Ataki kanałem bocznym

Patryk Iwasiuk & Damian Krata

20.03.2019

Idea ataku kanałem bocznym

- pomiar charakterystyk pracy urządzenia podczas realizacji potoku obliczeniowego:
  1. zmierzenie czasu realizacji operacji kryptograficznych,
  2. zmierzenie poboru mocy urządzenia,
  3. zmierzenie oddziaływania elektromagnetycznego emitowanego przez urządzenie,
- oddziaływanie na urządzenie podczas wykonywania potoku obliczeń poprzez:
  1. zmiany prądu zasilania,
  2. rozstrajanie zegara taktującego urządzenie,
  3. naświetlanie układu promieniowaniem rentgenowskim lub promieniowaniem podczerwonym,
  4. oddziaływanie promieniowaniem elektromagnetycznym innego urządzenia.

Ze względu na sposób ingerencji w urządzenie wyróżniamy:

1. ataki inwazyjne (ang. *invasive attacks*), w których adwersarz ma możliwość uzyskania bezpośredniego dostępu do elementów układu znajdujących się w jego wnętrzu,
2. ataki nieinwazyjne (ang. *non-invasive attacks*) - atakujący nie ma dostępu do wewnętrznych elementów układu, może jedynie wykonywać pomiary działania, obserwacje danych wejściowych i wyjściowych układu oraz oddziaływać na urządzenie jedynie w sposób zdalny (poprzez np. zakłócanie napięcia zasilania),
3. ataki półinwazyjne (ang. *semi-invasive attacks*), w których adwersarz nie posiada bezpośredniego dostępu, niemniej jednak jest w stanie pozbawić układ wszystkich warstw ochronnych, uzyskując dostęp do układów mikroprocesorowych.

Ze względu na metodę oddziaływania na urządzenie rozróżniamy:

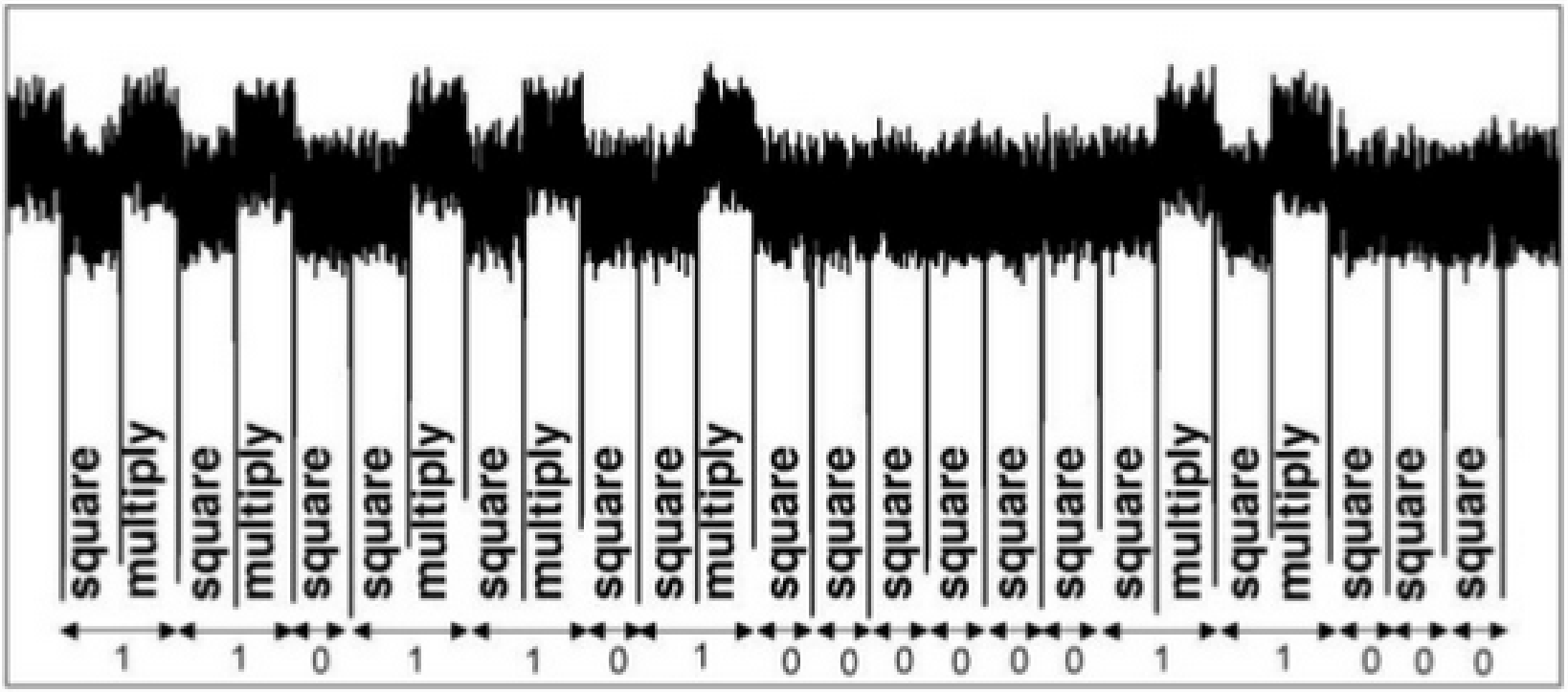
1. ataki pasywne (ang. *passive attacks*), w których atakujący prowadzi jedynie obserwacje działanie układu, nie ingerując w jego elementy wewnętrzne, zasoby oraz komponenty,
2. ataki aktywne (ang. *active attacks*), w których atakujący może wykonywać dodatkowe czynności (np. zakłócać napięcie zasilania, przykładać pole elektromagnetyczne) i analizować reakcje układu na te czynności.

