Tsinghua Science and Technology
Doi: 10.26599/TST.2026.90100034

Research Article

Optimizing Linear Codes for Code-based Masking against Side-Channel Attacks

Xinyu Chen, Jihao Fan (✉), Wei Cheng, and Yongbin Zhou

Abstract Code-based masking is one of the most important countermeasures to prevent side-channel attacks. Dual distance and kissing number of linear codes are critical metrics indicating the side-channel resistance of code-based masking. However, calculating the value of these indicators depends on the choice of irreducible polynomials of the corresponding finite field. Through simulation experiments, we discovered that different irreducible polynomials significantly impact the side-channel resistance. Our findings suggest that the optimal linear codes derived from a single irreducible polynomial may not be globally optimal. By going through all irreducible polynomials over GF(256), we identify the optimal linear codes for 2-Share inner product masking (IPM) and (3,1)-Shamir's secret sharing (SSS) based masking in this field. Furthermore, we explore the application of higher-order masking defenses to the lightweight encryption scheme PRESENT. Additionally, we demonstrate through comprehensive simulation experiments that 3-share IPM provides substantial security advantages over 2-share IPM. We also extend our analysis to GF(32) and GF(64) to validate the generalizability of our approach.

Keywords Code-based masking, Side-channel attacks, Irreducible polynomials, Dual distance, Kissing number

1 Introduction

Side-channel analyses (SCAs) [1] can exploit unintentional physical leakages from cryptographic devices during the algorithm execution to extract sensitive data. These leakages are typically associated with the internal states or behaviors of the device and can be observed through power consumption and electromagnetic emanations [2, 3], as well as timing information [4].

Numerous countermeasures have been developed to combat SCAs, with masking protection [5, 6] emerging as a widely adopted method. Masking enhances security by splitting sensitive variables across multiple shares, breaking the direct correlation between critical variables and observable measurements. Boolean masking (BM) [7] was one of the earliest techniques adopted. As SCAs became more sophisticated, more advanced masking schemes such as inner product masking (IPM) [8, 9] and Shamir's secret sharing (SSS) based masking [10, 11] were developed to provide stronger security guarantees.

With the emergence of various masking methods, generalized code-based masking (GCM) [12, 13] has been proposed. Based on GCM, the side-channel resistance of code-based masking schemes can be quantified through two coding-theoretic properties: dual distance $d_{\mathcal{D}}^{\perp}$ [14–16] and kissing number f$B_{d_{\mathcal{D}}^{\perp}}$ [13, 16]. Moreover, Ref. [13] suggests that the optimal linear codes, later formally defined in [17], are those with maximized $d_{\mathcal{D}}^{\perp}$ and minimized $B_{d_{\mathcal{D}}^{\perp}}$. Through side-channel attack experiments, Ref. [18] verify that maximizing $d_{\mathcal{D}}^{\perp}$ and minimizing $B_{d_{\mathcal{D}}^{\perp}}$ provide the best achievable side-channel resistance. Accordingly, Ref. [18] has identified the optimal linear codes for 2-Share IPM, 3-Share IPM, and (3,1)-SSS-based masking.

To maintain consistency with the Advanced Encryption Standard (AES), Ref. [18] employs the irreducible polynomial $g(X) = X^8 + X^4 + X^3 + X + 1$. However, there are multiple irreducible polynomials for AES to select. Moreover, studies by [19] have demonstrated that certain irreducible polynomials offer superior structural properties in S-Box compared to the conventional option. Additionally, Ref. [20] presents a new S-Box construction method utilizing different irreducible polynomials. Based on these observations, we noted that the experimental process in [18] considered only a single irreducible polynomial, thereby neglecting the potential impact of alternative irreducible polynomials. Hence, we speculate that the optimal linear codes for code-based masking obtained in [18] may not be globally optimal linear codes.

Furthermore, we found that the work in [18] only considered the masking performance of first-order IPM and did not

• Xinyu Chen is with School of Cyber Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China. E-mail: xinyuchen@njust.edu.cn
• Jihao Fan is with School of Cyber Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China, and also with Laboratory for Advanced Computing and Intelligence Engineering, Wuxi 214083, China. E-mail: jihao.fan@outlook.com
• Wei Cheng is with LTCI, T´el´ecom Paris, Institut Polytechnique de Paris, Palaiseau 91120, France, and also with Secure-IC S.A.S., Paris 75015, France. E-mail: wei.cheng@telecom-paris.fr
• Yongbin Zhou is with School of Cyber Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China. Email:zhouyongbin@njust.edu.cn
Manuscript received: 2025-04-06; revised: 2025-10-25; accepted: 2026-03-20

address the masking performance of higher-order IPM. It is well known that higher-order masking encryption schemes offer significant advantages in side-channel resistance, with protective capabilities that increase exponentially compared to lower-order approaches. However, simulation-based research on higher-order masking has been relatively limited due to the complexity of analyzing these advanced protection mechanisms. To address this research gap, we plan to conduct performance validation work on higher-order IPM. Given that PRESENT [21] has lightweight characteristics compared to AES, we attempt to explore the effectiveness of second-order IPM based on the PRESENT algorithm.

In this work, we conduct an in-depth investigation of code-based masking schemes, focusing on the impact of irreducible polynomial selection on side-channel resistance. The main contributions of this paper can be summarized as follows: first, we demonstrate through specific examples that distinct irreducible polynomials yield varying results for $d_{\mathcal{D}}^{\perp}$ and $B_{d_{\mathcal{D}}^{\perp}}$ when applied to the same masking matrix. Subsequently, we confirm through simulation experiments that under the same masking matrix, different irreducible polynomials produce varied side-channel resistances. We discover that the optimal linear codes based on a single irreducible polynomial may not be a globally optimal scheme. To address this, we explore all irreducible polynomials to determine the globally optimal scheme. Simulation experiments confirm that the globally optimal linear codes we identify offer superior side-channel resistance compared to the optimal scheme based on a single irreducible polynomial. Notably, the optimal linear codes for 2-Share IPM are equivalent to the BKLC. Second, we extend our research to higher-order masking protection for the PRESENT encryption algorithm. We successfully identify the optimal linear codes for second-order IPM for PRESENT. Higher-order masking schemes offer exponentially stronger resistance against side-channel attacks compared to lower-order schemes. To comprehensively evaluate the differences between higher-order and lower-order masking schemes in terms of performance and security, we conduct systematic simulation experiments. The experimental results clearly demonstrate that higher-order IPM provides significant security advantages. This finding offers an important reference for the secure implementation of practical cryptographic systems.

2 Preliminaries

2.1 Side-channel attacks

We present a comprehensive evaluation of side-channel resistance in code-based masking schemes through extensive simulation experiments. Our methodology employs challenging attack scenarios utilizing a higher-order optimal distinguisher (HOOD) [22], [23], based on the Maximum Likelihood (ML) principle [24]. The ML attack demonstrates significant efficacy when the leakage distribution is known. HOOD exploits power consumption profiles to extract sensitive information from cryptographic algorithms protected by masking techniques. To enhance analysis efficiency, HOOD implements preprocessing methods that transform multivariate leakage into univariate leakage. This transformation dramatically improves the effectiveness of higher-order analysis compared to conventional lower-order power analysis techniques.

