Instruction Prediction in Microprocessor Unit Based on Power Supply Line

Michał Maćkowski and Krzysztof Skoroniak

Silesian University of Technology, Institute of Computer Science,
Akademicka 16, 44-100 Gliwice, Poland
{michal.mackowski,krzysztof.skoroniak}@polsl.pl
http://www.polsl.pl/

Abstract. This paper illustrates the research results concerning the character of signals emitted by the selected microcontroller via the power supply lines. The main purpose of the study is to determinate the instruction that is currently realized by the microprocessor, based on the conducted emission in the power supply lines.

The research results presented in the study indicate that there are the differences in the spectrum of the signal emitted by the processor, depending on the program being executed. Thus, it can be presumed that there is a partly possibility to determinate the instruction currently realized by a microprocessor based on the conducted disturbances emitted by the power supply lines. It can be suggested that there is a risk for programs written in microprocessor memory, which should be protected from copying.

Keywords: conducted emission, electromagnetic compatibility (EMC), electromagnetic disturbances, microcontroller, program code.

1 Introduction

The source of electromagnetic field diffusing in the space is each device supplied with electric energy. This kind of field can disturbs the work of various electric and electronic devices. However, the disturbances are not the only problem that accompanies electromagnetic emission. It is possible, in some cases, to get the information about signals appearing inside the device if the emission from the device is recorded, and the received signals are decoded and interpreted by the appropriate methods. Such situation is especially value in the case of digital devices because the remote reconstruction of signals inside the device may enable to regenerate information processing by this device.

The high integration scale and permanent increase of the frequency of microprocessor circuit, entail that current peaks are generated with higher amplitudes and shorter rise times on the power supply lines of the electronic circuits. These impulses are generated by simultaneous switching of millions of transistors inside of the integrated unit. The total power drawing by all gates that execute a single instruction may indicate the kind of instruction which is already executed. Moreover, the propagation of these currents through lines and paths on

A. Kwiecień, P. Gaj, and P. Stera (Eds.): CN 2010, CCIS 79, pp. 173–182, 2010.

PCB board into other electronic devices may cause problems with their proper functioning.

The network controller placed in the network card can be also considered as a microprocessor unit, which is responsible for data processing of transmitted frames. Such unit can be also the source of electromagnetic disturbances that can interfere the work of other electronic devices.

The previous article [1] aimed mainly at determining the spectrum of signal emitted by the processor during realization of a particular single instruction. Nevertheless, this instruction was realized in the loop. This paper presents the methodology and the research, that allow determining and comparing the spectrum of a specific single instruction. This issue is opposite to the one discussed in the publications [2] and [3], where authors intended to predict the emission of electromagnetic disturbances emitted by the microprocessor under different program behavior.

The main purpose of the research is to determine the instruction currently realized by the microprocessor based on the emission of conducted disturbances on the power supply lines. The test bench constructed for the research is discussed in the Sect. 2. Determining the instruction currently executed, which is based on the disturbances on the power supply lines may lead to unauthorized reconstruction of a program without any directly interference into the microprocessor memory. Protection of information is a very essential issue; otherwise the cost of so far, very expensive systems of confidential information increases. Moreover, an inappropriate attitude to this issue may expose the protected information to be used in an unauthorized way.

2 Test Bench

The research used a microprocessor PIC16F84A produced by Microchip. The test bench illustrated in the Fig. 1 consists of microprocessor to which the power supply and 2 MHz external square waveform generator were connected. In order to exclude conducted disturbances that can get into microprocessor when using an external AC/DC power supply, a complete of batteries was used instead.

The oscilloscope was connected to the power supply lines to monitor the decreases of voltage. With the using batteries as an unstable source of power supply, the voltage decreases were equivalent to the current in the power supply lines. Such solution was dictated by the difficulties in finding a proper current probe that could have measured 1 milli- or even 1 microampere current with the approximate 1 GHz sampling frequency. The microchip programmer used in the research, was connected to the microprocessor only for the period of programming, in order to avoid conducted disturbances that can get from the programmer to the supplying lines.

