CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Techniky maskování chyb založené na lokalizaci


Jan Bělohoubek

jan.belohoubek@fit.cvut.cz

ČVUT v Praze

2. ročník

Školitel: Petr Fišer, specialista: Jan Schmidt


PAD 2016, Kraví Hora

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Dokončený výzkum

## Využití rychlého offline testu v systému se schopností maskování jedné chyby

- Co?
  - Kombinace redundance v čase a v ploše pro maskování chyb
  - Redukce počtu testovacích vektorů tisíce $\rightarrow$ desítky
- Proč?
  - Redukce nákladů
  - Zkrácení doby testu a zjednodušení testovacího hardware
- Jak?
  - Krátký offline test – *short-duration offline test*
  - Popis vlastností obvodu nutných pro krátký test
  - Nové struktury umožňující krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE
Faculty of Information Technology

# Dokončený výzkum

## Využití rychlého offline testu v systému se schopností maskování jedné chyby

- Co?
  - Kombinace redundance v čase a v ploše pro maskování chyb
  - Redukce počtu testovacích vektorů tisíce $\rightarrow$ desítky
- Proč?
  - Redukce nákladů
  - Zkrácení doby testu a zjednodušení testovacího hardware
- Jak?
  - Krátký offline test – *short-duration offline test*
  - Popis vlastností obvodu nutných pro krátký test
  - Nové struktury umožňující krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE
Faculty of Information Technology

# Dokončený výzkum

## Využití rychlého offline testu v systému se schopností maskování jedné chyby

- Co?
  - Kombinace redundance v čase a v ploše pro maskování chyb
  - Redukce počtu testovacích vektorů tisíce $\rightarrow$ desítky
- Proč?
  - Redukce nákladů
  - Zkrácení doby testu a zjednodušení testovacího hardware
- Jak?
  - Krátký offline test – *short-duration offline test*
  - Popis vlastností obvodu nutných pro krátký test
  - Nové struktury umožňující krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE
Faculty of Information Technology

# Dokončený výzkum

## Využití rychlého offline testu v systému se schopností maskování jedné chyby

- Co?
  - Kombinace redundance v čase a v ploše pro maskování chyb
  - Redukce počtu testovacích vektorů tisíce $\rightarrow$ desítky
- Proč?
  - Redukce nákladů
  - Zkrácení doby testu a zjednodušení testovacího hardware
- Jak?
  - Krátký offline test – *short-duration offline test*
  - Popis vlastností obvodu nutných pro krátký test
  - Nové struktury umožňující krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Dokončený výzkum

## Využití rychlého offline testu v systému se schopností maskování jedné chyby

- Co?
  - Kombinace redundance v čase a v ploše pro maskování chyb
  - Redukce počtu testovacích vektorů tisíce $\rightarrow$ desítky
- Proč?
  - Redukce nákladů
  - Zkrácení doby testu a zjednodušení testovacího hardware
- Jak?
  - Krátký offline test – *short-duration offline test*
  - Popis vlastností obvodu nutných pro krátký test
  - Nové struktury umožňující krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE
Faculty of Information Technology

# Dokončený výzkum

## Využití rychlého offline testu v systému se schopností maskování jedné chyby

- Co?
  - Kombinace redundance v čase a v ploše pro maskování chyb
  - Redukce počtu testovacích vektorů tisíce → desítky
- Proč?
  - Redukce nákladů
  - Zkrácení doby testu a zjednodušení testovacího hardware
- Jak?
  - Krátký offline test – *short-duration offline test*
  - Popis vlastností obvodu nutných pro krátký test
  - Nové struktury umožňující krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Dokončený výzkum

## Využití rychlého offline testu v systému se schopností maskování jedné chyby

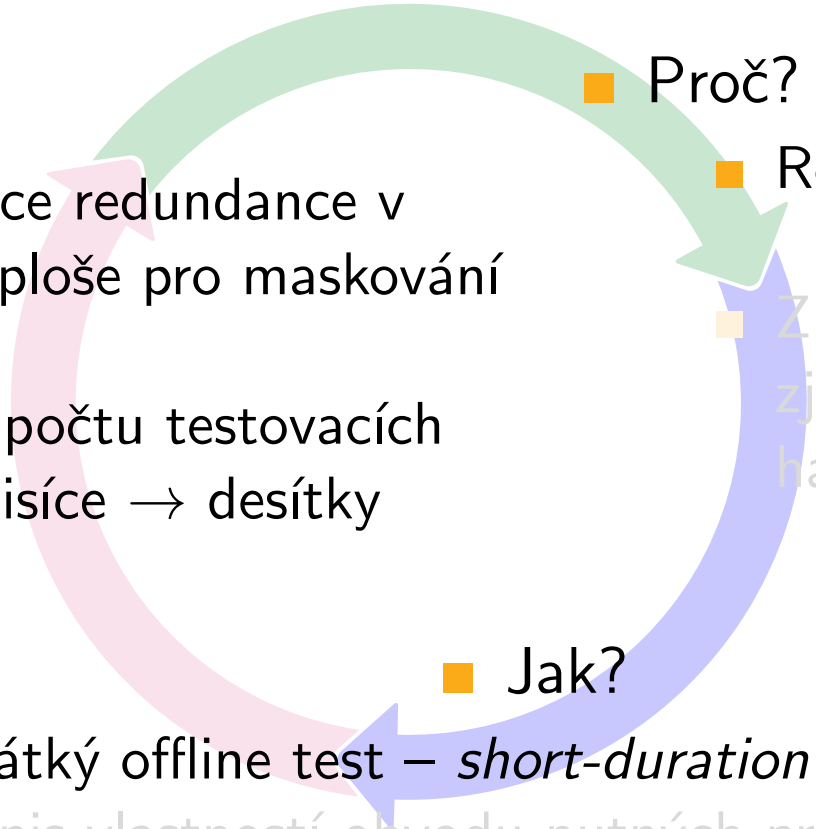
- Co?
  - Kombinace redundance v čase a v ploše pro maskování chyb
  - Redukce počtu testovacích vektorů tisíce → desítky
- Proč?
  - Redukce nákladů
  - Zkrácení doby testu a zjednodušení testovacího hardware
- Jak?
  - Krátký offline test – *short-duration offline test*
  - Popis vlastností obvodu nutných pro krátký test
  - Nové struktury umožňující krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Dokončený výzkum

## Využití rychlého offline testu v systému se schopností maskování jedné chyby



- Co?
  - Kombinace redundance v čase a v ploše pro maskování chyb
  - Redukce počtu testovacích vektorů tisíce → desítky
- Proč?
  - Redukce nákladů
  - Zkrácení doby testu a zjednodušení testovacího hardware
- Jak?
  - Krátký offline test – *short-duration offline test*
  - Popis vlastností obvodu nutných pro krátký test
  - Nové struktury umožňující krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Dokončený výzkum

## Využití rychlého offline testu v systému se schopností maskování jedné chyby

- Co?
  - Kombinace redundance v čase a v ploše pro maskování chyb
  - Redukce počtu testovacích vektorů tisíce $\rightarrow$ desítky
- Proč?
  - Redukce nákladů
  - Zkrácení doby testu a zjednodušení testovacího hardware
- Jak?
  - Krátký offline test – *short-duration offline test*
  - Popis vlastností obvodu nutných pro krátký test
  - Nové struktury umožňující krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Dokončený výzkum

## Využití rychlého offline testu v systému se schopností maskování jedné chyby

- Co?
  - Kombinace redundance v čase a v ploše pro maskování chyb
  - Redukce počtu testovacích vektorů tisíce $\rightarrow$ desítky
- Proč?
  - Redukce nákladů
  - Zkrácení doby testu a zjednodušení testovacího hardware
- Jak?
  - Krátký offline test – *short-duration offline test*
  - Popis vlastností obvodu nutných pro krátký test
  - Nové struktury umožňující krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE
Faculty of Information Technology

# Dokončený výzkum

## Využití rychlého offline testu v systému se schopností maskování jedné chyby

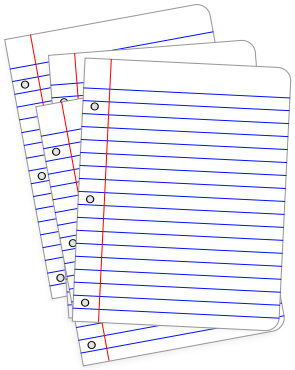
- Co?
  - Kombinace redundance v čase a v ploše pro maskování chyb
  - Redukce počtu testovacích vektorů tisíce $\rightarrow$ desítky
- Proč?
  - Redukce nákladů
  - Zkrácení doby testu a zjednodušení testovacího hardware
- Jak?
  - Krátký offline test – *short-duration offline test*
  - Popis vlastností obvodu nutných pro krátký test
  - Nové struktury umožňující krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE

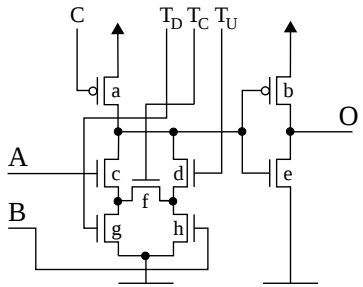
Faculty of Information Technology

# Dokončený výzkum
## Metodologie výzkumu

Problém



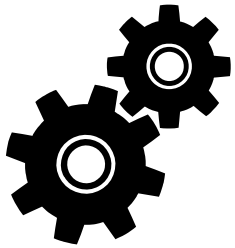
Kandidátní řešení




Extrakce důležitých parametrů

SPICE, ...

