用于收发器的灵活置乱器 / 解置乱器架构

摘要

本发明涉及一种设备，其包含具有多个位的多项式寄存器（510），其中所述多项式寄存器经配置以存储用户定义的多项式。收发器（406、408）耦合到第一总线、第二总线及所述多项式寄存器。所述收发器包含：自同步置乱器（502），其经配置以使用所述用户定义的多项式从第一信号产生经置乱信号；及自同步解置乱器（506），其经配置以使用所述用户定义的多项式从第二信号产生经解置乱信号。
1. 一种设备，其包括：
多项式寄存器，其具有多个位，其中所述多项式寄存器经配置以存储用户定义的多项式；
第一总线；
第二总线；以及
收发器，其耦合到所述第一总线、所述第二总线及所述多项式寄存器，其中所述收发器包含：
自同步置乱器，其经配置以使用所述用户定义的多项式从第一信号产生经置乱信号；以及
自同步解置乱器，其经配置以使用所述用户定义的多项式从第二信号产生经解置乱信号。

2. 根据权利要求 1 所述的设备，其中所述第一总线进一步包括第一输入总线及第二输入总线，且其中所述第二总线进一步包括第一输出总线及第二输出总线，且其中所述收发器进一步包括：
发射器，其具有耦合到所述第一输入总线及所述自同步置乱器的编码器，其中所述自同步置乱器耦合到所述第一输出总线；以及
接收器，其具有耦合到所述第二输出总线及所述自同步解置乱器的解码器，其中所述自同步解置乱器耦合到所述第二输入总线。

3. 根据权利要求 2 所述的设备，其中所述第一输入总线具有可编程宽度。

4. 根据权利要求 2 所述的设备，其中所述自同步置乱器及自同步解置乱器中的每一者进一步包括：
第一矩阵电路，其经配置以包含对应于所述用户定义的多项式的第一矩阵；
第二矩阵电路，其经配置以包含对应于所述用户定义的多项式的第一矩阵；
第一乘法器，其耦合到所述第二矩阵电路且耦合到所述编码器及所述第二输入总线中的相应一者；
数据寄存器；
第二乘法器，其耦合到所述第一矩阵电路及所述数据寄存器；以及
“异或”电路，其耦合到所述第一及第二乘法器且耦合到所述第一输出总线及所述解码器中的相应一者。

5. 根据权利要求 4 所述的设备，其中所述自同步置乱器的所述数据寄存器耦合到所述编码器，且其中所述自同步解置乱器的所述数据寄存器耦合到所述第二输入总线。

6. 根据权利要求 5 所述的设备，其中所述多项式寄存器具有 32 个位。

7. 一种方法，其包括：
从具有多个位的多项式寄存器检索用户定义的多项式；
至少部分地基于所述用户定义的多项式而产生第一及第二矩阵；
将所述第一矩阵乘以第一数据集以产生第二数据集；
从数据寄存器检索第三数据集；
将所述第三数据集乘以所述第二矩阵以产生第四数据集；
对所述第二与第四数据集进行“异或”运算以产生第五数据集；以及
输出所述第五数据集。
8. 根据权利要求 7 所述的方法，其中所述方法进一步包括将所述第五数据集加载到所述数据寄存器中以形成所述第三数据集。
9. 根据权利要求 8 所述的方法，其中所述输出步骤进一步包括经由总线输出所述第五数据集。
10. 根据权利要求 7 所述的方法，其中所述方法进一步包括将所述第一数据集加载到所述数据寄存器中以形成所述第三数据集。
11. 一种设备，其包括：
    媒体接入控制 MAC 电路；
    接口，其耦合到所述 MAC 电路；
    物理收发器 PHY，其具有；
    物理译码子层 PCS 逻辑，其具有；
    多项式寄存器，其具有多个位，其中所述多项式寄存器经配置以存储用户定义的多项式；
    总线，其耦合到所述接口；
    编码器，其耦合到所述总线；
    自同步置乱器，其耦合到所述编码器及第一输出总线，其中所述自同步置乱器经配置以使用所述用户定义的多项式从第一信号产生经置乱信号；
    解码器，其耦合到所述总线；以及
    自同步解置乱器，其经配置以使用所述用户定义的多项式从第二信号产生经解置乱信号；
    前向错误校正 FEC 逻辑，其耦合到所述 PCS 逻辑；
    物理媒体附接 PMA 逻辑，其耦合到所述 FEC 逻辑；以及
    物理相依媒体 PMD 逻辑，其耦合到所述 PMA 逻辑。
12. 根据权利要求 11 所述的设备，其中所述 PCS 逻辑进一步包括：
    第一齿轮箱，其耦合于所述自同步置乱器与所述 FEC 逻辑之间；以及
    第二齿轮箱，其耦合于所述自同步解置乱器与所述 FEC 逻辑之间。
13. 根据权利要求 12 所述的设备，其中所述总线具有可编程宽度。
14. 根据权利要求 13 所述的设备，其中所述自同步置乱器及自同步解置乱器中的每一者进一步包括：
    第一矩阵电路，其经配置以包含对应于所述用户定义的多项式的矩阵第一矩阵；
    第二矩阵电路，其经配置以包含对应于所述用户定义的多项式的矩阵第二矩阵；
    第一乘法器，其耦合到所述第二矩阵电路且耦合到所述编码器及第二输入总线中的相应者；
    数据寄存器；
    第二乘法器，其耦合到所述第一矩阵电路及所述数据寄存器；以及
    “异或”电路，其耦合到所述第一及第二乘法器。
15. 根据权利要求 15 所述的设备，其中所述设备进一步包括：
    主机，其耦合到所述 MAC 电路；以及
通信媒体，其耦合到所述 PHY。
16. 根据权利要求 16 所述的设备，其中所述多项式寄存器具有 32 个位。
用于收发器的灵活置乱器 / 解置乱器架构

