Zvyšování spolehlivosti a bezpečnosti číslicových obvodů na úrovni mikroarchitektury

Jan Bělohoubek
4. ročník, prezenční studium
Školitel: doc. Ing. Petr Fišer, Ph.D.
Školitel specialista: doc. Ing. Jan Schmidt, Ph.D.

Fakulta informačních technologií ČVUT v Praze
Thákurova 9, 160 00 Praha 6
jan.belohoubek@fit.cvut.cz

***Abstrakt*—Spolehlivost a bezpečnost jsou důležité vlastnosti vyžadované od mnoha zařízení. Zvýšení spolehlivosti a bezpečnosti systému lze dosáhnout mimo jiné vhodnou mikroarchitekturou. Dokončený výzkum se věnoval právě zvyšování spolehlivosti číslicových systémů na úrovni mikroarchitektury. Výzkum na něj bezprostředně navazující cílí na řešení spojující přístupy zajišťující zároveň bezpečnost i spolehlivost dílčích částí číslicových systémů. Velká část příspěvku je věnována rešerši, jež se váže k navrhovanému konceptu μTMR.**

***Klíčová slova*—Spolehlivost, bezpečnost, Time-Extended Duplex, dvoudrátová logika, monotónní obvod, postranní kanál**

I. Úvod

Spolehlivost a bezpečnost jsou důležité vlastnosti vyžadované od mnoha zařízení. Vzhledem k širokému použití číslicových (digitálních) systémů v různých podmínkách se stále zvyšují nároky kladené na spolehlivost (*dependability*, *reliability*, *safety*) a bezpečnost (*security*) těchto systémů.

Vysoká spolehlivost a bezpečnost zařízení (při zvážení provozních podmínek a konkrétního nasazení) je podmíněna dobrým návrhem architektury celého systému. Zvýšení spolehlivosti a bezpečnosti systému lze však dosáhnout i na úrovni mikroarchitektury – např. použitým návrhovým stylem, či speciálních logických prvků zaručujících určité vlastnosti. V některých případech je dokonce nutné použít speciální návrhové postupy na úrovni mikroarchitektury, aby bylo možné zajistit požadované vlastnosti na makroúrovni.

Některé prvky systému, např. kryptografické obvody, mohou vyžadovat zvýšenou úroveň zabezpečení proti možnému odcizení tajného klíče (příkonová charakteristika zařízení musí být nezávislá na zpracovávaných datech). Jiné části systému, např. řídící systém musí být schopen celý systém uvést při poruše do bezpečného stavu, apod.

Příspěvek je členěn takto: ve zbytku úvodní kapitoly jsou shrnuty cíle dizertační práce a současný stav jejího řešení. Kapitola II slouží jako stručná rešerše, ve které je shrnut současný stav problematiky okolo útoků na kryptografická zařízení se zaměřením na oblast současné výzkumné aktivity. V kapitole III je rozebrán současný stav řešení dosud rozpracované části práce.

Příspěvek se věnuje výhradně tématům výzkumu souvisejícím s dizertační prací. Ostatní aktivity a publikace jsou uvedeny na webu autora[1].

A. Cíle dizertační práce

V rámci výzkumu vedoucího k vypracování dizertační práce jsem se zaměřil na návrhové postupy na úrovni mikroarchitektury číslicových systémů, tj. na úrovni hradel a obvodů, vedoucí ke zvýšení spolehlivosti dílcích částí číslicového systému.

Vzhledem k důležitosti problematiky bezpečnosti, a s přihlédnutím k zaměření výzkumného pracoviště (*Digital Design research Group na FIT ČVUT*) a řešeným výzkumným grantům, se významná pozornost výzkumu soustředila také na hodnocení bezpečnosti kryptografických zařízení a jejího možného zvýšení právě z pohledu mikroarchitektury.

Oba cíle dizertační práce jsou vzájemně komplementární vzhledem k použitým metodám, simulačním a vývojovým prostředkům.

