On the Duality of Probing and Fault Attacks

Berndt M. Gammel and Stefan Mangard

Infineon Technologies AG
Munich, Germany

Feb. 12, 2009

Berndt.Gammel@infineon.com
Stefan.Mangard@infineon.com

Abstract. In this work we investigate the problem of simultaneous privacy and integrity protection in cryptographic circuits. We consider a white-box scenario with a powerful, yet limited attacker. A concise metric for the level of probing and fault security is introduced, which is directly related to the capabilities of a realistic attacker. In order to investigate the interrelation of probing and fault security we introduce a common mathematical framework based on the formalism of information and coding theory. The framework unifies the known linear masking schemes. We proof a central theorem about the properties of linear codes which leads to optimal secret sharing schemes. These schemes provide the lower bound for the number of masks needed to counteract an attacker with a given strength. The new formalism reveals an intriguing *duality principle* between the problems of probing and fault security, and provides a unified view on privacy and integrity protection using error detecting codes. Finally, we introduce a new class of linear tamper-resistant codes. These are eligible to preserve security against an attacker mounting simultaneous probing and fault attacks.

Keywords. probing attacks, fault attacks, side channel attacks, coding theory, secret sharing, secure computation.

1 Introduction

In the traditional cryptographic setting it is assumed that the adversary has only *black-box* access to the cryptographic algorithm. He can query the apparatus executing the algorithm with inputs of his choice and observe the answer (chosen plain text scenario). The secret key has been loaded into the device in the outset and is not accessible to the adversary. A further basic assumption is that the attacker has full knowledge of the algorithm—he can build a model of the device and query it based on his guess for the secret.

In practice, however, the black-box assumption is realized rarely. This applies particularly to a device which can be physically accessed by the attacker during operation. Present-day society heavily relies on the security of such cryptographic devices. Examples are electronic ID cards, smart cards for payment purposes, mobile phones, network devices, and personal computers. All of these can be easily seized by an attacker. In this setting both the *privacy* and the *integrity* assumption inherent in the black-box model do not hold any more:

Firstly, due to the physical nature of computation there is always some amount of information leakage from intermediate stages of the computation. Secondly, information from intermediate stages can be actively probed without disturbing the computation. Thirdly, the physical processes taking place during computation can be actively disturbed in order to induce faulty intermediate values. These three fundamental physical constraints on cryptographic computation are known as the *side-channel* (SCA), the *probing* (PRA), and the *fault* (FA) attack scenario, respectively.

There are many physical sources for side-channel information leakage during the execution of an algorithm which is otherwise secure under the black-box assumption. Especially the analysis of the information leakage on the power line of a physical device has had considerable impact on the art of secure cryptographic algorithm implementation during the last decade [13]. Differential Power Analysis (DPA) represents an actual threat for commonly used cryptographic devices, because the work factor for a DPA attack is comparably moderate with respect to the equipment, the skill, and the computing power [6, 15, 17].

Probing attacks can be considered as even more powerful than SCA attacks, because the attacker monitors a *local* physical value (e.g. a voltage level on some wire), which is directly related to a data value. There are many sophisticated probing techniques available ranging from the placement of needles to optical probing methods [1, 4]. Throughout this paper we will use the term *probe* for any method that allows to record a local value in a computation.

Both SCA and PRA attacks are highly efficient if they are used in the differential setup. Here, a few carefully chosen local values are probed and traces for several runs of the algorithm with different inputs are recorded. The analysis of the collected data values can already reveal the whole key or at least reduce the key space to a level that allows a brute force attack. Theoretical results on highly efficient differential probing attacks (DPRA) on private key and public key cryptosystems have recently been reported [9, 19].

The third class of physical attacks, fault attacks, is particularly interesting, because the violation of integrity can be exploited to break privacy [1, 22]. It has been demonstrated that the injection of a small number of a specific kind of faults can be used to break private key [3] and public key [5] cryptosystems.

Clearly, there is a tireless quest for countermeasures against all of these kinds of attacks. As physical security seems to be out of reach (in the sense that anything can be proven) countermeasures based on mathematical reasoning are of particular interest. However, in the field of probing attacks the impossibility of obfuscation [2] rules out the security against an all-powerful attacker. Hence, the capabilities of the attacker have to be restricted by model assumptions [18]. *Secret sharing* schemes have been proposed to provide privacy against an attacker who is limited to place at most q needles [12]. In the context of DPA secret sharing schemes have been introduced as *data masking*. For example, in a simple masking scheme with two shares a data value x is lifted to the pair of values $(x \oplus m, m)$, where the mask value m has the properties of a uniformly distributed random variable. Obviously the pair $(x \oplus m, m)$ is secure against probing with one needle.

The detection (and correction) of faults has a long history in coding theory [14, 20]. Trivially, the capability to detect errors requires the introduction of information redundancy. An appropriate error detection code can be devised depending on the kind of errors the attacker is able to inject. If, for example, it can be assumed that an attacker is able to flip at most f bits in a memory word, and the attack should be detected with certainty, an error detection code with minimum distance $f + 1$ could be used. On the other hand error detecting codes have also be used for the construction of secret sharing schemes [16].

The crucial challenge is, however, to provide security against an attacker of limited, but considerable power, who is able to perform both probing and fault attacks. First theoretical foundations for such *tamper-resistant* devices have been laid in recent works [8, 11]. Both, secret sharing schemes and error detection codes introduce redundancy into the realization of the cryptographic device. However, little is known about the interrelation between simultaneous probing and fault resistance countermeasures.

This work is organized in four sections. In Section 2 we define a concise metric for the level of probing security, which is directly related to the capabilities of a realistic attacker. In order to investigate the interrelation of probing security and fault security we introduce a common mathematical language within the framework of information and coding theory. In Section 3 we prove a theorem about the properties of codes which can be used for the construction of optimal masking schemes. In particular, we describe linear codes which are optimal with respect to the number of introduced masks (OPS codes). The new formalism reveals an intriguing *duality principle* between the problems of probing and fault security. In Section 4 we compare the information leakage of optimal privacy preserving codes and classical masking schemes. Finally, in Section 5 we fuse privacy and integrity protection and introduce a new class of optimal tamper-resistant codes (OTR codes), which are eligible to preserve security against an attacker mounting simultaneous probing and fault attacks.