Modele pomiaru emisji urządzeń

- odległość Hamminga,
- waga Hamminga.

$$HD(V_1, V_2) = HW(V_1 \oplus V_2)$$

Przykład praktyczny



Rodzaje ataków

- SPA
- DPA

SPA

Atak Bezpośredniej analizy poboru mocy jest skuteczny w przypadku algorytmów, w których wykonanie się dalszego potoku obliczeń zależy od przetwarzanych danych i może być różne dla różnych danych wejściowych. W szczególności operacjami wrażliwymi są:

1. przesunięcia (rotacje) i permutacje,
2. instrukcje warunkowe, których argument wpływa na wybór ścieżki obliczeń. W przypadku przedstawionym powyżej, dla pozycji wykładnika równej 1, realizowane było mnożenie, natomiast dla 0 podnoszenie do kwadratu,
3. mnożenia, dla których pobór prądu zależy od specyficznych właściwości operandów,
4. potęgowania wykonywane przy pomocy algorytmów *square and multiply*, np. dla RSA.

DPA

- Przeprowadzenie pomiarów dla znanych danych wejściowych,
- minimalizacja zakłóceń zewnętrznych poprzez uśrednienie wyników,
- ustalenie funkcji wyboru i wyprowadzenie hipotezy,
- podział pomiarów na podzbiory na podstawie funkcji wyboru,
- wyznaczenie średniej dla każdego podzbioru,
- konfrontacja wyników z hipotezą.

