Analysis of power constraints for cryptographic algorithms in mid-cost RFID Tags

Tobias Lohmann, Matthias Schneider, Christoph Ruland

Institute for Data Communication Systems
University of Siegen
Hoelderlinstraße 3; D- 57076 Siegen, Germany
{tobias.lohmann, matthias.schneider, christoph.ruland}@uni-siegen.de

Abstract. Radio Frequency Identification (RFID) systems can be found in wide spread applications – from simple theft prevention over multi bit transponders up to complex applications involving contactless smartcards. This paper shows that the security gap between low-cost RFID Tags that only provide simple security features and contactless smartcards can be filled. It is examined how much energy a passive tag can gain from a magnetic field and which amount is needed by basic logic functions. The gate-equivalents of several cryptographic operations are then compared with the available energy and a conclusion is drawn if they are feasible for RFID tags.

1 Introduction

Modern automatic identification (Auto-ID) systems have a long technological history and multiple roots. The most widely recognized Auto-ID system is the bar code system developed during the early 1970's [1] but the technology which is more related to the actual one is even older. During the 2nd World War, allied planes were equipped with devices that allowed a friend or foe recognition [2]. A civil variant is able to detect friends and foes inside a shop: the well known electronic article surveillance (EAS) system. More sophisticated systems also found their way in public life and people are using ID technology for entering their ski-lift or to disable the immobilizer of their car. In the last couple of years there has been done lot of work to map all those ″root-technologies″ to one inheritor: Radio Frequency Identification (RFID). Some of them just had to be renamed to the term RFID, others had to be reinvented like the EPC tag (Electronic Product Code) to replace EAN bar codes (Electronic Article Number) [3]. The major task in this sector is to downsize the costs of a tag, so that it is lower than the monetary benefit that the RFID-System is able to gain. This still seems to be hard because the ink which is needed for bar codes is nearly free.

Another fact is that there are rising concerns about the technology that provides information and can be read wirelessly and without notice of its owner. People are afraid (or aware) of the probability that they can loose their privacy [4]. A lot of suggestions have been made to maintain privacy by adding extra functionality to the RFID tags but they all add more circuitry and higher costs. One basic method is to introduce a kill-command that disables a tag [5] – but the question is: who will be authorized to issue such a command? It is clear that this function has to be protected by a key or password. It must be secured. Applying even simple means against unauthorised tag access introduce the problem of key management. It is necessary to find a trade-off between the relative gain in security and the costs that come with them. When we talk about costs in this paper we do not only mean increasing chip sizes and increasing monetary costs, in the scope of this paper we especially address the increasing power consumption. 90% to 95% of the RFID devices are passive [7] which implies that they have to be powered by inductive coupling. Chapter 2 will show that increasing power consumption leads to a lowered maximum read range.

Developers of smartcards already had to face and solve most of the questions and problems that occur when adding security functions in embedded systems in the last decade. Smartcards have become very powerful and are able to process various cryptographic protocols such as 3DES and strong asymmetric computations with RSA and on Elliptic Curves (ECC) [6]. They are designed to fulfil high demanding security requirements and are evaluated up to Common Criteria EAL5. Most RFID tags also need electronic circuitry inside. Therefore a tag can be seen as an embedded system with wireless interface. It was just a logic step to add the wireless RF interface to existing smartcard controllers. The result is a very secure RFID tag with state of the art cryptography. The resulting device is also only able to operate close to a reader and the monetary cost for a smartcard is 20 times higher than for a simple tag.

This research was driven by the fact that the authors could not find products that offer good asymmetric cryptography and the full functionality according to ISO15693 ″Identification cards – Contactless integrated circuit(s) cards - Vicinity cards″ that operate at distances up to a meter.

