CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

Zvyšování spolehlivosti a bezpečnosti číslicových obvodů na úrovni mikroarchitektury

Jan Bělohoubek

jan.belohoubek@fit.cvut.cz

ČVUT v Praze

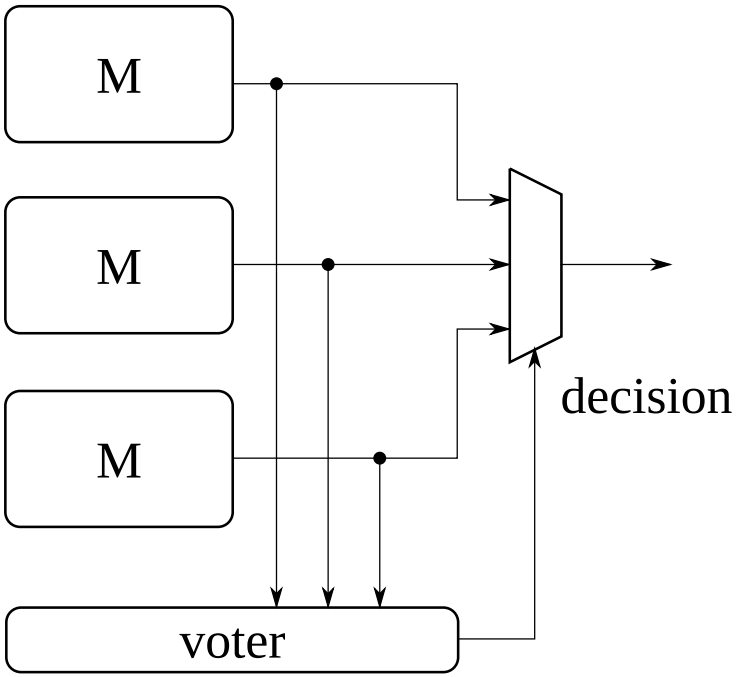
4. ročník

Školitel: Petr Fišer, specialista: Jan Schmidt

PAD 2018, Stachy – Zadov

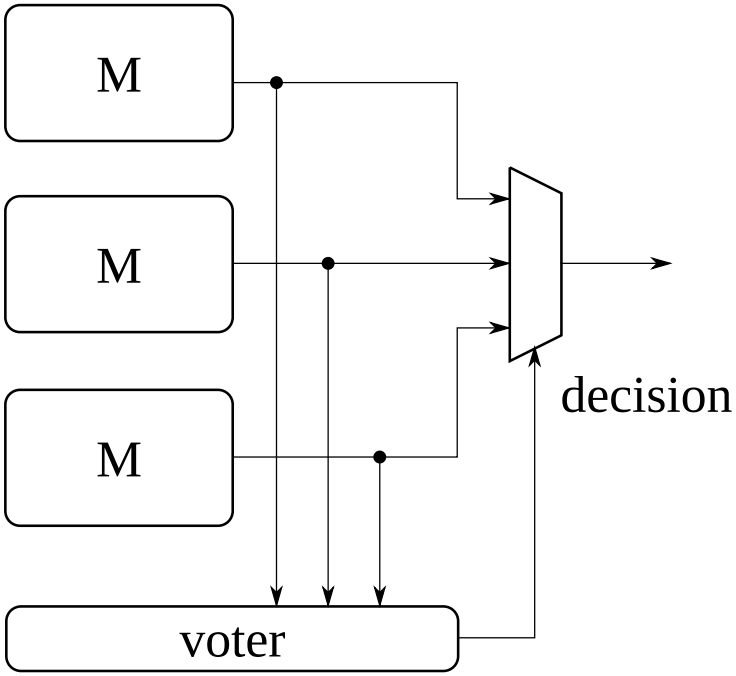
Dokončený výzkum
Maskování chyb (projevů poruch)

- TMR

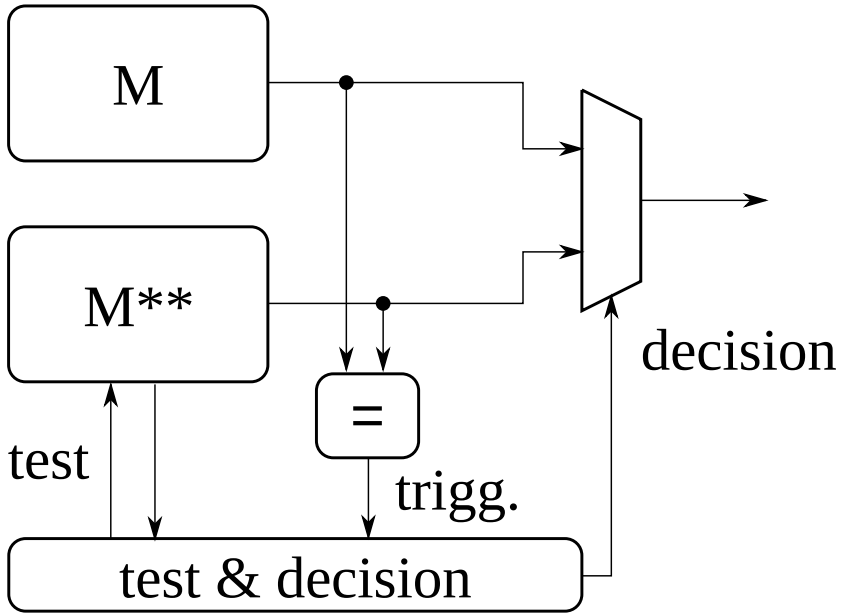


Dokončený výzkum
Maskování chyb (projevů poruch)

- TMR

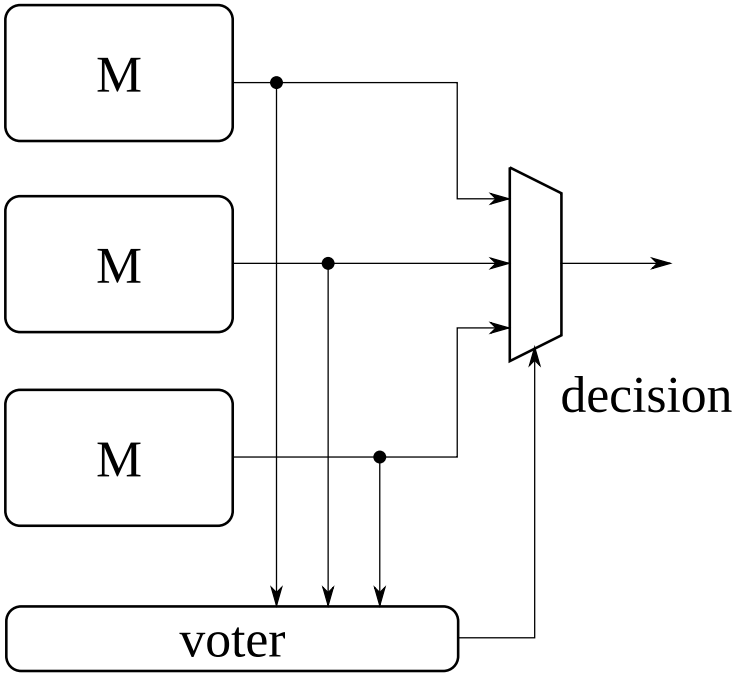


- Navržené řešení – *Time-Extended Duplex* (TED)

