podziału sekretu działają dobrze przy założeniu, że wszystkie strony postępują zgodnie ze z góry przyjętym protokołem. Jednak w rzeczywistości założenie takie jest dość ryzykowne. PSW umożliwia zabezpieczenie się przed próbami oszustwa ze strony innych udziałowców lub nawet algorytmu rozprowadzającego (por. [29], [18]). Weryfikacja jest szczególnie ważna, kiedy spójność udziałów jest kluczowa (np. aktywacja broni nuklearnej lub choćby „zwykłe" klucze kryptograficzne). Możliwość weryfikacji istnieje zarówno dla warunkowo bezpiecznych schematów podziału sekretu (zob. [34]), jak i bezwarunkowo bezpiecznych (zob. [13]). W tym miejscu należy podkreślić, że oszukańcze praktyki mogą nie tylko spowodować załamanie wykonania protokołu (np. poprzez uniemożliwienie odtworzenia sekretu), ale również w krańcowym przypadku odtworzenie sekretu przez oszusta na własną rękę, jak pokazali Tompa i Woll w pracy [37]. Procedura weryfikacji może odbywać się za pomocą zaufanej trzeciej strony, jednak lepiej jest, kiedy udziałowcy sekretu mogą ją przeprowadzić bezpośrednio między sobą. Jeśli procedura weryfikacji udziałów sekretu odbywa się publicznie (np. w sieci) lub korzysta z publicznie dostępnych danych, wówczas mamy do czynienia z *podziałem sekretu z publiczną weryfikacją* (PSPW) (zob. [34]). Choć możliwość weryfikacji udziałów jest w praktyce bardzo cenna, pociąga za sobą utratę części własności teorio-informacyjnych, z reguły doskonałości. Pewnym sposobem obejścia lub optymalizacji tego problemu jest alternatywne podejście do podziału sekretu z weryfikacją, zaproponowane w [25].

Automatyczne tworzenie i podział sekretu. Istnieją sytuacje, kiedy sekret jest tworzony przed momentem, kiedy zostaje podzielony. Dobrym przykładem jest tu wykorzystanie podziału sekretu do uwierzytelnienia/identyfikacji, jak opisano w rozdziale 2. W takim przypadku udziałowcy, którzy są w stanie odtworzyć poprawny sekret, jednocześnie uwierzytelniają/identyfikują siebie jako autoryzowany zbiór udziałowców. Sam sekret ma tu znaczenie drugorzędne i często jest tworzony tuż przed dystrybucją udziałów.

Automatyczne tworzenie sekretu zajmuje się obsługą takich właśnie sytuacji. Niejednokrotnie sekret tworzony jest od razu w postaci udziałów (w formie rozproszonej) i pozostaje nieznany do czasu pierwszego odtworzenia (użycia algorytmu łączącego).

Innym problemem jest to, że z reguły algorytm rozprowadzający musi poznać sekret, aby móc dokonać jego podziału. Daje mu to pewną przewagę, która może stać się podstawą nadużyć. Automatyczne dzielenie sekretu pozwala wyeliminować tradycyjnie pojmowany algorytm rozprowadzający i podzielić udziały w taki sposób, że będą one miały czysto losowe wartości. Dodatkowo zaletą takiego podejścia jest to, że nawet właściciel sekretu nie zna wartości poszczególnych udziałów ani tego, jak zostały rozprowadzone. Opisane powyżej własności są często umieszczane w ramach *group oriented cryptography* i po raz pierwszy zostały opisane przez Desmedta w [17]. Praktyczne rozwiązanie w kontekście schematów z progiem bazujących na problemie logarytmu dyskretnego zostało przedstawione przez Pedersena w [28] i następców w pracach [22], [19]. Automatyczne tworzenie i podział sekretu są często dyskutowane w kontekście rozproszonego obliczania kluczy RSA (zob. [10]), niejednokrotnie połączonego z rozproszonym testowaniem pierwszości (zob. [1]). Takie zastosowania często są umieszczane w bezpiecznych obliczeniach wielostronnych (zob. [12], [14]). Jeśli chodzi o „czyste dzielenie sekretu", to problem po raz pierwszy został opisany w pracy [36] i szczegółowiej zbadany przez Blundo, Gaggia i Stinsona w pracach [7], [8].