Y = AB, LSB = 1

Y = 32, LSB = 0

Y = 81, LSB =1

Y = 9A, LSB = 0

Y = 9F, LSB = 1

Y = 90, LSB = 0

AVERAGE

DIFFERENCE

Y = AB, LSB = 1

Y = 32, LSB = 0

Y = 81, LSB =1

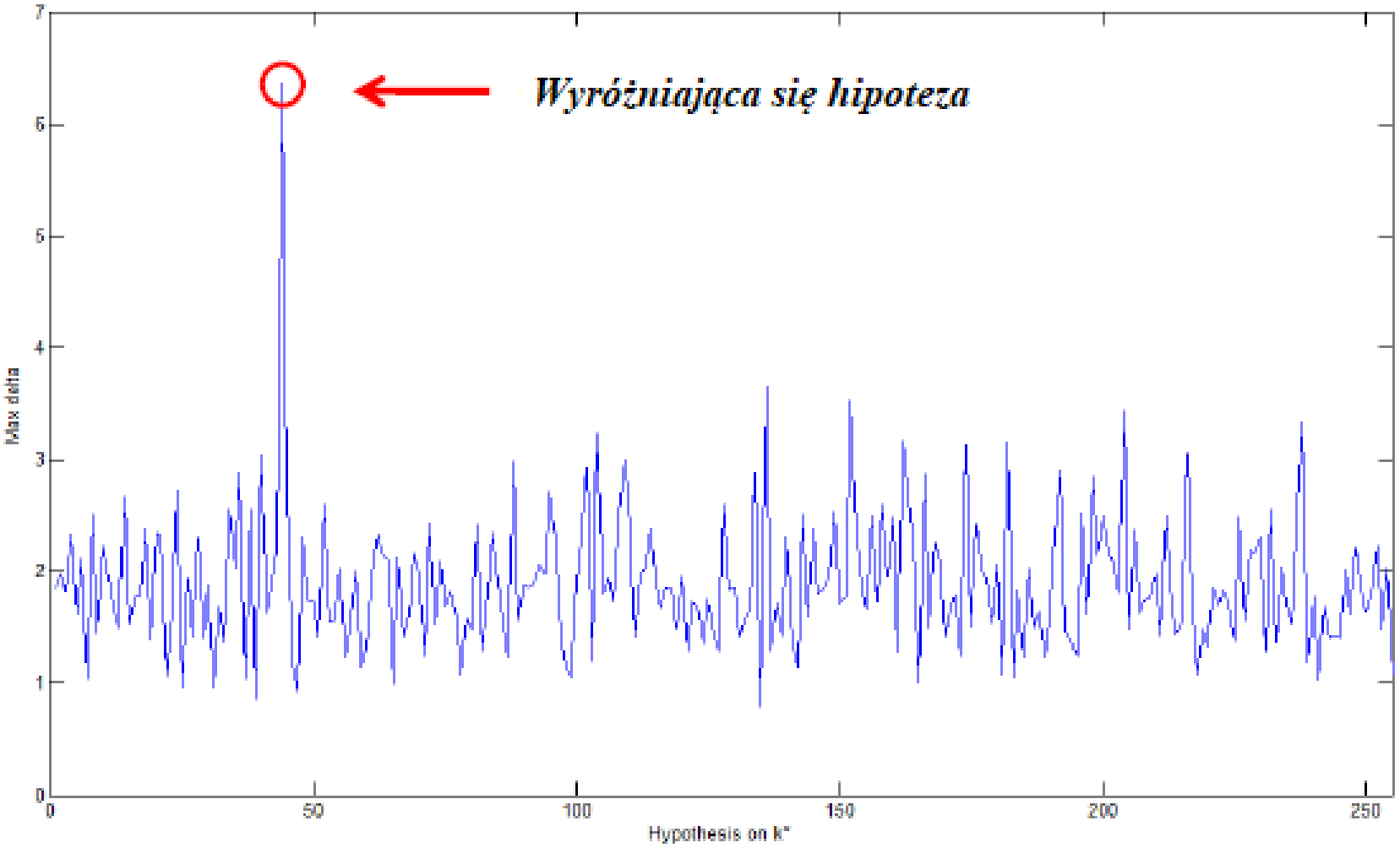
Y = 9A, LSB = 0

Y = 9F, LSB = 1

Y = 90, LSB = 0

AVERAGE

DIFFERENCE


Wyróżniająca się hipoteza
Max delta
Hypothesis on k*
0
1
2
3
4
5
6
7
0
50
100
150
200
250

Dziękuję za uwagę!