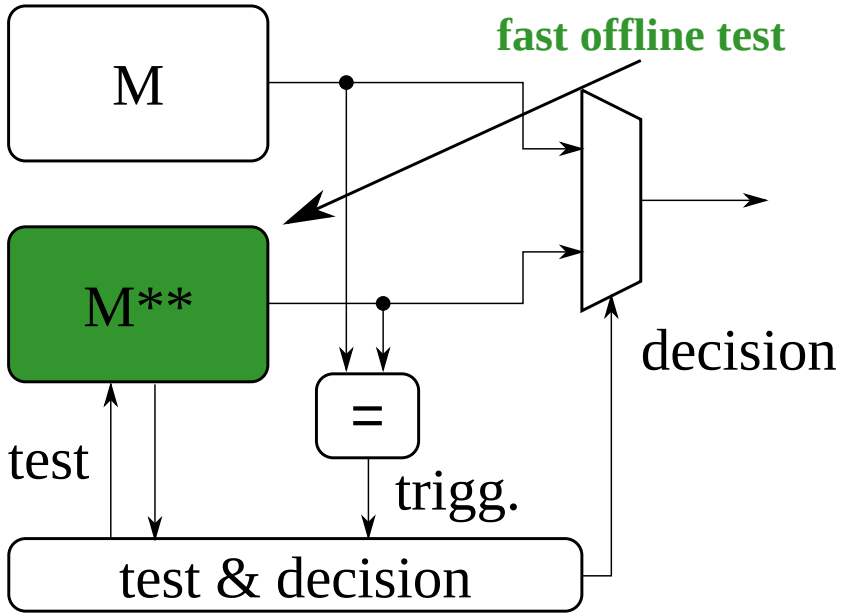


Dokončený výzkum
Maskování chyb (projevů poruch)

- TMR



- Navržené řešení – *Time-Extended Duplex* (TED)



Dokončený výzkum
Teoretické výsledky: Stuck-At-Fault model

- Pro 100% pokrytí poruch stačí dva vektory: *samé nuly* a *samé jedničky*

Theorem

Existuje třída obvodů, kde existuje test o dvou vektorech vzhledem ke stuck-at-fault modelu.

Dokončený výzkum
Teoretické výsledky: Stuck-At-Fault model

- Pro 100% pokrytí poruch stačí dva vektory: *samé nuly* a *samé jedničky*

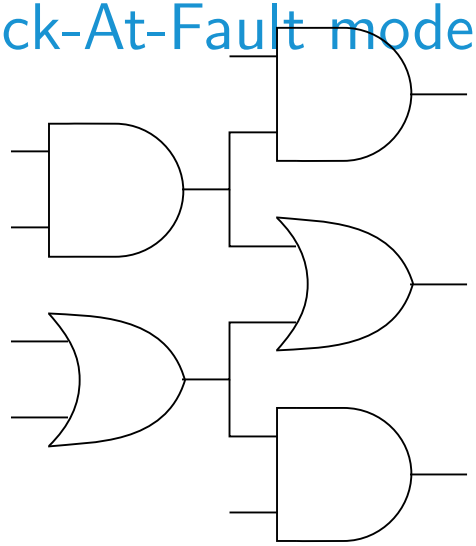
Theorem

Existuje třída obvodů, kde existuje test o dvou vektorech vzhledem ke stuck-at-fault modelu.

Požadované vlastnosti obvodů:

- Monotónní obvod neobsahuje invertory $\rightarrow$ *symptom poruchy* se při propagaci obvodem nemění

Dokončený výzkum
Teoretické výsledky: Stuck-At-Fault model

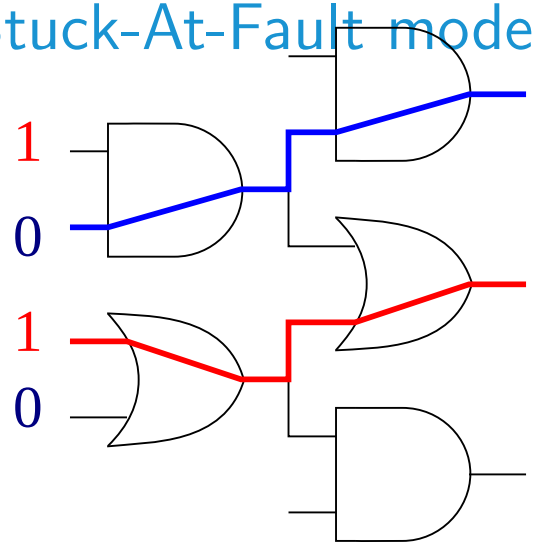


Požadované vlastnosti obvodů:

- Monotónní obvod neobsahuje invertory $\rightarrow$ *symptom poruchy* se při propagaci obvodem nemění
- Obvod vyhovuje *principu indikace* $\rightarrow$ výstup každého hradla je připojen alespoň k jednomu hradlu AND a jednomu hradlu OR

Dokončený výzkum

Teoretické výsledky: Stuck-At-Fault model



stuck-at-1 / fault symptom: 1

stuck-at-0 / fault symptom: 0

Požadované vlastnosti obvodů:

- Monotónní obvod neobsahuje invertory → *symptom poruchy* se při propagaci obvodem nemění
- Obvod vyhovuje *principu indikace* → výstup každého hradla je připojen alespoň k jednomu hradlu AND a jednomu hradlu OR

Dokončený výzkum
Teoretické výsledky: Stuck-At-Fault model

- Pro 100% pokrytí poruch stačí dva vektory: *samé nuly* a *samé jedničky*

Theorem

Existuje třída obvodů, kde existuje test o dvou vektorech vzhledem ke stuck-at-fault modelu.

