DOI:10.11784/tdxbz202502010

一种基于 CRC 的 DRAM 抗电磁故障注入攻击检测方法

刘　强[1,2]，郭龙韬[1,2]

（1. 天津大学微电子学院，天津 300072；2. 天津市成像与感知微电子技术重点实验室，天津 300072）

摘　要：电磁故障注入攻击可以导致动态随机存储器（DRAM）产生多比特错误，威胁到存储数据的安全性. 校验码是一种用于检测数据中错误的技术，广泛用于数据存储和传输过程中. 然而，在处理多比特错误时，以奇偶校验和汉明纠错码为代表的传统校验方式面临失效的风险. 因此，本文提出了一种基于循环冗余校验（CRC）的检测方法，用于检测电磁故障注入攻击在 DRAM 中引发的错误. 首先，基于对错误特征的分析，在读写过程中增加额外校验步骤，实现对错误的检出. 其次，针对增加校验带来的存储和传输开销，本文通过构建最优化问题并将各项成本量化，实现不同应用场景下参数的最优选取. 最后，对这一方法进行全面评估，搭建故障注入攻击实验，分析其复杂度、检测率、存储和传输等成本. 结果表明，所提出的方法能够实现接近 100%错误检测率，同时相比于传统校验方法不显著增加计算复杂度.

关键词：硬件安全；电磁故障注入攻击；循环冗余校验；动态随机存储器

中图分类号：TN432　　**文献标志码**：A　　**文章编号**：0493-2137（2026）02-0164-08

Detection Method for DRAM Against EMFI Attacks Based on CRC

Liu Qiang[1,2]，Guo Longtao[1,2]

（1. School of Microelectronics，Tianjin University，Tianjin 300072，China；
2. Tianjin Key Laboratory of Imaging and Sensing Microelectronic Technology，Tianjin 300072，China）

Abstract：Research indicates that electromagnetic fault injection（EMFI）attacks can cause multibit errors in dynamic random access memory（DRAM）and threaten the security of stored data. Check code is a technology used to detect errors in data and is widely applied in data storage and transmission processes. However，when dealing with multibit errors，the traditional check methods represented by parity check and Hamming code face the risk of failure. Therefore，this paper proposed a solution based on cyclic redundancy check（CRC）to detect errors caused by EMFI attacks in DRAM. First，based on the analysis of error characteristics，additional verification steps were added during the read and write processes to achieve error detection. Second，in response to the storage and transmission overhead caused by the added verification，an optimization problem with the quantified costs was constructed to achieve optimal parameter selection under different application scenarios. Finally，the proposed method was comprehensively evaluated，and a fault injection attack experiment was set up to analyze complexity，detection rate，storage，and transmission costs. Results show that the proposed method can achieve an error detection rate close to 100% while not substantially increasing computational complexity compared with the traditional check methods.

Keywords：hardware security；electromagnetic fault injection（EMFI） attack；cyclic redundancy check（CRC）；dynamic random access memory（DRAM）

随着信息技术产业的快速发展，集成电路在关系国计民生的各个领域中都处于越来越重要的地位，成为了各种现代电子设备的核心部件. 然而，随着集成电路重要性的提高，其面临的安全威胁也与日俱增.

收稿日期：2025-02-13；**修回日期**：2025-05-26.
作者简介：刘　强（1978—　　），男，博士，教授，qiangliu@tju.edu.cn.
通信作者：刘　强，qiangliu@tju.edu.cn.
基金项目：国家自然科学基金资助项目（U21B2031）.
Supported by the National Natural Science Foundation of China（No. U21B2031）.

存储芯片，作为信息系统中的核心部件之一，承担着存储关键信息和数据的作用，同时也成为攻击的重要目标[1]. 目前已有针对存储器的攻击成功案例. Menu 等[2]将激光故障注入攻击应用于闪存芯片，成功在数据和指令中引发单比特翻转. Viera 等[3]利用针对闪存的激光故障注入攻击成功破解了一个运行在 32 位微控制器上的密码系统，成功篡改了存储在闪存芯片中的密码.

动态随机存储器（dynamic random access memory，DRAM）是一种常见的存储器件，由于其大容量、高读写速度、随机存取、重复读写寿命长等特点，被广泛用作计算机系统的内存. 行锤攻击是目前最常见的 DRAM 攻击手段之一，其原理是通过对目标行的相邻行进行反复读写，利用 DRAM 存储电路中相邻行间的耦合作用，引发目标行的电荷泄露，实现对目标数据的篡改[4]. 例如，Jattke 等[5]对 AMD CPU 进行逆向工程，使用特制的访问模式进行数据同步，并精心调度了刷新和隔离指令，首次在 AMD 的 Zen 平台上实现了行锤位翻转. 电磁故障注入攻击是另一种针对 DRAM 的常见攻击手段，通过施加高强度电磁脉冲，导致存储数据出现位翻转、控制信号错误等内存错误. Narayanan 等[1]设计了名为 ChipShouter 的专用攻击工具，对运行 Ascon 密码的摄像头模块进行攻击，成功向其中注入故障. Tang 等[6]使用电磁故障注入攻击，通过直接篡改内存数据，破解了运行在嵌入式系统上的高级加密标准（advanced encryption standard，AES）加密算法. 行锤攻击需要首先进行内存剖析，绕过高速缓存层次结构，才能实现对 DRAM 单元的直接访问，相比之下，电磁故障注入攻击不需要额外的预处理，具有成本低、灵活性高等特点，对 DRAM 的安全性构成了严重威胁.

