New Lightweight DES Variants

Gregor Leander, Christof Paar, Axel Poschmann, and Kai Schramm

Horst Görtz Institute for IT Security
Communication Security Group (COSY)
Ruhr-University Bochum, Germany
{cpaar,poschmann,schramm}@crypto.rub.de,
leander@rub.de

Abstract. In this paper we propose a new block cipher, DESL (DES Lightweight), which is based on the classical DES (Data Encryption Standard) design, but unlike DES it uses a single S-box repeated eight times.[1] On this account we adapt well-known DES S-box design criteria, such that they can be applied to the special case of a single S-box. Furthermore, we show that DESL is resistant against certain types of the most common attacks, i.e., linear and differential cryptanalyses, and the Davies-Murphy attack. Our hardware implementation results of DESL are very promising (1848 GE), therefore DESL is well suited for ultra-constrained devices such as RFID tags.

Keywords: RFID, DES, DESL, lightweight cryptography, S-box design criteria.

1 Introduction

A flawless and remote identification of products, people or animals plays an important role in many areas of daily life. For example, farmers often have to keep track of the fertility rate of their cattle and hence, identify calf-bearing cows. Other examples are the permanent identification of industrial goods, which improves the supply chain in factories and countersteers thievery, or the need of reliable access control devices, e.g. in form of ski passes or train tickets.

An automatic identification can be achieved with RFID (Radio Frequency Identification) tags. Basically, RFID tags consist of a transponder and an antenna and are able to remotely receive data from an RFID host or reader device. In general, RFID tags can be divided into passive and active devices: active tags provide their own power supply (i.e. in form of a battery), whereas passive tags solely rely on the energy of the carrier signal transmitted by the reader device. As a result, passive RFID devices are not only much less expensive, but also require less chip size and have a longer life cycle [Fin03]. Our proposed DESL algorithm and its low-power, size-optimized implementation aims at very constrained devices such as passive RFID tags.

[1] Part of this work has already been presented at RFIDSec '06, a non-proceeding workshop.

A. Biryukov (Ed.): FSE 2007, LNCS 4593, pp. 196–210, 2007.

Very often it is desired to use RFID tags as cryptographic tokens, e.g. in a challenge response protocol. In this case the tag must be able to execute a secure cryptographic primitive. Contactless microprocessor cards [RE02], which are capable to execute cryptographic algorithms, are not only expensive and, hence, not necessarily suited for mass production, but also draw a lot of current. The high, non-optimal power consumption of a microprocessor can usually only be provided by close coupling systems, i.e. a short distance between reader and RFID device has to be ensured [Fin03]. A better approach is to use a custom made RFID chip, which consists of a receiver circuit, a control unit[2], some kind of volatile and/or non-volatile memory and a cryptographic primitive. In [FWR05], Feldhofer et al. propose a very small AES implementation with 3400 gates, which draws a maximum current of $3.0\mu A$ @ $100kHz$. Their AES design is based on a byte-per-byte serialization, which only requires the implementation of a single S-box [DR02] and achieves an encryption within 1032 clock cycles ($= 10.32ms$ @ $100kHz$). Unfortunately, the ISO/IEC 18000 standard requires that the latency of a response of an RFID tag does not exceed $320\mu s$, which is why Feldhofer et al. propose a slightly modified challenge-response protocol based on interleaving.

The remainder of this work is organized as follows: In Section 2 we stress why DES was chosen as the basis for our new family of lightweight algorithms, which we present in Section 3. Subsequently, in Section 4 we show the design criteria for DESL and its lightweight implementation in Section 5. Finally, in Section 6 we summarize our results and conclude this work.

2 Design Considerations for Lightweight Block Ciphers

The pretext of our algorithm family is the desire to find a design for a cipher for extremely lightweight applications such as passive RFIDs. Thus far, there have been two approaches for providing cryptographic primitives for such situations: 1) Optimized low-cost implementations for standardized and trusted algorithms, which means in practice in essence block ciphers such as AES, see e.g., [FDW04]. And 2) design new ciphers with the goal of having low hardware implementation costs (see, e.g., the profile 2 algorithms of the eStream project). Even though both approaches are valid and yielding results, we believe both are not optimum. The problem with the first approach is that most modern block ciphers were primarily designed with good software implementation properties in mind, and not necessarily with hardware-friendly properties. We strongly believe that this was the right approach for today's block ciphers since on the one hand the vast majority of algorithms run in software on PCs or embedded devices, and on the other hand silicon area has become so inexpensive that very high performance hardware implementations (achieved through large chip area) are not a problem any more. However, if the goal is to provide extremely low-cost security on devices where both of those assumptions do not hold, one has to wonder whether modern block ciphers are the best solution.