2 Preliminaries

It is suggestive to describe an arbitrary apparatus used to perform a cryptographic computation in terms of an (electronic) switching circuit. Then the collection of interconnects between the switching elements, the *wires* $x_1, x_2, \ldots, x_k$, carry the complete intermediary state information. Each wire x_i transports an information signal $x_i(t)$ as a function of time. To simplify notation, we consider only discrete evaluation cycles in time, $t = 1, 2, \ldots, T$, and binary signal values on the wires throughout this paper. This model fits CMOS circuit technology already very well, which is today the dominating technology for the implementation of electronic (cryptographic) devices. Hence we can express all $x_{it} = x_i(t)$ by elements of the binary field $\mathbb{F}_2$. A generalization to n-ary circuit logic is immediate. Also the problem of probing analogue signals can be described in the presented formalism by quantizing and mapping the continuum of analogue values to an appropriate number of discrete values. We are now ready to define probing attacks given an adversary of quantifiable strength. All the definitions are in accordance with the definitions of differential cryptanalysis, differential fault attacks, and differential power analysis (of order q).

Definition 1. *In a* ***Probing Attack of Order q, PRA(q),*** *an adversary is capable of obtaining the values* $(x_{1,t}, x_{2,t}, \ldots, x_{q,t})$ *on* q *wires of his choice in a circuit for an arbitrary number of evaluation cycles* $t = 1, 2, \ldots, T$.

Definition 2. *In a* ***Differential Probing Attack of Order q, DPRA(q),*** *an adversary is capable of obtaining the values* $\mathbf{x}_t = (x_{1,t}, x_{2,t}, \ldots, x_{q,t})$ *on* q *wires of a circuit for an arbitrary number of evaluation cycles* $t = 1, 2, \ldots, T$*. Furthermore,* $\mathbf{x}_t$ *is related to some known information (e.g. the cipher text) and a secret* $\mathbf{k}$ *via a set of* λ *equations* $f_i(\mathbf{x}_t, \mathbf{c}_t, \mathbf{k}) = 0$*,* $1 \leq i \leq \lambda$*. By collecting multiple different pairs* $(\mathbf{x}_t, \mathbf{c}_t)$ *and evaluating these equations the adversary determines some or all bits of the secret* $\mathbf{k}$.

It should be noted that DPRA(q) attacks can be highly efficient. DPRA(q) works in the cipher text only scenario and is even more efficient in a known plain text setting. Probing one bit at a carefully selected position and collecting the values of a few encryptions can already reveal the whole key or at least reduce the key space to a work factor that allows a brute force attack. Examples for efficient DPRA(1) and DPRA(3) attacks on the AES are given in [19]: The information collected from a single probe during 168 encryptions reveals the secret key. In a known plain text setting three probes and 26 cipher texts are already sufficient. Less efficient attacks on DES, RC5, and public cryptosystems have already been described in an early work [9].

Let us now formally consider the state of the k wires of the circuit at time t as a message word

$$\mathbf{x}_t = (x_{1,t}, x_{2,t}, \ldots, x_{k,t}) \in \mathcal{X} = \mathbb{F}_2^k.$$

in some message space $\mathcal{X}$. If an attacker has access to a small, but carefully selected set of q coordinates of the message word over some period of time, he will generally be able to extract the secret in a DPRA(q) attack. Privacy can be preserved if the message is augmented by a number of s masks

$$\mathbf{m}_t = (m_{1,t}, m_{2,t}, \ldots, m_{s,t}) \in \mathcal{M} = \mathbb{F}_2^s.$$

Definition 3. *A **mask** m_{it} is defined to be a value (on a wire) which can be described as an independent and uniformly distributed binary random variable.*

In practical circuit designs a balanced i.i.d. sequence of mask bits could be generated by a random bit stream generator (RBG). This sequence is routed on a wire to a destination circuit element in which the mask bits are finally combined with message bits. The crucial point is the setup of an optimal *masking scheme* against an adversary with given probing capabilities. A masking scheme describes the way the vector of masks m_t is combined with the message vector x_t in each evaluation cycle. In the following we show that the problem of finding an optimal masking scheme can be expressed as a channel coding problem.

In general we have an encoding function g, which is a map

$$\begin{aligned} g : \mathcal{X} \times \mathcal{M} &\to \mathcal{Y} \subseteq \mathbb{F}_2^N \\ (\mathbf{x}, \mathbf{m}) &\mapsto \mathbf{y} = (y_1, y_2, \ldots, y_N) \end{aligned}$$

with $n = s + k$, $N \geq n$. The dimension of the image is equal to n, because we must be able to decode the message and we assume that every mask is used. If no redundancy for integrity protection is introduced we have $N = n$. In the next sections we consider pure masking schemes ($N = n$). Finally, in section 5 we will introduce tamper-resistant codes which are both, capable of preserving privacy and integrity ($N > n$).

The following definition is crucial:

Definition 4. *A circuit is **probing secure of order q**, we write **PS(q)**, if for each choice of indices $i_1, i_2, \ldots, i_q$ with $1 \leq i_1 < i_2 < \cdots < i_q \leq n$ the condition*

$$I(X_1, X_2, \ldots, X_k; Y_{i_1}, Y_{i_2}, \ldots, Y_{i_q}) = 0$$

on the mutual information [7] holds, where the message X_i and the masked message Y_i are represented by discrete random variables with $p(x_i) = \Pr\{X_i = x_{i,t}\}$ and $p(y_i) = \Pr\{Y_i = y_{i,t}\}$, respectively, at each point in time t.

In other words, a circuit is PS(q), if it does not leak any information on the message bits x_i to an attacker, who can simultaneously probe q wires y_i of his choice over an arbitrary period of time. If this condition holds the attack will fail regardless of whether a simple or differential probing setup is used according to Definition 1 or 2, respectively. It should be noted, that Definition 4 is a natural generalization of the notion of correlation-immunity of a Boolean function, introduced by Siegenthaler [21]. This definition is also in accordance with the definition of a power analysis of order q, *cf.* [15].