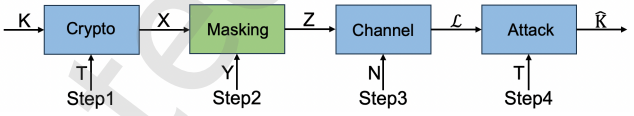

Fig. 1 The process of simulated experiments for side-channel analysis

To precisely evaluate the side-channel resistance of code-based masking, we employ an attack-based assessment methodology. This approach provides a direct measure of exploitable leakages. Fig. 1 illustrates our simulation process.

First, we consider uniformly distributed plaintext $T \sim \mathcal{U}(\mathbb{K})$ and secret key $K \sim \mathcal{U}(\mathbb{K})$, where $\mathbb{K} = \mathbb{F}_{2^s}$, computing the sensitive variable $X = S(T \oplus K)$. Next, we generate t random masks $Y \in \mathbb{K}$, with the code-based masking scheme producing n shares $Z = (Z_1, Z_2, \ldots, Z_n)$. In the third step, for each share Z_i we obtain simulated measurements $\mathcal{L}_i = w_H(Z_i) + N_i$, $1 \leqslant i \leqslant n$, where w_H is the Hamming weight function and $N_i \sim \mathcal{N}(0, \sigma^2)$ represents Gaussian noise. For q traces, we obtain $\mathcal{L} = (\mathcal{L}_i^j)$ for $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant q$. Finally, we employ HOOD to recover the secret key using these simulated measurements. The HOOD is therefore equivalent to the following distinguisher score [25],[26]:

$$S(k) = \sum_{j=1}^{q} \log \sum_{y \in \mathbb{K}^{n-1}} \prod_{i=1}^{d} \mathcal{N}(\mathcal{L}_i^j | \omega_H(z_i^j), \sigma^2). \quad (1)$$

S(k) is the score of the guessed key. Therefore, the key hypothesis is given by:

$$\hat{k} = \arg\max_{k \in \mathbb{K}} \hat{\Delta}(k). \quad (2)$$

2.2 Code-based masking scheme

Code-based masking [12, 13] provides a systematic cryptographic protection framework that integrates coding theory with masking techniques. This approach leverages the mathematical structure of linear codes to construct corresponding

masking schemes, where the generator matrices of linear codes directly correspond to the masking matrices.

Currently, the most widely employed masking schemes include Boolean masking (BM) [7], polynomial masking, inner product masking (IPM) [8], Shamir's secret sharing (SSS)-based masking [10], [11], and direct sum masking (DSM) [14]. This study focuses on IPM and SSS-based masking, representing non-redundant and redundant schemes, respectively.

As a fundamental concept, BM randomizes internal states by splitting sensitive variables into several shares. The key principle ensures that an attacker gaining any subset of $n-1$ shares obtains no information about the original sensitive variable. For a sensitive variable $X \in \mathbb{K} = \mathbb{F}_{2^\ell}$ and $n-1$ masks $Y_i \in \mathbb{K}$, the BM scheme protects X as:

$$Z = X\mathbf{G} + Y\mathbf{H} \in \mathbb{K}^n, \tag{3}$$

where $\mathbf{G}$ and $\mathbf{H}$ are the generator matrices of two codes $\mathcal{C}$ and $\mathcal{D}$, respectively. Moreover, we also refer to the generator matrix $\mathbf{H}$ as the masking matrix.

However, with advancements in side-channel attack, IPM has been proposed in [8] to enhance the algebraic complexity by mixing bits in each share. Notably, IPM utilizes a different generator matrix $\mathbf{H}$ compared to the BM. The generator matrix $\mathbf{G}$ and $\mathbf{H}$ as follows:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \end{pmatrix} \in \mathbb{K}^{1\times n}$$
$$\mathbf{H} = \begin{pmatrix} \alpha_2 & 1 & 0 & \cdots & 0 \\ \alpha_3 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_n & 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathbb{K}^{(n-1)\times n}. \tag{4}$$

The inner product is defined as: $f_i(y_i) = \alpha_i y_i$ where $\alpha_1 = 1$ and $\alpha_i \in \mathbb{K} \setminus \{0\}$ for $i \in \{2, 3, \ldots, n\}$. Consequently, the IPM scheme can be expressed as follows:

$$Z = \left(X + \sum_{i=2}^{n} f_i(Y_i), Y_2, Y_3, \ldots, Y_n\right). \tag{5}$$

While the IPM scheme improves side-channel resistance compared to BM, it remains vulnerable to fault injection attacks (FIA). To address this vulnerability, Shamir's secret sharing (SSS)-based masking scheme was introduced in [10], [11]. When $t = n-1$, the SSS scheme functions as a non-redundant masking approach. When $t < n-1$, it becomes a redundant scheme. The generator matrix used for masking under the SSS scheme is shown below:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix} \in \mathbb{K}^{1\times n}$$
$$\mathbf{H} = \begin{pmatrix} \alpha_1^1 & \alpha_2^1 & \cdots & \alpha_n^1 \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^t & \alpha_2^t & \cdots & \alpha_n^t \end{pmatrix} \in \mathbb{K}^{(n-1)\times n}. \tag{6}$$

Given $n = 3$ and $t = 1$, the (3,1)-SSS based masking scheme is expressed as: $Z = (X+\alpha_1 Y, X+\alpha_2 Y, X+\alpha_3 Y)$. It is evident that if an attacker attains any two shares of Z, they can extract information about the sensitive variable X.

In code-based masking, two critical indicators of side-channel resilience are the dual distance $d_{\mathcal{D}}^{\perp}$ and the kissing number $B_{d_{\mathcal{D}}^{\perp}}$.

Definition 1 (Dual Distance [27]). *Considering a linear code $\mathcal{C}$ its dual distance $d_{\mathcal{C}}^{\perp}$ is the minimum Hamming weight $\omega_H(u)$ of nonzero $u \in \mathbb{K}$, such that $\sum_{c\in\mathcal{C}}(-1)^{d\cdot u} \neq 0$.*

Definition 2 (Kissing Number[①] [28]). *Considering a linear code $\mathcal{C}$, its kissing number B_d is the number of nonzero codewords in $\mathcal{C}$ with the minimum Hamming weight, or equivalently: $B_d = |\{x \in \mathcal{C} | \, \omega_H(x) = d_{\mathcal{C}}\}|$.*

Definition 3 (Optimal linear code [13, 17]). *A linear code $\mathcal{C}$ of parameter $[n, k]$ over $\mathbb{F}_{2^\ell}$ is said to be (d, B_d)-optimal if its subfield extension $[\mathcal{C}]$ has the largest minimum distance d and the lowest kissing number B_d.*

Definition 4 (Best Known Linear Code [16]). *A linear code $\mathcal{C}$ of length n and dimension k is considered as Best Known Linear Code (BKLC) if it has the largest Hamming distance d among all known $[n, k]$ linear codes.*

3 The Globally Optimal Linear Codes

3.1 Code expansion

To calculate the dual distance $d_{\mathcal{D}}^{\perp}$ and the kissing number $B_{d_{\mathcal{D}}^{\perp}}$, it is essential to perform code expansion for the generator matrix of the linear code. In the process of code expansion, we use sub-field representation, the elements in $\mathbb{F}_{2^\ell}$ are decomposed over $\mathbb{F}_2$. We have the following code expansion as in [17]:

$$(1, L_2, \ldots, L_n)_{2^\ell} \mapsto (I_\ell, \mathbb{L}_2, \ldots, \mathbb{L}_n)_2, \tag{7}$$

where I_l is the $\ell \times \ell$ identity matrix in $\mathbb{F}_2$ and $\mathbb{L}_i$ are $\ell \times \ell$ matrix for $2 \leqslant i \leqslant n$.

