Artur Karpiński

Studium możliwości zastosowania technik *hashcash* dla ograniczenia transmisji nielegalnych komunikatów w sieciach bezprzewodowych

CEL PRACY

Zastosowanie technik *hashcash* w sieciach bezprzewodowych

- Sztuczne zwiększanie kosztu transmisji przy pomocy funkcji umiarkowanie złożonych (funkcje skrótu);

- Protokół wg schematu wyzwanie-odzew (ang. *challenge-response)*, ogólne zasady i etapy jego działania;

- Wpływ generowania skrótów typu SHA-1 na wydajność sprzętu;

- Wyniki badań stosowania technik *hashcash*.

SYSTEM REPUTACJI

Opracowany w pracy **protokół** oparty na systemie reputacji.

•niska reputacja - odrzucenie połączenia i obniżenie reputacji;

•wysoka reputacja - akceptacja połączenia i wzrost reputacji.

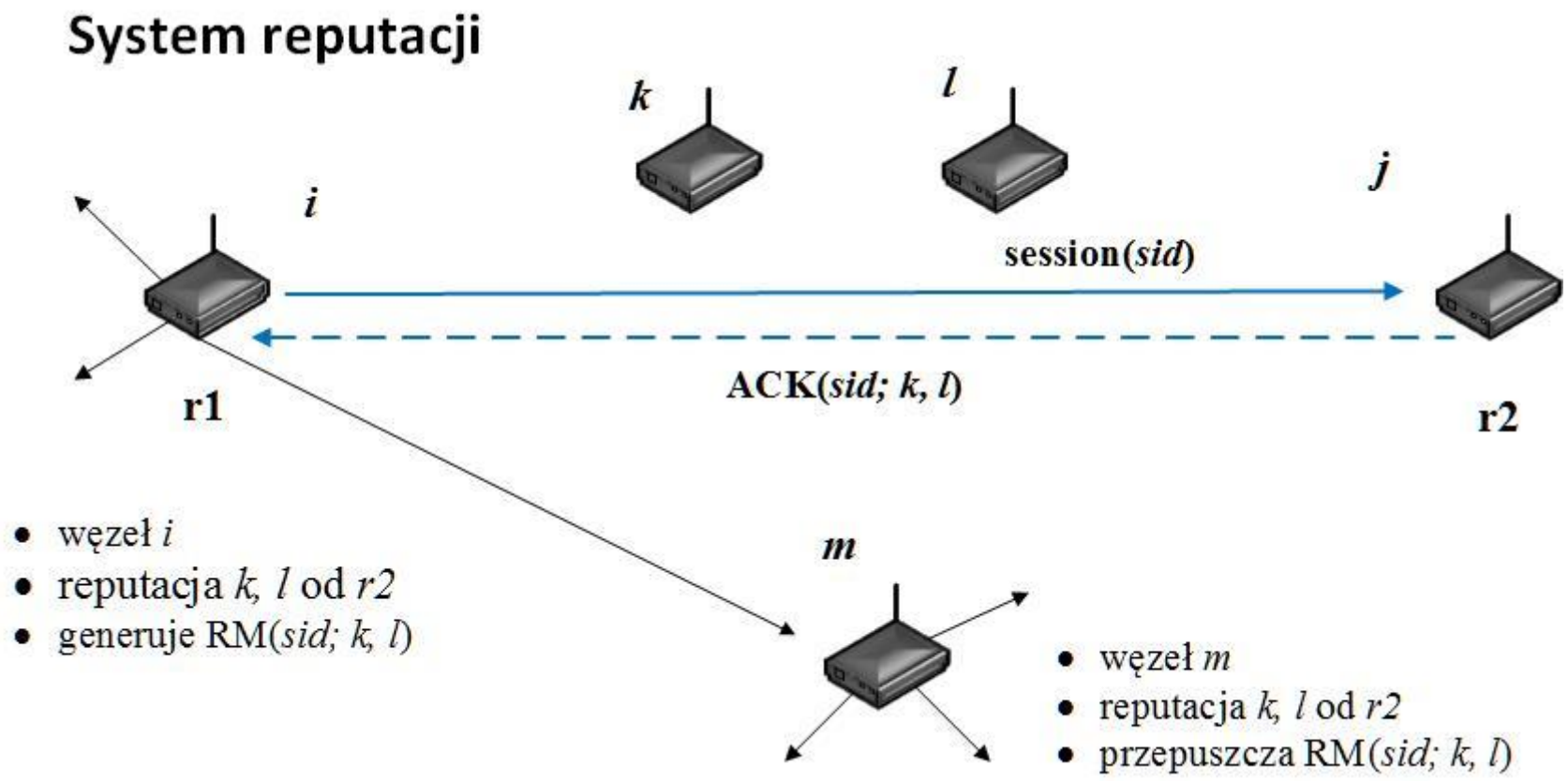
Zalety stosowania systemu reputacji:

•wzrost szybkości nawiązywania nowych połączeń;

•mniejsze ryzyko ataku ze strony nieznanego węzła;

•spadek fałszywych rekomendacji w systemach reputacji.

SCHEMAT DZIAŁANIA **SYSTEMU REPUTACJI**



ATAKI NA SYSTEMY REPUTACYJNE

Dla zwiększania poziomu wiarygodności w protokole opracowanym w pracy atakujący może stosować:

- **atak autopromocji** (ang. *Self-Promoting*) - manipulacja własną reputacją fałszywie ją zwiększając przez promocję w sieci;

- **atak egoistyczny** (ang. *Self-Serving or Whitewashing*) – atakujący w innym systemie poprawia poziom reputacji;

- **atak zorganizowany, skoordynowany** (ang. *Orchestrated*) - zgranie kilku strategii działania;

ZASADA HASHCASH

Dowód wykonania operacji obliczeniowej na funkcji haszującej.

•Celem **funkcji kosztów** (ang. *hashcash*) jest otrzymanie konkretnego **dowodu wykonanej pracy** (ang. *proof-of-work*).

•Na zasadzie **wyzwanie-odzew** przekazywany jest poprawny (?) wynik jako dowód wykonanej pracy.

•**Funkcja skrótu** (ang. *hash*) daje dowód konkretnej pracy przez dodanie **pieczęci tekstowej** do przesyłanych informacji przed próbą połączenia.

DOWÓD PRACY

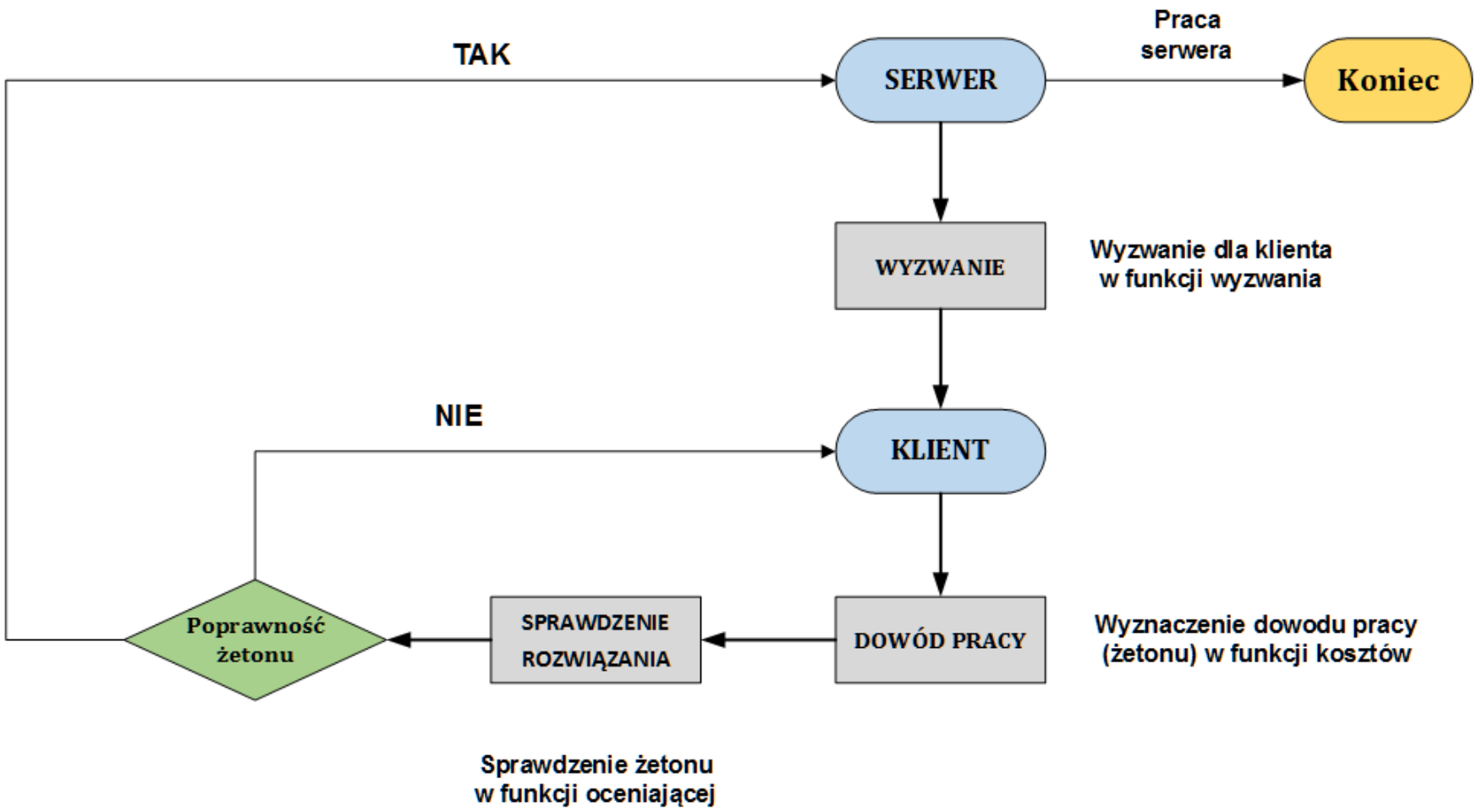
- Wykonanie określonej pracy i przekazania odbiorcy dowodu na to (wynik obliczeń na funkcji haszującej).