[2] i.e. a finite state machine.

There are also problems with the second approach, designing low cost ciphers anew. First it is well known that it is painfully difficult to design new ciphers without security flaws. Furthermore, as can be seen from the eStream profile 2 algorithms (which have low-cost hardware properties as a main objective), it is far from straightforward to design a new cipher which has a lower hardware complexity than standard DES.

It is fair to claim that an optimum approach would be to have a well investigated cipher, the design of which was driven by low hardware costs. The only known cipher to this respect is the Data Encryption Standard, DES. (The obvious drawback of DES is that its key length is not adequate for many of today's applications, but this will be addressed in Section 3 below.) The promise that DES holds for lightweight hardware implementation can easily be seen by the following observation. If we compare a standard, one-round implementation[3] of AES and DES, the latter consumes about 6% (!) of the logic resources of AES, while having a shorter critical path [VHVM88], [ASM01]. Of course, DES uses a much shorter key so that a direct comparison is not completely accurate, but the time-area advantage of more than one order of magnitude gives an indication. We would also like to stress that it is not a coincidence that DES is so efficient in hardware. DES was designed in the first half of the 1970s and the targeted implementation platform was hardware. However, by today's standard, digital technology was extremely limited in the early 1970s. Hence, virtually all components of DES were heavily driven by low hardware complexity: bit permutation and small S-Boxes.

3 DESL and DESXL: Design Ideas and Security Consideration

The main design ideas of the new cipher family, which are either original DES efficiently implemented or a variant of DES, are:

1. Use of a serial hardware architecture which reduces the gate complexity.
2. Optionally apply key-whitening in order to render brute-force attacks impossible.
3. Optionally replace the 8 original S-Boxes by a single one which further reduces the gate complexity.

If we make use of the first idea, we obtain a lightweight implementation of the original DES algorithm which consumes about 35% less gates than the best known AES implementation [FWR05]. To our knowledge, this is the smallest reported DES implementation, trading area for throughput. The implementation requires also about 86% fewer clock cycles for encrypting of one block than the serialized AES implementation in [FWR05](1032 cycles vs. 144) which makes it easier to use in standardized RFID protocols. However, the security provided is limited by the 56 bit key. Brute forcing this key space takes a few months

[3] i.e. one plaintext block is encrypted in one clock cycle.

and hundreds of PCs in software, and only a few days with a special-purpose machine such as COPACOBANA [KPP+06]. Hence, this implementation is only relevant for application where short-term security is needed, or where the values protected are relatively low. However, we can imagine that in certain low cost applications such a security level is adequate.

In situation where a higher security level is needed key whitening, which we define here as follows:

$$DESX_{k.k1.k2}(x) = k2 \oplus DES_k(k1 \oplus x)$$

can be added to standard DES, yielding DESX. The bank of XOR gates and registers increase the gate count by about 14%[4]. The best known key search attack uses a time-memory trade-off and requires 2^{120} time steps and 2^{64} memory locations, which renders this attack entirely out of reach. The best known mathematical attack is linear cryptanalysis [Mat94]. Linear cryptanalysis requires about 2^{43} chosen ciphertext blocks together with the corresponding plaintexts. At a clock speed of 500 kHz, our DESX implementation will take more than 80 years, so that analytical attacks do not pose a realistic threat. Please note that parallelization is only an option if devices with identical keys are available.

In situations where extremely lightweight cryptography is needed, we can further decrease the gate complexity of DES by replacing the eight original S-Boxes by a single new one. This lightweight variant of DES is named DESL and has a brute-force resistance of 2^{56}. In order to strengthen the cipher, key whitening can be applied yielding the cipher DESXL. The crucial question is what the strength of DESL and DESXL is with respect to analytical attacks. We are fully aware that any changes to a cipher might open the door to new attacks, even if the changes have been done very carefully and checked against known attacks. Hence, we believe that DESL (or DESXL) should primarily not be viewed as competitors to AES, but should be used in applications where established algorithms are too costly. In such applications which have to trade security (really: trust in an algorithm) for cost, we argue that it is a cryptographically sounder approach to modestly modify a well studied cipher (in fact, the world's best studied crypto algorithm), rather than designing a new algorithm altogether.

4 Design Criteria of DESL

In this section we describe how a variant of DES with a single S-box can be made resistant against the differential, linear, and Davis-Murphy attack. The work is based on the original design criteria for DES as published by Coppersmith [Cop94] and the work of Kim et al. [KPL93], [KLPL94], [KLPL95] where several criteria for DES type S-boxes are presented to strengthen the resistance against the above mentioned attacks.

