CUSTOM INTELLECTUAL PROPERTY BLOCK FOR LBLOCK CIPHER

Jakub Jedlička
Bachelor Programme (3), FEEC BUT
E-mail: xjedli24@stud.feec.vutbr.cz

Supervised by: David Smékal
E-mail: smekald@feec.vutbr.cz

Abstract: This paper presents the implementation of a lightweight cryptographic cipher for a hardware-constrained device. Describes the basic problems of lightweight cryptography on the field programmable gate array (FPGA) and its one representative cipher LBlock. Furthermore deals with the implementation of the LBlock cipher in a very high speed integrated circuit hardware description language (VHDL) on the FPGA. The LBlock cipher is used with a custom advanced extensible interface (AXI) wrapper for the creation of a custom intellectual property (IP) block. This IP block will be used to cipher files on the development board ZYBO Z7-20 powered by Zynq-7000. The final part of the paper describes testing of the IP block with a defined set of the inputs and the outputs are validated with the correct outputs.

Keywords: FPGA, LBlock, lightweight cipher, ZYBO Z7-20, Zynq-7000, IP block

1 ÚVOD

Kryptografie se využívá v různých formách již několik let, ale její expanze začala až s příchodem výpočetních zařízení. Kvůli potřebám šifrování na výkonově omezených zařízeních jako jsou mikrokontroléry, čipy využívající identifikace na rádiové frekvenci (RFID) a jim podobná zařízení, se vytvořila nová kategorie šifer nazývaná lehká kryptografie [1]. Standardní šifry by nemusely být pro tyto zařízení vhodné a to z důvodu jejich vyšších nároků na výkon. Proto pro kategorii lehkých šifer byly vytvořeny nové šifry jako je šifra PRESENT, vycházející ze šifry AES, dále čínská šifra LBlock, která vychází z šifry DES a mnoho dalších [2].

V posledních letech se zvýšila implementace kryptografie na programovatelných hradlových polích (FPGA) kvůli jejich čím dál většímu komerčnímu rozšíření. Hlavním důvodem, který k tomu vedl, je jejich výkon oproti procesorům a možnost přeprogramovaní na rozdíl od integrovaných obvodů určených pro aplikaci (ASIC) čipů. Lehká kryptografie se implementovala převážně na ASIC čipy, které byly výhodné, pokud se vytvářely ve velkém množství. Hlavní nevýhodou ASIC čipů je nemožnost přeprogramování po jejich výrobě. Z tohoto důvodu se čím dál více snaží prosadit implementace šifer lehké kryptografie na FPGA čipy, které jsou nízkoenergetické a v dnešní době cenově dostupné. Přeprogramování FPGA umožňuje opravit případné nově nalezené chyby v šifrách po implementaci. Poslední výhodou je možnost přidat kryptografický IP blok do návrhu nebo upravit aktuální návrh ke zmenšení celkové spotřeby plochy a tím i nákladů s tím spojených [3].

2 ŠIFRA LBLOCK

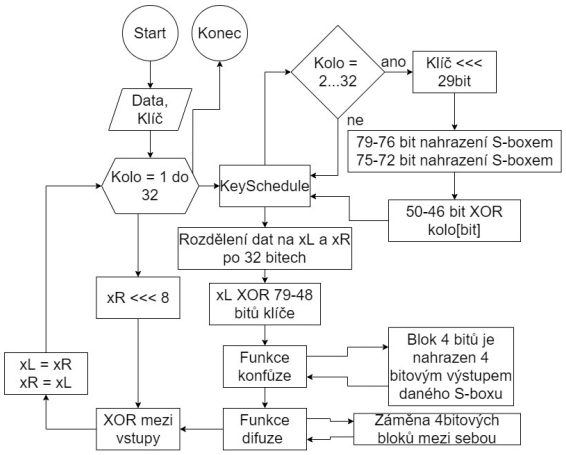
Šifra LBlock spadá do blokových šifer lehké kryptografie. Je založena na Feistelově síti, kde vstupem i výstupem je blok bitů o velikosti 64. Využívá klíč o délce 80 bitů, který je stanoveným minimem pro šifry lehké kryptografie. LBlock se skládá z 32 kol, kdy se pracuje s dvěma bloky od délce 32 bitů. Levá strana je vstupem do funkce kola a novou pravou stranou pro následující kolo. Na pravou stranu je využit bitový posun o 8 bitů a exkluzivní disjunkce s výstupem funkce kola. Funkce kola se

