AI Tech

AKADEMIA INNOWACYJNYCH ZASTOSOWAŃ TECHNOLOGII CYFROWYCH

Podział sekretu

Cyberbezpieczeństwo

Anna Grocholewska-Czuryło, Maj'2022

Sekret

- Hasło do ważnego zasobu np. systemu operacyjnego,
- Ziarno generatora
- Symetryczny klucz do szyfrowania/deszyfrowania
- Asymetryczny klucz do cyfrowego podpisywania wiadomości/kontraktów

Pierwsze protokoły opracowali: Adi Shamir i George Blackley (1979)

Motywacja współdzielenia sekretów

- Ochrona przed utratą kluczy kryptograficznych poprzez ich powielenie - wprowadzenie nowego sposobu zarządzania kluczami
- Rozproszone zaufanie przy dostępie do ważnych zasobów - wykonywanie operacji we współpracy t z n użytkowników

Podział sekretu

Podział sekretu - to protokół kryptograficzny, złożony z pary algorytmów:

- Rozdzielającego - sekret na n udziałów
- Łączącego - połączenie t z n udziałów ($t <= n$)

Podział realizowany jest z zachowaniem następujących wymogów:

- Wymóg poprawności - co najmniej t spośród n udziałów pozwala na odtworzenie sekretu
- Wymóg prywatności - znajomość mniejszej liczby niż t spośród n udziałów uniemożliwia wyznaczenie sekretu

Klasyfikacja metod

- Trywialne/Proste metody (*ang. Trivial secret sharing*) - metody należące do tej grupy umożliwiają podział sekretu w taki sposób, że potem wszystkie udziały konieczne są do jego odtworzenia
- Efektywne/Schematy progowe (*ang. Efficient secret sharing)* - sekret dzielony jest na n udziałów, ale do jego odtworzenia wystarcza mniejsza od n liczba t udziałów