- Trudniej rozwiązać przez nadawcę zadanie niż sprawdzić przez odbiorcę.

- Praca dla nadawcy umiarkowanie złożona, ale możliwa do wykonania.

- Odbiorca małym kosztem obliczeniowym sprawdza czy pieczęć jest ważna.

Weryfikacja funkcji kosztów



Weryfikacja funkcji kosztów

- Weryfikacja funkcji haszującej po stronie odbiorcy prosta, ale obliczenie **funkcji skrótu** (np. SHA-1) po stronie nadawcy wymaga większego wysiłku.

- Nadawca przygotowuje nagłówek, dodaje do niego wyznaczony losowo ciąg i oblicza pieczęć *hashcash* (160-bitowy SHA-1 nagłówka).

- Wiadomość akceptowana, gdy ustalona liczba pierwszych bitów nagłówka dla SHA-1 jest zerowa, w przeciwnym wypadku sprawdza inny losowo generowany ciąg.

Główne cechy **prawidłowo generowanej pieczęci** typu *hashcash*:

- do wykorzystania tylko jeden raz,
- odbiorca ma bazę pieczęci otrzymanych z wiadomościami,
- sprawdzane daty pieczęci,
- zmiana daty wymaga nowej pieczęci,
- nie uznawane pieczęcie z przyszłą datą,
- nie można wykorzystać przeterminowanych pieczęci.

Kolejne etapy schematu **Wyzwanie-Odzew**

Wyzwanie - Odzew

Schemat **WYZWANIE-ODZEW** (ang. *challenge-response*)

Wyzwaniem może być obliczenie oparte na **funkcji haszującej**.

Obliczenie wartości funkcji z określonego argumentu o wiele prostsze niż wyznaczenie argumentu funkcji, który da określoną wartość.