Požadované vlastnosti obvodů:

- Monotónní obvod neobsahuje invertory $\rightarrow$ *symptom poruchy* se při propagaci obvodem nemění
- Obvod vyhovuje *principu indikace* $\rightarrow$ výstup každého hradla je připojen alespoň k jednomu hradlu AND a jednomu hradlu OR

Dokončený výzkum
Implementace libovolného KO

Jak vytvořit obvod splňující dané podmínky:

- převést obvod na monotónní – *dual-rail logika*

Dokončený výzkum
Implementace libovolného KO

Jak vytvořit obvod splňující dané podmínky:

- převést obvod na monotónní – *dual-rail logika*
  - → metodologie + heuristiky

Dokončený výzkum
Implementace libovolného KO

Jak vytvořit obvod splňující dané podmínky:

- převést obvod na monotónní – *dual-rail logika*
  - → metodologie + heuristiky
- použít rekonfigurovatelná hradla – OR/AND

Dokončený výzkum
Implementace libovolného KO

Jak vytvořit obvod splňující dané podmínky:

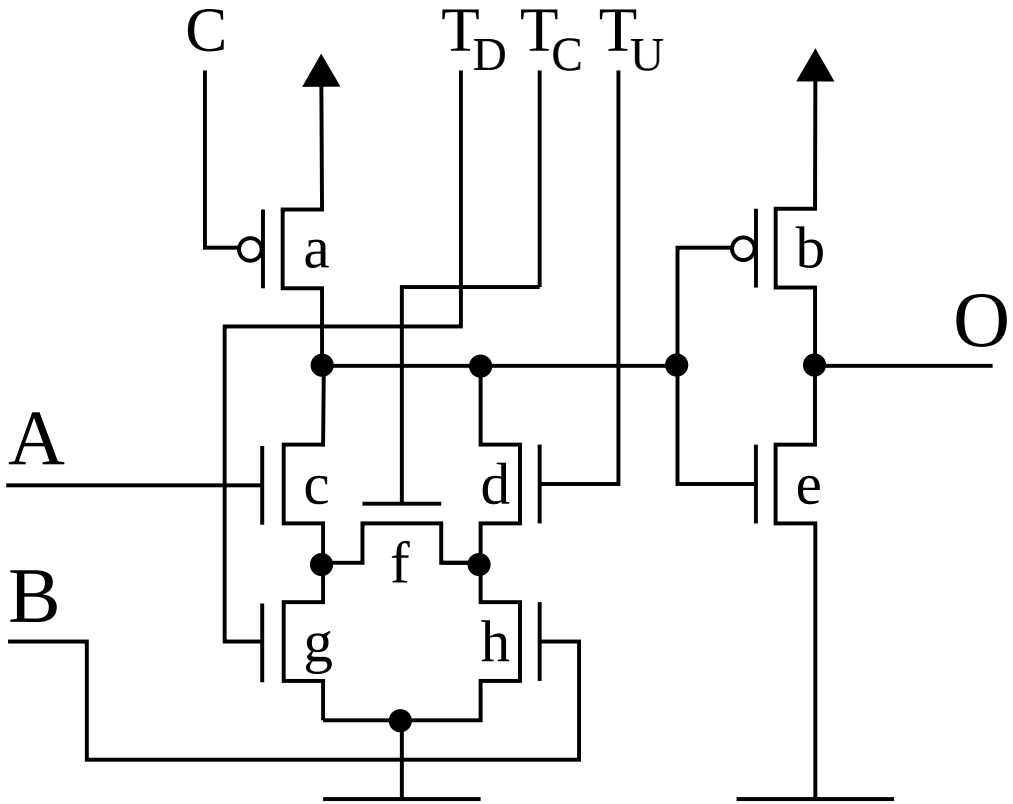
- převést obvod na monotónní – *dual-rail logika*
  - → metodologie + heuristiky ✓
- použít rekonfigurovatelná hradla – OR/AND

Dokončený výzkum
Implementace libovolného KO

Jak vytvořit obvod splňující dané podmínky:

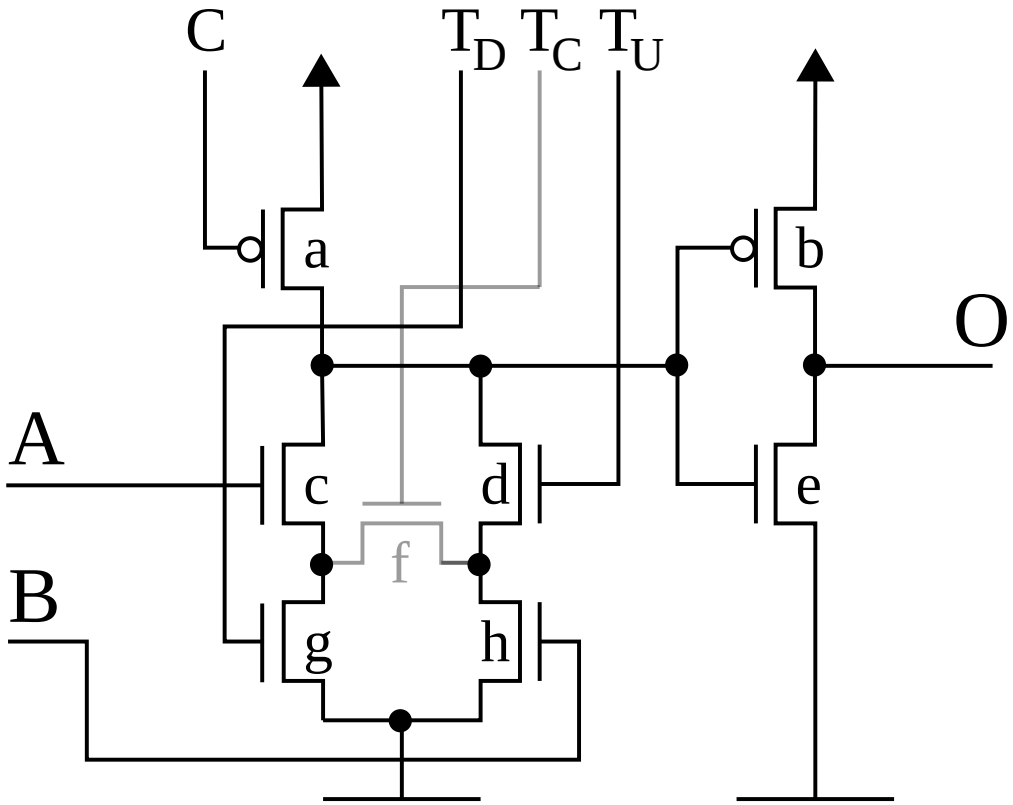
- převést obvod na monotónní – *dual-rail logika*
  - → metodologie + heuristiky ✓
- použít rekonfigurovatelná hradla – OR/AND ✓