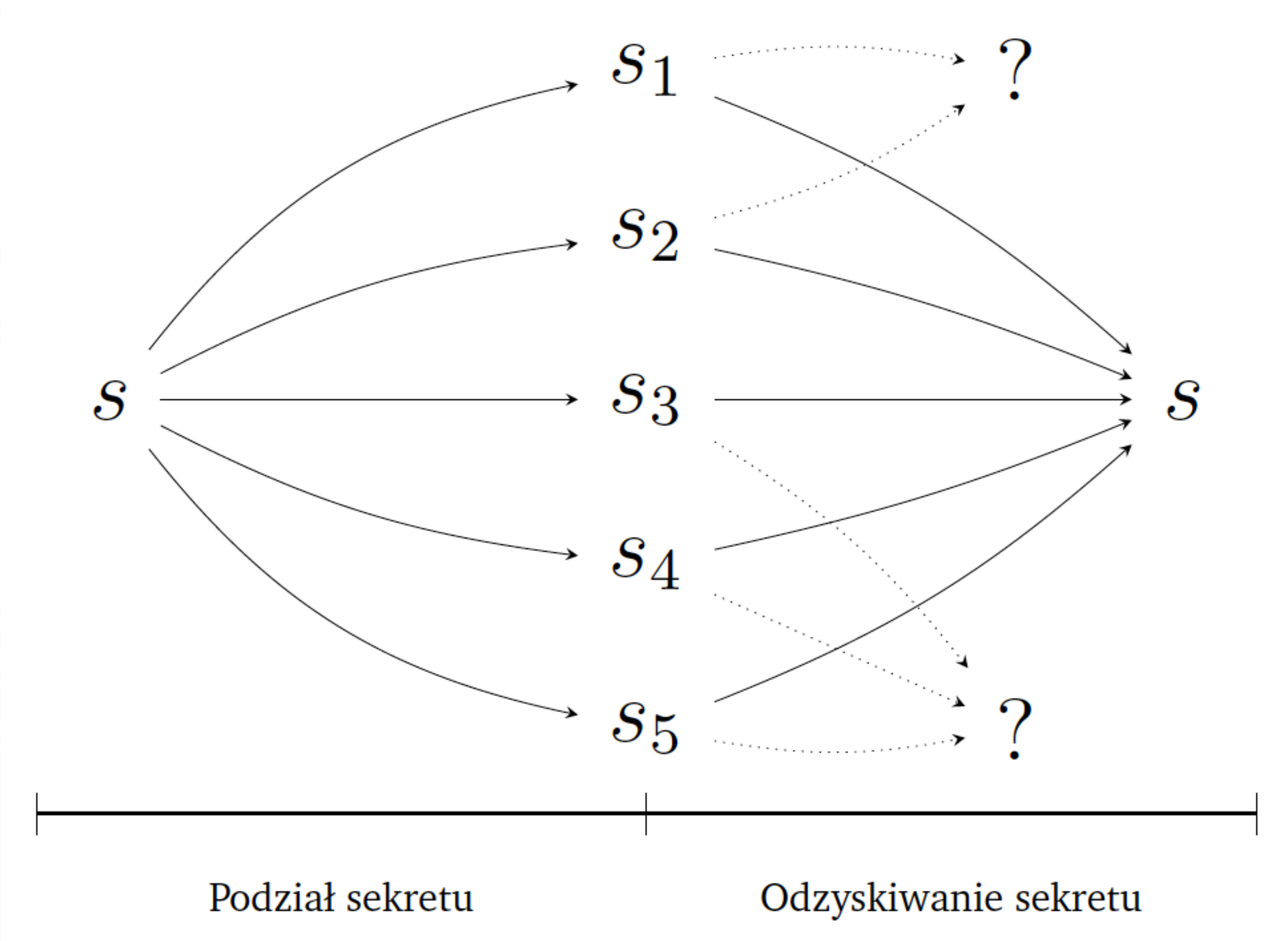
Klasyfikacja metod

- Weryfikowalne (*ang. Verifiable secret sharing*) - są rozszerzeniem metod efektywnych, umożliwiają zweryfikowanie prawidłowości udziałów, a jeśli udział został sfałszowany, mogą umożliwić wskazanie oszusta
- Proaktywne (*ang. Proactive secret sharing*) - metody umożliwiające okresowe aktualizowanie udziałów (obliczenie od nowa udziałów bez zmiany sekretu)

Metoda trywialna

Uwaga:
wszystkie udziały powinny mieć pełną długość.

Dlaczego?