Wielosekretowe schematy progowe. Takie schematy najlepiej opisuje cytat z książki Menezesa i in. ([27]): *W przypadku tych schematów współdzielenia sekretu różne sekrety są związane z różnymi uprawnionymi podzbiorami.* Powyższy cytat tak naprawdę dotyczy jeszcze bardziej ogólnej sytuacji, odnosząc się do schematów wielosekretowych, które niekoniecznie muszą mieć strukturę dostępu z progiem. W schematach progowych wraz ze zmianą ilości udziałowców zmienia się też i sekret, z reguły w taki sposób, że jego waga wzrasta wraz z progiem. Niewątpliwie jest to cenne udogodnienie, choć większość używanych praktycznie schematów jest wykorzystywana w konstrukcjach z progiem. Przywołując stały w tej pracy przykład: ilość i ewentualna ranga generałów potrzebnych do aktywacji danego typu broni (np. nuklearne pociski artyleryjskie czy broń taktyczna) rośnie wraz z mocą głowicy mierzoną w kilotonach.

Po tym krótkim przeglądzie rozszerzonych własności mogłoby się wydawać, że są one dość dobrze zbadane i opisane. Nie do końca jest to prawda i jest ciągle wiele możliwych usprawnień i rozszerzeń. Np. stosowanie rozszerzonych własności dla uogólnionych struktur dostępu rodzi liczne problemy. Często korzystanie z rozszerzonych własności kosztuje, np. wspomniana powyżej możliwość weryfikacji powoduje utratę doskonałości. Dzieje się tak,

gdyż często rozszerzone własności skutkują wzajemnie sprzecznymi wymaganiami, tak więc budowanie schematów podziału sekretu z kilkoma rozszerzonymi własnościami jest ciągle dużym wyzwaniem.

6. Podsumowanie. W pracy tej zajmowaliśmy się dzieleniem tajemnic zwanym również podziałem sekretu. Omówiliśmy podstawowe schematy podziału sekretu, podaliśmy metody z teorii informacji mające zastosowanie do ich opisu oraz pokazaliśmy przykłady rozszerzonych własności podziału sekretu. Przy okazji zaprezentowaliśmy dwa paradoksy: pierwszy dotyczył własności doskonałości (udziały sekretu nie kumulują informacji), natomiast drugi pokazywał, że doskonałe i idealne nie muszą oznaczać tego samego. W ten sposób udało się nam zarysować zakres tematyczny związany z podziałem sekretu. Schematy podziału sekretu stanowią podstawę dla bardziej złożonych konstrukcji, takich jak bezpieczne obliczenia wielopodmiotowe (zob. [14]). Dobrze znany jest fakt, że dowolny liniowy schemat podziału sekretu (a tylko takie omawialiśmy w tej pracy) może służyć do tego celu (zob. [15]). Z kolei bezpieczne obliczenia wielopodmiotowe są o tyle ważne, że korzystając z nich, można, przynajmniej w teorii, zbudować dowolny protokół kryptograficzny (zob. [14]). Na bardziej praktycznym poziomie bezpieczne obliczenia wielostronne mogą być używane do zapewnienia bezpieczeństwa dużych medycznych baz danych lub agentów mobilnych (zob. [5], [16]).

Na samym końcu chcieliśmy ustosunkować się do rzuconego mimochodem na początku pracy pytania, czy schematy podziału sekretu dla liczb są wystarczające. Przecież w świecie rzeczywistym istnieje wiele obiektów mających bardziej złożoną naturę, którą zdecydowanie lepiej opisuje się za pomocą np. grafów niż liczb. W dodatku zastosowania co najmniej niektórych z nich mogą już wkrótce wymagać użycia schematów podziału sekretu. Na przykład można zastanowić się nad biotechnologiami związanymi z DNA (zob. [9]) lub projektowaniem układów o wysokiej skali integracji (zob. [26]). Czy więc schematy podziału sekretu dla liczb wystarczą, czy trzeba będzie wymyślić coś nowego? Odpowiedź na to pytanie nie jest trywialna, choć na razie wydaje się, że w wielu zastosowaniach będzie można zaadaptować obecne schematy do pracy z obiektami o innej strukturze (zob. [24]) — ale to już historia na zupełnie inny artykuł.

