VLSI ARCHITECTURE FOR NANO WIRE BASED ADVANCED ENCRYPTION STANDARD (AES) WITH THE EFFICIENT MULTIPLICATIVE INVERSE UNIT

K.Sandyarani[1] and P. Nirmal Kumar[2]

[1]Research Scholar, Department of ECE, Sathyabama University, Chennai, India
[2]Associate Professor, Department of ECE, College of Engineering, Guindy, Anna University, Chennai, India

ABSTRACT

Advanced Encryption Standard (AES) Algorithm has been extensively applied in the present financial applications. Sub-channel attacks are one of the main problems occurred n the AES Algorithm. Asynchronous AES Architecture is one of the leading solutions of the sub-channel attacks due to its natural properties. The AES architecture with the enhanced mix column to be proposed with reduced number of transistor counts.. Then, the Verilog A modeling is used to evaluate the performance of the proposed AES Architecture. Finally, the VLSI Implementations of the AES Processor is implemented with CMOS technology 0.25 μm. By using the net list generations, the proposed AES Architecture is analyzed regarding the VLSI design environment. The simulation results of the proposed structure are performed with the minimum number of transistor counts as well as power utilizations. Moreover, the proposed CMOS technology based AES Algorithm is integrated into the backend based chip technology.

KEYWORDS

Advanced Encryption Standard, Sub-Channel, Mix-Column, Verilog A, Complementary metal oxide semiconductor, Nano-technology.

1. INTRODUCTION

Data security is one of the major concerns for the data communication systems. There is various security algorithms are developed for protecting the information in the data communication networks. Advanced Encryption Standard (AES) is one of the highly secured algorithms for data protections. The AES Algorithm is used to encrypt and decrypt the data by the three sizes of bits that are, 128,192 and 256The symmetric algorithm in AES and Asymmetric algorithm in RSA are the two classes of encryption methods which are commonly used. The first algorithm uses the same key for encrypting or decrypting data and is very fast due to its small key size but suffers the exchange of this key. Whereas the next one is secure because it uses a pair of keys, one for encrypting and another for decrypting, but suffers the encryption slowness due to complex computations involved by large key size (1024 bits and more).The FIPS-197 specification, some standard modes of operation. The Easiest and simplest is the electronic code book (ECB).

However, this may occur some security vulnerabilities. Additional resistance to attack may be achieved using one o f the recognized feedback modes, for instance, cipher block chaining (CBC).

However, the benefit of a feedback mode can limit the effectiveness of pipelining in a hardware implementation. Feedback modes have concentrated on the patterns which only need the encipher data path such as output feedback (OFB) mode. In recent years, the asynchronous circuit has been giving the more requirements due to the security problems and power utilizations. The state of the system and hand shake clock signals are observed by using the external and internal events of the asynchronous circuits. These circuits are also described as the self-timed circuits due to the circuit timing assumptions.

2. RELATED WORKS

Linearity and Non-Linearity technique based AES algorithms are required the Look-Up-Tables (LUT) to register the substitution value of the given input data. [1] Described the reduction of the complexity in the multiplicative inverse unit for the Advanced Encryption Standard (AES) algorithm. Multiplicative Inverse is one of the essential parts of the AES Structure. (Galois Field) GF 2^4 based multiplicative inverse unit is used to overcome the disadvantage of the conventional Linearity and Non-Linearity based AES algorithm. Composite S-Box based multiplicative inverse unit offers the minimum number of logical elements counts as the well efficient computational delay. Composite S-Box and a Multiplicative Inverse unit are used to provide the efficient cryptographic techniques.

The proposed sub-bytes transformation eliminates the usage of the LUT. The proposed composite field is used as the data path for the Sub-bytes and Inv-Sub-Bytes transformations. [2] Presented the efficient Mix-column transformation for high-speed AES Architecture. The decompose the inversion is mainly proposed in this work to provide the efficient structure with the minimized area and smaller critical path. Non-LUT based algorithm can provide the further efficiency in pipelining architecture. Mix-column transformations are designed by using simple logical ex-or gates to reduce the logical elements counts as well as efficient power utilizations.