Simulace
High-Level modelu

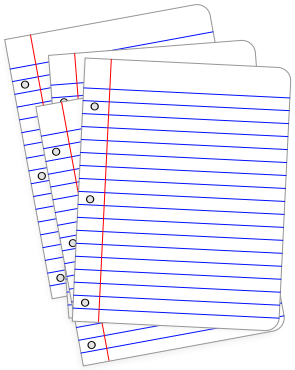


CZECH TECHNICAL UNIVERSITY IN PRAGUE

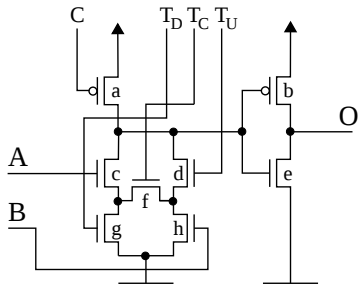
Faculty of Information Technology

# Dokončený výzkum
## Metodologie výzkumu

Problém



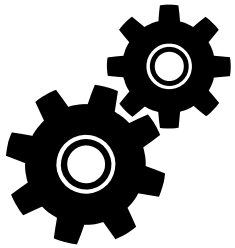
Kandidátní řešení




Extrakce důležitých parametrů

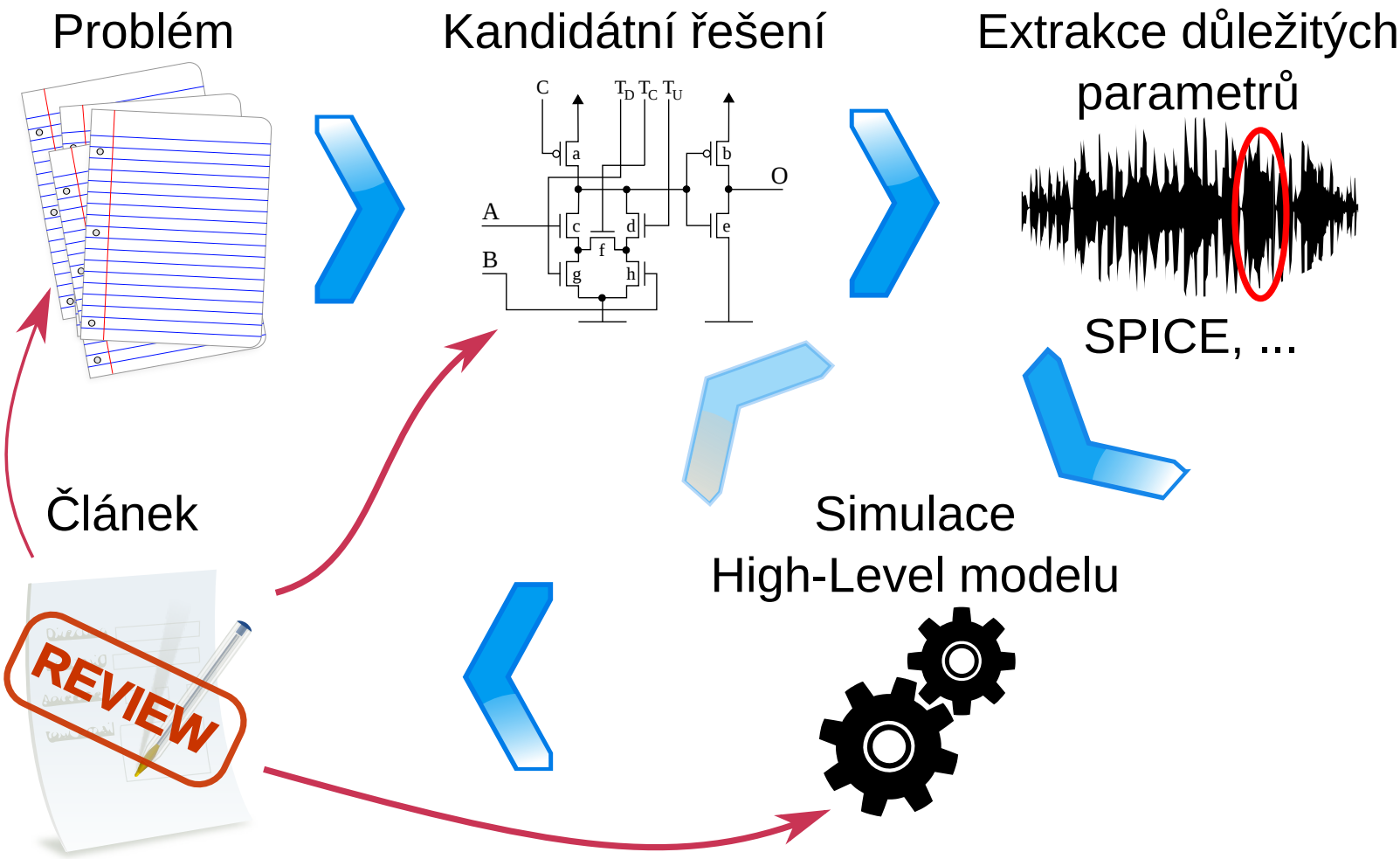
SPICE, ...