Literatura

[1] J. Algesheim, J. Camenish, V. Shoup, *Efficient computation modulo a shared secret with applications to the generation of shared safe prime products*, w: Advances in Cryptology—CRYPTO'97, Lecture Notes in Computer Science 1294, Springer-Verlag, 1997, 425–439.

[2] R. Anderson, *Inżynieria zabezpieczeń*, WNT, Warszawa, 2005.

[3] C. Asmuth, J. Bloom, *A modular approach to key safeguarding*, IEEE Trans. on Information Theory IT-29 (1983), 208–211.

[4] J. Benaloh, J. Leichter, *Generalized secret sharing and monotone functions*, w: Advances in Cryptology—CRYPTO'88, Lecture Notes in Computer Science, Springer-Verlag, 1988, 27–36.

[5] T. Bilski, T. Pankowski, J. Stokłosa, *Bezpieczeństwo danych w systemach informatycznych*, PWN, Poznań. 2001.

[6] G. R. Blakley, *Safeguarding cryptographic keys*, w: Proc. AFIPS 1979 National Computer Conference, AFIPS, 1979, 313–317.

[7] C. Blundo, A. G. Gaggia, D. R. Stinson, *On the dealer's randomness required in secret sharing schemes*, Designs, Codes and Cryptography 11 (1997), 107–122.

[8] C. Blundo, D. R. Stinson, *Anonymous secret sharing schemes*, Discrete Applied Mathematics 77 (1997), 13–28.

[9] J. Błażewicz, M. Kasprzak, *Complexity of DNA sequencing by hybridization*, Theoretical Computer Science 290 (2003).

[10] D. Boneh, M. K. Franklin, *Efficient generation of shared RSA keys*, w: Advances in Cryptology—CRYPTO'97, Lecture Notes in Computer Science 1294, Springer-Verlag, 1997, 425–439.

[11] E. F. Brickell, *Some ideal secret sharing schemes*, Journal of Combinatorial Mathematics and Comb. Computing 6 (1989), 105–113.

[12] D. Catalano, *Efficient distributed computation modulo a shared secret*, w: Advanced Course on Contemporary Cryptology, Centre de Reserca Matematica, Barcelona 2004.

[13] D. Chaum, C. Crepeau, I. Damgard, *Multiparty unconditionally secure protocols*, w: Proc. 20th Annual Symp. on Theory of Computing, ACM, 1988, 11–19.

[14] R. Cramer, I. Damgard, *Multiparty computations, an introduction*, w: Advanced Course on Contemporary Cryptology, Centre de Reserca Matematica, Barcelona 2004.

[15] R. Cramer, I. Damgard, U. Maurer, *General secure multi-party computation from any linear secret-sharing scheme*, w: Advances in Cryptology—EUROCRYPT 2000, Lecture Notes in Computer Science 1807, Springer-Verlag, 2000, 316–334.

[16] D. E. R. Denning, *Kryptografia i ochrona danych*, WNT, Warszawa, 1993.

[17] Y. Desmedt, *Society and group oriented cryptography: a new concept*, w: Advances in Cryptology—CRYPTO'87, Lecture Notes in Computer Science, Springer-Verlag, 1987, 120–128.

[18] C. Dwork, *On verification in secret sharing*, w: Advances in Cryptology—CRYPTO'91, Lecture Notes in Computer Science, Springer-Verlag, 1992, 114–128.

[19] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, *Secure distributed key generation for discrete-log based cryptosystems*, w: EUROCRYPT'99, Lecture Notes in Computer Science 1592, Springer-Verlag, 295–310.