Counter mode based architecture is used to overcome the limitation compare than the ECB and CBC modes. [3] Analyze the counter mode based AES algorithm with the nonlinearity based S-box architecture. The Counter mode based AES has not encrypted the data directly like ECB and CBC modes. The counter mode is first encrypting the counter, and then the values are XOR'ed. At each successive block of the system, the counter value is incremented by one. The virtual s-box is generated at the each input data. In the virtual S-Box, the input data are mapped by the virtual s-box to provide the encrypted data. The proposed virtual s-box architecture is performed with the efficient power utilizations as well as fewer area utilizations.

By using the CBC mode, the plaintext of the encrypted data is XOR'ed with the last cipher text of the architecture. [4] Stated the eliminate the single event upsets (SEU) and composite s-box into the AES modes of operations. Each cipher text is performed depend on the plain text in the CBC mode. The counter mode is used to overcome the disadvantage of the CBC mode. The counter mode is generating the arbitrary value for encryption and then performs the XOR operations. The reductions of the ADP (Area-Delay Product) are highly achieved by the LUT fewer Field transformations.

The proposed composite field arithmetic based S-Box transformations are providing better logical elements utilizations. [5] Described Complementary Metal-Oxide Semiconductor (CMOS) technology based Advanced Encryption and Decryption. The proposed composite S-Box design is implemented by using the 250 nm CMOS technology. By implementing the backend design, the power utilizations are highly achieved. Composite s-box unit is entirely designed by using the simple ex-or gates. In inverse ISO technique, the logical gates are highly reduced compare than the conventional ISO technique.

3. MEMORY ARCHITECTURE BASED AES COMPUTING

In general, the data stored in the memory cell is divided from the general processors and also that data is connected to I/O's. All the input data are required to mitigate, and the information is rewrite. Due to the rewrite functions, the I/O congestion occurs and also the overall system performance is affected due to the data mitigations. The power utilization of the system is also highly increased by the storage of the large data. There are some more I/O's are included in the data at high frequency is used to conquer the congestion problem in theoretical. This theoretical solution is limited by the CMOS scalability. The data preprocessing is required only the perform with a small amount of the intermediate results and also the data traffic is highly reduced by the data pre processing. The Memory logic architecture has performed some pre processing stages at locally.

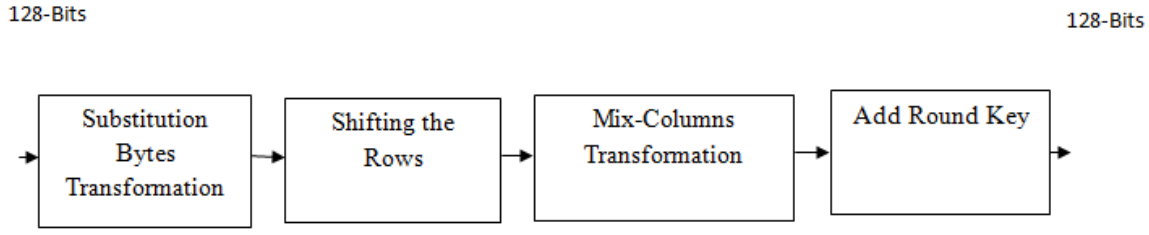

Figure 1: Flow Diagram for Advanced Encryption Standard Architecture

The memory logic in the single cell causes the overhead of the higher data and also the communication traffic is limited. Due to the memory array, there is possibility of unique data is available at a given time sequence. Single data working process is also leading the wastage of the additional resources and high power utilizations. One more disadvantage of the memory logic is, the storage has required the ordering of the information.

4. PROPOSED NANO WIRE BASED AES ARCHITECTURE

In memory based architecture, the data encryption is performed openly on the cells. The encryption data has required the model for simulating the algorithms. The domain wall can perform the one input data at a given time. To separate the nano wires, the domain wall can perform the multiple data at a time that is the concurrent operations are achieved. Each row of the binary data is required to store in the domain wall Nano wire is develop the shift function of the algorithm. For performing the storage purpose, there are four Nano wires are required. The reduction of the circular left shift operations current is achieved by the redundant bits.

A) Sub-Bytes:

The S-Box design is implemented by using the general LUT that is; there are some memory based logical elements are needed for the S-Box design. The conventional S-Box design is performed with the highest number of the logical elements counts as well as the computational delay. To reduce the logical elements counts, the S-Box architecture is implemented by using the Nano wire based structure. By using the domain wall Nano wires, the power is reduced. The memory elements and decoders are collective for reducing the logical elements counts as well as the power utilizations.