Simulace High-Level modelu



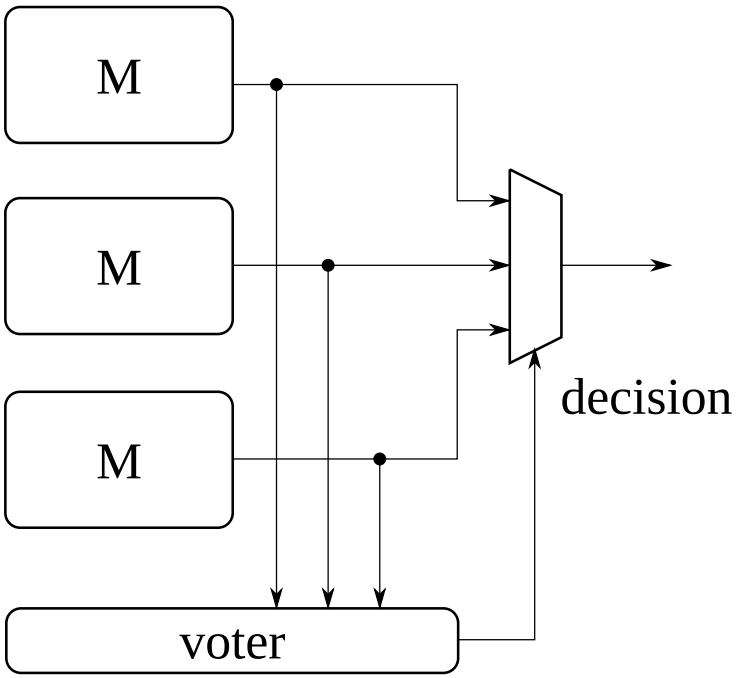
Článek

# Dokončený výzkum
## Metodologie výzkumu



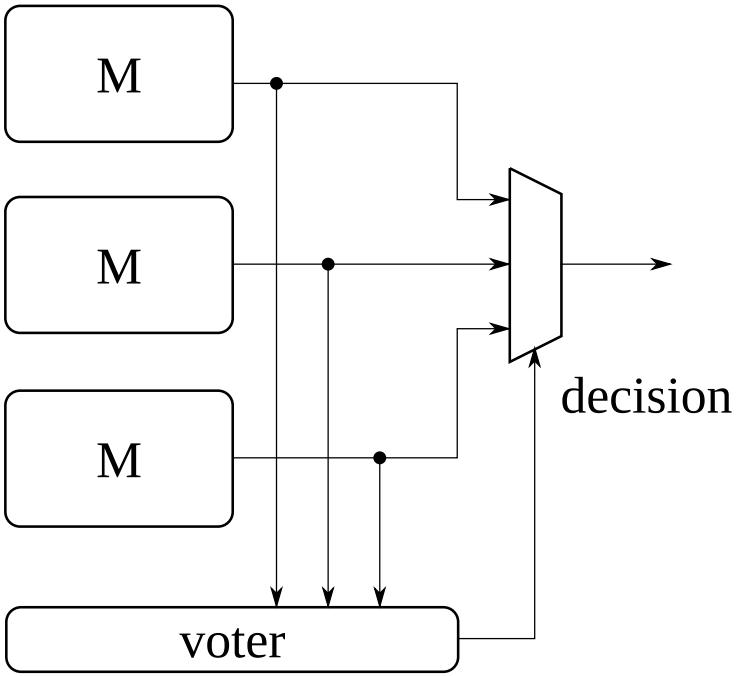
# Dokončený výzkum
## Maskování chyb

- TMR

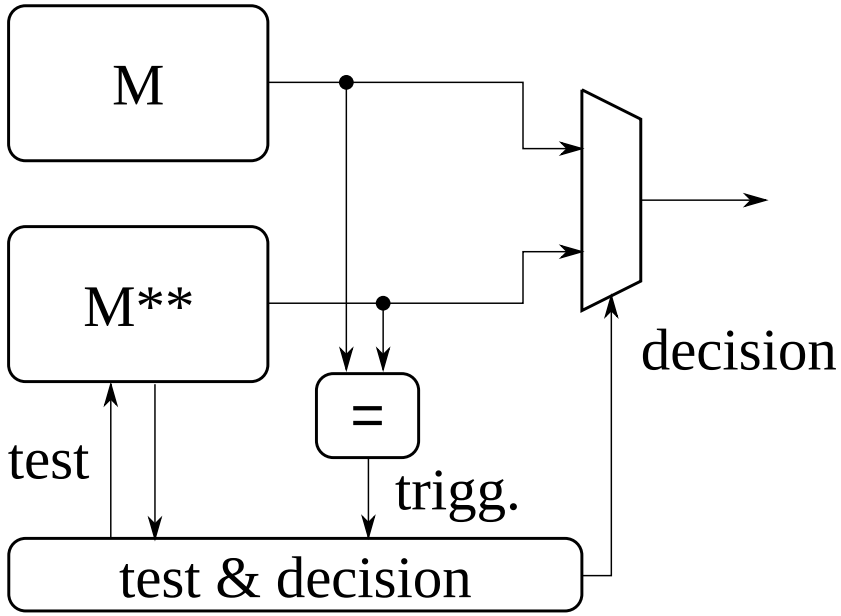


# Dokončený výzkum
## Maskování chyb

- TMR

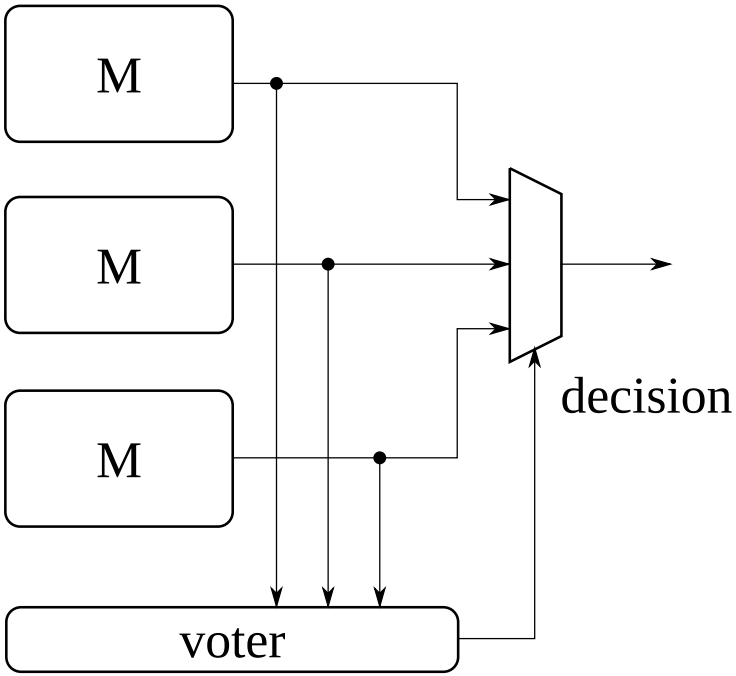



- Navržené řešení – *Time-Extended Duplex* (TED)

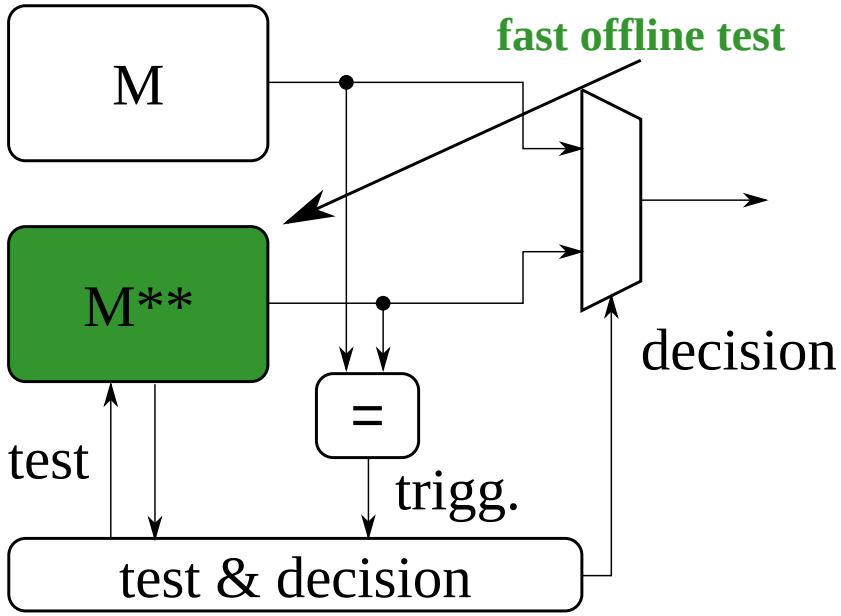


# Dokončený výzkum
## Maskování chyb

- TMR

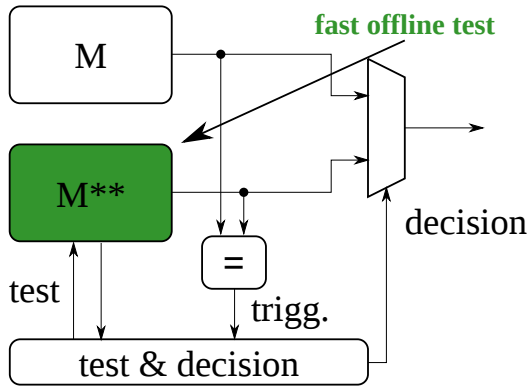



- Navržené řešení – *Time-Extended Duplex* (TED)

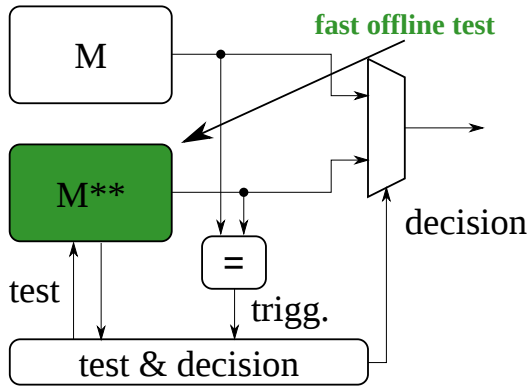


# Dokončený výzkum
## Velmi krátký Offline Test

Co potřebujeme:



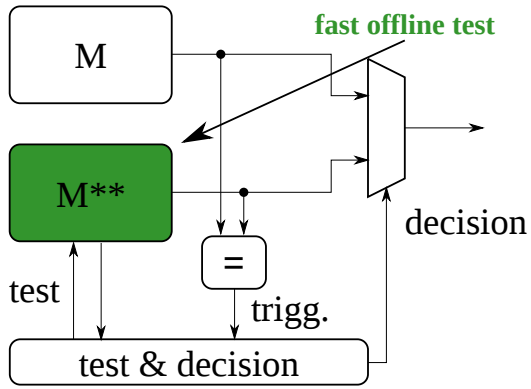
# Dokončený výzkum
## Velmi krátký Offline Test




Co potřebujeme:

- délka testu: desítky cyklů

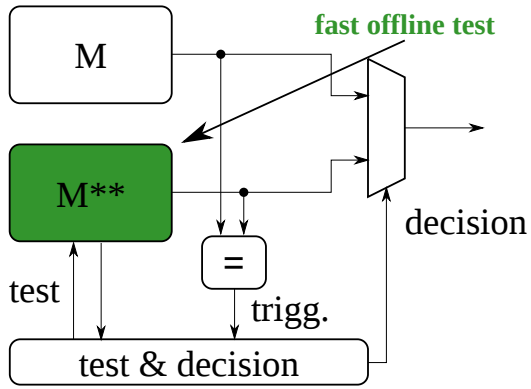
# Dokončený výzkum
## Velmi krátký Offline Test




Co potřebujeme:

- délka testu: desítky cyklů
- 100% pokrytí poruch při použití stuck-open/stuck-closed modelu

# Dokončený výzkum
## Velmi krátký Offline Test

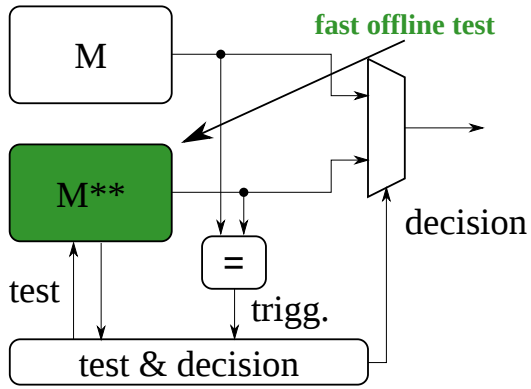



Co potřebujeme:

- délka testu: desítky cyklů
- 100% pokrytí poruch při použití stuck-open/stuck-closed modelu

→ *short-duration offline test*

# Dokončený výzkum
## Velmi krátký Offline Test




Co potřebujeme:

- délka testu: desítky cyklů
- 100% pokrytí poruch při použití stuck-open/stuck-closed modelu

→ *short-duration offline test*

→ *speciální struktury*

# Dokončený výzkum
## Stuck-At-Fault

- Pro 100% pokrytí 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
## Stuck-At-Fault

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

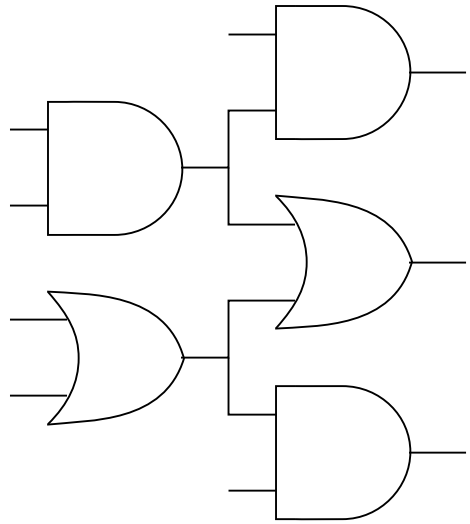
**Theorem**

*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

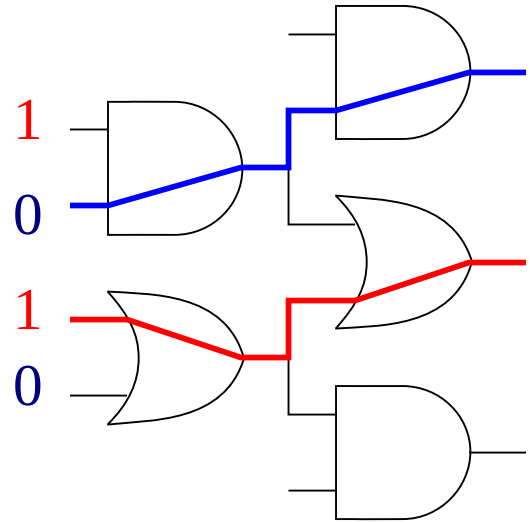
# Dokončený výzkum
## Stuck-At-Fault



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
## Stuck-At-Fault




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
## Stuck-At-Fault

- Pro 100% pokrytí 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:

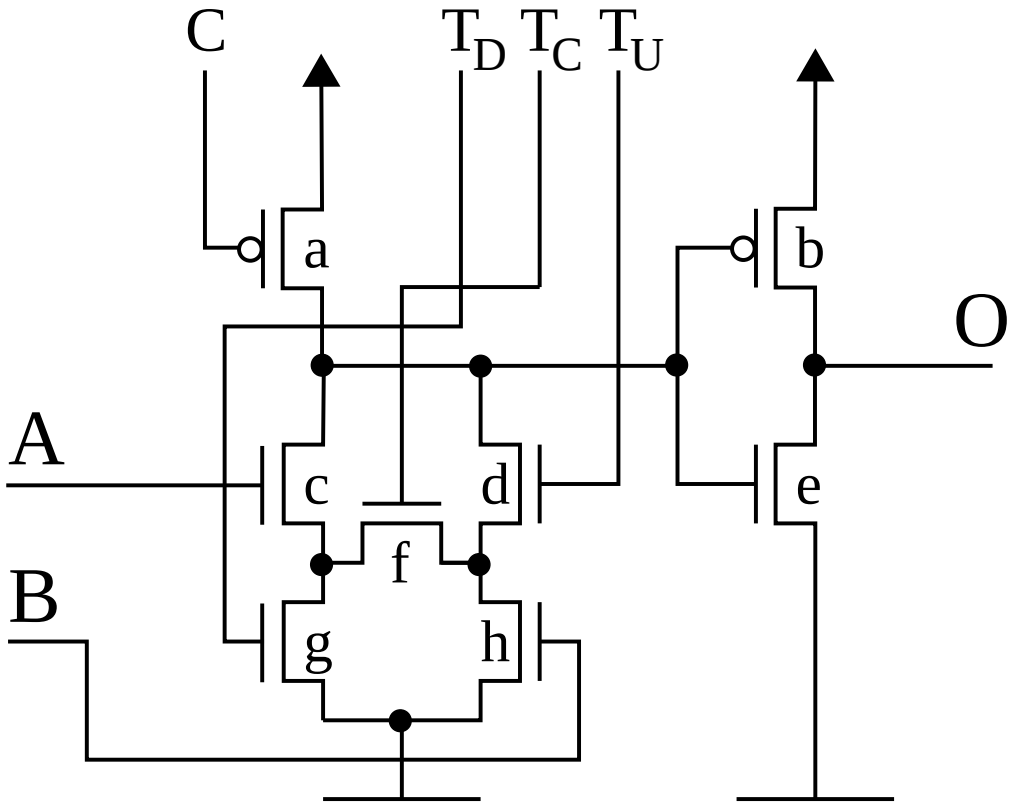
- Monotónní obvod neobsahuje invertory $\rightarrow$ *symptom poruchy* se při propagaci obvodem nemění
- Obvod vyhovuje *principu indikace* $\rightarrow$ výstup každého hradla je připojen alespoň k jednomu hradlu AND a jednomu hradlu OR

# Dokončený výzkum
## Efektivní implementace monotonního obvodu

Jak vytvořit obvod splňující dané podmínky:

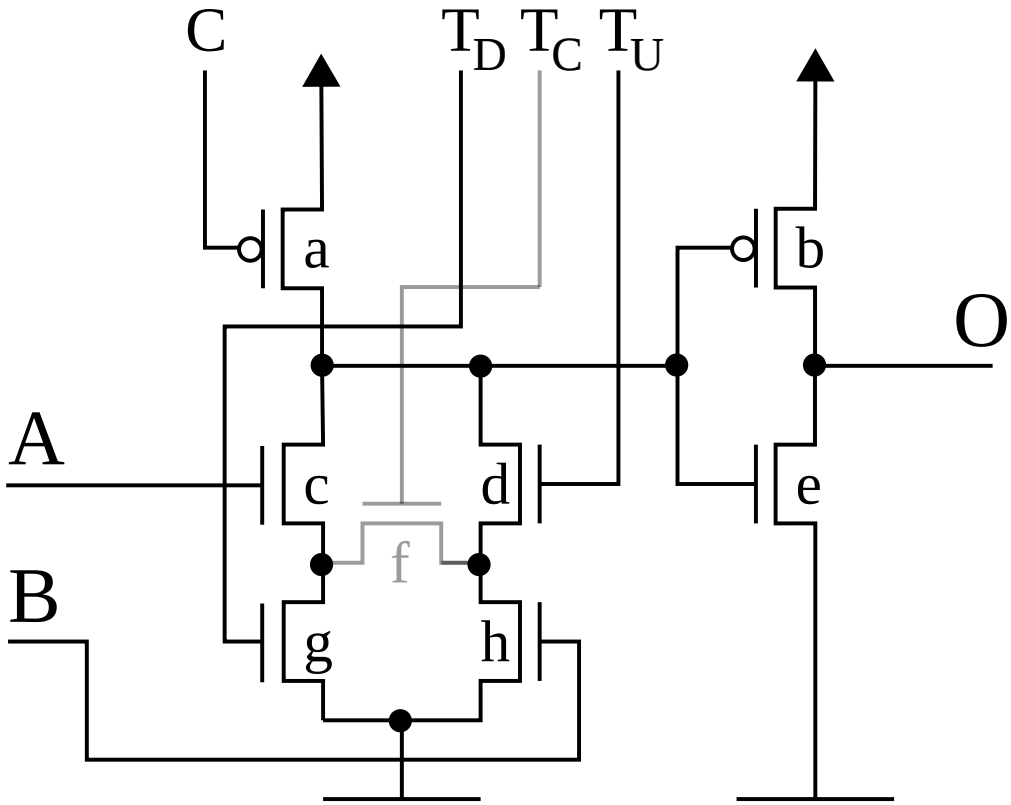
- převést obvod na monotónní – *dual-rail logika*
- použít rekonfigurovatelné hradla – OR/AND