The microprocessor PIC16F84A used in the research has one executive pipeline, which means that during one instruction cycle only one command is realized. One instruction cycle (2 μs) consists of four machine cycles (500 ns):

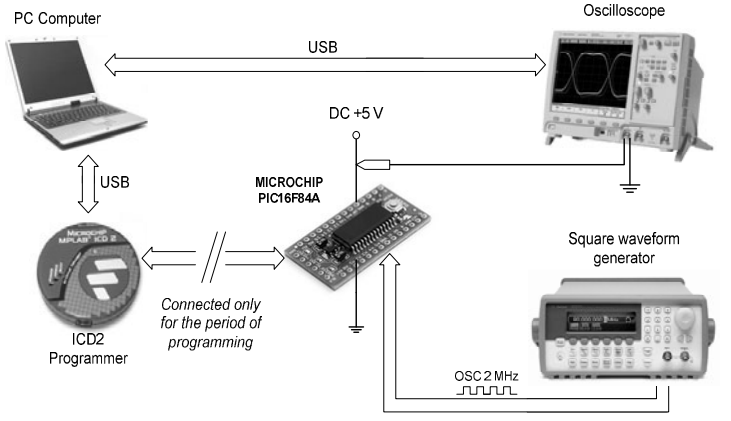

Fig. 1. The schema of research position

- Q1 – instruction decode cycle,
- Q2 – instruction read data cycle,
- Q3 – process the data,
- Q4 – instruction write data cycle and fetching the next instruction from the program memory.

Due to the fact that in the last cycle (Q4) another instruction is fetched from the program memory, thus not only currently realized instruction but also next instruction has the influence on the current flow (shape). Microcontroller PIC16F84A contains totally 35 instructions, among others:

- 1-cycle instructions ($2\,\mu$s): ADDWF, ANDWF, CLRF, CLRW, COMF, DECF, INCF, IORWF, MOVF, MOVWF, NOP, RLF, RRF, SUBWF, SWAPF, XORWF, BCF, BSF, ADDLW, ANDLW, CLRWDT, IORLW, MOVLW, SLEEP, SUBLW, XORLW,
- 2-cycle instructions ($4\,\mu$s): DECFSZ, INCFSZ, BTFSC, BTFSS, CALL, GOTO, RETFIE, RETLW, RETURN.

In the research presented in this work only 1-cycle instructions (24 instructions) were taking into account in order to simplify the analysis. However, the authors intend to test also 2-cycle instruction in the further research.

3 The Research Procedure

First, the two researches were conducted for all 24 one-cycle instructions, and next similarities among particular instructions were determined. The research procedure is as follows:

1. Determination of the time flow of the microprocessor power supply voltage during whole program (Fig. 2 and 3a).

2. Excision of part of the time flow which refers to the currently tested instruction (Fig. 3b).
3. Passing from time domain to frequency domain for the removed part of time flow using FFT calculation algorithm of Fourier Transform (Fig. 3c).
4. Comparison of amplitude spectra determined for particular instructions based on the least squares method.

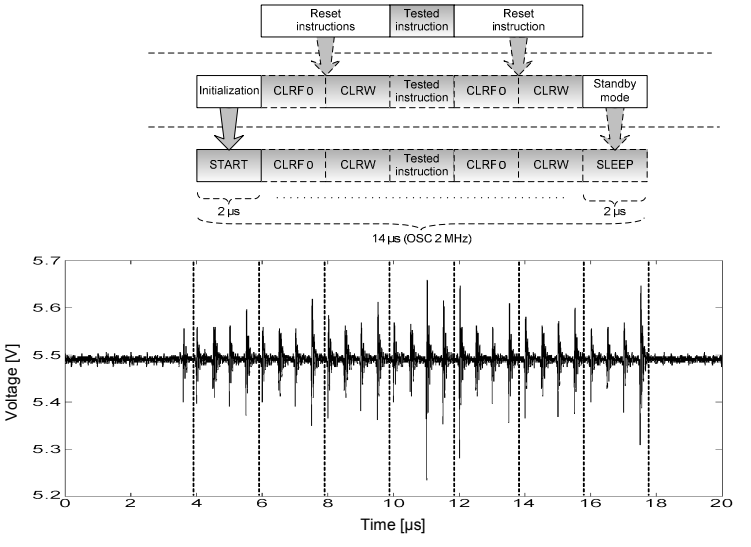

Fig. 2. The research procedure – microcontroller program construction

It was necessary, during the test of each instruction to record a proper program for the microprocessor (Fig. 2). Thus, each program consists totally of 7 instructions:

- the instruction that initiates the microprocessor, realized implicitly,
- the instructions that reset the value of accumulator and the first working register,
- the tested instruction,
- the instructions that reset the value of accumulator and the first working register,
- the SLEEP instruction that aim was to switch the microprocessor into standby mode.

In order to ensure the same conditions for realization of each instruction, the working registers that were used by a particular instruction, were reset each time. During the test the parameters of a particular instruction were set to 0.

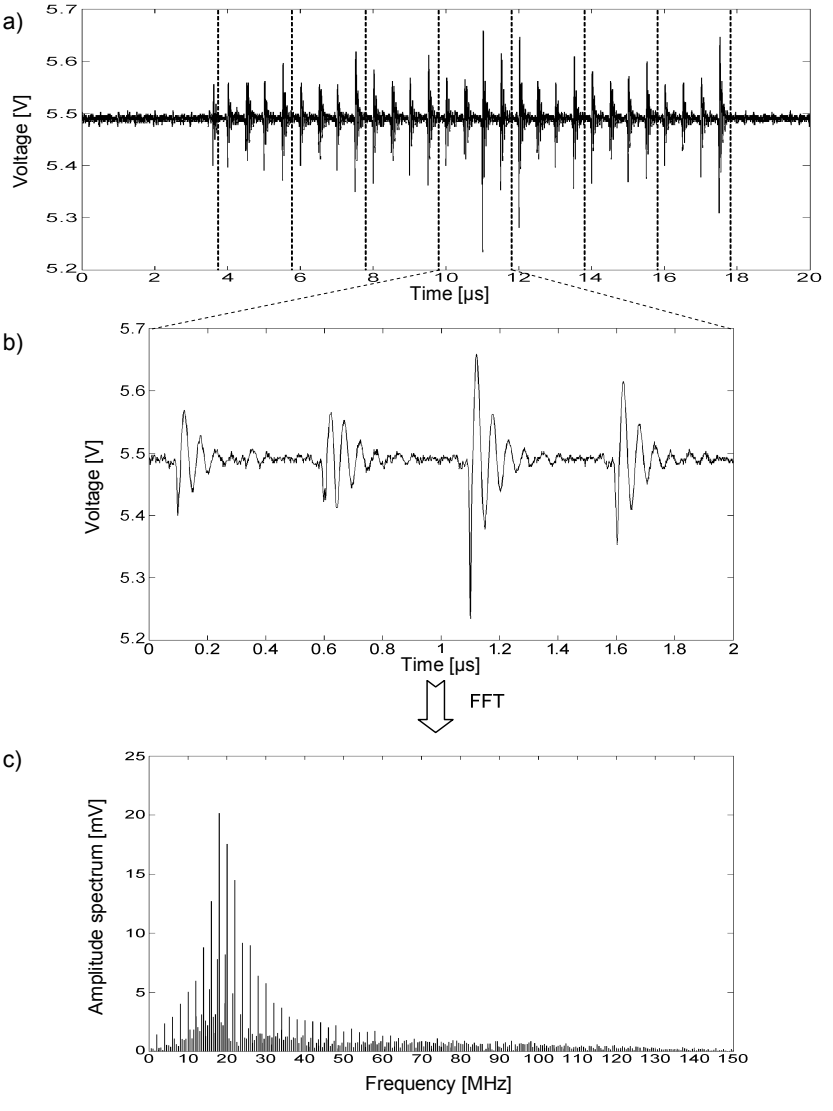

Fig. 3. The research procedure: (a) Voltage on power supply line – test 1, program 6, (b) Voltage on power supply line – test 1, program 6, DECF instruction (c) Amplitude spectrum – test 1, program 6, DECF instruction

4 The Research Results

As the test results illustrate 19 of 24 instructions were correctly recognized thanks to analysis of microprocessor supply voltage flow (Table 1).