[20] J. W. Greene, M. E. Hellman, E. D. Karnin, *On secret sharing systems*, IEEE Transactions on Information Theory IT-29 (1983), 35–41.

[21] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, *Proactive secret sharing or: how to cope with perpetual leakage*, w: Advances in Cryptology—CRYPTO'95, Lecture Notes in Computer Science, Springer-Verlag, 1996, 339–352.

[22] T. Hwang, N. Lee, C. Li, (t, n) *threshold signature schemes based on discrete logarithm*, w: EUROCRYPT'94, Lecture Notes in Computer Science 950, Springer-Verlag, 1994, 191–200.

[23] M. Ito, T. Nishizeki, A. Saito, *Secret sharing scheme realizing general access structure*, w: Proc. IEEE Globecom '87, IEEE, 1987, 99–102.

[24] K. Kulesza, *Secret sharing schemes for graphs*, praca doktorska, IPPT PAN 2004.

[25] K. Kulesza, Z. Kotulski, J. Pieprzyk, *On alternative approach for verifiable secret sharing*, w: 7th European Symposium on Computer Security, ESORICS2002, Zurich; dostępne z: IACR's Cryptology ePrint Archive (http://eprint.iacr.org/) report 2003/035.
[26] M. Kubale (red.), *Optymalizacja dyskretna. Modele i metody kolorowania grafów*, WNT, Warszawa, 2002.
[27] A. J. Menezes, P. van Oorschot, S. C. Vanstone, *Kryptografia stosowana*, WNT, Warszawa, 2005.
[28] T. Pedersen, *A threshold cryptosystem without a trusted third party*, w: EUROCRYPT'91, Lecture Notes in Computer Science 547, Springer-Verlag, 1991, 522–526.
[29] T. P. Pedersen, *Non-interactive and information-theoretic secure verifiable secret sharing*, w: Advances in Cryptology—CRYPTO'91, Lecture Notes in Computer Science, Springer-Verlag, 1992, 129–140.
[30] J. Pieprzyk, T. Hardjono, J. Seberry, *Teoria bezpieczeństwa systemów komputerowych*, Helion, Gliwice, 2005.
[31] A. Shamir, *How to share a secret*, Communication of the ACM 22 (1979), 612–613.
[32] C. E. Shannon, *Communication theory of secrecy systems*, Bell Systems Technical Journal 28 (1949), 656–715.
[33] G. J. Simmons, *How to (really) share a secret*, w: Advances in Cryptology—CRYPTO'88, Lecture Notes in Computer Science 403, Springer-Verlag, 1989, 390–448.
[34] M. Stadler, *Publicly verifiable secret sharing*, w: Advances in Cryptology—EUROCRYPT'96, Lecture Notes in Computer Science, Springer-Verlag, 1997, 190–199.
[35] D. R. Stinson, *Kryptografia. W teorii i w praktyce*, WNT, Warszawa, 2005.
[36] D. R. Stinson, S. A. Vanstone, *A combinatorial approach to threshold schemes*, SIAM J. Disc. Math. 1 (1988), 230–236.
[37] M. Tompa, H. Woll, *How to share a secret with cheaters*, Journal of Cryptology 1 (1988), 133–138.

Instytut Podstawowych Problemów Techniki
Polska Akademia Nauk
Świętokrzyska 21, 00-049 Warszawa
E-mail: Kamil.Kulesza@ippt.gov.pl

Wydział Matematyki,
Informatyki i Mechaniki
Uniwersytet Warszawski
Banacha 2, 02-097 Warszawa
E-mail: p.nowosielski@students.mimuw.edu.pl

Abstract. The paper is concerned with secret sharing schemes, a family of cryptographic protocols. First, we describe the basic schemes. Next, we present general secret sharing and the approach based on information theory. Finally, we outline extended capabilities of secret sharing schemes. An additional contribution of the paper is our effort to present unified terminology in Polish.
Keywords: cryptography, secret sharing schemes, data security.

(*wpłynęło 31 lipca 2006 r.*)