Coppersmith states the following eight criteria as the "only cryptographically relevant" ones for the DES S-boxes (see [Cop94]).

[4] This number only includes additional XOR gates, because we assume that all keys have to be stored at different memory locations anyway.

(S-1) Each S-box has six bits of input and four bits of output.
(S-2) No output bit of an S-box should be too close to a linear function of the input bits.
(S-3) If we fix the leftmost and rightmost input bits of the S-box and vary the four middle bits, each possible 4-bit output is attained exactly once as the middle input bits range over their 16 possibilities.
(S-4) If two inputs to an S-box differ in exactly one bit, the outputs must differ in at least two bits.
(S-5) If two inputs to an S-box differ in the two middle bits exactly, the outputs must differ in at least two bits.
(S-6) If two inputs to an S-box differ in their first two bits and are identical in their last two bits, the two outputs must not be the same.
(S-7) For any nonzero 6-bit-difference between inputs, ΔI, no more than eight of the 32 pairs of inputs exhibiting ΔI may result in the same output difference ΔO.
(S-8) Minimize the probability that a non zero input difference to three adjacent S-boxes yield a zero output difference.

4.1 Improved Resistance Against Differential Cryptanalysis and Davis Murphy Attack

The criteria (S-1) to (S-7) refer to one single S-box. The only criterion which deals with the combination of S-boxes is criterion (S-8). The designers' goal was to minimize the probability of collisions at the output of the S-boxes and thus at the output of the *f-function*. As a matter of fact, it is only possible to cause a collision, i.e. two different inputs are mapped to the same output, in three adjacent S-boxes, but not in a single S-box or a pair of S-boxes due to the diffusion caused by the expansion permutation. The possibility to have a collision in three adjacent S-boxes leads to the most successful differential attack based on a 2-round iterative characteristic with probability $\frac{1}{234}$.

Clearly better than minimizing the probability for collisions in three or more adjacent S-boxes, is to eliminate them. This was the approach used in [KPL93], [KLPL94], [KLPL95] and can easily be reached by improving one of the design criteria.

We replace (S-6) and (S-8) by an improved design criterion similar to the one given in [KPL93].

Condition 1. *If two inputs to an S-box differ in their first bit and are identical in their last two bits, the two outputs must not be the same.*

This criterion ensures that differential attacks using 2-round iterative characteristics, as the one presented by Biham and Shamir in [BS92], will have all eight S-boxes active and therefore will not be more efficient than exhaustive search anymore.

Moreover, the only criterion that refers to more than one S-box, i.e. (S-8), is now replaced by a condition that refers to one S-box, only. Thus, most of the security analysis remains unchanged when we replace the eight different S-boxes by one S-box repeated eight times.

Note that as described by Biham in [BB97] and by Kim et at. in [KLPL95] this condition also ensures resistance against the Davis Murphy attack [DM95].

4.2 Improved Resistance Against Linear Cryptanalysis

To improve the resistance of our variant of DES with only one S-Box against linear cryptanalysis (LC) is more complex than the protection against the differential cryptanalysis. Kim et.al presented a number of conditions that, when fulfilled by a set of S-boxes, ensure the resistance of DES variants against LC. However several of these conditions focus on different S-boxes and this implies that if one wants to replace all eight S-boxes by just one S-box, there are very tight restrictions to the choice of the S-box. This one S-box has to fulfill *all* conditions given in [KLPL95] referring to *any* S-box.

Let $S_b = \langle b, S(x) \rangle$ denote a combination of output bits that is determined by $b \in \mathrm{GF}(2)^4$. Then, the *Walsh-coefficient* $S_b^{\mathcal{W}}(a)$ for an element $a \in \mathrm{GF}(2)^6$ is defined by

$$S_b^{\mathcal{W}}(a) = \sum_{x \in \mathrm{GF}(2)^6} (-1)^{\langle b, S(x) \rangle + \langle a, x \rangle}. \tag{1}$$

The probability of a linear approximation of a combination of output bits S_b by a linear combination a of input bits can be written as

$$p = \frac{\#\{x | S_b(x) = \langle a, x \rangle\}}{2^6}. \tag{2}$$

Combining equations 1 and 2 leads to

$$p = \frac{S_b^{\mathcal{W}}(a)}{2^7} + \frac{1}{2}.$$

The *linear probability bias* ε is a correlation measure for this deviation from probability $\frac{1}{2}$ for which it is entirely uncorrelated. We have

$$\varepsilon = \left| p - \frac{1}{2} \right| = \left| \frac{S_b^{\mathcal{W}}(a)}{2^7} \right|.$$

Let us denote the maximum absolute value of the Walsh-Transformation by $S_{max}^{\mathcal{W}}$. Then clearly

$$\varepsilon \leq \left| \frac{S_{max}^{\mathcal{W}}(a)}{2^7} \right|$$

The smaller the linear probability bias ε is, the more secure the S-box is against linear cryptanalysis. We defined our criterion (S-2") by setting the threshold for $S_{max}^{\mathcal{W}}$ to 28.

