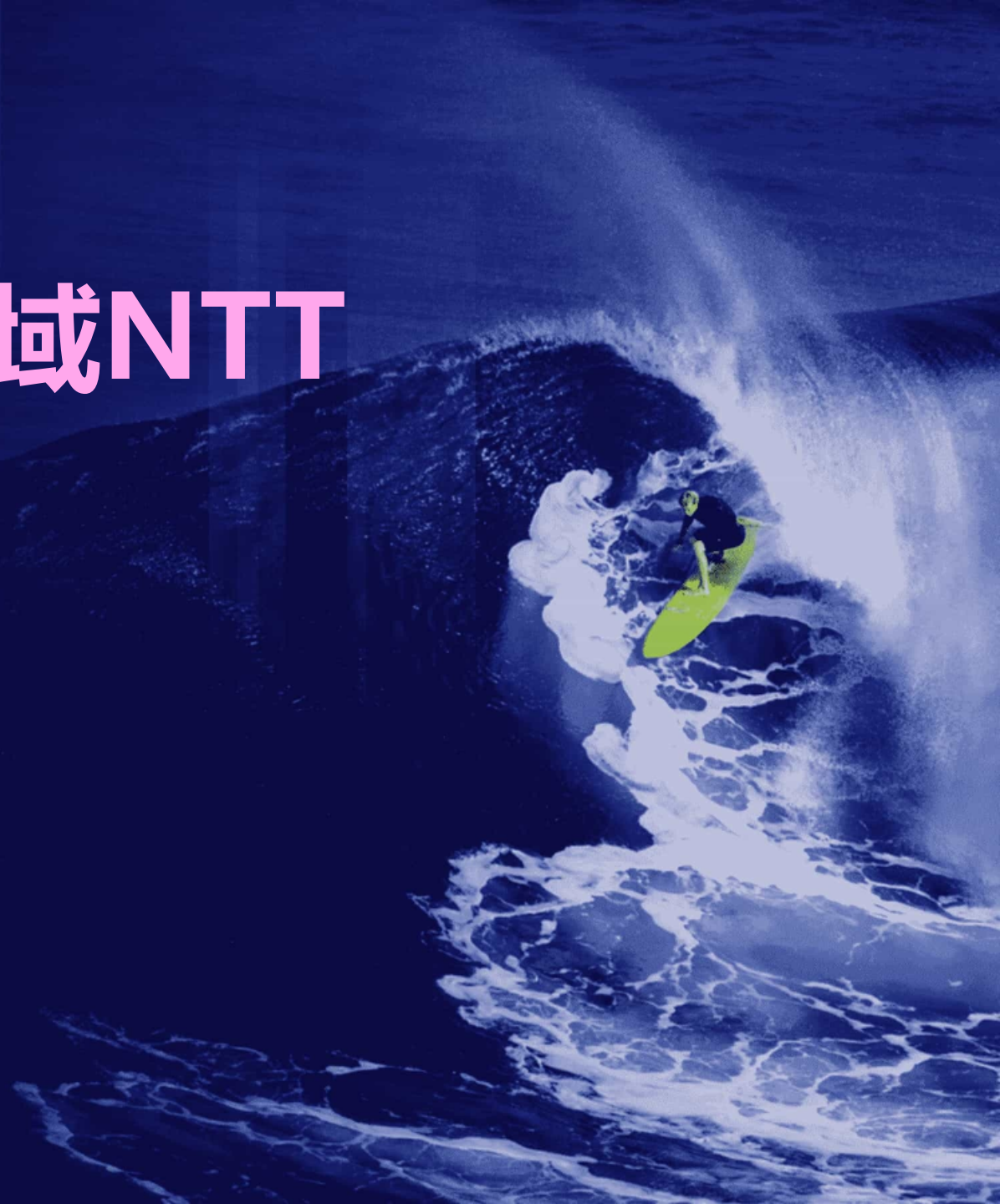
基于FPGA的有限域NTT算法设计与实现



汇报人：

2024-01-22

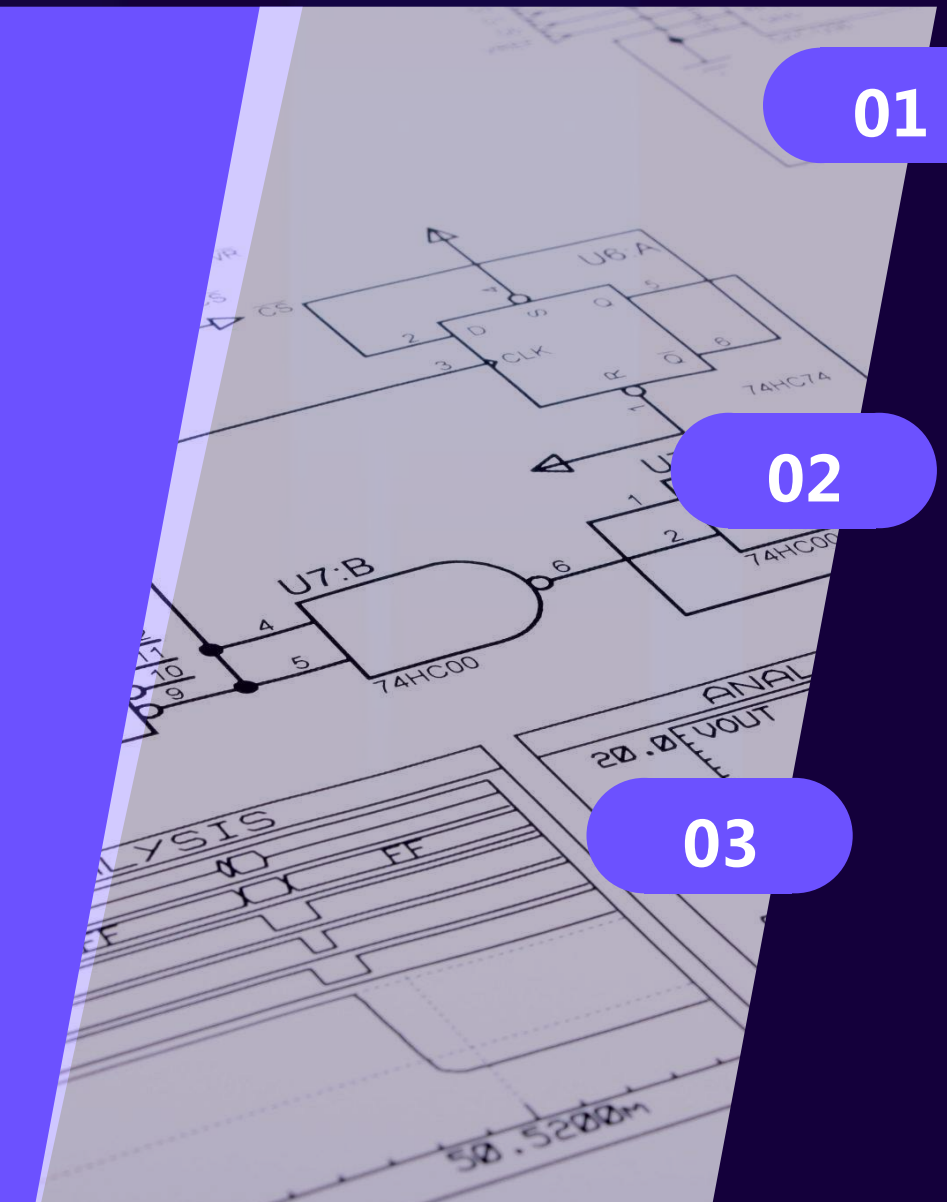
目录

contents

01

引言

研究背景与意义



01

有限域NTT算法是数论变换（Number Theoretic Transform，NTT）在有限域上的实现，具有高效、精确和可并行计算等优点，被广泛应用于多项式乘法、大数运算、密码学等领域。

02

随着大数据时代的到来，对高性能计算的需求日益增长，有限域NTT算法的高效实现对于提高计算速度、降低计算复杂度具有重要意义。

03

FPGA（Field Programmable Gate Array）作为一种可编程逻辑器件，具有并行处理、高灵活性、低功耗等优点，适合用于实现有限域NTT算法等高性能计算任务。

国内外研究现状及发展趋势

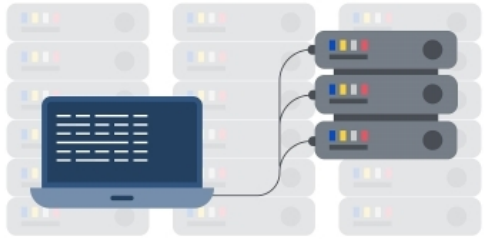
国内外研究现状

目前，有限域NTT算法已经在多个领域得到了广泛应用，如多项式乘法、大数运算、密码学等。同时，基于FPGA的有限域NTT算法实现也取得了一定的研究成果，但仍存在一些挑战和问题，如资源利用率不高、计算精度不够等。

