Scalable and Transparent Proofs over All Large Fields, via Elliptic Curves

(ECFFT Part II)

Eli Ben–Sasson
StarkWare

Dan Carmon
StarkWare

Swastik Kopparty
UToronto

David Levit
StarkWare

20th Theory of Cryptography Conference

University of Chicago, November 2022

Motivating problem

- Problem: Prove integrity of a long computation (with succinct description)
  - Transparent: No trusted setup
  - Scalable: Quasilinear Prover time, polylogarithmic Verifier time

Motivating problem

- Problem: Prove integrity of a long computation (with succinct description)
  - Transparent: No trusted setup
  - Scalable: Quasilinear Prover time, polylogarithmic Verifier time
- Solution: STIK/STARK proofs!
  - Over finite fields $\mathbb{F}_p$ with $p-1$ divisible by large power of 2, a.k.a., "FFT-friendly"

An example of a STIK

- Let $a_0 = 1, a_1 = 2$ and $a_{n+2} = a_{n+1}^2 + (-1)^n a_n^2 \pmod{p}$
- Wish to prove $a_{N-1} = A$, for $N = 2^{40}$.

An example of a STIK

- Let $a_0 = 1, a_1 = 2$ and $a_{n+2} = a_{n+1}^2 + (-1)^n a_n^2 \pmod{p}$
- Wish to prove $a_{N-1} = A$, for $N = 2^{40}$.
- Interpolate a degree $< N$ polynomial $f \in \mathbb{F}_p[X]$ with $f(\mathrm{g}^i) = a_i$, where g generates an order N subgroup of $\mathbb{F}_p^\times$.
- Evaluate f on cosets of $\langle \mathrm{g} \rangle$, and provide oracle access.

An example of a STIK

- Let $a_0 = 1, a_1 = 2$ and $a_{n+2} = a_{n+1}^2 + (-1)^n a_n^2 \pmod{p}$
- Wish to prove $a_{N-1} = A$, for $N = 2^{40}$.
- Interpolate a degree $< N$ polynomial $f \in \mathbb{F}_p[X]$ with $f(\mathrm{g}^i) = a_i$, where g generates an order N subgroup of $\mathbb{F}_p^\times$.
- Evaluate f on cosets of $\langle \mathrm{g} \rangle$, and provide oracle access.
- Prove that

$$\frac{f(X)-1}{X-1}, \quad \frac{f(X)-2}{X-\mathrm{g}}, \quad \frac{f(X)-A}{X-\mathrm{g}^{-1}},$$

$$(f(\mathrm{g}^2 X) - f(\mathrm{g}X)^2 - f(X)^2) \cdot \frac{X-\mathrm{g}^{-2}}{X^{N/2}-1},$$

$$(f(\mathrm{g}^2 X) - f(\mathrm{g}X)^2 + f(X)^2) \cdot \frac{X-\mathrm{g}^{-1}}{X^{N/2}+1}$$

are all polynomials of appropriate degrees.

An example of a STIK

- Let $a_0 = 1, a_1 = 2$ and $a_{n+2} = a_{n+1}^2 + (-1)^n a_n^2 \pmod{p}$
- Wish to prove $a_{N-1} = A$, for $N = 2^{40}$.
- Interpolate a degree $< N$ polynomial $f \in \mathbb{F}_p[X]$ with $f(\mathrm{g}^i) = a_i$, where g generates an order N subgroup of $\mathbb{F}_p^\times$.
- Evaluate f on cosets of $\langle \mathrm{g} \rangle$, and provide oracle access.
- Prove that

$$\frac{f(X)-1}{X-1}, \quad \frac{f(X)-2}{X-\mathrm{g}}, \quad \frac{f(X)-A}{X-\mathrm{g}^{-1}},$$

$$(f(\mathrm{g}^2 X) - f(\mathrm{g}X)^2 - f(X)^2) \cdot \frac{X-\mathrm{g}^{-2}}{X^{N/2}-1},$$

$$(f(\mathrm{g}^2 X) - f(\mathrm{g}X)^2 + f(X)^2) \cdot \frac{X-\mathrm{g}^{-1}}{X^{N/2}+1}$$

are all polynomials of appropriate degrees.

The FRI protocol—randomly folded FFT

- Problem: Show that $f : \mathcal{D} \to \mathbb{F}_p$ is a polynomial of degree $< \rho|\mathcal{D}|$.