Table 1. The results of amplitude spectra comparison determined for particular instructions using the least squares method

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
ADDWF	1	0.858	2.043	0.726	7.531	27.253	29.260	2.102	0.885	0.827	0.749	1.516	0.740	0.840	5.536	0.744	0.868	3.346	1.746	3.059	4.627	1.829	1.517	10.428	2.004
ANDWF	2	1.257	0.784	2.049	3.138	20.196	21.375	1.811	1.526	2.030	1.834	0.832	2.199	2.106	1.797	1.627	1.737	0.930	1.523	1.545	1.719	1.252	1.308	4.843	1.416
CLRF	3	1.230	2.639	0.556	7.982	29.847	31.935	2.716	1.145	0.843	0.681	2.170	0.950	1.028	6.513	0.966	1.048	3.756	1.818	3.988	5.802	2.770	2.013	12.204	2.705
CLRW	4	4.813	3.040	6.598	0.685	12.870	13.666	3.393	5.324	6.439	6.073	3.737	6.838	6.541	1.931	5.632	5.856	2.191	3.566	4.160	3.373	4.673	5.204	3.952	4.733
COMF	5	23.864	21.301	28.627	13.043	0.759	0.852	18.961	25.624	27.151	28.003	21.329	27.706	27.376	15.675	25.771	25.683	18.385	20.272	19.486	17.791	21.236	22.890	13.174	21.961
DECF	6	25.298	22.470	30.418	13.238	0.810	0.743	20.022	26.890	28.725	29.441	22.410	29.406	29.074	16.266	27.230	27.208	19.392	21.452	20.518	18.848	22.880	24.458	13.682	23.198
INCF	7	1.254	1.983	1.911	4.231	18.432	20.101	0.736	1.611	1.666	1.914	1.488	1.742	1.669	4.086	1.398	1.485	2.704	0.814	3.081	4.142	2.245	2.115	8.409	2.456
IORWF	8	0.632	1.631	0.919	5.900	24.516	26.426	1.649	0.577	0.680	0.797	0.985	0.922	0.895	4.445	0.615	0.592	2.621	1.334	2.543	3.852	1.536	0.946	9.194	1.661
MOVF	9	0.754	2.188	0.707	7.411	27.156	29.204	2.008	0.821	0.554	0.727	1.583	0.756	0.684	5.865	0.647	0.719	3.641	1.689	3.439	5.104	2.071	1.506	11.142	2.186
MOVWF	10	0.952	2.036	0.671	6.950	28.031	30.001	2.301	0.772	0.746	0.537	1.603	0.923	0.934	5.437	0.868	0.806	3.051	1.666	3.312	4.821	2.215	1.570	10.618	2.211
NOP	11	1.223	1.163	2.381	4.174	19.882	21.323	1.832	1.625	2.019	2.040	0.596	2.210	2.009	2.487	1.500	1.686	1.561	1.785	1.312	1.843	0.891	0.801	5.488	0.982
