MEASUREMENT OF SYMMETRIC CIPHER ON LOW POWER DEVICES FOR POWER GRIDS

Radek Fujdiak
Doctoral Degree Programme (2), FEEC BUT
E-mail: xfujdi00@stud.feec.vutbr.cz

Supervised by: Jiri Misurec
E-mail: misurec@feec.vutbr.cz

Abstract: The symmetric ciphers are often used in low power devices for its low requirements. This article provides a measurement of AES-128 cipher, which should be used for secure communication in power grid (smart grid) networks. We are using as low power devices the microcontroller MSP430 from Texas Instruments. These measurements, deal in this article, should help with implementation of the whole concept of encryption. Concretely, it shows the space left for the other algorithms (as for example elliptic curves algorithm for key distribution, communication protocols etc.)

Keywords: symmetric, low power, MSP430, power grid, measurement, communication

1 INTRODUCTION

The modern symmetric ciphers are known from 1970s. We have two types of symmetric ciphers - block cipher and stream cipher. The stream cipher is quit simple and basically it is XOR operation of key and plain text, which it creates the single bits of cryptogram. These ciphers are less popular than block ciphers [1]. We are concentrated to the Advanced Encryption Standard (AES) approved by NIST in December 2001 [2]. This is a block cipher, which is often used for communication encryption. The main advantage of symmetric cipher is their key-size requirements (and speed). The comparison with other algorithms is in table 1, all key-sizes are in secure bits (sb).

Symmetric key-size [sb]	ECC key-size in [sb]	Asymmetric key-size [sb]
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Table 1: Comparison of key-size requirements for different types of ciphers.

The requirements in general are critical parameters for choosing the right encryption algorithm for low power devices. We are focused on power grid networks (smart grid) networks, where the low power devices are often used as communication unit. This article deal with measurement of AES-cipher for low power device MSP430f5438. MSP430f5438 is microcontroller from Texas Instruments company (TI). TI come up with a new optimized library of AES-128 cipher [12] and [13]. This article deal with measurement of this library on MSP430f5438.

2 EXPERIMENTAL BACKGROUND

The figure 1 shows our contemplated network. This network might for example provide remote electricity take-off control (as well as water, gas and heat take-offs) [3]. The terminal equipment (e-meters, indicators and monitors) are connected via existing power lines, RS485 or USB to the Intelligent Communication Unit. Data from the Intelligent Communication Unit are transferred via wireless technology (e.g. General Packet Radio Service (GPRS)) or existing power lines (PLC [4]) into the Data concentrator, which aggregates data from a number of Intelligent Communication Units. From the Data concentrator, the data are transmitted via an appropriate communication channel into the central system, which is nowadays the Supervisory Control and Data Acquisition system (SCADA) and will be the Smart Grid network in the nearest future.

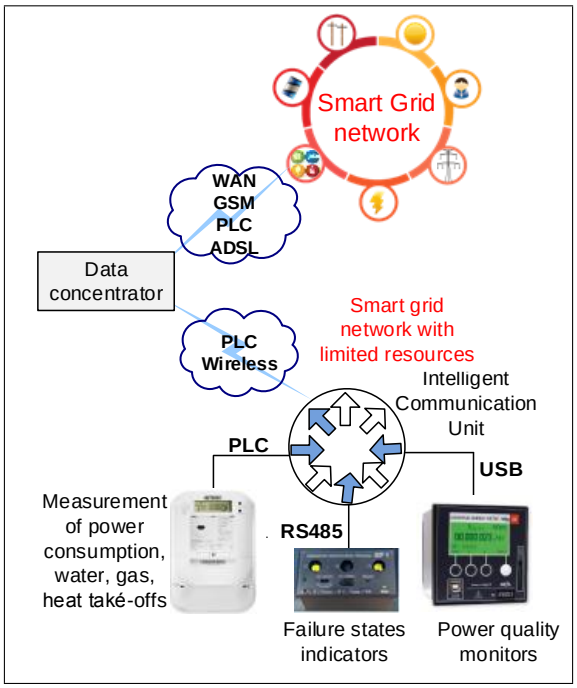

Figure 1: Smart Grid network for remote data acquisition [3]

