KronCrypt - A New Symmetric Cryptosystem Based on Kronecker's Approximation Theorem

Carsten Elsner
Fachhochschule für die Wirtschaft,
Freundallee 15, 30173 Hannover
carsten.elsner@fhdw.de

Martin Schmidt
Leibniz Universität Hannover, Institute of Applied Mathematics,
Welfengarten 1, 30167 Hannover
mschmidt@ifam.uni-hannover.de

Abstract. In this paper we show how to use an old mathematical concept of diophantine analysis, the approximation theorem of Kronecker, in symmetric cryptography. As a first practical application we propose and analyze the new symmetric 128-bit block cipher KronCrypt. The cipher is a 4-round Feistel network with a non-bijective round function f made up of a variable number of large key-dependent S-boxes, XORs and modular additions. Its key length is variable but not less than 128 bit. The main innovation of KronCrypt in the area of symmetric cryptography is the fact that the key-dependent S-boxes are based upon a constructive proof of the approximation theorem of Kronecker used as a boolean function. We prove the correctness of our concept in general and show how we designe the new cipher KronCrypt. Furthermore, results concerning statistical behaviour, i.e. confusion, diffusion and completeness, and differential cryptanalysis are presented.

1. Introduction

The resumption of old mathematical ideas sometimes led to new concepts in cryptography, e.g. the modular arithmetic and its usage in public-key cryptography and the application of finite fields in AES. A lot of concepts of number theory and algebra influenced new research topics in cryptography or gave rise to new ciphers.

In this paper we present a new idea for symmetric cryptography based on a well-known result from diophantine analysis. We show how a constructive proof of the approximation theorem of Leopold Kronecker can be used for a new private-key cryptosystem.

In the case of KronCrypt, the design process is somewhat different to that of lots of other private-key cryptosystems. Often, the designers want to achieve some cryptographic goals with their new cipher, and a lot of work is done to do so. Here for the main point we had the idea that a constructive proof of Kronecker's approximation theorem is a core component of new symmetric ciphers. After that, we tried to impose a classical and modern design on that core component. Finally,

we analyzed the resulting cipher with respect to some important modern concepts of symmetric cryptanalysis.

KronCrypt is a symmetric 128-bit block cipher with variable key size not less than 128 bit. The main structure is that of a Feistel network with a minimum of $r = 4$ rounds and a round function f made up of a variable number $s \in \{2, 4, 8\}$ of large parallel key-dependent S-boxes $\sigma : \{0,1\}^{s_1} \to \{0,1\}^{s_2}$, where $s_1 = 64/s, s_2 = 64$. Furthermore, compositions of XORs and additions mod s_2 are used. The KronCrypt key κ is a finite sequence of so-called partial quotients $a_0, \ldots, a_{\nu-1}$ of a regular continued fraction $\kappa = [0; a_0, a_1, \ldots, a_{\nu-1}]$ or – equivalent – a rational number c/d. Based on this main key, the round keys $\kappa_i, i = 1, \ldots, r$, are computed by the key schedule.

This paper is organized as follows: Section 2 introduces the main terms and definitions from diophantine analysis. This is required to understand the definition of KronCrypt in Section 3. In Section 4 we discuss the design goals and the various choices we made. The following Section 5 contains a mathematical result about KronCrypt's security. In Section 6 we describe the quality of KronCrypt with respect to the concepts arising from the theory of C. E. Shannon, i.e. the concepts of confusion, diffusion, completeness and the avalanche effect [**1, 2, 3, 4, 5**]. Section 7 presents first results in the context of differential cryptanalysis. At last in Section 8 we summarize and present ideas for further analysis. Numerical results and their plots are given in the Appendices A and B, test vectors can be found in Appendix C.

2. Tools from Diophantine Analysis: Kronecker's Theorem and Continued Fractions

In this section we introduce the main terms and definitions of diophantine analysis which are required to define and understand KronCrypt in the following Section. In diophantine analysis the approximation of irrational numbers $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ by rationals $p/q \in \mathbb{Q}$ is a main topic.[1] The principal tools are the regular *continued fractions*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_{N-1} + \cfrac{1}{a_N}}}}},$$

where the leading coefficient a_0 is an integer and all *partial quotients* $a_i\,(i = 1, \ldots, N)$ are positive integers. The continued fraction is said to be *normed*, if $a_N \neq 1$. It can be shown that for $N \to \infty$ the above given expression converges to some real number α depending on all partial quotients a_i. In that case we call the expression an *infinite continued fraction*, or simply *continued fraction*. Current notations are $[a_0; a_1, a_2, \ldots, a_N]$ (finite continued fraction) and $[a_0; a_1, a_2, \ldots]$ (infinite continued fraction).

An important term is a *convergent*, which is a rational number

$$[a_0; a_1, \ldots, a_n] =: \frac{p_n}{q_n} \quad (0 \leq n \leq N).$$

[1] Nice introductions to this discipline can be found in [**6, 7**].

p_n/q_n is called the n-th convergent of the continued fraction. Given the partial quotients of the continued fraction, the corresponding convergents can easily be computed using the recurrence formulas

$$p_0 = a_0, \qquad p_1 = a_1 a_0 + 1, \qquad p_n = a_n p_{n-1} + p_{n-2} \qquad (2 \leq n \leq N), \tag{1}$$

$$q_0 = 1, \qquad q_1 = a_1, \qquad q_n = a_n q_{n-1} + q_{n-2} \qquad (2 \leq n \leq N). \tag{2}$$

It is useful to know that p_n and q_n are coprime for all convergents and that there is an one-to-one-correspondence between the finite and normed continued fractions and the rational numbers $\mathbb{Q}$ – every rational number can be represented by a unique finite and normed continued fraction and vice versa. Thereby the partial quotients a_i of the continued fraction of a given rational number $p/q \in \mathbb{Q}$ are the quotients from the Euclidean Algorithm applied to p and q.

This can be generalized for irrational numbers $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ leading to an infinite continued fraction. Therefore we recursively define sequences $(a_n)_{n\in\mathbb{N}}$ over $\mathbb{N}$ (except $a_0 \in \mathbb{Z}$) and $(\theta_n)_{n\in\mathbb{N}}$ over $\mathbb{R}_{>1}$ (except $\theta_0 := \alpha \in \mathbb{R}$) by

$$a_n = [\theta_n], \quad \theta_{n+1} = \frac{1}{\theta_n - a_n} \quad (n \geq 0).$$

For an irrational number α its representation by a continued fraction is unique and

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$$

holds. Nothing is known about the size of partial quotients in the case of irrational numbers α except α is a real quadratic surd.

THEOREM 1 (Lagrange). *Let α be a real quadratic surd. Then there are non-negative integers n, m and partial quotients $a_0, a_1, \ldots, a_n$ and $b_0, b_1, \ldots, b_m$ such that*

$$\alpha = [b_0; b_1, \ldots, b_m, a_0, a_1, \ldots, a_n, a_0, a_1, \ldots, a_n, \ldots] \tag{3}$$

is periodic. Conversely, every periodic continued fraction of the form (3) *represents a real quadratic surd α.*

Convergents p_n/q_n are very useful in approximating the corresponding irrational number α. A theorem from diophantine analysis states that

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}} \leq \frac{1}{q_n^2}. \tag{4}$$

Furthermore, convergents are the best rational approximations with bounded denominators: for $n \geq 1, 0 < q \leq q_n$ and $p_n/q_n \neq p/q$, the inequality

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\alpha - \frac{p}{q}\right|$$

holds.

The main target of this section is to present a constructive proof of the approximation theorem of Kronecker, which is a inhomogenous generalization of the approximation theorem of Hurwitz. The latter one states that for every $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ there are infinitely many rationals p/q in lowest terms such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Now, we first state and then prove the approximation theorem of Kronecker:

THEOREM 2 (Kronecker). *For each $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $\eta \in \mathbb{R}$, $n > 0$ and $\delta \in \mathbb{R}$ with $\delta > 0$ there are integers p, q with $q > n$ such that*

$$|q\alpha - p - \eta| < \left(\frac{1}{2} + \frac{1}{\sqrt{5}} + \delta\right)\frac{1}{q}. \tag{5}$$

PROOF. Without loss of generality, let $\delta < 1$. Let $\vartheta := \delta/2$. From the theorem of Hurwitz it follows that there are coprime rational numbers $c/d \in \mathbb{Q}$, $d > \vartheta^{-1}n$, such that

$$|d\alpha - c| < \frac{1}{d\sqrt{5}}. \tag{6}$$

With $h := [d\eta + 1/2]$ we have $|h - d\eta| \leq 1/2$. From the elementary theory of diophantine equations we know that there are integers x, y such that $cx - dy = h$ and $\vartheta d - d < x \leq \vartheta d$. It follows that

$$d|(d+x)\alpha - (c+y) - \eta| \leq (d+x)|d\alpha - c| + |h - d\eta|. \tag{7}$$

Let $p := c + y$, $q := d + x$. Thus, we have $q > n$ because

$$q = d + x > d + \vartheta d - d = \vartheta d > \vartheta\vartheta^{-1}n = n.$$

That gives

$$|q\alpha - p - \eta| < (1+\vartheta)\left(d\sqrt{5}\right)^{-1} + (2d)^{-1}. \tag{8}$$

Furthermore, $d^{-1} \leq (1+\vartheta)q^{-1}$ holds, and this final inequality is used to conclude on

$$(1+\vartheta)\left(d\sqrt{5}\right)^{-1} + (2d)^{-1} < \left(\frac{1}{\sqrt{5}} + \frac{1}{2} + \delta\right)q^{-1}.$$

The theorem is proved. □

The type of approximation result in the theorem of Hurwitz is called *homogeneous diophantine approximation*, whereas the form of Kronecker's approximation theorem is called *inhomogeneous*, η is the *inhomogeneity* of the diophantine inequality. This additional term will be crucial for designing a cryptosystem based upon this proof.

At this point, it should also be remarked that there are k-dimensional versions of Kronecker's theorem. They are stated as follows:

THEOREM 3. *Let $\alpha_1, \ldots, \alpha_k$ be a family of linear independent real numbers over $\mathbb{Z}$, let $\eta_1, \ldots, \eta_k$ be arbitrary real numbers, and let N and ε be positive numbers. Then there are integers $q > N, p_1, \ldots, p_k$ such that*

$$|q\alpha_m - p_m - \eta_m| < \varepsilon \quad (m = 1, \ldots, k).$$

Thereby we call a family of numbers $\xi_1, \ldots, \xi_r$ linear independent over $\mathbb{Z}$ *if*

$$\sum_{i=1}^{r} a_i\xi_i = 0 \Rightarrow a_i = 0 \quad (i = 1, \ldots, r)$$

holds, where $a_i \in \mathbb{Z}$.

In contrast to the one-dimensional approximation theorem, there is no known constructive proof for the multi-dimensional versions. Hence, they cannot be used for cryptographic practice.

3. KronCrypt

In this section we define the new block cipher KronCrypt. In 3.1 the key schedule is discussed, followed by the description of encryption and decryption in 3.2.

3.1. The Key Schedule. Consider the positive integers s_1, s_2, m and K satisfying the following conditions:

$$2^{m-1} \geq K + 2, \quad s_2 - s_1 \geq m. \tag{9}$$

Later, it is proved that m denotes the minimal number of additional bits coming from the process of solving an inhomogeneous diophantine inequality of the form stated in (5). Thus, for a S-box input ρ with $\rho \in \{0,1\}^{s_1}$ and the S-box σ, in which an inhomogenous diophantine equation is solved by the process given by the constructive proof of Theorem 2, we have a S-box $\sigma : \{0,1\}^{s_1} \to \{0,1\}^{s_2}$ with $s_2 \geq m + s_1$.