Moreover, the process of sub-field representation depends on the choice of the irreducible polynomial. The author[18] utilizes the irreducible polynomial $g_1(X) = X^8 + X^4 + X^3$

① The kissing number of a linear code is firstly introduced in [28].

$+ \mathrm{X} + 1$ that is used in the (AES) to generate the finite field $\mathbb{K} = \mathbb{F}_{2^8}$. The author used the same irreducible polynomial $\mathrm{g}_1(\mathrm{X})$ for sub-field representation to ensure consistency with the polynomial used to construct the finite field $\mathbb{K}$. Hence, we hypothesize that different irreducible polynomials may lead to different expansion matrices. These variations in expansion matrices subsequently lead to differences in the calculation of $d_{\mathcal{D}}^{\perp}$ and $B_{d_{\mathcal{D}}^{\perp}}$. Such discrepancies in $d_{\mathcal{D}}^{\perp}$ and $B_{d_{\mathcal{D}}^{\perp}}$ could impact the side-channel resistance of code-based masking.

Theoretical Analysis.We now establish the rigorous connection between irreducible polynomial selection and the resulting code parameters through the following proof chain:

Step 1: Field Representation.Let $g_1(X), g_2(X) \in \mathbb{F}_2[X]$ be two distinct ℓ-degree irreducible polynomials. Although they define algebraically isomorphic finite fields $\mathbb{F}_{2^\ell} \cong \mathbb{F}_2[X]/(g_1(X)) \cong \mathbb{F}_2[X]/(g_2(X))$, the polynomial representations differ. For $g_1(X)$ with root α_1, any element $\beta \in \mathbb{F}_{2^\ell}$ can be expressed as $\beta = \sum_{i=0}^{\ell-1} b_i^{(1)} \alpha_1^i$. Similarly, for $g_2(X)$ with root α_2, we have $\beta = \sum_{i=0}^{\ell-1} b_i^{(2)} \alpha_2^i$. Since α_1 and α_2 satisfy different minimal polynomial relations, the coefficient vectors $(b_0^{(1)}, \ldots, b_{\ell-1}^{(1)})$ and $(b_0^{(2)}, \ldots, b_{\ell-1}^{(2)})$ are generally distinct.

Step 2: Sub-field Representation. The sub-field representation map $\phi : \mathbb{F}_{2^\ell} \to \mathbb{F}_2^\ell$ is defined by $\phi(\beta) = (b_0, b_1, \ldots, b_{\ell-1})$ where $\beta = \sum_{i=0}^{\ell-1} b_i \alpha^i$ and α is the root of the chosen irreducible polynomial. Since different irreducible polynomials $g_1(X)$ and $g_2(X)$ have different roots α_1 and α_2, they induce distinct polynomial bases $\{1, \alpha_1, \alpha_1^2, \ldots, \alpha_1^{\ell-1}\}$ and $\{1, \alpha_2, \alpha_2^2, \ldots, \alpha_2^{\ell-1}\}$ for $\mathbb{F}_{2^\ell}$. Therefore, we obtain distinct mappings ϕ_1 and ϕ_2. Consequently, for the same field element $\beta \in \mathbb{F}_{2^\ell}$ (except for elements in the prime field $\mathbb{F}_2$), the coordinate vectors generally satisfy $\phi_1(\beta) \neq \phi_2(\beta)$.

Step 3: Expansion Matrix Construction. In the code expansion (7), each $\ell \times \ell$ matrix $\mathbb{L}_i$ is constructed from the element $L_i \in \mathbb{F}_{2^\ell}$. Specifically, if $L_i = \alpha^{k_i}$, then the j-th column of $\mathbb{L}_i$ is given by $\phi(\alpha^{k_i+j-1})$. Since the computation of $\phi(\alpha^m)$ depends on the minimal polynomial relation satisfied by α, different irreducible polynomials yield different expansion matrices: $\mathbb{L}_i^{(1)} \neq \mathbb{L}_i^{(2)}$ where the superscripts indicate the choice of $g_1(X)$ or $g_2(X)$.

Step 4: Impact on $d_{\mathcal{D}}^{\perp}$ and $B_{d_{\mathcal{D}}^{\perp}}$. The dual code $\mathcal{D}^{\perp}$ is defined by the expanded generator matrix: $\mathcal{D}^{\perp} = v \in \mathbb{F}_2^{n\ell} : v\mathbf{H}^T = \mathbf{0}\}$ where $\mathbf{H} = (I_\ell, \mathbb{L}_2, \ldots, \mathbb{L}_n)$. Since $\mathbb{L}_i$ depends on the irreducible polynomial choice, different polynomials produce different dual codes, thereby affecting both the dual distance $d_{\mathcal{D}}^{\perp}$ and the kissing number $B_{d_{\mathcal{D}}^{\perp}}$.

Therefore, we will first provide an example to illustrate how different irreducible polynomials can result in distinct expansion matrices, as well as varying values of dual distance and kissing number.

For $n = 2$ and $t = 1$, IPM has a masking matrix $\mathbf{H} = (1\ \alpha)$, choosing the parameter $\alpha = 57$ ($\alpha \in \mathbb{K}$). Using the irreducible polynomial $\mathrm{g}_1(\mathrm{X})$, the expansion matrix $\mathbf{H}_1$ is represented as follows:

$$\begin{aligned}\mathbf{H}_1 &= \left(I_8 \middle| \mathbb{L}_\alpha^{(1)}\right) \\ &= \left(I_8 \middle| \begin{pmatrix}\phi_1(\alpha) & \phi_1(\alpha^2) & \cdots & \phi_1(\alpha^8)\end{pmatrix}\right).\end{aligned} \tag{8}$$

Simultaneously, employing the irreducible polynomial $\mathrm{g}_2(\mathrm{X}) = \mathrm{X}^8 + \mathrm{X}^5 + \mathrm{X}^4 + \mathrm{X}^3 + 1$, we obtain the expansion matrix $\mathbf{H}_2$ which is represented as follows:

$$\begin{aligned}\mathbf{H}_2 &= \left(I_8 \middle| \mathbb{L}_\alpha^{(2)}\right) \\ &= \left(I_8 \middle| \begin{pmatrix}\phi_2(\alpha) & \phi_2(\alpha^2) & \cdots & \phi_2(\alpha^8)\end{pmatrix}\right).\end{aligned} \tag{9}$$

In particular ,the matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ exhibit differences in specific elements in Eq. (10) and Eq. (11), which confirms our theoretical analysis. Using Magma, we compute the dual distance $d_{\mathcal{D}}^{\perp} = 4$ and the kissing number $B_{d_{\mathcal{D}}^{\perp}} = 7$ for $\mathbf{H}_1$, while for $\mathbf{H}_2$, the dual distance $d_{\mathcal{D}}^{\perp} = 5$ and the kissing number $B_{d_{\mathcal{D}}^{\perp}} = 24$. This significant difference in code parameters validates our theoretical prediction that irreducible polynomial selection critically impacts the side-channel resistance of code-based masking schemes.

$$H_1 = \begin{pmatrix} 10000000\ 10011100 \\ 01000000\ 01001110 \\ 00100000\ 00100111 \\ 00010000\ 11001011 \\ 00001000\ 10111101 \\ 00000100\ 01010110 \\ 00000010\ 01000011 \\ 00000001\ 11111001 \end{pmatrix} \tag{10}$$

$$H_2 = \begin{pmatrix} 10000000\ 10011100 \\ 01000000\ 01001110 \\ 00100000\ 00100111 \\ 00010000\ 10001111 \\ 00001000\ 11011011 \\ 00000100\ 11111011 \\ 00000010\ 11100100 \\ 00000001\ 01110010 \end{pmatrix} \tag{11}$$