The FRI protocol—randomly folded FFT

- Problem: Show that $f : \mathcal{D} \to \mathbb{F}_p$ is a polynomial of degree $< \rho|\mathcal{D}|$.
- Write $f(X) = f_0(X^2) + X f_1(X^2)$, or equivalently

$$f_0(X^2) = \frac{f(X) + f(-X)}{2}, \quad f_1(X^2) = \frac{f(X) - f(-X)}{2X}.$$

The FRI protocol—randomly folded FFT

- Problem: Show that $f : \mathcal{D} \to \mathbb{F}_p$ is a polynomial of degree $< \rho|\mathcal{D}|$.
- Write $f(X) = f_0(X^2) + X f_1(X^2)$, or equivalently

$$f_0(X^2) = \frac{f(X) + f(-X)}{2}, \quad f_1(X^2) = \frac{f(X) - f(-X)}{2X}.$$

- Let $\mathcal{D}' = \{x^2 : x \in \mathcal{D}\}$ and suppose $|\mathcal{D}'| = \frac{|\mathcal{D}|}{2}$.

The FRI protocol—randomly folded FFT

- Problem: Show that $f : \mathcal{D} \to \mathbb{F}_p$ is a polynomial of degree $< \rho|\mathcal{D}|$.
- Write $f(X) = f_0(X^2) + X f_1(X^2)$, or equivalently

$$f_0(X^2) = \frac{f(X) + f(-X)}{2}, \quad f_1(X^2) = \frac{f(X) - f(-X)}{2X}.$$

- Let $\mathcal{D}' = \{x^2 : x \in \mathcal{D}\}$ and suppose $|\mathcal{D}'| = \frac{|\mathcal{D}|}{2}$.
- Define $f' = f_0 + z \cdot f_1$, where $z \in \mathbb{F}_p$ is chosen by the verifier.
- Provide oracle access to $f' : \mathcal{D}' \to \mathbb{F}_p$, and prove it is a polynomial of degree $< \rho|\mathcal{D}'|$.

The FRI protocol—randomly folded FFT

- Problem: Show that $f : \mathcal{D} \to \mathbb{F}_p$ is a polynomial of degree $< \rho|\mathcal{D}|$.
- Write $f(X) = f_0(X^2) + X f_1(X^2)$, or equivalently

$$f_0(X^2) = \frac{f(X) + f(-X)}{2}, \quad f_1(X^2) = \frac{f(X) - f(-X)}{2X}.$$

- Let $\mathcal{D}' = \{x^2 : x \in \mathcal{D}\}$ and suppose $|\mathcal{D}'| = \frac{|\mathcal{D}|}{2}$.
- Define $f' = f_0 + z \cdot f_1$, where $z \in \mathbb{F}_p$ is chosen by the verifier.
- Provide oracle access to $f' : \mathcal{D}' \to \mathbb{F}_p$, and prove it is a polynomial of degree $< \rho|\mathcal{D}'|$.
- Rinse and repeat, until $|\mathcal{D}|$ is small.

The FRI protocol—randomly folded FFT

- Problem: Show that $f : \mathcal{D} \to \mathbb{F}_p$ is a polynomial of degree $< \rho|\mathcal{D}|$.
- Write $f(X) = f_0(X^2) + X f_1(X^2)$, or equivalently

$$f_0(X^2) = \frac{f(X) + f(-X)}{2}, \quad f_1(X^2) = \frac{f(X) - f(-X)}{2X}.$$

- Let $\mathcal{D}' = \{x^2 : x \in \mathcal{D}\}$ and suppose $|\mathcal{D}'| = \frac{|\mathcal{D}|}{2}$.
- Define $f' = f_0 + z \cdot f_1$, where $z \in \mathbb{F}_p$ is chosen by the verifier.
- Provide oracle access to $f' : \mathcal{D}' \to \mathbb{F}_p$, and prove it is a polynomial of degree $< \rho|\mathcal{D}'|$.
- Rinse and repeat, until $|\mathcal{D}|$ is small.

Elliptic curves to the rescue

- What can we do if $\mathbb{F}_p$ is not FFT-friendly?

Elliptic curves to the rescue

- What can we do if $\mathbb{F}_p$ is not FFT-friendly?
- We want an algebraic structure over $\mathbb{F}_p$, with a large cyclic 2-subgroup.
- We also need an analogue of the $x \mapsto x^2$ map and decompositions used in FFT and FRI.

Elliptic curves to the rescue

- What can we do if $\mathbb{F}_p$ is not FFT-friendly?
- We want an algebraic structure over $\mathbb{F}_p$, with a large cyclic 2-subgroup.
- We also need an analogue of the $x \mapsto x^2$ map and decompositions used in FFT and FRI.
- These can be found inside appropriate elliptic curves!