Dokončený výzkum
Implementace KO: Rekonfigurovatelné hradlo



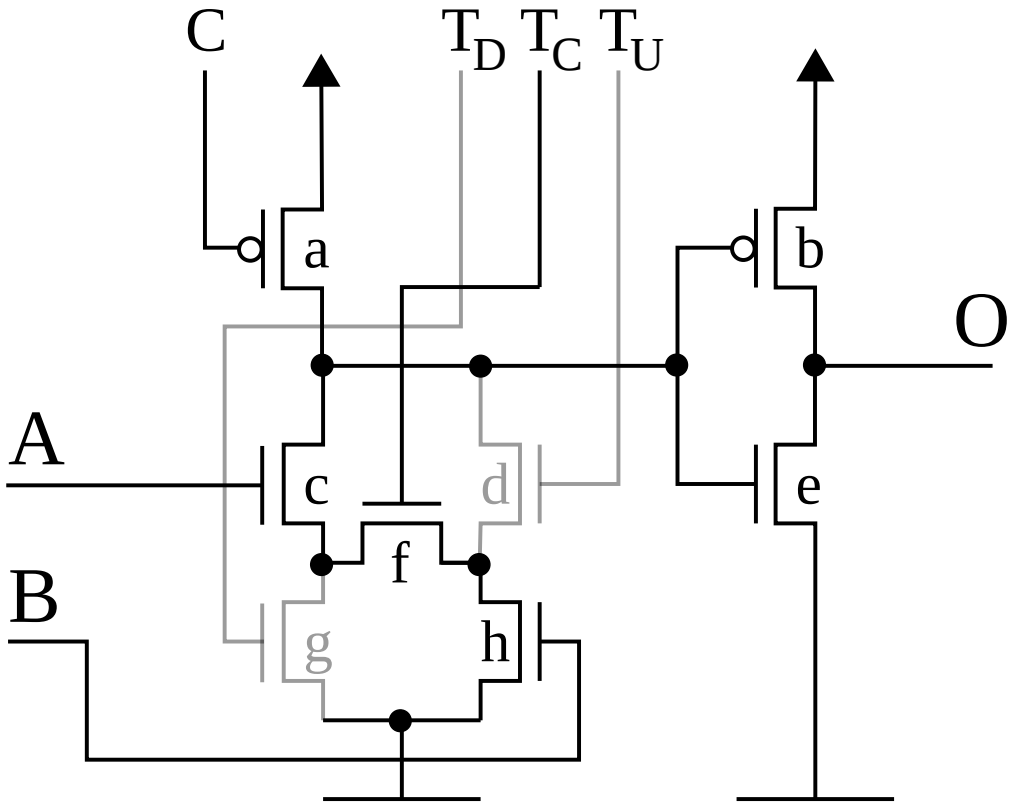
- Domino-logic AND/OR

Dokončený výzkum
Implementace KO: Rekonfigurovatelné hradlo



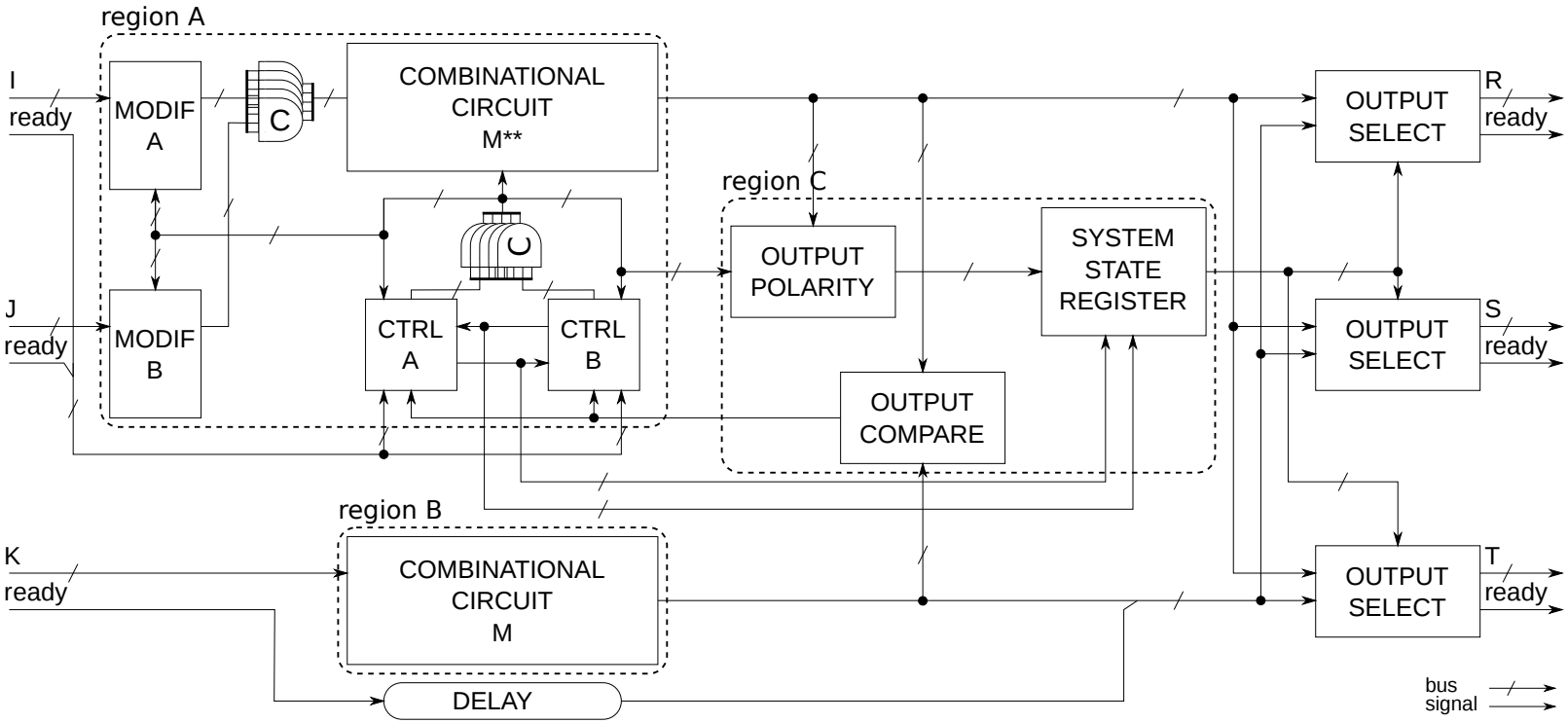
- Domino-logic OR $T_D = 1,\ T_C = 0,\ T_U = 1$

Dokončený výzkum
Implementace KO: Rekonfigurovatelné hradlo



- Domino-logic AND $T_D = 0,\ T_C = 1,\ T_U = 0$

Dokončený výzkum
Architektura TED



CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

Dokončený výzkum
Vlastnosti navrženého řešení

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

Dokončený výzkum
Vlastnosti navrženého řešení

+ délka testu: desítky cyklů – *short-duration offline test*

Dokončený výzkum
Vlastnosti navrženého řešení

+ délka testu: desítky cyklů – *short-duration offline test*
+ 100% pokrytí poruch při použití stuck-open/stuck-closed modelu

Dokončený výzkum
Vlastnosti navrženého řešení

+ délka testu: desítky cyklů – *short-duration offline test*
+ 100% pokrytí poruch při použití stuck-open/stuck-closed modelu
– speciální struktury (rekonfigurovatelné hradlo) – nemožnost použití standardních buněk

Dokončený výzkum
Vlastnosti navrženého řešení

+ délka testu: desítky cyklů – *short-duration offline test*
+ 100% pokrytí poruch při použití stuck-open/stuck-closed modelu
– speciální struktury (rekonfigurovatelné hradlo) – nemožnost použití standardních buněk
– složitější struktura obvodu