3.2 Optimal linear codes for each irreducible polynomial

We confirm that different irreducible polynomials yield varying values of $d_{\mathcal{D}}^{\perp}$ and $B_{d_{\mathcal{D}}^{\perp}}$. As highlighted in [18] , optimal side-channel resistance is achieved with maximized $d_{\mathcal{D}}^{\perp}$ and minimized $B_{d_{\mathcal{D}}^{\perp}}$. Based on this, they identified the optimal linear codes for both 2-Shares IPM and (3,1)-SSS based masking. However, their analysis only considered a single irreducible polynomial. We speculate that the optimal linear codes for IPM and SSS-based masking proposed in [18] may not be globally optimal. To address this limitation, we first conduct an exhaustive exploration of all irreducible polynomials to determine the theoretically optimal linear codes for each polynomial. Then, we validate and identify the globally optimal linear codes through simulation experiments.

Taking $n = 2$ and $t = 1$, IPM has a single parameter α with generator matrix $\mathbf{H} = (1\,\alpha)$, $\alpha \in \mathbb{F}_{2^8}$. For generator matrix $\mathbf{H}$, we present the optimal calculation results in Tab. 3, showing the maximized $d_{\mathcal{D}}^{\perp}$ and minimized $B_{d_{\mathcal{D}}^{\perp}}$ for each irreducible polynomial. For simplicity, irreducible polynomials are represented in a hexadecimal notation. In [18], the authors have verified through simulation experiments that the optimal linear codes for 2-Share IPM with $d_{\mathcal{D}}^{\perp} = 4$ and $B_{d_{\mathcal{D}}^{\perp}} = 4$ were constructed using irreducible polynomials 0x11b. To streamline notation, we denote the parameters $d_{\mathcal{D}}^{\perp} = a$ and $B_{d_{\mathcal{D}}^{\perp}} = b$ as $\langle a, b\rangle$. However, as shown in Tab. 3, the linear codes with parameters $\langle 4, 2\rangle$ and $\langle 4, 1\rangle$ theoretically offer superior side-channel resistance compared to $\langle 4, 4\rangle$ due to the smaller $B_{d_{\mathcal{D}}^{\perp}}$. Additionally, linear codes with parameters $\langle 5, 24\rangle$ are equivalent to the Best Known Linear Code (BKLC).

To obtain the optimal linear codes with parameters $\langle 4, 1\rangle$, the distribution of $d_{\mathcal{D}}^{\perp}$ and $B_{d_{\mathcal{D}}^{\perp}}$ for each linear codes with the irreducible polynomial 0x18b is presented in Tab. 1. As shown in Tab. 1, there are only two linear codes that achieve the parameters $\langle 4, 1\rangle$ when $\alpha = 103$ or 203. Similarly, we use the irreducible polynomial 0x139 to compute the distribution of $d_{\mathcal{D}}^{\perp}$ and $B_{d_{\mathcal{D}}^{\perp}}$ in Tab. 2. According to Tab. 2, there are only two linear codes with parameters $\langle 5, 24\rangle$ when $\alpha = 57$ or 114.

While our analysis demonstrates that theoretically superior linear codes compared to the optimal scheme proposed in [18], these findings require validation through simulation experiments. Furthermore, the masking effectiveness for the parameters $\langle 4, 1\rangle$ and $\langle 5, 24\rangle$ cannot be directly compared without further experimental evaluation. Moreover, it is crucial to verify whether different irreducible polynomials affect the side-channel resistance of code-based masking. Therefore, Sec. 4 will assess these hypotheses through simulation experiments and identify the optimal linear codes for 2-Share IPM and (3,1)-SSS based masking.

Table 1 Choice of the linear codes for IPM with 0x18*b*.

$d_{\mathcal{D}}^{\perp} = d$	$B_{d_{\mathcal{D}}^{\perp}} = B_d$	$\lvert\{\alpha\}\rvert$	Candidates of α
$d = 2$	$B_d = 8$	1	{1}
	$B_d = 1$	10	{3, 48, 49, 57, . . ., 196}
$d = 3$	$B_d = 6$	2	{110, 151 }
	$B_d = 1$	52	{11, 14, 15, 18, . . ., 254}
$d = 4$	$B_d = 14$	4	{81,140,147,237}
	$B_d = 1$	2	{103, 203}

Table 2 Choice of the linear codes for IPM with 0x139.

$d_{\mathcal{D}}^{\perp} = d$	$B_{d_{\mathcal{D}}^{\perp}} = B_d$	$\lvert\{\alpha\}\rvert$	Candidates of α
$d = 2$	$B_d = 8$	1	{1}
	$B_d = 1$	18	{9, 18, 19, 32, . . ., 219}
$d = 3$	$B_d = 5$	8	{3, 5, 79, 88, . . ., 233 }
	$B_d = 1$	64	{7, 14, 28, 42, . . ., 255}
$d = 4$	$B_d = 10$	4	{94,139,207,225}
	$B_d = 2$	2	{100, 177}
$d = 5$	$B_d = 24$	2	{57, 114}

3.3 Optimal linear codes for IPM with PRESENT

Compared to the AES encryption scheme, PRESENT is a lightweight encryption algorithm with lower computational complexity and smaller hardware resource requirements. The key space in the block cipher process of PRESENT belongs to the finite field GF(16), making it suitable for low-power and resource-constrained devices. We first consider $n = 2$ and $t = 1$, IPM has a single parameter α with generator matrix $\mathbf{H} = (1\,\alpha)$, $\alpha \in \mathbb{F}_{2^4}$. There are 15 candidates for α as it cannot be zero. To enable practical applications and ensure a fair comparison with state-of-the-art methods, we focus on the irreducible polynomial $g_3(X) = X^4 + X + 1$, which is used in PRESENT to generate the finite field $\mathbb{F}_{2^4}$. According to Tab. 4, there are 10 optimal linear codes with maximized $d_{\mathcal{D}}^{\perp} = 3$ and minimized $B_{d_{\mathcal{D}}^{\perp}} = 3$.

We also consider the second-order IPM for PRESENT, the masking matrix is given by $\mathbf{H} = (1\,\alpha_1\,\alpha_2)$, where $\alpha_1, \alpha_2 \in \mathbb{F}_{2^4}$, with parameters $n = 3$ and $t = 2$. The distribution of $d_{\mathcal{D}}^{\perp}$ and $B_{d_{\mathcal{D}}^{\perp}}$ for second-order IPM are enumerated in Tab. 4. As shown in Tab. 4 there are only 9 optimal linear codes with maximized $d_{\mathcal{D}}^{\perp} = 5$ and minimized $B_{d_{\mathcal{D}}^{\perp}} = 2$ at the same time.

3.4 Generalization to Other Finite Fields and Cryptographic Algorithms

To validate the generalizability of our approach beyond GF(256) and GF(16), we extend our analysis to additional finite fields and cryptographic algorithms. This section demonstrates that the impact of irreducible polynomial selection on code-based masking optimization is not limited to specific field sizes or cipher implementations.

We first extend our investigation to GF(64), which represents an intermediate complexity between GF(16) and GF(256). For 2-share IPM with generator matrix $\mathbf{H} = (1\,\alpha)$, where $\alpha \in \mathbb{F}_{2^6}$, we analyze all irreducible polynomials of degree 6 in Tab. 5.

