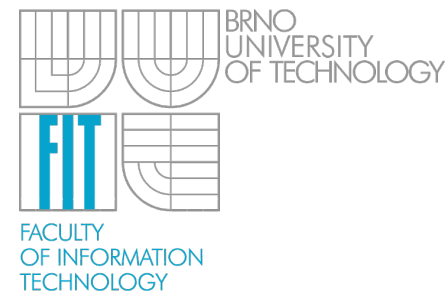


# Hardwarová akclerace algoritmů v počítačových sítích

Jan Kořenek

Brno University of Technology, Faculty of Information Technology  
Bozotechnova 2, 612 00 Brno, CZ  
<http://merlin.fit.vutbr.cz/ant/>



INVESTMENTS IN EDUCATION DEVELOPMENT

# Realizace algoritmu

## Algoritmus

- Hledání řetězců
- Šifrování dat
- Filtrace obrazu
- ...

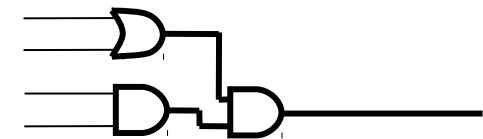
### Implementace pomocí programu



```
void main() {  
    ...  
    return 0;  
}
```

- Řízení programem
- Sekvenční zpracování programu na jednom nebo více procesorových jader

### Implementace pomocí hardwarové architektury



- Chování dáno zapojením obvodových prvků, které pracují paralelně
- Základní obvodové prvky se liší podle použité technologie – ASIC, FPGA, ...

# Paralelní zpracování

- **Příklad: Násobení matice rozměru ( $m \times n$ ) konstantou**



Implementace pomocí SW algoritmu

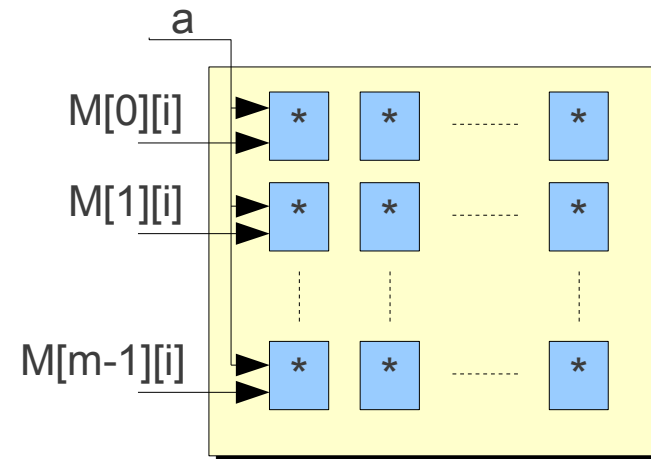
```
for (i=0; i<m; i++)  
  for (j=0; j<n; j++) {  
    D[i][j] = a * D[i][j];  
  }
```

- Procesorové jádro obsahuje v ALU **jednu násobičku**. V jednom kroku je vynásoben jeden prvek matice
- Celý výpočet bude hotov v  **$m \cdot n$  krocích**

**Kolik procent plochy procesoru je využito při výpočtu?**



Implementace pomocí hardwarové architektury



- Na čipu může být umístěno **a** vzájemně propojeno **více násobiček pracujících paralelně**.
- Pro  **$m$  násobiček** bude celý výpočet hotov v  **$n$  krocích** a pro  **$m \cdot n$  násobiček** v **1 kroku**

# Plocha na čipu

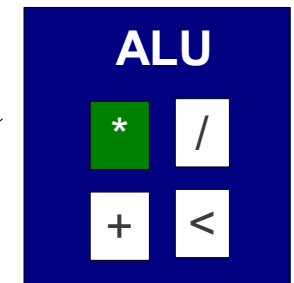
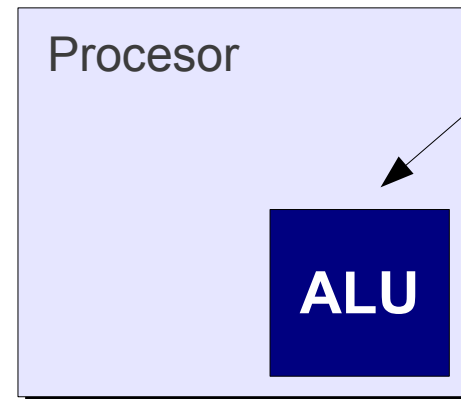
- **Příklad: Násobení matice konstantou**