目前，已有关于 DRAM 的防护方法，其中大多数方法都针对行锤攻击设计. 一种主流的防御行锤攻击的策略是目标行刷新[7-8]，这种方法对行锤攻击进行检测，一旦检测到行锤攻击，就对受害行进行刷新，从而抵御行锤攻击. 这种方法能够有效缓解行锤攻击带来的行翻转，其核心技术是检测 DRAM 的异常读取，具体方法有很多种，例如采用硬件计数器[9]或者机器学习[10]等方法. 由于电磁故障注入攻击无需依赖对 DRAM 的频繁访问即可实现数据篡改，因此这些防御方法面对电磁攻击时难以发挥作用. 此外，在硬件安全研究领域，DRAM 的随机掉电特性和易受行锤攻击特性也可以被用作物理不可克隆函数（physical unclonable function，PUF）[11]. 在这种应用场景下，DRAM 主要被用做真随机数生成器、设备身份认证和密钥生成等用途. 针对 DRAM 的电磁故障注入攻击及防御方法对这些应用也会产生影响，但不在本文工作的研究范围内.

现有研究表明，电磁故障注入攻击可以在 DRAM 芯片中造成连续多字节错误和一个字节中连续多比特错误[6,12]. 为避免数据错误对计算机系统带来负面影响，一个传统的解决方法是在存储器中使用纠错码（error correction code，ECC）对发生错误的比特进行检测和纠正，这种方法广泛应用在内存领域[13]；另一个传统的解决方法是在数据存储和传输中使用奇偶校验对发生的错误进行检测，这种方法广泛应用在通信和计算领域[14]. 然而，这些方法仅在面对偶发的、错误比特数较少的错误有效，无法对连续多比特错误实现有效检测，进而面临失效风险.

因此，本文提出了一种基于循环冗余校验（cyclic redundancy check，CRC）的 DRAM 芯片抗电磁故障注入攻击检测方法，借助循环冗余校验对输入变化的敏感性，实现对错误的有效检测，提高 DRAM 安全性. 本文首先分析电磁故障注入攻击下 DRAM 错误特点和现有校验方法存在的问题，提出了基于循环冗余校验的 DRAM 芯片抗电磁故障注入攻击的错误检测方法，随后对检测方法的安全性收益以及存储和传输成本进行量化分析，将校验参数选取转化为最优化问题，实现安全性与成本的平衡. 最后搭建了 DRAM 电磁故障注入攻击实验，对方法的检测率和对读写性能的影响进行全面评估，实验证明这一方法可以实现接近 100% 的错误检出率.

1　电磁攻击原理和现有方法的分析

电磁故障注入的原理是电磁感应定律，即感应电动势的大小与穿过电路的磁通量的变化率成正比. 在集成电路中，电源和地网络的金属层含有许多垂直和水平回路，这些回路会受到电磁脉冲的影响[15]. 对于 DRAM 芯片，电磁脉冲在存储节点、参考电压等节点感应产生电压脉冲，影响存储电容的正常充放电，进而导致 DRAM 读出或写入错误的数据. 由于 DRAM 内部的存储单元排列高度规则化，同一行的存储单元共享同一字线，同一列的单元共享同一位线，因此在电磁故障注入攻击下，DRAM 中的数据会出现连续多个字节出错和一个字节中多个比特出错的现象[12]. 针对这一问题，一种通常的解决方法是使用校验码对数据中的错误进行检测.

对于一种校验方法来说，如果在原始数据发生变化前后生成的校验码完全相同，那么就无法通过校验码来确定原始数据是否发生了变化. 这种情况称为校验失效. 在原始数据之后添加校验数据会增加额外的存储成本. 因此，理想的校验方法应具有尽可能低的失效概率和尽可能小的存储成本.

目前，在通信和存储领域中，奇偶校验和 ECC 校验是两种常见的校验方法. 奇偶校验在数据末尾添加一个校验位，标识数据中“1”的总数为偶数(偶校验)或奇数(奇校验)，从而检测数据传输中的单比特错误. 然而，当数据中错误的位数为偶数时，奇偶校验就存在失效的风险. 如果错误数量随机分布，则奇偶校验的失效率可达 50%. 尽管通过改进的校验形式[16]可以提高其校验有效性，在面对偶数位翻转时仍无法完全解决失效问题. 奇偶校验的存储成本取决于原始数据划分的粒度，即当对 m 位原始数据添加 1 位校验位时，额外存储占比为 $1/m$.