2 Estimation of the available energy

Passive RFID tags gain their energy form the alternating magnetic field that is radiated by the antenna of the reader. Formula (1) shows the equation of the magnetic field, given in spherical coordinates [9][10].

$$H = -\frac{Idl}{4\pi}\beta^2 2\cos\theta\left[\frac{1}{(j\beta r)^2}+\frac{1}{(j\beta r)^3}\right]e^{-j\beta r}\vec{e}_r - \frac{Idl}{4\pi}\beta^2\sin\theta\left[\frac{1}{j\beta r}+\frac{1}{(j\beta r)^2}+\frac{1}{(j\beta r)^3}\right]e^{-j\beta r}\vec{e}_\theta \qquad \mathbf{(1)}$$

with $\beta = \frac{2\pi}{\lambda}$

Inductive coupling is only possible in the so called ″near field″, which dimension is mainly conditioned by the used frequency. The maximum distance is determined by the simplified equation (2).

$$d = \frac{\lambda}{2\pi} \qquad \mathbf{(2)}$$

If βr is set << 1 (or r << λ/2π) the exponential term of equation (1) will be close to 1 and the magnetic field decreases with $1/r^3$. The complete derivation of those coherences cannot be covered by this paper and can be found in [2].

RFID Systems according to ISO14443 or ISO15693 operate at a frequency of 13.56MHz [8]. The upper bound of the operational radius is therefore 3.5 m.

This chapter provides an estimation of the available energy that can be induced in the coil of the tags antenna. Therefore, a closer look at the supplying magnetic field of the reader has to be taken. The highest strength of the magnetic field can always be found in orthogonal direction to the plane of the coil. We can therefore simplify equation (1) and obtain equation (3) which has been used during our simulations.

$$H(z) = \frac{N_1 I r_R^2}{2(r_R^2 + z^2)^{3/2}} \vec{e}_z \tag{3}$$

The curve is dependent on the current I, the number of windings N_1 and the square of the antenna radius r_R. Figure 1 shows the MATLAB [16] simulations of the emitted fields that are radiated by antennas with same currents and windings but different diameters.

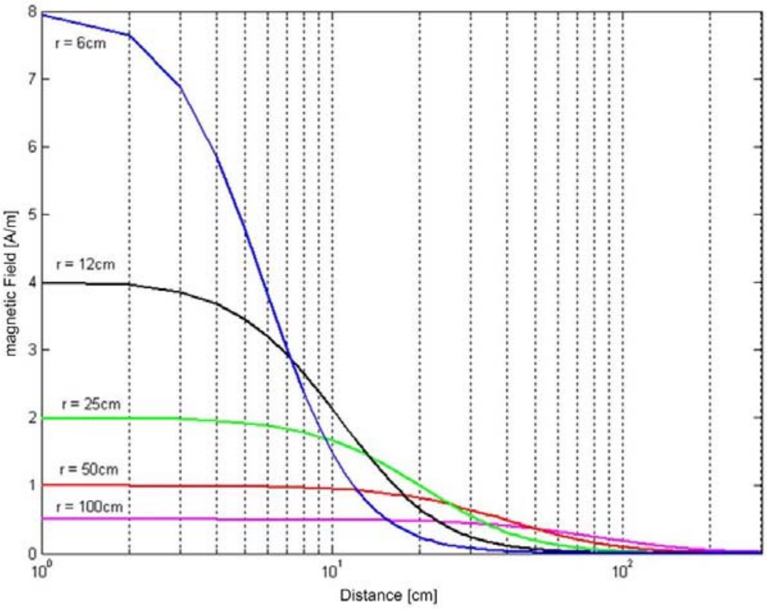

Fig. 1. The distribution of the magnetic flux by distance

Figure 1 shows that a smaller diameter of the antenna coil results in a higher initial strength of the magnetic field but an earlier and sharper decline as they occur with bigger loops.

It is not allowed to increase the strength of the magnetic field arbitrarily to achieve the needed distance because the usage of the electromagnetic spectrum is regulated by local authorities. They defined absolute maximum ratings of the power that an antenna may emit. In the European ISO14443 standard the maximum strength of the magnetic field is defined to be 7.5 H/m [8].

RFID Systems can basically be seen as a transformer with a big gap between primary- and secondary side. This implies that the well known electronic equations can be used.