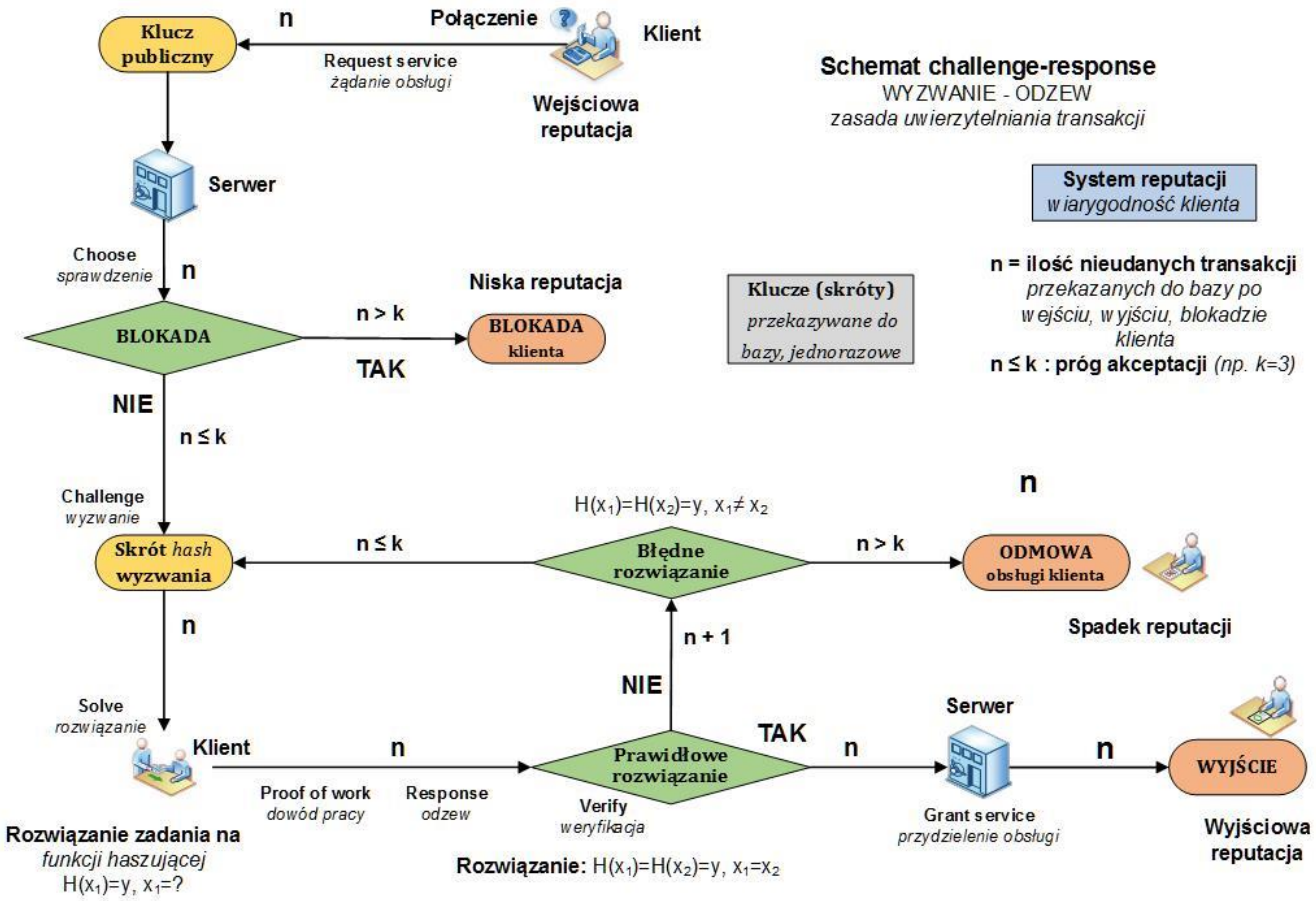
Ze wzrostem liczby początkowych bitów zerowych wzrasta wykładniczo ilość możliwych liczb do sprawdzenia i trudność zadania.

Liczba podana przez klienta jako rozwiązanie zadania i liczba użyta przy wyznaczaniu zadania po stronie serwera, muszą być identyczne.

$\mathbf{H(s_1)=H(s_2) \Rightarrow s_1=s_2}$

PRZYKŁADOWY PROTOKÓŁ WYKORZYSTUJĄCY SCHEMAT CHALLENGE-RESPONSE

Funkcje skrótu w systemie reputacji wykorzystywać można np. w banku dla weryfikacji wiarygodności klienta.