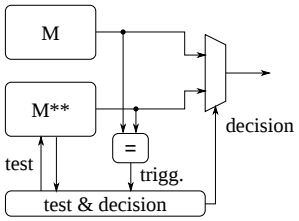
B. Dokončený výzkum: Time-Extended Duplex

Výzkum na nějž jsem se soustředil v prvních třech letech doktorského studia se zabýval návrhem spolehlivé architektury číslicových systémů – *Time-Extended Duplex (TED)* – kombinující redundanci v ploše a v čase, tak aby se minimalizovaly náklady na takové řešení (*area overhead*, *time overhead*). Konceptuální schéma výsledného řešení, které je hlediska plochy pro skupinu obvodů výhodnější než TMR (*Triple Modular Redundancy*), ale zároveň poskytuje srovnatelnou odolnost proti poruchám (*fault-tolerance*), je na obrázku 1.

Modul $\mathtt{M}^{\star\star}$ na obrázku 1 je testovatelný pomocí rychlého testu se 100% pokrytím poruch vzhledem k modelu poruch *trvalá 1/trvalá 0* (*stuck-at model*). Díky tomu je v případě poruchy možno lokalizovat poruchu a vybrat tak správný ze dvou výstupů duplexu.

Vzhledem ke speciálním vlastnostem umožňujícím rychlý test číslicového obvodu (jednotky cyklů) byly navrženy

[1] http://users.fit.cvut.cz/~belohja4/



Obrázek 1. Konceptuální schéma TED – jedná se o duplex se schopností opravy jedné chyby

speciální hradla inspirovaná metodami asynchronního návrhu [1]. Testovatelný obvod je navíc navržen jako modifikovaná $\mathtt{M}^{**}$ verze dvoudrátové logiky a je tedy monotónní [1].

Obdobnou problematikou se zabývali i Vierhaus [2], Kubalík [3], Borecký [4] nebo Baláž a Krištofík [5].

Dílčí výstupy výzkumu byly publikovány na řadě lokálních i mezinárodní workshopech a konferencích [JBn1], [JBn2], [JBn3], [JBn4], [JBr1], [JBr2].

Všechny výsledky, experimentální vyhodnocení a podrobný popis architektury a návrhového stylu byl publikován jako součást zprávy o průběhu doktorského studia (tzv. *minimum*) [JBn5] a v článku publikovaném v žurnálu *Microprocessors and Microsystems* [JBr3].

Do odevzdání dizertační práce bude ještě potřeba věnovat pozornost zobecnění podmínek umožňujícím krátký test číslicových obvodů s vysokým pokrytím poruch, případně možnostem realizace krátkého testu s vysokým pokrytím poruch při použití realističtějších poruchových modelů.

II. Útoky na kryptografická zařízení

I když jsou dnešní šifrovací algoritmy, např. AES s dostupnou technikou z principu neprolomitelné, tajný klíč, uložený v zařízení, je možno získat v reálném čase útokem na implementaci šifrovacího algoritmu v HW nebo v SW. Útokem se rozumí manipulace se zařízením, která má za cíl extrakci tajného klíče pomocí tzv. *postranního kanálu* (*side-channel*). Formálně řečeno: postranní kanál je sekundární projev zařízení umožňující kritické snížení entropie tajného klíče [6], [7].

Postranním kanálem může být jakýkoli proměnlivý (datově závislý) projev, např. čas výpočtu, odběr, EM vyzařování nebo dokonce chování při chybě. Podmínkou pro vedení útoku na HW kryptografické zařízení je (zpravidla) fyzický přístup k zařízení. Fyzický přístup je u některých zařízení omezen, avšak s rostoucím počtem *smart karet* nebo *IoT zřízení* (zařízení tzv. internetu věcí) se množství potenciálně zranitelných zařízení stále zvětšuje [8].

Útoky na kryptografická zařízení postranním kanálem můžeme rozdělit na [9]:

1) neinvazivní (non-invasive attack): měření běžných projevů zařízení: časová [10] a odběrová analýza – *Simple Power Analysis* (SPA) a *Differential Power Analyzis* (DPA) [11], [12], [9] – nebo analýza EM vyzařování, tj. *EM radiation*

2) poloinvazivní (semi-invasive attack): injekce přechodných poruch – EM impulzem nebo laserovým paprskem