ECC 校验包括多种校验方法，其中最经典的是汉明校验. 汉明校验通过向数据中添加足够数量的校验位，使得数据块中的每个校验位覆盖一定范围的数据位，从而实现对错误的检测和纠正. 它能够有效检测和纠正最多 2 位错误，在面对超过 2 位的错误时有失效风险. 汉明校验向长度为 m 位的原始数据中添加 n bit 校验数据，需满足 $2^n > m+n$，其额外存储开销为 n/m. BCH 码是一种针对多比特错误的 ECC 校验[17]，但其可检测的最大翻转位数需要在构造时预先指定，当翻转位数超过此限制时，BCH 码将面临失效风险. 例如，对于消息长度为 7 且可检测 3 位错误的 BCH 码，其码字总长度为 15，这需要添加 8 bit 校验位，额外存储开销比例为 8/7. 一般来说，能检测 k bit 错误的 BCH 码，其额外存储占比可表示为 $m+k\left[\mathrm{lb}(m+k+1)\right]/m$.

由于电磁注入故障攻击引起的错误具有随机性，错误比特的数量和位置都难以预测，纠正这些错误非常困难. 因此，如果仅考虑错误检测，理想的方法应对原始数据的变化高度敏感，以确保不会发生校验失效. 同时，该方法的校验码长度应尽可能短，以减少额外的存储开销. 相较于上述两种方法，CRC 的最大检测错误比特数没有限制，且校验码长度可以自由选择，能够满足这一场景的需求. 因此，本文基于 CRC 技术提出了针对 DRAM 的抗电磁故障注入攻击检测方法.

2 基于 CRC 的检测方法

2.1 待检测数据的错误特征

针对 DRAM 的电磁故障注入攻击研究[7]表明，攻击可以导致 DRAM 中出现列故障和区域故障，图 1 给出了这两种典型故障的特征. 其中列故障是指 DRAM 中某一列数据出现错误，而区域故障是指某一地址范围内的数据出现错误. 这些故障中部分会在若干刷新周期后消失，而另一些则会持续存在直至数据被重新写入. 尽管上述故障的持续时间和存在形式各不相同，但均属于多比特故障，即每次故障均涉及多个比特翻转，且翻转比特的最大数量可超过 4 096 位.

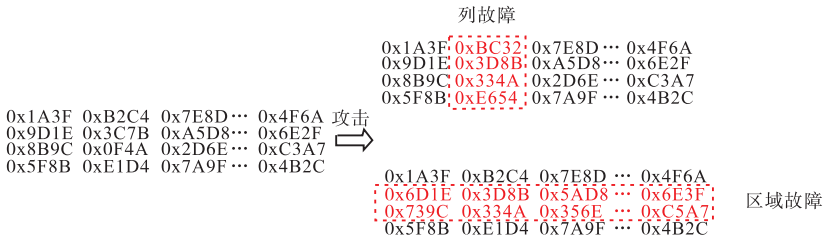


图 1 电磁攻击下数据错误类型及其特征

Fig.1 Error type and characteristics under electromagnetic attack

这种现象的成因与 DRAM 的结构密切相关. 一方面，目前主流 DRAM 基于 1T-1C 结构，即一个晶体管和一个电容构成一个存储单元. 数据的读写依赖于电容的充放电以及放大电路对微弱信号的放大. 因此，当电磁故障注入攻击在 DRAM 电路敏感节点(如电源、地或参考电压)感应产生电压脉冲时，数据的读写会受到干扰，进而导致数据被篡改. 另一方面，DRAM 将数百万个存储单元以阵列形式组织，控制电路通过字线和位线选择需要读取或写入的存储单元，同一行或列的存储单元共享相同的字线或位线. 当电磁故障注入攻击在某个存储单元上引发故障时，该故障可能沿字线或位线传播，从而影响相邻的存储单元. 由于一条字线或位线上包含大量存储单元，这种传播最终导致多个比特发生翻转.

通过上述分析，可以得到电磁故障注入攻击下错误的特征，这些特征为检测方法的设计提供了理论依据. 基于这些分析，本文提出基于循环冗余的检测流程，重点介绍其原理、具体流程和性能表现.

2.2　基于 CRC 的检测流程

CRC 是一种广泛应用于数字通信和存储系统中的错误检测技术. 其核心思想是将待校验的信息码视为一个二进制多项式，并与预定义的生成多项式进行模 2 运算，从而生成一个固定长度的冗余码，用于验证数据的完整性. CRC 的计算过程主要包括以下几个步骤. 首先，将信息码视为一个二进制多项式，并在其后附加若干个 0（通常为生成多项式的最高次幂减 1），以生成多项式为除数，用附加了 0 的信息码作为被除数进行模 2 除法. 模 2 除法不涉及进位操作，仅需按位异或. 在每次除法中，首先对齐生成多项式的最高位与当前被除数的最高位，然后对生成多项式和被除数对应位进行异或运算，得到新的余数，随后将余数与下一位数据拼接，继续下一轮运算，直至所有位运算完成，至此完成一轮模 2 除法. 最后，将余数作为冗余码附加到信息码末尾形成完整的数据帧. 在数据接收端，同样通过模 2 除法对接收到的数据进行验证. 如果余数为 0，则数据被认为未发生错误；否则，判定数据存在错误.