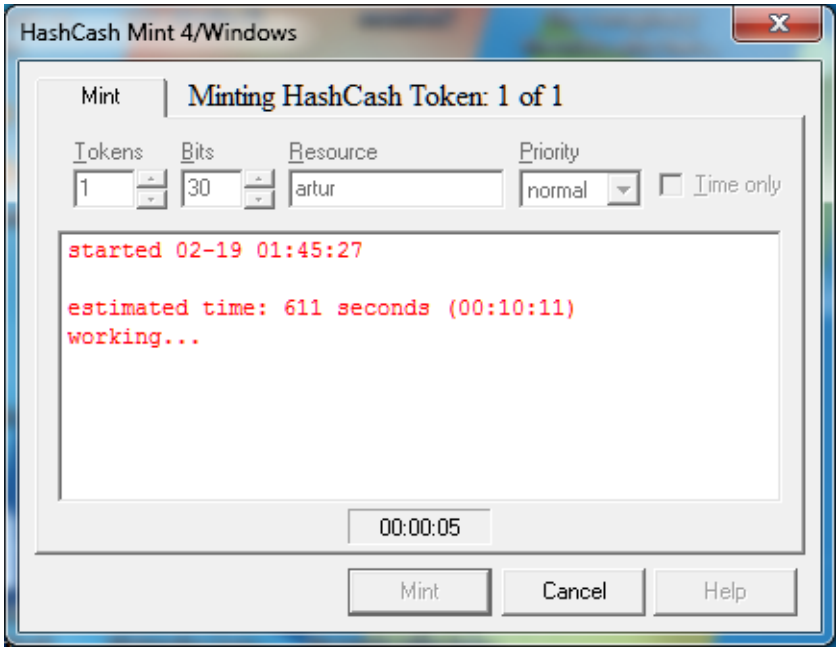
Pomiary na sprzęcie komputerowym:

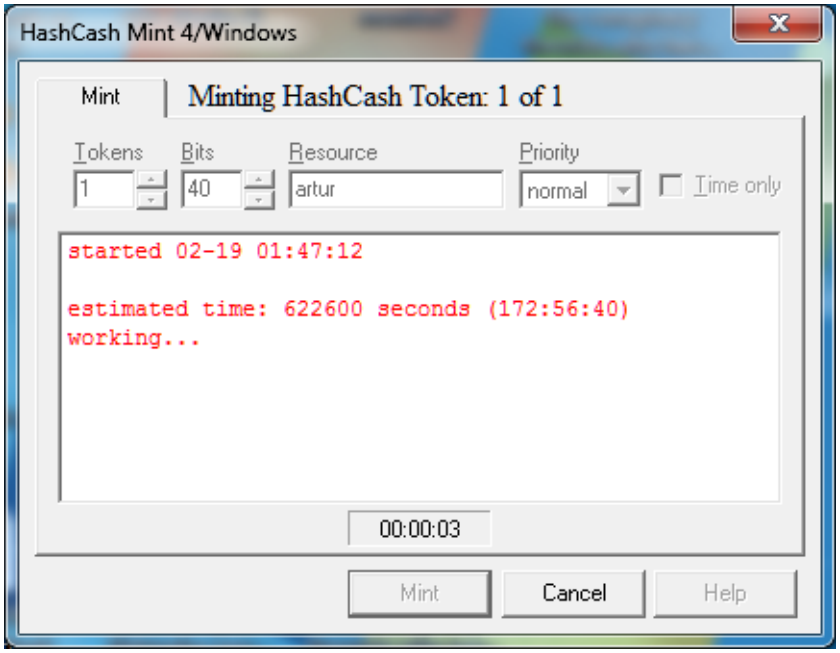
- komputer stacjonarny ze stałym zasilaniem, procesor 4-rdzeniowy;
- komputer przenośny Toshiba bez stałego zasilania, procesor 2-rdzeniowy.

Koszty transmisji, wydajności, zużycie baterii podczas generowania skrótów

- wpływ generowania skrótów na wydajność sprzętu, na którym wykonywane są obliczenia funkcji haszujących;
- obliczenia w algorytmie funkcji haszującej SHA-1.