3) invazivní (invasive attack): injekce trvalých poruch

A. Hodnocení útoků postranními kanály

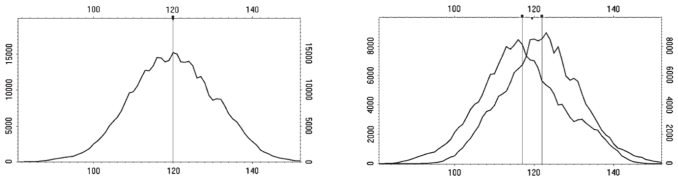
Závažnost různých typů útoku na kryptografické zařízení se obecně vyjadřuje náklady, které je nutné vynaložit k úspěšnému provedení útoku (*attack cost*), přičemž nejnebezpečnější útoky jsou takové, které lze provést s minimálním technickým vybavením, v minimálním čase a s minimálními znalostmi.

B. Neinvazivní útoky na základě příkonové analýzy

Z výše uvedeného důvodu jsou útoky na základě příkonové analýzy nejzkoumanější skupinou útoků a také skupinou útoků, kterým věnují největší pozornost výrobci HW. Postranním kanálem je zde příkonová charakteristika obvodu.

Útoky na kryptografická zařízení pomocí *příkonové analýzy* (*Simple Power Analyzis* (SPA) a *Differential Power Analyzis* (DPA)) byly představeny ve 2. pol. 90 let Kocherem a kol. [11], [12] z firmy Cryptography Research, Inc. (CRI) (od roku 2011 Rambus Inc.). Od té doby se intenzivní výzkum soustředil na jedné straně na metody útoků na kryptografická zařízení a na straně druhé na metody obrany (*countermeasures*). Společnost Rambus je dnes předním dodavatelem certifikovaných řešení odolných proti SPA/DPA [13].

Odběrová analýza pracuje s faktem, že odběr IC je datově závislý. Pouhým pohledem na odběrovou charakteristiku IC, v případě SPA, nebo pomocí matematické statistiky a za předpokladu velkého množství provedených měření, v případě DPA, lze odvodit tajný klíč používaný kryptografickým zařízením. Datovou závislost příkonové charakteristiky lze demonstrovat pomocí metody *rozdílu středních hodnot* [14] – viz obrázek 2.



Obrázek 2. Distribuce průběhu příkonové charakteristiky IC – pro směs všech průběhů a pro dvě směsi rozlišené dle hodnoty LSB (LSB = 0, resp. LSB = 1); převzato z [14]

C. Ochrany proti analýze odběru

Ochrany můžeme rozdělit i) na ty, které jsou aplikovány na úrovni mikroarchitektury – na úrovni tranzistorů a hradel, případně logického obvodu, rep. návrhového stylu a ii) na ochrany, které jsou aplikovány na úrovni algoritmu.

Na úrovni mikroarchitektury je cílem ochrany proti prosáknutí informace postranním kanálem snížením poměru signál/šum (*Signal to Noise Ratio (SNR)*. Toho lze dosáhnout zvýšením šumu (změna pořadí vykonávání nebo generování nekorelovaného šumu) nebo zmenšením signálu, tj. zvýšení nezávislosti mezi zpracovávanými daty a spotřebou.

Pro snížení závislosti průběhu příkonové charakteristiky na zpracovávaných datech se často používá *dvoudrátová logika*

(*Dual-Rail Precharge Logic*) v synchronní nebo asynchronní variantě, která je *monotónní* a pro každý signál pracuje zároveň s jeho komplementem. Upřednostňují se pak takové návrhové styly, které umožňují využít standardních knihovních buněk (*standard cells*) a nevyžadují tak tvorbu speciální knihovny pro každou technologii. Nejznámější takovou metodou je *Wave Dynamic Differential Logic (WDDL)* [15], [16], poměrně zajímavou alternativu představuje metoda *Dual Spacer Dual-Rail*, která umožňuje teoreticky dosáhnout naprosté nezávislosti zpotřebované energie na zpracovávaných datech (v průběhu jednoho cyklu) [17]. Další široce používanou metodou je *Masked Dual-rail with Pre-charge Logic (MDPL)* [13], [18], která vychází z dvoudrátové logiky, ale navíc přidává maskování na úrovni logických buněk.