Implementace pomocí SW algoritmu

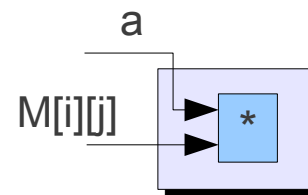
```
for(i=0;i<m;i++)
  for(j=0;j<n;j++){
    D[i][j] = a* D[i][j];
  }
```

- Procesorové jádro obsahuje v ALU **jednu násobičku**. V jednom kroku je vynásoben jeden prvek matice



Implementace pomocí hardwarové architektury

- Menší plocha na čipu
- Menší spotřeba energie



# Rozměry a příkon

## High Tech Cooling for Million Dollar Systems



Source: Roger Schmidt  
IBM Corp



**Příklad:** jeden FPGA čip je při analýze DNA sekvencí až 800x rychlejší než Intel Pentium Core 2 => **Jeden čip dokáže nahradit 800 počítačů**



K. Yazawa, Sony

- 400 Millions of Personal Computers world wide assumed to consume (Year 2000)  
0.16 Tera ( $10^{12}$ ) kWh per year  
→ equivalent to 26 Nuclear Power Plants
- Over 1 Giga kWh per year just for cooling with including manufacturing electricity [Bar-Cohen et al, 2000]

# Proč sítě a HW akcelerace?

- Časově kritické operace v počítačových sítích
  - **Filtrace paketů** - jak vybrat množinu pravidel nebo pravidlo, které odpovídá přijatému paketu?
  - **Hledání útoků** - Jak zajistit hledání tisíců regulárních výrazů v síťových tocích?
  - **Analýza paketů** - jak analyzovat hlavičky paketů a přesně určit umístění položek v hlavičce paketů?
  - **Stavové zpracování síťového provozu** - jak uchovat milióny záznamů o síťových tocích a zajistit vyhledání záznamu v konstantním čase?
- Výkonnost procesoru Intel Core2 Duo

Operace	Propustnost	1G	10G	40G	100G
Analýza paketů	14Gbps	✓	✓	STOP	STOP
Stavové zpracování prov.	6Gbps	✓	STOP	STOP	STOP
Filtrace paketů	1,3Gbps	✓	STOP	STOP	STOP
Hledání útoků (regex)	18Mb/s	STOP	STOP	STOP	STOP

*Výkonnost současných procesorů je nedostačující*

**Pro 10Gb linku je na zpracování jednoho paketu pouze 40 ns**

# Příklad: Detekce útoků na síti

- **Detekce nebezpečného provozu na počítačové síti**

- Programu Snort dokáže podle 17 tisíc řetězců (signatur) identifikovat podezřelý provoz na síti



## Implementace pomocí programu Snort

- Využití nejlepších známých algoritmů, podpora více jader
- SW implementace dokáže na současných procesorech zpracovat síťový tok do **18 Mb/s**

