# **Polynomial Commitments – Nền Tảng Của SNARKs & STARKs**

## **Meta Description**

Polynomial Commitments giúp Zero-Knowledge Proofs (ZKP) xác minh dữ liệu mà không tiết lộ nội dung. So sánh KZG vs. FRI & ứng dụng KZG trong EIP-4844!

## **Giới Thiệu**

Trong hệ thống Zero-Knowledge Proofs (ZKP), một trong những thách thức lớn là làm sao để cam kết và xác minh các tính toán phức tạp mà không tiết lộ thông tin gốc. **Polynomial Commitment Schemes** là một giải pháp quan trọng, được sử dụng trong **zk-SNARKs và zk-STARKs**, giúp đảm bảo tính bảo mật và hiệu quả của các bằng chứng.

Trong bài viết này, chúng ta sẽ tìm hiểu:

🔹 **Polynomial Commitment Scheme là gì?** 🔹 **So sánh KZG Commitment và FRI Commitment** 🔹 **Ứng dụng của KZG Commitment trong Ethereum EIP-4844 (Proto-Danksharding)**

Hãy cùng khám phá chi tiết!

## **Key Takeaways**

✅ **Polynomial Commitment Scheme** giúp cam kết với một đa thức mà không tiết lộ nội dung, đồng thời hỗ trợ kiểm tra giá trị đánh giá mà không cần toàn bộ dữ liệu.  
 ✅ **KZG Commitment** (Kate-Zaverucha-Goldberg) sử dụng đường cong elliptic và cặp ghép để tạo cam kết nhỏ gọn, phù hợp với **zk-SNARKs**.  
 ✅ **FRI Commitment** (Fast Reed-Solomon IOP) không cần thiết lập tin cậy, bảo mật trước máy tính lượng tử, nhưng bằng chứng lớn hơn, phù hợp với **zk-STARKs**.  
 ✅ **Ethereum EIP-4844 (Proto-Danksharding)** sử dụng **KZG Commitment** để tăng khả năng mở rộng và giảm phí gas bằng cách lưu trữ dữ liệu ngoài chuỗi.

## **Polynomial Commitment Scheme Là Gì?**

[Polynomial Commitment Scheme](https://cacr.uwaterloo.ca/techreports/2010/cacr2010-10.pdf#:~:text=We%20introduce%20and%20formally%20de%20ne%20polynomial%20commitment,con%20rm%20claimed%20evaluations%20of%20the%20committed%20polynomial.) là một kỹ thuật mật mã cho phép một người gửi **cam kết với một đa thức mà không tiết lộ nội dung**, sau đó chứng minh giá trị đánh giá tại một điểm cụ thể.

### **Nguyên lý hoạt động**

Một Polynomial Commitment Scheme bao gồm ba thuật toán chính:

1️⃣ **Commit:** Người gửi chọn một đa thức f(x)f(x) và tạo cam kết CC, thường là một phần tử nhóm hoặc giá trị băm.  
 2️⃣ **Prove:** Người gửi tạo bằng chứng π\pi cho giá trị đánh giá f(z)f(z) tại một điểm zz.  
 3️⃣ **Verify:** Người kiểm tra xác minh rằng f(z)f(z) là đúng dựa trên cam kết CC và bằng chứng π\pi.

### **Tính chất bảo mật**

✔️ **Hiding**: Cam kết không tiết lộ thông tin về đa thức ngoài những gì được công bố.  
 ✔️ **Binding**: Người gửi không thể tạo hai đa thức khác nhau có cùng cam kết.

⏩ **Ứng dụng:** Polynomial Commitment Schemes được sử dụng trong **SNARKs và STARKs** để chứng minh tính đúng đắn của các tính toán phức tạp mà không tiết lộ toàn bộ dữ liệu.

## **So Sánh KZG Commitment vs. FRI Commitment**

[KZG Commitment](https://medium.com/@abhiveerhome/zero-knowledge-proofs-kzg-polynomial-commitment-and-verification-5a82d62fdefd) và [FRI Commitment](https://medium.com/@aannkkiittaa/understanding-fri-polynomial-commitments-scheme-7391da74c9d9) là hai cách tiếp cận chính để cam kết với đa thức trong SNARKs và STARKs.