由于 CRC 的计算具有非线性特征，当其输入发生变化时，其对应的输出也会对应发生变化，且这种变化通常为多个比特的改变，即输出对输入的变化敏感，有助于检测数据中的多比特错误.

图 2 是本文提出的基于 CRC 的检测流程. 图中 A 表示要存储进 DRAM 中的一块输入数据. 在存储之前，计算 A 对应的冗余码 $C(A)$，附在 A 后一并存入 DRAM，称为一个数据块. 在 DRAM 中，数据可能受到攻击而发生改变，假设 A 变成 A' 而 $C(A)$ 变成 $C'(A)$. 从 DRAM 中读出数据时，一次突发可以读出多个数据块. 例如突发长度是 8，即 64 byte，数据块长度是 32 bit，则一次突发传输可以传输 16 个数据块. 读出后对每个数据块分别进行模 2 除法，判断数据是否发生改变. 如果判断某个数据块发生了改变，则标记这个数据块中的数据不安全，从外存中重新读取这段数据.

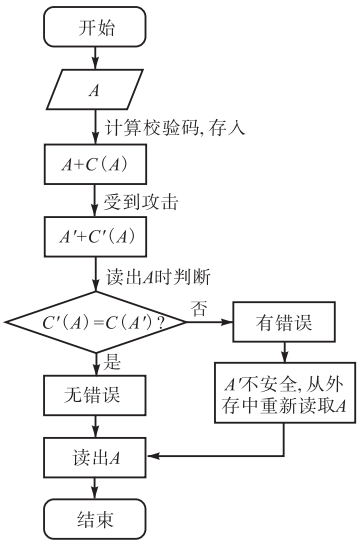


图 2　基于循环冗余校验的检测流程

Fig.2　Detection process based on CRC

在实际电磁故障注入攻击中，单次故障注入攻击可以导致连续多个比特出错. 连续出错的比特数可能超过一个数据块的长度. 一个长度较长的错误可以视作分散在多个相邻数据块的错误，分散在不同数据块的错误可以分别被检测.

根据错误发生的不同情况，有以下 4 种可能性：① $A'=A$ 且 $C'(A)=C(A)$，此时数据和校验码中均无错误，$C(A')=C'(A)$ 校验通过，数据正常进入后续计算流程；② $A'\neq A$ 且 $C'(A)=C(A)$，即错误位于数据中，此时在大概率下 $C(A')\neq C'(A)$ 校验不通过，错误被成功检出，对应数据被标记为不可信. 同时，也存在小概率情况使得 $C(A')=C(A)=C'(A)$，此时 CRC 校验出现失效；③ $A'=A$ 且 $C'(A)\neq C(A)$，即错误位于校验数据中，此时 $C(A')\neq C'(A)$ 校验不通过，数据被标记为不可信；④ $A'\neq A$ 且 $C'(A)\neq C(A)$，此时原始数据和校验数据均有错误，此时在大概率下 $C(A')\neq C'(A)$ 校验不通过，数据被标为不可信. 也有小概率情况使得 $C(A')=C'(A)$，校验也出现失效.

CRC 校验出现失效的原因如下. 可以将故障注入对原始数据的影响视作对原始数据多项式与一个多项式进行异或操作，称这个多项式为错误模式多项式. 对于 CRC，失效的本质是错误模式多项式与生成多项式存在整除关系[18]，即 CRC 是否失效取决于错误模式，而与错误比特数无关. 目前，已有针对 CRC 失效概率的相关研究. 文献[19]指出，CRC 的平均失效概率与生成多项式的最高阶数 r 有关，可以近似表示为 $1/2^r$. 因此，可以通过选择更高阶数的 CRC 来降低校验的失效概率.

2.3　检测过程中的参数选择

在实际使用中，由于 CRC 可以接受任意长度的数据作为输入，输出冗余码的长度根据 CRC 多项式最高次幂的不同也有多种尺寸可选，因此需要对信息码长度 m 和冗余码长度 n 做出合理选择. 一方面，输入输出长度的选择会影响校验的失效概率（即安全性）

和存储成本. 另一方面,在计算机系统中,DRAM 中的数据以突发长度为单位传输,选取信息码和冗余码长度的时候应当尽量考虑这个因素,使得一段信息码连带其对应的冗余码组成的数据块长度能和缓存行与突发长度对齐,以减少额外的访存需求. 即如果突发长度为 l,则应该尽量保证 $l=k(m+n)$,其中 k 是任意正整数. 为了实现安全性和性能的最优平衡,需要对各项成本进行量化,然后找到整体最优的信息码和冗余码的长度选择方案.