At this point a natural question arises:

> *What is the lower bound for the number of masks needed to protect a circuit with k wires against an adversary who is able to mount a probing attack of order q?*

This information is important for the design of privacy preserving masked circuits, because *circuit size increases strongly with the number of masks.* Luckily, experience from physical failure analysis shows that in recent IC technologies access to single wires becomes painfully difficult [4]. Hence the relation between the number of probes and the work factor of the attack is also a strongly increasing function. Therefore, in order to design an optimal privacy preserving circuit for a work factor which is commensurate with the protection period and value of the secret, it is necessary to know the lower bound for the number of masks. If the optimal number is known, this value can be used as a target or benchmark for designs of cryptographic circuits. The construction of the masking schemes presented in the next section is based on linear block codes. These linear schemes are optimal in the sense that they require the smallest number of masks for a given number of information bits.

3 Optimal linear masking schemes, OPS-Codes

We shall use the following notation: $\mathbf{G}_{ij}$ is a $i \times j$ matrix over $\mathbb{F}_2$, $\mathbf{I}_k$ is the $k \times k$ unit matrix, $\mathbf{O}_{ij}$ is the $i \times j$ zero matrix, and $\mathbf{1}_k$ is the row vector of k ones. Furthermore, $\mathbf{x}^T$ is the transposed vector (matrix) of $\mathbf{x}$. The message augmented with the vector of masks is denoted by the row vector $\mathbf{u} = (\mathbf{x}, \mathbf{m})$. We can express any linear masking scheme by

$$\mathbf{y} = \mathbf{uG},$$

where $\mathbf{G}$ is the generator matrix of the code. As usual the parity check matrix is defined by

$$\mathbf{Hy}^T = 0,$$

and we have the relations

$$\mathbf{H} = (\mathbf{Q}|\mathbf{I}), \quad \mathbf{G} = (\mathbf{I}|\mathbf{Q}^T) \tag{1}$$

choosing the systematic form of the code.

We now define the canonical form of the code for a linear masking scheme.

Proposition 1. *The $n \times n$ generator matrix $\mathbf{G}$ for a masking scheme with s masks and $n - s$ data values can be written in the following canonical form:*

$$\mathbf{G} = \left(\frac{\mathbf{I}_{n-s}|\mathbf{O}_{n-s,s}}{\mathbf{P}^q_{s,n}} \right) \quad \textit{with} \quad \mathbf{P}^q_{s,n} = (\mathbf{Q}_{s,n-s}|\mathbf{I}_s). \tag{2}$$

Proof. Using elementary row operations and column interchanges the generator matrix of a code can be converted into that of an equivalent code in the given canonical form. □

In the canonical form the first $k = n - s$ coordinates y_i of a code word $\mathbf{y}$ are given by the corresponding message bits plus a linear combination of masks, $y_i = x_i + \sum_{j=1}^{s} m_j Q_{ji}, 1 \leq i \leq k$. The last s coordinates are single mask bits.

Definition 5. *We shall call* $\mathbf{P}^q_{s,n}$ *the* ***probing matrix of order q****.*

It has s rows (number of masks) and $n = k + s$ columns (number of masks plus data bits). The probing security of the corresponding masking scheme is indicated by the superscript q. We now provide some examples.

The classical one-time pad (OTP) encryption scheme of Gilbert Vernam [23] follows in a natural way as one special case. Every bit of the message is masked with an individual key stream (mask) bit. OTP provides perfect secrecy under the black-box assumption for the masks. However, in the setting of physically observable computation the masks are also subject to the q-th order probing attack. In our new formalism Vernam's masking scheme is defined by the probing matrix

$$\mathbf{P}^1_{k,2k} = (\mathbf{I}_k | \mathbf{I}_k).$$

Obviously the OTP scheme is only PS(1). An attacker with two needles is able to probe a masked value and the corresponding mask bit and can therefore compromise the security of the masking scheme. With one needle no attack is possible. It is important to point out that there are other PS(1) masking schemes. One mask is already sufficient to protect an arbitrary number of k information bits against a PA(1) attack. The corresponding canonical probing matrix is

$$\mathbf{P}^1_{1,k} = (\mathbf{1}_k | 1).$$

We note that this matrix is identical to the H-Matrix of a single parity check code for k data bits. Another trivial case is the construction of the PS(q) masking scheme for maximum probing security of one data bit. Clearly we need $s = q$ masks to expand one information bit to $q + 1$ shares. The corresponding canonical probing matrix

$$\mathbf{P}^q_{q,q+1} = (\mathbf{1}^T_q | \mathbf{I}_q)$$

is the H-Matrix of a repetition code. Inspired by these observations we can now formulate one of our main results.

Theorem 1. *A linear masking scheme is probing secure of order* q*, if and only if the probing matrix* $\mathbf{P}^q_{s,n}$ *has the property that any* q *columns are linearly independent.*

Proof. Let us denote the ith column of the probing matrix by P_i so that $\mathbf{P}^q_{s,n} = (P_1, P_2, \ldots, P_n)$.

To show the necessity of the condition, assume to the contrary that there are h columns of $\mathbf{P}^q_{s,n}$ with $h \leq q$ such that $P_{i_1} + \cdots + P_{i_h} = \mathbf{0}$. By summing up the corresponding $y_{i_1}, \ldots, y_{i_h}$ all involved mask bits will cancel out resulting in $y_{i_1} + \cdots + y_{i_h} = x_{j_1} + \cdots + x_{j_b}$. It follows that $I(x_1, \ldots, x_k; y_{i_1} + \cdots + y_{i_h}) = 1$ which implies that $I(x_1, \ldots, x_k; y_{i_1}, \ldots, y_{i_h})$ cannot be zero, and the masking scheme cannot be probing secure of order q according to Definition 4.

To show the sufficiency we consider the table of function values of the function $f : \mathbf{u} \in \mathbb{F}_2^n \mapsto \mathbf{uG} \in \mathbb{F}_2^n$. This is a $2^n \times 2n$ matrix denoted by $[\mathbf{u}, \mathbf{uG}]$ where $\mathbf{u}$ runs through the elements of $\mathbb{F}_2^n$.