Condition 2. $|S_b^{\mathcal{W}}(a)| \leq 28$ *for all* $a \in \mathrm{GF}(2)^6,\ b \in \mathrm{GF}(2)^4$.

Note that this is a tightened version of Condition 2 given in [KLPL95] where the threshold was set to 32. In the original DES the best linear approximation has a maximum absolute Walsh coefficient of 40 for S-box S5.

If an LC attack is based on an approximation that involves n S-boxes, under the standard assumption that the round keys are statistically independent, the overall bias ε is (see [Mat94])

$$\varepsilon = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i$$

where the values ε_i are the biases for each of the involved S-box.

A rough approximation of the effort of a linear attack based on a linear approximation with bias ε is ε^{-2}, thus if we require that such an attack is no more efficient than exhaustive search we need $\varepsilon < 2^{-28}$.

It can be easily seen that any linear approximation for 15 round DES involves at least 7 approximations for S-boxes. But as

$$2^6 \prod_{i=1}^{7} \varepsilon_i \leq 2^6 \prod_{i=1}^{7} \frac{7}{32} \approx 2^{-9.35}$$

this bound is clearly insufficient.

Thus in order to prove the resistance against linear attack, we have to make sure that either enough S-boxes are active, i.e. enough S-Boxes are involved in the linear approximation, or, if fewer S-boxes are active, the bound on the probabilities can be tightened. In the first case we need more than 23 active S-boxes as

$$2^{21} \left(\frac{S^{\mathcal{W}}_{max}}{128} \right)^{22} > 2^{-28} > 2^{22} \left(\frac{S^{\mathcal{W}}_{max}}{128} \right)^{23} \tag{3}$$

For the second case several conditions have been developed in [KLPL94], [KLPL95]. Due to our special constraints we have to slightly modify these conditions. Following [KLPL95] we discuss several cases of iterative linear approximations. We denote a linear approximation of the F function of DES by

$$\langle I, Z_1 \rangle + \langle K, Z_3 \rangle = \langle O, Z_2 \rangle$$

where $Z_1, Z_2, Z_3 \in \mathrm{GF}(2)^{32}$ specify the input, output and key bits used in the linear approximation.

An n round iterative linear approximation is of the form

$$\langle I_1, \cdot \rangle + \langle I_n, \cdot \rangle = \langle K_2, \cdot \rangle + \cdots + \langle K_{n-1}, \cdot \rangle$$

and consists of linear approximations for the rounds 2 until $n-1$.

Similar as it was done in [KLPL94] it can be shown that a three round (3R) iterative linear approximation is not possible with a non zero bias, due to condition 1.

We therefore focus on the case of a 4 and 5 round iterative approximation only.

4.3 4R Iterative Linear Approximation

A four round iterative linear approximation consists of two linear approximations for the F function of the second and third round. We denote these approximations as

$$A : \langle I_2, Z_1\rangle + \langle K_2, Z_3\rangle = \langle O_2, Z_2\rangle$$
$$B : \langle I_3, Y_1\rangle + \langle K_3, Y_3\rangle = \langle O_3, Y_2\rangle$$

In order to get a linear approximation of the form

$$\langle I_1, \cdot\rangle + \langle I_4, \cdot\rangle = \langle K_2, \cdot\rangle + \langle K_3, \cdot\rangle$$

Using $O_2 = I_1 + I_3$ and $O_3 = I_2 + I_4$ it must hold that

$$Z_2 = Y_1 \text{ and } Z_1 = Y_2$$

The 15 round approximation is

$$-AB - BA - AB - BA - AB$$

If the number of S-boxes involved in the approximation of A is a and for B is b we denote by $\mathcal{A} = (a, b)$. First assume that $\mathcal{A} = (1, 1)$. Due to $Z_2 = Y_1$ and the property of the P-permutation, which distributes the output bits of one S-box to 6 different S-Boxes in the next round, it must hold that $|Y_1| = |Z_2| = 1$. For the same reason we get $|Z_1| = |Y_2| = 1$. To minimize the probability of such an approximation we stipulate the following condition

Condition 3. *The S-box has to fulfill* $S_b^{\mathcal{W}}(a) \leq 4$ *for all* $a \in \mathrm{GF}(2)^6, b \in \mathrm{GF}(2)^4$ *with* $\mathrm{wt}(a) = \mathrm{wt}(b) = 1$.