首先,存储成本函数 C_{s} 可以用存储额外增加的比例表示,即

$$C_{\mathrm{s}}=n/m \tag{1}$$

其次,传输成本函数 C_{t} 可以用传输次数增加的比例表示. 设 DRAM 一次突发传输的长度为 l,DRAM 中存储的数据的总长度为 L. 增加校验前传输的次数为

$$n_{\mathrm{t}}=\lceil L/l\rceil \tag{2}$$

增加冗余码后,存储数据的总长度从 L 增加为 $\frac{m+n}{m}L$,增加后的传输次数为

$$n_{\mathrm{t}}'=\left\lceil\frac{\frac{m+n}{m}L}{l}\right\rceil \tag{3}$$

即

$$C_{\mathrm{t}}=\frac{n_{\mathrm{t}}'-n_{\mathrm{t}}}{n_{\mathrm{t}}}=\frac{\left\lceil\frac{\frac{m+n}{m}L}{l}\right\rceil-\lceil L/l\rceil}{\lceil L/l\rceil} \tag{4}$$

最后,考虑安全成本函数. 尽管可以通过选择合适的 CRC 多项式确保 CRC 在数学上是均匀的,但是受限于 CRC 的原理,依然会存在失效现象. 失效现象越多,表示方法的安全性越低,因此使用失效数量衡量方法的安全性. 对于长度为 m 的信息码,其输入空间大小为 2^m,冗余码长度为 n,失效概率近似表示为 2^{-n},因此失效数量可以近似表示为 2^{m-n}. 考虑到此表达式的指数形式会导致在 m 较大时函数值过大,不利于后续分析,因此对其取对数后归一化,得到此时安全成本函数表达式为

$$C_{\mathrm{f}}=a(m-n) \tag{5}$$

式中 a 为归一化系数,其意义是控制 C_{f} 的最大值,即当 m 取值较大时(如 $m=200$),C_{f} 的值能够维持在与 C_{s} 和 C_{t} 同一数量级. 一个可行的取值方法是让 $m=m_{\max}$ 时,$C_{\mathrm{f}}=1$,以此可以反推出此时 a 的取值为 $1/(m_{\max}-n)$,其中 $m_{\max}$ 是设定的 m 的最大值. 综合上述分析,合理的 m 和 n 取值应该让 3 个指标的和最小,因此 m 和 n 的取值问题可以转化为最优化问题,即

$$\min\ F(m,n)=w_1C_{\mathrm{f}}+w_2C_{\mathrm{s}}+w_3C_{\mathrm{t}} \tag{6}$$

式中 w_1、w_2、w_3 为安全性、存储开销和传输开销 3 个指标的权重. 通过调节 3 个指标的权重,可以得到不同偏好场景下最佳参数选择.

3 检测方法的评估

3.1 检测成功率的评估

为了评估提出的方法对错误的检测率,本文搭建了针对 DRAM 的电磁故障注入攻击实验. 在攻击实验中,使用型号为镁光 MT41J256M16 的第 3 代双速率(double data rate 3,DDR3)芯片作为被攻击芯片,攻击实验平台主要由电脑、步进电机、脉冲发生器组成. 电脑作为上位机对被攻击芯片进行读写,步进电机控制脉冲发生器的探头与被芯片的相对位置,脉冲发生器产生电磁脉冲对被攻击芯片进行故障注入攻击. 芯片表面被划分成 12×7 个网格,每个网格边长为 1 mm. 攻击实验开始时,上位机生成随机数据及其对应的校验码存入被攻击芯片. 随后步进电机驱动电磁脉冲发生器的探头靠近芯片表面,开始电磁故障注入攻击. 在攻击过程中,探头沿着划分的网格遍历整个被攻击芯片表面,并在每个格点进行 20 次故障注入攻击. 当每个节点均被遍历后攻击结束,将存储的数据全部读出,执行错误检测并将读出的数据与存入的数据对比,统计总数据块数量、检测出错误的数据块数量和实际产生的错误的数据块数量. 总数据块数量等于总数据量除以每个数据块的数据量,实际产生错误的数据块指的是与存入时的数据对比,至少有 1 bit 发生改变的数据块,检测出错误的数据块指的是通过相应的校验方法,能检测出其中错误的数据块.

本文进行了多组平行实验,对不同校验方法进行对比. 由于对于同一种方法,检测率受到原始数据和校验码长度影响,为了确保数据可比性,实验中控制不同方法的原始数据与校验码的比值,即存储成本基本相同,对比检测成功率和额外传输成本. 在设定原始数据和校验码长度时,由于汉明码受原理限制,只能采用固定的原始数据和校验码长度,本文选用 4 bit 原始数据和 3 bit 校验数据,比例接近 1∶1,因此其他方法也采用相同的 1∶1 长度比. 即对于奇偶校验采用每 1 bit 原始数据分配 1 bit 校验数据,数据块长度为 2 bit,对于 CRC-8、CRC-16、CRC-32,采用每 8、

16、32 bit 原始数据分配 8、16、32 bit 校验数据，数据块长度为 16、32、64 bit. 由于不同校验方法对应的单个数据块长度不同，总数据块和出现错误的数据块数量也不完全相同. 表 1 展示了不同校验方法对应的实际检测成功率和理论上额外增加的传输成本.