技术领域
[0001] 本发明大体来说涉及一种收发器，且更特定来说，涉及一种具有灵活架构的物理收发器（PHY）。

背景技术
[0003] 然而，此处所关注的是 PHY 110-1 到 110-N，且如在图 2 中可更详细地看到，PHY 1101 到 110-N（下文称 PHY 110），PHY 110 采用数个子层。此 PHY 110 可为独立集成电路 (IC) 或可与 MAC 电路（即，MAC 电路 106-1）及 MII 108 集成在一起。如所示，PHY 110 通常由以下各项构成：物理层媒体依（PMD）子层逻辑 212，物理媒体附接（PMA）子层逻辑 210，前向错误校正（FEC）子层逻辑 204，及物理模拟子层逻辑 202。这些子层逻辑电路 202、204、210 及 212 彼此交互以在 MII 108 与通信媒体 112 之间提供通信。对于发射，FEC 子层逻辑 204 采用如 IEEE 标准 802.3-2008 第 74 款中所描述的编解码器 206，且对于接收，FEC 子层逻辑 204 采用如 IEEE 标准 802.3-2008 第 74 款中所描述的编解码器 308。
[0004] 如在图 3 中可看到，PCS 子层逻辑 202 可为具有 PCS 发射器 302 及 PCS 接收器 304 的收发器。在此实例中，发射器 302 能够从 MII 108 接收数据，借助编解码器 306 对数据进行编码，借助置乱器 308 对经编码数据进行置乱，并借助齿轮箱 310 进行转换（以便由 FEC 子层逻辑 204 使用）。在此实例中，接收器 304 能够使用齿轮箱 312 转换来自 FEC 子层逻辑 204 的数据、借助解置乱器 314 对数据进行解置乱，并借助解解码器 316 对数据进行解码（以供与 MII 108 一起使用）。举例来说，PCS 子层逻辑 202 的细节可见于 IEEE 标准 802.3-2008 第 48 及 74 款中。
[0005] 此处所关注的是置乱器 308 及解置乱器 314。在此实例中，置乱器 308 及解置乱器 314 能够执行数据置乱 / 解置乱及错误检查。借助 PHY 110-1 到 110-N 对数据进行置乱 / 解置乱的一个目的是实质上将数据随机化以减少电磁干扰（EMI）的影响且改进信号完整性。这通常通过使用借助指定多点产生的伪随机位序列（PRBS）来实现。举例来说，对于 8b/10b 码，可采用 PRBS-7（或 1+x^8+x）且对于同步光学连网或 SONET（如 ITU 0.150 中所指定），可采用 PRBS-23（或 x^23+x^{18}+1）。类似地，可采用此 PRBS 信令来进行错误检查。
[0006] 然而，如上文所证实，一个多功能通常并不适用于所有标准（例如，802.3-2008 及
SONET)，每一标准通常指定其自身的多项式。惯例上，这意味着每一 PHF（例如，110-1）将针对特定标准加以设计（例如，针对 802.3-2008，为 PRBS-7）且将缺乏与其它标准一起使用的灵活性。造成这种情形的原因是，用于 PHF（例如，110-1）的串行及并行实施方案将在面积、价格及功率消耗方面过于昂贵以致不能普遍适用。