Metoda trywialna - wymagane wszystkie udziały

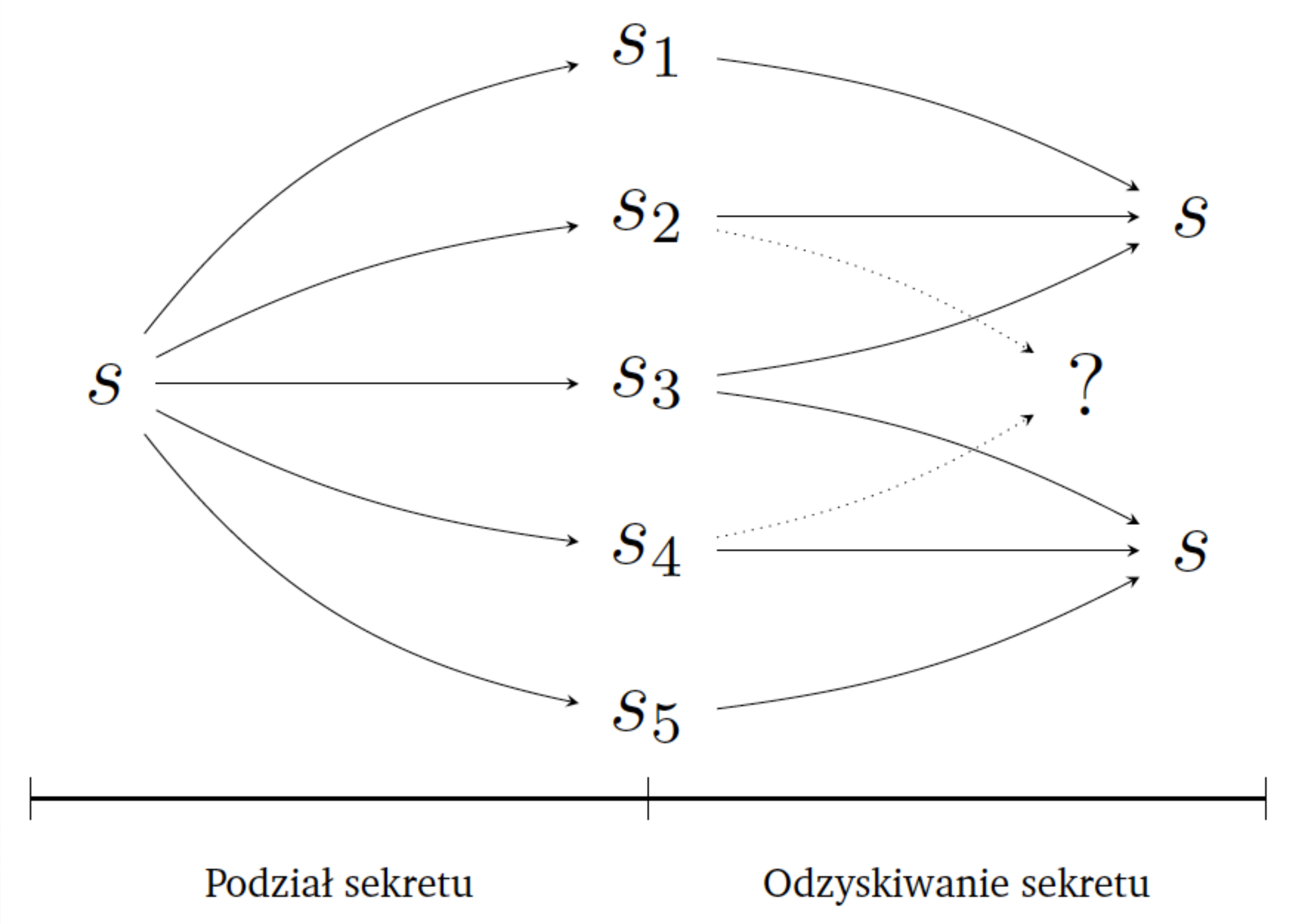
- Sekret reprezentowany jest za pomocą liczby całkowitej s z zakresu (0, k-1)
- Udziały s_1, s_2, …, s_{n-1} są generowane losowo, każdy z nich jest równy liczbie mniejszej od k. Ostatni udział obliczany jest z wykorzystaniem wzoru:

$$s_n = (s - s_1 - s_2 - \ldots - s_{n-1}) \ mod \ k$$

- Mając wszystkie udziały można odzyskać sekret podstawiając do wzoru:

$$s = (s_1 + s_2 + \ldots + s_n) \ mod \ k$$

Schemat progowy Shamira (t, n)



Schemat progowy Shamira (t, n)

Metoda została oparta na interpolacji wielomianowej Lagrange'a

Wiadomo, że:

- Dwa punkty jednoznacznie wyznaczają linię prostą,
- Trzy punkty są konieczne w celu odwzorowania paraboli
- Istnieje jeden i tylko jeden wielomian $f(x)$ stopnia $t-1$, taki, że dla każdego i zachodzi równość $f(x_i) = y_i$

Algorytm rozdzielający

Aby podzielić sekret s na n udziałów $s_1, s_2, \ldots, s_n$ należy wygenerować losowy wielomian stopnia $t\text{-}1$, w którym sekret jest równy wyrazowi wolnemu

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

Algorytm:

1. Wygeneruj losową, dużą liczbę pierwszą p taką, że $p > s$, $p > n$

2. wybierz t-1 losowych liczb $a_1, a_2, \ldots, a_{t-1}$

Algorytm rozdzielający

3. Dla każdego $i = 1, 2, \ldots, n$ oblicz:

$$s_i = s + \sum_{j=1}^{t-1} a_j x^j \bmod p$$

4. Każdy z udziałów reprezentowany jest jako para współrzędnych:

$$(x, y) = (x, f(x)) = (i, s_i)$$

Algorytm łączący

Sekret można odtworzyć na dwa sposoby. Pierwszy z nich polega na rozwiązaniu układu t równań liniowych:

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

Drugą z możliwości jest wykorzystanie wielomianu interpolacyjnego Lagrange'a:

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

Przykład

Sekret wynosi 954 ($s = 954$). Zostanie podzielony na 4 fragmenty ($n = 4$), z których 3 będą wymagane do jego odtworzenia ($t = 3$). Losowo wygenerowane zostały stałe:

- $P = 1523$,
- $a_1 = 352$
- $a_2 = 62$

Otrzymamy wielomian drugiego stopnia ($t - 1$):

$$f(x) = a_2x^2 + a_1x^1 + a_0 = 62x^2 + 352x^1 + 954$$

Obliczenie udziałów

$s_1 = f(1) = 62x^2 + 352x^1 + 954 \; mod \; 1523 = 1368$

$s_2 = f(2) = 62x^2 + 352x^1 + 954 \; mod \; 1523 = 383$

$s_3 = f(3) = 62x^2 + 352x^1 + 954 \; mod \; 1523 = 1045$

$s_4 = f(4) = 62x^2 + 352x^1 + 954 \; mod \; 1523 = 308$

Łączenie udziałów/odzyskanie sekretu

Metoda I

Do odtworzenia sekretu wykorzystano udziały s_1, s_3, s_4, rozwiązując układ równań:

$$1368 = a_0 + a_1 + a_2 \bmod 1523$$

$$1045 = a_0 + 3a_1 + 9a_2 \bmod 1523$$

$$308 = a_0 + 4a_1 + 16a_2 \bmod 1523$$

Wyznaczone wartości: $a_2 = 62$, $a_1 = 352$, $a_0 = s = 954$

Obliczenie sekretu z interpolacji wielomianowej

Do obliczeń wykorzystano punkty: $(x_0, y_0) = (2, 383)$, $(x_1, y_1) = (3,1045)$, $(x_2, y_2) = (4, 308)$:

$$\ell_0(x) = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x-3}{2-3} \cdot \frac{x-4}{2-4} = \frac{x^2 - 7x + 12}{2} = \frac{1}{2}x^2 - \frac{7}{2}x + 6$$

$$\ell_1(x) = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x-2}{3-2} \cdot \frac{x-4}{3-4} = \frac{x^2 - 6x + 8}{-1} = -x^2 + 6x - 8$$

$$\ell_2(x) = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x-2}{4-2} \cdot \frac{x-3}{4-3} = \frac{x^2 - 5x + 6}{2} = \frac{1}{2}x^2 - \frac{5}{2}x + 3$$

cd..

Powstałe wielomiany $l_0(x)$, $l_0(x)$, $l_0(x)$ należy pomnożyć przez odpowiadające im współrzędne y_0, y_1, y_2.

Interesują nas tylko wyrazy wolne wielomianów $y_0l_0(x)$, $y_1l_1(x)$, $y_2l_2(x)$, ponieważ ich suma:

$$y_0l_0(x) + y_1l_1(x) + y_2l_2(x) \text{ (mod 1523)} = s$$

Dla rozpatrywanego przykładu:

(775+778+924) mod 1523 = 954

Właściwości

1. Jeżeli t nie ulega zmianie, można dodawać nowe fragmenty poprzez obliczenie wartości wielomianu $f(x)$ w kolejnym, unikalnym punkcie

2. Fragmenty s_i można zmodyfikować bez zmiany sekretu s. W tym celu należy wyznaczyć nowy wielomian $f(x)$ z takim samym jak poprzednio wyrazem wolnym a_0. Często zmiana tego typu pomaga zwiększyć bezpieczeństwo. Atakujący musiałby zebrać potrzebną liczbę udziałów z danego okresu czasu, ponieważ tylko połączenie udziałów pochodzących z tego samego wielomianu pozwoli odzyskać sekret.