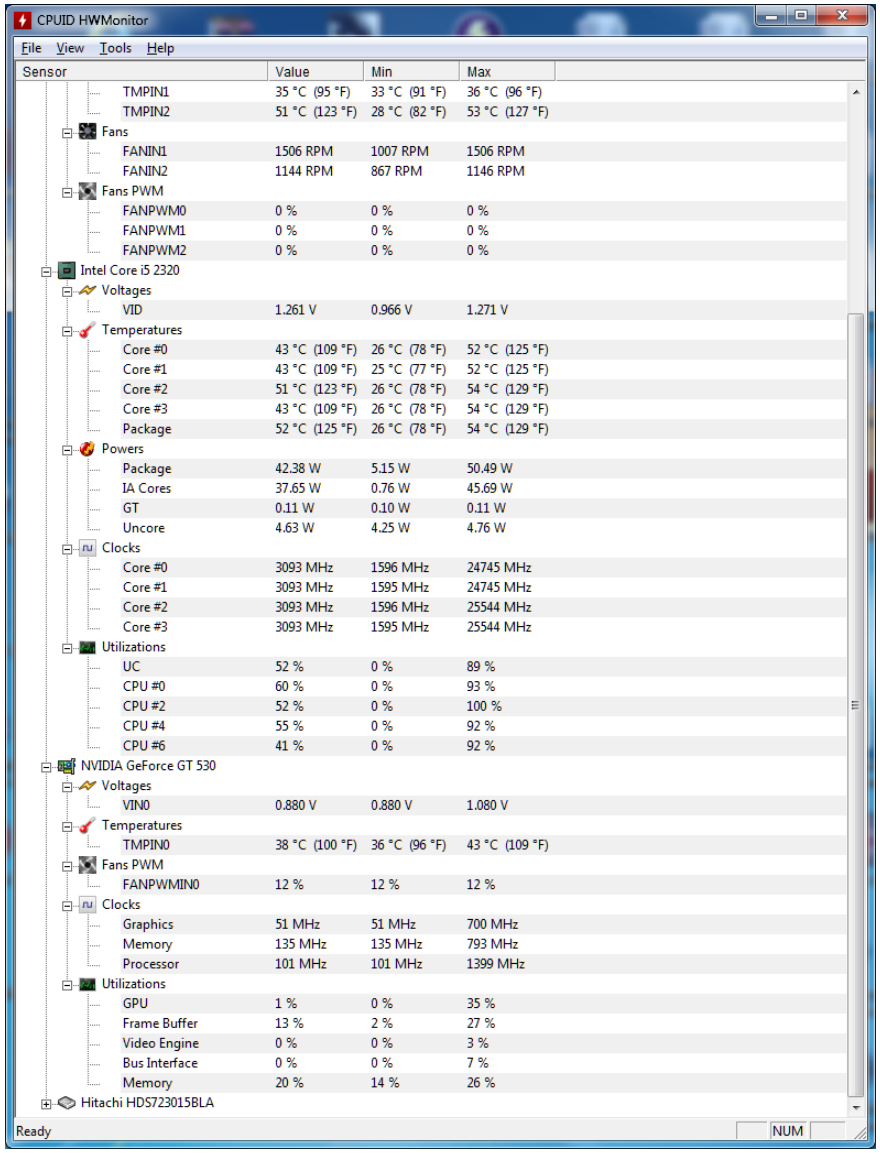
Czas generowania skrótów na programie **HashCash Mint** w zależności od liczby wymaganych bitów zerowych





Liczba bitów zerowych	Liczba skrótów	Czas generowania skrótów
25	1	15 sek.
25	10	2 min. 43 sek.
30	1	10 min. 11 sek.
40	1	176 godz. 35 min. 40 sek.

Program **HWMonitor** przy generowaniu skrótu typu **SHA-1**



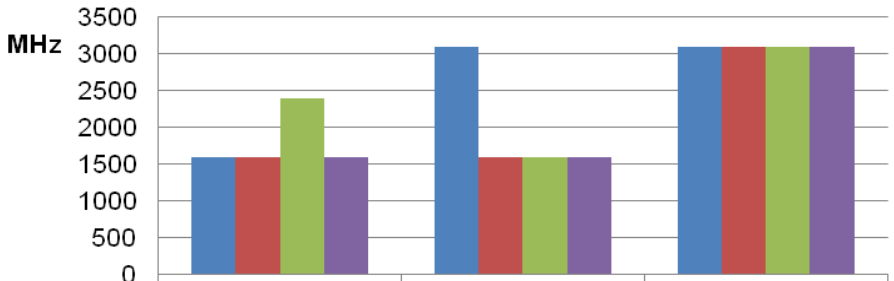
Pomiar wydajności komputera

- wentylator (obr./min)
- temperatura procesora
- moc zasilania (W)
- zegar procesora (MHz)
- zużycie procesora (%)

