ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 2011. No. 2(108)
ELEKTRONIKA IR ELEKTROTECHNIKA

SYSTEM ENGINEERING, COMPUTER TECHNOLOGY
T 120
SISTEMŲ INŽINERIJA, KOMPIUTERINĖS TECHNOLOGIJOS

Energy Efficiency Comparison with Cipher Strength of AES and Rijndael Cryptographic Algorithms in Mobile Devices

J. Toldinas
Computer Department, Kaunas University of Technology,
Studentų str. 50, LT-51368, Kaunas, Lithuania, e-mail: eugenijus.toldinas@ktu.lt
V. Stuikys, R. Damasevicius, G. Ziberkas
Software Engineering Department, Kaunas University of Technology,
Studentų str. 50, LT-51368, Kaunas, Lithuania, phone: +370 37 300399, e-mails: vytautas.stuikys@ktu.lt, damarobe@soften.ktu.lt, ziber@soften.ktu.lt
M. Banionis
Computer Department, Kaunas University of Technology,
Studentų str. 50, LT-51368, Kaunas, Lithuania, e-mail: mindaugas.banionis@stud.ktu.lt

Introduction

Currently, mobility is highly important. Everyone has mobile devices: not only laptops, but also smart phones, pocket PCs, GPS receivers, etc. Mobile/wireless devices are increasingly used not only for communication, but also for other critical applications such as data storage. However, due to small size they can be easily lost or stolen. Cryptography is used for securing information stored in mobile devices. Usage time of a mobile device is constrained by its most critical resource – battery. The user must be aware of the energy consumption characteristics of the applications and services he/she uses on the mobile device [1]. Encryption algorithms, which play a main role in information security systems, consume a significant amount of computing resources and battery energy, which are very limited. High energy consumption has a direct impact on the battery life, and, consequently, on the duration and extent of the user's mobility. Thus, the reduction of energy consumption of a portable system is of the primary importance [2].

The design of crypto algorithms typically does not account for physical constraints such as limited battery energy. Therefore, the primary challenge in providing security in mobile devices is minimizing energy consumption and maximizing security [3]. Scalable features such as scalable key establishment protocols and scalable authentication schemes, in which different security, performance and energy trade-offs are enabled for different application scenarios are especially desirable [4].

Here we evaluate cipher strength (the number of bits in the key used to encrypt data) of AES and Rijndael crypto algorithms versus energy consumption in mobile devices aiming to find an energy efficient combination of crypto algorithm parameters for different user application scenarios and energy consumption strategies.

Context of Research

AES (Advanced Encryption Standard) is an encryption standard adopted by the U.S. government starting in 2001. It is widely used to protect network traffic, personal data, and corporate IT infrastructure. AES is a symmetric block cipher that encrypts/decrypts data in several rounds by taking a fixed block of 128 bits of data and producing the encrypted data. Each round for encryption uses a sub-key that is generated using a key schedule and performs a sequence of steps on the input state, which is then fed into the next round.

In 2003, the Government of USA announced that AES may be used to protect classified information: the cipher strength of all key lengths of AES are sufficient to protect classified information up to the SECRET level, however, TOP SECRET information requires use of either 192 or 256 bit keys [5]. However, the recent paper [6] claims that the 10-round AES is theoretically possible to crack by cryptanalysis [7].

The Rijndael algorithm is a symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in variable-length blocks. The block length and the key length can be set independently (AES cannot do this) to 128, 192 or 256 bits. Rijndael uses a variable number of rounds, depending on the key/block sizes, as follows:

- 9 rounds if both the key and block size is 128 bits;
- 11 rounds if either the key or block size is 192 bits;
- 13 rounds if either the key or block size is 256 bits.

Rijndael is expected to replace Data Encryption Standard (DES) and its later version Triple DES over the next few years in many cryptography applications.

Microsoft® provides a .NET framework technology that has a crypto service provider for information encryption/ decryption on a handheld PC with DES, 3DES, AES, RC2 algorithms [8].

As energy consumption awareness is highly important in mobile devices, we must ensure required functionality, data security level and reasonable use of energy at the same time. Empirically we can predict that cryptography with a longer key will ensure higher levels of security at the cost of higher energy consumption. However, block size also has influence, because larger blocks will require more encryption rounds. Energy consumption also depends on the application scenario, e.g., if the user only encrypts data on a mobile device but decrypts its elsewhere, the energy/cipher strength trade-off will differ from the scenario, when a user encrypts/decrypts data on a mobile device only. Therefore, in order to use crypto algorithms energy-efficiently one needs to understand the relationships between energy consumption and encryption parameters. Once these relationships are understood well then it is possible to optimize energy consumption vs. security requirement or vice-versa.

