Groth16 算法为 Poseidon2 电路生成证明

一、概述

Groth16 是一种高效的零知识证明算法，具有证明体积小、验证速度快的特点，非常适合与 Circom 生成的电路配合使用。本文档详细介绍为 Poseidon2 哈希电路生成零知识证明的完整流程，包括环境准备、电路编译、信任设置、证明生成与验证等关键步骤，旨在帮助使用者快速掌握基于 Groth16 的 Poseidon2 电路证明生成方法。

二、程序

1、电路编译

电路编译是将 Circom 代码转换为可用于生成证明的约束系统等文件的过程。

执行编译命令：

在包含 Poseidon2 电路代码（poseidon2.circom）的目录下，运行以下命令：

```
circom poseidon2.circom --r1cs --wasm --sym
```

生成文件说明：

poseidon2.r1cs：电路的约束系统文件，描述了电路中的所有约束条件。

poseidon2_js/：目录中包含 WebAssembly 模块（poseidon2.wasm）和生成见证的 JavaScript 代码（generate_witness.js）。

poseidon2.sym：符号表文件，用于调试和映射变量与约束的关系。

2、准备输入数据

输入数据需包含公开输入的预期哈希值和隐私输入的哈希原象，以 JSON 格式存储。

创建输入文件：

在当前目录下创建 input.json 文件，内容如下：

```
{
    "expectedHash": 123456789,  // 替换为实际计算的哈希值
    "preimage": [987654321, 1122334455]  // 替换为实际的原象
}
```

3、生成见证（Witness）

见证是满足电路约束的输入数据映射，用于后续证明生成。

执行生成命令：

进入 poseidon2_js 目录，运行生成见证的脚本：

```
cd poseidon2_js
node generate_witness.js poseidon2.wasm ../input.json ../witness.wtns
cd ..
```

生成文件：在上级目录生成 witness.wtns 文件，即见证文件。

4、信任设置（Trusted Setup）

信任设置是 Groth16 算法中的关键步骤，分为通用预处理和电路特定处理阶段。

获取 Powers of Tau 文件：

Powers of Tau 是通用的预处理阶段产物，与具体电路无关。若当前目录不存在 pot12_final.ptau 文件，可通过以下命令下载：

```
wget https://hermez.s3-eu-west-1.amazonaws.com/powersOfTau28_hez_final_12.ptau -O pot12_final.ptau
```

电路特定信任设置：

运行以下命令为 Poseidon2 电路生成特定的证明密钥：

```
snarkjs groth16 setup poseidon2.r1cs pot12_final.ptau poseidon2_0000.zkey
```

生成 poseidon2_0000.zkey 文件，包含电路的证明密钥信息。

5、导出验证密钥

验证密钥用于后续证明的验证过程，运行以下命令导出：

```
snarkjs zkey export verificationkey poseidon2_0001.zkey verification_key.json
```

生成 verification_key.json 文件，包含验证证明所需的密钥信息。

6、生成零知识证明

使用见证文件和证明密钥生成零知识证明：

```
snarkjs groth16 prove poseidon2_0001.zkey witness.wtns proof.json public.json
```

生成两个文件：

proof.json：生成的零知识证明文件。

public.json：公开输入信息文件。

7、验证证明

验证生成的证明是否有效：

```
snarkjs groth16 verify verification_key.json public.json proof.json
```

若证明有效，将输出“OK”；否则，输出错误信息。