Maskování na úrovni algoritmu je v principu silnější [16]. Používá se k odstranění závislosti odběru na zpracovávaných datech. Místo toho je odběr IC závislý na maskovaných datech. Nevýhodou těchto metod, např. *Boolean masking* [16] nebo *Threshold Implementation* je velmi výrazná penalizace v oblasti plochy, spotřeby a výkonu – např. $\approx$ 5x větší plocha u (velice efektivní) implementace od A. Moradiho a kol. [19].

Z důvodu obecně menší složitosti metod, větší přímočarosti implementace a zejména pak nižší penalizace v oblasti plochy, výkonu a spotřeby a zároveň uspokojivé bezpečnosti je v průmyslu preferována první skupina ochran proti analýze odběru [13]. De-fakto standardem jsou tak metody maskování založené na dvoudrátové logice.

D. Poloinvazivní a invazivní útoky na základě injekce poruch

Další široce zkoumanou skupinou útoků na kryptografická zařízení jsou útoky využívající injekce (trvalých nebo přechodných) poruch. Tyto metody lze kategorizovat dle způsobu injekce poruch, např.: optická injekce, glitch na hodinovém signálu, rušení napájení, elektromagnetický impulz, apod. Jejich historie sahá do roku 1996, kdy byla představena metoda *Differential Fault Analyzis (DFA)* [20].

Metoda DFA používá výstupy šifrovacího algoritmu bez přítomnosti poruchy a za přítomnosti poruchy pro totožný klíč. Na základě diferencí je pak možno výrazně zmenšit počet kandidátů tajného klíče nebo dokonce klíč přesně určit.

Další metodou je *Fault Sensitivity Analyzis (FSA)* [21], jejíž princip spočívá ve vyžití závislosti délky faktické kritické cesty v kryptografickém obvodu na zpracovávaných datech.

Velmi zajímavou metodou je *Safe-Error Attack (SEA)*, kde k určení tajného klíče postačuje informace o tom, zda injekce poruchy způsobila změnu hodnoty na výstupu, či nikoli [22].

E. Ochrany proti (polo)invazivním útokům

Základní ochranou proti útokům založeným na injekci poruch je detekce projevu poruchy, tj. chyby, založená na duplexní architektuře [23]. Je-li detekována chyba, vystaví se na výstup obvodu definovaná (neplatná) data – u dvoudrátové logiky typicky `NULL`, tj. `(0, 0)`.

Pro některé typy útoků, např. *Safe-Error Attack (SEA)*, však nemusí být detekce chyby dostatečná, protože stačí informace, zda injekce poruchy způsobila např. změnu hodnoty v registru – chybu je potřeba opravit, ne pouze detekovat.

F. Kombinované útoky

Z hlediska zranitelnosti kryptografických obvodů je velmi problematická skupina tzv. *kombinovaných útoků*, kde se pro získání tajného klíče využívá nejen znalost chybového/bezchybného výstupu, ale také jiného postranního kanálu, např. příkonové charakteristiky [24].

Takové útoky jsou potenciálně velmi nebezpečné, protože znamenají nutnost integrace ochran pro různé typy útoků tak, aby informace pokud možno neunikla žádným postranním kanálem.

III. Koncept μTMR pro kryptografické aplikace

Jako ochranu proti kombinovaným útokům a zároveň jako spolehlivostní řešení navrhuji koncept *μTMR*. Cílem μTMR je zvýšení odolnosti proti přirozeným zdrojům poruch i proti útokům injekcí poruch. Zároveň by μTMR mělo minimalizovat množství informace potenciálně dostupné přes všechny možné postranní kanály. To vše při co nejmenším nárůstu plochy a spotřeby a ideálně za použití standardních buněk.

Návrhový styl využívající μTMR použije tzv. *μ-voterů* rozprostřených v celém obvodu tak, aby detekce a oprava chyb (vniklých vlivem přirozených nebo nebo injektovaných poruch) probíhala co nejblíže místu poruchy (lokalita), a tak byl projev poruchy v postranních kanálech co nejmenší.

Podobný koncept byl zkoumán na platformě FPGA, avšak pouze z hlediska spolehlivosti [25], [26].