RLF	12	0.796	2.053	0.601	7.173	26.624	28.603	1.848	0.741	0.609	0.744	1.448	0.575	0.607	5.668	0.605	0.673	3.350	1.533	3.273	4.789	1.965	1.375	10.691	2.083
RRF	13	0.773	1.714	0.813	6.265	25.400	27.327	1.635	0.719	0.710	0.812	1.174	0.836	0.836	4.884	0.686	0.691	2.849	1.343	2.804	4.176	1.742	1.223	9.658	1.746
SUBWF	14	3.662	1.886	5.407	2.139	14.981	15.709	3.690	4.244	5.290	4.848	2.369	5.591	5.313	0.839	4.550	4.583	1.093	3.354	2.057	1.033	2.553	3.067	1.949	2.701
SWAPF	15	0.658	1.619	0.804	6.294	25.244	27.187	1.592	0.708	0.617	0.760	1.099	0.673	0.641	4.711	0.571	0.693	2.776	1.313	2.679	4.081	1.596	1.090	9.554	1.629
XORWF	16	0.673	1.571	1.031	5.753	24.260	26.221	1.511	0.983	0.757	0.869	0.973	0.854	0.857	4.303	0.647	0.690	2.497	1.226	2.369	3.783	1.650	1.050	9.003	1.413
BCF	17	2.867	1.395	4.092	2.200	18.008	18.837	3.191	3.188	4.160	3.534	1.830	4.549	4.216	1.022	3.516	3.634	0.624	2.660	1.796	1.189	2.043	2.447	3.016	2.151
BSF	18	1.011	1.662	1.235	4.701	20.552	22.179	1.139	1.279	1.384	1.264	1.214	1.355	1.405	3.907	1.124	1.230	2.169	0.686	2.664	3.646	1.712	1.599	8.029	1.912
ADDLW	19	2.020	1.616	3.452	4.399	18.701	19.946	2.876	2.696	3.177	3.184	1.337	3.523	3.088	2.156	2.569	2.658	1.530	2.629	0.680	1.029	0.841	1.166	3.722	0.868
ANDLW	20	3.446	1.985	5.287	3.187	17.121	17.956	3.952	4.113	5.056	4.701	2.150	5.561	5.137	1.080	4.301	4.338	1.128	3.722	1.123	0.532	1.766	2.334	1.824	1.812
IORLW	21	1.555	1.674	2.996	4.857	20.527	22.027	2.575	1.976	2.425	2.492	0.877	2.843	2.598	2.521	1.877	2.051	1.757	2.295	0.841	1.494	0.852	0.713	5.029	0.696
MOVLW	22	1.029	1.563	1.918	5.903	23.214	24.861	2.301	1.297	1.515	1.677	0.772	1.776	1.573	3.550	1.120	1.256	2.041	1.919	1.179	2.236	0.691	0.470	6.764	0.695
SUBLW	23	7.847	5.181	10.709	3.781	13.244	13.559	7.753	8.695	10.291	9.845	5.711	10.961	10.399	2.018	9.113	9.231	3.295	7.481	3.497	1.865	5.107	6.096	0.704	5.123
XORLW	24	1.524	1.357	2.730	4.749	20.049	21.483	2.571	1.942	2.454	2.432	0.917	2.820	2.418	2.369	1.926	1.991	1.548	2.158	0.790	1.317	0.668	0.835	4.550	0.727