For generating a KronCrypt key κ, we randomly choose partial quotients from the interval $I := [K, 2K-1]$, where the inequality in (9) is temporarily strengthen to an equation. Thus we have

$$K = 2^{m-1} - 2. \tag{10}$$

Moreover we set the leading coefficient equal to zero, thus achieving a sequence of partial quotients representing a rational number $c/d \in (0,1)$ as the KronCrypt key:

$$\kappa = [0; a_0, a_1, \ldots, a_{\nu-1}] \quad (a_k \in I \text{ for } k = 0, \ldots, \nu-1)\,. \tag{11}$$

ν is chosen sufficiently large to ensure that the binary representation of κ is greater than 128 bit.

With the recurrence formulas it follows easily that the finite sequence of partial quotients as well as the final corresponding convergent are both equivalent representations of one KronCrypt key κ. So the process of key generating has to ensure that both representations have a binary length not less than 128 bit.

The computation of the round keys $\kappa_i, i = 1, \ldots, r$, from the KronCrypt key κ is very simple. For each round the appropriate round key is derived from κ by running through the finite sequence $a_0, \ldots, a_{\nu-1}$ in a cyclic way, starting at the index

$$k = \lambda \cdot i \bmod \nu, \quad \lambda = \max\left\{\left[\frac{\nu}{r}\right], 1\right\} \quad (i = 1, \ldots, r)\,.$$

Again, we set the leading coefficient equal to zero to guarantee that the round keys κ_i represent rational numbers in $(0,1)$, too. The resulting infinite sequence of partial quotients

$$\alpha_i = [0; a_k, a_{k+1}, \ldots, a_{\nu-1}, a_0, a_1, \ldots] \tag{12}$$

is then truncated after the index μ, where the μ-th convergent satisfies the inequality

$$d_{i,\mu-1} \leq \left(1 + \frac{2}{K}\right) 2^{s_1} < d_{i,\mu} \leq 2^{s_2}. \tag{13}$$

As before, the convergents are derived from the sequence of partial quotients using the recurrence formulas. The resulting finite sequence of $\mu + 2$ partial quotients defines the round key

$$\kappa_i = [0; a_{k \bmod \nu}, a_{k+1 \bmod \nu}, \ldots, a_{k+\mu \bmod \nu}]\,.$$

In accordance with the KronCrypt key κ the round keys κ_i are considered as convergents, i.e. rational numbers, respectively. In this way, the κ_i are the convergents

$$\frac{c_i}{d_i} := \frac{c_{i,\mu}}{d_{i,\mu}}$$

of the irrational number α_i. In the following we denote by $\tilde{K}$ the set of all possible round keys. The next theorem guarantees that it is possible to compute a number $d_{i,\mu}$ satisfying (13).

THEOREM 4. *By the method described above for deriving the round keys from the KronCrypt key, there is a denominator $d_{i,\mu}$ of a convergent of α_i satisfying* (13).

PROOF. It follows easily from the recurrence formulas that the sequence of denominators of convergents $(d_{i,0}, d_{i,1}, \ldots)$ is monotone increasing with respect to the second subscript. For this reason, the left-hand side of the inequality

$$d_{i,\mu-1} \leq \left(1 + \frac{2}{K}\right) 2^{s_1} < d_{i,\mu} \tag{14}$$

is obviously true. So we prove the right-hand inequality. Assume that it does not hold, i.e.

$$d_{i,\mu} > 2^{s_2}. \tag{15}$$

Then, on the one side, we get

$$\frac{d_{i,\mu}}{d_{i,\mu-1}} > \frac{2^{s_2}}{(1+2/K)2^{s_1}} \geq \frac{2^{m+s_1}}{(1+2/K)2^{s_1}} = 2K$$

from (10), (14) and (15). On the other side, we have from the recurrence formula for the denominators and from (11) that

$$d_{i,\mu} = a_{k+\mu \bmod \nu} \cdot d_{i,\mu-1} + d_{i,\mu-2} \leq 2K \cdot d_{i,\mu-1},$$

a contradiction. This proves the upper bound for $d_{i,\mu}$. □

3.2. Encryption. Similar to most Feistel ciphers, the plaintext is divided into two halves of equal length. In the case of KronCrypt, we have

$$P = (L_0, R_0) \in \left(\{0,1\}^{64}\right)^2.$$

In each round of the Feistel cipher we define a round function

$$f : \{0,1\}^{64} \times \tilde{K} \to \{0,1\}^{64}$$

operating on the 64-bit string $R_i\,(i = 0, \ldots, r-1)$, and on a round key $\kappa_{i+1} \in \tilde{K}$. Then, the 64-bit output of f is XORed with the left side $L_i\,(i = 0, \ldots, r-1)$, and both sides are swapped for the next round. After the last round of the Feistel cipher, the swapping of both sides is reversed and the algorithm is finished.

3.2.1. *The Round Function f.* The round function f is made up of a parallel usage of $s \in \{2, 4, 8\}$ key-dependent and large S-boxes. Therefore, the input $R_i \in \{0,1\}^{64}$ splits into $64/s$-bit strings $\rho_1, \ldots, \rho_s$, which are inputs of the S-boxes σ_j ($j = 1, \ldots, s$). These S-boxes are nonlinear mappings

$$\sigma : \{0,1\}^{s_1} \to \{0,1\}^{s_2} \quad \left(s_1 = \frac{64}{s}, s_2 = 64\right) \tag{16}$$

which are the same in one round of the Feistel cipher but differ key-dependently from one round to the next. The results $\tau_1, \ldots, \tau_s$ are combined alternately with XOR and addition mod 2^{64} yielding the round function output $z \in \{0,1\}^{64}$. More precisely, we have for each round $i = 1, \ldots, r$ of the Feistel cipher that

$$\begin{aligned} R_i &= (\rho_1, \ldots, \rho_s)\,, \\ \tau_j &= \sigma(\rho_j), \\ j &= 1, \ldots, s. \end{aligned}$$

Finally we compute the output $z = f(R_i, \kappa_{i+1})$ by

$$z = \begin{cases} ((((((\tau_1 \oplus \tau_2) \boxplus \tau_3) \oplus \tau_4) \boxplus \tau_5) \oplus \tau_6) \boxplus \tau_7) \oplus \tau_8 & \text{, if } s = 8 \\ ((\tau_1 \oplus \tau_2) \boxplus \tau_3) \oplus \tau_4 & \text{, if } s = 4 \\ \tau_1 \oplus \tau_2 & \text{, if } s = 2 \end{cases} \tag{17}$$

It is also possible to modify (17) to a symmetric bracketing which is cheaper in hardware. Since we assume a more secure cipher (especially against differential and linear attacks) when using the asymmetric bracketing we compute z as described in (17).

3.2.2. *The S-boxes σ.* The S-boxes σ form the heart of KronCrypt. Implementing the proof of Kronecker's approximation theorem as a boolean function, we get a real innovation in cryptography. For the substitution procedure in KronCrypt we solve an inhomogeneous diophantine inequality. Thus, by following the lines of the proof of Theorem 2, we define the KronCrypt S-boxes.

The terms α, c, d satisfying the inequality of the approximation theorem of Hurwitz result from the key schedule (see 3.1). For the i-th round of the Feistel cipher let[2]

$$\alpha := \alpha_i \notin \mathbb{Q}, \quad c := c_{i,\mu}, \quad d := d_{i,\mu}, \tag{18}$$

whereas it follows from (12) and Theorem 1 that α is a quadratic surd and therefore no rational number. The inhomogeneity represents the input ρ of σ in a scaled way:

$$\eta := \frac{\rho}{2^{s_1}} \quad (s_1 \text{ like in (16)})\,.$$

In accordance with the proof of Theorem 2, let

$$h := \left\lfloor d\eta + \frac{1}{2} \right\rfloor .$$

Solving the diophantine equation

$$cx - dy = h, \quad -d \le x < 0\,, \tag{19}$$

[2]In the following we drop the indices i and j by reasons of clarity.

we know from the elementary theory of diophantine equations that there is a *unique* solution. To do so, we first solve the diophantine equation

$$cu - dv = 1$$

by computing

$$u = c^{-1} \bmod d, \quad v = \left[c \cdot \frac{u}{d} \right].$$

Then, a solution of $cx - dy = h$ is now given by

$$x_0 = uh, \quad y_0 = vh\,,$$

and finally we derive the unique solution of (19) by

$$x = x_0 - td, \quad y = y_0 - tc,$$

where

$$t = \left[\frac{x_0}{d} \right] + 1.$$

Hence, it follows that

$$0 \leq d + x < d. \tag{20}$$

For the completion of the S-box we put

$$p = c + y, \quad q = d + x$$

and find that p and q fulfill the inhomogeneous diophantine inequality of Kronecker's approximation theorem with $1/2 + 1/\sqrt{5} + \delta$ replaced by $1/2 + 1/K$. As the result of this procedure we use the quantity q.

---

input ($\rho \in \{0,1\}^{s_1}$, round key c/d, $u = c^{-1} \bmod d$)
$\eta := \rho / 2^{s_1}$
$h := [d \cdot \eta + 1/2]$
$x_0 := u \cdot h$
$t := [x_0/d] + 1$
$x := x_0 - t \cdot d$
$q := d + x$
output ($\tau = q \in \{0,1\}^{64}$)

ALGORITHM 1

Algorithm 1 provides a formal account of the S-boxes in pseudocode, where those computations from the proof of Kronecker's theorem are omitted which are not needed for the computation of the output $q = \tau$.

The kernel of the following theorem is that the S-box given by Algorithm 1 really computes an output $\tau \in \mathbb{N}_0$ whose binary length is bounded above by $s_2 \geq m + s_1$.

THEOREM 5. *Let s_1, s_2, m, K be the numbers defined in the preceding sections. In particular, equation $s_2 - s_1 \geq m$ holds (see (9)). Furthermore, let $\rho \in \mathbb{N}_0$ such that $\rho < 2^{s_1}$, i.e. ρ is an integer with binary length bounded above by s_1. Then the S-box σ described in Algorithm 1 computes an output $\sigma(\rho) = \tau \in \mathbb{N}_0$ such that $\tau < 2^{s_2}$, i.e. its binary length is bounded above by s_2.*

PROOF. The Theorem follows easily with the equations (20) and (13). □

We now complete the description of the encryption scheme by two final remarks on the choice of the parameters.

REMARK 1. *From* (10) *we have that* $K = 2^{m-1} - 2$. *To guarantee that* $I \neq \emptyset$ *we choose the parameter* $m \geq 3$ *since*

$$I := [K, 2K-1] \neq \emptyset \Leftrightarrow m \geq 3.$$

REMARK 2. *Although any S-box expands the length of its input, the additions mod* 2^{64} *and the XORs afford a round function*

$$f : \{0,1\}^{64} \times \tilde{K} \to \{0,1\}^{64}$$

with a common input and output length. Therefore the number of parallel used S-boxes must be $s \geq 2$.

3.3. Decryption. Similar to any Feistel cipher the decryption algorithm is the same as the encryption algorithm apart from reversing the sequence of round keys.

This completes the definition of KronCrypt.

4. The Design Criteria of KronCrypt

Because of the cipher's Feistel structure the mechanism of decryption is the same as that one for encryption. The idea of using the approximation theorem of Kronecker for symmetric cryptography is quite more useful in theory as described for its practical application in KronCrypt in the last section. The proof of Kronecker's theorem also provides a decryption scheme that can be used in structures different from the Feistel structure, e.g. in a Substitution-Permutation-Network, because the mapping defined by Algorithm 1 is invertible. This will be stated in the following theorem, in which the terms of the last section will be used. Let

$$\|\xi\| := \xi - [\xi], \quad \xi \in \mathbb{R}_{\geq 0}$$

be the fractional part of a non-negative real number ξ, and denote by

$$|\xi|_{\mathbb{Z}} := \max\left\{z \in \mathbb{Z} : |z - \xi| \leq \frac{1}{2}\right\}$$

the nearest integer of a real number ξ. We shall prove the following theorem.