Table 3 The calculation results of maximized $d_{\mathcal{D}}^{\perp}$ and minimized $B_{d_{\mathcal{D}}^{\perp}}$ for each irreducible polynomial.

$d_{\mathcal{D}}^{\perp} = d$	$B_{d_{\mathcal{D}}^{\perp}} = B_d$	No.	Candidates of irreducible polynomial
$d = 4$	$B_d = 4$	8	{ **0x11b(AES)**, 0x171, 0x11d, 0x1dd, 0x1b1, 0x1f9, 0x177,0x13f }
	$B_d = 3$	8	{0x169, 0x18d, 0x12d, 0x163, 0x1f5, 0x15f, 0x1bb, 0x17b }
	$B_d = 2$	10	{ 0x1f3, 0x14d, 0x19f, 0x1a9, 0x1c3, 0x1e7, 0x165, 0x117, 0x12b, 0x1cf }
	$B_d = 1$	2	{ 0x1a3, 0x18b }
$d = 5$	$B_d = 24$	2	{ 0x139, 0x1d7 }

Table 4 Choice of the codes for IPM with different parameters for PERSENT.

n	$d_{\mathcal{D}}^{\perp} = d$	$B_{d_{\mathcal{D}}^{\perp}} = B_d$	No.	candidates
$n = 2$	$d = 2$	$B_d = 4$	1	$\{1\}$
		$B_d = 3$	1	$\{2\}$
	$d = 3$	$B_d = 4$	3	$\{3, 4, 5\}$
		$B_d = 3$	10	$\{6, 7, 8, 9, 10, \ldots, 15\}$
$n = 3$	$d = 3$	$B_d = 3$	4	$\{(1, 2), (1, 9), (2, 2), (9, 9)\}$
		$B_d = 2$	7	$\{(1, 4), (1, 13), \ldots, (13, 13)\}$
		$B_d = 1$	6	$\{(1, 8), (2, 8), \ldots, (8, 8)\}$
	$d = 4$	$B_d = 4$	2	$\{(2, 3), (8, 9)\}$
		$B_d = 1$	23	$\{(1, 10), (2, 14), \ldots, (12, 12)\}$
	$d = 5$	$B_d = 6$	2	$\{(1, 7), (6, 6)\}$
		$B_d = 2$	9	$\{(3, 5), (3, 7), \ldots, (7, 12), (12, 14)\}$

The results confirm our hypothesis that different irreducible polynomials yield varying dual distances and kissing numbers. Notably, the optimal parameters $\langle 4,\ 8\rangle$ achieved with polynomials 0x5b or 0x6d for 2-share IPM.

Furthermore, we provide the optimal parameters that maximized dual distance $d_{\mathcal{D}}^{\perp}$ and the minimized kissing number $B_{d_{\mathcal{D}}^{\perp}}$ for 3-share IPM masking scheme. These optimal parameters are determined for each irreducible polynomial when the matrix $\mathbf{H} = (1\,\alpha_1\,\alpha_2)$, $\alpha_1, \alpha_2 \in \mathbb{F}_{2^6}$. The results of the computations are presented in Tab. 5.

ASCON [29, 30], the winner of the NIST Lightweight Cryptography standardization process, operates on a 320-bit state and employs a different algebraic structure compared to PRESENT. Although ASCON uses a larger state size, its S-box operations can be protected using similar masking principles. For ASCON's 5-bit S-box operations over GF(32), we analyze 2-share and 3-share IPM schemes. The generator matrices for ASCON masking are constructed as follows. For 2-share IPM: $\mathbf{H} = (1\,\alpha)$, where $\alpha \in \mathbb{F}_{2^5}$. And for 3-share IPM: $\mathbf{H} = (1\,\alpha_1\,\alpha_2)$, where $\alpha_1, \alpha_2 \in \mathbb{F}_{2^5}$. A comprehensive analysis of all degree-5 irreducible polynomials for IPM with $n = 2$ and $n = 3$ is presented in Tab. 5. From Tab. 5 the optimal parameters with maximized $d_{\mathcal{D}}^{\perp}$ and minimized $B_{d_{\mathcal{D}}^{\perp}}$ $\langle 3,\ 1\rangle$ are achieved using irreducible polynomials 0x25 or 0x29 for 2-share IPM.

4 Numerical Results

4.1 Experimental results on 2-share IPM

We begin by considering IPM as an example of a non-redundant masking scheme. In Sec. 3, we demonstrat that different irreducible polynomials result in distinct values for $d_{\mathcal{D}}^{\perp}$ and $B_{d_{\mathcal{D}}^{\perp}}$. To investigate whether these differences impact the side-channel resistance, we conduct simulation experiments. Our analysis employs same masking matrix $\mathbf{H} = (1\,57)$ with four irreducible polynomials: 0x139, 0x11b, 0x1a3, and 0x18b.

As previously mentioned, the simulated traces are represented as $\mathcal{L} = (\mathcal{L}_i^j)$ for $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant q$ where $\mathcal{L}_i^j = w_H(Z_i{}^j) + N_i{}^j$ denotes the leakage of i-th share in j-th trace. The evaluation metric is the minimum number of traces required to achieve $P_s \geqslant 90\%$, where P_s represents the success rate, across different noise levels. Consequently, we present the evaluation results of IPM with $n = 2$ using the same metric $\mathbf{H} = (1\,57)$ across different irreducible

Table 5 The calculation results for irreducible polynomials in different finite fields and parameters.

n	GF	$d_{\mathcal{D}}^{\perp} = d$	$B_{d_{\mathcal{D}}^{\perp}} = B_d$	No.	irreducible polynomial
$n = 2$	GF(32)	$d = 3$	$B_d = 1$	2	{ 0x25, 0x29 }
			$B_d = 2$	2	{ 0x37, 0x3b }
			$B_d = 3$	2	{ 0x2f, 0x3d }
	GF(64)	$d = 3$	$B_d = 1$	3	{ 0x57, 0x75, 0x49 }
		$d = 4$	$B_d = 8$	4	{ 0x5b, 0x6d, 0x61, 0x43 }
			$B_d = 10$	2	{ 0x73, 0x67 }
$n = 3$	GF(32)	$d = 5$	$B_d = 1$	2	{ 0x37, 0x3d }
		$d = 6$	$B_d = 4$	2	{ 0x2f, 0x3d }
			$B_d = 6$	2	{ 0x25, 0x29 }
	GF(64)	$d = 6$	$B_d = 1$	4	{ 0x5b, 0x6d, 0x75, 0xa7 }
		$d = 7$	$B_d = 8$	2	{ 0x61, 0x43 }
			$B_d = 11$	1	{ 0x49 }
			$B_d = 14$	2	{ 0x73, 0x67 }

polynomials in Fig. 2 by using up to $q = 180000$ traces. Additionally, we include Boolean masking (BM) with $n = 3$ shares in comparison.