Methodology

The task of the experiments is to identify dependencies between cryptography key lengths and block sizes on one hand, and energy consumption strategy, energy / cipher strength trade-offs and cryptography application scenarios on the other hand. These dependencies are expressed using a feature diagram in Fig.1.

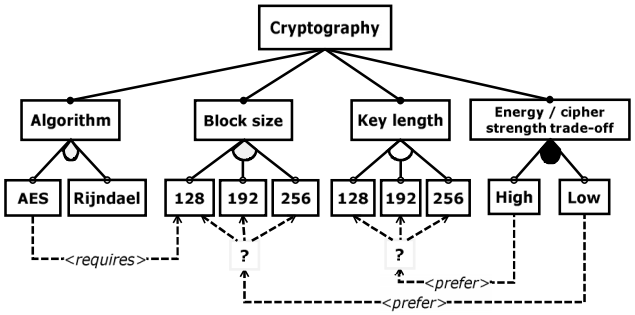

Fig. 1. Feature model of dependencies in cryptography domain

Fig. 2 outlines an algorithm that enables to perform measurements of energy consumption and obtain the desired relationships. We apply the OS-based measuring scheme [9], where the amount of the consumed energy over time is periodically written to the file during the data cryptography process. The remaining part of analytic framework and result interpretation was described in [10].

The energy consumption values for individual crypto algorithms are obtained by running their .NET Compact Framework Crypto Service Provider implementations, and measuring the current battery drain. For getting valuable results of the battery drain when data is encrypted/decrypted, we iterate the cryptography process. Since encryption and decryption time may vary we perform encryption and decryption separately.

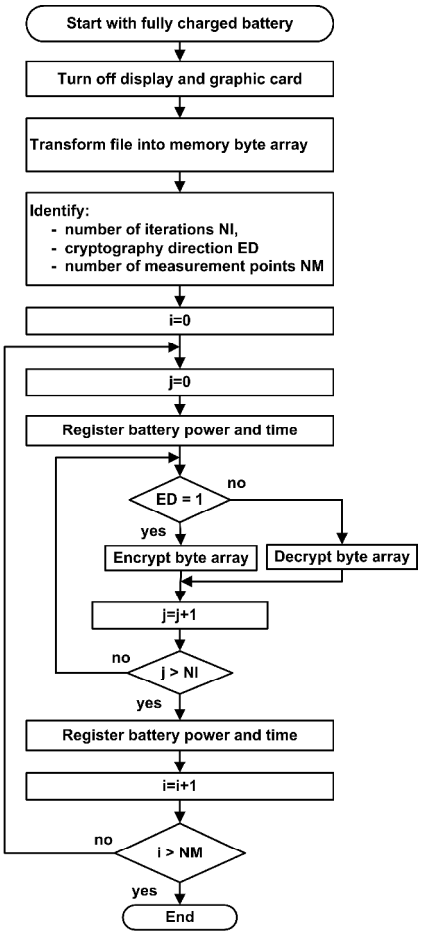

Fig. 2. Energy measurement algorithm for a crypto algorithm

Experiments

To realize the experiments we have developed the program that implements the algorithm (Fig. 2) in C# language for .the NET Compact Framework. The experiments were performed on the PDA of the model ASUS P750 (Pocket PC platform, Intel PXA270 520 MHz CPU, 256 MB RAM, Windows Mobile © 6 Professional CE OS 5.2). We used .NET Compact Framework v3.5.

Motivated by the fact that the largest amount of information the users work on locally as well as on the internate is made by the media files (pictures, music, video), for encoding we used a benchmark 'Lena.bmp' (size = 786,486 B) image (see Fig. 3).

Fig. 3. Benchmark image used for encoding

The initial condition for all experiments is the same: battery is fully charged at 100% level. The image file is loaded from a storage memory to an array and an encryption algorithm is applied. To achieve a significant battery drain for more precise measurement, the encryption process is repeated 6000 times. After each experiment, the battery is charged again to 100%. The same procedure is also applied for measuring energy consumption of a decryption algorithm.

We provide the summary of the experiment results in Tables 1 (for AES with fixed block size of 128 bytes) and Tables 2 (for Rijndael with variable block sizes of 128 bytes, 192 bytes and 256 bytes).