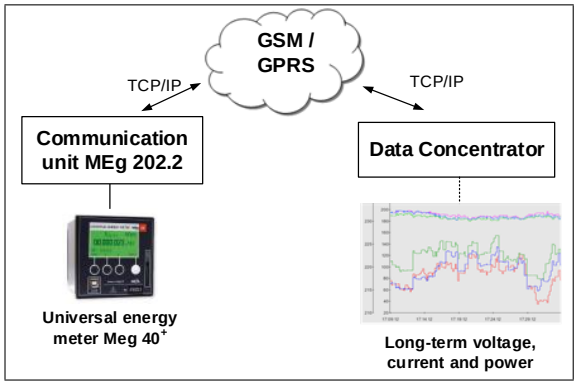

Figure 2: Block diagram of the experimental network for secure remote measurement [3]

The designed secure communication for a network with limited resources has been tested in an experimental network in ČEZ Distribuce, a.s. The communication chain is shown in Fig. 2. The MEg40+ Universal energy meter is installed in the Noviny transformer station, Velky Grunov area, the Czech Republic. The Data Concentrator is located in Brno, the Czech Republic. The communication distance is approximately 240 km [3].

Our developed communication algorithm is in Fig. 3. The EC is a group of elliptic curves, ECC is a block with elliptic curve cryptography logic (algorithms), ECDH is algorithm of Diffie-Hellman over Elliptic Curves and AES-128 is algorithm AES with 128 bits key.

The Elliptic Curves and Elliptic Curve cryptography are deal in [8], for this was also done the random number generator [4], [6], [7] and [9] and in general the communication is discussed in [3] and [5]. The communication algorithm (of two sides A and B) is as following:

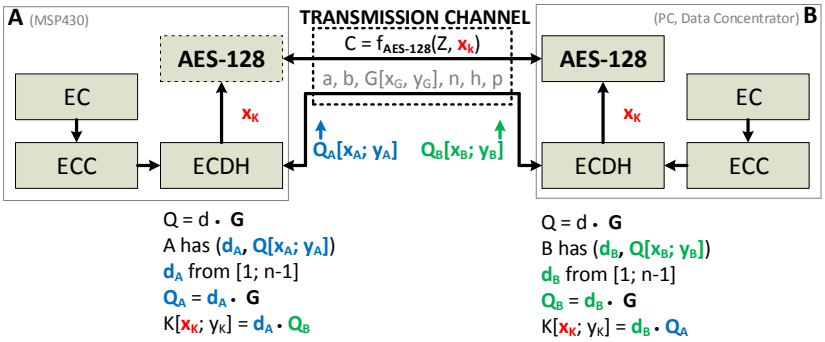

Figure 3: Communication algorithm for securing the communication in contemplated network

1. It is chosen elliptic curve, after is computed this curve (the points).
2. The algorithm ECDH compute the key K. The parameters are published (multiplies from curve equitation a, b, the point on the curve G (generator of points with co-ordinations x, y), grade of elliptic curve n, cofactor h and number p defining the GF_p). Both sides compute the points Q and exchange them and after is computed the key K.
3. It is used the x co-ordination from the key K as key for AES-128 cipher. It is possible to securely communicate over transmission channel with using the AES cipher (Z is the plain text, C is the cryptogram, f is the AES function or algorithm).