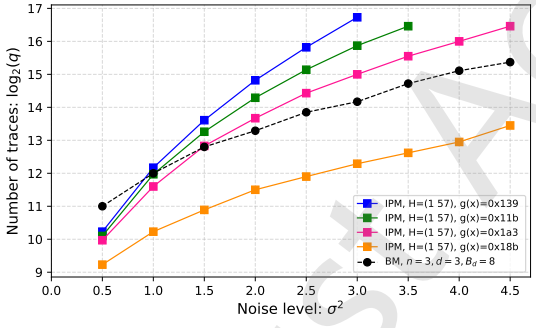

Fig. 2 The effect of irreducible polynomial for the side-channel resistance of non-redundant masking scheme

The primary conclusion drawn from Fig. 2 is that the selection of irreducible polynomials has a notable impact on the side-channel resistance of IPM. Moreover, as the noise level increases, the differences in performance become increasingly pronounced. Specifically, when the noise level exceeds 1.5, the side-channel resistance of 2-Shares IPM using irreducible polynomials 0x139, 0x11b, and 0x1a3 consistently surpasses that of 3-Shares BM. However, the 2-Share IPM scheme employing 0x18b underperforms compared to the 3-Share BM across all noise levels. Therefore, for IPM with $n = 2$, the selection of the irreducible polynomial has a significant impact on the side-channel resistance.

Tab. 1 and Tab. 2 reveal that the optimal linear codes for 2-Share IPM with parameters $\langle 4, 1\rangle$ and $\langle 5, 24\rangle$ are

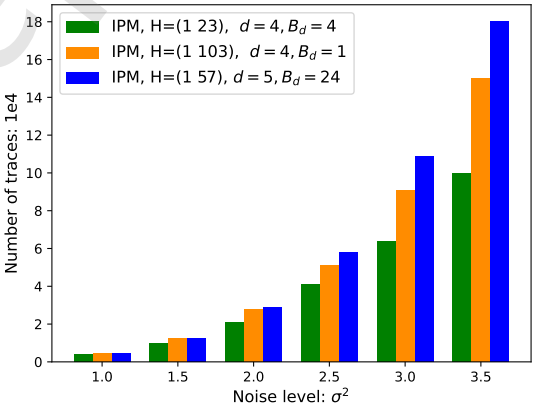

Fig. 3 The optimal linear codes for 2-Share IPM

obtained using the irreducible polynomials 0x18b and 0x139, respectively. Theoretically, these linear codes could provide better side-channel resistance compared to the optimal scheme $\langle 4, 4\rangle$ utilizes 0x11b, as presented in [18]. Therefore, it is essential to validate our hypothesis and find the globally optimal linear codes through simulation experiments.

The experimental results presented in Fig. 3 demonstrate that at the noise level of 1.0, all three linear codes exhibit similar side-channel resistance. However, as the noise level exceeds 1.5, the side-channel resistance with parameters $\langle 4, 1\rangle$ and $\langle 5, 24\rangle$ gradually surpasses that with parameters $\langle 4, 4\rangle$. Furthermore, when the noise level achieves 2.0, the side-channel resistance with parameters $\langle 5, 24\rangle$ begins to outperform $\langle 4, 1\rangle$. Ultimately, at the noise level of 3.5, successful key recovery requires 100,000 traces for the linear code with parameters $\langle 4, 4\rangle$, whereas the linear code with

parameters $\langle 5,\ 24\rangle$ needs 180,000 traces. This significant difference allows us to conclude that the optimal linear codes for 2-Share IPM are achieved when the irreducible polynomial selects 0x139 and the generator matrix of the linear code is given by $\mathbf{H} = (1\,57)$. All these experiments can be reproduced through the following GitHub repository [31].

4.2 Experimental results on (3,1)-SSS based masking

Redundancy is crucial for fault detection in computations. While code-based masking can be configured for redundancy to counter both side-channel and fault injection attacks, IPM inherently lacks this redundancy. Therefore, we focus on SSS-based masking, a redundant code-based masking scheme. Considering $n = 3$ and $t = 1$, the (3,1)-SSS based masking scheme has generator matrices $\mathbf{G}$ and $\mathbf{H}$ as follows:

$$\begin{aligned} \mathbf{G} &= \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \\ \mathbf{H} &= \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix}. \end{aligned} \tag{12}$$

We aim to investigate whether different irreducible polynomials influence the side-channel resistance of SSS-based masking. Initially, we establish the same masking matrix $\mathbf{H} = (1\,141\,232)$ and select three irreducible polynomials: 0x1dd, 0x11b, and 0x139. Subsequently, we conduct simulation experiments to assess differences in the side-channel resistance of (3,1)-SSS based masking scheme when selecting different irreducible polynomials. These experiments are conducted under the same conditions as those used in the evaluation of IPM. The evaluation results for (3,1)-SSS based masking are presented in Fig. 4. We include Boolean masking with $n = 2$ and $n = 3$ shares in comparison.

From Fig. 4, the key takeaway is that there are significant differences in side-channel resistance, even with the same masking matrix employed. The figure demonstrates that when the irreducible polynomial 0x1dd was utilized, it exhibited the best side-channel resistance among three irreducible polynomials across all noise levels. Conversely, the selection of 0x11b resulted in the poorest performance. In the worst scenario, the (3,1)-SSS based masking demonstrates inferior performance compared to the 2-Share BM at all noise levels. Therefore, we confirm that the choice of irreducible polynomial significantly influences the side-channel resistance of the redundant masking scheme under the same masking matrix.

Furthermore, we attempt to identify the optimal linear codes for (3,1)-SSS based masking. We identify the optimal linear codes for each irreducible polynomial by traversing all irreducible polynomials. After obtaining the optimal calculation result for each polynomial, we select both the best and worst cases displayed in Tab. 6. According to the calculation of Magma, when using the generator matrix

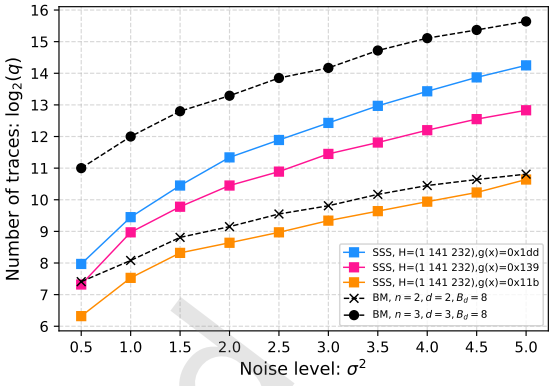

Fig. 4 The effect of irreducible polynomial for the side-channel resistance of redundant masking scheme

Table 6 The calculation results of maximized $d_{\mathcal{D}}^{\perp}$ and minimized $B_{d_{\mathcal{D}}^{\perp}}$.

$d_{\mathcal{D}}^{\perp} = d$	$B_{d_{\mathcal{D}}^{\perp}} = B_d$	No.	irreducible polynomial
$d = 4$	$B_d = 49$	2	{ 0x1dd, 0x177 }
	$B_d = 37$	2	{ **0x11b(AES)**, 0x1b1 }
	$B_d = 32$	1	{ 0x139 }

$\mathbf{H} = (1\,147\,100)$, we obtain the optimal linear codes with parameters $\langle 4, 32\rangle$ based on 0x139. When using the generator matrix $\mathbf{H} = (1\,144\,161)$ with the irreducible polynomial 0x1dd, we obtain the optimal linear codes with parameters $\langle 4, 49\rangle$. Subsequently, we conduct simulation experiments to verify whether the linear code with parameters $\langle 4,\ 32\rangle$ exhibits superior side-channel resistance compared to the optimal linear code with parameters $\langle 4,\ 37\rangle$ based on 0x11b in [18].