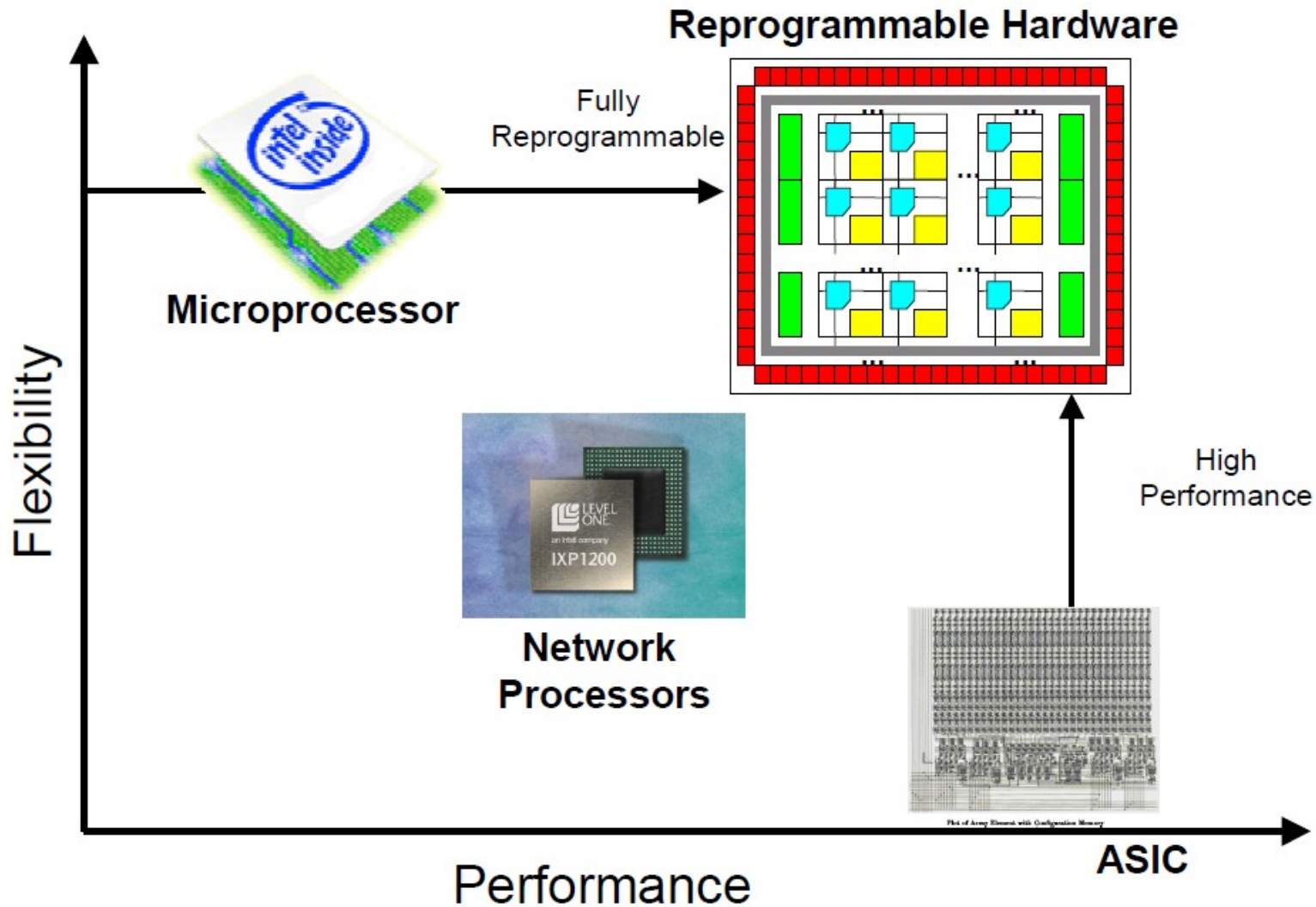
**Nelze použít pro sítě pracující na rychlosti 1 Gbps nebo 10 Gb/s!**



## Implementace pomocí hardwarové architektury

- Je možné **paralelně hledat řetězce** nebo **zpracovat více znaků v jenom kroku**
- S využitím technologie FPGA dosažena propustnost **10 Gb/s**,
- Speciální ASIC obvody dosahují rychlosti **40 Gb/s**