The voltage V$_{tag}$ that is available for the logic of the tag is [7]

$$V_{tag} = \frac{V_{2,1}}{\sqrt{(\omega L_2 / R_L + \omega R_{L_2} C_2)^2 + (1 + R_{L_2} / R_L - \omega^2 L_2 C_2)^2}}\,. \tag{4}$$

The load R$_L$ has a major effect on the available voltage as it can be seen in equation (4). This formula is converted to formula (5) to show the possible value of the load resistor for a given and needed voltage.

$$R_L = \left(\frac{R_{L_2}}{\left(\frac{V_{2;1}}{V_{tag}}\right)^2 - 1 - \left(\omega R_{L_2} C_2\right)^2 + 2\omega^2 L_2 C_2 - \left(\omega^2 L_2 C_2\right)^2} \right) \pm \frac{\sqrt{R_{L_2}^2 - \left(\left(R_{L_2}^2 + \left(\omega L_2\right)^2\right) \left(1 + \left(\omega R_{L_2} C_2\right)^2 - 2\omega^2 L_2 C_2 + \left(\omega^2 L_2 C_2\right)^2 - \left(\frac{V_{2;1}}{V_{tag}}\right)^2 \right) \right)}}{1 + \left(\omega R_{L_2} C_2\right)^2 - 2\omega^2 L_2 C_2 + \left(\omega^2 L_2 C_2\right)^2 - \left(\frac{V_{2;1}}{V_{tag}}\right)^2} \tag{5}$$

In the last step, we obtain the available power by applying formula (6).

$$P = \frac{U^2}{R_L}\,. \tag{6}$$

A more handy representation is obtained in Figure 2 where the absolute power in dependence of the distance is shown. It gives the maximum range of a tag whose power consumption is known. Or in the other direction: the curve defines the upper bound of the power which could be consumed if the tag has to operate at a given distance.

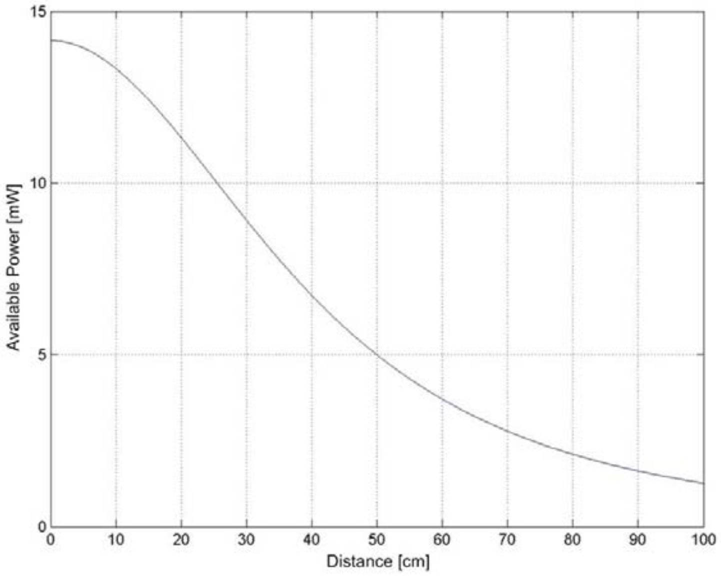

Fig. 2. Available tag power in dependence of the range

The proof of these results is obtained by comparing the calculated curve with data sheets of several tags. For example, if the average power consumption is given by 2 mW, they should not have a read range greater than 70 cm.

3 Estimation of a tags power consumption

The circuitry of most RFID tags is based on CMOS (complementary metal oxide semiconductor) technology. CMOS technology has the great advantage that it is possible to design electronic circuits with only relevant power consumption when the transistors change their operational state.

This chapter investigates the average power consumption needed by basic logic functions. The integrated circuits are simulated with WinSpice [17] which allows a good reproduction of the real hardware behavior. The transistors were designed to provide the needed functionality with the smallest possible geometry. A lot of process dependent parameters were obtained by the databases of the MOSIS service [11]. This allowed comparing the influence of different manufacturing sizes and technologies.

This paper presents an analysis of three basic building blocks often needed by cryptographic operations. These are shift-registers, XOR operations and NAND gates.

Shift-register cell

A shift-register like shown in Figure 3 is built by serialization of two inverters that are clocked by orthogonal signals clk and $\overline{clk}$.