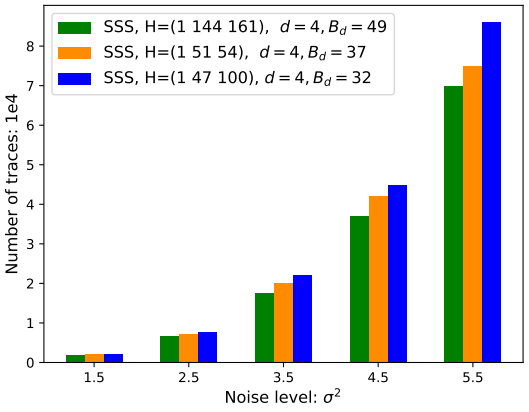

Fig. 5 The optimal linear codes for (3,1)-SSS based masking

The evaluation results for the (3,1)-SSS based masking are presented in Fig. 5 using up to $q = 80000$ traces. The

primary conclusion from Fig. 5 is that our identified linear codes with parameters $\langle 4, 32\rangle$, based on the irreducible polynomial 0x139, outperform the optimal linear codes with parameters $\langle 4, 37\rangle$ in [18]. Furthermore, as the noise increases, the differences become more pronounced. The distinction between linear codes with parameters $\langle 4, 32\rangle$ and linear codes with parameters $\langle 4, 49\rangle$ is even more significant.

Ultimately, our study of the (3,1)-SSS redundant masking scheme confirms that the choice of different irreducible polynomials significantly influences the side-channel resistance of redundant masking. We also identify optimal linear codes based on (3,1)-SSS when the irreducible polynomial is 0x139, and the generator matrix is given by $\mathbf{H} = (1\,147\,100)$.

4.3 Experimental results on 3-share IPM for PERSENT

The complexity of IPM schemes increases exponentially with higher security levels, yet most analyses remain theoretical with limited experimental validation. While AES encryption's complexity makes simulating high-order IPM masking challenging, PRESENT's lightweight structure offers a viable alternative for practical implementation and verification. In Sec. 3, we successfully identify the optimal linear codes for IPM in the PRESENT encryption algorithm for $n = 2$ and $n = 3$. Tab. 4 shows that when $n = 2$, the masking matrix $\mathbf{H} = (1\,11)$ has the optimal parameters with maximized $d_{\mathcal{D}}^{\perp} = 3$ and minimized $B_{d_{\mathcal{D}}^{\perp}} = 3$. Meanwhile, from Tab. 4 , the second-order masking matrix $\mathbf{H} = (1\,9\,9)$ has the worst parameters with minimized $d_{\mathcal{D}}^{\perp} = 3$ and maximized $B_{d_{\mathcal{D}}^{\perp}} = 3$. Based on these findings, we conduct simulation experiments in Fig. 6 that verify the performance differences between the optimal linear codes for 2-share IPM and the worst linear codes for 3-share IPM. At the same time, we include Boolean Masking(BM) with $n = 3$ shares and 3-share IPM with parameters $\langle 4, 1\rangle$, $\langle 3, 1\rangle$ and $\langle 4, 4\rangle$ in comparison.

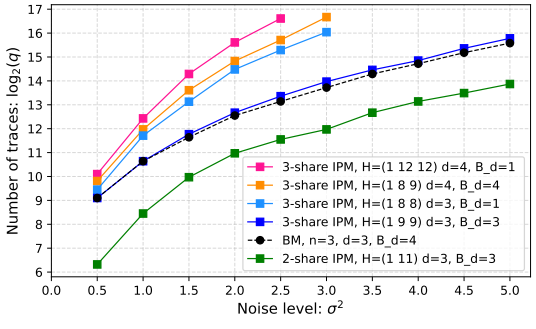

Fig. 6 The performance differences between 3-share IPM and 2-share IPM

Our empirical results presented in Fig. 6 demonstrate that even the worst linear codes for 3-share IPM implementation exhibit substantially superior performance compared to the optimal linear codes for 2-share IPM. Across all noise levels examined, the worst 3-share IPM schemes require approximately three times more traces for successful key recovery than the optimal 2-share IPM. Furthermore, the Boolean masking (BM) with $n = 3$ significantly outperforms the optimal 2-share IPM implementation.

When selecting 3-share IPM schemes with different parameters, the security performance improvement is significantly more pronounced compared to 2-share IPM. Experimental results demonstrate that at a noise level of 0.5, the 3-share IPM employing a masking matrix $\mathbf{H} = (1\,12\,12)$ requires approximately 1,100 traces for successful key recovery. In contrast, the optimal 2-share IPM under identical noise conditions requires merely 100 traces for successful key recovery. As noise levels increase, the performance disparity between the two schemes becomes increasingly evident. When the noise reaches a level of 2.5, the 3-share IPM requires approximately 100,000 traces for successful key recovery. In comparison, the optimal 2-share IPM scheme requires only about 3,000 traces. This indicates that noise intensity has markedly different effects on the performance of 3-share IPM versus 2-share IPM. Specifically, the 3-share IPM demonstrates substantially superior resistance to side-channel attacks, particularly in high-noise environments.

Furthermore, parameters selection for the 3-share IPM significantly influences its side-channel resistance capabilities. For instance, the selection of the masking matrix $\mathbf{H} = (1\,12\,12)$ demonstrates notable performance enhancement compared to $\mathbf{H} = (1\,9\,9)$. Experimental data reveal that at a noise level of 0.5, the performance differential between these configurations is approximately 1-fold. However, as noise levels increase, the performance gap becomes increasingly pronounced. Especially when the noise level reaches 2.5, utilizing masking matrix $\mathbf{H} = (1\,9\,9)$ requires approximately 10,500 traces for successful key recovery, while employing masking matrix $\mathbf{H} = (1\,12\,12)$ necessitates approximately 100,000 traces.

Therefore, we conclude that 3-share IPM demonstrates significant security performance improvements compared to 2-share IPM. Additionally, within 3-share IPM implementations, the selection of parameters plays a crucial role in enhancing the side-channel resistance.

5 Conclusions

This research demonstrates that the selection of irreducible polynomials significantly impacts the side-channel resistance

of code-based masking schemes. Our comprehensive investigation reveals that optimal linear codes derived from a single irreducible polynomial may not achieve global optimality. Through extensive simulation experiments and theoretical analysis across all possible irreducible polynomials, we identify the truly optimal linear codes for both 2-share IPM and (3,1)-SSS based masking schemes over $\mathbb{F}_{2^8}$. Our findings also indicate that conventional AES encryption implementations, which typically rely on a single irreducible polynomial for code-based masking, may not achieve optimal side-channel protection. Furthermore, we explore the application of higher-order masking defenses to the lightweight encryption scheme PRESENT and evaluate the performance improvements of 3-share IPM over 2-share masking schemes through simulation experiments. Notably, provide the first visualized experimental demonstration of the performance improvements that higher-order masking schemes offer over lower-order ones. This work emphasizes the critical importance of incorporating multiple irreducible polynomials in the design of side-channel countermeasures, potentially enabling enhanced security robustness in cryptographic communication systems. Future extensions should explore the use of GPU acceleration to enable higher-order masking validation beyond current computational limitations.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Nos. 62371240, 61802175), the fund of Laboratory for Advanced Computing and Intelligence Engineering (No. 2023-LYJJ-01-009).

Reference

[1] T.-H. Le, C. Canovas, and J. Clédiere, An overview of side channel analysis attacks, pp. 33–43, 2008.

[2] M. Randolph and W. Diehl, Power side-channel attack analysis: A review of 20 years of study for the layman, *Cryptography*, vol. 4, no. 2, p. 15, 2020.