As was mentioned, we use the ultra-low microcontroller MSP430f5438A from Texas Instruments. The microcontroler has a many strong sides for example digitally controlled oscillator stability and internal physical crystal (no needs of external crystal), stack processing capability, many operating modes (AM, LPM0 - LPM4), 16-bit operations, up to 32 MHz crystals, 32-bit hardware multiplier, 256 KB FLASH, 16 KB RAM and many others [10]. The microcontroler presets for the experiment were: The Digital Clock Oscillator (DCO) was used as source for CPU. We were using default DCO frequency 1MHz. That means 100ns for one single cycle ($T_{cycle} = 1/f_{CPU}$). V_{cc} was 3000mV and operating mode was Active Mode (AM). The I_{cc} is 300μA for our V_{cc} and f_{CPU}.

3 EXPERIMENTAL RESULTS

We measure from the point of speed (in cycles) the AES-128 cipher (provided in [12], [13]), which should be used for our communication model Fig. 1. The final results are in Tab. 2.

	Encryption	Decryption	Whole
Optimized	8000	11250	19300
not Optimized	11100	16500	27600

Table 2: Requirements of whole AES encryption and decryption process.

In the table 2 is two values, optimized and not optimized. The optimized value means that we used software optimization ([11]). The software optimization transfer mathematical computation to the better shape for the microcontroler. Each measured part of AES algorithm is in Tab. 3.

The Mix Columns is the most demanding part of the algorithm, how is evident from our results. The Fig. 4 shows the algorithm parts (byte shifting, row shift, column mixing, round key add and their

Operation Type	Encryption		Decryption	
	Not Optimized	Optimized	Not Optimized	Optimized
Byte Substitution	277	233	258	166
Shift Rows	63	56	48	46
Mix Columns	602	397	981	638
Add Round Key	214	150	201	168
Whole Iteration (1-9)	1156	826	1515	1018
Last iteration	755	731	2834	2124
Others	20	20	13	13

Table 3: The AES operations requirements in cycles.

inversions for decryption) complexity.

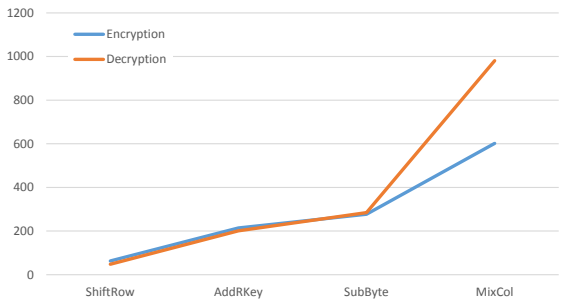

Figure 4: The algorithm parts complexity for encryption and decryption.

It is also visible the big impact of optimization, the impact is in tenth percents. The final impact of the optimization for encryption can be seen in Fig. 5 and the final impact of the optimization for decryption can be seen in Fig 6.

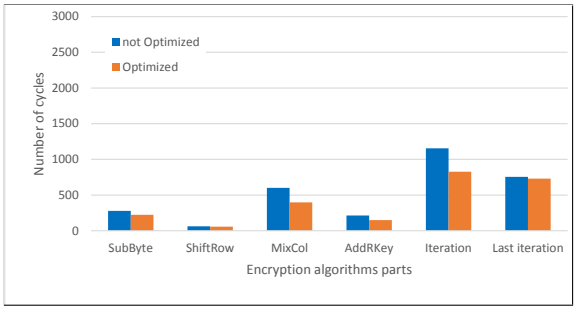

Figure 5: The impact of the software optimization to the encrypt algorithm speed.

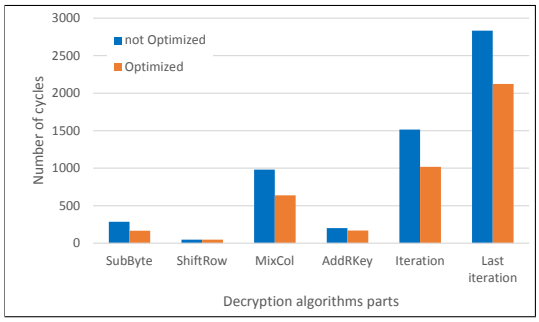

Figure 6: The impact of the software optimization to the decrypt algorithm speed.