Table 1. Experimental results for AES/Rijndael encryption

Block size, b	Key size, b	Elapsed time (all iterations), hh:mm	Battery energy consumed, %
128	**128**	**02:01:04**	**50**
128	192	02:19:10	57
128	256	02:38:13	64
192	128	02:27:01	55
192	**192**	**02:27:01**	**55**
192	256	02:12:51	62
256	128	02:12:15	60
256	192	02:27:09	59
256	**256**	**02:27:01**	**60**

Table 2. Experimental results for AES/Rijndael decryption

Block size, b	Key size, b	Elapsed time (all iterations), hh:mm	Battery energy consumed, %
128	**128**	**02:29:59**	**57**
128	192	02:40:07	65
128	256	02:57:59	72
192	128	02:35:12	62
192	**192**	**02:35:03**	**63**
192	256	02:53:58	70
256	128	02:48:54	69
256	192	02:48:54	68
256	**256**	**02:48:09**	**68**

Analysis of experimental results

We treat the problem of finding best energy efficiency vs cipher strength as the *Pareto optimality* problem. Let E be a set of feasible design choices, where $e_{ij} = f(b_i, k_j)$, $e_{ij} \in E$ is a choice dependant upon two criteria: b_i (block size) and k_j (key size). Let Y be a subset of E, where $y_j = \min_{b_i} f(b_i, k_j)$, $y_j \in Y$. Then Y is a set of the Pareto-optimal solutions of E. The experimental results, which belong to a set of the Pareto-optimal solutions, are shown in Tables 1 and 2 in grey. We can note that for all Pareto optimal solutions the block size and the key size are equal.

Based on these results, we can construct three security profiles for mobile device users as follows:

1) *Low energy / low security:* so far considered secure, but theoretically crackable.

2) *Medium energy / medium security:* suitable for top secret information; consumes ~ 10% more energy than low energy/security profile.

3) *High energy / high security:* suitable for top secret information; consumes ~ 8% more energy than medium energy/security profile.

These profiles are summarized in Fig. 4.

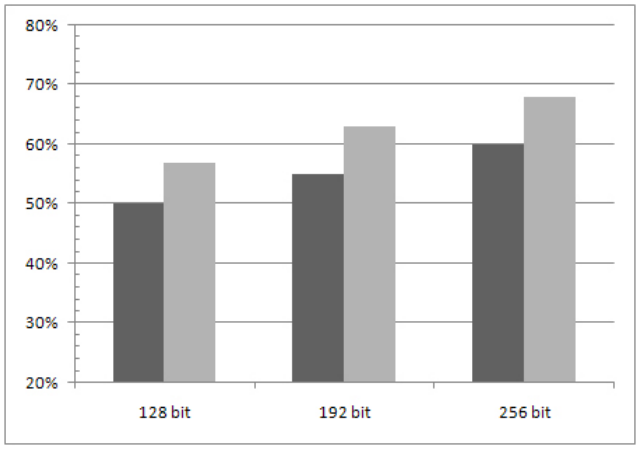

Fig. 4. Comparison of security profiles for encryption (left) and decryption (right): energy consumption vs block/key size

Another finding from Tables 1 and 2 is that decryption requires more battery energy than encryption. Furthermore, there is a linear relationship between enryption energy and decryption energy: decryption requires ~14% ($R^2 = 0.985$) more energy than encryption (see Fig. 5).

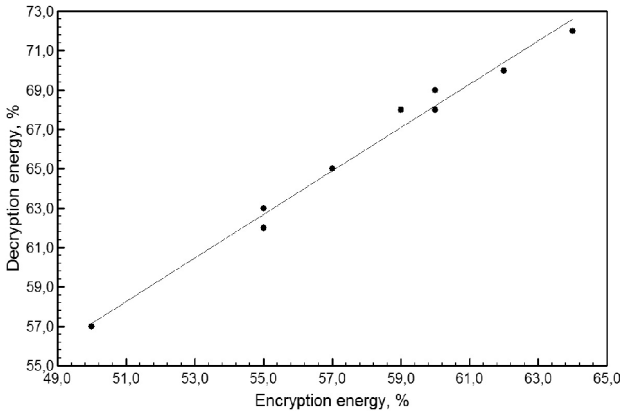

Fig. 5. Relationship between decryption vs. encryption energy

Evaluation and conclusions

For experiments, we use the Microsoft .NET Compact Framework as a modern and popular platform for safe development mobile applications and secure information management. Though there are many encryption/ decryption algorithms we were restricted with the algorithms provided by this Framework. The energy-efficiency of crypto algorithms with varying key and block

sizes is highly different. Therefore, the users of a mobile system should choose the most appropriate parameters of a crypto algorithm by taking into account the level of security required and the operational cost that the users are willing to accept depending on the security level they choose, and energy needed to perform encryption/ decryption operation with respect to the battery lifetime.