THEOREM 6. *Let* ρ_0 *be a positive integer such that* $\rho_0 \equiv \Omega \pmod{2^{s_1}}$ *for some integer* Ω *with* $0 \leq \Omega < 2^{s_1}$. *Moreover, let* $\eta = \rho_0/2^{s_1}$. *With a valid round key* c/d *given by a convergent of the real number* α *(see* (18)*) and* r *defined by*

$$r := \left| \, 2^{s_1} \, \|q \cdot \alpha\| \, \right|_{\mathbb{Z}}$$

we have $r = \Omega$, *where* ρ_0 *is considered as the S-box input. In the case* $0 \leq \eta < 1$ *we even have* $r = \rho_0$. *So, the S-box input can be computed with the S-box output and by the round key, provided that* $0 \leq \rho_0 < 2^{s_1}$.

PROOF. For $\rho_0 = 0$ we have $q = r = 0$ and the theorem trivially holds. So we may assume that $\rho_0 > 0$ and therefore $\Omega > 0$. From (4), the recurrence formulas and (11) we have

$$|d\alpha - c| < \frac{1}{Kd}.$$

Applying the inequality (7) of the proof of Kronecker's theorem and using $|h - d\eta| \leq 1/2$, we obtain

$$d\,|(d+x)\alpha - (c+y) - \eta| < (d+x)\,|d\alpha - c| + |h - d\eta| < (d+x) \cdot \frac{1}{Kd} + \frac{1}{2}.$$

Let $p := c + y$ and $q := d + x$. From the description of the S-boxes and (20) it follows that

$$d\,|q\alpha - p - \eta| < \frac{d+x}{d} \cdot \frac{1}{K} + \frac{1}{2} < \frac{1}{K} + \frac{1}{2}.$$

Furthermore, dividing by d and using (13), we have

$$|q\alpha - p - \eta| < \frac{1}{d}\left(\frac{1}{K} + \frac{1}{2}\right) < \frac{1}{(1+2/K)\,2^{s_1}}\left(\frac{1}{K} + \frac{1}{2}\right) = \frac{1}{2^{s_1+1}}. \tag{21}$$

In the following we abbreviate by $\varepsilon := q\alpha - p - \eta$. Let $\rho_0 = w2^{s_1} + \Omega$ for some integer $w \geq 0$. Because $\eta = w + \Omega/2^{s_1} \in (w, 1+w)$ and $1 \leq \Omega \leq 2^{s_1} - 1$, we get the inequalities

$$\begin{aligned} w &< w + \frac{1}{2^{s_1}} - \frac{1}{2^{s_1+1}} < \eta - |\varepsilon| < \eta + |\varepsilon| \\ &< w + \frac{2^{s_1}-1}{2^{s_1}} + \frac{1}{2^{s_1+1}} = w + 1 - \frac{1}{2^{s_1+1}} < w + 1\,. \end{aligned}$$

Therefore, we conclude on $w < \eta + \varepsilon < w + 1$. Because of $q\alpha = p + \eta + \varepsilon$ we get $\|q\alpha\| = \eta + \varepsilon - w$ and

$$r = |2^{s_1}\,(\eta + \varepsilon - w)|_{\mathbb{Z}} = \left|2^{s_1}\left(\frac{\Omega}{2^{s_1}} + \varepsilon\right)\right|_{\mathbb{Z}} = |\Omega + \varepsilon \cdot 2^{s_1}|_{\mathbb{Z}}\,.$$

From (21) we derive that

$$-\frac{1}{2} < \varepsilon \cdot 2^{s_1} < \frac{1}{2}\,.$$

Finally, we get

$$r = |\Omega + \varepsilon \cdot 2^{s_1}|_{\mathbb{Z}} = \Omega\,,$$

which proves the theorem for $\rho_0 > 0$ and some arbitrary $w \geq 0$. For $w = 0$ (and $\rho_0 > 0$) we obtain $r = \Omega = \rho_0$. □

Generally speaking, the last theorem converts the constructive proof of Kronecker's approximation theorem into a construction scheme for symmetric cryptosystems. The question arises why the described encryption mechanism is not used for KronCrypt. The answer to this question and a description of the design principles of further components of KronCrypt are now given.

4.1. The Structure of an Iterated Block Cipher. The diffusion and confusion properties of one S-box are not satisfying modern demands of new private-key cryptosystems. Neither all input bits nor all partial quotients of the KronCrypt key κ optimally influence the S-box output. In particular, the partial quotients close to $\nu - 1$ have a very small effect on the encryption. So, the well known principle of creating a stronger cipher by iterating a weaker one is applied here – the delineated problems are solved by transition to an iterated block cipher and by using the key schedule defined in 3.1.

4.2. The Feistel Cipher Structure and Parallel S-boxes. Because of the iterated block cipher a further disadvantage appears, namely the enlargement of the S-box input by applying it to the S-box. According to our present knowledge it is not possible to omit the enlargement, but by the definition of KronCrypt in Section 3 we control it using the parameter m. Thus, the use of $s \geq 2$ parallel S-boxes whose enlargements can be controlled permit the construction of a round function f with a common input and output bit size. This property is achieved by using the XORs and additions mod 2^{64}, but the round function therefore loses its characteristic feature of invertibility. This fact is the main reason for using a Feistel structure for KronCrypt, because Feistel ciphers always define a cryptosystem despite of the properties of the round function f.

4.3. The XORs and Additions mod 2^{64}. There are two main reasons for the usage of these operations. First, the whole cipher gets an additional nonlinear component, because the composition of two operations from different algebraic structures leads to a nonlinear mapping. Second, the quality of KronCrypt concerning concepts like diffusion and confusion is optimized by using both methods (see section 6).

4.4. The Design of the Key Schedule. We mention a very important detail from the simple design of the KronCrypt key schedule: the randomly and equally distributed choice of the partial quotients from the interval I.

Another obvious idea may be the random generation of a 128-bit string and after that the computation of the continued fraction expansion of this number by interpreting the 128-bit integer as the decimal places of a number in $(0, 1)$. However, the depicted characteristics of KronCrypt concerning the concepts of diffusion and confusion are optimized, if the enlargement controlled by m is bounded above by s_2 (see Theorem 5). The enlargement mainly depends on the partial quotients of the continued fraction expansion. It is known from measure theory of continued fractions that the small numbers dominate the partial quotient expansion [**8**]. This is the reason why the enlargement in this case of key organization almost never takes maximum values.

Therefore, we have the main reason for the current design of the key generation and key schedule, in which we choose a series of equally distributed partial quotients from a precomputed interval. In addition, this key generation is obviously more secure against brute-force attacks.

4.5. Reversibility of More Than One Iteration of a S-box. It follows from Theorem 6 and the condition $0 \leq \rho < 2^{s_1}$ that the output $\tau = q = d + x$ of a S-box (see Algorithm 1) can be decrypted simply by computing

$$r = \left| \; 2^{s_1} \, \| \tau \cdot \alpha \| \; \right|_{\mathbb{Z}} . \tag{22}$$

It is possible to iterate the process behind the S-box to strengthen the S-box. In this case, we use the output $q = \tau$ of one iteration as input for the next iteration. Here $\eta \in [0, 1)$ must not hold and the outputs of the second, third and subsequent iterations of the S-box cannot be decrypted by the above process – we only get an *decryption* mod 2^{s_1} as stated in Theorem 6. But adapting the encryption algorithm in the following way, we again guarantee the reversibility of every round by using the decryption formula (22). For this purpose it is necessary to generate round keys $c/d = c_{i,\mu,j}/d_{i,\mu,j}$ for every iteration j of the S-box in addition to the round keys

κ_i $(i = 1, \dots, r)$. This can be done in the same way as described for the round keys in Section 3.1. The key c/d is uniquely determined by the inequalities

$$d_{i,\mu-1,j} \leq \left(1 + \frac{2}{K}\right) 2^{s_1+m(j-1)} < d_{i,\mu,j} \leq 2^{s_1+mj} \quad (j = 1, \dots, l)$$

which we now apply instead of the conditions from (13) and where l represents the number of iterations. Simultaneously, we define η in iteration j of the S-box by $\eta = \tau/2^{s_1+(j-1)m}$, where $\tau = \rho$ when $j = 1$, and τ represents the output of iteration $j-1$ when $j \geq 2$. To ensure an output τ of the iterated process that is bounded above by 2^{s_2} we have to choose l such that $s_1 + ml \leq s_2$.

Of course, the computation of such additional round keys will complicate the whole cipher. The computations for the keys of each iteration of the S-boxes can be done in a pre-processing step, whereas the new definition of η in every iteration increases the time complexity of encryptions and decryptions.

5. Some Comments on the Security of KronCrypt

As already mentioned, in any S-box we compute a pair p, q of integers satisfying an inequality given by (21),

$$|q\alpha - p - \eta| < \frac{1}{2^{s_1+1}}, \quad \eta = \frac{\rho}{2^{s_1}}.$$

The number p is ignored; for the decryption process using the formula

$$r = \left| \; 2^{s_1} \, \|q \cdot \alpha\| \; \right|_{\mathbb{Z}}$$

from Theorem 6 only the integer q is used, but not p. An attacker should not know p, q and ρ simultaneously, since otherwise he has chances to find the correct value of the partial quotient a_k from the actual key $\alpha_i = [0; a_k, a_{k+1}, \dots]$ of the cipher. The (geometric) probability P to conclude on a_k from p, q, ρ is given by the following theorem.

THEOREM 7. *Let $\alpha = [0; a_0, a_1, \dots]$ be a round key. Let ρ be some nonnegative integer, and let p, q be integers satisfying the inequality*

$$|q\alpha - p - \eta| \; < \; \frac{1}{2^{s_1+1}}.$$

Furthermore, let

$$\begin{aligned} \alpha_1 &= \frac{p+\eta}{q} - \frac{1}{q2^{s_1+1}} = [0; b_0, b_1, \dots], \\ \alpha_2 &= \frac{p+\eta}{q} + \frac{1}{q2^{s_1+1}} = [0; c_0, c_1, \dots] \end{aligned}$$

be the continued fraction expansion of the two rationals α_1 and α_2. Then, we have

$$b_0 = c_0 \qquad \Longrightarrow \qquad b_0 = c_0 = a_0 \, .$$

Let $p > 0$. Then, the (geometric) probability P for the hypothesis $b_0 = c_0$ satisfies the inequality

$$P(b_0 = c_0) \; \geq \; 1 - \frac{p+q}{p^2 2^{s_1}} \, .$$

PROOF. (i) We know that

$$a_0 \,=\, \left[\,\frac{1}{\alpha}\,\right], \quad b_0 \,=\, \left[\,\frac{1}{\alpha_1}\,\right], \quad c_0 \,=\, \left[\,\frac{1}{\alpha_2}\,\right],$$

and $\alpha_1 < \alpha < \alpha_2$. Therefore, $1/\alpha_2 < 1/\alpha < 1/\alpha_1$, hence the hypothesis $b_0 = c_0$ implies that $b_0 \le 1/\alpha_2 < 1/\alpha < 1/\alpha_1 < b_0 + 1$. Then, from $a_0 \le 1/\alpha < a_0 + 1$ we conclude on $a_0 = b_0\,(= c_0)$, which proves the first statement of the theorem.
(ii) We may assume that $p > 0$. There is an unique integer $n \ge 1$ satisfying

$$\frac{1}{n+1} \,<\, \frac{p+\eta}{q} \,\le\, \frac{1}{n}\,.$$

Then, $b_0 = c_0 (= n)$ holds if and only if the inequalities

$$\frac{1}{n+1} \,<\, \frac{p+\eta}{q} - \frac{1}{q2^{s_1+1}} \,<\, \frac{p+\eta}{q} + \frac{1}{q2^{s_1+1}} \,\le\, \frac{1}{n}$$

are satisfied. Again, this is equivalent with the fact that

$$\frac{1}{n+1} + \frac{1}{q2^{s_1+1}} \,<\, \frac{p+\eta}{q} \,\le\, \frac{1}{n} - \frac{1}{q2^{s_1+1}}\,,$$

or

$$\frac{p+\eta}{q} \,\in\, J \,:=\, \left(\,\frac{1}{n+1} + \frac{1}{q2^{s_1+1}}\,,\, \frac{1}{n} - \frac{1}{q2^{s_1+1}}\,\right]\,.$$