# Dokončený výzkum
## Rekonfigurovatelné hradlo



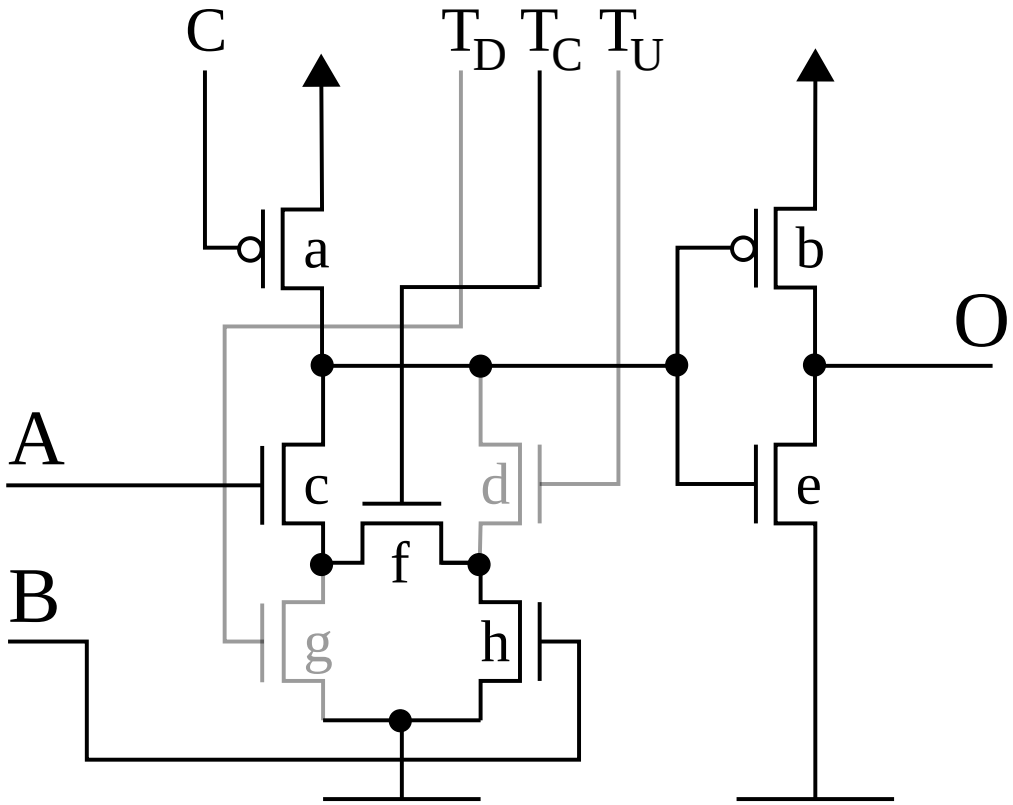

- Domino-logic AND/OR

# Dokončený výzkum
## Rekonfigurovatelné hradlo



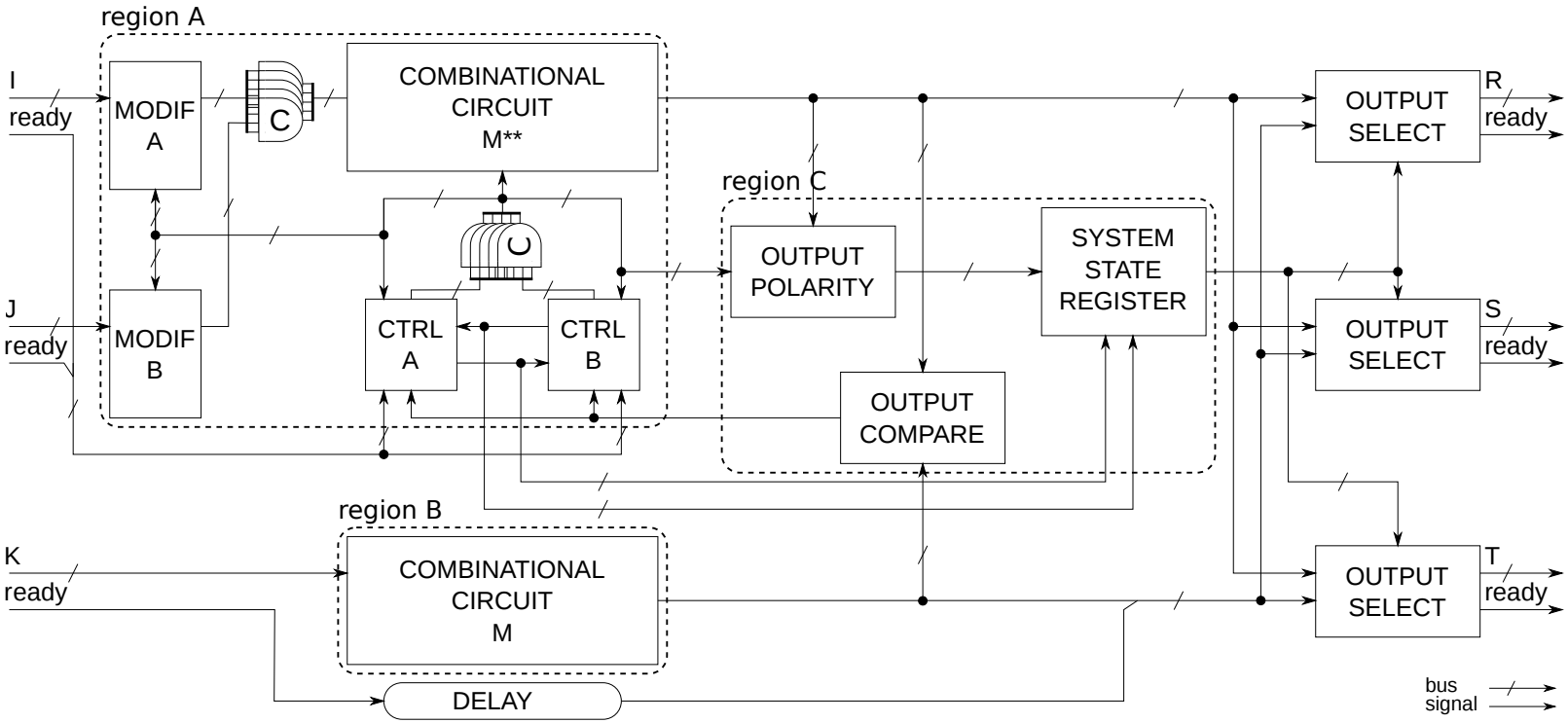

- Domino-logic OR $T_D = 1,\ T_C = 0,\ T_U = 1$

# Dokončený výzkum
## Rekonfigurovatelné hradlo

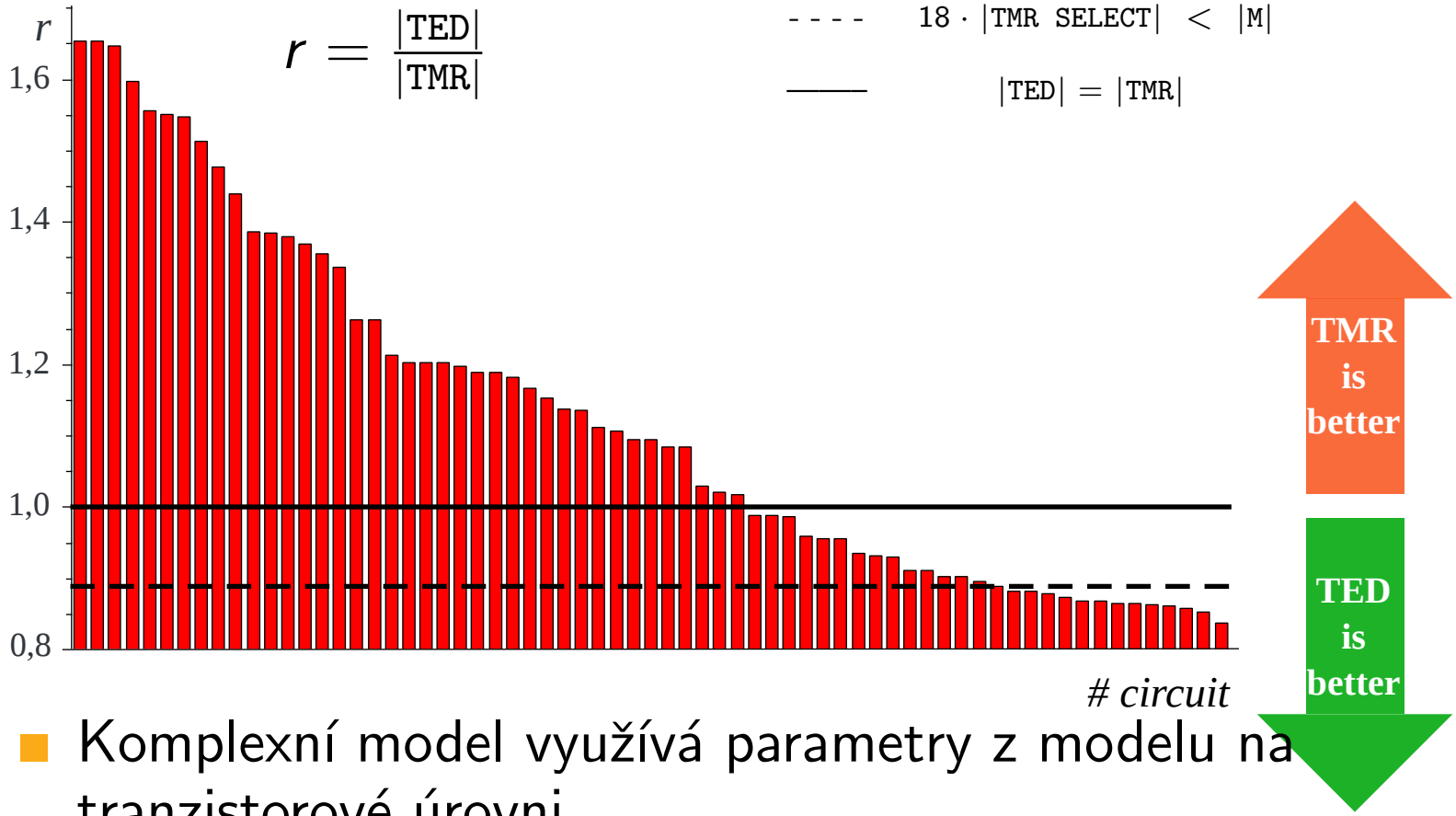



- Domino-logic AND $T_D = 0,\ T_C = 1,\ T_U = 0$

# Dokončený výzkum
## Architektura TED

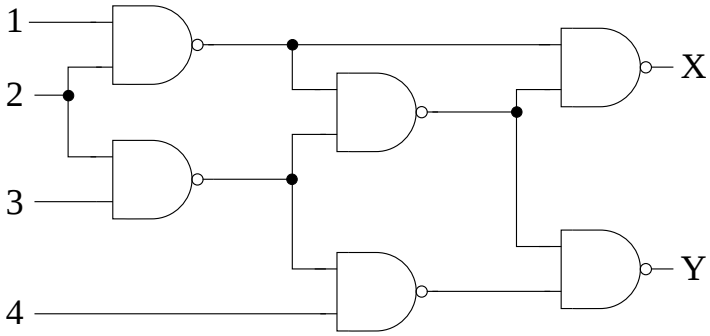


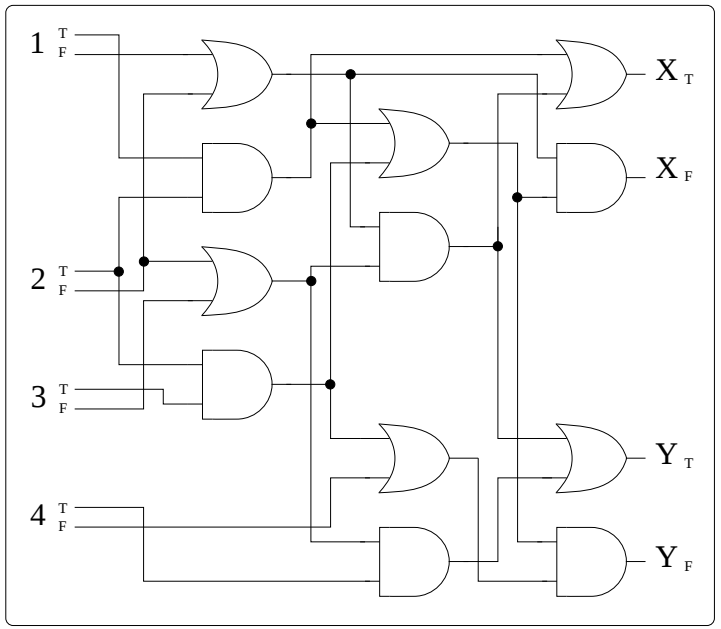
# Dokončený výzkum
## Výsledky: Obvody IWLS'2005



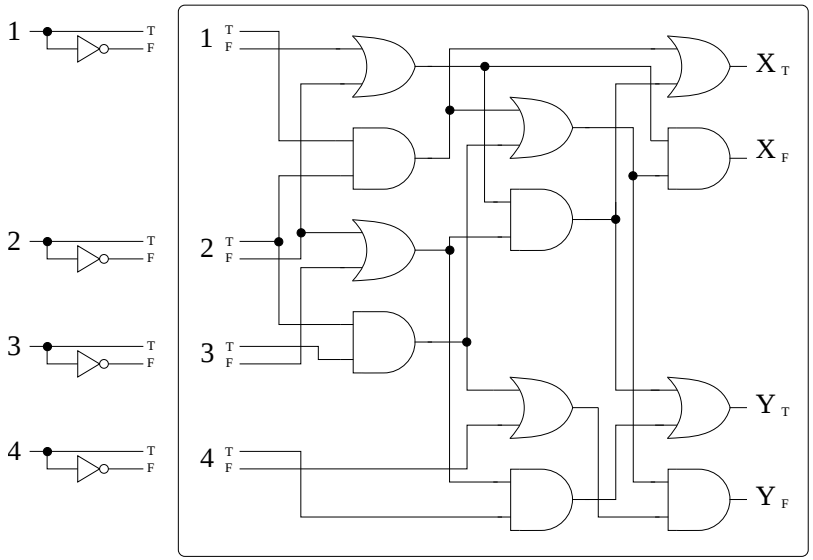