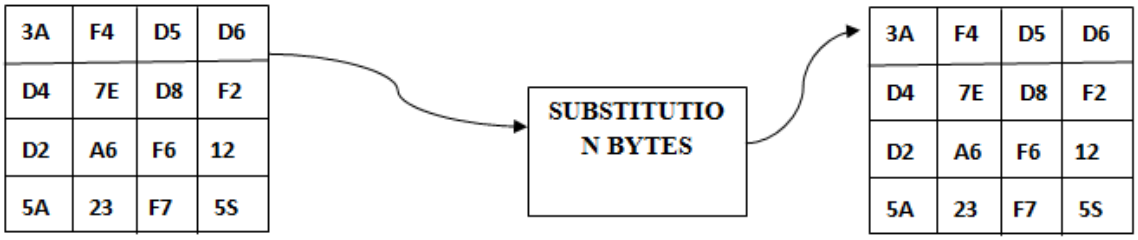

Figure 2: Proposed S-Box Architecture based Nano-Wire

B) Shift Rows:

The shift rows are performed by using the general shift property in the conventional method. In the proposed computations, the input data are shifted by using the unique domain wall Nano wire based property. The input data are operated circularly by performing the left shift operations of the binary data in the Nano wires. In the shift rows transformations, the second row of the matrix is to be left shifted by cylindrically. The second rows of the matrix are shifted by the two bits, and the third row of the matrix is shifted by the three bits. The virtual cycle on the Nano wire is formed to eliminate the storage of MSB to LSB. The circular left shifted rows are used to determine the Nano wire bits added in the system. In the Nano wire system, the various numbers of input bits are performed concurrently, so the congestion occurrence is highly avoided by using the Nano wire technology

C) Add-Round Key:

The Add round key stage is to be performing the bitwise XOR operations with the corresponding bytes of the matrix. In general, the standard XOR gate is used for the add round key operations.

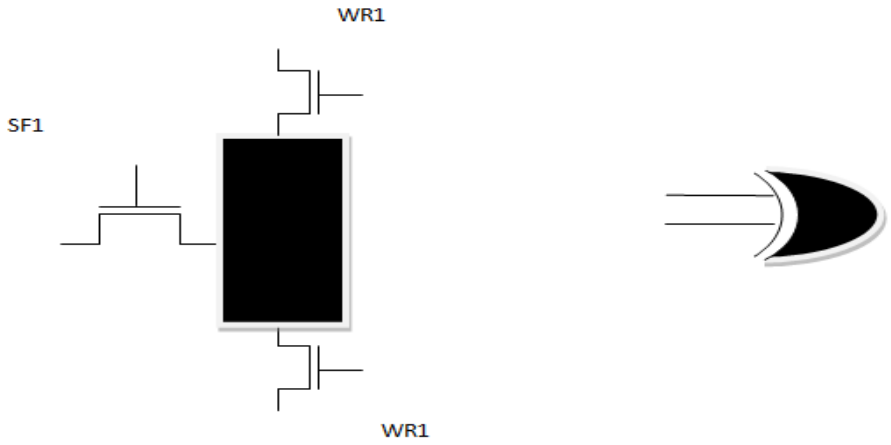

Figure 3: Nano wire based XOR Gate and Symbolic View of the XOR Gate

This Add-Round fundamental structure is performed with the highest number of area utilizations as well as the power utilization is not efficient. Nano-Wire based X-OR gate is used to implement the add-round key stage. In the proposed Nano wire based XOR gate, the output data are measured by using the low or high resistance value of the Multiple Tunnel Junction (MTJ).

D) Mix-Column Transformations:

The proposed mix column transformations are implemented by using the Domain-Wall Nano wire based EX-OR gate and Domain wall Nano wire LUT. In traditional mix column transformations, the memory based architecture is used for the both mix and inverse mix column matrix. In the proposed mix column design, the X-time multiplications and domain wall based XOR gate. There are two x-time multiplications are required for the mix-column process. The X-time 2 is slightly different from the general integer multiplications by left shift, and the bit is XORed. The proposed mix column transformations utilize the domain wall based XOR gate and domain wall based LUT, and also the xtime multiplications are used to generate the efficiency.