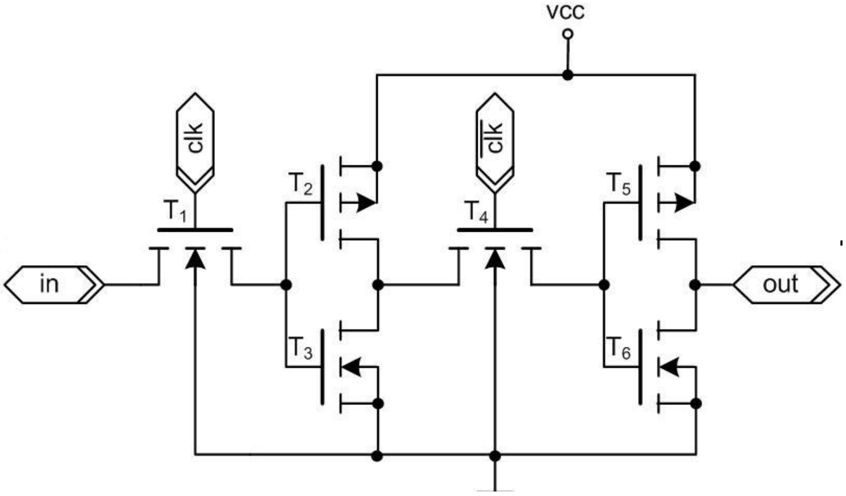

Fig. 3. CMOS shift-register [14]

The power of the register cell is supplied by VCC and only has to deliver current when the level of the input signal is changing. This correlation is shown in the following plot where the output curve v(5) is delayed by the clock rate.

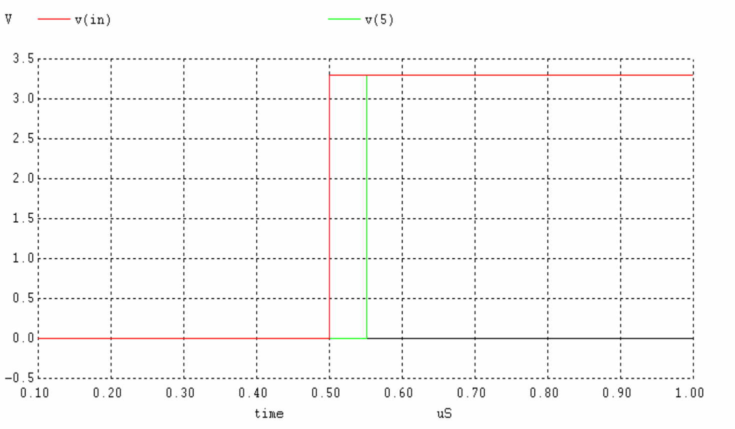

Fig. 4. Input and output voltages of a shift register

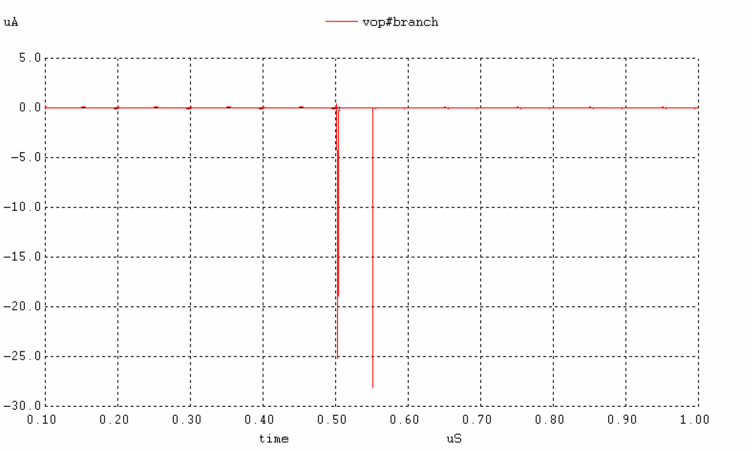

Fig. 5. Current consumption of a register cell when changing its state

Static and other currents can be omitted because their amplitudes are negligible. They can be seen in the upper simulation plot as small dips in the current curve vop#branch. Results of the simulation runs are given in table 1. The resulting energy is obtained by multiplying the average of the current with the voltage VCC and the time interval where the current occurred. It is estimated that the transitions between logic ″1″ and logic ″0″ are equally distributed and the mean energy will be used for further calculations.

