LETTER

# Cryptographic Energy Costs are Assumable in Ad Hoc Networks

**Helena RIFÀ-POUS**[†a)], ***Student Member***
*and* **Jordi HERRERA-JOANCOMARTÍ**[†,††b)], ***Nonmember***

**SUMMARY** Performance of symmetric and asymmetric cryptography algorithms in small devices is presented. Both temporal and energy costs are measured and compared with the basic functional costs of a device. We demonstrate that cryptographic power costs are not a limiting factor of the autonomy of a device and explain how processing delays can be conveniently managed to minimize their impact.

***key words:*** *performance, energy, cryptography, ad hoc networks, mobile*

## 1. Introduction

Security has become one of the principal challenges for deploying ad hoc networks, which are usually comprised of small mobile terminals. Hence, it is important to know the real costs of cryptography in handheld devices for designing efficient protocols that suit this context. We present a practical comparative study of security-related costs in an up-to-date PDA, measuring the computational ability and the battery power consumption to process cryptographic algorithms, as well as the energy costs associated with the network interface.

Previous works have studied the performance of cryptographic algorithms in constrained devices [1]–[6]. However, they focus on the utilization of some particular resources in a specific set of algorithms with the aim to detect bottlenecks and improve algorithm implementations. Our analysis covers diverse cryptographic techniques that provide user authenticity and give a global view of their impact in ad hoc network protocols.

We have conducted benchmarking tests for the most used algorithms nowadays and the ones recommended by international organizations. The chosen block cipher algorithms are Data Encryption Standard (DES), Triple DES (3DES) and Advanced Encryption Standard (AES). In public key cryptography, we have tested Rivest Shamir Adleman (RSA), Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA) and emerging algorithms based on pairings (Boneh-Lynn-Shacham (BLS) and Boneh-Boyen (BB)) [7], [8]. We have used the procedures of OpenSSL-0.98 C library[*] to program the tests, except for the pairing schemes, in which we have used the PBC_sig-0.0.2 library[**].

## 2. Benchmark Results

Tests were launched on an HP iPAQ 2790b with an Intel XScale PXA270 processor at 624 MHz and 64 MB of SDRAM memory. It runs Windows Mobile 5.0 operating system. We have used the function *times* of the C Standard Library to control the elapsed CPU time for every process. The energy costs have been estimated from the battery status information provided by the battery driver. In particular, we have used the *GetSystemPowerStatusEx2* function from the Windows MSDN library.

First we measured the basic costs of the PDA. The expended power with the screen switched off is 213.28mW, and with the screen at maximum luminescence is 714.35mW. The screen is usually switched on when the user is working and so, it is one of the main reasons that can limit the autonomy of the device and a good reference to weight other's functions costs. We observe that using the PDA with the screen at maximum luminescence increases the power expenses of the basic functionality of the PDA more than a 100%, and that a good policy to reduce the energy costs is decreasing the glow.

We have also considered the cost of communication for its relevance in network protocols. The energy consumed by an interface depends on its operating mode. We have measured the energy of the IEEE 802.11b interface at 15dBm (~32mW) in idle state and also during transmission and receiving processes. Idle state consumes 792.68mW, and then, moreover, when using the communication channel, the transmission of data costs 10.40$\mu J$ per byte, while the reception is 3.48$\mu J$ per byte. As indicated, transmitting requires more energy than receiving, but the difference is not so notorious

[†] The author is with the Computer Science and Multimedia Studies, Universitat Oberta de Catalunya, 08018-Barcelona, Spain

[††] The author is with the Information and Communications Engineering Department, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain

a) E-mail: hrifa@uoc.edu

b) E-mail: jherrera@deic.uab.cat

[*] OpenSSL Project: http://www.openssl.org

[**] PBC_Sig Project: http://crypto.stanford.edu/pbc/sig

**Table 1** Costs of symmetric algorithms in a PDA

| | Time (ms) | Energy cost (mJ) |
|---|---|---|
| **DES-64** | 0.01 + 0.27x | 0.01 + 0.34x |
| **3DES-192** | 0.03 + 0.72x | 0.03 + 0.91x |
| **AES-128** | 0.16x | 0.21x |
| **AES-256** | 0.21x | 0.28x |

bearing in mind that both processes have associated an intrinsic idle state cost. Network idle costs are critical and a main concern for ad hoc networks