Dokončený výzkum
Vlastnosti navrženého řešení

+ délka testu: desítky cyklů – *short-duration offline test*
+ 100% pokrytí poruch při použití stuck-open/stuck-closed modelu
– speciální struktury (rekonfigurovatelné hradlo) – nemožnost použití standardních buněk
– složitější struktura obvodu

→ vhodné jen pro některé návrhy

Dokončený výzkum
Vlastnosti navrženého řešení

+ délka testu: desítky cyklů – *short-duration offline test*
+ 100% pokrytí poruch při použití stuck-open/stuck-closed modelu
– speciální struktury (rekonfigurovatelné hradlo) – nemožnost použití standardních buněk
– složitější struktura obvodu

→ vhodné jen pro některé návrhy

– Řídící signály (+3) komplikují hradlo – metalové vrstvy

Dokončený výzkum
Vlastnosti navrženého řešení

+ délka testu: desítky cyklů – *short-duration offline test*
+ 100% pokrytí poruch při použití stuck-open/stuck-closed modelu
– speciální struktury (rekonfigurovatelné hradlo) – nemožnost použití standardních buněk
– složitější struktura obvodu

→ vhodné jen pro některé návrhy

– Řídící signály (+3) komplikují hradlo – metalové vrstvy
– Hradlo s více než dvěma vstupy se stejnými vlastnostmi je problém!

Dokončený výzkum
Vlastnosti navrženého řešení

+ délka testu: desítky cyklů – *short-duration offline test*
+ 100% pokrytí poruch při použití stuck-open/stuck-closed modelu
– speciální struktury (rekonfigurovatelné hradlo) – nemožnost použití standardních buněk
– složitější struktura obvodu

→ vhodné jen pro některé návrhy

– Řídící signály (+3) komplikují hradlo – metalové vrstvy
– Hradlo s více než dvěma vstupy se stejnými vlastnostmi je problém!

→ pouze dvouvstupová hradla

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

Otevřené problémy
Plánováno dokončení do obhajoby DP

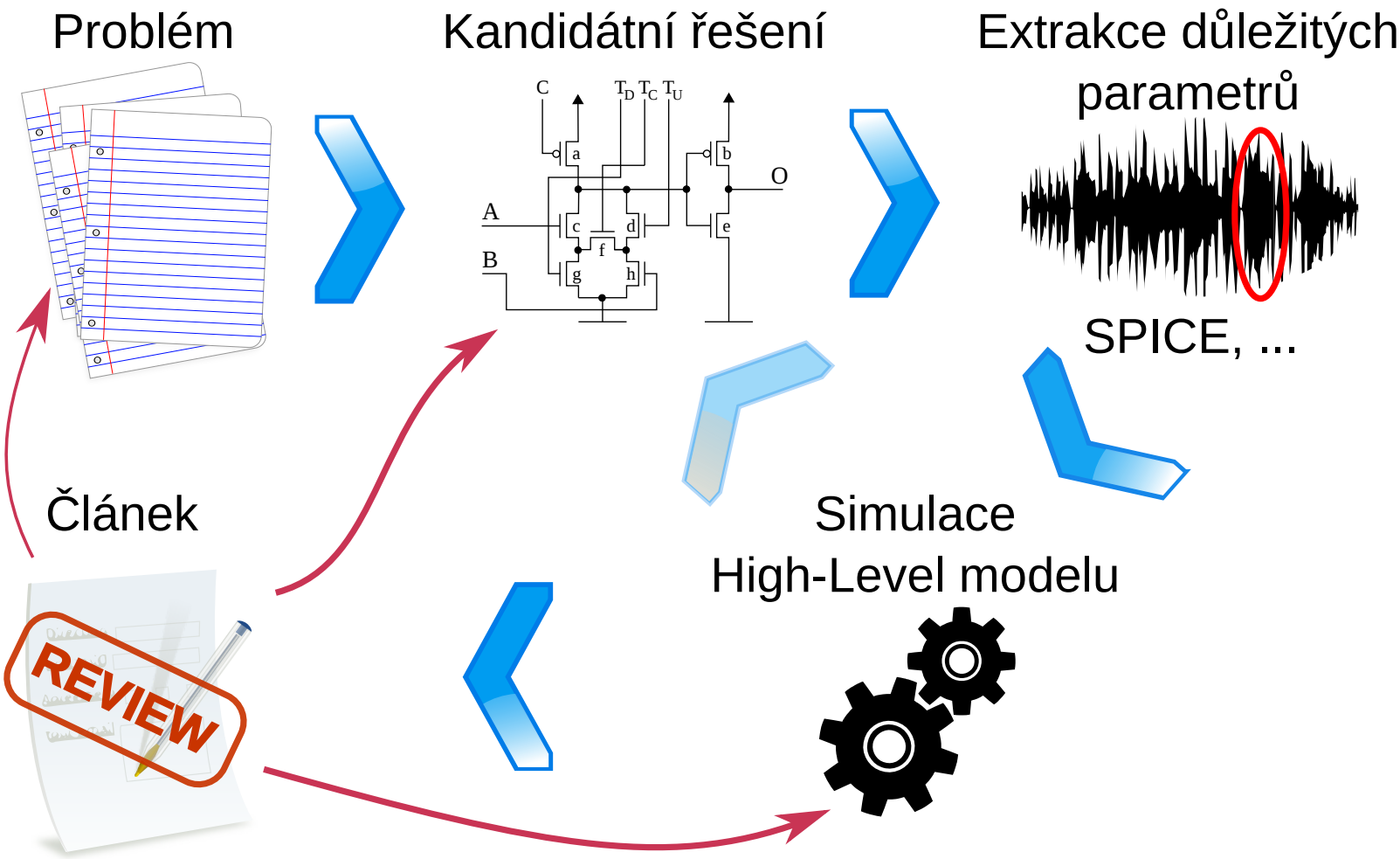
- syntéza monotónních obvodů
- formulace *nutných podmínek* pro krátký test

Restart
Probíhající výzkum

Vzhledem k účasti na projektech GA16-05179S a RCI (Research Center for Informatics) bylo zaměření výzkumu posunuto blíže k systémům odolným proti poruše a zároveň proti útokům postranními kanály.

Téma *Zvyšování spolehlivosti a bezpečnosti číslicových obvodů na úrovni mikroarchitektury* umožňuje využít kompetence nabyté v průběhu práce na předchozím (téměř) dokončeném výzkumu.

Probíhající výzkum
Metoda výzkumu



Probíhající výzkum – definice pojmů
Bezpečnost a spolehlivost

- Útoky na kryptografická zařízení (Bezpečnost):
  - Neinvazivní

Probíhající výzkum – definice pojmů
Bezpečnost a spolehlivost

- Útoky na kryptografická zařízení (Bezpečnost):
  - Neinvazivní
    - Analýza postranních kanálů (příkonová analýza)

Definition

Postranní kanál je sekundární projev zařízení umožňující kritické snížení entropie tajného klíče.