可以看出，相较于传统的校验方法，基于 CRC 的校验方法有明显较高的检测成功率. 使用 CRC-16 及以上的校验可以使失效概率降低到 1×10^{-3} 以下. 在控制存储成本一致时，传输增加的比例也基本一致.

表 1　不同校验方法对应的检测成功率

Tab.1　Detection success rates for different detection methods

校验方法	出现错误的数据块数/个	检出错误的数据块数/个	检测成功率/%	传输增加/%
奇偶校验	268 433 564	125 894 731	46.9	100
汉明校验	67 115 927	62 544 950	93.2	75
CRC-8	33 554 158	33 423 967	99.6	100
CRC-16	16 816 954	16 816 937	99.9	100
CRC-32	8 388 608	8 388 608	100.0	100

3.2　检测时间消耗的评估

在读写过程中增加额外的校验步骤会带来额外的计算量，进而导致读写性能的损失. 额外的计算量可以用计算耗时衡量，计算耗时越多表明应用在校验过程中带来的性能损失越大. 为了评估对比不同方法的计算时间消耗，本文分别将不同的校验方法部署在桌面级 CPU（Intel i7-11700，主频 2.5 GHz）和嵌入式 MCU（STM32F407VG，主频 168 MHz）对攻击实验中读出的 320 Mbytes 数据进行校验计算，统计校验算法从开始到结束的运行时间. 实验结果如图 3 和图 4 所示. 可以看出，在桌面级 CPU 上，基于循环冗余的校验方法由于单次计算数据量大，相比于奇偶校验和汉明校验，在计算同等数量数据时具有较短的耗时. 部署在嵌入式设备上时，受制于嵌入式设备的计算性能，基于循环冗余的检测方法耗时与汉明校验接近，高于奇偶校验.

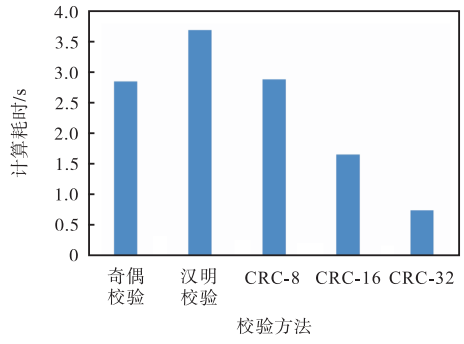


图 3　不同校验方法在桌面级处理器上的计算耗时

Fig.3　Time consumption for different check methods on desktop CPU

为了评估提出的方法在高吞吐场景下的性能损耗，本文进行了高吞吐量下的性能测试. 实验以 CRC-32 为例，测量当计算量从 1×10^6 个数据块增长至 1×10^{10} 个数据块时，这一方法计算耗时的变化. 实验结果如图 5 蓝色线所示. 可以看出计算耗时与数据块数量呈现近似线性关系. 校验计算对性能的影响可以通过算法优化缓解[20]. 在计算过程中可以建立查找表，存储每个字节值与 CRC 多项式进行模 2 除法后的结果，以查表代替计算. 图 5 中的橘黄色线展示了采用此种优化方式后的时间消耗. 可以看出，通过对方法进行优化，本文提出的方法计算耗时平均减少了约 75%.

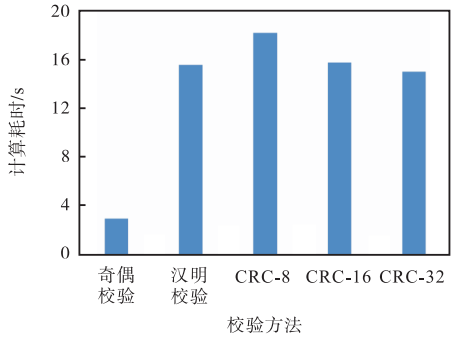


图 4　不同校验方法在嵌入式设备上的计算耗时

Fig.4　Time consumption for different check methods on embedded devices

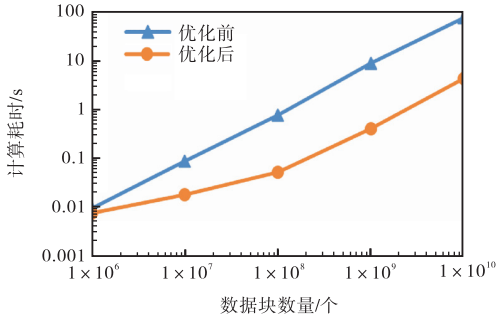


图 5　优化前后计算耗时对比

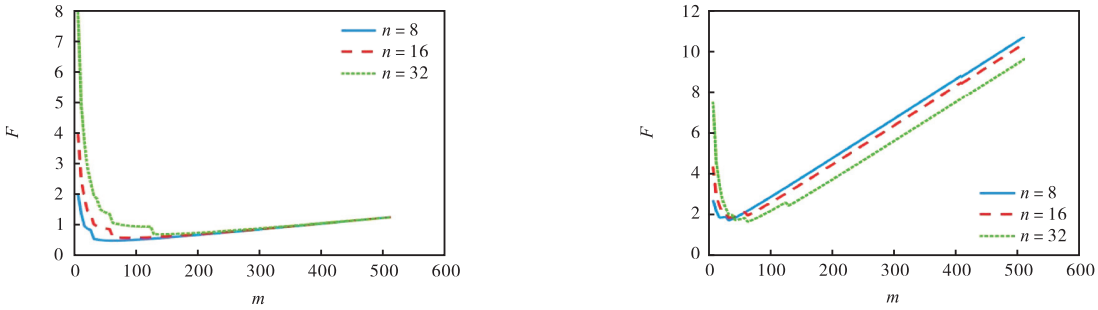
Fig.5　Comparison of time consumption before and after optimization