This condition is comparable to Condition 4 in [KLPL95], however, as we only have a single S-box, we could not find a single S-box fulfilling all the restrictions from condition 4 in [KLPL95]. If the S-box fulfils condition 3 the overall bias for the linear approximation described above is bounded by

$$\varepsilon \leq 2^9 \left(\frac{4}{128}\right)^{10} < 2^{-40}.$$

As this is (much) smaller than 2^{-28} this does not yield to a useful approximation.

Assume now that $\mathcal{A} = (1, 2)$ (the case $\mathcal{A} = (2, 1)$ is very similar). If B involves two S-boxes we have $|Y_1| = |Y_2| = 2$ and thus $|Y_2| = |Z_1| = 2$. In particular for both S-boxes involved in B Condition 3 applies which results in a threshold

$$\varepsilon \leq 2^{14} \left(\frac{4}{128}\right)^{10} \left(\frac{28}{128}\right)^{5} < 2^{-46}$$

for the overall linear bias.

Next we assume that $\mathcal{A} = (2, 2)$. In this case we get (through the properties of the P function) that each S-box involved in A and B has at most two input and output bits involved in the linear approximation. In order to avoid this kind of approximation we add another condition.

Condition 4. *The S-box has to fulfill* $S_b^{\mathcal{W}}(a) \leq 16$ *for all* $a \in \mathrm{GF}(2)^6, b \in \mathrm{GF}(2)^4$ *with* $\mathrm{wt}(a), \mathrm{wt}(b) \leq 2$.

This condition is a tightened version of Condition 5 in [KLPL95] where the threshold was set to 20 . In this case (remember that we now have 20 S-boxes involved) we get

$$\varepsilon \leq 2^{19} \left(\frac{16}{128}\right)^{20} < 2^{-40}.$$

In all other cases, more than 23 S-boxes involved and thus the general upper bound (3) can be applied.

4.4 5R Iterative Linear Approximation

A five round iterative linear approximation consists of three linear approximations for the F function of the second, third and fourth round. We denote these approximations as

$$\begin{aligned} A &: \langle I_2, Z_1\rangle + \langle K_2, Z_3\rangle = \langle O_2, Z_2\rangle \\ B &: \langle I_3, Y_1\rangle + \langle K_3, Y_3\rangle = \langle O_3, Y_2\rangle \\ C &: \langle I_4, X_1\rangle + \langle K_4, X_3\rangle = \langle O_4, X_2\rangle. \end{aligned}$$

In order to get a linear approximation of the form

$$\langle I_1, \cdot\rangle + \langle I_5, \cdot\rangle = \langle K_2, \cdot\rangle + \langle K_3, \cdot\rangle + \langle K_4, \cdot\rangle$$

it must hold that

$$Z_1 = Y_2 = X_1 \text{ and } Y_1 + Z_2 + X_2 = 0$$

The 15 round approximation is

$$-ABC - CBA - ABC - DE$$

for some linear approximations D and E each involving at least one S-box. Clearly, as the inputs of A and C are the same we have $\mathcal{A} = (a, b, a)$, i.e. the number of involved S-boxes in A and C are the same.

Case $b = 1$: Assume that $b = 1$, i.e. only one S-box is involved in the linear approximation B. If $|Z_1| \geq 3$ than we must have $a \geq 3$ and so the number of S-boxes involved is at least 23, which makes the approximation useless. If $|Z_1| = 2$ we have two active S-boxes for A and B. Moreover as $b = 1$ we must have $|Y_1| = |Z_2 + X_2| = 1$. Due to properties of the P function, the S-boxes involved in A and B are never adjacent S-boxes, therefore exactly one input bit is involved in the approximation for each of the two S-boxes. In order to minimize the probability for such an approximation, we stipulate the following condition

Condition 5. *The S-box has to fulfill*

$$|S^{\mathcal{W}}_{b_1}(a) S^{\mathcal{W}}_{b_2}(a)| \leq 240$$

for all $a \in \mathrm{GF}(2)^6, b_1, b_2 \in \mathrm{GF}(2)^4$ *with* $\mathrm{wt}(a) = 1, \mathrm{wt}(b_1 + b_2) = 1.$

This is a modified version of Condition 7 in [KLPL95]. With an S-box fulfilling this condition we derive an upper bound for the overall bias

$$\varepsilon \leq 2^{16} \left(\frac{240}{128^2}\right)^6 \left(\frac{16}{128}\right)^3 \left(\frac{28}{128}\right)^2 < 2^{-33}$$

If $|Z_1| = 1$ then $a = 1$ and we have $|Y_1| = |Z_2 + X_2| = 1$ and $|Z_1| = 1$. We stipulate one more condition.