Probíhající výzkum – definice pojmů
Bezpečnost a spolehlivost

- Útoky na kryptografická zařízení (Bezpečnost):
  - Neinvazivní
    - Analýza postranních kanálů (příkonová analýza)
  - Invazivní

Definition

Postranní kanál je sekundární projev zařízení umožňující kritické snížení entropie tajného klíče.

Probíhající výzkum – definice pojmů
Bezpečnost a spolehlivost

- Útoky na kryptografická zařízení (Bezpečnost):
  - Neinvazivní
    - Analýza postranních kanálů (příkonová analýza)
  - Invazivní
    - Injekce poruch – sledujeme rozdíl v bezchybné a chybovém výstupu zařízení

Definition

Postranní kanál je sekundární projev zařízení umožňující kritické snížení entropie tajného klíče.

Probíhající výzkum – definice pojmů
Bezpečnost a spolehlivost

- Útoky na kryptografická zařízení (Bezpečnost):
  - Neinvazivní
    - Analýza postranních kanálů (příkonová analýza)
  - Invazivní
    - Injekce poruch – sledujeme rozdíl v bezchybné a chybovém výstupu zařízení
  - Kombinované

Definition

Postranní kanál je sekundární projev zařízení umožňující kritické snížení entropie tajného klíče.

Probíhající výzkum – definice pojmů
Bezpečnost a spolehlivost

- Útoky na kryptografická zařízení (Bezpečnost):
  - Neinvazivní
    - Analýza postranních kanálů (příkonová analýza)
  - Invazivní
    - Injekce poruch – sledujeme rozdíl v bezchybné a chybovém výstupu zařízení
  - Kombinované
    - Injekce poruch – chybový výstup + další postranní kanály (např. příkonová analýza)

Definition

Postranní kanál je sekundární projev zařízení umožňující kritické snížení entropie tajného klíče.

Probíhající výzkum – definice pojmů
Bezpečnost a spolehlivost

- Útoky na kryptografická zařízení (Bezpečnost):
  - Neinvazivní
    - Analýza postranních kanálů (příkonová analýza)
  - Invazivní
    - Injekce poruch – sledujeme rozdíl v bezchybné a chybovém výstupu zařízení
  - Kombinované
    - Injekce poruch – chybový výstup + další postranní kanály (např. příkonová analýza)
- Spolehlivost (fault-tolerance):

Definition

Postranní kanál je sekundární projev zařízení umožňující kritické snížení entropie tajného klíče.

Probíhající výzkum – definice pojmů
Bezpečnost a spolehlivost

- Útoky na kryptografická zařízení (Bezpečnost):
  - Neinvazivní
    - Analýza postranních kanálů (příkonová analýza)
  - Invazivní
    - Injekce poruch – sledujeme rozdíl v bezchybné a chybovém výstupu zařízení
  - Kombinované
    - Injekce poruch – chybový výstup + další postranní kanály (např. příkonová analýza)
- Spolehlivost (fault-tolerance):
  - Výstup zařízení je správný za přítomnosti poruchy

Definition

Postranní kanál je sekundární projev zařízení umožňující kritické snížení entropie tajného klíče.

Probíhající výzkum – cíle

Cílem je navrhnout architekturu (μTMR), jejíž vyzařování (příkonová charakteristika) do postranních kanálů a výstup budou za použití μVoterů:

Otevřené problémy:

Probíhající výzkum – cíle

Cílem je navrhnout architekturu (μTMR), jejíž vyzařování (příkonová charakteristika) do postranních kanálů a výstup budou za použití μVoterů:

- nezávislé na zpracovávaných datech

Otevřené problémy:

Probíhající výzkum – cíle

Cílem je navrhnout architekturu (μTMR), jejíž vyzařování (příkonová charakteristika) do postranních kanálů a výstup budou za použití μVoterů:

- nezávislé na zpracovávaných datech
- nezávislé na přítomnosti poruch

Otevřené problémy:

Probíhající výzkum – cíle

Cílem je navrhnout architekturu (μTMR), jejíž vyzařování (příkonová charakteristika) do postranních kanálů a výstup budou za použití μVoterů:

- nezávislé na zpracovávaných datech
- nezávislé na přítomnosti poruch

→ tj.: konstantní odběr, správný výstup (i za při poruše) → porucha se opraví lokálně

Otevřené problémy:

Probíhající výzkum – cíle

Cílem je navrhnout architekturu (μTMR), jejíž vyzařování (příkonová charakteristika) do postranních kanálů a výstup budou za použití μVoterů:

- nezávislé na zpracovávaných datech
- nezávislé na přítomnosti poruch

$\rightarrow$ tj.: konstantní odběr, správný výstup (i za při poruše) $\rightarrow$ porucha se opraví lokálně

Otevřené problémy:

- Distribuce μVoterů v obvodu (architektura μTMR)

Probíhající výzkum – cíle

Cílem je navrhnout architekturu (μTMR), jejíž vyzařování (příkonová charakteristika) do postranních kanálů a výstup budou za použití μVoterů:

- nezávislé na zpracovávaných datech
- nezávislé na přítomnosti poruch

$\rightarrow$ tj.: konstantní odběr, správný výstup (i za při poruše) $\rightarrow$ porucha se opraví lokálně

Otevřené problémy:

- Distribuce μVoterů v obvodu (architektura μTMR)
- Návrh μVoteru

Probíhající výzkum – metody

Poruchový model:

- Budeme uvažovat jednu poruchu (SEU, stuck-at, laser), následně shluky poruch (defekt, EM pulz)

Nástroje:

Návrhový styl:

Probíhající výzkum – metody

Poruchový model:

- Budeme uvažovat jednu poruchu (SEU, stuck-at, laser), následně shluky poruch (defekt, EM pulz)
- Model stuck-open/stuck-on (stuck-at na tranz. úrovni)

Nástroje:

Návrhový styl:

Probíhající výzkum – metody

Poruchový model:

- Budeme uvažovat jednu poruchu (SEU, stuck-at, laser), následně shluky poruch (defekt, EM pulz)
- Model stuck-open/stuck-on (stuck-at na tranz. úrovni)
- Trvání poruchy:

Nástroje:

Návrhový styl:

Probíhající výzkum – metody

Poruchový model:

- Budeme uvažovat jednu poruchu (SEU, stuck-at, laser), následně shluky poruch (defekt, EM pulz)
- Model stuck-open/stuck-on (stuck-at na tranz. úrovni)
- Trvání poruchy:
  - nejprve poruchy trvalé (permanent fault) a přechodné, ale dostatečně dlouhé (long-duration transient)

Nástroje:

Návrhový styl:

Probíhající výzkum – metody

Poruchový model:

- Budeme uvažovat jednu poruchu (SEU, stuck-at, laser), následně shluky poruch (defekt, EM pulz)
- Model stuck-open/stuck-on (stuck-at na tranz. úrovni)
- Trvání poruchy:
  - nejprve poruchy trvalé (permanent fault) a přechodné, ale dostatečně dlouhé (long-duration transient)
  - zkusíme správně modelovat poruchy přechodné – glitche