POLITECHNIKA GDAŃSKA
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

HWMonitor na **KOMPUTERZE STACJONARNYM** - 20, 27, 30 bitów zerowych

Zegar procesora: MHz

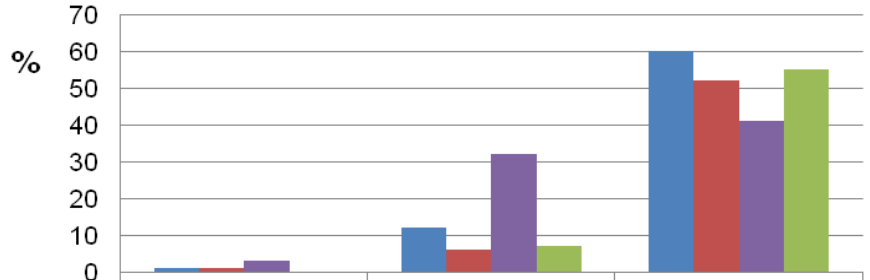


	20-bit	27-bit	30-bit
Core#0	1596	3093	3093
Core#1	1596	1596	3093
Core#2	2394	1596	3093
Core#3	1596	1596	3093

Moc zasilania: W

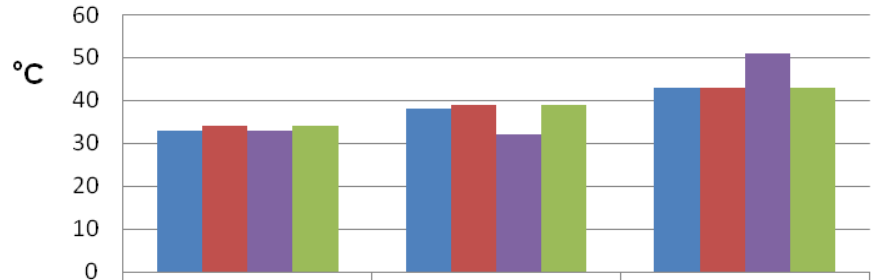
	20-bit	27-bit	30-bit
Power	6,16	11,95	42,38

Zużycie procesora: %



	20-bit	27-bit	30-bit
CPU#0	1	12	60
CPU#2	1	6	52
CPU#6	3	32	41
CPU#4	0	7	55

Temperatura procesora: °C



	20-bit	27-bit	30-bit
Core#0	33	38	43
Core#1	34	39	43
Core#2	33	32	51
Core#3	34	39	43

Badania na **KOMPUTERZE PRZENOŚNYM** bez stałego zasilania

Mniej wydajna praca od strony sprzętowej (token 30-bitowy):

- 2-krotnie dłuższy **czas generowania skrótu** (ok. 20 min.) niż na komputerze stacjonarnym (ok. 10 min.),
- większy wzrost **temperatury procesora**,
- maksymalne wykorzystanie mocy na procesorze, **zużycie procesora,**
- maksymalna częstotliwość **taktowania zegara,**
- duży wzrost **zużycia baterii** (czyli szybkość wyczerpania).

WNIOSKI Z CZĘŚCI BADAWCZEJ PRACY

- Spadek wydajności sprzętu przy generowaniu skrótów **SHA-1** na protokole wyzwanie-odzew z systemem reputacyjnym;
- Wykładniczy wzrost koszów przy wzroście stopnia trudności zadania (wymagane bity zerowe w skrócie);
- Jednoczesne obliczanie wielu skrótów wywołuje spadek wydajności;
- *hashcash* nie obniża wydajności użytkownika o wysokim stopniu reputacji;
- Niska reputacja nieuczciwego nadawcy zwiększa koszt połączenia.

POLITECHNIKA GDAŃSKA

111 LAT

POLITECHNIKA GDAŃSKA

WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

Katedra Teleinformatyki