skládá ze tří částí. První částí je exkluzivní disjunkce vstupu a klíče, druhou funkce konfúze starající se o záměnu 4bitových bloků a třetí funkce difúze využívající 4bitové S-boxy. Dále je každé kolo upravován klíč pomocí bitových posunů, dvou S-boxů a operace exkluzivní disjunkce [4].

Šifra LBlock byla vybrána na základě srovnání šifer lehké kryptografie. Výběr probíhal z porovnávaní výkonu a hardwarových požadavků a byl proveden na šifrách LBlock, LED, mCRYPTON, PRESENT a SIMON. Jako nejoptimálnější se jeví šifry LBlock a PRESENT, které mají velmi podobné nároky. Z uvedených šifer byla vybrána šifra LBlock, jejíž popis implementace pomocí VHDL byl nalezen pouze v odborných článcích ale ne v podobě opensource.

3 IMPLEMENTACE ŠIFRY LBLOCK

Pro implementaci šifry byl vytvořen vývojový diagram, který je na obr. 1. Tento diagram popisuje průběh při procesu šifrovaní.



Obrázek 1: Vývojový diagram šifry LBlock

Důležité části z vývojového diagramu byly rozčleněny na moduly. Těchto modulů je celkově 17, z toho 10 modulů je pouze pomocných k funkcionalitě S-boxů a jsou rozděleny kvůli přehlednosti kódu. Zbylých 7 modulů tvoří hlavní logiku, kde nejvyšší modul nese název `LBlockTOP`. Celý návrh využívá 142 vyhledávacích tabulek (LUT) a 216 vstupních a výstupních (I/O) portů.

Modul `LBlockTOP` má v sobě jako jediný sekvenční logiku, která využívá hodin (clk). Řídí levou a pravou stranu Feistelovy sítě a také hodnoty klíče kola a počet kol opakovaní. Modul v každém kole volá dva submoduly, z nichž jeden má na starosti výpočet klíče a druhý průběh celého kola.

4 IMPLEMENTACE VLASTNÍHO IP BLOKU

Při vytváření IP bloku se vzala v potaz architektura cílové vývojové desky ZYBO Z7-20, která obsahuje 40 I/O portů dostupných pro uživatele. Jak vstupní i výstupní blok k šifrovaní, tak klíč mají velikost větší než je možný počet I/O portů. Z tohoto důvodu musel být použít tzv. „AXI stream wrapper“, využívající sekvenční logiku. AXI stream wrapper má za úkol načtení dat k šifrovaní ve dvou cyklech, po kterých následují tři cykly pro čtení klíče. Každý z těchto cyklů načítá blok 32 bitů dat. U načítání klíče se ve třetím cyklu vybírá pouze 16 bitů z 32 bitů, jelikož by to způsobilo přetečení signálu. Hodnota 32 bitů byla vybrána z důvodu potřeby využití řídících signálů pro fáze načítaní a výstupu dat, které jsou nad rámec 32 bitů. Druhým důvodem je, že hodnota 32 je mocnina čísla dva, stejně jako hodnoty 64 a 16. V důsledku této skutečnosti lze efektivně rozdělit vstupní a výstupní bloky, aniž by byla potřebná nadbytečná režie. Po načtení obou hodnot modul předává hodnoty modulu `LBlockTOP`, který provádí šifrovaní a vrací šifrovaná data. Tyto data poté načítá a posílá na výstup ve dvou cyklech.