The Figures 4, 5 and 6 present an exemplary microprocessor supply voltage flow for entire program. Figure 4 comes from program 6 executed during the first test, whereas Fig. 5 comes from program 6 which was executed in the test 2. As it can be seen there is a similarity between the two charts. However, Fig. 6 shows that the flow of voltage for program 7 differs a lot from the two others. That can indicate the differences in the microprocessor supply voltage which depend on a particular executed program or a single instruction. The Figures 7, 8 and 9 present the same programs, but only the parts of voltage that refer to the tested instruction were specified. Whereas Figs. 10, 11 and 12 present amplitude spectra for Figs. 7, 8 and 9 that were determined by the FFT algorithm. The spectra determined for the whole instructions were afterwards compared using the method of the least squares. The results are presented in Table 1.

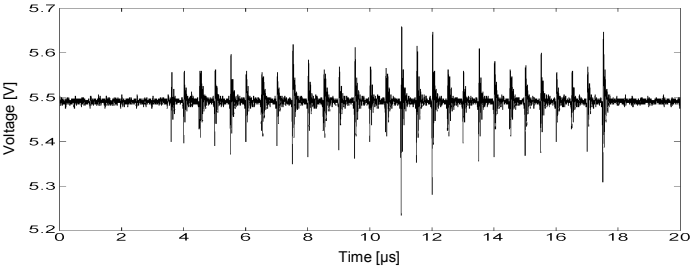

Fig. 4. Voltage on power supply lines – test 1, program 6

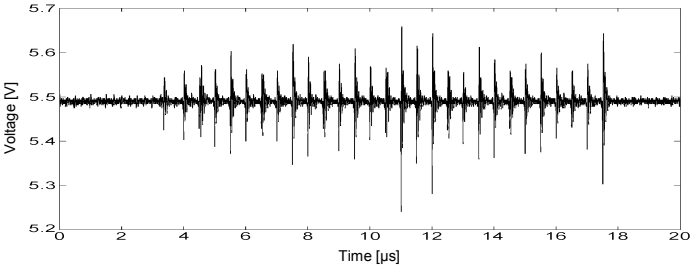

Fig. 5. Voltage on power supply lines – test 2, program 6

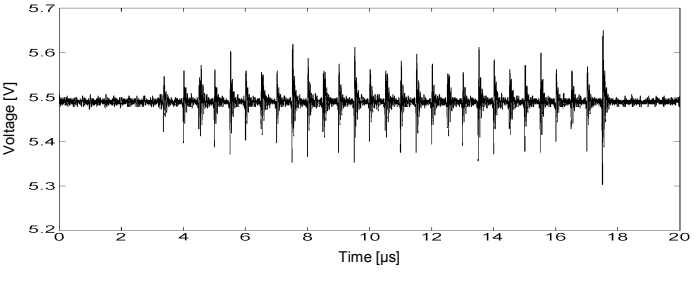

Fig. 6. Voltage on power supply lines – test 2, program 7

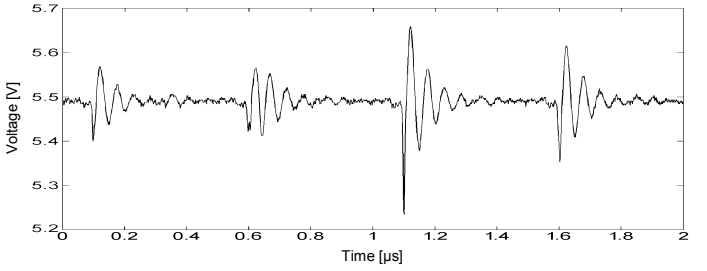

Fig. 7. Voltage on power supply lines – test 1, program 6, DECF instruction

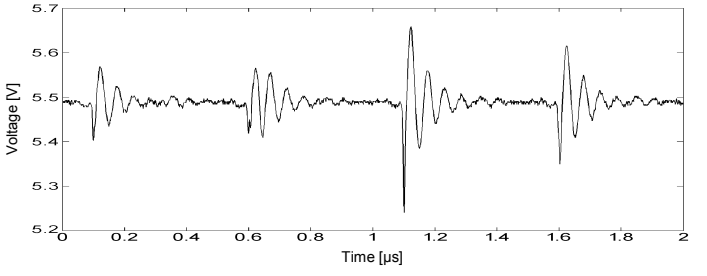

Fig. 8. Voltage on power supply lines – test 2, program 6, DECF instruction

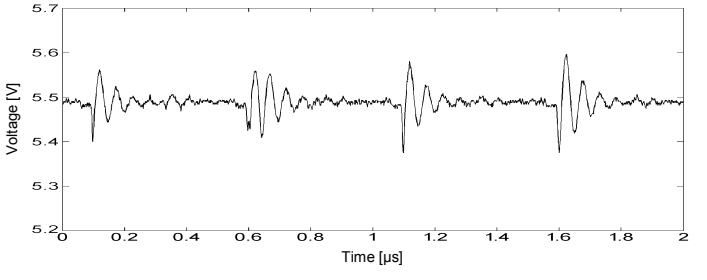

Fig. 9. Voltage on power supply lines – test 2, program 7, INCF instruction

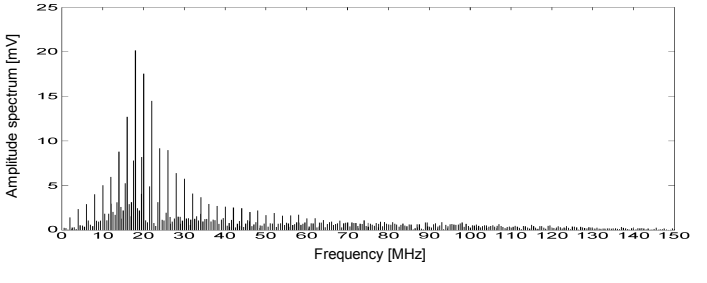

Fig. 10. Amplitude spectrum – test 1, program 6, DECF instruction

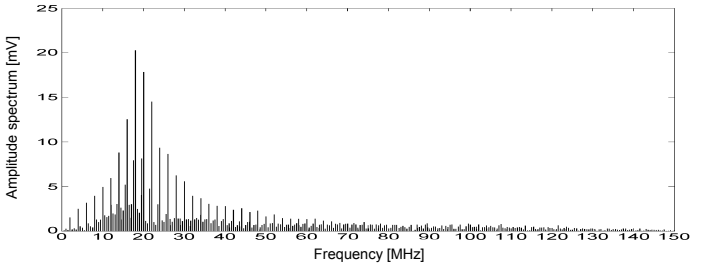

Fig. 11. Amplitude spectrum – test 2, program 6, DECF instruction

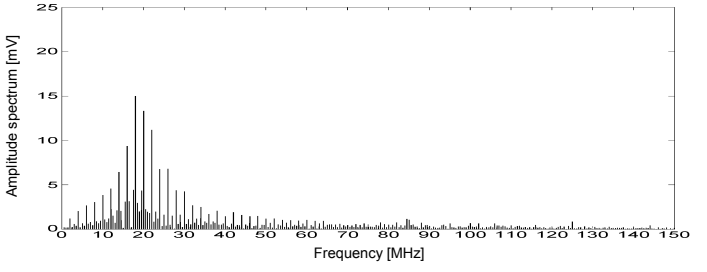

Fig. 12. Amplitude spectrum – test 2, program 7, INCF instruction

The fields in the Table 1 present the result of the least squares method between two particular instructions. Because of the fact that the method of the least squares was used, thus the smallest value is in a particular field the more similarity is between two instructions. Instructions mentioned in the following verses represent the first research, whereas instructions in the columns refer to the research 2. The expected minimal values should appear along a diagonal line