Nástroje:

Návrhový styl:

Probíhající výzkum – metody

Poruchový model:

- Budeme uvažovat jednu poruchu (SEU, stuck-at, laser), následně shluky poruch (defekt, EM pulz)
- Model stuck-open/stuck-on (stuck-at na tranz. úrovni)
- Trvání poruchy:
  - nejprve poruchy trvalé (permanent fault) a přechodné, ale dostatečně dlouhé (long-duration transient)
  - zkusíme správně modelovat poruchy přechodné – glitche

Nástroje:

- SPICE simulace, zjednodušená simulace odběru

Návrhový styl:

Probíhající výzkum – metody

Poruchový model:

- Budeme uvažovat jednu poruchu (SEU, stuck-at, laser), následně shluky poruch (defekt, EM pulz)
- Model stuck-open/stuck-on (stuck-at na tranz. úrovni)
- Trvání poruchy:
  - nejprve poruchy trvalé (permanent fault) a přechodné, ale dostatečně dlouhé (long-duration transient)
  - zkusíme správně modelovat poruchy přechodné – glitche

Nástroje:

- SPICE simulace, zjednodušená simulace odběru
- Simulace poruch, logická simulace

Návrhový styl:

Probíhající výzkum – metody

Poruchový model:

- Budeme uvažovat jednu poruchu (SEU, stuck-at, laser), následně shluky poruch (defekt, EM pulz)
- Model stuck-open/stuck-on (stuck-at na tranz. úrovni)
- Trvání poruchy:
  - nejprve poruchy trvalé (permanent fault) a přechodné, ale dostatečně dlouhé (long-duration transient)
  - zkusíme správně modelovat poruchy přechodné – glitche

Nástroje:

- SPICE simulace, zjednodušená simulace odběru
- Simulace poruch, logická simulace

Návrhový styl:

- varianty dvoudrátové logiky (viz rešerše)

Otevřené problémy – μTMR
Distribuce μVoterů v obvodu

- Jaký má rozmístění μVoterů v obvodu vliv na:
  - spolehlivost

Otevřené problémy – μTMR
Distribuce μVoterů v obvodu

- Jaký má rozmístění μVoterů v obvodu vliv na:
  - spolehlivost
  - plochu

Otevřené problémy – μTMR
Distribuce μVoterů v obvodu

- Jaký má rozmístění μVoterů v obvodu vliv na:
  - spolehlivost
  - plochu
  - spotřebu a zpoždění

Otevřené problémy – μTMR
Distribuce μVoterů v obvodu

- Jaký má rozmístění μVoterů v obvodu vliv na:
  - spolehlivost
  - plochu
  - spotřebu a zpoždění
  - vyzařování postranními kanály při poruše

Otevřené problémy – μTMR
Distribuce μVoterů v obvodu

- Jaký má rozmístění μVoterů v obvodu vliv na:
  - spolehlivost ✓
  - plochu
  - spotřebu a zpoždění
  - vyzařování postranními kanály při poruše

Otevřené problémy – μTMR
Distribuce μVoterů v obvodu

- Jaký má rozmístění μVoterů v obvodu vliv na:
  - spolehlivost ✓
  - plochu ✓
  - spotřebu a zpoždění
  - vyzařování postranními kanály při poruše

Otevřené problémy – μTMR
Distribuce μVoterů v obvodu

- Jaký má rozmístění μVoterů v obvodu vliv na:
  - spolehlivost ✓
  - plochu ✓
  - spotřebu a zpoždění ✓
  - vyzařování postranními kanály při poruše

Otevřené problémy – μTMR
Distribuce μVoterů v obvodu

- Jaký má rozmístění μVoterů v obvodu vliv na:
  - spolehlivost ✓
  - plochu ✓
  - spotřebu a zpoždění ✓
  - **vyzařování postranními kanály při poruše**
- Metoda:

Otevřené problémy – μTMR
Distribuce μVoterů v obvodu

- Jaký má rozmístění μVoterů v obvodu vliv na:
  - spolehlivost ✓
  - plochu ✓
  - spotřebu a zpoždění ✓
  - **vyzařování postranními kanály při poruše**
- Metoda:
  - Předpoklad ideálního μVoteru s konstantním (nulovým) vyzařováním

Otevřené problémy – μTMR
Distribuce μVoterů v obvodu

- Jaký má rozmístění μVoterů v obvodu vliv na:
  - spolehlivost ✓
  - plochu ✓
  - spotřebu a zpoždění ✓
  - **vyzařování postranními kanály při poruše**
- Metoda:
  - Předpoklad ideálního μVoteru s konstantním (nulovým) vyzařováním
  - Zkoumá se pouze vliv **rozmístění** μVoterů (nikoli vliv samotného voteru) na vyzařování celého obvodu při poruše, a dále na na plochu, spotřebu, zpoždění, ...

Otevřené problémy – μTMR
Návrh μVoterů

- Optimální návrh μVoteru s ohledem na:
  - vyzařování (konstantní odběr)

Otevřené problémy – μTMR
Návrh μVoterů

- Optimální návrh μVoteru s ohledem na:
  - vyzařování (konstantní odběr)
  - plochu

Otevřené problémy – μTMR
Návrh μVoterů

- Optimální návrh μVoteru s ohledem na:
  - vyzařování (konstantní odběr)
  - plochu
  - spotřebu

Otevřené problémy – μTMR
Návrh μVoterů

- Optimální návrh μVoteru s ohledem na:
  - vyzařování (konstantní odběr)
  - plochu
  - spotřebu
- Návrh μVoteru s využitím:

Otevřené problémy – μTMR
Návrh μVoterů

- Optimální návrh μVoteru s ohledem na:
  - vyzařování (konstantní odběr)
  - plochu
  - spotřebu
- Návrh μVoteru s využitím:
  - **standardních buněk**

Otevřené problémy – μTMR
Návrh μVoterů

- Optimální návrh μVoteru s ohledem na:
  - vyzařování (konstantní odběr)
  - plochu
  - spotřebu
- Návrh μVoteru s využitím:
  - **standardních buněk**
  - specializovaná buňka v technologii CMOS

Otevřené problémy – μTMR
Návrh μVoterů

- Optimální návrh μVoteru s ohledem na:
  - vyzařování (konstantní odběr)
  - plochu
  - spotřebu
- Návrh μVoteru s využitím:
  - **standardních buněk**
  - specializovaná buňka v technologii CMOS
  - využití nestandardních postupů (?) – PTL (pass transistor logic), ...