Defining the geometric probability $P(b_0 = c_0)$ by

$$P(b_0 = c_0) \,:=\, P\Big(\,\frac{p+\eta}{q} \in J\,\Big)\,,$$

we conclude using the basic interval $E := \big((n+1)^{-1}, n^{-1}\big]$ on

$$P(b_0 = c_0) = \frac{|J|}{|E|} \,=\, \frac{\left(\dfrac{1}{n} - \dfrac{1}{q2^{s_1+1}}\right) - \left(\dfrac{1}{n+1} + \dfrac{1}{q2^{s_1+1}}\right)}{\dfrac{1}{n} - \dfrac{1}{n+1}}$$

$$= 1 - \frac{n(n+1)}{q2^{s_1}}\,.$$

Since $p \ge 1$ and $\eta \ge 0$, we have

$$n \,=\, \left[\,\frac{q}{p+\eta}\,\right] \,\le\, \frac{q}{p+\eta} \,\le\, \frac{q}{p}\,,$$

hence

$$P(b_0 = c_0) \,\ge\, 1 - \frac{1 + q/p}{p2^{s_1}} \,=\, 1 - \frac{p+q}{p^2 2^{s_1}}\,,$$

as desired. □

6. Confusion, Diffusion and Completeness of KronCrypt

Most symmetric cryptosystems have explicit design goals and the originators work hard to achieve these goals. As mentioned above, in the case of KronCrypt, our procedure was somewhat different. First, we realized that a constructive proof of Kronecker's approximation theorem can be changed into a private-key cryptosystem. Then, we built up a modern designed private-key cryptosystem with the above described S-boxes by implementing the proof as its core component. At least, we

analyzed the quality of the resulting cryptosystem according to nowadays standard techniques in cryptanalysis.

In this section, we present our analysis of KronCrypt concerning the concepts arising from C. E. Shannon's theory of secrecy systems from 1949 [**1**], i.e. especially diffusion, confusion and completeness as well as the related concept of the (strict) avalanche effect, respectively. Therefore, we first describe the algorithms we used to analyze KronCrypt and then present the results.

6.1. Analysis of the S-boxes. As it is well-known, we use the term *confusion* to measure the relationship between the cipher and plain text. Combined with the term *diffusion*, which measures how strong the cipher text depends on the plain text and on the key, we implemented some test scenarios. They were applied for each s and some exemplary values for the parameter m. This implementation is presented in the following.

6.1.1. *Analysis Concerning Variability in the Input.* Let the parameters m and s be given. We randomly generate a KronCrypt key κ, compute a valid round key c/d from it and also generate a $64/s$-bit S-box input ρ_1. Afterwards, ρ_1 is swapped in one randomly chosen bit $i\,(i = 0, \ldots, 64/s - 1)$, leading to ρ_2. Then, ρ_1 and ρ_2 are substituted by the S-box σ which is defined by the parameters m and s. We get the outputs $\tau_1 = \sigma(\rho_1)$ and $\tau_2 = \sigma(\rho_2)$. For both substitutions, we use the same round key c/d. Subsequently, we count the positions where the resulting outputs τ_1 and τ_2 differ. This procedure is repeated $n = 100000$ times with different randomly generated S-box inputs ρ_1 und ρ_2. In each run a new round key c/d is randomly generated and it is used for both substitutions. Therefore, the results are independent of a single round key.

In addition, a counter is incremented for each output bit $j\,(j = 0, \ldots, 63)$, if this bit differs in the considered output pair τ_1 and τ_2. For such a large number of runs like $n = 100000$ we may draw a conclusion on the probability for a certain output bit to change because of an arbitrary change of a single input bit. So, by this procedure we are informed on the diffusion, confusion and completeness properties of the S-boxes as well as on the (strict) avalanche effect, respectively.

Table 1(a) and Figure 1(a) give an outline of the results. The tables and plots can be found in Appendix A. The first two columns of Table 1(a) define the S-box. k_1 counts the number of output bits that change with a probability p_1, where $0.45 < p_1 < 0.55$, after changing a single bit in the input. These bits are called *strong bits*. k_2 counts the number of output bits, which change with the probability p_2, where $0.05 \leq p_2 \leq 0.45$. These bits are called *unexplicit bits*. At last k_3 counts the output bits, that change with a probability p_3, where $p_3 < 0.05$. These are called *weak bits*. Terms in brackets represent the positions of the considered bits. Finally, k_4 lists the amount of bit differences between the outputs τ_1 and τ_2. k_4 can be independent from the position of bit swapping in the input. If not, the whole range of amount is listed when the bit changes occur at different bit positions in the input.

Of course, the optimum result in this scenario would be a maximum k_1 with minimum k_2 and k_3 as well as a value of k_4 close to $s_2/2 = 32$. In this optimal case, an attacker would have no chance to exploit some statistical relationships between input and output bits.

The characteristics of the S-boxes harmonize with the arranged analysis. The amount of strong bits is significantly dominating for almost all parameter combinations. We see that ϕ gets approximately 1 for each $s \in \{2, 4, 8\}$ and $m = 3$. Hence, the strict avalanche criterion is fulfilled and the S-boxes are complete. Every other choice of m leads to a significantly smaller ϕ except of the case $s = 2$ and maximal $m = 32$, where the S-box approximately achieves completeness, too.

At this point, the strongest point of criticism reveals: the unexplicit bits and the weak bits are the leading ones without exception. The reason for this phenomenon is based on the estimation for the enlargement of the S-box input in Theorem 5. Therefore, we explain the failure of change in the leading bits by the fact that these bits are only rarely needed in the binary representation of the S-box output. Thus, they equal to zero in both τ_1 and τ_2. Obviously, the estimation in Theorem 5 gets more strict, if the number m is minimized, because we get a smaller difference $|d_{i,\mu} - 2^{s_2}|$ between the denominator of the round key and its upper bound with higher probability.

The existence of leading zeros in the S-box output is another reason for using XORs and additions mod 2^{64} to combine the several S-box outputs. When only using XORs, the leading zeros remain unchanged and a larger range of leading bits equals to zero. Obviously, this problem is solved by the usage of additions mod 2^{64}.

6.1.2. *Analysis Concerning Variability in the Key.* Similar to the analysis concerning variability in the S-box input, we also analyzed the S-boxes regarding the variability in the round key, i.e. the key for the S-boxes. Therefore, we randomly generate a $64/s$-bit input ρ and a round key $\kappa = c/d$ from which we derive a second round key $\kappa' = c'/d'$ by changing one randomly chosen position of κ. Here we have to ensure that $(c', d') = 1$, because this is required by the S-boxes. Afterwards we compute τ and τ' from ρ by using κ and κ' within the S-box and accomplish the same analysis as in the case of variability in the input.

Table 1(b) and Figure 1(b) give an outlook on the results (similar to Table 1(a) and Figure 1(a) for the variability in the input).

We see that these results approximately reflect the results discussed above – the tendency to minimize m for getting optimized statistical behaviour can be seen here, too. Moreover, the $(32, 64)$-S-box is the only one that fulfills the strict avalanche criterion with a choice of m differing from $m = 3$, namely $m = 32$. Again, the existence of leading zeros can be seen here and has the analogous explanation.

Summing up, we have a little better results in the case of variability in the input, i.e. the results for $s = 8$ and $m \geq 40$. Nevertheless, both results of the S-box analysis give us occasion to the usage of these S-boxes within a Feistel cipher. They will lead to quite well statistical behaviour with a small number of rounds r for some parameter combination.

6.2. Analysis of the Entire Cryptosystem. Both, analysis of variability in the input and analysis of variability in the key, are useful to investigate the statistical behaviour of the entire cryptosystem. As input pairs we now consider 128-bit plaintext blocks, which exactly differ in one randomly chosen position, and the corresponding 128-bit ciphertext blocks. For the analysis of the variability in the key we consider valid KronCrypt keys $\kappa = c/d$ with numerator or denominator changed in a randomly chosen position. By doing so, we have to ensure that the resulting second key $\kappa' = c'/d'$ is a valid KronCrypt key.

For the investigation of the entire cryptosystem we focus on the *degree of completeness* of the resulting Feistel cipher, which is the quotient $\phi = k_1/128$. Here, we only consider even round numbers only, i.e. cycles of the Feistel cipher. To do so, we accomplish the described algorithms for each s to the same exemplary parameters m as in 6.1 and $r = 2, 4, 6$.

Table 2 and Figure 2 show the results for k_1, k_2, k_3, ϕ and $r = 2, 4, 6$.

It can be seen, that the statistical behaviour of the S-boxes governs the behaviour of the whole cryptosystem. Like in the preceding analysis, we have the best results in the cases $s = 2, 4, 8$ and minimal $m = 3$ as well as $m = 32$ for $s = 2$. Another interesting fact is that we have a great increase of ϕ by the transition from 2 to 4 rounds, but we have approximately the same curves for $r = 4$ and $r = 6$.

Finally, we can hold the fact that KronCrypt fulfills the strict avalanche criterion and therefore achieves completeness for both variability in the input and in the key for the following parameter combinations:

(1) $m = 3, s = 2, 4, 8$ and $r \geq 4$
(2) $m = 32, s = 2$ and $r \geq 4$

In order to increase the cipher's speed as well as to ensure optimal statistical behaviour we propose to run KronCrypt with $s = 2$ parallel S-boxes and a minimum of 4 rounds.

7. Differential Cryptanalysis of KronCrypt

Due to the fact that differential cryptanalysis [**9, 10**] is one of the most powerful techniques for attacking a symmetric cipher we analyzed the security of KronCrypt against it. For presenting our results we have to fix some notations from the area of differential cryptanalysis. This is done in Section 7.1. In Section 7.2 we discuss our numerical results. The corresponding plots are given in Appendix B.

7.1. Notations and Algorithms. Consider a S-box $\sigma : \{0,1\}^m \to \{0,1\}^n$. Let $(x, x^*) \in (\{0,1\}^m)^2$ be an ordered pair with XOR-difference $x' = x \oplus x^*$. We call $x \oplus x^*$ a *XOR input-difference* and $\sigma(x) \oplus \sigma(x^*)$ a *XOR output-difference* of σ. For a constant difference $x' \in \{0,1\}^m$ the set

$$\Delta(x') := \{(x, x \oplus x') : x \in \{0,1\}^m\}$$

is called the *set of all ordered pairs* (x, x^*) *with XOR input-difference* x'. Later, we need the fact that $|\Delta(x')| = 2^m$ holds.

The main idea of differential cryptanalysis is to analyze the so-called *XOR difference distribution table* of the S-box σ (see [**11**] for a detailed description of differential cryptanalysis). This $2^m \times 2^n$ table consists of the entries

$$N_D(x', y') = |\{(x, x^*) \in \Delta(x') : \sigma(x) \oplus \sigma(x^*) = y'\}|.$$

The probability that a given input difference x' leads to a given output difference y' can easily be computed by the formula

$$R_p(x', y') = \frac{N_D(x', y')}{2^m}.$$

$R_p(x', y')$ is called *propagation probability* of the pair (x', y').