A. Otevřené problémy

V rámci práce na tématu μTMR budu řešeny následující otevřené problémy (klesající priorita):

- Efektivní implementace μ-voteru ze standardních buněk
- Rozmístění μ-voterů v obvodu a jeho vliv na požadované vlastnosti systému založeného na konceptu μTMR: vliv na zranitelnost útoky postranními kanály, realistický model injekce poruch a spolehlivostní parametry
- Optimální implementace μ-voterů v technologii CMOS (nehledě na standardní buňky)
- Simulace velkých (komb.) obvodů s podporou SPICE

B. Metodologie

Na základě předchozích zkušeností z práce na spolehlivostních architekturách, monotónních, synchronních i asynchronních obvodech a jejich mikroarchitektuře a vzhledem k návrhovým stylům preferovaných průmyslem bude μTMR stavět na variantě dvoudrátové logiky od Sokolova a kol. [17], s tím, že v úvahu bude vzato maskování mezivýsledků [13].

Na sadě benchmarků bude provedeno hodnocení ceny (plocha, rychlost), zranitelnosti a spolehlivosti obvodů. Malé benchmarkové obvody budou ověřeny v systému SPICE (ngSPICE) pro relevantní CMOS technologie. Pro větší obvody bude použit méně přesný simulátor, nebo rychlejší simulace s podporou SPICE (ve vývoji).

C. Přípravné práce – μTMR

Výsledky týkající se hodnocení zranitelnosti obvodů na základě simulace (ngSPICE, IRSIM) byly publikovány na workshopu CryptArchi 2017 [JBn6] a výsledky týkající se kvality dat použitých pro realizaci DPA byly prezentovány na workshopu Trudevice 2018 [JBn7].

Na základě zkuseností získaných z experimentů prezentovaných v [JBn7] lze pomocí simulace provést férové zhodnocení zranitelnosti systému založeného na µTMR.

IV. Závěr

Příspěvek shrnuje současný stav řešení dizertační práce. Část práce týkající se zvyšování spolehlivosti číslicových obvodů na úrovni mikroarchitektury je již dokončena.

Většina příspěvku je věnována probíhajícímu výzkumu spolehlivých a bezpečných mikroarchitektur, zejména rešerši. Dokončení druhé části výzkumu a doktorského studia je plánováno na následující rok.

Poděkování

GAČR GA16-05179S, ČVUT SGS17/213/OHK3/3T/18.

Reference

[1] J. Sparsø and S. Furber, *Principles of Asynchronous Circuit Design: A Systems Perspective*, 1st ed. Kluwer Academic Publishers, Boston, 2001.

[2] T. Koal, M. Scholzel, and H. Vierhaus, "Combining fault tolerance and self repair at minimum cost in power and hardware," in *17th International Symposium on Design and Diagnostics of Electronic Circuits Systems*, April 2014, pp. 153–158.

[3] P. Fiser, P. Kubalik, and H. Kubatova, "An Efficient Multiple-Parity Generator Design for On-Line Testing on FPGA," in *11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools, 2008, DSD'08*, Sept 2008, pp. 96–99.

[4] J. Borecký, "Dependable Systems Design Methods for FPGAs," Ph.D. dissertation, the Faculty of Information Technology, Czech Technical University in Prague, 8 2015.

[5] M. Balaz and S. Kristofik, "Generic Self Repair Architecture with Multiple Fault Handling Capability," in *Euromicro Conference on Digital System Design (DSD), 2015*, Aug 2015, pp. 197–204.

[6] L. T. L. M. T. W. . W. G. Killmann, W., "Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations." BSI, Jul 2011. [Online]. Available: http://www.bsi.bund.de

[7] K. Lemke-Rust, "Models and Algorithms for Physical Cryptanalysis." Dissertation, Europäischer Universitätsverlag, 2007.

[8] T. Snyder and G. Byrd, "The Internet of Everything," *Computer*, vol. 50, no. 6, pp. 8–9, 2017. [Online]. Available: doi.ieeecomputersociety.org/10.1109/MC.2017.179

[9] Y. Li, M. Chen, and J. Wang, "Introduction to side-channel attacks and fault attacks," in *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, vol. 01, May 2016, pp. 573–575.

[10] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Annual International Cryptology Conference*. Springer, 1996, pp. 104–113.

[11] P. Kocher, J. Jaffe and B. Jun, "Introduction to Differential Power Analysis and Related Attacks," 1998, technical report. [Online]. Available: http://www.cryptography.com/dpa/

[12] ——, "Differential power analysis," in *Annual International Cryptology Conference*. Springer, 1999, pp. 388–397.