V případě potřeby úpravy AXI stream wrapper, například z důvodu nedostatečného počtu I/O portů, který má druhá verze vývojové desky ZYBO Z7 stanoven na 32, by musela být snížena velikost vstupu a výstupu na 16 bitů a navýšen počet cyklů pro vstup a výstup dat. Velikost 16 bitů je zvolena z důvodu zmíněných v předchozím odstavci.

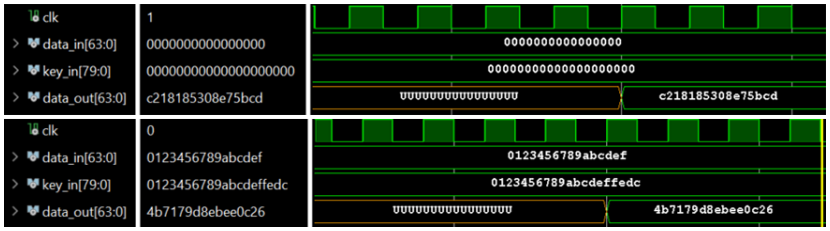
5 VALIDACE FUNKČNOSTI MODULŮ

Pro každý modul byly napsány testy, aby byla ověřena validita výstupů dle vstupních dat. Nejdůležitější částí při validaci bylo ověřit správnost modulu `LBlockTOP` a jeho AXI stream wrapper. Tato validace byla provedena pomocí simulace ve vývojovém prostředí Vivado Design Suite. Pro uvedené dva moduly byly použity vstupní data z návrhové publikace Wenling a Zhang (2011)[4], které jsou uvedeny v tabulce 1.

Tabulka 1: Výsledné vektory pro LBlock v hexadecimalním tvaru [4].

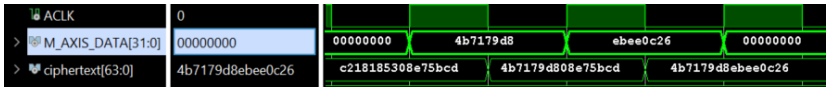
	Zpráva	Klíč	Šifrovaný text
1	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00	c2 18 18 53 08 e7 5b cd
2	01 23 45 67 89 ab cd ef	01 23 45 67 89 ab cd ef fe dc	4b 71 79 d8 eb ee 0c 26

Simulace probíhaly pomocí tzv. „testbench“, přes které jsou do modulů postupně načítány hodnoty z tabulky 1. Výsledky zprávy 1 a zprávy 2 pro modul `LBlockTOP` jsou zobrazeny na obrázku 2, kde vstupní hodnota zprávy je označena *data_in*, hodnota klíče *key_in* a výstupní hodnota *data_out*.



Obrázek 2: Testovaní vstupů pro `LBlockTOP`

Výsledky zprávy 1 a zprávy 2 pro modul `axi_stream_wrapper` jsou zobrazeny na obrázku 3. Je zde zobrazen výstup obou dvou šifrovaných zpráv a je také vidět přechodná fáze načítaní z *M_AXIS_DATA* do vytvořeného pomocného logického vektoru *ciphertext*. V pomocném vektoru se nachází jako první hodnota šifrovaného textu pro zprávu 1 a po dvou cyklech hodin hodnota pro zprávu 2.



Obrázek 3: Testovaní výstupu pro `axi_stream_wrapper`

6 POROVNÁNÍ IMPLEMENTACE ŠIFRY LBLOCK S OSTATNÍMI ZÁSTUPCI

Tabulka 2 porovnává požadovaný počet LUT tabulek vybraných šifer, kde hodnoty LUT jsou převzaty z článku DIEHL (2017) [5]. Výstupem této implementace je v tabulce uvedená hodnota LUT pro šifru LBlock.

Tabulka 2: Požadované LUT tabulky pro šifry lehké kryptografie [5].