# Technologie pro síťové zařízení

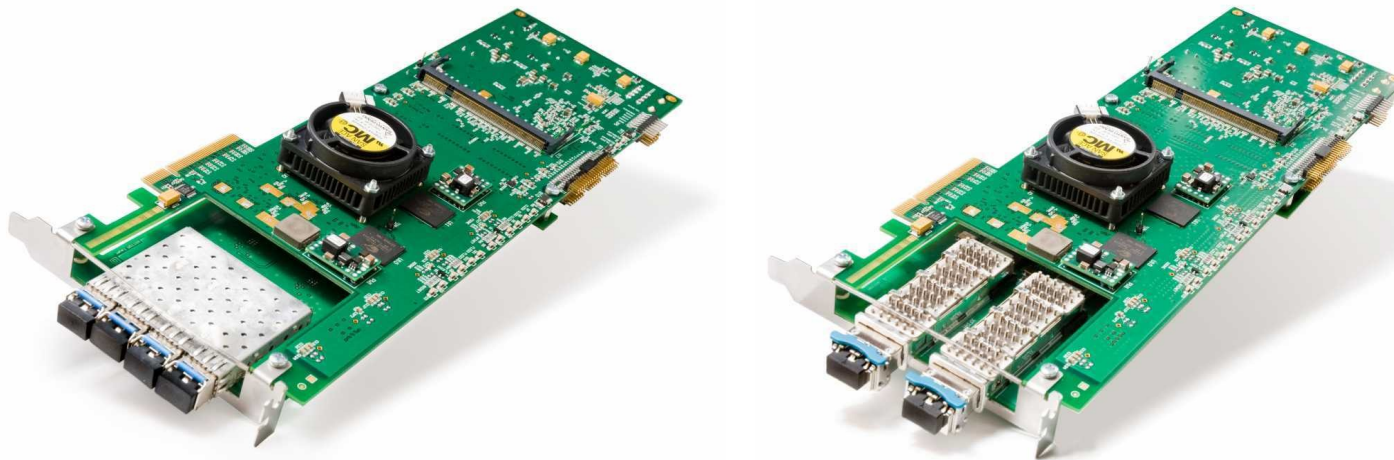


*John Lockwood, Stanford University*



# Výzkumný tým ANT@FIT

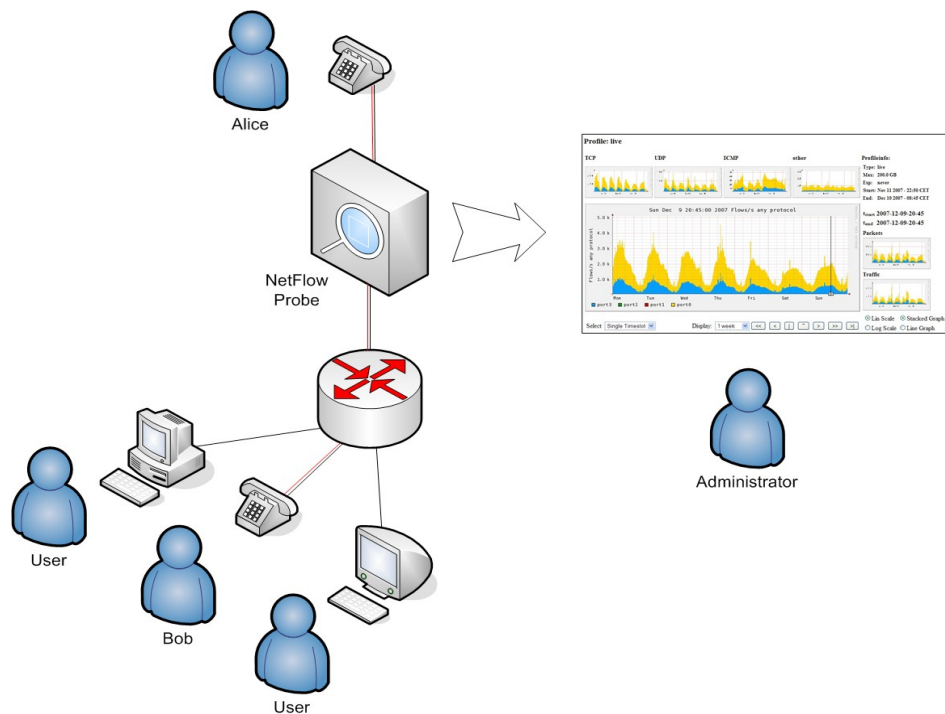
- Akcelerace algoritmů a architektur pro monitorování a bezpečnost vysokorychlostních sítí
  - Vývoj nových prototypů zařízení pro monitorování a bezpečnost počítačových sítí
  - Technologie pro 10, 40 a 100 Gbps sítě a vestavěné systémy
  - Optimalizace algoritmů a architektur pro **FPGA** a **MultiCORE**