[0007] 因此，需要一种灵活的收发器架构。


发明内容

[0009] 根据一实施例，提供一种设备。所述设备包括：多项式寄存器，其具有多个位，其中所述多项式寄存器经配置以存储用户定义的多项式；第一总线；第二总线；及收发器，其耦合到所述第一总线、所述第二总线及所述多项式寄存器，其中所述收发器包含：自同步位乱器，其经配置以使用所述用户定义的多项式从第一信号产生经位乱信号；及自同步解位乱器，其经配置以使用所述用户定义的多项式从第二信号产生经位乱信号。

[0010] 根据一实施例，所述第一总线进一步包括第一输入总线及第二输入总线，且其中所述第二总线进一步包括第一输出总线及第二输出总线，且其中所述收发器进一步包括：发射器，其具有耦合到所述第一输入总线及所述第二输入总线的编码器，其中所述自同步乱器耦合到所述第一输出总线；及接收器，其具有耦合到所述第二输出总线及所述自同步解位乱器的解码器，其中所述自同步解位乱器耦合到所述第二输入总线。

[0011] 根据一实施例，所述第一输入总线具有可编程宽度。

[0012] 根据一实施例，所述自同步位乱器及自同步解位乱器中的每一者进一步包括：第一矩阵电路，其经配置以包含对应于所述用户定义的多项式的第一矩阵；第二矩阵电路，其经配置以包含对应于所述用户定义的多项式的第一矩阵；第一乘法器，其耦合到所述第二矩阵电路且耦合到所述编码器及所述第二输入总线中的相应一者；数据寄存器，第二乘法器，其耦合到所述第一矩阵电路及所述数据寄存器；及‘异或’电路，其耦合到所述第一及第二乘法器且耦合到所述第一输出总线及所述解码器中的相应一者。

[0013] 根据一实施例，所述自同步位乱器的所述数据寄存器耦合到所述编码器，且其中所述自同步解位乱器的所述数据寄存器耦合到所述第二输入总线。

[0014] 根据一实施例，所述多项式寄存器具有 32 个位。

[0015] 根据一实施例，提供一种方法。所述方法包括：从具有多个位的多项式寄存器检索用户定义的多项式；至少部分地基于所述用户定义的多项式而产生第一及第二矩阵；将所述第一矩阵乘以所述数据集以产生第二数据集；从数据寄存器检索第三数据集；将所述第二数据集乘以所述第二矩阵以产生第四数据集；对所述第二与第四数据集进行“异或”运算以产生第五数据集；及输出所述第五数据集。

[0016] 根据一实施例，所述方法进一步包括将所述第五数据集加载到所述数据寄存器中以形成所述第三数据集。
附图说明
[0024] 图 1 是常规系统的实例的图；
[0025] 图 2 是图 1 的 PHY 的实例的图；
[0026] 图 3 是图 2 的 PCS 子层逻辑的图；
[0027] 图 4 及 5 是根据本发明的实施例的 PCS 子层逻辑的实例的图；
[0028] 图 6 是图 4 及 5 的可编程发射及接收电路的实例的图；
[0029] 图 7 是图 6 的置乱器的实例的图；以及
[0030] 图 8 是图 6 的解置乱器的实例的图。

具体实施方式
[0031] 图 4 及 5 说明收发器 400-A 及 400-B 的实例。所说明收发器 400-A 可用作图 3 的 PCS 子层逻辑 202 的一部分，且如图 5 的实例中所展示，收发器 400-B 可用于与串行化器/解串行化器 (SERDES) 装置进行通信。其它实施方案也可使用收发器 400-A 及 400-B，包含省略编码器 306 及解码器 316 的实施方案。在每一情况中，收发器 400-A 及 400-B 均采
用可基于用户指定或用户定义的多项式执行置乱 / 解置乱及错误检查的可编程发射电路 406-A/406-B 及可编程接收电路 408-A/408-B。