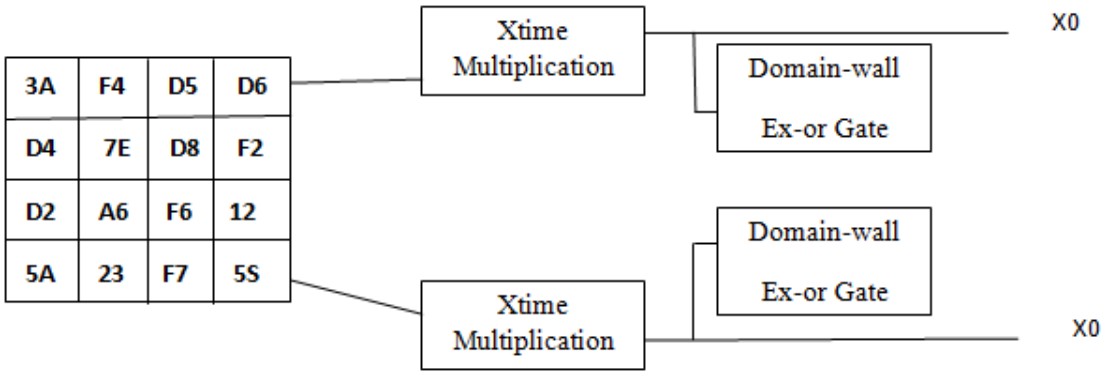

Figure 4: Proposed Mix-Column Transformations

5. EXPERIMENTAL RESULTS

The validations of the proposed AES Encryption and Decryption by using CMOS technology is implemented by using Tanner EDA and their synthesis results are carried out by using the T-Spice. Verilog A Language is used to implement the proposed design in the spice simulator to evaluate the performance characteristics. Nano-Wire based XOR Gate, and the Multiplicative inverse unit is shown in Fig.5 and Fig.6.