Kryptografia wizualna

Przykład metody podziału sekretu na obrazach

- Schemat podziału sekretów
- Szyfrowanie obrazów
- Naor i Shamir - Eurocrypt’94 - przedstawili sposób kodowania obrazów czarno-białych przy pomocy n-udziałów
- odkodowanie odbywa się za pomocą wzroku

Naor M., Shamir A.: Visual Cryptography. Advances in Cryptology – Eurocrypt ‘94,

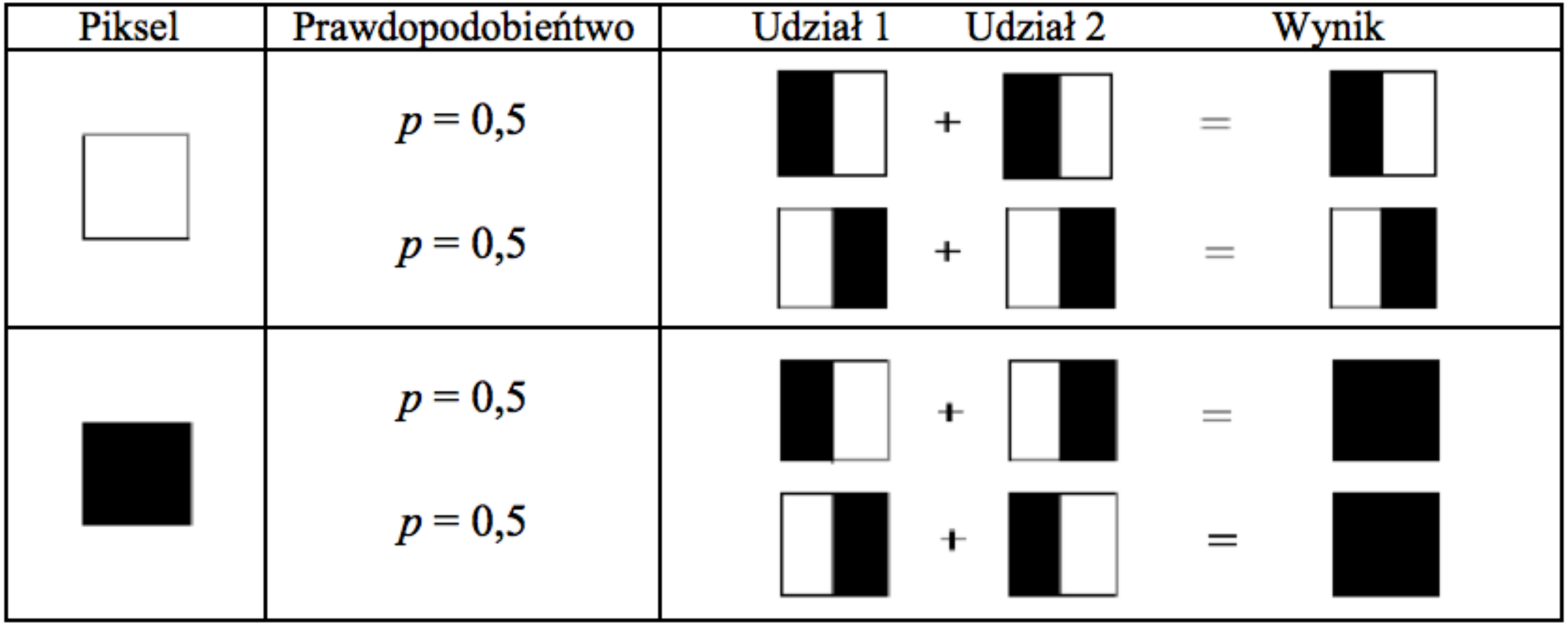
Podział sekretu (t, n)