# Cílové aplikace

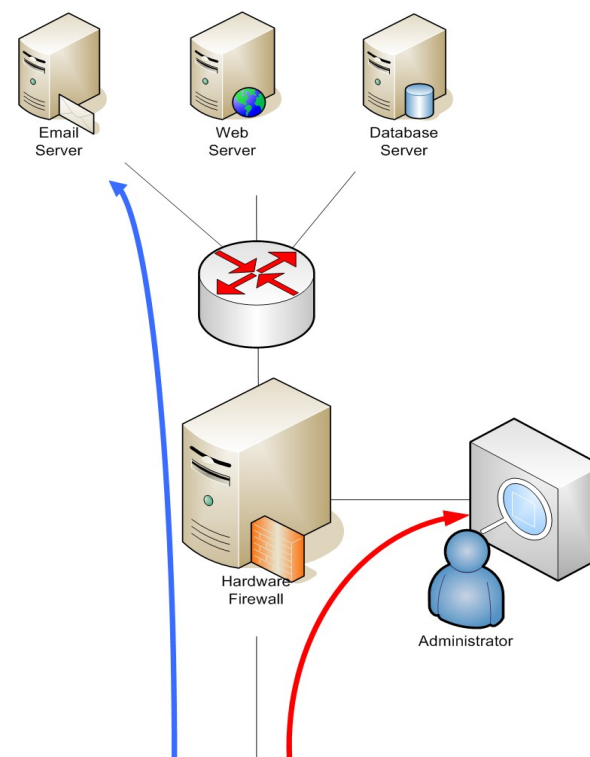
## Monitorovací sondy

- **Sledování provozu na síti**
  - Na rychlosti deset gigabitů a více
  - Vyhledávání anomálií
  - Sledování kvality spojení



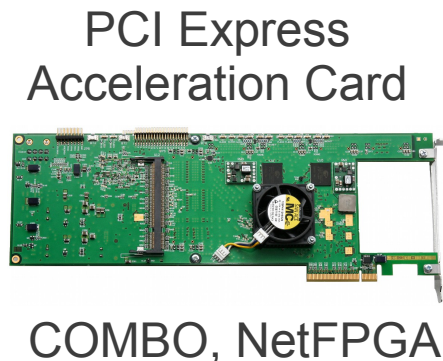
## Filtrování provozu

- **Filtrování a odposlech provozu**
  - Odposlech podezřelých aktivit
  - Filtrování škodlivého provozu



# Technologie a aplikace

- Vysokorychlostní síť s propustností 10, 40 a 100 Gb/s



- Hardware Firewall
- Linux Base Router
- NetFlow Probe
- Traffic Generator

- Vestavěné systémy – Ethernet, WiFi



Spartan-3E 1600E  
MicroBlaze Development Kit

- Veškerá funkce soustředěna na jeden čip FPGA
- V FPGA core procesoru MicroBlaze s OS Linux
- Časově kritické operace procesoru akcelerovány v logice FPGA

***Předpokládáme vývoj vlastní platformy  
pro vestavěné systémy***

# Vybrané výsledky skupiny

- **EU Projekt SCAMPI zachráněn před zrušením**
  - V roce 2003 vytvořena jedna z prvních monitorovacích 10 Gbps karet v Evropě
- **FlowMon sonda se stala součástí bezpečnostního balíčku doporučeného EU projektem GEANT2 k monitorování sítí**
- **Pravidelná účast na Xilinx Academic fóru**
- **Převedení výsledků vědy a výzkumu do praxe (INVEA-TECH)**
  - Monitorování vysokorychlostních sítí na bázi NetFlow
- **Individuální ocenění**
  - Junior Scientist Conference (2008)
  - IT Diplomka roku (2007, 2008)
  - Diplomová práce roku (2008)
  - Cena Josefa Hlávky (2008)



Kobierský, P.: Hardware Acceleration of Protocol Identification. The best MSc thesis in IT 2008 (Czech Rep.)