It is possible to compute the difference distribution table (DDT) by using Algorithm 2. Its time complexity is $\mathcal{O}(2^{2m})$ and its space complexity is $\mathcal{O}(2^{m+n})$. By considering the values m and n in the case of KronCrypt, $m = s_1 \in \{8, 16, 32\}$ and

$n = s_2 = 64$, we obtain requirements on time and space complexity which are not practicable.

```
input ((m,n)–S–Box σ (constant))
for x' := 0 to 2^m − 1 do
    for y' := 0 to 2^n − 1 do
        D[x', y'] := 0
for each Input–Difference x' := 0 to 2^m − 1 do
    for each Input–Pair (x, x*) with Difference x' do
        y := σ(x)
        y* := σ(x*)
        y' := y ⊕ y*
        D[x', y'] := D[x', y'] + 1
output (DDT D of σ)
```

Algorithm 2

Because of the discussed complexities we focus ourselves on some single values of the DDT instead of analyzing the whole table. First, these are the maximal values in the table, which yield to the maximal values of R_p. Second, we analyze the amount of non-zero values in the DDT. Both aspects are important for mounting a feasible differential cryptanalysis of the whole cipher.

These values are the output of Algorithm 3 which we used in our analysis. We see that the time complexity increases to $\mathcal{O}(2^{2m} + 2^{m+n})$ but that the memory requirement is decreasing to $\mathcal{O}(2^n)$. Because the space requirement is more crucial for our computers, Algorithm 3 is more convenient for our practice.

```
input ((m,n)–S–Box σ (constant))
for i := (0) to 2^n − 1 do
    R[i] := 0
max := 0
zeroCounter := 0
for each Input–Difference x' := 0 to 2^m − 1 do
    for each Input–Pair (x, x*) with Difference x' do
        y := σ(x)
        y* := σ(x*)
        y' := y ⊕ y*
        R[y'] := R[y'] + 1
    for each i := 0 to 2^n − 1 do
        if (i ≠ 0 and x' ≠ 0 and R[i] > max) then
            max := R[i]
        if (R[i] = 0) then
            zeroCounter := zeroCounter+1
        R[i] := 0
output (max, zeroCounter)
```

Algorithm 3

7.2. Numerical Results. One of the main characteristics of our cipher are the key-dependent S-boxes. This key-dependence naturally leads to a strong resistance against differential cryptanalysis (see the attacks on Khufu and Khafre [**12**]

in [**13, 14**] or on Blowfish [**15**] in [**16**]). Being completely uninformed on the structure of the DDTs, an attacker gets much weaker. A standard strategy for analyzing the properties concerning differential attacks of key-dependent S-boxes is to assume constant S-boxes by fixing a key that defines the S-box (see [**16**]).

For analyzing the properties of the KronCrypt S-boxes we apply Algorithm 3 on $n = 10000$ fixed and randomly chosen round keys κ_i defining known and constant S-boxes. Thereby we extract the following values:

- The maximum m_{max} of all maximal entries of the n DDTs. Thus we can execute the maximal propagation ratio $R_{p,max}$ of all maximal R_p of the n DDTs.
- The minimum m_{min} of all maximal entries of the n DDTs. Thus we can execute the minimal propagation ratio $R_{p,min}$ of all maximal R_p of the n DDTs.
- The average m_d of all maximal entries of the n DDTs. Thus we can execute the average propagation ratio $R_{p,d}$ of all maximal R_p of the n DDTs.
- The maximum n_{max} of non-zero entries in the n DDTs.
- The minimum n_{min} of non-zero entries in the n DDTs.
- The average n_d of non-zero entries in the n DDTs.

Because of its complexity, Algorithm 3 can only be applied to the $(8, 64)$ S-boxes on our computers. To get some more numerical results we additionally compute the values for the smaller $(8, 16)$, $(8, 24)$ and $(8, 32)$ S-boxes. In each of these cases we compute all results for every valid parameter $3 \leq m \leq s_2 - s_1$.

The results are shown in the tables in Appendix B using the notation listed above. We recognize that values of $R_{p,min}$ and n_{max}, $R_{p,max}$ and n_{min} as well as $R_{p,d}$ and n_d are associated with each other in an antiproportional way. Because of the density of measurements this can cleary be seen in Figure 6. By analyzing the most important value $R_{p,d}$ it comes out that its shape is that of a saw tooth with highest values at points for which n_d gets minimal. A reason for this *saw tooth phenomenon* could not be found yet.

KronCrypt should be used by a parameter combination that leads to minimal values of $R_{p,min}, R_{p,max}$, and R_d, because this obviously complicates a differential attack of the whole cryptosystem. For almost every considered S-box size (s_1, s_2) we get minimal values for $R_{p,min}, R_{p,max}$ and $R_{p,d}$ by choosing $m = 3$ which corresponds to the results in Section 6.

Additionally, the maximal values for $R_{p,d}$ are monotonously decreasing with the S-box output size s_2, which is also known from the theory (see [**17**]).

These facts, the computational complexity of Algorithms 2 and 3 in the case of KronCrypt-specific m and n as well as the restriction of our analysis to the situation with known S-boxes, allow us to presume a strong security of KronCrypt against differential attacks.

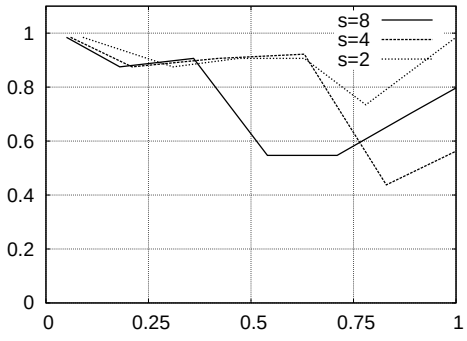
8. Conclusions and Further Work

In this paper we presented how to use an old mathematical concept of diophantine analysis, the approximation theorem of Kronecker, in symmetric cryptography. We proved the correctness of our idea and designed the 128-bit block cipher KronCrypt. The main parts of KronCrypt are its key-dependent and large S-boxes

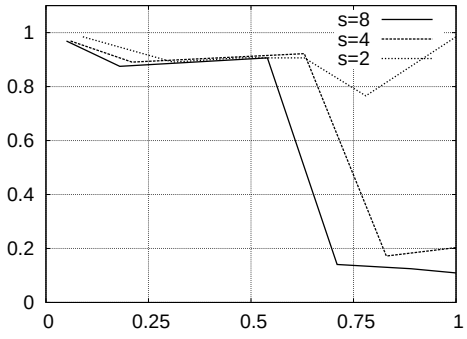
which are based on a constructive proof of Kronecker's theorem used as a boolean function.

Beyond its theoretical appeal we were able to show its practicability by the statistical results and the first results concerning differential cryptanalysis. Further work may be the investigation of a hardware implementation and other cryptanalysis techniques, first of all linear cryptanalysis.

Appendix A. Numerical Results Concerning Confusion, Diffusion and Completeness



(a) Variability in the input



(b) Variability in the key

FIGURE 1. Degrees of completeness ϕ versus $m/(s_2 - s_1)$ of KronCrypt's S-boxes for $s = 2, 4, 8$

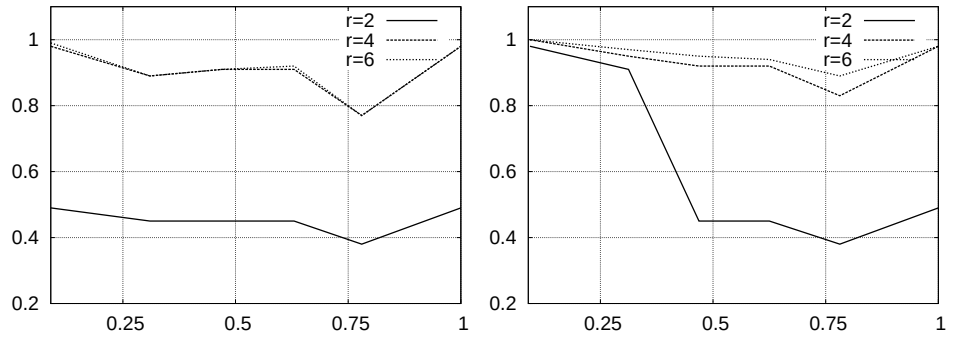
(a) Statistical analysis of KronCrypt's S-boxes concerning variability in the input

(s_1, s_2)	m	k_1	k_2	k_3	k_4	ϕ
$(8, 64)$	3	63 (1-63)	1 (0)	0	32	0.984
$(8, 64)$	10	56 (8-63)	2 (6,7)	6 (0-5)	28-29	0.875
$(8, 64)$	20	58 (6-63)	2 (4,5)	4 (0-3)	28-29	0.906
$(8, 64)$	30	35 (5-7,32-63)	25 (4,8-31)	4 (0-3)	23-30	0.547
$(8, 64)$	40	35 (29-63)	5 (24-28)	24 (0-23)	17-20	0.547
$(8, 64)$	50	45 (19-63)	5 (14-18)	14 (0-13)	23-25	0.703
$(8, 64)$	56	51 (13-63)	5 (8-12)	8 (0-7)	25-28	0.797
$(16, 64)$	3	63 (1-63)	1 (0)	0	32	0.984
$(16, 64)$	10	56 (8-63)	2 (6,7)	6 (0-5)	28-29	0.875
$(16, 64)$	20	58 (6-63)	2 (4,5)	4 (0-3)	28-29	0.906
$(16, 64)$	30	59 (5-63)	1 (4)	4 (0-3)	23-30	0.922
$(16, 64)$	40	28 (36-63)	12 (24-35)	24 (0-23)	14-20	0.438
$(16, 64)$	48	36 (28-63)	12 (16-27)	16 (0-15)	17-24	0.563
$(32, 64)$	3	63 (1-63)	1 (0)	0	32	0.984
$(32, 64)$	10	56 (8-63)	2 (6,7)	6 (0-5)	28-29	0.875
$(32, 64)$	15	58 (6-63)	1 (5)	5 (0-4)	27-29	0.906
$(32, 64)$	20	58 (6-63)	2 (4,5)	4 (0-3)	27-30	0.906
$(32, 64)$	25	47 (17-63)	3 (14-16)	14 (0-13)	19-25	0.734
$(32, 64)$	32	63 (1-63)	1 (0)	0	25-32	0.984

(b) Statistical analysis of KronCrypt's S-boxes concerning variability in the key

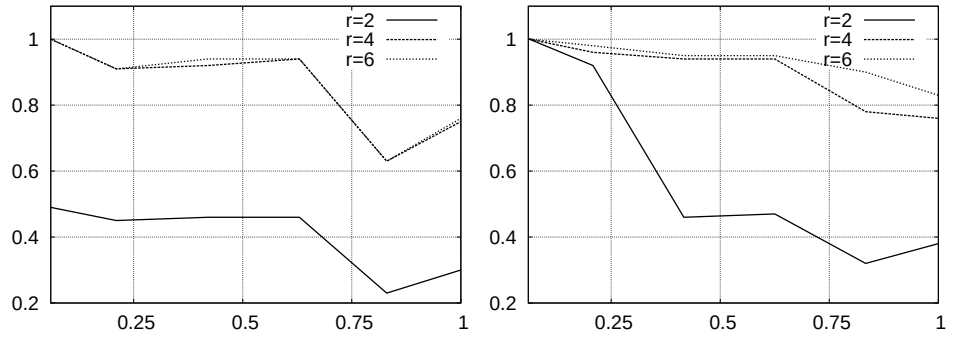
(s_1, s_2)	m	k_1	k_2	k_3	k_4	ϕ
$(8, 64)$	3	62 (1-62)	2 (0,63)	0	29-31	0.969
$(8, 64)$	10	56 (7-62)	2 (6,63)	6 (0-5)	26-33	0.875
$(8, 64)$	20	57 (6-62)	2 (5,63)	5 (0-4)	25-30	0.891
$(8, 64)$	30	58 (5-62)	2 (4,63)	4 (0-3)	26-29	0.906
$(8, 64)$	40	9 (53-61)	27 (28-52,62,63)	28 (0-27)	2-18	0.141
$(8, 64)$	50	8 (51-58)	36 (20-50,59-63)	20 (0-19)	2-21	0.125
$(8, 64)$	56	7 (50-56)	41 (16-49,57-63)	16 (0-15)	2-23	0.109
$(16, 64)$	3	62 (1-62)	2 (0,63)	0	29-31	0.969
$(16, 64)$	10	57 (7-63)	1 (6)	6 (0-5)	27-37	0.891
$(16, 64)$	20	58 (6-63)	1 (5)	5 (0-4)	27-31	0.906
$(16, 64)$	30	59 (5-63)	1 (4)	4 (0-3)	25-29	0.922
$(16, 64)$	40	11 (53-63)	25 (28-52)	28 (0-27)	2-20	0.172
$(16, 64)$	48	13 (51-63)	30 (21-50)	21 (0-20)	2-24	0.203
$(32, 64)$	3	63 (1-63)	1(0)	0	29-31	0.984
$(32, 64)$	10	57 (7-63)	1 (6)	6 (0-5)	27-28	0.891
$(32, 64)$	15	58 (6-63)	1 (5)	5 (0-4)	27-29	0.906
$(32, 64)$	20	58 (5-62)	1 (5)	5 (0-4)	27-29	0.906
$(32, 64)$	25	49 (15-63)	1 (14)	14 (0-13)	22-24	0.766
$(32, 64)$	32	63 (1-63)	1 (0)	0	28-31	0.984