- Komplexní model využívá parametry z modelu na tranzistorové úrovni
  - → přesný odhad plochy a zpoždění
- TED-friendly obvody byly identifikovány

# Otevřené problémy
## Dual-Rail implementace

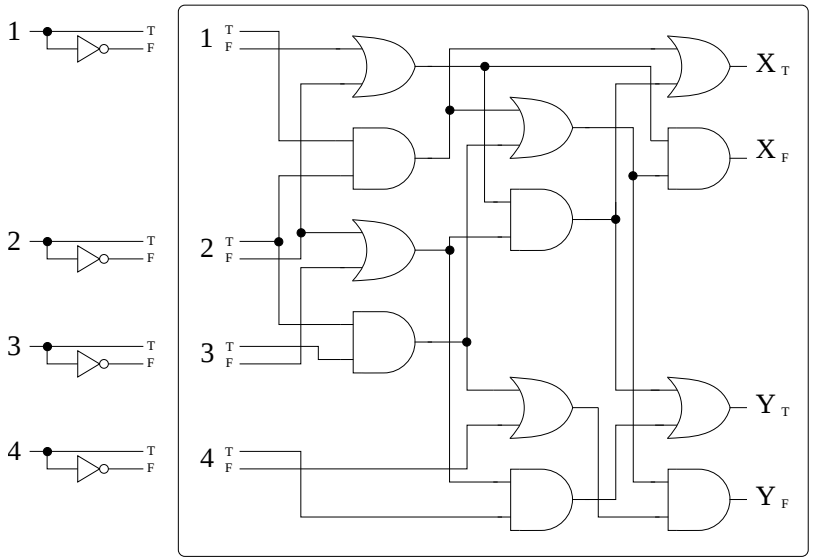


# Otevřené problémy
## Dual-Rail implementace

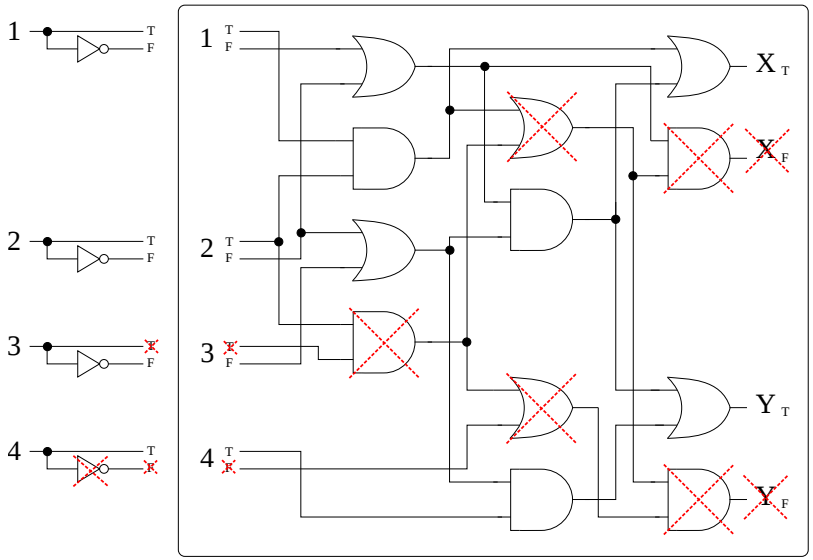


# Otevřené problémy
## Dual-Rail implementace



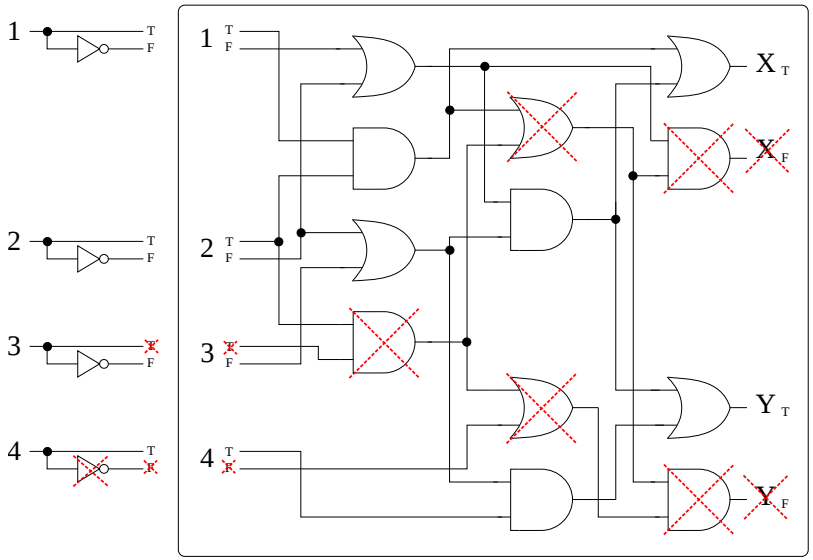

- Je-li dual-rail logika použita pouze jako náhrada invertorů, (většinou) lze (výrazně) redukovat počet hradel