图 6 更详细地说明可编程发射电路 406-A/406-B 及可编程接收电路 408-A/408-B（下文称为 406 及 408）。电路 406 与 408 可共同被视作收发器。如此实例中所显示，电路 406 通常包括 PRBS 产生器 504 及置乱器 502，而电路 408 通常包括解置乱器 506 及 PRBS 检查器 508。如所展示，还可能存在与 PRBS 产生器 504 及 508 进行通信的检测器 512。此检测器 512 可致使 PRBS 产生器 504 经由通信媒体（例如，112）发射 PRBS 数据集并从 PRBS 检查器 508 接收位错误。基于此信息，检测器 512 可通过发射重复的 PRBS 数据集（在每一调整反复之后）并接收位错误来搜索最优设定，或其可对通信信道（例如，114）进行表征，从而允许检测器 512 检测通信媒体类型（例如，双绞线、光学等等）。另外，与置乱器 502 及解置乱器 506 进行通信的总线可具有可编程宽度（例如，最大宽度为 32 个位，但可向下调整到 1 个位）。

此外，如在图 6 的实例中可看到，其展示了多项式寄存器 510。此多项式寄存器 510 通常具有用户可存取的预定宽度或位数目（例如，32 位）。用户能够向此寄存器 510 写入以便存储用户定义的多项式。作为一实例，如果用户选择用于置乱器 502 使用 PRBS-7（其具有多项式 1+x^5+x^7），那么所述用户可将以下序列写入到 32 位寄存器（例如，寄存器 510）：

```
0000000000000000000000000000000000000000000000000000000000001
```

因此，对于具有 32 位宽度的实例性寄存器（例如，5），用户可指定大约 2x10^9 个多项式中的任一个。此用户定义的多项式（可从寄存器 510 检索所述多项式）可相应地由置乱器 502、PRBS 产生器 504、解置乱器 506 及 PRBS 检查器 508 使用。替代地，可存在多个多项式寄存器（例如，510），且置乱器 502、PRBS 产生器 504、解置乱器 506 及 PRBS 检查器 508 中的每一者可具有单独的多项式寄存器（例如，510）。