### 2.1 Symmetric Algorithms

We analyze the resources employed by DES, 3DES and AES to encrypt and decrypt a file using the Electronic Code Book (ECB) cipher mode, because of its simplicity and its widespread use. Since in ECB the plaintext is cut in blocks of a predefined size and these blocks are sequentially encrypted by the processor, we model the consumed energy and time of symmetric encryption with a linear equation. Table 1 shows the processing costs of each tested algorithm and also, the consequent basic costs of the PDA during the elapsed time of computations (both network and O.S. expenses with the screen switched on).

It is clearly remarkable from the results that AES performs very much better than DES and 3DES in ARM processors. Moreover, the required initialization costs for DES and 3DES algorithms are greater than that of AES. Thus, AES is not only the best algorithm for ciphering large documents, but also for small ones. Besides, it offers a greater security level.

In [3] and [4] some temporal benchmarking tests are executed in PDAs of similar characteristics than ours. The first has a throughput for AES-256 of 149.5 KBps, and the second 1382.7 KBps. Our results are much better, 4761.9 KBps. We impute the differences with [3] to the algorithms implementation (we use plain C instead of C#), and with [4] to the fact that they tested the cipher with very small input data (128 bits) so the operational costs of the initialization are not amortized. Finally, we compare the results with [1] that used an optimized self implementation library of AES. Although the differences in the processor, it is clear that our results are worst. Hence, the implementation of OpenSSL can be clearly optimized.

Energy costs results are in accordance with other studies like [2] in the sense that AES-128 is about a 60% more efficient than DES, and 3DES, as expected, is three times more consuming than DES. However, values differ substantially depending on the device and implementation.

### 2.2 Digital Signature Algorithms

**Table 2** Costs of asymmetric algorithms in a PDA

| | Time (ms) | | Energy (mJ) | |
|---|---|---|---|---|
| | Sign | Verify | Sign | Verify |
| **RSA-512** | 6.46 | 1.77 | 7.59 | 2.09 |
| **RSA-1024** | 24.05 | 2.72 | 25.87 | 3.24 |
| **DSA-512** | 4.35 | 4.70 | 5.93 | 5.76 |
| **DSA-1024** | 11.27 | 13.00 | 13.30 | 17.80 |
| **ECDSA-112** | 25.00 | 25.16 | 28.09 | 28.01 |
| **ECDSA-160** | 32.20 | 36.03 | 32.66 | 38.83 |
| **BLS** | 48.49 | 99.49 | 50.23 | 112.59 |
| **BB** | 49.41 | 159.96 | 56.46 | 190.44 |

We test asymmetric cryptography using different algorithms. RSA-512, DSA-512 and ECDSA-112 have similar security levels, as well as RSA-1024, DSA-1024, ECDSA-160, BLS and BB. We use relatively short keys because the aim of the network protocols is in-line security, not non-repudiation. The robustness of the system is assured if keys a renewed in a regular basis.

Table 2 shows the temporal and energetic costs of digital signature algorithms. The results evidence that the best performances in handheld devices are from RSA and DSA. The average costs of signatures generation and verification is more or less the same for the two algorithms, however, RSA has best results in verification, while DSA is faster in signature generation. For this reason, RSA is well suited for systems that require only few signature generations but thousands of signature verifications.

Although ECDSA is not so efficient as RSA and DSA for short key lengths, is remarkable the low incremental costs when increasing the security level. In average, RSA operations using 512 bit keys are about 4 times faster than using 1024 bit keys. In DSA this ratio is around 3. Besides, this ratio increases when the length of the RSA and DSA keys gets longer. In contrast, the ratio for ECDSA keys of 112 and 160 bits is less than twofold and shrinks when increasing the security level. On the other hand, the length of a signature generated with ECDSA is 224 bits for ECDSA-112, and 320 bits for ECDSA-160, which is much shorter than the signatures generated with RSA. These results are coherent with other research works [2], [5], although the notable differences between implementations.

