Agentúra na podporu výskumu a vývoja
Mýtna 23, P.O.BOX 839 04, 839 04 Bratislava 32

Formulár ZK

Záverečná karta projektu

Názov projektu

Útok na elektronický podpis prostredníctvom analýzy spotreby energie a realizácia protiopatrení

Evidenčné číslo projektu **APVV–0586–11**

Zodpovedný riešiteľ **Ing. Michal Varchola, PhD.**

Príjemca **Fakulta elekrotechniky a informatiky TUKE**

Názov pracoviska, na ktorom bol projekt riešený

1. Fakulta elektrotechniky a informatiky TUKE
2. Fakulta elektrotechniky a informatiky STU
3.
4.
5.

Názov a štát zahraničného pracoviska, ktoré spolupracovalo pri riešení

1.
2.
3.

Udelené patenty/podané patentové prihlášky, vynálezy alebo úžitkové vzory, ktoré sú výsledkami projektu

1.
2.
3.

Najvýznamnejšie publikácie (knihy, články, prednášky, správy a pod.) zhrňujúce výsledky projektu – uveďte aj publikácie prijaté do tlače

1. Martin Petrvalsky, Milos Drutarovsky: Constant-weight coding based software implementation of DPA countermeasure in embedded microcontroller, Microprocessors and Microsystems, Elsevier, ISSN 0141-9331. Available online 18 January 2016, http://dx.doi.org/10.1016/j.micpro.2016.01.002 (cc článok)

2. Marek Repka, Michal Varchola, Milos Drutarovsky: Improving CPA Attack Against DSA and ECDSA, Journal of ELECTRICAL ENGINEERING, VOL. 66, NO. 3, 2015, 159–163, ISSN 1335-3632

3. Pavol Zajac: Constructing S-boxes with low multiplicative complexity. In Studia Scientiarum Mathematicarum Hungarica. Vol. 52, No. 2 (2015), pp. 135-153. ISSN 0081-6906

4. Martin Petrvalsky, Tania Richmond, Milos Drutarovsky, Pierre-Louis Cayrel, Viktor Fischer: Countermeasure against the SPA Attack on an Embedded McEliece Cryptosystem. Radioelektronika (RADIOELEKTRONIKA), 2015 25th International Conference, Pardubice, Czech Republic, 21-22 April 2015. ISBN 978-1-4799-8117-5. pp. 462 - 466

5. Michal Varchola, Miloš Drutarovský, Viktor Fischer: New Universal Element with Integrated PUF and TRNG Capability. International Conference on Reconfigurable Computing and FPGAs (ReConFig 2013), 9.-11. Decemeber 2013, Cancun, Mexico. - USA : IEEE, 2013 pp. 1-6. ISBN 978-1-4799-2079-2

Uplatnenie výsledkov projektu

Výsledky projektu sú využiteľné pri realizácii kryptografického hardvéru ktorý musí spĺňať vysoké nároky na bezpečnosť z pohľadu útokov na báze postranných kanálov. Realizačné výstupy projektu je možné využíť pri vývoji kryptografických blokov na platformách mikroprocesorov a obvodov FPGA ako aj pri testovaní účinnosti implementovaných protiopatrení zameraných na zníženie úniku citlivých informácií cez postranné kanály na báze analýzy spotreby. Výsledky navrhnutých algoritmických úprav je možné využiť pri zrobustnení implementácie záverečnej fázy algoritmu výpočtu elektronického podpisu na báze algoritmu ECDSA.

CHARAKTERISTIKA VÝSLEDKOV

Súhrn výsledkov riešenia projektu a naplnenia cieľov projektu v slovenskom jazyku (max. 20 riadkov)

V rámci riešenia projektu boli navrhnuté a vyrobené špecializované hardvérové platformy DISIPA-FPGA a DISIP-MCU, ktoré umožnili realizovať vývoj a overovanie navrhnutých konštrukčných a algoritmických protiopatrení umožňujúcich znížiť únik informácie pomocou postranných kanálov s využitím analýzy spotreby. Platforma DISIPA bola využitá na otestovanie rôznych meracích bodov, ktoré je možné využívať pri získavaní informácií z postranných kanálov získaných analýzou spotreby. Bolo experimentálne ukázané aký je vplyv hardvérových protiopatrení (filtračné prvky, tienenie, konštrukčné riešenie) na efektivitu získavania citlivých informácií v rôznych bodoch chráneného hardvérového kryptografického modulu pri implementácií nechráneného kryptografického algoritmu, čo je v praxi dôležité na zistenie kvalifikovaného odhadu akú úroveň kryptografických protiopatrení je potrebné na ochranu v reálnej aplikácii nasadiť. Pre algoritmus digitálneho podpisu na báze algoritmu ECDSA bola analyzovaná a prakticky overená možnosť útoku na operáciu modulárneho násobenia v záverečnej fáze algoritmu ECDSA pre scenár implementácie pomocou výpočtových prostriedkov s malou šírkou dátových ciest. Tieto dátové cesty sa typicky využívajú pri implementácii kryptografických algoritmov s verejným kľúčom (vrátane ECDSA algoritmu) v cenovo kritických aplikáciách, ktoré sú realizované pomocou škálovateľných algoritmov v obvodoch FPGA alebo MCU. Pre uvedené implementácie bolo formulované algoritmické protiopatrenie na zamedzenie útoku na škálovateľnú implementáciu modulárneho násobenia.

Súhrn výsledkov riešenia projektu a naplnenia cieľov projektu v anglickom jazyku (max. 20 riadkov)

We developed and produced specialized hardware paltforms DISIPA-FPGA and DISIPA-MCU during project solving. These DISIPA platforms enabled us to develop and test proposed hardware and algorithmic countermeasures for decreasing side-channel leakage based on power consumption analysis. We used our DISPA platform for evaluation of several possible measurement points that can be used for leakaged information from power consumption related side-channels. Our experimental results showed influence of hardware countermeasures (filtration elements, shielding, hardware design) to effectivness of sensitive information acquisition in different points of the protected hardware cryptographic module and unprotected implemented cryptographic algorithm. Such evealuation is an important factor for competent estimation about countermeasure level required for a practical application. We

analyzed and experimentally evaluated a possible attack to the last phase of the digital signature algorithm based on ECDSA implemented with narrow-width datapath. Such datapaths are typically used for implementations of public-key cryptographic algorithms (including ECDSA) in cost-sensitive applications. As target hardware FPGA and MCU devices are typically used. We formulated algorithmic countermeasures that disable proposed side-channel attack in scalable implementations of modular multiplication.

Svojím podpisom potvrdzujem, že údaje uvedené v záverečnej karte sú pravdivé a úplné a súhlasím s ich zverejnením.

Zodpovedný riešiteľ

Ing. Michal Varchola, PhD.

V Košiciach 29. 1. 2016

.....
podpis zodpovedného riešiteľa

Štatutárny zástupca príjemcu

prof. Ing. Stanislav Kmeť, CSc.
Rektor Technickej univerzity v Košiciach

V Košiciach 29. 1. 2016

.....
podpis štatutárneho zástupcu príjemcu