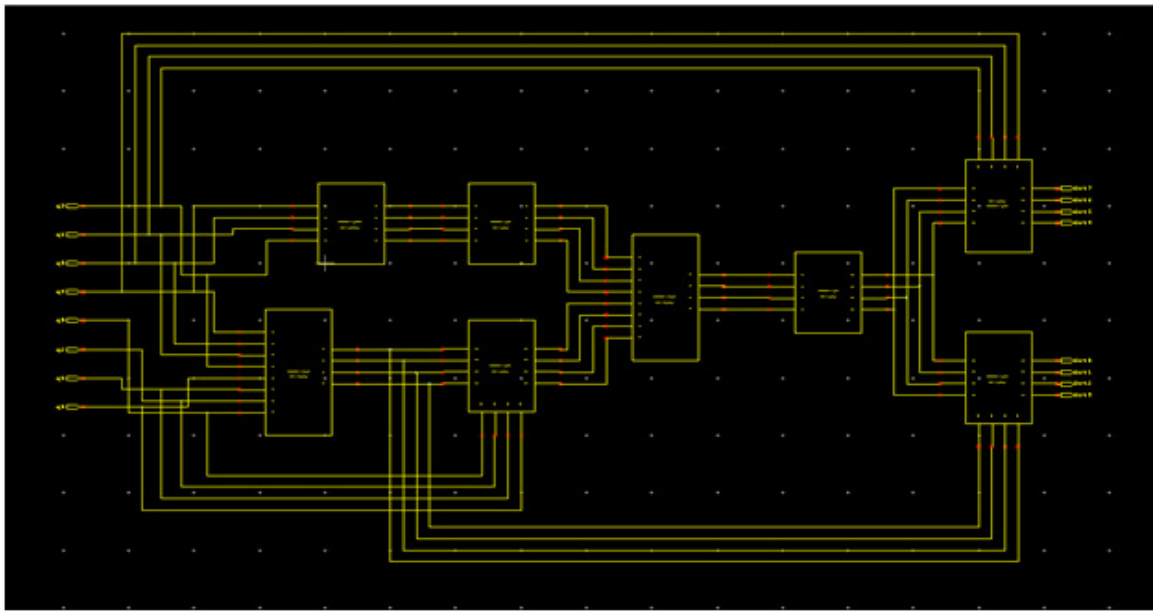

Figure 5: Schematic Design of the proposed Multiplicative Inverse Unit

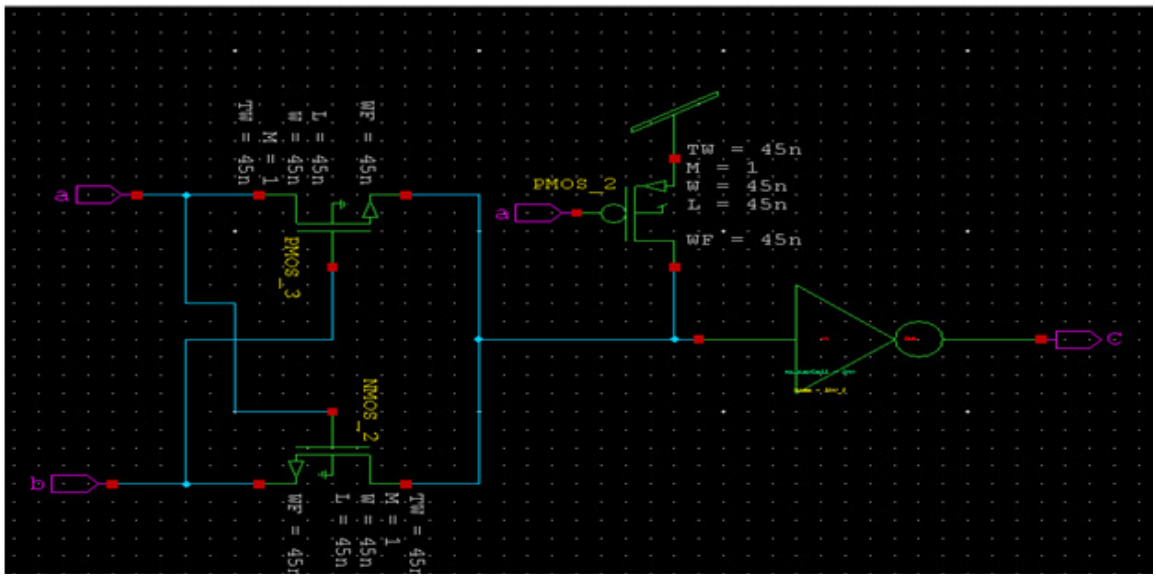

Figure 6: Proposed Nano-Wire based XOR gate

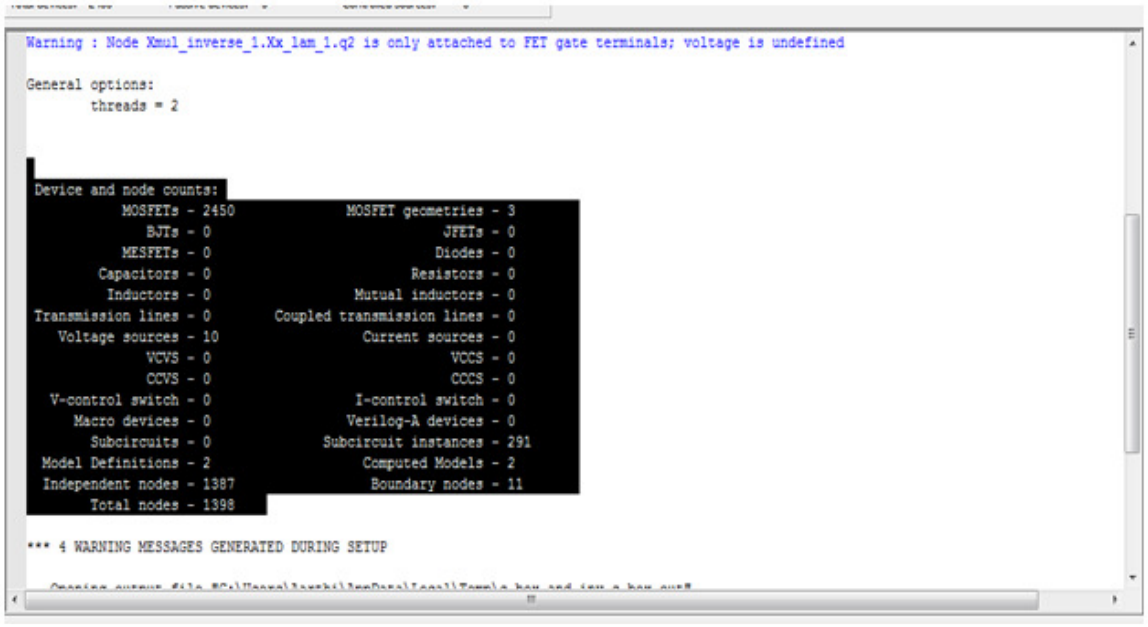

Figure 7: Synthesis Results for Number of MOSFET Counts

6. CONCLUSION

In this paper, the domain wall Nano-wire based Advanced Encryption Standard (AES) Encryption and Decryption have been implemented with the Verilog A Language. By using Verilog A Language, the proposed Nano-Wire based Multiplicative Inverse Unit is designed by using the CMOS Technology with the help of Tanner EDA and Spice simulator. The proposed schematic design is implemented in the S-Edit, and the synthesis results are carried out by using the Spice simulations. In the traditional method, the AES Encryption and Decryption is performed based on the Domino logic. The Domino logic is generating the high number of logical elements counts due to the general blocks of the CMOS technology. To reduce the number of logical elements counts, the AES Architecture is implemented by using the Domain wall Nano-Wire Technology. By using the Domain wall Nano-wire technology, the transistor sizing is highly reduced compare than the traditional logic.

REFERENCES

[1] Sandyarani, K. and Kumar, P.N., "Low Power and low CMOS Complexity Based Composite S-Box for Aes Encryption and Aes Decryption", Indian Journal of Applied Research, Vol. 5, No. 10, 2016.

[2] Sandyarani, K. and Kumar, P.N., 2014, Design of High-Speed AES – 128 using Novel MixColumn Transformation & Sub Bytes. Journal of computer applications (JCA), 2014.

[3] Sandyarani, K. and Kumar, P.N., 2013, July. Design and analysis of AES-CM with nonlinearity S-box architecture. In Current Trends in Engineering and Technology (ICCTET), 2013 International Conference on (pp. 252-254). IEEE.