TABLE 1. Statistical analysis of KronCrypt's S-boxes



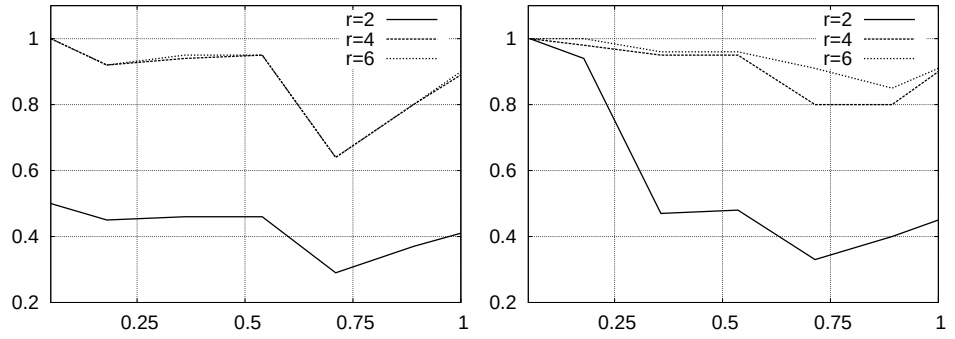
(a) Variability in the input, ϕ for $s = 2$

(b) Variability in the key, ϕ for $s = 2$



(c) Variability in the input, ϕ for $s = 4$

(d) Variability in the key, ϕ for $s = 4$



(e) Variability in the input, ϕ for $s = 8$

(f) Variability in the key, ϕ for $s = 8$

FIGURE 2. Degrees of completeness ϕ versus $m/(s_2 - s_1)$ of KronCrypt with $s = 2, 4, 8$ and $r = 2, 4, 6$ rounds

(a) Statistical analysis of KronCrypt concerning variability in the plaintext

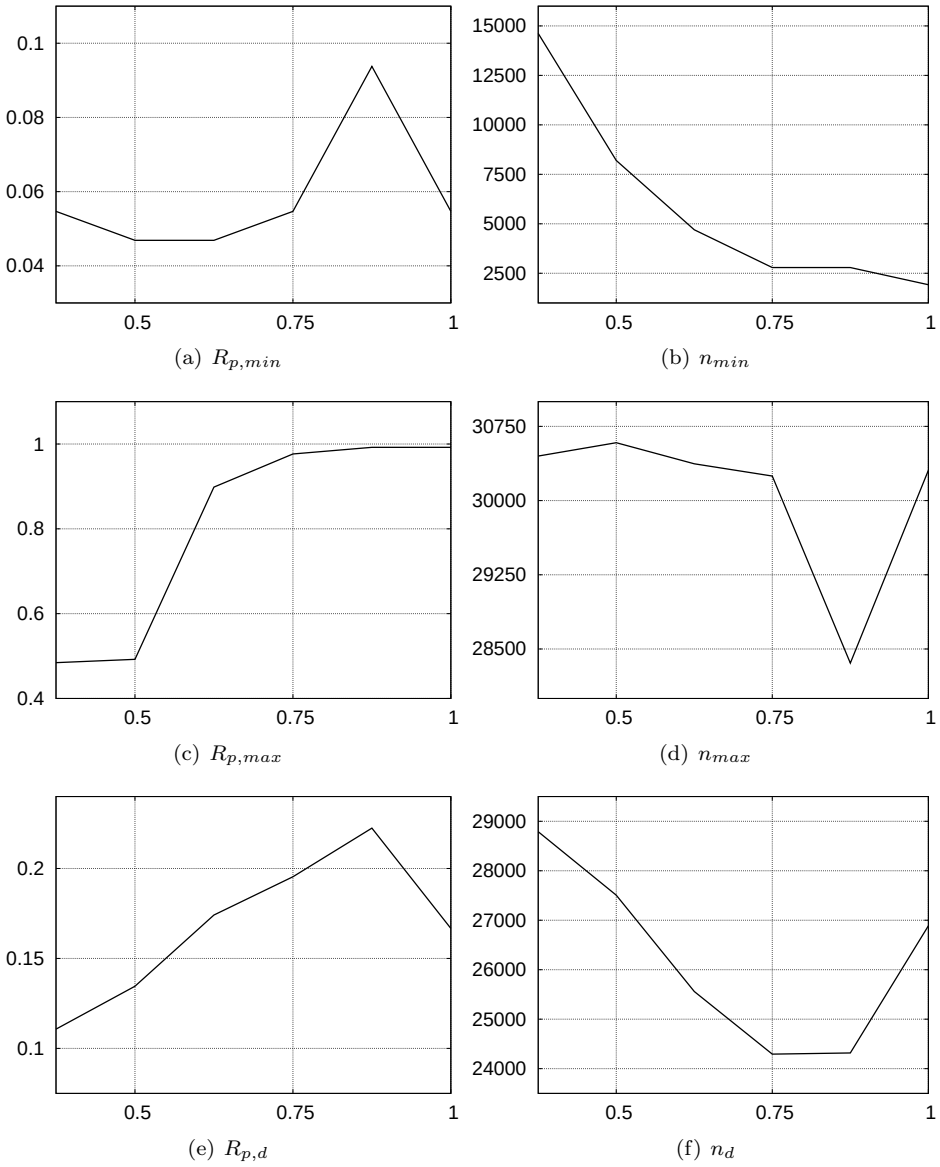
		$r=2$				$r=4$				$r=6$			
(s_1, s_2)	m	k_1	k_2	k_3	ϕ	k_1	k_2	k_3	ϕ	k_1	k_2	k_3	ϕ
$(8, 64)$	3	64	64	0	0.500	128	0	0	1.000	128	0	0	1.000
$(8, 64)$	10	57	63	8	0.445	118	3	7	0.922	118	4	6	0.922
$(8, 64)$	20	59	63	6	0.461	120	4	4	0.938	122	2	4	0.953
$(8, 64)$	30	59	64	5	0.461	122	2	4	0.953	122	2	4	0.953
$(8, 64)$	40	37	47	44	0.289	82	2	44	0.641	82	2	44	0,641
$(8, 64)$	50	47	57	24	0.367	102	2	24	0.797	102	2	24	0.797
$(8, 64)$	56	53	63	12	0.414	114	2	12	0.891	115	1	12	0.898
$(16, 64)$	3	63	65	0	0.492	128	0	0	1.000	128	0	0	1.000
$(16, 64)$	10	57	61	10	0.445	116	4	8	0.906	116	4	8	0.906
$(16, 64)$	20	59	62	7	0.461	118	4	6	0.922	120	2	6	0.938
$(16, 64)$	30	59	63	6	0.461	120	2	6	0.938	120	2	6	0.938
$(16, 64)$	40	30	51	47	0.234	80	2	46	0.625	80	2	46	0.625
$(16, 64)$	48	38	59	31	0.297	96	2	30	0.750	97	1	30	0.758
$(32, 64)$	3	63	65	0	0.492	126	2	0	0.984	127	1	0	0.992
$(32, 64)$	10	57	60	11	0.445	114	4	10	0.891	114	4	10	0.891
$(32, 64)$	15	58	60	10	0.453	116	3	9	0.906	116	4	8	0.906
$(32, 64)$	20	58	61	9	0.453	117	3	8	0.914	118	2	8	0.922
$(32, 64)$	25	48	52	28	0.375	98	2	28	0.766	98	2	28	0.766
$(32, 64)$	32	63	65	0	0.492	126	2	0	0.984	126	2	0	0.984

(b) Statistical analysis of KronCrypt concerning variability in the key

		$r=2$				$r=4$				$r=6$			
(s_1, s_2)	m	k_1	k_2	k_3	ϕ	k_1	k_2	k_3	ϕ	k_1	k_2	k_3	ϕ
$(8, 64)$	3	128	0	0	1.000	128	0	0	1.000	128	0	0	1.000
$(8, 64)$	10	120	8	0	0.938	125	3	0	0.977	128	0	0	1.000
$(8, 64)$	20	60	68	0	0.469	122	6	0	0.953	123	5	0	0.916
$(8, 64)$	30	61	67	0	0.477	122	6	0	0.953	123	5	0	0.961
$(8, 64)$	40	42	86	0	0.328	102	26	0	0.797	117	11	0	0.914
$(8, 64)$	50	51	70	7	0.398	103	25	0	0.805	109	19	0	0.852
$(8, 64)$	56	57	70	1	0.445	115	13	0	0.898	116	12	0	0.906
$(16, 64)$	3	128	0	0	1.000	128	0	0	1.000	128	0	0	1.000
$(16, 64)$	10	118	10	0	0.922	123	5	0	0.961	126	2	0	0.984
$(16, 64)$	20	59	69	0	0.461	120	8	0	0.938	121	7	0	0.945
$(16, 64)$	30	60	68	0	0.469	120	8	0	0.938	121	7	0	0.945
$(16, 64)$	40	41	86	1	0.320	100	28	0	0.781	115	13	0	0.898
$(16, 64)$	48	48	70	10	0.375	97	31	0	0.758	106	22	0	0.828
$(32, 64)$	3	126	2	0	0.984	128	0	0	1.000	128	0	0	1.000
$(32, 64)$	10	116	11	1	0.906	121	7	0	0.945	124	4	0	0.969
$(32, 64)$	15	58	69	1	0.453	118	10	0	0.922	122	6	0	0.953
$(32, 64)$	20	58	69	1	0.453	118	10	0	0.922	120	8	0	0.938
$(32, 64)$	25	49	78	1	0.383	106	22	0	0.828	114	14	0	0.891
$(32, 64)$	32	63	65	0	0.492	126	2	0	0.984	126	2	0	0.984