Condition 6. *The S-box has to fulfill*

$$S_b^{\mathcal{W}}(a) = 0$$

for $a \in \{(010000), (000010)\}, b \in \mathrm{GF}(2)^4$ *with* $\mathrm{wt}(b) = 1$.

This implies that the input to B is such that a middle bit is affected. Due to the properties of the P function this implies that in the input of A and C a non-middle bit is affected. As for any DES type S-box it holds that $S_b^{\mathcal{W}}(100000) = S_b^{\mathcal{W}}(000001) = 0$ for all b the only possible input values for the S-box involved in A and C are (010000) and (000010). To avoid the second one we define the next condition.

Condition 7

$$|S_{b_1}^{\mathcal{W}}(000010) S_{b_2}^{\mathcal{W}}(000010)| = 0$$

for all $b_1, b_2 \in \mathrm{GF}(2)^4$ *with* $\mathrm{wt}(b_1 + b_2) = 1$.

The other possible input value, i.e. 01000 occurs only when S-box 1 is active in B and S-box 5 is active in A and C. In this case the input values for the S-box in B is (000100) and the output value is (0100). The next condition makes this approximation impossible.

Condition 8. *The S-box has to fulfill*

$$S_{(0100)}^{\mathcal{W}}(000100) = 0$$

Case $b = 2$: Assume that $b = 2$, i.e. exactly two S-boxes are involved for B. If $a > 2$ then at least 23 S-boxes are involved in total. If $a = 2$ we have for each S-box involved in B at most 2 input bits and at most 2 output bits. Therefore we can apply the bound from condition 4 to the two S-boxes from B. Applying the general bound for all the other S-boxes we get

$$\varepsilon \leq 2^{19} \left(\frac{16}{128}\right)^6 \left(\frac{28}{128}\right)^{14} < 2^{-29}.$$

In the case where $a = 1$ the two S-boxes involved in B have one input and one output bit involved each, thus we can apply the strong bound from condition 3 for these S-boxes (6 in total) and the general bound for the other S-boxes to get

$$\varepsilon \leq 2^{13} \left(\frac{4}{128}\right)^6 \left(\frac{28}{128}\right)^8 < 2^{-34}.$$

Case $b > 2$*:* In this case we must have $a, b \geq 2$ and thus at least 29 S-boxes are involved in total.

4.5 nR Iterative Linear Approximation

For an n round iterative linear approximation with only one S-box involved in each round (denoted as Type-I by Matsui) our condition 3 ensures that if more than 7 S-boxes are involved in total the approximation will not be useful for an attack as

$$\varepsilon \leq 2^6 \left(\frac{4}{128}\right)^7 = 2^{-29} \tag{4}$$

4.6 Resistance Against Algebraic Attacks

There is no structural reason why algebraic attacks should pose a greater threat to DESL than to DES. The DESL S-box has been randomly generated in the set of all S-boxes fulfilling the design criteria described above. Therefore we do not expect any special weakness of the chosen S-box. Indeed we computed the number of low degree equations between the input and output bits of the S-box. There exist one quadratic equation and 88 equations of degree 3. Note that for each 6 to 4 Bit S-box, there exist at least 88 equations of degree 3. Given the comparison with the corresponding results for the original DES S-boxes in Table 1 we anticipate that DESL is as secure as DES with respect to algebraic attacks.

Table 1. Number of Degree two and Degree three Equations

DES S-box	S1	S2	S3	S4	S5	S6	S7	S8	DESL
# deg 2	1	0	0	5	1	0	0	0	1
# deg 3	88	88	88	88	88	88	88	88	88

4.7 Improved S-Box

We randomly generated S-boxes, which fulfill the original DES criteria (S-1), (S-3), (S-4), (S-5), (S-7), the condition 1 and our modified conditions 2 to 8. Our goal was to find one single S-box, which is significantly more resistant against differential and linear cryptanalyses than the original eight S-boxes of DES. In our DESL algorithm this S-box is repeated eight times and replaces all eight S-boxes in DES.

5 Lightweight Implementation of DESL

We implemented DES in the hardware description language VHDL, where we sacrificed time for area wherever possible. In this serialized DES ASIC design, registers take up the main part of chip size (33.78%), followed by the S-boxes (32.11%), and multiplexors (31.19%). Chip size of registers and multiplexors can

Table 2. Improved DESL S-box

S															
14	5	7	2	11	8	1	15	0	10	9	4	6	13	12	3
5	0	8	15	14	3	2	12	11	7	6	9	13	4	1	10
4	9	2	14	8	7	13	0	10	12	15	1	5	11	3	6
9	6	15	5	3	8	4	11	7	1	12	2	0	14	10	13

not be minimized any further, hence we thought about further possibilities to optimize the chip size of the S-boxes.