Recall that $\mathbf{u}$ has the form $\mathbf{u} = (\mathbf{x}, \mathbf{m})$, where $\mathbf{x} = (x_1, \ldots, x_k)$ is the vector of all k information bits, and $\mathbf{m} = (m_1, \ldots, m_s)$ is made up by the s masking bits. Because of the linearity of f, we can add any two rows of $[\mathbf{u}, \mathbf{uG}]$, and the sum will be again a row of $[\mathbf{u}, \mathbf{uG}]$. In other words, the rows of the matrix $[\mathbf{u}, \mathbf{uG}]$ constitute an n-dimensional vector space over $\mathbb{F}_2$ denoted by W which is a subspace of $\mathbb{F}_2^{2n}$.

Let $1 \leq i_1 < i_2 < \cdots < i_q \leq n$ be arbitrary. Set $[\mathbf{u}, \mathbf{uG}] = (A_1, \ldots, A_n; B_1, \ldots, B_n)$. For the proof the following $2^n \times (k+q)$ submatrix $\mathbf{M}$ of $[\mathbf{u}, \mathbf{uG}]$ is essential, where

$$\mathbf{M} = (A_1, \ldots, A_k; B_{i_1}, \ldots, B_{i_q}). \tag{3}$$

We claim that among the 2^n rows of $\mathbf{M}$ there are exactly 2^{s-q} all-zero rows. We will make use of the standard basis vectors of the vector space $\mathbb{F}_2^n$ given by

$$\mathbf{e}_1 = (1, 0, \ldots, 0), \quad \mathbf{e}_2 = (0, 1, \ldots, 0), \quad \ldots, \quad \mathbf{e}_n = (0, 0, \ldots, 1).$$

Consider the s standard basis vectors $\mathbf{e}_{k+1}, \mathbf{e}_{k+2}, \ldots, \mathbf{e}_{k+s}$. The 2^s linear combinations (over $\mathbb{F}_2$) of these vectors will produce *all* row vectors of $\mathbb{F}_2^n$ whose first k coordinates are zero.

Let $V \subset \mathbb{F}_2^n$ be the vector space spanned by $\mathbf{e}_{k+1}, \ldots, \mathbf{e}_{k+s}$. Clearly, $\dim(V) = s$. By hypothesis, the q columns $P_{i_1}, \ldots, P_{i_q}$ of the probing matrix $\mathbf{P}^q_{s,n}$ are linearly independent. This implies that the matrix $B = (B_{i_1}, \ldots, B_{i_q})$ has rank q. Consider the linear mapping

$$\phi : \mathbf{v} \in V \mapsto \mathbf{v}B \in \mathbb{F}_2^q.$$

By elementary linear algebra,

$$\dim(V) = \dim(\ker(\phi)) + \dim(\mathrm{Im}(\phi)).$$

Since $\dim(V) = s$, and $\dim(\mathrm{Im}(\phi)) = \mathrm{rank}(B) = q$, we conclude that $\dim(\ker(\phi)) = s - q$. Thus there are 2^{s-q} vectors $\mathbf{v} \in V$ for which $\mathbf{v}B = \mathbf{0}$. It follows that the matrix $\mathbf{M}$ in (3) has 2^{s-q} all-zero rows.

It is now easy to see, that the set U of all vectors of W, which are zero in positions $1, \ldots, k, i_1, \ldots, i_q$, forms a $(s-q)$-dimensional subspace of the n-dimensional vector space W. Consider the cosets $w + U$, $w \in W$, of the subspace U in W. The distinct cosets of U have all the same cardinality, namely 2^{s-q}, the cardinality of U. This implies that among the 2^n rows of the matrix $\mathbf{M}$ in (3) each of the vectors of $\mathbb{F}_2^{k+q}$ occurs exactly 2^{s-q} times or, equivalently, with probability 2^{s-q-n}. Thus, for $\mathbf{x} = (x_1, \ldots, x_k)$ and $\mathbf{z} = (y_{i_1}, \ldots, y_{i_q})$, we have $p(\mathbf{x}, \mathbf{z}) = 2^{s-q-n}$, $p(\mathbf{x}) = 2^{-k}$, and $p(\mathbf{z}) = 2^{-q}$. Since $k = n - s$ it follows that the mutual information, *cf.* Definition 4, of $\mathbf{x}$ and $\mathbf{z}$ vanishes:

$$I(\mathbf{x}; \mathbf{z}) = \sum_{\mathbf{x}} \sum_{\mathbf{z}} p(\mathbf{x}, \mathbf{z}) \log_2 \frac{p(\mathbf{x}, \mathbf{z})}{p(\mathbf{x}) p(\mathbf{z})} = 2^{n-s+q} 2^{s-q-n} \log_2 \frac{2^{s-q-n}}{2^{-k} 2^{-q}} = 0.$$

□

Theorem 1 shows that the problem of constructing a masking scheme for a given order of probing security PS(q) is equivalent to the problem of constructing a code with given minimum distance $d_{\min} = q + 1$. This is immediate, if we recall that the minimum distance $d_{\min}$ of a linear code equals the smallest positive integer n such that there are n columns in the parity check matrix which are linearly dependent [14].

The difference in the case of masking is, that the probing matrix has to meet the constraints that are usually imposed on the parity check matrix in the setting of channel coding. Hence we can state:

> *In the coding theoretical sense the problem of preserving privacy in a circuit subject to probing attacks is dual to the problem of preserving integrity in a circuit subject to fault attacks.*

In Section 5 the duality aspect will be treated further by considering simultaneous probing and forcing attacks.

Based on Theorem 1 we now provide constructions for codes with different levels of probing security, which are optimal with respect to the number of masks.