Název šifry	LBlock	PRESENT-80	LED-80	SIMON 96/96	AES-128
Počet LUT	142	311	358	435	318

7 NÁROKY IP BLOKU A JEHO VYUŽITELNOST

V tabulce 3 lze vidět jednotlivá rozložení prostředků pro modul `axi_stream_wrapper` podle funkcionálních kategorií po syntéze ve Vivado design Suite.

Tabulka 3: Využití prostředků pro AXI stream wrapper.

Název	LUT6	LUT5	LUT4	FDRE	I/O	LUT celkově	Flips-flops celkově
Počet	5	4	6	9	36	15	9

Z tabulky je patrné, že se jedná o návrh s nízkými požadavky na vyhledávací tabulky. IP blok je navržen pro vývojovou desku ZYBO Z7-20, která má 53 200 dostupných vyhledávacích tabulek. To znamená využití přibližně 1% celkové kapacity. V případě vstupů a výstupů lze tento návrh považovat za náročný.

Momentální cílová frekvence pro hodiny ACLK je 125MHz, kdy probíhá testovaní z možností navýšení frekvence. Celková spotřeba návrhu na čipu by se dle kompilátoru měla pohybovat na úrovni 0,106W. Aktuální návrh by měl být použitelný na většině FPGA, které splňují podmínky dostatečného počtu I/O portů.

8 ZÁVĚR

V článku byla přiblížena problematika lehké kryptografie na FPGA a implementace modulu šifry LBlock a jejího IP bloku, který je určen pro šifrovaní na vývojové desce ZYBO Z7-20. Funkčnost IP bloku popsaného v článku je již implementována a otestována. Dle testů se implementace IP bloku prokázala jako funkční. IP blok není finální a dále bude upravována maximální frekvence k nalezení optima s dostupnými prostředky.

REFERENCE

[1] POSCHMANN, Axel. *LIGHTWEIGHT CRYPTOGRAPHY: Cryptographic Engineering for a Pervasive World* [online]. Bochum, 2009, [cit. 5. 3. 2021]. Dostupné z URL: <https://www.ei.ruhr-uni-bochum.de/media/crypto/veroeffentlichungen/2011/09/16/thesisp.pdf> Disertační práce. Ruhr-University Bochum, Germany, Faculty of Electrical Engineering and Information Technology.

[2] NEKUŽA, Karel, *Odlehčená kryptografie pro embedded zařízení* [online]. Brno, 2016, [cit. 5. 3. 2021]. Dostupné z URL: <https://www.vutbr.cz/studenti/zav-prace?zp_id=93665.> Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Ing. Zdeněk Martinásek, Ph.D.

[3] YALLA, Panasayya a KAPS, Jens-Peter, *Lightweight Cryptography for FPGAs* [online]. 2009 International Conference on Reconfigurable Computing and FPGAs, Cancun, Mexico, 2009, s. 225-230 [cit. 5. 3. 2021]. Dostupné z: doi: <https://doi.org/10.1109/ReConFig.2009.54>

[4] WENLING, Wu a ZHANG, Lei, *LBlock: A Lightweight Block Cipher. Applied Cryptography and Network Security* [online]. Germany: Springer, Berlin, Heidelberg, 2011, s. 327-344 [cit. 5. 3. 2021]. ISBN 978-3-642-21554-4. Dostupné z: doi: <https://doi.org/10.1007/978-3-642-21554-4_19>

[5] DIEHL, William, FARAHMAND, Farnoud, YALLA, Panasayya, KAPS, Jens-Peter, GAJ, Kris *Comparison of hardware and software implementations of selected lightweight block ciphers* [online]. 2017 27th International Conference on Field Programmable Logic and Applications (FPL), Ghent, Belgium, 2017, [cit. 23. 3. 2021]. Dostupné z: doi: <https://doi.org/10.23919/FPL.2017.8056808>