TABLE 2. Statistical analysis of KronCrypt

Appendix B. Plots of the Numerical Results Concerning Differential Cryptanalysis

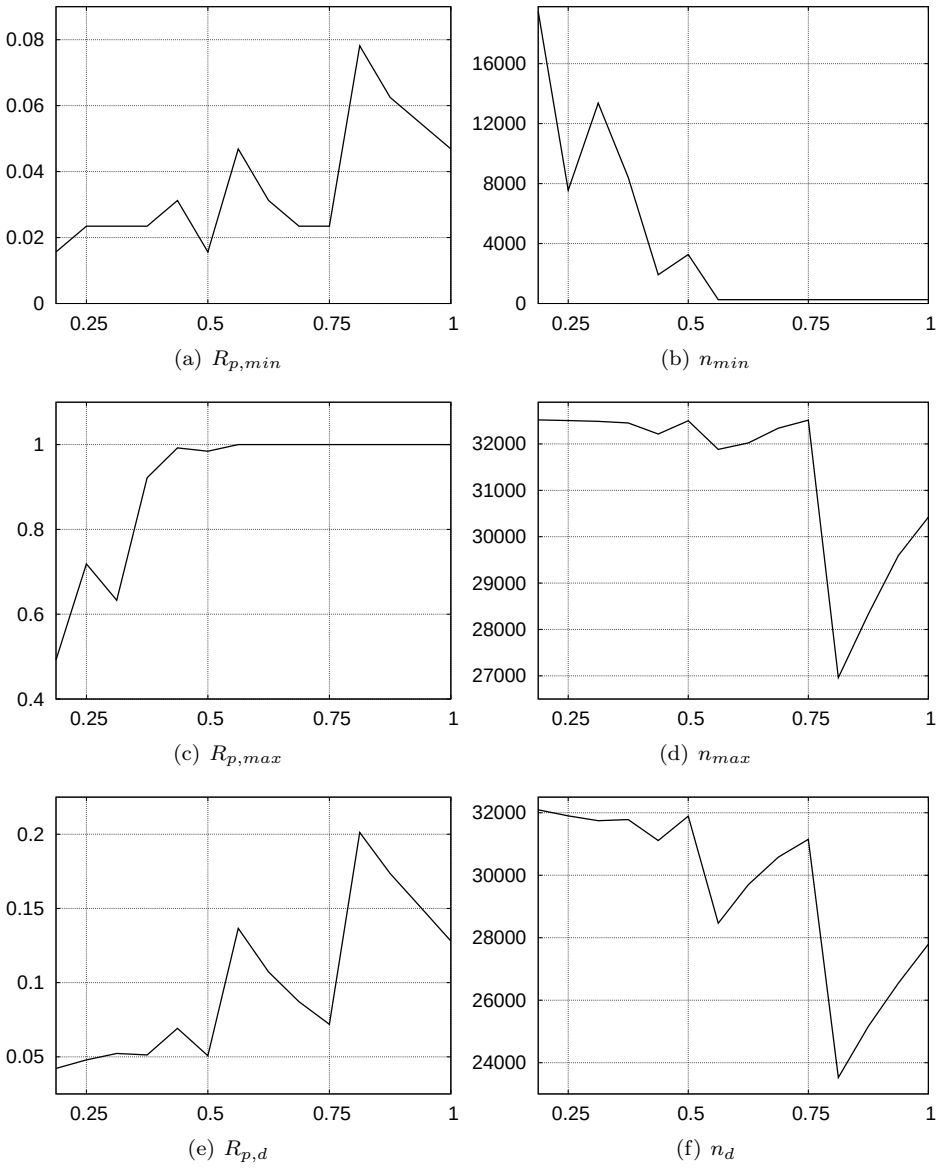


(a) $R_{p,min}$ (b) n_{min}

(c) $R_{p,max}$ (d) n_{max}

(e) $R_{p,d}$ (f) n_d

FIGURE 3. Numerical results concerning differential cryptanalysis of KronCrypt's $(8, 16)$-S-boxes versus $m/(s_2 - s_1)$

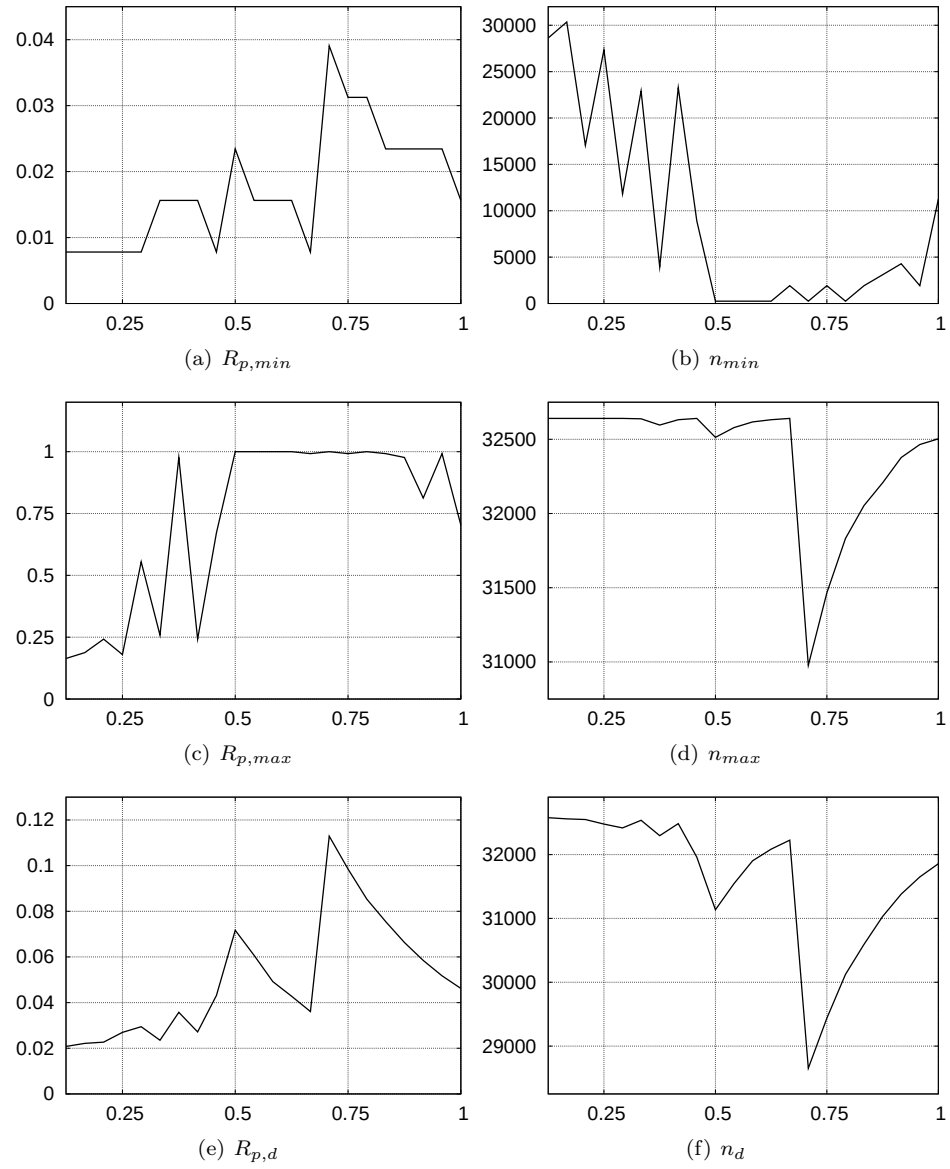


(a) $R_{p,min}$ (b) n_{min}

(c) $R_{p,max}$ (d) n_{max}

(e) $R_{p,d}$ (f) n_d

FIGURE 4. Numerical results concerning differential cryptanalysis of KronCrypt's $(8, 24)$-S-boxes versus $m/(s_2 - s_1)$

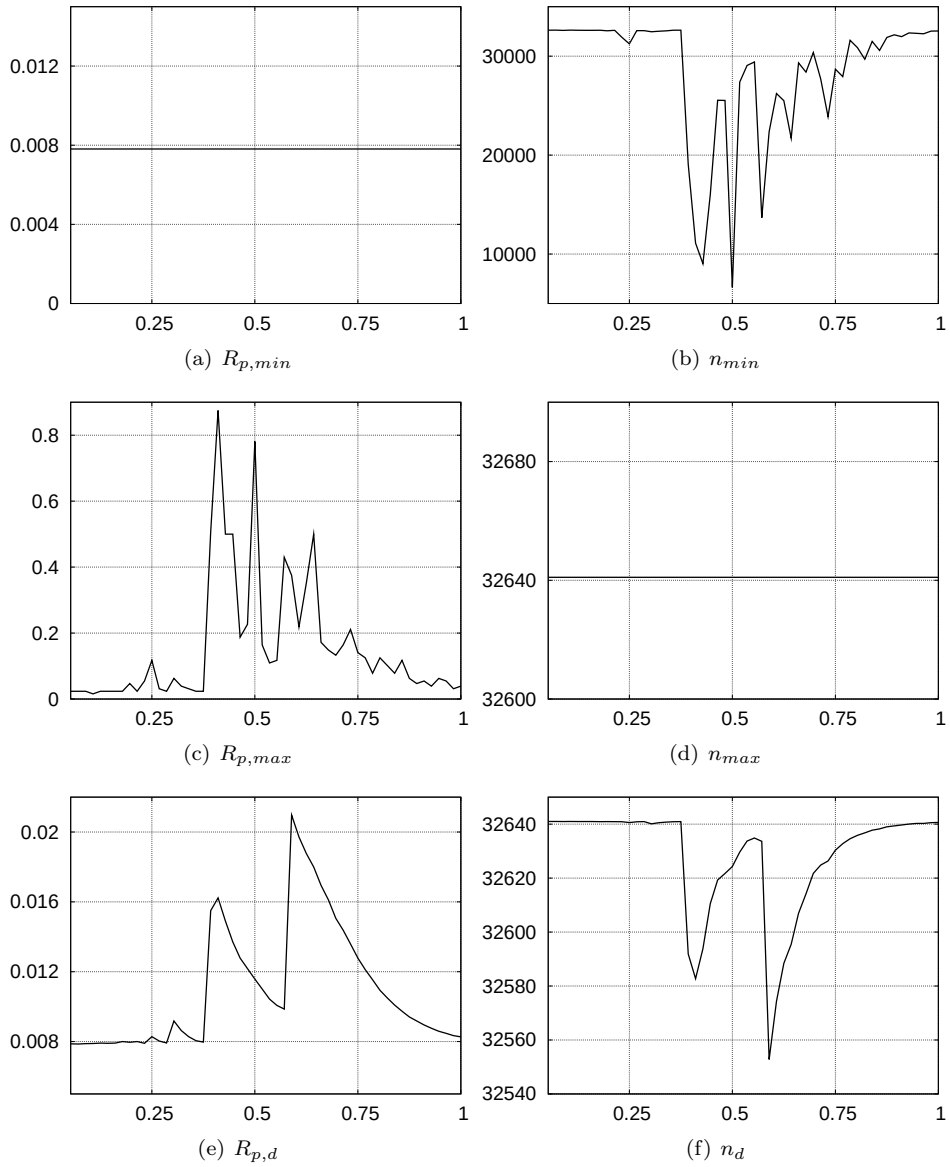


(a) $R_{p,min}$ (b) n_{min}

(c) $R_{p,max}$ (d) n_{max}

(e) $R_{p,d}$ (f) n_d

FIGURE 5. Numerical results concerning differential cryptanalysis of KronCrypt's $(8, 32)$-S-boxes versus $m/(s_2 - s_1)$



(a) $R_{p,min}$ (b) n_{min}

(c) $R_{p,max}$ (d) n_{max}

(e) $R_{p,d}$ (f) n_d

FIGURE 6. Numerical results concerning differential cryptanalysis of KronCrypt's $(8, 64)$-S-boxes versus $m/(s_2 - s_1)$

Appendix C. Test vectors

C.1. Encryptions with $s = 2, m = 3$ und $r = 4$.