[4] Sandyarani, K. and Kumar, P.N., 2014. Incorporation of Composite Field S-box into AES-CBC and AES-CM Modes to Avoid SEUs. Research Journal of Applied Sciences, Engineering and Technology, 8(12), pp.1424-1428.

[5] Sandyarani, K. and Kumar, P.N., Low Power and Low CMOS Complexity Based Composite S-Box for AES Encryption and AES Decryption. Indian Journal of Applied Research, 2015.

[6] Su, C.P., Lin, T.F., Huang, C.T. and Wu, C.W., "A high-throughput low-cost AES processor", IEEE Communications Magazine, Vol. 41, No. 12, pp.86-91, 2003.

[7] Zhang, X. and Parhi, K.K., "High-speed VLSI architectures for the AES algorithm. IEEE transactions on very large scale integration (VLSI) systems", Vol. 12, No. 9, pp.957-967.

[8] Ahmad, N. and Hasan, S.R., "Low-power compact composite field AES S-Box/Inv S-Box design in 65nm CMOS using Novel XOR Gate. Integration", the VLSI journal, Vol. 46, No.4, pp.333-344, 2013.

[9] Ahmad, N., Hasan, R. and Jubadi, W.M., "Design of AES S-Box using combinational logic optimization. In Industrial Electronics & Applications (ISIEA)", 2010 IEEE Symposium on (pp. 696-699). IEEE,2010.

[10] Feldhofer, M., Dominikus, S. and Wolkerstorfer, J., "Strong authentication for RFID systems using the AES algorithm", In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 357-370). Springer Berlin Heidelberg, 2004.

[11] Good, T. and Benaissa, M., "Very small FPGA application-specific instruction processor for AES", IEEE Transactions on Circuits and Systems I: Regular Papers, Vol. 53, No. 7, pp.1477-1486, 2006.

[12] Irwin, J. and Page, D., "Using media processors for low-memory AES implementation", In Application-Specific Systems, Architectures, and Processors, 2003. Proceedings. IEEE International Conference on (pp. 144-154). IEEE.

[13] Moradi, A., Poschmann, A., Ling, S., Paar, C. and Wang, H., "Pushing the limits: a very compact and a threshold implementation of AES", In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 69-88). Springer Berlin Heidelberg, 2011.