[3] T. Kitazawa, L. Wouters, B. Gierlichs, D. Fujimoto, I. Verbauwhede, and Y. Hayashi, Active electromagnetic side-channel analysis: Crossing physical security boundaries through impedance variations, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2026, no. 1, pp. 376–401, 2026.

[4] P. Kocher, Differential power analysis, in *Proc. Advances in Cryptology (CRYPTO'99)*, 1999.

[5] H. Groß and S. Mangard, A unified masking approach, *Journal of cryptographic engineering*, vol. 8, pp. 109–124, 2018.

[6] J. Hermelink, K.-C. Ning, and R. Petri, Finding and protecting the weakest link: On side-channel attacks on y in masked ml-dsa, in *Annual International Cryptology Conference*. Springer, 2025, pp. 3–37.

[7] J.-S. Coron and L. Goubin, On boolean and arithmetic masking against differential power analysis, in *Cryptographic Hardware and Embedded Systems—CHES 2000: Second International Workshop Worcester, MA, USA, August 17–18, 2000 Proceedings 2*. Springer, 2000, pp. 231–237.

[8] J. Balasch, S. Faust, and B. Gierlichs, Inner product masking revisited, in *Advances in Cryptology–EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I 34*. Springer, 2015, pp. 486–510.

[9] J. Gaspoz and S. Dhooghe, Bit t-sni secure multiplication gadget for inner product masking, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2025, no. 1, pp. 104–127, 2025.

[10] L. Goubin and A. Martinelli, Protecting aes with shamir's secret sharing scheme, in *Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13*. Springer, 2011, pp. 79–94.

[11] E. Prouff and T. Roche, Higher-order glitches free implementation of the aes using secure multi-party computation protocols, in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2011, pp. 63–78.

[12] W. Wang, P. Méaux, G. Cassiers, and F.-X. Standaert, Efficient and private computations with code-based masking, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 128–171, 2020.

[13] W. Cheng, S. Guilley, C. Carlet, J.-L. Danger, and S. Mesnager, Information leakages in code-based masking: A unified quantification approach, *Cryptology ePrint Archive*, 2021.

[14] J. Bringer, C. Carlet, H. Chabanne, S. Guilley, and H. Maghrebi, Orthogonal direct sum masking: A smartcard friendly computation paradigm in a code, with builtin protection against side-channel and fault attacks, in *IFIP International Workshop on Information Security Theory and Practice*. Springer, 2014, pp. 40–56.

[15] R. Poussier, Q. Guo, F.-X. Standaert, C. Carlet, and S. Guilley, Connecting and improving direct sum masking and inner product masking, in *Smart Card Research and Advanced Applications: 16th International Conference, CARDIS 2017, Lugano, Switzerland, November 13–15, 2017, Revised Selected Papers*. Springer, 2018, pp. 123–141.

[16] W. Cheng, S. Guilley, C. Carlet, S. Mesnager, and J.-L. Danger, Optimizing inner product masking scheme by a coding theory approach, *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 220–235, 2020.

[17] W. Cheng, Y. Liu, S. Guilley, and O. Rioul, Toward finding best linear codes for side-channel protections (extended version), *Journal of Cryptographic Engineering*, vol. 14, no. 1, pp. 131–145, 2024.

[18] W. Cheng, S. Guilley, and J.-L. Danger, Information leakage in code-based masking: A systematic evaluation by higher-order attacks, *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1624–1638, 2022.

[19] D. Wang and S.-L. Sun, Replacement and structure of s-boxes in rijndael, in *2008 International Conference on Computer Science and Software Engineering*, vol. 3. IEEE, 2008, pp. 782–784.

[20] A. Seghier, J. Li, and D. Z. Sun, Advanced encryption standard based on key dependent s-box cube, *IET Information Security*, vol. 13, no. 6, pp. 552–558, 2019.

[21] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, Present: An ultra-lightweight block cipher, in *Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9*. Springer, 2007, pp. 450–466.

[22] A. Heuser, O. Rioul, and S. Guilley, Good is not good enough: Deriving optimal distinguishers from communication theory, in *Cryptographic Hardware and Embedded Systems–CHES 2014: 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings 16*. Springer, 2014, pp. 55–74.

[23] N. Bruneau, S. Guilley, A. Heuser, and O. Rioul, Masks will fall off: higher-order optimal distinguishers, in *Advances in Cryptology–ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, China, ROC, December 7-11, 2014, Proceedings, Part II 20*. Springer, 2014, pp. 344–365.

[24] S. Chari, J. R. Rao, and P. Rohatgi, Template attacks, in *Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4*. Springer, 2003, pp. 13–28.

[25] N. Costes and M. Stam, Redundant code-based masking revisited, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 426–450, 2021.

[26] H. Chabanne, H. Maghrebi, and E. Prouff, Linear repairing codes and side-channel attacks, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 118–141, 2018.

[27] F. MacWilliams, The theory of error-correcting codes, *Elsevier Science Publishers BV google schola*, vol. 2, pp. 39–47, 1977.

[28] P. Solé, Y. Liu, W. Cheng, S. Guilley, and O. Riou, Linear programming bounds on the kissing number of q-ary codes, in *2021 IEEE Information Theory Workshop (ITW)*. IEEE, 2021, pp. 1–5.

[29] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, Ascon v1. 2: Lightweight authenticated encryption and hashing, *Journal of Cryptology*, vol. 34, no. 3, p. 33, 2021.

[30] H. Zhang, Y. Gao, Y. Zhou, and J. Ming, Side-channel collision attacks against ascon, in *2025 Design, Automation & Test in Europe Conference (DATE)*. IEEE, 2025, pp. 1–6.

[31] X. Chen, Code-Based Masking Implementation, https://github.com/xinyuchen123/code-based-masking, 2025.

Author biography

Xinyu Chen received the B. E. degree from Shaanxi Normal University, Xi'an, China in 2023. He is now pursuing a master's degree at Nanjing University of Science and Technology, Nanjing, China. His research interests include cryptography, code-based masking and side-channel attacks.

Jihao Fan received the B.S. degree from Lanzhou University, Lanzhou, China, in 2009, and the Ph.D. degree in computer software and theory from Southeast University, Nanjing, China, in 2016. He is currently an Associate Professor with the Nanjing University of Science and Technology, Nanjing, China. His research interests include classical and quantum coding theory, information theory, and side-channel attacks.

Wei Cheng received the B. E. degree from Wuhan University, Wuhan, China in 2014, the M. E. degree from Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China in 2017 and received the Ph.D. degree in information and communications from Télécom Paris, Institut Polytechnique de Paris, France, in 2021. He is currently a Post-Doctoral Researcher with Secure-IC S.A.S., and also an (invited) Associate Researcher with Télécom Paris. His research interests include information theory, side-channel analysis, related countermeasures (mainly on code-based masking, including inner product masking, direct sum masking, polynomial masking, and other variants) for embedded systems, and secure cryptographic implementations. He also works on machine learning-based analysis on physical unclonable functions.

Yongbin Zhou received the B. E. degree from Wuhan University of Technology, Wuhan, China in 1996, the M. E. degree from Shandong University, Jinan, China in 2000, and the Ph.D. degree from Institute of Software Chinese Academy of Sciences, Beijing, China in 2004. He is currently a full-time Professor with the School of Cyber Security and Engineering, Nanjing University of Science and Technology. He is also an Adjunct Professor with the Institute of Information Engineering, Chinese Academy of Sciences. His main research interests include theories and technologies of network and information security.