发展趋势

随着FPGA技术的不断发展和完善，基于FPGA的有限域NTT算法实现将更加注重高性能、高效率和低功耗等方面的优化。同时，随着人工智能、云计算等技术的快速发展，有限域NTT算法的应用领域将进一步拓展。

研究内容、目的和方法



研究内容

本研究旨在设计和实现一种基于FPGA的有限域NTT算法，通过优化算法设计和FPGA实现方式，提高有限域NTT算法的计算效率和资源利用率。

研究目的

通过本研究，期望能够实现一种高性能、高效率的基于FPGA的有限域NTT算法，为多项式乘法、大数运算、密码学等领域的应用提供有力支持。

研究方法

本研究将采用理论分析和实验验证相结合的方法进行研究。首先，对有限域NTT算法进行理论分析，确定算法的关键技术和优化方向；然后，基于FPGA平台进行算法设计和实现，并通过实验验证算法的性能和效率。

02

FPGA技术基础

FPGA概述

FPGA（Field Programmable Gate Array）即现场可编程门阵列，是一种可编程使用的信号处理芯片，具有高度的灵活性和并行处理能力。

FPGA内部包含大量的可编程逻辑单元和可编程互连资源，用户可以通过编程来配置这些资源，实现复杂的数字逻辑功能。

与ASIC相比，FPGA具有更短的开发周期、更低的开发成本和更高的灵活性，因此在通信、图像处理、视频处理等领域得到了广泛应用。

FPGA基本结构

可编程逻辑单元（CLB）

CLB是FPGA内的基本逻辑单元，由查找表（LUT）和寄存器组成，可以实现组合逻辑和时序逻辑功能。

可编程互连资源（IR）

IR用于连接FPGA内部的各个逻辑单元，构成复杂的逻辑网络。IR包括各种长度的线段、连接点和开关等。

输入/输出单元（IOB）

IOB是FPGA与外部电路的接口部分，用于实现信号的输入和输出。

配置逻辑单元（CFG）

CFG用于存储FPGA的配置信息，包括逻辑单元的功能和互连资源的连接关系等。在FPGA上电后，配置逻辑单元将配置信息加载到FPGA中，实现电路功能。

FPGA设计流程

需求分析

明确设计目标，分析系统需求，确定FPGA需要实现的功能和性能指标。

综合与布局布线

将硬件描述语言代码进行综合，生成门级网表。然后进行布局布线，将门级网表映射到FPGA芯片上。

算法设计

根据系统需求，设计相应的算法，并进行仿真验证。

功能仿真与验证

对布局布线后的设计进行功能仿真和验证，确保设计功能的正确性。

硬件描述语言编程

使用硬件描述语言（如VHDL或Verilog）对算法进行描述，编写相应的代码。

下载与调试

将验证通过的设计下载到FPGA芯片中，进行实际调试和运行。

03

有限域NTT算法原理

有限域基本概念

有限域定义

有限域是包含有限个元素的域，具有加法和乘法两种运算，并满足域的性质。

有限域特征

有限域中元素的个数必须是某个素数的幂，且有限域具有循环性和对称性。

有限域在密码学中的应用

有限域在密码学中广泛应用于加密算法、数字签名、密钥交换等领域，提供高效且安全的计算环境。

NTT算法原理及优势

01

NTT算法原理

NTT（Number Theoretic Transform）算法是一种基于数论的快速变换算法，用于在有限域上进行多项式乘法运算。它将多项式表示为点值形式，通过选取适当的模数和根，实现快速且精确的多项式乘法。

02

NTT算法优势

相比于传统的多项式乘法算法，NTT算法具有更高的计算效率和更低的复杂度。它利用有限域的性质和快速傅里叶变换（FFT）的思想，通过减少运算次数和降低数据精度，实现高效的多项式乘法计算。

03

NTT算法在密码学中的应用

NTT算法在密码学中用于加速多项式运算，如椭圆曲线密码体制中的标量乘法和格密码体制中的多项式乘法等。它可以提高密码算法的执行效率，降低计算资源的消耗。