[13] "Security: DPA Countermeasures," 2018. [Online]. Available: https://www.rambus.com/security/dpa-countermeasures/

[14] L. V. Lu Zhang and M. Taylor, "Power Side Channels in Security ICs: Hardware Countermeasures." arXiv, 2016.

[15] Y. Li, K. Ohta, and K. Sakiyama, "Revisit fault sensitivity analysis on wddl-aes," in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, June 2011, pp. 148–153.

[16] V. Lomné, T. Roche, and A. Thillard, "On the Need of Randomness in Fault Attack Countermeasures - Application to AES," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on*, Sept 2012, pp. 85–94.

[17] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Design and analysis of dual-rail circuits for security applications," *IEEE Transactions on Computers*, vol. 54, no. 4, pp. 449–460, April 2005.

[18] A. Moradi and M. Kirschbaum and T. Eisenbarth and C. Paar, "Masked Dual-Rail Precharge Logic Encounters State-of-the-Art Power Analysis Methods," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 9, pp. 1578–1589, Sept 2012.

[19] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: a very compact and a threshold implementation of AES," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2011, pp. 69–88.

[20] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in *Annual international cryptology conference*. Springer, 1997, pp. 513–525.

[21] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2010, pp. 320–334.

[22] S.-M. Yen and M. Joye, "Checking before output may not be enough against fault-based cryptanalysis," *IEEE Transactions on Computers*, vol. 49, no. 9, pp. 967–970, Sep 2000.

[23] S. Bhasin, J. L. Danger, F. Flament, T. Graba, S. Guilley, Y. Mathieu, M. Nassar, L. Sauvage, and N. Selmane, "Combined SCA and DFA Countermeasures Integrable in a FPGA Design Flow," in *2009 International Conference on Reconfigurable Computing and FPGAs*, Dec 2009, pp. 213–218.

[24] F. Amiel, K. Villegas, B. Feix, and L. Marcel, "Passive and active combined attacks: Combining fault attacks and side channel analysis," in *Fault Diagnosis and Tolerance in Cryptography, 2007. FDTC 2007. Workshop on*, Sept 2007, pp. 92–102.

[25] G. L. Nazar, "Fine-grained error detection techniques for fast repair of FPGAs," 2013.

[26] M. Niknahad, *Using Fine Grain Approaches for Highly Reliable Design of FPGA-based Systems in Space*. KIT Scientific Publishing, 2013, vol. 9.

Recenzované publikace autora

[JBr1] 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, pp. 280–283.

[JBr2] J. Belohoubek, P. Fišer, and J. Schmidt, "Error Correction Method Based on the Short-Duration Offline Test," in *2016 Euromicro Conference on Digital System Design (DSD)*, Aug 2016, pp. 495–502.

[JBr3] J. Bělohoubek, P. Fišer, and J. Schmidt, "Error masking method based on the short-duration offline test," *Microprocessors and Microsystems*, vol. 52, pp. 236–250, 2017.

Ostatní publikace autora

[JBn1] J. Bělohoubek, "Fully asynchronous QDI implementation of DES in FPGA," Annency, France, 2014. [Online]. Available: https://labh-curien.univ-st-etienne.fr/cryptarchi/workshop14/presentations.html

[JBn2] ——, "Novel gate design methodology for short-duration test," Prague, Czech Republic, 2015.

[JBn3] ——, "Novel Error Detection and Correction Method Combining Time and Area Redundancy," Zlín, Czech Republic, 2015.

[JBn4] ——, "Využití rychlého offline testu v systému se schopností maskování jedné chyby," Kraví Hora - Bořetice, Czech Republic, 2016.

[JBn5] ——, "Error Correction Method Based on the Efficient Offline Test," Czech Technical University in Prague, Faculty of Information Technology, Tech. Rep., 05 2016.

[JBn6] ——, "The Design-Time Side-Channel Information Leakage Estimation," Smolenice, Slovakia, 2017. [Online]. Available: https://labh-curien.univ-st-etienne.fr/cryptarchi/workshop17/presentations.html

[JBn7] ——, "Effect of Power Trace Set Properties to Differential Power Analysis," Dresden, Germany, 2018.