Process	VCC [V]	Interval t(0-1) [ns]	Current I_{mittel} (0-1) [µA]	Energy W_{0-1} [fWs]	Interval t(1-0) [ns]	Current I_{mean}(1-0) [µA]	Energy W_{1-0} [fWs]	Energy W_{mean} [fWs]
0.35 µm TSMC	3.3	4.5	7.2716	140.18	1.1	11.8731	176.94	158.56
		1.1	8.86937		5	8.11171		
0.25µm TSMC	2.5	4.5	8.84425	128.78	1.1	12.8971	142.23	135.51
		1.1	10.6490		5.6	7.60818		
0.18µm TSMC	1.8	5	3.70572	42.21	1.4	7.66053	62.96	52.59
		0.8	6.15294		6	4.04206		

Table 1. Energy overview of a shift-register

XOR

XOR Gates can be implemented in various ways. We examined realisations based on transmission gates, CVSL (Cascode Voltage Switch Logic) and in AOI (And Or Inverter) realisation. Since the CVSL solution had a high dynamic loss and the current peaks of the transmission gate implementation were too short for WinSpice, only the results of our AOI-based XOR simulations are presented.

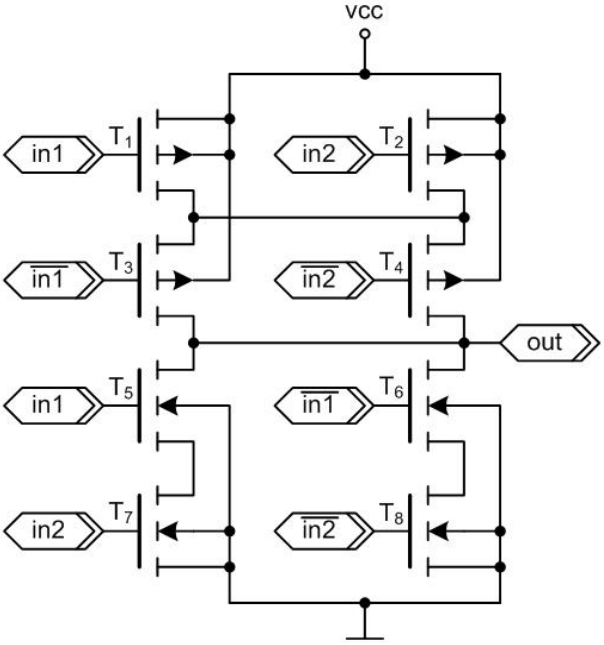

Fig. 6. XOR-Gate in AOI realization [14]

Although the other realisations might be more effective, it is estimated that the lower performance should not affect the decision if one cryptographic scheme is practicable or not, because the presented results of chapter 2 are absolute maximum ratings and there should always be a margin to ensure reliable functionality. An XOR gate with two inputs has four different states, each with three possible transitions. The results of those single simulations are shown in the following tables. For presentation purposes we change the notation and write A1 if input ″in1″ is logic high or B0 for ″in2″ at low level. A0 and B1 are built respectively.

Technology	A0,B0 → A0,B1 [fWs]	A0,B1 → A0,B0 [fWs]	A0,B0 → A1,B0 [fWs]	A1,B0 → A0,B0 [fWs]	A0,B0 → A1,B1 [fWs]	A1,B1 → A0,B0 [fWs]
0.35 µm	158.7	160.92	73.46	70.76	52.26	32.50
0.25 µm	128.82	129.06	60.56	54.28	39.48	22.12
0.18 µm	38,34	61.02	18.5	13.8	10.1	4.78

Technology	A0,B1 → A1,B0 [fWs]	A1,B0 → A0,B1 [fWs]	A0,B1 → A1,B1 [fWs]	A1,B1 → A0,B1 [fWs]	A1,B0 → A1,B1 [fWs]	A1,B1 → A1,B0 [fWs]	Mittel [fWs]
0.35 µm	37.74	31.44	73.66	70.76	157.94	160.18	90.03
0.25 µm	26.92	21.02	61.10	54.86	128.72	129.06	71.34
0.18 µm	7.02	9.08	18.32	13.54	37.84	35.94	22.52

Table 2. CMOS AOI XOR energy consumption

NAND

In order to find an approximation for the power consumption of a certain algorithm, the NAND gate has a special relevance. In the development of highly integrated circuits, there are often used ″ready made″ VHDL cores. The complexity of these logic components are mainly given by a certain number of gates. A gate in this context is equivalent to one NAND.