3.3　不同场景下的性能评估

在第 2.3 节的分析中，通过调整每一项的权重，可以求解出不同场景下的最优参数选择. 本节对 4 种典型场景的性能进行评估，分别为均衡场景、安全性场景、存储成本场景和传输成本场景，针对每种场景下的检测率、额外存储和额外传输进行评估.

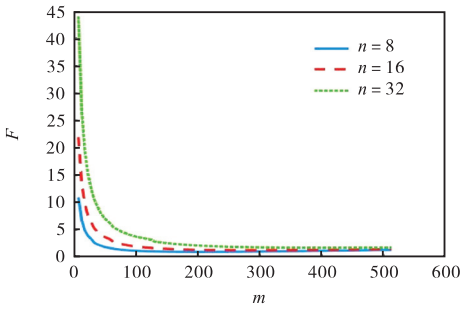
目前，一种主流的 DDR 芯片突发长度为 8[21]，假设总数据长度为 64，m 最大值为 512，n 取常见的 CRC 多项式次数 8、16、32. 在没有特殊需求的均衡场景，例如个人电脑，可以让每一项具有相同的权重，以综合考虑各项成本，因此可以取 $w_1=w_2=w_3=1$. 在注重安全性的场景下，例如密码系统，可以牺牲部分存储空间和传输性能，因此安全成本的权重应当显著高于另外两项，本文以 $w_1=10$、$w_2=w_3=1$ 为例进行分析. 在嵌入式应用、边缘计算等资源受限场景下，存储空间相对宝贵，如果处理的数据敏感性不高，则可以考虑牺牲部分安全性，选择较低的存储成本，类似地，本文以 $w_2=10$、$w_1=w_3=1$ 为例. 在服务器等需要高吞吐量的场景下，访存可能成为制约系统计算性能的瓶颈，则可以考虑选择牺牲安全性和存储空间，换取更高的传输效率，本文以 $w_3=10$、$w_1=w_2=1$ 为例. 将设定的参数和权重代入式(6)计算并绘图，可以得到图 6 所示 4 个函数图像，图中不同颜色的曲线表示不同的 n 取值，横轴表示 m 取值，纵轴表示成本函数 F 的值，函数图像最低点对应的 m 和 n 表示该场景下的最优解.

对上述 4 种参数选择进行横向对比，实验测得 4 种选择下对错误的检测成功率和额外存储开销，同时计算理论额外传输成本，如表 2 所示. 可以看出，安全场景下的最优解具有最长的冗余码和极短的信息码，这使得在实验中测得的检测成功率达到 100.0%，但是会增加 50% 的存储和传输开销；存储成本场景和传输成本场景下的最优解具有最短的冗余码和最长的信息码，但会使检测成功率降至约 87.5%；均衡场景选择适中的信息码和冗余码长度，其检测成功率、额外存储和额外传输也都介于上述两种情况之间.

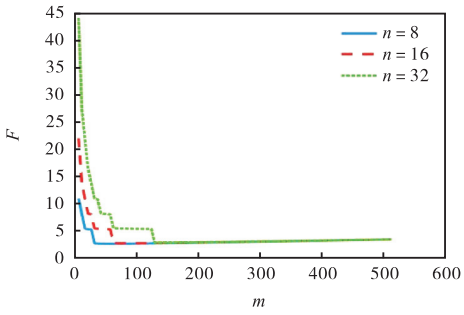


(a) 均衡场景

(b) 安全性场景



(c) 存储成本场景



(d) 传输成本场景

图 6　4种不同场景下的成本函数

Fig.6　Cost functions under four different scenarios

表 2　4种场景下最优参数选择的对比

Tab.2　Comparison of optimal parameter selection under four scenarios

场景	信息码 + 冗余码/bit	检测成功率/%	额外存储增加/%	额外传输增加/%
均衡场景	64 + 16	99.8	12.5	12.5
安全性场景	64 + 32	100.0	50.0	50.0
存储成本场景	512 + 8	87.5	1.5	1.5
传输成本场景	512 + 8	87.5	1.5	1.5

4　结　语

本文提出了一种基于循环冗余的错误检测方法，旨在检测电磁故障注入攻击对 DRAM 内数据的篡改. 基于对电磁故障注入攻击下 DRAM 数据错误特点的分析，选择循环冗余校验作为核心校验算法. 针对在校验过程中出现的安全成本、存储成本和传输成

本之间的权衡问题，通过将各项成本进行量化，将参数选择问题转化为优化问题，实现了不同场景下参数的最优选取. 最后对该方法的检测率和性能进行了详细评估，并与奇偶校验和汉明校验等传统方法进行对比. 实验结果表明，该方法具有更高的检测成功率，且相比于传统方法没有明显的性能下降.