Otevřené problémy – μTMR
Návrh μVoterů

- Optimální návrh μVoteru s ohledem na:
  - vyzařování (konstantní odběr)
  - plochu
  - spotřebu
- Návrh μVoteru s využitím:
  - **standardních buněk**
  - specializovaná buňka v technologii CMOS
  - využití nestandardních postupů (?) – PTL (pass transistor logic), ...
- Ověření vlastností μVoteru (SPICE):

Otevřené problémy – μTMR
Návrh μVoterů

- Optimální návrh μVoteru s ohledem na:
  - vyzařování (konstantní odběr)
  - plochu
  - spotřebu
- Návrh μVoteru s využitím:
  - **standardních buněk**
  - specializovaná buňka v technologii CMOS
  - využití nestandardních postupů (?) – PTL (pass transistor logic), ...
- Ověření vlastností μVoteru (SPICE):
  - diverzita chování v závislosti na zpracovávaných datech (vyzařování)

Probíhající výzkum
Přípravné práce

- Hodnocení zranitelnosti obvodů v závislosti na zvoleném návrhovém stylu – CryptArchi 2017 ✓

Probíhající výzkum
Přípravné práce

- Hodnocení zranitelnosti obvodů v závislosti na zvoleném návrhovém stylu – CryptArchi 2017 ✓
- Metoda hodnocení zranitelnosti (korelace mezi zpracovávanými daty a příkonovou charakteristikou) obvodů v simulaci – CryptArchi 2017 ✓

Probíhající výzkum
Přípravné práce

- Hodnocení zranitelnosti obvodů v závislosti na zvoleném návrhovém stylu – CryptArchi 2017 ✓
- Metoda hodnocení zranitelnosti (korelace mezi zpracovávanými daty a příkonovou charakteristikou) obvodů v simulaci – CryptArchi 2017 ✓
- Vliv kvality datasetu na DPA (počet měření) – TRUDEVICE 2018 ✓

Probíhající výzkum
Přípravné práce

- Hodnocení zranitelnosti obvodů v závislosti na zvoleném návrhovém stylu – CryptArchi 2017 ✓
- Metoda hodnocení zranitelnosti (korelace mezi zpracovávanými daty a příkonovou charakteristikou) obvodů v simulaci – CryptArchi 2017 ✓
- Vliv kvality datasetu na DPA (počet měření) – TRUDEVICE 2018 ✓
- Rešerše: utoky postranními kanály, invazivní a kombinované útoky a protiopatření – PAD 2018 ✓

Projekty

- Czech Technical University in Prague:
  - SGS14/105/OHK3/1T/18
  - SGS15/119/OHK3/1T/18
  - SGS16/121/OHK3/1T/18
  - SGS17/213/OHK3/3T/18
- GA16-05179S of the Czech Grant Agency: *Fault-Tolerant and Attack-Resistant Architectures Based on Programmable Devices: Research of Interplay and Common Features (2016 – 2018)*
- RCI Research Center for Informatics (od července 2018)

Publikace
Publikace nesouvisející s dizertací

- Bělohoubek J., "Smart re-use of hardware peripherals for better software UART," *in The 3rd Prague Embedded Systems Workshop, 2015, Roztoky u Prahy, Czech Republic*.
- Bělohoubek, J, "KETCube – the Prototyping and Educational Platform for IoT Nodes," *in: The 6th Prague Embedded Systems Workshop 2018, Roztoky u Prahy, Czech Republic*.
- Bělohoubek, J; Čengery, J.; Freisleben, J.; Kašpar, P.; Hamáček, A., "KETCube – the Universal Prototyping IoT Platform," *in: Euromicro Conference on Digital System Design – DSD 2018. Prague, Czech Republic, August 29-31, 2018* .

Publikace I
Relevantní publikace

- J. Bělohoubek, "Novel gate design method for short-duration test," *in POSTER 2015, 2015, Prague, Czech Republic*.
- J. Bělohoubek, "Novel Error Detection and Correction Method Combining Time and Area Redundancy," *in Počítačové architektury a diagnostika 2015, 2015, Zlín, Czech Republic*.
- J. Bělohoubek, "Využití rychlého offline testu v systému se schopností maskování jedné chyby," *in Počítačové architektury a diagnostika 2016, 2016, Kraví Hora, Czech Republic*.

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

Publikace II
Relevantní publikace

- J. Bělohoubek, "The Design-Time Side-Channel Information Leakage Estimation," *CryptArchi 2017, Smolenice, Slovakia, 2017-06-19*.
- J. Bělohoubek, "Effect of Power Trace Set Properties to Differential Power Analysis," *TRUDEVICE 2018, Dresden, Germany, 2018-03-23*.

Publikace
Recenzované relevantní publikace

- J. Bělohoubek, P. Fišer, and J. Schmidt, "Novel C-Element Based Error Detection and Correction Method Combining Time and Area Redundancy," *in Euromicro Conference on Digital System Design (DSD), 2015, Aug 2015, Funchal, Madeira, Portugal*. (Poster)
- J. Bělohoubek, P. Fišer, and J. Schmidt, "Error Correction Method Based On The Short-Duration Offline Test," *in Euromicro Conference on Digital System Design (DSD), 2016, Aug 2016, Limassol, Cyprus*. (Full Paper)
- J. Bělohoubek, P. Fišer, and J. Schmidt, "Error Masking Method Based On The Short-Duration Offline Test," *Microprocessors and Microsystems (MICPRO), Elsevier, vol. 52, July 2017, pp. 236-250*. (Journal)

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

Plán prací

- Zobecnění výsledků a rozšíření teorie z první části výzkumu

Plán prací

- Zobecnění výsledků a rozšíření teorie z první části výzkumu
- Pro útoku-odolné a spolehlivé systémy je lokalizace poruch a maskování chyb na co nejnižší úrovni nutné $\rightarrow$ μTMR

Plán prací

- Zobecnění výsledků a rozšíření teorie z první části výzkumu
- Pro útoku-odolné a spolehlivé systémy je lokalizace poruch a maskování chyb na co nejnižší úrovni nutné $\rightarrow$ μTMR
- Otevřené problémy – μTMR:

Plán prací

- Zobecnění výsledků a rozšíření teorie z první části výzkumu
- Pro útoku-odolné a spolehlivé systémy je lokalizace poruch a maskování chyb na co nejnižší úrovni nutné $\rightarrow$ μTMR
- Otevřené problémy – μTMR:
  - Distribuce μVoterů v obvodu (architektura μTMR)

Plán prací

- Zobecnění výsledků a rozšíření teorie z první části výzkumu
- Pro útoku-odolné a spolehlivé systémy je lokalizace poruch a maskování chyb na co nejnižší úrovni nutné $\rightarrow$ μTMR
- Otevřené problémy – μTMR:
  - Distribuce μVoterů v obvodu (architektura μTMR)
  - Návrh μVoteru

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

Děkuji za pozornost!

- Zobecnění výsledků a rozšíření teorie z první části výzkumu
- Pro útoku-odolné a spolehlivé systémy je lokalizace poruch a maskování chyb na co nejnižší úrovni nutné $\rightarrow$ μTMR
- Otevřené problémy – μTMR:
  - Distribuce μVoterů v obvodu (architektura μTMR)
  - Návrh μVoteru