Elliptic curves to the rescue

- What can we do if $\mathbb{F}_p$ is not FFT-friendly?
- We want an algebraic structure over $\mathbb{F}_p$, with a large cyclic 2-subgroup.
- We also need an analogue of the $x \mapsto x^2$ map and decompositions used in FFT and FRI.
- These can be found inside appropriate elliptic curves!
  - Sets of points $(x, y) \in \mathbb{F}_p^2$ satisfying $y^2 = x^3 + Ax + B$
  - Come equipped with a group action
  - Sizes in the range $[p \pm 2\sqrt{p} + 1]$ depending on A, B

Elliptic curves to the rescue

Theorem

For any prime power $q \geq 7$ and any $1 < \mathsf{N} = 2^{\mathsf{n}} \leq 2\sqrt{q}$, there exist:

- *elliptic curves $E_0, E_1, \ldots, E_{\mathsf{n}}$ over $\mathbb{F}_q$ in Weierstrass form,*
- *a cyclic subgroup $G_0^{(\mathsf{n})} = \langle \mathsf{g}_0 \rangle \subseteq E_0$ of size N,*
- *2-isogenies $\phi_i : E_i \to E_{i+1}$,*
- *projection maps $\pi_i : E_i \to \mathbb{P}^1$,*
- *and rational functions $\psi_i : \mathbb{P}^1 \to \mathbb{P}^1$ of degree 2,*

such that $|\phi_{i-1} \circ \cdots \circ \phi_0(G_0^{(\mathsf{n})})| = \frac{1}{2^i}|G_0^{(\mathsf{n})}| = 2^{\mathsf{n}-i}$ and the following diagram is commutative:

$$\begin{array}{ccccccc} E_0 & \xrightarrow{\phi_0} & E_1 & \xrightarrow{\phi_1} & \cdots & \xrightarrow{\phi_{\mathsf{n}-1}} & E_{\mathsf{n}} \\ \downarrow{\scriptstyle \pi_0} & & \downarrow{\scriptstyle \pi_1} & & & & \downarrow{\scriptstyle \pi_{\mathsf{n}}} \\ \mathbb{P}^1 & \xrightarrow{\psi_0} & \mathbb{P}^1 & \xrightarrow{\psi_1} & \cdots & \xrightarrow{\psi_{\mathsf{n}-1}} & \mathbb{P}^1 \end{array} \tag{1}$$

Elliptic curve analogues

- Polynomials of degree $< N \Leftrightarrow$ Rational functions on E_0 with at most simple poles in $G_0^{(\mathsf{n}+1)}$
- Evaluations on cosets of $\langle \mathsf{g} \rangle \Leftrightarrow$ Evaluations on sets $C \cup -C$, where C is a coset of $G_0^{(\mathsf{n})}$
- Multiplying by $\mathsf{g} \Leftrightarrow$ Adding the point g_0
- Decomposition of degree $< N$ polynomials into degree $< N/2$ polynomials $\Leftrightarrow$ Decomposition of rational functions on E_0 into rational functions in one variable, and of those functions into lower degree ones
- Vanishing polynomials $\Leftrightarrow$ Rational functions with appropriate zeros and poles

Thanks for listening!

EC-FFT and EC-FRI

- Rational functions f on E_0 with poles on $G_0^{(\mathsf{n}+1)}$ can be decomposed as

$$f(X,Y) = \frac{g(X)}{\Omega_0(X)} + \frac{Y}{X}\frac{h(X)}{\Omega_0(X)}, \quad \deg(g), \deg(h) < N,$$

  where Ω_0 is a polynomial of degree $N-1$.

EC-FFT and EC-FRI

- Rational functions f on E_0 with poles on $G_0^{(\mathsf{n}+1)}$ can be decomposed as

$$f(X,Y) = \frac{g(X)}{\Omega_0(X)} + \frac{Y}{X}\frac{h(X)}{\Omega_0(X)}, \quad \deg(g), \deg(h) < N,$$

  where Ω_0 is a polynomial of degree $N-1$.

- Rational functions $f(X)$ with denominator Ω_i can be decomposed as

$$f(X) = g(\psi_i(X)) + \frac{X+b_i}{X-b_i} h(\psi_i(X)),$$

  where g, h have denominator Ω_{i+1}.

EC-FFT and EC-FRI

- Rational functions f on E_0 with poles on $G_0^{(\mathsf{n}+1)}$ can be decomposed as

$$f(X,Y) = \frac{g(X)}{\Omega_0(X)} + \frac{Y}{X}\frac{h(X)}{\Omega_0(X)}, \quad \deg(g), \deg(h) < N,$$

  where Ω_0 is a polynomial of degree $N-1$.

- Rational functions $f(X)$ with denominator Ω_i can be decomposed as

$$f(X) = g(\psi_i(X)) + \frac{X+b_i}{X-b_i} h(\psi_i(X)),$$

  where g, h have denominator Ω_{i+1}.