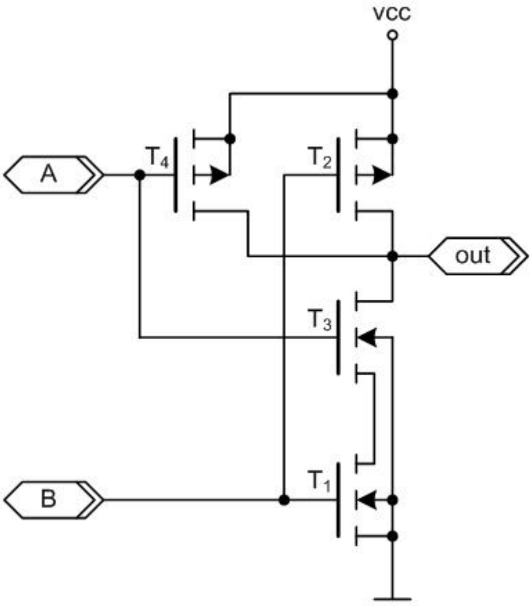

Fig. 7. CMOS NAND [14]

An ideal NAND-gate only needs power if its output changes the logic level. Although we do not deal with ideal transistors, other static losses can be neglected.

Technology	A0,B0 → A1,B1 [fWs]	A1,B0 → A1,B1 [fWs]	A0,B1 → A1,B1 [fWs]	A1,B1 → A0,B0 [fWs]	A1,B1 → A1,B0 [fWs]	A1,B1 → A0,B1 [fWs]	Mittel [fWs]
0.35 µm	15.28	20.78	22.11	65.98	78.03	53.21	42.57
0.25 µm	5.71	8.96	9.87	49.85	57.95	40.9	28.87
0.18 µm	0.02	1.48	1.64	15.54	16.89	12.85	8.07

Table 3. CMOS NAND energy consumption

4 Cryptographic Implementations

Since we have not implemented cryptographic algorithms so far, we present some commercial implementations of arithmetic operations and cryptographic schemes. This allows us to obtain the margins of the needed resources. Those implementations are available in IP (Intellectual Property) –cores which are ready made models, written in VHDL (Very High Speed Integrated Circuit Hardware Description Language). The modules can be integrated in most development environments for designing ASICs (Application Specific Integrated Circuit), FPGAs (Field Programmable Gate Arrays) or other hardware [12][13].

Arithmetic Operation	Number of gates
32 bit Add/Subtract Unit	4488
32 bit Multiply Unit	12155
32 bit Divide Unit	30294
32 bit Compare Unit	514
64 bit Add/Subtract Unit	9069
64 bit Multiply Unit	38568
64 bit Compare Unit	1028

Cryptographic scheme	Number of gates
DES	3000
3DES	5500
AES encryption	38000
AES decryption	50000
RSA 1024 bit	34000
ECC 163 bit	3260

Table 4. Cost of basic arithmetic and cryptographic operations

5 Analysis of RFID Cryptography

In order to determine if and which type of cryptographic algorithm can be implemented in RFID tags, this paper takes an approach which implies that the only limiting factor is the straitened power transfer between an RFID reader and the tag. Since the specific implementations were not analysed in detail, the resulting assumptions had to be done from a more “global” point of view. As an indication for the complexity of the desired algorithm, the parameters given in chapter 4 were used. The complexities are given as a certain number of gates because they are basic building blocks in an FPGA design.

The knowledge about available power at a certain distance was obtained in chapter two. Together with the amount of energy needed for switching one NAND gate and the desired clock rate, it is possible to estimate if selected cryptography is possible or not.