While it does not seem to be possible to find better logic minimizations of the original DES S-boxes, there have been other approaches to alter the S-boxes, e.g. key-dependent S-boxes [BB94], [BS92] or the so-called s^i*DES* [KLPL94], [KLPL95], [KPL93]. While all these approaches, despite the fact that some of them have worse cryptographic properties than DES [Knu92], just change the content and not the **number** of S-boxes. To the best of our knowledge, no DES variant has been proposed in the past which uses a single S-box, repeated eight times.

The main difference between DESL and DES lies in the f-function. We substituted the eight original DES S-boxes by a single but cryptographically stronger S-box (see Table 2), which is repeated eight times. Furthermore, we omitted the initial permutation (IP) and its inverse (IP^{-1}), because they do not provide additional cryptographic strength, but at the same time require area for wiring. The design of our DESL algorithm is exactly the same as for the DES algorithm, except for the (IP) and (IP^{-1}) wiring and the *sbox* module.

We used Synopsys Design Vision V-2004.06-SP2 to map our DESL design to the Artisan UMC 0.18μm L180 Process 1.8-Volt Sage-X Standard Cell Library and Cadence Silicon Ensemble 5.4 for the Placement & Routing-step. Synopsys NanoSim was used to simulate the power consumption of the back-annotated verilog netlist of the ASIC.

Our serialized DESL ASIC implementation has an area requirement of 1848 GE (gate equivalences) and it takes 144 clock cycles to encrypt one 64-bit block of plaintext. For one encryption at 100 kHz the average current consumption is 0.89 μA and the throughput reaches 5.55 KB/s. For further details on the implementational aspects of our DES and DESL architecture we refer to [PLSP07].

6 Results and Conclusion

In Section 2 we stated eight conditions which a single S-box has to fulfill in order to be resistant against certain types of linear and differential cryptanalyses, and the Davies-Murphy attack. We presented a strengthened S-box, which is used in the single S-box DES variants DESL and DESXL. Furthermore, we showed, that a differential cryptanalysis with characteristics similar to the characteristics used by Biham and Shamir in [BS91] is not feasible anymore. We also showed, that

DESL is more resistant against the most promising types of linear cryptanalysis than DES due to the improved non-linearity of the S-box.

Table 3 shows, that our DESL cipher needs 20% less gate equivalences and uses 25% less average current than our DES implementation. In comparison with the AES design presented by Feldhofer et al. [FWR05], our design needs 45% less gate equivalents and 86% less clock cycles. Note that the AES design by Feldhofer et al. was implemented in a $0.35\mu m$ standard cell technology, whereas our design was implemented in a $0.18\mu m$ standard cell technology. Therefore a fair comparison is only possible with regard to the gate equivalences. Regarding area consumption, our DESL is competitive even to stream ciphers recently proposed within the eSTREAM project [GB07]. More interesting, DESL would be the second smallest stream cipher in terms of gate count compared to all eSTREAM candidates (see Table 3). Due to the low current consumption and the small chip size required for our DESL design, it is especially suited for resource limited applications, for example RFID tags and wireless sensor nodes.

Table 3. Comparison of Efficient Ciphers based on Gate Count, Clock Cycles, and Current Consumption

	gate equiv.		cycles /	μA at	Process
	total	rel.	block	100 kHz	μm
DESL	**1848**	**1**	**144**	**0.89**	0.18
DES	2309	1.25	144	1.19	0.18
DESX	2629	1.42	144	–	0.18
DESXL	2168	1.17	144	–	0.18
AES-128 [FWR05]	3400	1.84	1032	3.0	0.35
HIGHT [HSH+06]	3048	1.65	1	–	0.25
Trivium [GB07]	2599	1.41	–	–	0.13
Grain-80 [GB07]	1294	0.70	–	–	0.13

Finally, we can conclude, that DESL is more secure against certain types of linear and differential Cryptanalyses and the Davies-Murphy attack, more size-optimized, and more power efficient than DES. Furthermore, DESL is worth to be considered as an alternative for stream ciphers.

Acknowledgments

The authors would like to thank Matt Robshaw for his insights and valuable comments on various aspects of the S-boxes. The work presented in this paper was supported in part by the European Commission within the STREP UbiSec&Sens of the EU Framework Programme 6 for Research and Development (`www.ist-ubisecsens.org`). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the UbiSecSens project or the European Commission.