The main results of this paper are as follows:

1) The Pareto-optimal values for energy consumption of AES/Rijndael crypto algorithm are achieved when block sizes and key sizes are equal.

2) We proposed three energy/security profiles for users of mobile devices based on using 128, 192 and 256 b blocks/keys.

3) The results of energy consumption measurements when performing data encrypion can be used to reliably predict energy consumption of decryption operation: decryption requires 14% more energy than encryption.

References

1. **Tiliute D. E.** Battery management in wireless sensor networks // Electronics and Electrical Engineering. – Kaunas: Technologija, 2007. – No. 4(76). – P. 9–12.
2. **Baums A.** Energy consumption optimization in hard real-time system CMOS processors // Electronics and Electrical Engineering. – Kaunas: Technologija, 2006. – No. 4(68). – P. 19–22.
3. **Chandramouli R.** Battery power-aware encryption. // ACM Transactions on Information and System Security (TISSEC), 2006. – Vol. 9. – No. 2. – P. 162-180.
4. **Dumčius A., Gužauskas N.** Mixed Data Encryption System // Electronics and Electrical Engineering. – Kaunas: Technologija, 2002. – No. 6(41). – P. 12–15.
5. **Kelsey J., Lucks S., Schneier B., Stay M., Wagner D., Whiting D.** Improved Cryptanalysis of Rijndael // Fast Software Encryption, 2000. – P. 213–230.
6. **Biryukov A., Keller N., Khovratovich D., Shamir A.** Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds // Advances in Cryptology - Eurocrypt 2010, 29th Int. Conf. on the Theory and Applications of Cryptographic Techniques, Lecture Notes in Computer Science, 2010. – Vol. 6110. – P. 299–319.
7. **Toemeh R., Arumugam S.** Breaking Transposition Cipher with Genetic Algorithm // Electronics and Electrical Engineering. – Kaunas: Technologija, 2007. – No. 7(79). – P. 75–78.
8. **Toldinas J., Rudzika D., Štuikys V., Ziberkas, G.** Rootkit Detection Experiment within a Virtual Environment // Electronics and Electrical Engineering – Kaunas: Technologija, 2009. – No. 8(104). – P. 63–68.
9. **Toldinas E., Štuikys V., Damaševičius R., Ziberkas G.** Application–level energy consumption in communication models for handhelds // Electronics and Electrical Engineering – Kaunas: Technologija, 2009. – No. 6(94). – P. 73–76.
10. **Damaševičius R., Štuikys V., Toldinas E.** Embedded program specialization for multiple criteria trade–offs // Electronics and Electrical Engineering. – Kaunas: Technologija, 2008. – No. 8(88). – P. 9–14.

Received 2010 11 16

J. Toldinas, V. Stuikys, R. Damasevicius, G. Ziberkas, M. Banionis. Energy Efficiency Comparison with Cipher Strength of AES and Rijndael Cryptographic Algorithms in Mobile Devices // Electronics and Electrical Engineering. – Kaunas: Technologija, 2011. – No. 2(108). – P. 11–14.

We analyse energy efficiency vs. cipher strenth of AES/Rijndael crypto algorithms in a mobile device with respect to block and key size. The experimental results show that Pareto-optimal solutions have equal block and key sizes. We also propose three energy/security profiles for the users of mobile devices. As decryption operation requires 14% more energy than encryption, the results of energy consumption measurements when performing data encrypion can be used to predict energy consumption of decryption operation. Ill. 5, bibl. 10, tabl. 2 (in English; abstracts in English and Lithuanian).

J. Toldinas, V. Štuikys, R. Damaševičius, G. Ziberkas, M. Banionis. Mobiliųjų įrenginių AES ir Rijndael kriptoalgoritmų energijos sąnaudų ir saugumo palyginimas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2011. – Nr. 2(108). – P. 11–14.

Nagrinėjamoss AES ir Rijndael algoritmų energijos sąnaudos, esant įvairiems šių algoritmų parametrams – bloko ir rakto dydžiams. Remiantis gautais eksperimentiniais rezultatais: 1) siūloma naudoti vienodus bloko ir rakto dydžius, 2) pasiūlyti trys energijos sąnaudų ir saugumo profiliai, 3) pastebėta tiesinė priklausomybė tarp šifravimo ir dešifravimo metu suvartojamos energijos kiekio, kuriuo remiantis galima prognozuoti dešifravimo metu suvartojamos energijos kiekį. Il. 5, bibl. 10, lent. 2 (anglų kalba; santraukos anglų ir lietuvių k.).