Definition 6. *An* ***Optimal Probing Secure Code, OPS(n,k;q),*** *is a linear block code of length n and dimension k which provides probing security of order q, PS(q), for k information bits and has the minimal number $s = n - k$ of mask bits.*

By virtue of Theorem 1 the existing results from the field of coding theory can be used for the construction of good masking schemes for any order of probing security. The construction of optimal masking schemes for PS(2) and PS(3) is quite easy:

- The canonical probing matrix $\mathbf{P}^2_{n-k,n}$ of the OPS(n,k;2) code is identical to the parity check matrix of a (shortened) $[2^s - 1, 2^s - s - 1, 3]$ Hamming code. An example for the OPS(7,4;2) masking scheme can be found in Appendix A.
- The canonical probing matrix $\mathbf{P}^3_{n-k,n}$ of the OPS(n,k;3) code is identical to the parity check matrix of a (shortened) $[2^{s-1}, 2^{s-1} - s, 4]$ Hsiao code [10]. An example for the OPS(16,11;3) masking scheme can be found in Appendix B.

		order of probing security q											
		1	2	3	4	5	6	7	8	9	10	11	12
	1	∞											
	2	∞	3										
	3	∞	7	4									
	4	∞	15	8	5								
	5	∞	31	16	6	6							
s	6	∞	63	32	8	7	7						
	7	∞	127	64	11	9	8	8					
	8	∞	255	128	17	12	9	9	9				
	9	∞	511	256	23	18	11	10	10	10			
	10	∞	1023	512	*34-37*	24	15	12	11	11	11		
	11	∞	2047	1024	*48-60*	*35-37*	23	16	12	12	12	12	
	12	∞	4095	2048	*66-88*	*49-61*	24	24	14	13	13	13	13

Table 1. Maximum lengths n of OPS(n,k;q) codes for masking schemes given the number of masks s and the order of probing security q.

For probing security PS(q) with order $q > 3$ the task of finding the optimal code becomes already nontrivial. Table 1 shows the upper bound on the length n of the optimum code given the number of masks $1 \leq s \leq 12$ and the probing security $1 \leq q \leq 12$. The condensed information in Table 1 reflects various sources—books, articles, as well as online data bases. For some values only intervals for the maximum possible length can be given, because only lower and upper bounds for the minimum distances of the corresponding codes are known. These table entries are italicized.

Probing security of order PS(1) for an unbounded number of information bits can already be achieved by introducing one mask (Tab. 1, column 1). The maximum lengths for OPS(n,k;2) and OPS(n,k;3) masking schemes are $2^s - 1$ and 2^{s-1}, respectively. These are shown in columns 2 and 3. The probing matrices correspond to the mentioned Hamming and Hsiao codes, respectively. The trivial OPS(n,1;n-1) codes, which provide maximum probing security for one data bit, are found on the diagonal line. Some comments on a few more selected entries of the table are given: The entry for $q = 4, s = 8$ corresponds to the $[17, 9, 5]$ quadratic residue code which generates an OPS(17,9;4) masking scheme. This scheme will be used as an example in the following section, *cf.* also Appendix C. The entries for $q = 6, s = 11$ and $q = 7, s = 12$ are the $[23, 12, 7]$ Golay code $\mathcal{G}_{23}$ and the $[24, 12, 8]$ Golay code $\mathcal{G}_{24}$, respectively. It should be noted that the maximal length of a code for a given number of masks decreases rapidly with increasing order of probing security. Hence, achieving a high order of probing security in a circuit, say $q \geq 4$, becomes inefficient in terms of the number of masks. PS(2) and PS(3) masking schemes, however, are efficient and may be of high practical relevance.

4 Information leakage of OPS Masking schemes

Let us consider a simple probing attack PA(q) on a masked circuit for increasing order $q = 1, 2, \ldots$. Obviously, with an increasing number of probes q the circuit will leak more and more information. For the moment we do not take into account the possibility that a differential DPRA(q) attack might reveal the total information already for a small number of probes. Furthermore, let us consider an intelligent attacker who follows the optimum strategy in placing the probes. The incremental information leakage for different masking schemes will generally look different. In Fig. 1 the information leakage of a circuit protected by Vernam's OTP scheme ($\times$), *i.e.* one mask per information bit, an OPS(16,11;3) masking scheme with 5 mask bits ($\bigtriangledown$) and an OPS(17,9;4) masking scheme with 8 mask bits ($\bigtriangleup$) are compared. For reference purposes the information leakage of an unmasked circuit ($+$) is also shown. The unmasked circuit exhibits a constant information leakage rate of one bit per probe. (We assume that the information on the wires is statistically independent.) The Vernam masking scheme shows a constant average leakage rate of 0.5 bit per probe, because the best attack strategy is to probe one masked wire and the corresponding mask. In contrast, the OPS masking schemes leak no information up to the built-in level of probing security, which is 3 and 4 needles, respectively, in our example. For an increasing number of probes the information leakage is still below that of the Vernam scheme. The OPS(16,11;3) masking scheme reaches the Vernam leakage rate at 7 probes, while the OPS(17,9;4) scheme arrives at this rate not until 15 probes. Asymptotically all OPS leakage rates converge to a rate of one bit per probe like in an unmasked circuit. Metaphorically speaking an OPS masking scheme draws on a private credit to bravely resist attacks with a moderate number of needles, but the scheme collapses, if a critical charge is reached.

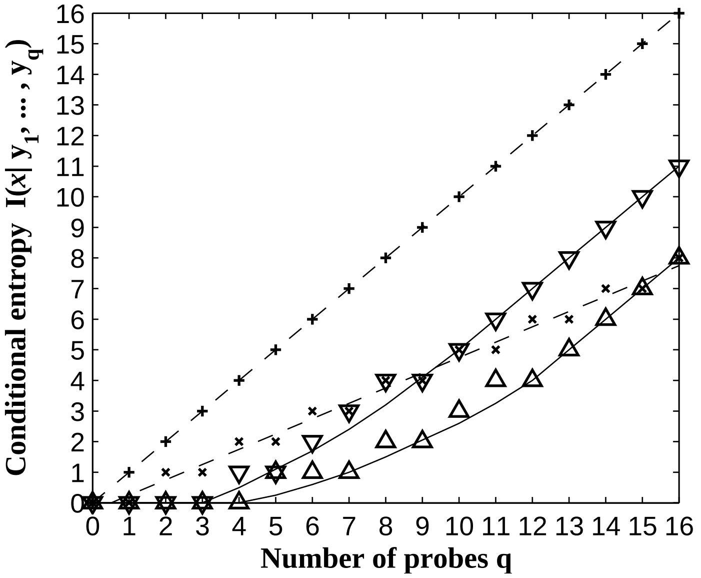

Fig. 1. Information leakage of an OPS(16,11;3) code (▽) and and OPS(17,9;4) code (△) in a probing attack with increasing number of needles. For comparison an unmasked circuit (+) and Vernam's masking scheme (×) is also shown. The lines serve as a guide to the eye.