# Otevřené problémy
## Dual-Rail redukce



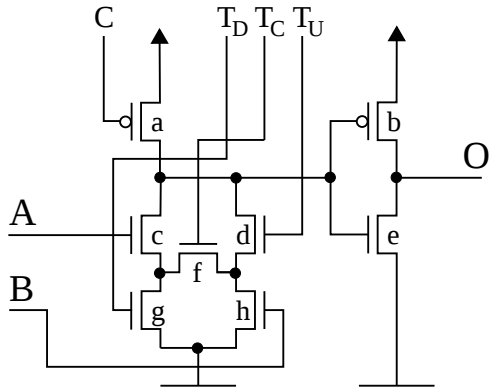

- Je-li dual-rail logika použita pouze jako náhrada invertorů, (většinou) lze (výrazně) redukovat počet hradel
- V nejlepším případě může dojít k redukci počtu hradel až o polovinu

# Otevřené problémy
## Dual-Rail redukce



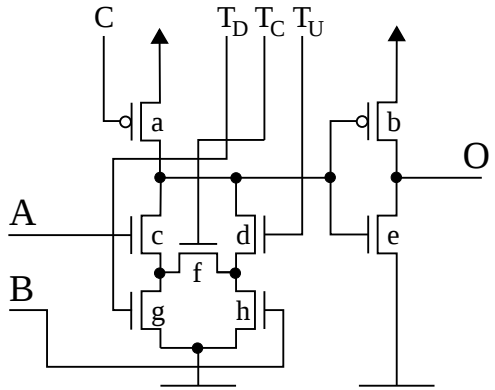

- Je-li dual-rail logika použita pouze jako náhrada invertorů, (většinou) lze (výrazně) redukovat počet hradel
- V nejlepším případě může dojít k redukci počtu hradel až o polovinu
- Někdy může být polarita výstupů volitelná – to ovlivňuje *úspěšnost redukce* → heuristiky

# Dokončený výzkum
## Těžko řešitelné problémy



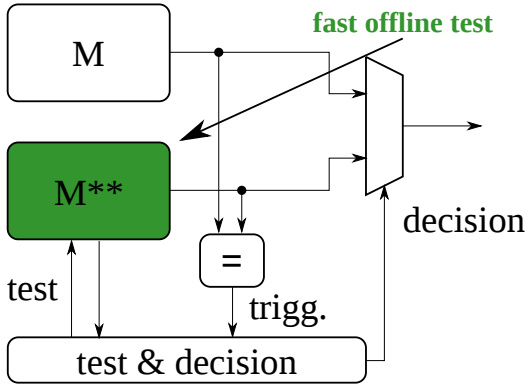

- Řídící signály (+3) komplikují hradlo – metalové vrstvy

# Dokončený výzkum
## Těžko řešitelné problémy




- Řídící signály (+3) komplikují hradlo – metalové vrstvy
- Lze navrhnout hradlo s více než dvěma vstupy se stejnými vlastnostmi? Velmi těžko! Možno spojením dvouvstupových hradel $\rightarrow$ zvýšení hloubky obvodu

# Dokončený výzkum
## Těžko řešitelné problémy




- Řídící signály (+3) komplikují hradlo – metalové vrstvy
- Lze navrhnout hradlo s více než dvěma vstupy se stejnými vlastnostmi? Velmi těžko! Možno spojením dvouvstupových hradel → zvýšení hloubky obvodu
- Lze usuzovat, že když nenaleznu chybu v jednom modulu, je určitě v druhém? I při použití přesného poruchového modelu to nelze tvrdit s jistotou (i když ppst je velmi vysoká)

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Další kroky v doktorském studiu

- Otevřené problémy – předchozí výzkum:
  - single-rail $\rightarrow$ dual-rail – "syntéza na míru"
  - *nutné podmínky* pro krátký test

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Další kroky v doktorském studiu

- Otevřené problémy – předchozí výzkum:
  - single-rail $\rightarrow$ dual-rail – "syntéza na míru"
  - *nutné podmínky* pro krátký test
- Mikroarchitektury pro zvýšení spolehlivosti a odolnosti proti kombinovaným útokům:

# Další kroky v doktorském studiu

- Otevřené problémy – předchozí výzkum:
  - single-rail $\rightarrow$ dual-rail – "syntéza na míru"
  - *nutné podmínky* pro krátký test
- Mikroarchitektury pro zvýšení spolehlivosti a odolnosti proti kombinovaným útokům:
  - šifrovací klíč nelze zrekonstruovat z pozorování výstupu zařízení, či postranních kanálů, a to i při poruše

# Další kroky v doktorském studiu

- Otevřené problémy – předchozí výzkum:
  - single-rail $\rightarrow$ dual-rail – "syntéza na míru"
  - *nutné podmínky* pro krátký test
- Mikroarchitektury pro zvýšení spolehlivosti a odolnosti proti kombinovaným útokům:
  - šifrovací klíč nelze zrekonstruovat z pozorování výstupu zařízení, či postranních kanálů, a to i při poruše
  - předpokládáme, že útočník má plný přístup k zařízení

# Další kroky v doktorském studiu

- Otevřené problémy – předchozí výzkum:
  - single-rail $\rightarrow$ dual-rail – "syntéza na míru"
  - *nutné podmínky* pro krátký test
- Mikroarchitektury pro zvýšení spolehlivosti a odolnosti proti kombinovaným útokům:
  - šifrovací klíč nelze zrekonstruovat z pozorování výstupu zařízení, či postranních kanálů, a to i při poruše
  - předpokládáme, že útočník má plný přístup k zařízení
  - eliminace vyzařování postranními kanály vyžaduje návrh na co nejnižší úrovni