References

[ASM01] Satoh, K.T.A., Morioka, S., Munetoh, S.: A Compact Rijndael Hardware Architecture with S-Box Optimization. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 239–254. Springer, Heidelberg (2001)

[BB94] Biham, Biryukov,: How to Strengthen DES Using Existing Hardware. In: Safavi-Naini, R., Pieprzyk, J.P. (eds.) ASIACRYPT 1994. LNCS, vol. 917, Springer, Heidelberg (1995), available for download at `citeseer.ist.psu.edu/biham94how.html`

[BB97] Biham, E., Biryukov, A.: An Improvement of Davies' Attack on DES. Journal of Cryptology: the journal of the International Association for Cryptologic Research 10(3), 195–205 (1997), available for download at `citeseer.ist.psu.edu/467934.html`

[BS91] Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1991)

[BS92] Biham, E., Shamir, A.: Differential Cryptanalysis of the Full 16-Round DES. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 487–496. Springer, Heidelberg (1993), available for download at `citeseer.ist.psu.edu/biham93differential.html`

[Cop94] Coppersmith, D.: The Data Encryption Standard (DES) and its Strength Against Attacks. Technical report rc 186131994, IBM Thomas J. Watson Research Center (December 1994)

[DM95] Davies, D., Murphy, S.: Pairs and Triplets of DES S-Boxes. Journal of Cryptology 8(1), 1–25 (1995)

[DR02] Daemen, J., Rijmen, V.: The Design of Rijndael. Springer Verlag, Berlin, Heidelberg (2002)

[FDW04] Feldhofer, M., Dominikus, S., Wolkerstorfer, J.: Strong Authentication for RFID Systems. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 357–370. Springer, Heidelberg (2004)

[Fin03] Finkenzeller, K.: RFID-Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley and Sons, Chichester (2003)

[FWR05] Feldhofer, M., Wolkerstorfer, J., Rijmen, V.: AES Implementation on a Grain of Sand. Information Security, IEE Proceedings 152(1), 13–20 (2005)

[GB07] Good, T., Benaissa, M.: Hardware Results for selected Stream Cipher Candidates. State of the Art of Stream Ciphers 2007 (SASC 2007), Workshop Record (February 2007)

[HSH+06] Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B.-S., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., Chee, S.: HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 46–59. Springer, Heidelberg (2006)

[KLPL94] Kim, K., Lee, S., Park, S., Lee, D.: DES Can Be Immune to Linear Cryptanalysis. In: Proceedings of the Workshop on Selected Areas in Cryptography SAC'94, pp. 70–81 (May 1994), available for download at `citeseer.csail.mit.edu/kim94des.html`

[KLPL95] Kim, K., Lee, S., Park, S., Lee, D.: Securing DES S-boxes Against Three Robust Cryptanalysis. In: Proceedings of the Workshop on Selected Areas in Cryptography SAC'95, pp. 145–157 (1995), available for download at `citeseer.ist.psu.edu/kim95securing.html`

[Knu92] Knudsen, L.R.: Iterative Characteristics of DES and s^2-DES. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 497–511. Springer, Heidelberg (1993)

[KPL93] Kim, K., Park, S., Lee, S.: Reconstruction of s^2-DES S-Boxes and their Immunity to Differential Cryptanalysis. In: Proceedings of 1993 Korea-Japan Joint Workshop on Information Security and Cryptology (JW-ISC'93) (October 1993), available for download at `citeseer.csail.mit.edu/kim93reconstruction.html`

[KPP+06] Kumar, S., Paar, C., Pelzl, J., Pfeiffer, G., Schimmler, M.: Breaking Ciphers with COPACOBANA - A Cost-Optimized Parallel Code Breaker. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, Springer, Heidelberg (2006)

[Mat94] Matsui, M.: Linear Cryptanalysis of DES Cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 286–397. Springer, Heidelberg (1994)

[PLSP07] Poschmann, A., Leander, G., Schramm, K., Paar, C.: New Ligh-Weight Crypto Algorithms for RFID. In: Proceedings of The IEEE International Symposium on Circuits and Systems 2007 – ISCAS 2007, IEEE Computer Society Press, Los Alamitos, 2007 (to appear)

[RE02] Rankl, W., Effing, W.: Smart Card Handbook. Carl Hanser Verlag, München, Germany, 2nd edn. (2002)

[VHVM88] Verbauwhede, I., Hoornaert, F., Vandewalle, J., De Man, H.: Security and Performance Optimization of a New DES Data Encryption Chip. IEEE Journal of Solid-State Circuits 23(3), 647–656 (1988)