5 Simultaneous probing and fault security, OTR-Codes

It is evident to ask for the generalization of a probing secure circuit to a *tamper-resistant* circuit, which simultaneously preserves privacy and integrity. Before further analysis we need to set up a precise fault attack model for an attacker who can simultaneously mount probing and fault attacks. An important subclass of physical fault attacks are *forcing attacks.* In this model we assume that a powerful attacker has full control on the values of up to f wires of his choice. An attacker has various physical methods to perform such a *surgical*, *i.e.* local attack. A powerful attacker could place f probes and overdrive the signal values on the wire by applying the appropriate electric potential. The work factor for such an attack resembles that of a probing attack. In a weaker, *i.e.* less controlled forcing attack (of statistical nature), pulses of electromagnetic radiation (e.g. from one or more lasers) could be used to flip signal values within some radius of influence. The faulty signal values will follow some probability distribution (depending on several physical parameters). In this attack the work factor for the setup will be smaller. However, the attacker will have to repeat the attack many times to generate an error vector that will lead to the intended information leakage. If we can assume that only up to f bits are modified, this attack is also covered by our model (random forcing attack).

Definition 7. *In a* ***Forcing Attack of Order f, FRA(f),*** *an adversary is able to force values* $(x_{1,t}, x_{2,t}, \ldots, x_{f,t})$ *on* f *wires of his choice in a circuit to 0 or 1 for an arbitrary number of evaluation cycles* $t = 1, 2, \ldots, T$*. That means he is able to imprint a (possibly changing) vector of values* $\mathbf{e}_t = (e_{1,t}, e_{2,t}, \ldots, e_{f,t})$ *on a subset of* f *wires in subsequent evaluation cycles* t*.*

Definition 8. *A circuit is* ***forcing secure of order f****, we write* ***FRS(f)****, if every error in a forcing attack of order* f *can be detected.*

It should be noted, that with Definition 8 we stress the importance of error detection as a precondition to a reaction on the error. We do not impose any restriction on the decision whether the circuit should be constructed such that the error can be corrected or whether the circuit should enter a secure state. The latter could be an irreversible transition to a state in which the secrets are deleted and the circuit is inoperative (self-destruction).

We can now proceed, in the spirit of Definition 6, to develop an encoding scheme for intermediary state variables, e.g. the wires of a circuit, which provides security against simultaneous probing and fault attacks.

Definition 9. *An* ***Optimal Tamper Resistant Code, OTR(n,k,j;f,q),*** *is a linear block code of length n, dimension k, and j information bits, which is simultaneously forcing secure of order f and probing secure of order q, i.e. PS(q) and FRS(f). The number of redundancy bits $r = n - k$ and the number of mask bits $s = k - j$ are minimal.*

In the second central theorem the canonical form of the OTR code is given and necessary conditions for the existence are derived.

Theorem 2. *W.l.o.g. the canonical shape of the generator matrix of an OTR code can be written in the form*

$$\mathbf{G} = \left(\begin{array}{c|c|c} \mathbf{I}_j & \mathbf{O} & \mathbf{S}_{j,r} \\ \hline \mathbf{Q}_{s,j} & \mathbf{I}_s & \mathbf{R}_{s,r} \end{array}\right), \tag{4}$$

where the probing matrix (cf. Eqn. 2) is given by

$$\mathbf{P}^q_{s,n} = (\mathbf{Q}_{s,j} | \mathbf{I}_s | \mathbf{R}_{s,r}). \tag{5}$$

The code is OTR(n,k,j;f,q), i.e. simultaneously PS(q) and FRS(f), if and only if the following three conditions hold:

1. *The parity check matrix of the code is given by*

$$\mathbf{H}^f_{r,k} = (\mathbf{S}^T_{r,j} | \mathbf{R}^T_{r,s} - \mathbf{S}^T_{r,j}\mathbf{Q}^T_{j,s} | \mathbf{I}_r). \tag{6}$$

2. *Any q columns of $\mathbf{P}^q_{s,n}$ are linearly independent.*
3. *Any f columns of $\mathbf{H}^f_{r,k}$ are linearly independent.*

Proof. Given the parity check matrix (6) and using (1) the corresponding generator matrix

$$\mathbf{G}' = \left(\begin{array}{c|c|c} \mathbf{I}_j & \mathbf{O} & \mathbf{S}_{j,r} \\ \hline \mathbf{O} & \mathbf{I}_s & \mathbf{R}_{s,r} - \mathbf{Q}_{s,j}\mathbf{S}_{j,r} \end{array}\right)$$

is obtained. We now transform $\mathbf{G}'$ to an equivalent code $\mathbf{G}$. Multiplying the upper slice by $\mathbf{Q}_{s,j}$ and adding the result to the lower slice we arrive at (4). The second condition follows immediately from Theorem 1. The third condition follows trivially from the definition of the minimum distance of a code. □

The construction of an OTR code for a given number of wires and a given order of probing and forcing security, *i.e.* the triplet (j, q, f), is a nontrivial task. It corresponds to the problem of finding a triplet of matrices $(\mathbf{Q}_{s,j}, \mathbf{S}_{j,r}, \mathbf{R}_{s,r})$, such that the corresponding probing (5) and parity check (6) matrices simultaneously fulfil the constraints on the minimum number of linearly independent columns. The competing constraints on the probing and the parity check matrix indicate again the *duality of the privacy and the integrity protection problem*, *cf.* Section 3.

It is convenient to recall a theorem of Gilbert and Varshamov:

Theorem 3. *(**Gilbert & Varshamov**) Let $l, m, n \in \mathbb{N}$ with $l \leq m \leq n$. There exists a binary $m \times n$ matrix with the property that any l columns are linearly independent, if $\sum_{i=0}^{l-1} \binom{n-1}{i} < 2^m$.*

Evidently, an OTR$(n, k, j; f, q)$ code fulfils the two Gilbert-Varshamov inequalities

$$\sum_{i=0}^{q-1} \binom{n-1}{i} < 2^{k-j} \quad \text{and} \quad \sum_{i=0}^{f-1} \binom{n-1}{i} < 2^{n-k}.$$

Conversely, it is not obvious whether choosing the smallest possible values of $s = k - j$ and $r = n - k$ independently for each inequality does imply the existence of the OTR-code. However, we observed experimentally that this was a sufficient condition for all tested small parameters. Usually an even better code can be found.