Sekret 1

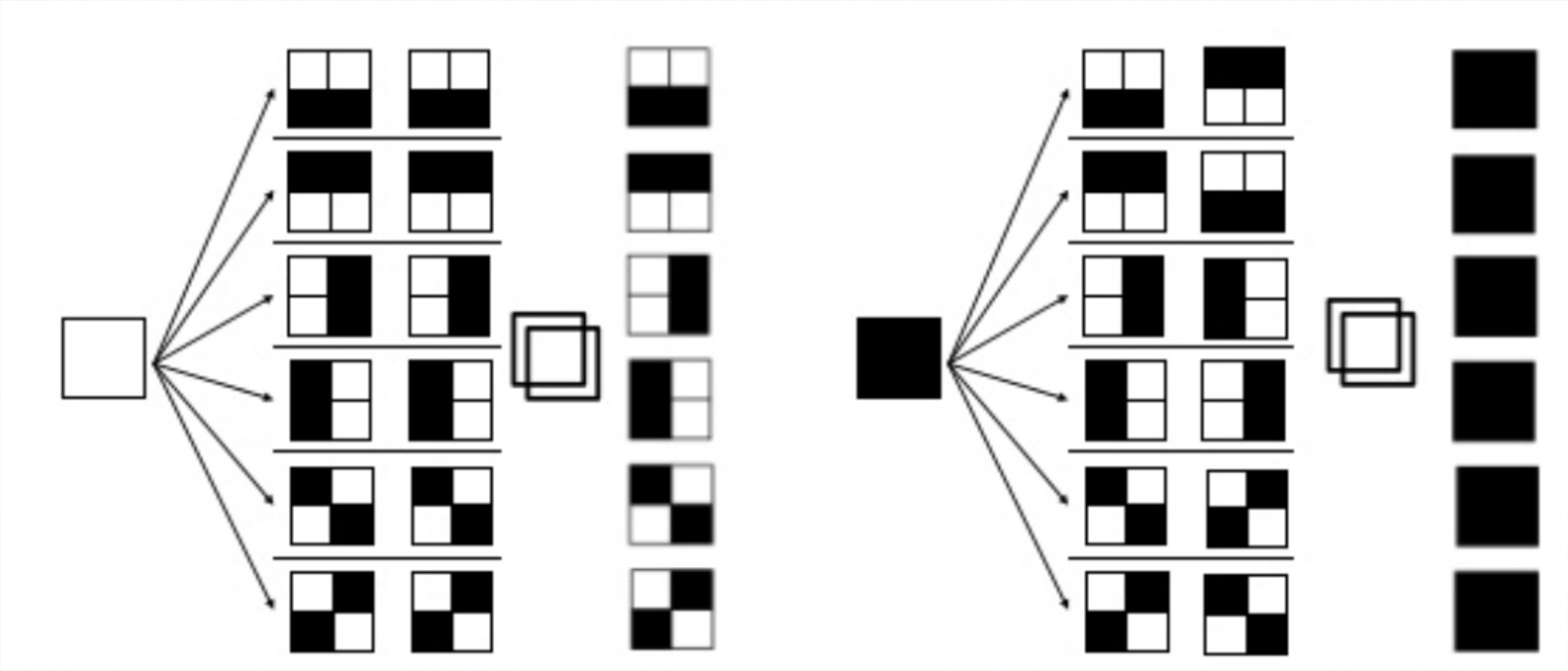
Sekret 2

Sekret 1+2

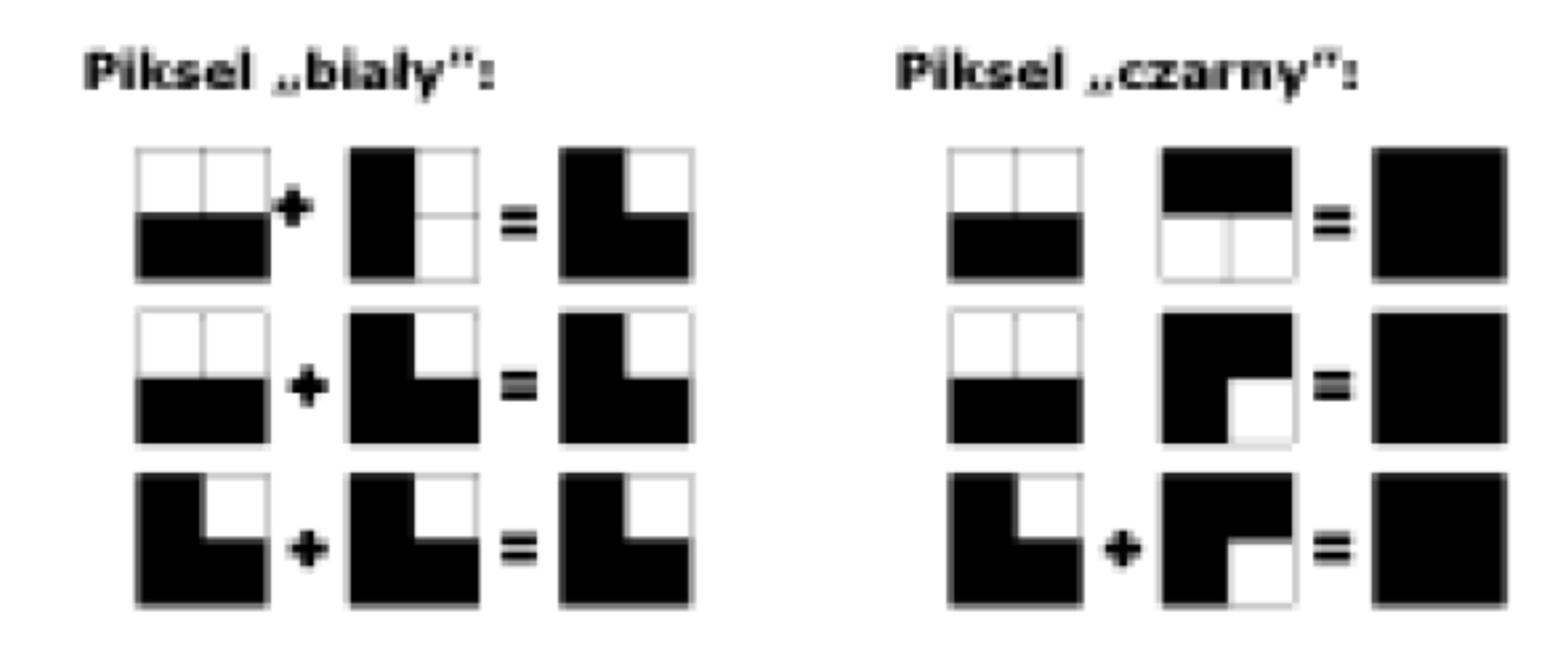
Algorytm podziału na udziały (1 piksel na 2 piksele)



Algorytm podziału (1 na 4)



MODYFIKACJE



Kryptografia wizualna - zalety

- łatwa implementacja
- nie jest potrzebny program deszyfrujący
- możemy wysłać udział mailem
- sekret rozszyfrowywany jest „w mgnieniu oka”

Kryptografia wizualna - wady

- odszyfrowany sekret posiada „zakłócenia”
- trzeba bardzo dokładnie dopasować folie
- rozmiar odszyfrowanego sekretu jest różny od oryginału

Jak ocenić bezpieczeństwo Kryptografii Wizualnej?

Akademia Innowacyjnych Zastosowań Technologii Cyfrowych (AI-TECH) projekt finansowany z środków Programu Operacyjnego Polska Cyfrowa POPC.03.02.00-00-0001/20

Fundusze Europejskie
Polska Cyfrowa

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Rozwoju Regionalnego