κ 29971484512172614953111722835 / 1023485494271462581521517648 79
P 0110000101100010011000110110010001100101011001100110011101101000
0110100101101010011010110110110001101101011011100110111101110000
$r = 1$
L_0 0110000101100010011000110110010001100101011001100110011101101000
R_0 0110100101101010011010110110110001101101011011100110111101110000
κ_1 5018234687389167242 / 17136589972067380361
ρ_1 01101001011010100110101101101100
ρ_2 01101101011011100110111101110000
τ_1 1100011110001110000100000011110011010010000011001100001100100101
τ_2 0010110001001010010000101101111011001100100100001000010001001101
z 1110101111000100010100101110001000011110100111000100011101101000
$r = 2$
L_1 0110100101101010011010110110110001101101011011100110111101110000
R_1 1000101010100110001100011000011001111011111110100010000000000000
κ_2 4984539458730689309 / 17118198018267727342
ρ_1 10001010101001100011000110000110
ρ_2 01111011111110100010000000000000
τ_1 1100100111001011001100111100110101011111001111111111111111100011011
τ_2 0100010010010110010000001101000010111011010111001111011101001111
z 1000110101011101011100110001110111100100011000110000100001010100
$r = 3$
L_2 1000101010100110001100011000011001111011111110100010000000000000
R_2 1110010000110111000110000111000110001001000011010110011100100100
κ_3 3641946298204066007 / 12506654049047454902
ρ_1 11100100001101110001100001110001
ρ_2 10001001000011010110011100100100
τ_1 0100001001000100111001111101101001100111000000011101100000010 1110
τ_2 0100111011001100111000110001101111111111011111111111011101010 10011
z 0000110010001000000001001010111100110000111111000110110101111101
$r = 4$
L_3 1110010000110111000110000111000110001001000011010110011100100100
R_3 1000011000101110001101010010100101001011000001100100110101111101
κ_4 2860501376884794256 / 9414431604641819697
ρ_1 10000110001011100011010100101001
ρ_2 01001011000001100100110101111101
τ_1 0010011000011111100001010000101011100011010001100001111101100111
τ_2 1000000011110011111100101010001000110111100111110011111110000101
z 1010011011101100011101111010100011010100110110010010000011100010
C 0100001011011011011011111101100101011101110101000100011111000110
1000011000101110001101010010100101001011000001100100110101111101

C.2. Encryptions with $s = 4, m = 3$ und $r = 4$.

κ 21282526008087077425019331688 / 73089666176017277308918010773
P 0110000101100010011000110110010001100101011001100110011101101000
0110100101101010011010110110110001101101011011100110111101110000

$r = 1$
L_0 01100001011000100110001101100100011001010110011001100111011010000
R_0 01101001011010100110101101101100011011010110111001101111011100000
κ_1 2025241147057871419 / 6955198800562814117
ρ_1 0110100101101010
ρ_2 0110101101101100
ρ_3 0110110101101110
ρ_4 0110111101110000
τ_1 0000010001011111000001110011100101111001001000101001110101010000
τ_2 0011111110101100101000001001000100101100001010100101001001111100
τ_3 0100010001011010101111101000101110011111000001000010110101101001
τ_4 0100100100001000110111001000011000010001110111100000100001010110
z 1100100101000110101110101011010111100101110100101111010011000011
$r = 2$
L_1 01101001011010100110101101101100011011010110111001101111011100000
R_1 10101000001001001101100111010001100000001011010010010011101010011
κ_2 3849375744588087084 / 13128282104354463059
ρ_1 1010100000100100
ρ_2 1101100111010001
ρ_3 1000000010110100
ρ_4 1001001110101011
τ_1 0011111101011100110100011001001101000011001001001100100101011011
τ_2 1010111000100100001010100101001101010101001111000001011001100000
τ_3 0111101010010011111011011000111100010010111100100101101000010111
τ_4 0101010100110100111101100101111000101000100011111011011010101100
z 0101100100111000000111110001000100000001100001001000100100011110
$r = 3$
L_2 10101000001001001101100111010001100000001011010010010011101010011
R_2 00110000010100100111010001111101011011001110101011100110011011110
κ_3 5238135505307822960 / 17300425148116151117
ρ_1 0011000001010010
ρ_2 0111010001111101
ρ_3 0110110011101010
ρ_4 1110011001101110
τ_1 0000001110101001010011011001111111111100011110011010101000011100 1
τ_2 0001110011010110101000101101100001011011100110000010100011000101
τ_3 1110011001001010011111011000001100001110100011000010110101001111
τ_4 0110111000100010010000100100110100110110000001111001000101010110 1
z 0110101111101000001011010000111100001111111100010001000110011100110
$r = 4$
L_3 00110000010100100111010001111101011011001110101011100110011011110
R_3 11000011110011001111011101010110000001110100110000011011010011 01
κ_4 3497795483847331591 / 12018664703155587250
ρ_1 1100001111001100
ρ_2 1111011101010110
ρ_3 0000011101001100
ρ_4 0001101101001101
τ_1 0110010101110010000000010001100000100011000100100110011110011110

τ_2 0101000110100111100101110010001011110101001011010000100001101000
τ_3 0100110001000101110100010101010011110010110001100011100010100110
τ_4 0101001101101110000010000101110110100100100010000111100000101110
z 1101001001110101011011111101001001101101100011011101000010110010
C 1110001000100111000110111010111100000001011001110011011011011100
1100001111001100111101110101011000000111010011000001101101001101

C.3. Encryptions with $s = 8, m = 3$ und $r = 4$.

κ 30165371238712301410949887311 / 9965700230848344529159637460 8
P 0110000101100010011000110110010001100101011001100110011101101000
0110100101101010011010110110110001101101011011100110101111011110000
$r = 1$
L_0 0110000101100010011000110110010001100101011001100110011101101000
R_0 0110100101101010011010110110110001101101011011100110101111011110000
κ_1 4054236783315847143 / 13393937083576672408
ρ_1 01101001
ρ_2 01101010
ρ_3 01101011
ρ_4 01101100
ρ_5 01101101
ρ_6 01101110
ρ_7 01101111
ρ_8 01110000
τ_1 0100000100010101010100010101110001101111010100100111010100011010
τ_2 0111010100000011100110101001110010011111111110101110101111101 1001
τ_3 1010100011110001111000111101110011010000100110010011101010011000
τ_4 0101101101000010001110111011001100100110011111100110110010101 1000
τ_5 1000111100110000100001001111001101010111001000000011110000010111
τ_6 0100000110000000110111001100100110101101000000111101101011010111
τ_7 0111010101101111001001100000100111011101101001110011110110010110
τ_8 1010100101011101011011110100101000001110010010101010000001010101
z 0110100101101010011010110110110001101101011011100110101111011110000
$r = 2$
L_1 0110100101101010011010110110110001101101011011100110101111011110000
R_1 0000001001010101111001111101101100011010001010100001111101011110
κ_2 4712468829696520393 / 16089361046427246436
ρ_1 00000010
ρ_2 01010101
ρ_3 11100111
ρ_4 11011011
ρ_5 00011010
ρ_6 00101010
ρ_7 00011111
ρ_8 01011110
τ_1 0011100111101110100111000011001100011101111010010000101100010011
τ_2 1100010101100110101110010100111000100110000101011100100100001000
τ_3 1011110100100000000100001011010010001111100001101100011101110011
τ_4 0010010001000101001101101111011011011110110111000111101100101011
τ_5 0000111001110000111011100010100000101010000010000101111111110000

τ_6 00111011111000000001101110101011101010110011011100100011011111010
τ_7 01101110100101100100000011001010101101000001101111111110000010101
τ_8 10111010001000000101111110110110100000001010110111011101111101111
z 10111100011101000110100110111001110010001101011010110011011010 11
$r = 3$
L_2 00000010010101011110011111011011000110100010101000011111010111 10
R_2 11010101000111100000001011010101101001011011100011011100000011011
κ_3 3865162501421527814 / 8863525713655776461
ρ_1 11010101
ρ_2 00011110
ρ_3 00000010
ρ_4 11010101
ρ_5 10100101
ρ_6 10111000
ρ_7 11011100
ρ_8 00011011
τ_1 01001100000110111110001010000000010000011001111001100110110000111
τ_2 00100011110001111010011001110110010110010110110001111111011101 10
τ_3 00000110110001011100101010000100110100111100001011100001001010 11
τ_4 01001100000110111110001010000000010000011001111001100110110000111
τ_5 01001001110010001000000111011101111101111101011001111000000111100
τ_6 00100000101111110100001010111110101001001110100011100100111001 00
τ_7 00010000010111111010000101011111010100100111010001110010011100 10
τ_8 00100100100101101101010100111100110010001111001010100000010111000
z 10010000000010100001101111111001100111001010110011000011100111 01
$r = 4$
L_3 11010101000111100000001011010101101001011011100011011100000011011
R_3 10010010010111111111110000100010100001101000011011011100110000 11
κ_4 3913009352745776291 / 9533874608435290511
ρ_1 10010010
ρ_2 01011111
ρ_3 11111100
ρ_4 00100010
ρ_5 10000110
ρ_6 10000110
ρ_7 11011100
ρ_8 11000011
τ_1 00111001100111111000101111101101100110001110110010101011010000 01
τ_2 01110101111010011100001001001011011011011110101011011101100100 01
τ_3 01111000110110101111010000001110001001001110010010100011100111 11
τ_4 00010001010000100110100100111111000001111111111001001001101111010
τ_5 00111111010011111000111011001010011001011111000100101011011110000
τ_6 00111111010011111000111011001010011001011111000100101011011110000
τ_7 01101101010100101010000100000000110101101110100100101111000111 01
τ_8 00011111101001111100011101100101001100101111100010010111011111000
z 10000110001001111100100111111010100010100001101001010001011 01010
C 01010011001110011100101100101111100101111101000101000110101110001
100100100101111111111110000100010100001101000011011011100110000 11

References

[1] C. E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, (28):656–715, 1949.

[2] J. B. Kam and G. I. Davida. Structured design of substitution-permutation encryption networks. *IEEE Transactions on Computers*, 28(10):747–753, 1979.

[3] H. Feistel. Cryptography and computer privacy. *Scientific American*, 228(5):15–23, Mai 1973.

[4] H. Feistel, W. A. Notz, and J. L. Smith. Some cryptographic techniques for machine-to-machine data communications. *Proceedings of the IEEE*, 63(11):1545–1554, November 1975.

[5] A. F. Webster and S. E. Tavares. On the design of s-boxes. In H. C. Williams, editor, *Advances in Cryptology - CRYPTO '85*, number 218 in Lecture Notes in Computer Science, pages 523–534. Springer-Verlag, 1986.

[6] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Clarendon Press, Oxford, fifth edition, 1979.

[7] H. Loo-Keng. *Introduction to Number Theory*. Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[8] A. Khintchine. *Kettenbrüche*. Teubner, Leipzig, 2. edition, 1949.

[9] E. Biham and A. Shamir. Differential cryptanalysis of des-like cryptosystems. In A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90*, number 537 in Lecture Notes in Computer Science, pages 2–21. Springer-Verlag, 1991.

[10] E. Biham and A. Shamir. Differential cryptanalysis of des-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[11] H. M. Heys. A tutorial on linear and differential cryptanalysis. *Cryptologia*, 26(3):189–221, 2002.

[12] R. Merkle. Fast software encryption functions. In A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90*, number 537 in Lecture Notes in Computer Science, pages 476–501. Springer-Verlag, 1991.

[13] H. Gilbert and P. Chauvaud. A chosen plaintext attack of the 16-round khufu cryptosystem. In Y. G. Desmedt, editor, *Advances in Cryptology - CRYPTO '94*, number 839 in Lecture Notes in Computer Science, pages 359–368. Springer-Verlag, 1994.

[14] E. Biham, A. Biryukov, and A. Shamir. Miss in the middle attacks on idea, khufu and khafre. In L. R. Knudsen, editor, *Fast Software Encryption, 6th International Workshop '99*, number 1636 in Lecture Notes in Computer Science, pages 124–138. Springer-Verlag, 1999.

[15] B. Schneier. Description of a new variable-length key, 64-bit block cipher (blowfish). In R. Anderson, editor, *Fast Software Encryption: Cambridge Security Workshop Proceedings '93*, number 809 in Lecture Notes in Computer Science, pages 191–204, 1994.

[16] S. Vaudenay. On the weak keys of blowfish. In D. Gollmann, editor, *Fast Software Encryption: Third International Workshop '96*, number 1039 in Lecture Notes in Computer Science, pages 27–32. Springer-Verlag, 1996.

[17] E. Biham. On matsui's linear cryptanalysis. In A. De Santis, editor, *Advances in Cryptology - EUROCRYPT '94*, number 950 in Lecture Notes in Computer Science, pages 398–412. Springer-Verlag, 1995.