### **KZG Commitment – Tối Ưu Cho SNARKs**

📌 **Mô tả:** KZG (Kate-Zaverucha-Goldberg) sử dụng **cặp ghép elliptic curve** để tạo cam kết nhỏ gọn.  
 📌 **Hiệu suất:** ✅ Kích thước cam kết và bằng chứng nhỏ (vài trăm byte).  
 ✅ Xác minh nhanh, chỉ cần vài phép toán cặp ghép.  
 📌 **Bảo mật:** ✅ Dựa trên bài toán **Discrete Logarithm Problem (DLP)**, có tính bảo mật cao.  
 ❌ Yêu cầu **thiết lập tin cậy (Trusted Setup)**, có thể là điểm yếu nếu bị xâm phạm.

### **FRI Commitment – Tối Ưu Cho STARKs**

📌 **Mô tả:** FRI (Fast Reed-Solomon IOP) sử dụng **cây Merkle** và mã hóa Reed-Solomon, không cần cặp ghép.  
 📌 **Hiệu suất:** ❌ Kích thước cam kết lớn hơn KZG, thường lên đến vài kilobytes.  
 ❌ Xác minh chậm hơn do phải kiểm tra nhiều đường dẫn trong cây Merkle.  
 📌 **Bảo mật:** ✅ **Không cần thiết lập tin cậy**, an toàn hơn trong môi trường phi tập trung.  
 ✅ **Post-quantum secure**, không bị đe dọa bởi máy tính lượng tử.

| **Tiêu chí** | **KZG Commitment** | **FRI Commitment** |
| --- | --- | --- |
| **Kích thước cam kết** | Nhỏ (vài trăm byte) | Lớn (vài kilobytes) |
| **Kích thước bằng chứng** | Nhỏ | Lớn |
| **Tốc độ xác minh** | Nhanh (cặp ghép elliptic) | Chậm hơn (cây Merkle) |
| **Yêu cầu thiết lập** | Cần Trusted Setup | Không cần |
| **Bảo mật** | Dựa trên DLP | Post-quantum secure |

📌 **Tóm lại:**

* **KZG Commitment** phù hợp với **zk-SNARKs**, nơi cần hiệu suất cao và bằng chứng nhỏ gọn.
* **FRI Commitment** phù hợp với **zk-STARKs**, nơi cần tính minh bạch và bảo mật cao hơn.

## **Ứng Dụng KZG Commitment Trong EIP-4844 (Proto-Danksharding)**

**Ethereum EIP-4844 (Proto-Danksharding)** là một nâng cấp quan trọng giúp giảm phí gas và mở rộng quy mô bằng cách **lưu trữ dữ liệu giao dịch ngoài chuỗi**.

📌 **KZG Commitment đóng vai trò gì?** 1️⃣ **Dữ liệu giao dịch được lưu dưới dạng "blob" (khối dữ liệu lớn)**.  
 2️⃣ **Mỗi blob được cam kết bằng KZG Commitment**.  
 3️⃣ **Các node xác minh dữ liệu mà không cần lưu trữ toàn bộ blob**, chỉ cần kiểm tra KZG Commitment.

📌 **Lợi ích của KZG trong EIP-4844:** ✅ **Giảm phí gas**, vì các node không cần tải toàn bộ dữ liệu.  
 ✅ **Mở rộng quy mô**, giúp Ethereum hỗ trợ nhiều giao dịch hơn.  
 ✅ **Xác minh nhanh chóng**, giúp các node nhẹ hoạt động hiệu quả hơn.

💡 **Chi tiết bất ngờ:** KZG Commitment không chỉ cải thiện **khả năng mở rộng**, mà còn giúp **Layer 2 như Optimistic Rollups và ZK-Rollups hoạt động hiệu quả hơn**, giảm chi phí giao dịch.

## **Kết Luận**

Polynomial Commitment Schemes là nền tảng quan trọng của SNARKs và STARKs, giúp xác minh tính toán mà không cần tiết lộ thông tin.

📌 **KZG Commitment** tối ưu cho **SNARKs**, với hiệu suất cao nhưng yêu cầu **Trusted Setup**.  
 📌 **FRI Commitment** phù hợp cho **STARKs**, minh bạch hơn và bảo mật trước máy tính lượng tử.  
 📌 **Ethereum EIP-4844 (Proto-Danksharding)** sử dụng **KZG Commitment** để mở rộng quy mô và giảm phí gas.

💡 **Bài tiếp theo:** zk-SNARKs - Giao Thức Zero-Knowledge Proof Cổ Điển & Trusted Setup 🚀