参考文献：

[1] Narayanan V，Sankaran S. Electromagnetic fault injection attack on ASCON using ChipShouter[C]//IFIP Advances in Information and Communication Technology. Denton，USA，2024：114-131.

[2] Menu A，Dutertre J M，Rigaud J B，et al. Single-bit laser fault model in nor flash memories：Analysis and exploitation[C]//2020 Workshop on Fault Detection and Tolerance in Cryptography(FDTC). Piscataway，USA，2020：41-48.

[3] Viera R，Dutertre J M，Dumont M，et al. Permanent laser fault injection into the flash memory of a microcontroller[C]//2021 19th IEEE International New Circuits and Systems Conference(NEWCAS). Piscataway，USA，2021：1-4.

[4] Kim D，Park H，Yeo I，et al. Rowhammer attacks in dynamic random-access memory and defense methods[J]. Sensors，2024，24(2)：592.

[5] Jattke P，Wipfli M，Solt F，et al. ZenHammer：Rowhammer attacks on AMD zen-based platforms[C]//33rd USENIX Security Symposium. Berkeley，USA，2024：1615-1633.

[6] Tang H H，Liu Q. MPFA：An efficient multiple faults-based persistent fault analysis method for low-cost FIA[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems，2021，41(9)：2821-2834.

[7] Jiang Y C，Zhu H F，Shan H Q，et al. TRRScope：Understanding target row refresh mechanism for modern DDR protection[C]//2021 IEEE International Symposium on Hardware Oriented Security and Trust. Piscataway，USA，2021：239-247.

[8] Marazzi M，Jattke P，Solt F，et al. ProTRR：Principled yet optimal in-DRAM target row refresh[C]//43rd IEEE Symposium on Security and Privacy. Piscataway，USA，2022：735-753.

[9] Yaglikci A G，Patel M，Kim J S，et al. BlockHammer：Preventing rowhammer at low cost by blacklisting rapidly-accessed DRAM rows[C]//2021 IEEE International Symposium on High-Performance Computer Architecture(HPCA). Seoul，Republic of Korea，2021：345-358.

[10] Joardar B，Bletsch K，Chakrabarty K，et al. Machine learning-based rowhammer mitigation[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2023，42(5)：1395-1405.

[11] Ahr P，Lipps C，Schotten H，et al. DRAM-based physically unclonable functions and the need for proper evaluation[C]//21st European Conference on Cyber Warfare and Security. Chester，UK，2022：430-433.

[12] Liu Q，Guo L T，Tang H H. Fault model analysis of DRAM under electromagnetic fault injection attack[C]//2023 Design，Automation & Test in Europe Conference & Exhibition(DATE). Antwerp，Belgium，2023：1-6.

[13] Li Y S. Analysis and methodological advancements in software-defined error correction codes[C]//2024 4th International Signal Processing，Communications and Engineering Management Conference(ISPCEM). Montreal，Canada，2024：133-138.

[14] Selvi M，Jeeva S，Jaswanth J. Review of performance of LDPC codes for various OFDM systems[C]//2024 5th International Conference on Mobile Computing and Sustainable Informatics(ICMCSI). Lalitpur，Nepal，2024：864-869.

[15] Gaine C，Aboulkassimi D，Pontié S，et al. Electromagnetic fault injection as a new forensic approach for SoCs[C]//2020 IEEE International Workshop on Information Forensics and Security(WIFS). New York，USA，2020：1-6.

[16] Renner J，Jerkoviys T，Bartz H. Efficient decoding of interleaved low-rank parity-check codes[EB/OL] https://arxiv. org/abs/1908.10839，2019-08-28.

[17] Jiang Y N. Analysis of bit error rate between BCH code and convolutional code in picture transmission[C]//2022 3rd International Conference on Electronic Communication and Artificial Intelligence(IWECAI). Zhuhai，China，2022：77-80.

[18] Schiller F，Mattes T，Weber U，et al. Undetectable manipulation of CRC checksums for communication and data storage[C]//International Business Conference on Communications and Networking in China. Hangzhou，China，2008：1-9.

[19] Owunwanne D N. Analysis of the effectiveness of error detection in data transmission using polynomial code method[J]. International Journal of Management & Information Systems，2010，14(2)：105-112.

[20] Pan Y，Ge N，Dong Z W. CRC look-up table optimization for single-bit error correction[J]. Tsinghua Science & Technology，2007，12(5)：620-623.

[21] Micron Technology Inc. MT41K64M16TW-107 AAT-J：DDR3 SDRAM Part Catalog[EB/OL]. https://www.micron.com/products/memory/dram-components/ddr3-sdram/part-catalog/part-detail/mt41k64m16tw-107-aat-j，2018-05-20.

（责任编辑：孙立华）