转到图 7，可更详细地看到置乱器 502 的实例。在操作中，矩阵电路 602 及 604 可使用信号 POLY（其通常对应于存储于寄存器 510 中的用户定义的多项式）来产生矩阵，所述矩阵可分别称为多项式状态矩阵（或 P 矩阵）及数据矩阵或（D 矩阵）。P 矩阵 P 及 D 矩阵 D 通常为用户提供定义的多项式的函数或至少部分地基于用户定义的多项式的正方形二进制矩阵。形成 P 矩阵 P 及 D 矩阵 D 的基础是识别矩阵 I_P 及 I_D（分别地），识别矩阵 I_P 及 I_D 通常具有用于 P 矩阵 P 及 D 矩阵及 D 的第一行的第一列的每一列的唯一指派向量（即，P_{i,j} 及 D_{i,j}）。以下可看到识别矩阵 I_P 的实例：

```
[0037]
识别矩阵 $I_D$ 通常由基于所要输入总线宽度而移位或调整的矩阵 $I_P$ 构成。举例来说，对于 20 位总线宽度，识别矩阵 $I_D$（其是从上文所展示的矩阵 $I_P$ 导出）可为如下：

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
[0038]
[0040] 还确定调整向量 \( \vec{A} \)。通常，当发射信号 POLY1 时，截断最低位，并将 ‘0’ 附加到信号
POLY1 以形成调整向量 $\vec{A}$。举例来说，在上文所使用的 PRBS-7 多项式的情况下，调整向量 $\vec{A}$ 将为：

$$
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
$$

[0041]

接着可确定 P 矩阵 $P$ 及 D 矩阵 $D$。

[0042] 首先参看 P 矩阵 $P$, 可通过使用矩阵集 (例如, 32×32 矩阵) 逐步地来确定 P 矩阵 $P$。所述矩阵集可称作工作矩阵 $\overline{W}\mathbf{r}[r]$, 其中 r 表示 P 矩阵 $P$ 行。在此实例中，这些工作矩阵 $\overline{W}\mathbf{r}[r]$ 是至少部分地基于识别矩阵 $I_P$ 且可使用以下公式来确定：

[0044] $\overline{W}\mathbf{r}[r] = \left\{ \begin{array}{l}
WP[0] = I_P \\
WP[i, j][r] = WP[i-1, j-1][r], 1 \leq r, i, j \leq n; 2 \leq j \leq n \\
WP[i, 0][r] = FNP[r], 1 \leq r \leq n
\end{array} \right.$

[0045] 其中

[0046] $FNP[r] = (WP[j][r-1] \oplus \overline{A}) \cdots (WP_0[r-1] \oplus \overline{A})$

[0047] 接着可通过应用以下方程式来从工作矩阵 $\overline{W}\mathbf{r}[r]$ 提取 P 矩阵 $P$；

[0048] $P_{i, j} = \left\{ \begin{array}{l}
0, \quad i > BW \\
WP[i, j][BW-1]
\end{array} \right.$

[0049] 其中 BW 为总线宽度。举例来说，在上文所使用的 PRBS-7 多项式以及 20 位总线宽度 BW 的情况下，P 矩阵 $P$ 应为：

$$
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
$$

[0051]
说明 书

[0052] 类似地，对于 D 矩阵 $\mathbf{D}$，可通过使用矩阵集（例如：32-32x32 矩阵）或工作矩阵 $\mathbf{WD}[r]$ 逐行地确定 D 矩阵 $\mathbf{D}$。在此实例中，这些工作矩阵 $\mathbf{WD}[r]$ 是至少部分地基于识别矩阵 $I_D$ 且可使用以下公式来确定：

\[
\mathbf{WD}[r] = \begin{cases} 
\mathbf{WD}[0] = I_D \\
\mathbf{WD}_{i,j}[r] = \mathbf{WD}_{i-1,j-1}[r], 1 \leq r, i \leq n; 2 \leq j \leq n \\
\mathbf{WD}_{i,0}[r] = \mathbf{FND}[r], 1 \leq r \leq n 
\end{cases}
\]

[0053] 其中

\[
\mathbf{FND}[r] = (\mathbf{WD}[r-1] \oplus \mathbf{A}) \cdots (\mathbf{WD}_0[r-1] \oplus \mathbf{A}).
\]

[0054] 接着，可通过应用以下方程式从工作矩阵 $\mathbf{WD}[r]$ 提取 D 矩阵 $\mathbf{D}$：

12
(6) \[ D_{i,j} = \begin{cases} 0, & i > BW \\ \text{否则} & WD_{i,j}[BW-1] \end{cases} \]

一旦已分别通过矩阵电路 602 及 604 产生了 P 矩阵 \( \mathbf{P} \) 及 D 矩阵 \( \mathbf{D} \)，便得到置乱器 502 的输入数据 \( \text{DATAIN1} \)。乘法器 606 可将输入数据 \( \text{DATAIN1} \)（举例来说，其可为 20 位宽数据向量）乘以 D 矩阵 \( \mathbf{D} \)。可借助乘法器 612 将 P 矩阵 \( \mathbf{P} \) 乘以存储于寄存器 610 中的信息（例如，向量）。可接着借助电路 608 对乘法器 606 与 612 的输出进行“异或”运算，将其写入到寄存器 610，并输出（例如，作为输出数据向量 \( \text{DATAOUT1} \)）。因此，置乱器 502 可充当使用用户定义的多项式以便允许置乱器 502 符合多种多样的标准（例如，通信协议）的自同步置乱器或并行乘法置乱器。

在图 8 中可看到，解置乱器 506 以与置乱器 502 的方式类似的方式进行操作。矩阵电路 702 及 704 可以与上文关于矩阵电路 602 及 604 所描述的方式类似的方式来计算 P 矩阵 \( \mathbf{P} \) 及 D 矩阵 \( \mathbf{D} \)，且乘法器 706 及 712、寄存器 710 及“异或”电路 708 可执行与置乱器 502 中的乘法器 606 及 612、寄存器 610 以及“异或”电路 608 相同的函数。一个差异为，在每一循环（举例来说），将输入数据向量 \( \text{DATAIN2} \) 写入到寄存器 710，而非写入数据输出向量 \( \text{DATAOUT2} \)（这将对应于置乱器 502 的操作）。与置乱器 502 一样，解置乱器 506 可充当使用用户定义的多项式以便允许解置乱器 502 符合多种多样的标准（例如，通信协议）的自同步解置乱器或并行乘法解置乱器。

所属领域的技术人员将了解，在所主张发明的范围内，可对所描述的实施性实施方案做出修改，且也存在许多其它实施例。
图 1（现有技术）

图 2（现有技术）
图3（现有技术）

图4
图 5

图 6