- These decompositions enable both FFT-like interpolations and FRI low-degree testing.

EC-STIKs

- $a_0 = 1, a_1 = 2$ and $a_{n+2} = a_{n+1}^2 + (-1)^n a_n^2 \pmod{p}$

EC-STIKs

- $a_0 = 1, a_1 = 2$ and $a_{n+2} = a_{n+1}^2 + (-1)^n a_n^2 \pmod{p}$
- Take some $Q_0 \in E_0$, and interpolate a rational function f with poles on $G_0^{(\mathsf{n}+1)}$ and $f(Q_0 + j \cdot \mathrm{g}_0) = a_j$, $f(-Q_0 + j \cdot \mathrm{g}_0) = 0$.

EC-STIKs

- $a_0 = 1, a_1 = 2$ and $a_{n+2} = a_{n+1}^2 + (-1)^n a_n^2 \pmod{p}$
- Take some $Q_0 \in E_0$, and interpolate a rational function f with poles on $G_0^{(\mathsf{n}+1)}$ and $f(Q_0 + j \cdot \mathrm{g}_0) = a_j$, $f(-Q_0 + j \cdot \mathrm{g}_0) = 0$.
- Evaluate f on more points of the form $\pm Q_i + j \cdot \mathrm{g}_0$ by ECFFT

EC-STIKs

- $a_0 = 1, a_1 = 2$ and $a_{n+2} = a_{n+1}^2 + (-1)^n a_n^2 \pmod p$
- Take some $Q_0 \in E_0$, and interpolate a rational function f with poles on $G_0^{(\mathsf{n}+1)}$ and $f(Q_0 + j \cdot \mathsf{g}_0) = a_j$, $f(-Q_0 + j \cdot \mathsf{g}_0) = 0$.
- Evaluate f on more points of the form $\pm Q_i + j \cdot \mathsf{g}_0$ by ECFFT
- Consider $\gamma(P) := f(P + 2\mathsf{g}_0) - f(P + \mathsf{g}_0)^2 - f(P)^2$.
- It can be evaluated on our sets, has at most *double* poles on $G_0^{(\mathsf{n}+1)}$, and should have zeros on $(Q_0 + 2G_0^{(\mathsf{n})}) \setminus \{Q_0 - 2\mathsf{g}_0\}$.

EC-STIKs

- $a_0 = 1, a_1 = 2$ and $a_{n+2} = a_{n+1}^2 + (-1)^n a_n^2 \pmod p$
- Take some $Q_0 \in E_0$, and interpolate a rational function f with poles on $G_0^{(\mathsf{n}+1)}$ and $f(Q_0 + j \cdot \mathrm{g}_0) = a_j$, $f(-Q_0 + j \cdot \mathrm{g}_0) = 0$.
- Evaluate f on more points of the form $\pm Q_i + j \cdot \mathrm{g}_0$ by ECFFT
- Consider $\gamma(P) := f(P + 2\mathrm{g}_0) - f(P + \mathrm{g}_0)^2 - f(P)^2$.
- It can be evaluated on our sets, has at most *double* poles on $G_0^{(\mathsf{n}+1)}$, and should have zeros on $(Q_0 + 2G_0^{(\mathsf{n})}) \setminus \{Q_0 - 2\mathrm{g}_0\}$.
- There exists a succinct rational function ω, such that γ is as above $\Leftrightarrow \omega \cdot \gamma$ has at most simple poles on $G_0^{(\mathsf{n}+2)}$

EC-STIKs

- $a_0 = 1, a_1 = 2$ and $a_{n+2} = a_{n+1}^2 + (-1)^n a_n^2 \pmod p$
- Take some $Q_0 \in E_0$, and interpolate a rational function f with poles on $G_0^{(\mathsf{n}+1)}$ and $f(Q_0 + j \cdot \mathsf{g}_0) = a_j$, $f(-Q_0 + j \cdot \mathsf{g}_0) = 0$.
- Evaluate f on more points of the form $\pm Q_i + j \cdot \mathsf{g}_0$ by ECFFT
- Consider $\gamma(P) := f(P + 2\mathsf{g}_0) - f(P + \mathsf{g}_0)^2 - f(P)^2$.
- It can be evaluated on our sets, has at most *double* poles on $G_0^{(\mathsf{n}+1)}$, and should have zeros on $(Q_0 + 2G_0^{(\mathsf{n})}) \setminus \{Q_0 - 2\mathsf{g}_0\}$.
- There exists a succinct rational function ω, such that γ is as above $\Leftrightarrow \omega \cdot \gamma$ has at most simple poles on $G_0^{(\mathsf{n}+2)}$
- The Prover can argue $\omega \cdot \gamma$ has this property using ECFRI!

Thanks for listening even more!