thanks to the special construction of the chart. The gray fields stand for the smallest values where the analysis was correct. Meanwhile the incorrect results of analysis were marked with black background and white text. Fields marked with black border in particular columns refer to instructions, which were recognized as those of more possibility than tested instructions.

5 Conclusion

The research results presented in the paper indicate that there are unambiguous differences in the spectrum of conducted signal emitted by the microprocessor, depending on an executing instruction. Therefore, it can be concluded that there is a partly possibility to determine the currently executing instruction by the microprocessor based on the conducted disturbances emitted through the power supply lines. However, that situation may be dangerous for programs saved in memory of microprocessors, which should be protected from being copied.

In the further research the authors intend firstly to take into account 2-cycle instructions. Next, to increase the precise of receiving results, create a possibility

to determine instructions executing in the sequence, and yet consider the instructions parameters in tests.

If the further research allows increasing the precise of foreseeing currently executing instruction, then there is a serious risk for programs saved in the memory of microprocessors. In the conducted research it was possible to foreseen the currently executing instruction with the 79% of probability (19 of 24 instructions recognized correctly). Determination of the currently executing instruction based on the disturbances in the power supply lines, may allow for unauthorized reconstruction of program without directly intervention in the microprocessor memory.

References

1. Maćkowski, M., Skoroniak, K.: Electromagnetic emission measurement of microprocessor units. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) 16th Conference on Computer Networks, CN 2009, Wisła, Poland. CCIS, vol. 39. Springer, Heidelberg (2009)
2. Bendhia, S., Labussiere-Dorgan, C., Sicard, E., Tao, J.: Modeling the electromagnetic emission of a microcontroller using a single model. IEEE transactions on Electromagnetic compatibility (2008)
3. Chen, C.K., Liao, S.S., Sicard, E., Yang, C.F., Yuan, S.Y.: EMI prediction under different program behavior. In: IEEE EMC Symposium, Honolulu, USA (2007)