For example, if the target application has to operate at a distance of 1 meter, the available power P(d) is 1.2651 mW. If the logic is clocked with 6.78 MHz (half rate of the reader’s frequency)

$$E_{clock} = \frac{P(d)}{f_{clock}} \tag{7}$$

the available energy per clock cycle is 186.59 pWs like derived from formula 7. This energy is divided by the consumption of a singe 0.35µm NAND gate.

$$N_{gates} = \frac{E_{clock}}{E_{NAND}} \tag{8}$$

It is therefore enough energy for operating 4383 gates in 0.35µm CMOS technology and should be sufficient for implementing elliptic curve cryptography.

In this calculation, we assume that the whole circuitry is operating the whole time. This might be imprecise but will at least compensate some of the best case assumptions made in chapter 2.

6 Conclusion

The amount of power which is available for a tag at a certain distance was given in chapter two. Together with the results of chapter three it was therefore possible to estimate the maximum number of NAND gates that can be driven at a certain clock rate. This value was compared with the complexity of a cryptographic algorithm.

The authors are aware of the fact that tags cannot be designed under the assumption that the position of tag and reader are in such optimum positions like it is done in chapter 2 but it was shown that strong asymmetric should even be possible with a relative coarse semiconductor process of 0.35µm. Furthermore, an RFID specific implementation will probably not only use NAND based circuits when it is possible to perform the specific operation with a custom made design. We therefore also simulated basic building blocks like a shift-register and XOR gates like they are uses in praxis. The actual algorithms should be deeply analysed in further studies in order to obtain better knowledge about their actual hardware utilisation. Unfortunately, we had no further information on the algorithms i.e. how many clock cycles they need for execution or if they already contain the amount of RAM they need. Another fact is that the available power cannot be exclusively used by the cryptographic engine. RFID Tags have to contain other circuitries which handle radio access (anti-collision) and other functions. There are two other important facts that should also be mentioned. It is theoretically possible to obtain as much energy as needed, as long as the tag stays in the supplying magnetic field of the reader. The problem is that it is not possible or payable to store noteworthy amounts of energy in the tag. The second factor is the speed in which the algorithm has to run. If it is possible for the application and the user to wait longer for the tag's response, the clock rate can be reduced and the number of possible gates increases by the same factor.

Anyway, the semiconductor technology is still under rapid development. The authors predict that the capabilities of RFID tags will increase in the same way. If the market for RFID providing public key cryptography is big enough it should be possible to fill the mentioned security gap between AutoID tags and Smartcards.

References

[1] S. E. Sarma, S. A. Weis, D. W. Engels. *RFID Systems and Security and Privacy Implications*. Cryptographic Hardware and Embedded Systems - CHES, August 2002.

[2] K. Fong. *RFID Security*, http://www.cs.siu.edu/~kfong/research/RFID.ppt

[3] MIT Auto-ID Center. http://www.autoidcenter.org

[4] CASPIAN. http://www.nocards.org

[5] Auto-id Center. *Draft protocol specification for a 900 MHz class 0 Radio Frequency Identification Tag*, 23 Feb 2003.

[6] Infineon technologies. *SLE 66CLX641P Short Product Information*, April 2004.

[7] K. Finkenzeller. *RFID-Handbuch*, Hanser Verlag 2002.

[8] ISO/IEC 14443. *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface*, July 2001.

[9] G. Lehner, G. *Elektomagnetische Feldtheorie für Ingenieure und Physiker*, Springer Verlag, 1990

[10] W.R. Smythe. *Static and Dynamic Electricity, McGraw-Hill Book Company*, 1968

[11] MOSIS, www.mosis.org

[12] ASICSws, www.asics.ws

[13] J. Krasner. *Using Elliptic Curve Cryptography (ECC) for Enhanced Embedded Security*, November 2004.

[14] R. J. Baker, H. W. Li, D. E. Boyce. *CMOS Circuit Design, Layout, And Simulation.* IEEE Press 1998.

[16] MATLAB. http://www.mathworks.com

[17] WinSpice. http://www.winspice.com