Finally, costs of pairing based signatures are quite expensive compared with the others. The advantages of these schemes are shortness of the signatures and the possibility to build multisignature and batch signature verification mechanisms over them. Moreover, pairing based operations can be optimized (about 95%) in hardware implementations thus reducing the overhead of BLS and BB signatures. Then, the development of short signature schemes could get performances better than elliptic curve cryptography.

### 2.3 Remarks

Results attest that cpu energy spent in cryptographic operations represent around 45% of the total expenses of a PDA in basic state. The rest is due to network interface, screen and basic operative system functions. During the execution of a network security protocol, the major costs of a node are not because of its own computations, but for the waiting time to receive responses from other nodes, which much depend on the size and congestion of the network.

For example, in a network with an effective transmission rate of 5Mbps and a radix of 10 nodes, the costs of a node during the execution of a secure routing protocol (i.e. SAODV [9], SEDYMO[10]), are equally divided into cryptographic operations and data transmission (10%). The rest (90%) is due to the basic costs of the device during the waiting time. Delays are mainly caused by computational operations in the intermediate nodes of the routing path.

## 3. Conclusions

Today's handheld devices are designed to support network security protocols that involve symmetric and asymmetric cryptography. The test results show that symmetric cryptography is the most efficient when dealing with short files, but digital signatures are the best way to get authenticity and integrity over data packets about 30KB or more (digital signatures use hash algorithms which costs are nearly negligible). On the other hand, network interface and screen are the key elements that limit the autonomy of a device, and so, protocols shall be designed to reduce delay times as much as possible.

## Acknowledgments

This work was partially supported by the Spanish Ministry of Science and Education under grants TSI-020100-2008-365 SAT2, TSI2007-65406-C03-03 E-AEGIS and CONSOLIDER CSD2007-00004 ARES.

## References

[1] J. Großschädl, S. Tillich, C. Rechberger, M. Hofmann, and M. Medwed, "Energy evaluation of software implementations of block ciphers under memory constraints," Proceedings of the conference on Design, automation and test in Europe (DATE), San Jose, CA, USA, pp.1110–1115, EDA Consortium, 2007.

[2] N. Potlapally, S. Ravi, A. Raghunathan, and N. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," Transactions on Mobile Computing, vol.5, no.2, pp.128–143, Feb. 2006.

[3] C. Hager, S. Midkiff, J. Park, and T. Martin, "Performance and energy efficiency of block ciphers in personal digital assistants," IEEE International Conference on Pervasive Computing and Communications (PerCom), pp.127–136, March 2005.

[4] A. Ramachandran, Z. Zhou, and D. Huang, "Computing cryptographic algorithms in portable and embedded devices," IEEE International Conference on Portable Information Devices (PORTABLE), pp.1–7, May 2007.

[5] C. D.Westhoff, B.Lamparter and A.Weimerskirch, "On digital signatures in ad hoc networks," Wiley Journal European Transactions on Telecom., vol.16, no.5, pp.411–425, October 2005.

[6] K. Mahmud, M. Inoue, H. Murakami, M. Hasegawa, and H. Morikawa, "Energy consumption measurement of wireless interfaces in multi-service user terminals for heterogeneous wireless networks," IEICE Trans. Commun., vol.88, no.3, pp.1097–1110, March 2005.

[7] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001.

[8] R. Dutta, R. Barua, and P. Sarkar, "Pairing-based cryptographic protocols: A survey," Cryptology ePrint Archive, 2004.

[9] M. Guerrero Zapata, "Secure Ad hoc On-Demand Distance Vector Routing," ACM Mobile Computing and Communications Review (MC2R), vol.6, no.3, pp.106–107, July 2002.

[10] H. Rifà-Pous and J. Herrera-Joancomartí, "Secure Dynamic MANET On-demand (SEDYMO) Routing Protocol," Fifth Annual Conference on Communication Networks and Services Research (CNSR), pp.372–380, IEEE Computer Society, 2007.