For moderate values of (j, q, f) OTR codes can be efficiently constructed using the following algorithm: For r and s choose the smallest values according to Table 1 (or more conservatively according to the Gilbert-Varshamov bound). Choose the parity check matrix of a $[j + s + r, j + s, f + 1]$ code. Calculate the corresponding generator matrix. Transform the generator matrix using elementary row operations to the canonical form by taking care that any q columns in the parity check matrix are linearly independent. If this constraint cannot be met select another parity check matrix and repeat the procedure. Increasing s or r will generally increase the number of solutions. Two examples for OTR codes can be found in appendix D: OTR(7,4,1;2,2) and in appendix E: OTR(16,11,6;3,3). It should be noted, that optimal solutions are usually obtained for smaller values of r and s than indicated by Gilbert's theorem. The OTR(16,11,6;3,3) code is such an example.

6 Summary

We have considered the problem of privacy and integrity protection in cryptographic circuits in a white-box scenario for a powerful, yet limited attacker. By introducing a coding theoretical framework we have shown that constructing an optimal masking scheme (as a privacy protection method) can be considered as the dual problem to finding an optimal error code (as an integrity protection method). The new formulation unifies the known linear masking schemes and allows us to find lower bounds for the number of masks needed to protect a circuit against qth order probing attacks. In this attack scenario the information leakage of the OPS code based masking schemes is smaller than that of Vernam's OTP scheme. Finally, we considered combined probing and forcing attacks and derived the structure of optimal linear tamper resistant codes (OTR), which are eligible to preserve both, privacy and integrity, in qth order probing and fth order forcing attacks. A procedure for the construction of OTR codes has been proposed.

It is immediate that all linear structures of a cryptographic algorithm can be efficiently protected by OPS and OTR codes. Although the lower bounds given by the linear constructions are still applicable for the nonlinear parts of an algorithm a linear coding scheme generally does not propagate through a nonlinear operation. Tamper protection of nonlinear structures will, for example, necessitate the application of extra masks and of nonlinear codes which are compatible with the specific nonlinear operation. This is a target for future analysis.

References

1. Ross J. Anderson and Markus G. Kuhn. Tamper Resistance - A Cautionary Note. In *Second Usenix Workshop on Electronic Commerce*, pages 1–11, November 1996.
2. Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (Im)possibility of Obfuscating Programs (Extended Abstract). In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001- 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 1–18. Springer-Verlag, 2001.
3. Eli Biham and Adi Shamir. Differential Fault Analysis of Secret Key Cryptosystems. In Burton S. Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, volume 1294 of *Lecture Notes in Computer Science*, pages 513–525. Springer-Verlag, 1997.
4. Christian Boit, Rudolf Schlangen, Uwe Kerst, and Ted Lundquist. Physical Techniques for Chip-backside IC Debug in Nanotechnologies. *IEEE Design & Test of Computers*, 25(3):250–257, May/June 2008.
5. Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the Importance of Eliminating Errors in Cryptographic Computations. *Journal of Cryptology*, 14(2):101–119, 2001.
6. Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards Sound Approaches to Counteract Power-Analysis Attacks. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412. Springer-Verlag, 1999.
7. Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory.* Wiley Series in Telecommunications and Signal Processing. Wiley-Interscience, second edition, 2006. ISBN 0-471-24195-4.
8. Rosario Gennaro, Anna Lysyanskaya, Tal Malkin, Silvio Micali, and Tal Rabin. Algorithmic Tamper-Proof (ATP) Security: Theoretical Foundations for Security Against Hardware Tampering. In Moni Naor, editor, *Theory of Cryptography. First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 258–277. Springer-Verlag, 2004.
9. Helena Handschuh, Pascal Paillier, and Jacques Stern. Probing Attacks on Tamper-Resistant Devices. In Çetin Kaya Koç and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES'99, First International Workshop, Worcester, MA, USA, August 12-13, 1999, Proceedings*, volume 1717 of *Lecture Notes in Computer Science*, pages 303–315. Springer-Verlag, 1999.
10. M.Y. Hsiao. A Class of Optimal Minimum Odd-Weight-Column SEC-DED Codes. *IBM Journal of Research and Development*, 14:395–401, 1970.
11. Yuval Ishai, Manoj Prabhakaran, Amit Sahai, and David Wagner. Private Circuits II: Keeping Secrets in Tamperable Circuits. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*, pages 308–327. Springer-Verlag, 2006.
12. Yuval Ishai, Amit Sahai, and David Wagner. Private Circuits: Securing Hardware against Probing Attacks. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481. Springer-Verlag, 2003.
13. Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer-Verlag, 1999.
14. Florence Jessie MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*, volume 16 of *Mathematical Library.* North-Holland, twelfth edition, 2006. ISBN 0-444-85193-3.
15. Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks – Revealing the Secrets of Smart Cards.* Springer-Verlag, 2007. ISBN 0-387-30857-1.
16. James L. Massey. Minimal Codewords and Secret Sharing. In *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, pages 276–279, 1993.
17. Thomas S. Messerges. Securing the AES Finalists Against Power Analysis Attacks. In Bruce Schneier, editor, *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*, volume 1978 of *Lecture Notes in Computer Science*, pages 150–164. Springer-Verlag, 2000.

18. Silvio Micali and Leonid Reyzin. Physically Observable Cryptography (Extended Abstract). In Moni Naor, editor, *Theory of Cryptography. First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 278–296. Springer-Verlag, 2004.
19. Jörn-Marc Schmidt and Chong Hee Kim. A Probing Attack on AES. In Kyo-Il Chung, Kiwook Sohn, and Moti Yung, editors, *Information Security Applications: 9th International Workshop, WISA 2008, Jeju Island, Korea, September 23-25, 2008, Revised Selected Papers*, volume 5379 of *Lecture Notes in Computer Science*, pages 256–265. Springer-Verlag, 2009.
20. Claude Elwood Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28:656–715, 1949.
21. Thomas Siegenthaler. Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications. *IEEE Transactions on Information Theory*, 30(5):776–780, 1984.
22. Sergei P. Skorobogatov and Ross J. Anderson. Optical Fault Induction Attacks. In Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, volume 2523 of *Lecture Notes in Computer Science*, pages 2–12. Springer-Verlag, 2003.
23. Gilbert Sandford Vernam (AT&T Bell Labs). Secret Signaling System. United States Patent 1,310,719, July 22, 1919, filed Sept. 13, 1918, 1919.