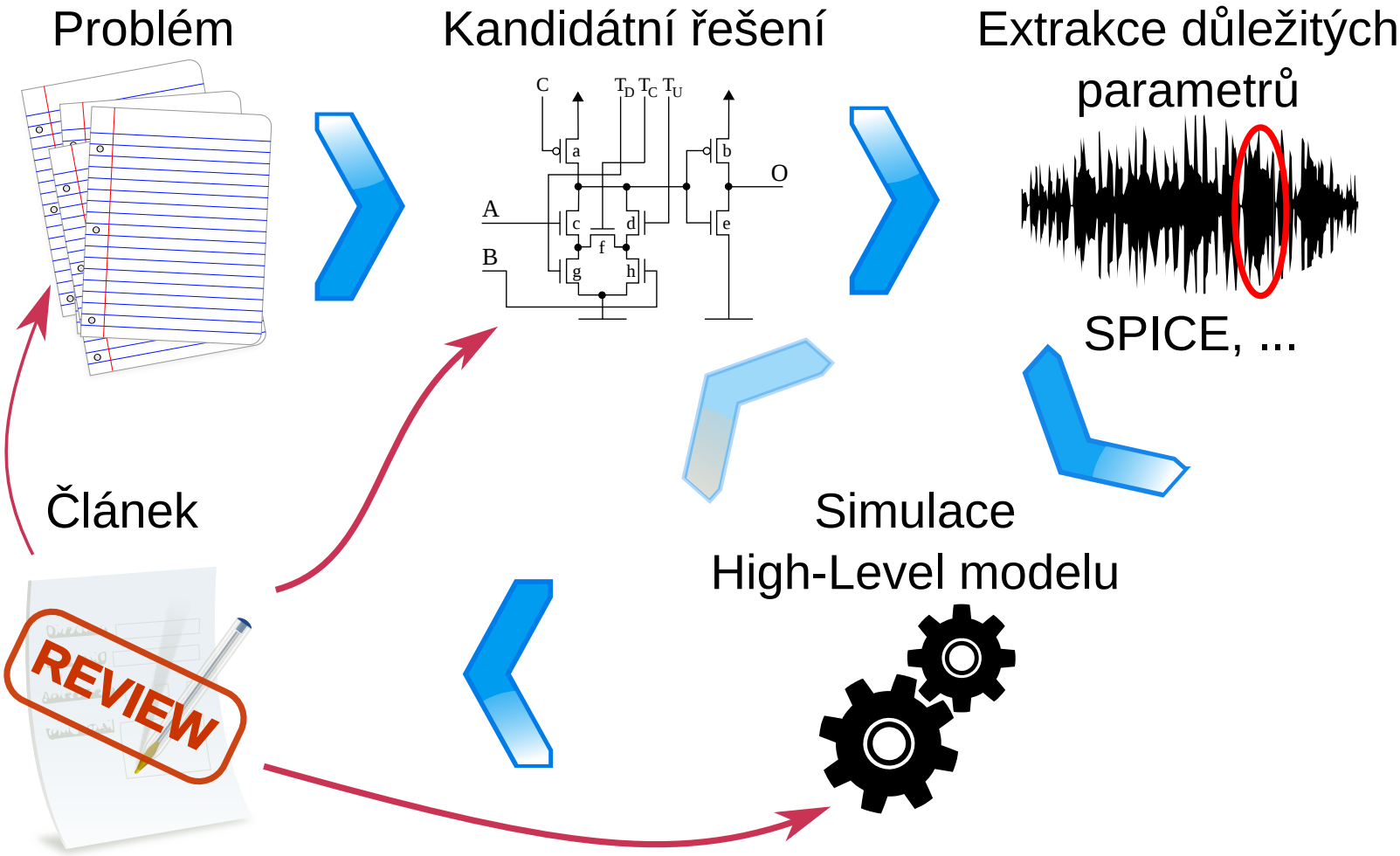
# Další kroky v doktorském studiu

- Otevřené problémy – předchozí výzkum:
  - single-rail $\rightarrow$ dual-rail – "syntéza na míru"
  - *nutné podmínky* pro krátký test
- Mikroarchitektury pro zvýšení spolehlivosti a odolnosti proti kombinovaným útokům:
  - šifrovací klíč nelze zrekonstruovat z pozorování výstupu zařízení, či postranních kanálů, a to i při poruše
  - předpokládáme, že útočník má plný přístup k zařízení
  - eliminace vyzařování postranními kanály vyžaduje návrh na co nejnižší úrovni
  - řešení odolná proti kombinovaným útokům (téměř) neexistují (jsou velmi slabá)

# Další kroky v doktorském studiu

- Otevřené problémy – předchozí výzkum:
  - single-rail $\rightarrow$ dual-rail – "syntéza na míru"
  - *nutné podmínky* pro krátký test
- Mikroarchitektury pro zvýšení spolehlivosti a odolnosti proti kombinovaným útokům:
  - šifrovací klíč nelze zrekonstruovat z pozorování výstupu zařízení, či postranních kanálů, a to i při poruše
  - předpokládáme, že útočník má plný přístup k zařízení
  - eliminace vyzařování postranními kanály vyžaduje návrh na co nejnižší úrovni
  - řešení odolná proti kombinovaným útokům (téměř) neexistují (jsou velmi slabá)
  - maskování chyb se (téměř) neuvažuje

# Budoucí výzkum
## Metodologie výzkumu



CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Projekty


- SGS14/105/OHK3/1T/18, Czech Technical University in Prague
- SGS15/119/OHK3/1T/18, Czech Technical University in Prague
- SGS16/121/OHK3/1T/18, Czech Technical University in Prague
- 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)*

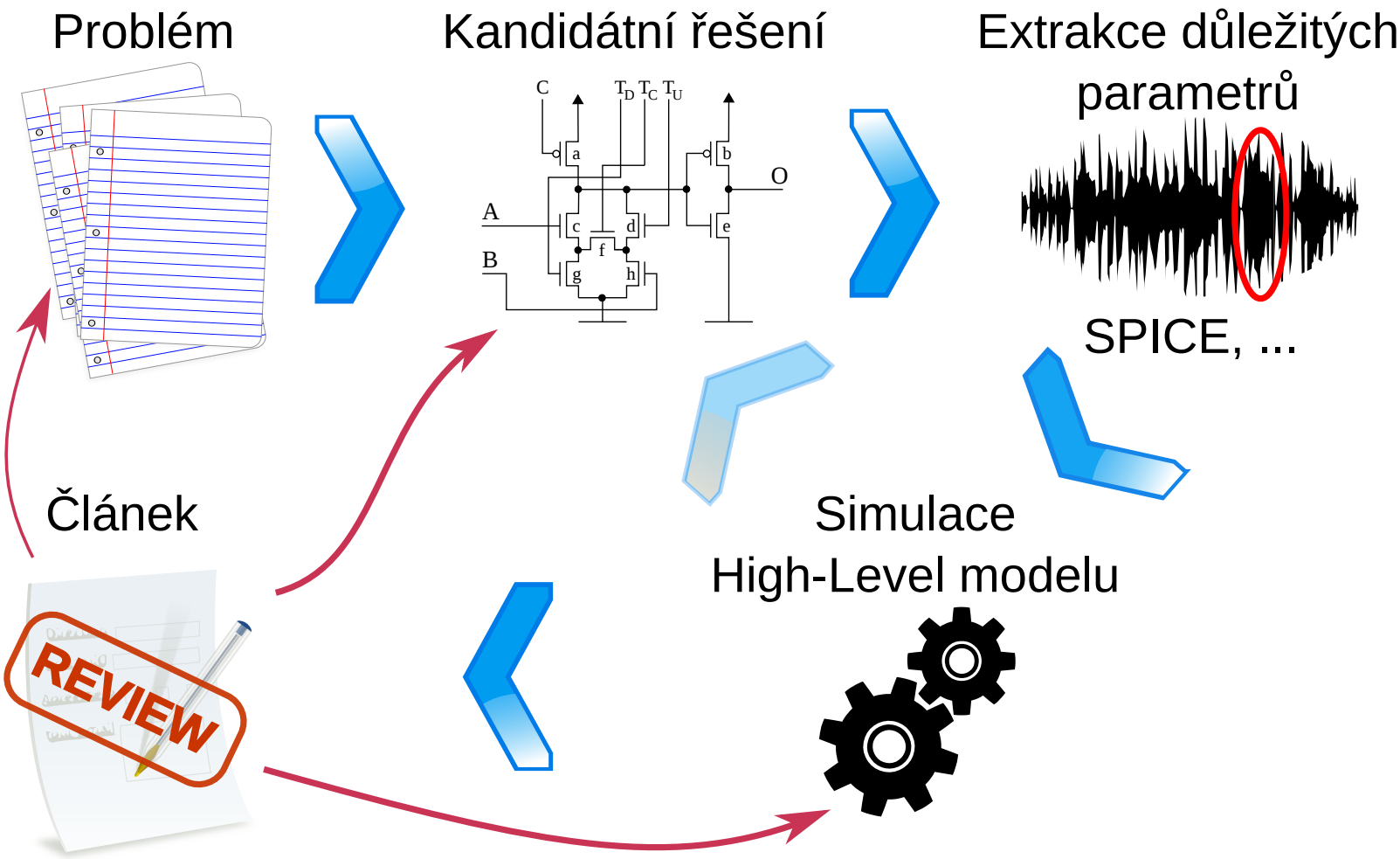
# Publikace
## Publikace nesouvisející s dizertací

- J. Bělohoubek, "Smart re-use of hardware peripherals for better software UART," *in The 3rd Prague Embedded Systems Workshop, 2015, Roztoky u Prahy, Czech Republic*.

# Publikace
## Nepřijaté publikace

- J. Bělohoubek, P. Fišer, and J. Schmidt, "Design for Short-Duration Test Based on Dynamic Logic," *was submitted to the 22nd IEEE International Symposium on Asynchronous Circuits and Systems, 2016, Porto Alegre, Brazil*.

# Publikace
## Nepřijaté publikace



# Publikace
## 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*.

# 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)

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Budoucí výzkum

- monotónní obvody jsou zajímavé – zkusíme dát dohromady syntézu a snížit overhead při převodu single-rail $\rightarrow$ dual-rail (spolupráce s VUT Brno)

# Budoucí výzkum

- monotónní obvody jsou zajímavé – zkusíme dát dohromady syntézu a snížit overhead při převodu single-rail $\rightarrow$ dual-rail (spolupráce s VUT Brno)
- pro útoku-odolné a spolehlivé systémy je lokalizace poruch a maskování chyb na co nejnižší úrovni nutné

# Budoucí výzkum

- monotónní obvody jsou zajímavé – zkusíme dát dohromady syntézu a snížit overhead při převodu single-rail $\rightarrow$ dual-rail (spolupráce s VUT Brno)
- pro útoku-odolné a spolehlivé systémy je lokalizace poruch a maskování chyb na co nejnižší úrovni nutné
- metodologie je správná – umožňuje (relativně) rychlý postup vpřed, dává přesné výsledky, odhaluje slabiny

# Budoucí výzkum

- monotónní obvody jsou zajímavé – zkusíme dát dohromady syntézu a snížit overhead při převodu single-rail $\rightarrow$ dual-rail (spolupráce s VUT Brno)
- pro útoku-odolné a spolehlivé systémy je lokalizace poruch a maskování chyb na co nejnižší úrovni nutné
- metodologie je správná – umožňuje (relativně) rychlý postup vpřed, dává přesné výsledky, odhaluje slabiny
- recenze korigují směr výzkumu

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Děkuji!

- monotónní obvody jsou zajímavé – zkusíme dát dohromady syntézu a snížit overhead při převodu single-rail $\rightarrow$ dual-rail (spolupráce s VUT Brno)
- pro útoku-odolné a spolehlivé systémy je lokalizace poruch a maskování chyb na co nejnižší úrovni nutné
- metodologie je správná – umožňuje (relativně) rychlý postup vpřed, dává přesné výsledky, odhaluje slabiny
- recenze korigují směr výzkumu