# Reference a spolupráce

- Spolupráce s akademickými institucemi



Stanford  
University



UNIVERSITY OF  
CAMBRIDGE

Computer  
Laboratory



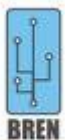
UVT MU



Czech  
NREN

- Nasazení vyvinuté technologie prostřednictvím spin-off společnosti INVEA-TECH

SURFnet



SWITCH

GRnet



CARnet  
CROATIAN ACADEMIC AND RESEARCH NETWORK

SLOANE PARK

SEZNAM



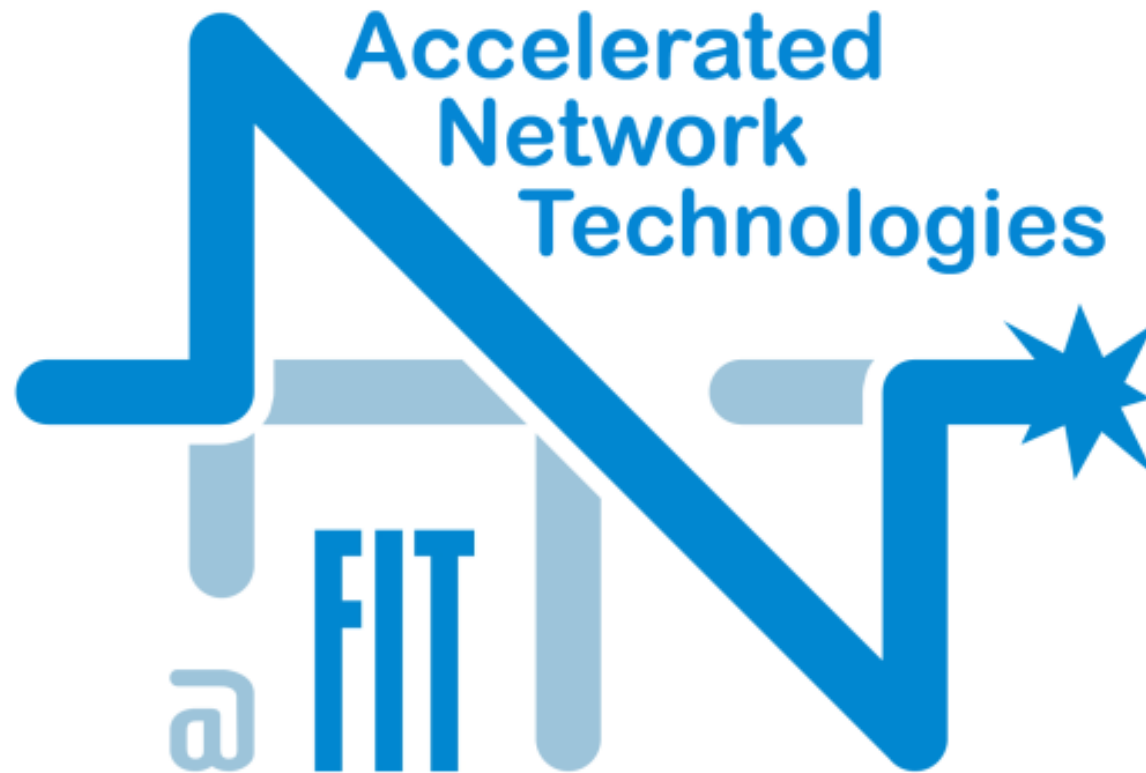
THE ACADEMY  
OF SCIENCES  
OF THE CZECH  
REPUBLIC



CO VISTA

CASABLANCA INT  
INTERNET EXPERIENCE

# Připojte se k naší skupině



## Research Group