A Example for OPS(7,4;2) masking scheme

A number of $s = 3$ mask bits provides probing security PS(2) for data words of length $k = 4$. The canonical probing matrix in the OPS(7,4;2) masking scheme is a $[7, 4, 3]$ Hamming code.

$$\mathbf{P}^2_{3,7} = \left(\begin{array}{cccc|ccc} 1&1&0&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 0&1&1&1&0&0&1 \end{array}\right). \tag{7}$$

In explicit terms, the corresponding generator matrix (2) induces the masking scheme

$$(x_1, \ldots, x_4, m_1, m_2, m_3) \mapsto (x_1{+}m_1{+}m_2, x_2{+}m_1{+}m_3, x_3{+}m_2{+}m_3, x_4{+}m_1{+}m_2{+}m_3, m_1, m_2, m_3).$$

B Example for OPS(16,11;3) masking scheme

A number of $s = 5$ mask bits can provide probing security PS(3) for data words of length $k = 11$. The canonical probing matrix in the OPS(16,11;3) masking scheme is a $[16, 11, 4]$ Hsiao code [10].

$$\mathbf{P}^3_{5,16} = \left(\begin{array}{ccccccccccc|ccccc} 1&1&1&1&1&1&0&0&0&0&1&1&0&0&0&0 \\ 1&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0 \\ 1&0&0&1&1&0&1&1&0&1&1&0&0&1&0&0 \\ 0&1&0&1&0&1&1&0&1&1&1&0&0&0&1&0 \\ 0&0&1&0&1&1&0&1&1&1&1&0&0&0&0&1 \end{array}\right). \tag{8}$$

C Example for OPS(17,9;4) masking scheme

The $[17, 9, 5]$ quadratic residue code, *cf.* [14], generates an OPS(17,9;4) masking scheme. Using the generator polynomial $x^8+x^5+x^4+x^3+1$ the following canonical probing matrix is obtained.

$$\mathbf{P}^4_{9,17} = \left(\begin{array}{ccccccccc|cccccccc} 1&0&0&1&1&1&1&0&0&1&0&0&0&0&0&0&0 \\ 0&1&0&0&1&1&1&1&0&0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&1&1&1&1&0&0&1&0&0&0&0&0 \\ 1&0&0&0&1&1&0&1&1&0&0&0&1&0&0&0&0 \\ 1&1&0&1&1&0&0&0&1&0&0&0&0&1&0&0&0 \\ 1&1&1&1&0&0&1&0&0&0&0&0&0&0&1&0&0 \\ 0&1&1&1&1&0&0&1&0&0&0&0&0&0&0&1&0 \\ 0&0&1&1&1&1&0&0&1&0&0&0&0&0&0&0&1 \end{array}\right). \tag{9}$$

D Example for OTR(7,4,1;2,2) tamper resistant code

To achieve a forcing security of order 2, FRS(2), we start with the parity check matrix of a $[7, 4, 3]$ Hamming code. The distance of this code is $d_{\text{min}} = 3$ and the number of redundancy bits is $r = n - k = 3$.

$$\mathbf{H} = \left(\begin{array}{cccc|ccc} 1&1&0&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 0&1&1&1&0&0&1 \end{array}\right). \tag{10}$$

As given by Tab. 1 a number of $s = 3$ masks bits is required to achieve PS(2) for an OPS code of length $n = 7$. Hence a maximum of $j = k - s = 1$ information bits can be protected. The canonical generator matrix can be easily constructed by applying elementary row operations:

$$\mathbf{G} = \left(\begin{array}{c|ccc|ccc} 1&0&0&0&1&1&0 \\ \hline 1&1&0&0&0&1&1 \\ 1&0&1&0&1&0&1 \\ 0&0&0&1&1&1&1 \end{array}\right). \tag{11}$$

It is immediate that any two columns in the probing matrix (lower part of $\mathbf{G}$) are linearly independent. Hence this OTR code is PS(2).

E Example for OTR(16,11,6;3,3) tamper resistant code

In this nontrivial example we use a minimum weight Hsiao code ($d_{\text{min}} = 4$) of length $n = 16$ and dimension $k = 11$ as a starting point to achieve FRS(3),

$$\mathbf{H} = \left(\begin{array}{ccccccccccc|ccccc} 1&1&1&1&1&1&0&0&0&0&1&1&0&0&0&0 \\ 1&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0 \\ 1&0&0&1&1&0&1&1&0&1&1&0&0&1&0&0 \\ 0&1&0&1&0&1&1&0&1&1&1&0&0&0&1&0 \\ 0&0&1&0&1&1&0&1&1&1&1&0&0&0&0&1 \end{array}\right). \tag{12}$$

From Tab. 1 we see that $s = 5$ masks are necessary to secure $n = 16$ bits against a probing attack of order 3. Applying elementary row operations the generator matrix of an equivalent PS(3)-secure code can be constructed:

$$\mathbf{G} = \left(\begin{array}{cccccc|ccccc|ccccc}
1&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0\\
0&1&0&0&0&0&0&0&0&0&0&1&1&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&1&1&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&1&0&1&1&0\\
0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&1\\
0&0&0&0&0&1&0&0&0&0&0&1&0&0&1&1\\
\hline
1&1&1&1&1&0&1&0&0&0&0&1&0&0&1&0\\
1&0&1&0&0&1&0&1&0&0&0&1&1&0&1&1\\
1&0&0&1&1&1&0&0&1&0&0&0&0&1&1&1\\
1&1&1&0&1&0&0&0&0&1&0&0&1&1&0&1\\
1&1&0&1&0&1&0&0&0&0&1&1&1&1&0&0
\end{array}\right) . \tag{13}$$

This OTR code can secure $j = k - s = 6$ bits of information simultaneously against FRA(3) and PA(3) attacks.