We also measure the memory requirements of this algorithm, the RAM requirements was 0.16 B from 16 kB and the FLASH requirements was 1.73 B from 42 kB.

4 CONCLUSION

This article provide complex measurement of AES library from Texas Instruments. We provide the speed and also memory point of view. The memory requirements are minimal (FLASH 4% and RAM

1%). The speed requirements are for whole encryption process 11000 cycles and for decryption 16500 cycles. We also shows the impact of software optimization, which is in tenth percents (for encryption in example it means decreasing the cycles from 11000 to the 8000, where the impact is 30% and similar impact the optimization has to the decryption, where from 16500 cycles is the process decreased to the 11250, which is again around 30%). The measurement shows that the most demanding part of the processes is the mix columns (there could be the space for future optimization of this library).

REFERENCES

[1] Paar, C.; Pelzl J.: Understanding Cryptography, (Chapter 2), Springer-Verlag, Berlin Heidelberg 2010, ISBN 978-3-642-04101-3.

[2] NIST: Announcing the Advanced Encryption Standard (AES), Publication 197 (FIPS PUB 197), November 26, 2001.

[3] Mlynek, P.; Misurec, J.; Koutny, M. ; Raso, O.: Design of Secure Communication in Network with Limited Resources, In Proceedings of the 4th European Innovative Smart Grid Technologies (ISGT), 2013. s. 1-5. ISBN: 978-1-4799-2984- 9.

[4] Mlynek, P.; Misurec, J.; Koutny, M.; Silhavy, P.: Two-port network transfer function for power line topology modeling,In RADIOENGINEERING, 2012, vol. 21, no. 1, pp. 356-363.

[5] Mlynek, P.; Koutny, M.; Misurec, J.; Raso, O.: Design of Secure Communication in Network with Limited Resources, In Proceedings of the 4th European Innovative Smart Grid Technologies (ISGT), 2013. s. 1-5. ISBN: 978-1-4799-2984- 9.

[6] Fujdiak, R.; Mlynek, P.; Misurec, J.; Raso, O.: Random Number Generator in MSP430 x5xx Families.,In Elektrorevue, 2013, vol. 4, num. 1, pp. 70-74. ISSN: 1213- 1539.

[7] Fujdiak, R.; Mlynek, P.; Misurec, J.; Raso, O.: Cryptography in ultra- low power Microcontroller MSP430., In International Journal of Engineering Trends and Technology (IJET), 2013, vol. 6, num. 8, pp. 398-404. ISSN: 2231- 5381.

[8] Mlynek, P.; Raso, O.; Fujdiak, R.; Pospichal, L.; Kubicek, P.: DImplementation of Elliptic Curve Diffie Hellman in Ultra- Low Power Microcontroller, In Proceedings of the 2014 37th International Conference on Telecommunications and Signal Processing (TSP), Berlin, German, 2014, s. 267-271. ISBN: 978-80-214-4983- 1.

[9] Fujdiak, R.; Misurec, J.; Mlynek, P.: Analysis of Random Number Generator from Texas Instrument in MSP430 x5xx Families, In 37th International Conference on Telecommunications and Signal Processing - TSP' 2014, Berlin, German, 2014, s. 1-4. ISBN: 978-80-214-4983- 1.

[10] Texas Instruments: MSP430f5438A Datasheet, Technical Report (SLAS612E), August 2009 (last revision August 2014).

[11] Texas Instruments: Code Composer Studio Getting Started Guide, Literature SPRU50C, November 2001.

[12] Jace, H.H.: C Implementation of Cryptographic Algorithms, Texas Instruments Application Report (SLAA547A), July 2013.

[13] Texas Instruments: Advanced Encryption Standard, AES-128. Available from (cited 6.3. 2015): http://www.ti.com/tool/AES-128