Aug. 2025: "40 years of ECC"

Modern Applications of Pairings

Dan Boneh

Stanford University

In the beginning …

There was the projective line:

(dim 0)

$\mathbb{F}_p^*$

Lots of amazing applications:

- Diffie-Hellman key exch., pub-key encryption, digital signatures

… and all was good

But the DLOG in $\mathbb{F}_p^*$ is only sub-exp hard: $\exp(\approx \log^{1/3}(p))$

Then came the elliptic curve …

$$E_{a,b}/\mathbb{F}_p \coloneqq \{\ (x,y) \in \mathbb{F}_p^2 \ :\ y^2 = x^3 + ax + b\ \} \qquad 4a^2 + 27b^2 \neq 0$$

Finite abelian group of order $\approx p$

$\Rightarrow$ Same apps, but the DLOG is much harder: $\exp(\log(p/2))$

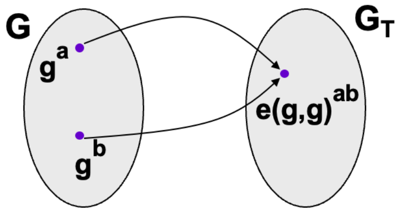
$\Rightarrow$ Scales better to higher security

we hope …

- H. Poincaré, 1901
- "Diophantus and Diophantine Equations," Bashmakova, 1997

A magical new structure on EC

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$: finite groups of prime order p



Def: A **pairing** $e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a map s.t.:

- Bilinear: $e(aG_1, bG_2) = e(G_1, G_2)^{ab} \quad \forall a, b \in \mathbb{Z},\ G_1 \in \mathbb{G}_1, G_2 \in \mathbb{G}_2$
- Poly-time computable and non-degenerate:

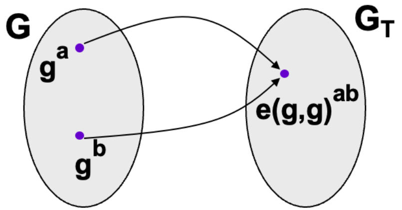
  G_1, G_2 generate $\mathbb{G}_1, \mathbb{G}_2$ resp. $\Rightarrow$ $e(G_1, G_2)$ generates $\mathbb{G}_T$

Good examples: $\mathbb{G}_1 \subseteq E(\mathbb{F}_p), \quad \mathbb{G}_2 \subseteq E(\mathbb{F}_{p^\alpha}), \quad \mathbb{G}_T \subseteq \mathbb{F}^*_{p^\alpha}$

Alin Tomescu: the history of Weil's pairing.

A magical new structure on EC

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$: finite groups of prime order p



Def: A **pairing** $e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a map s.t.:

- Bilinear: $e(aG_1, bG_2) = e(G_1, G_2)^{ab}$ $\forall a, b \in \mathbb{Z}$, $G_1 \in \mathbb{G}_1, G_2 \in \mathbb{G}_2$
- Poly-time computable and non-degenerate:

  G_1, G_2 generate $\mathbb{G}_1, \mathbb{G}_2$ resp. $\Rightarrow$ $e(G_1, G_2)$ generates $\mathbb{G}_T$

Good examples: $\mathbb{G}_1 \subseteq E(\mathbb{F}_p)$, $\mathbb{G}_2 \subseteq E(\mathbb{F}_{p^\alpha})$, $\mathbb{G}_T \subseteq \mathbb{F}_{p^\alpha}^*$

Computing the pairing: using Miller's alg. [M'86, M'04]

BLS: a sig scheme from pairings [BLS'01]

$e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, $|\mathbb{G}_1| = |\mathbb{G}_2| = p$, $G_b \in \mathbb{G}_b$ gens., $h\colon M \longrightarrow \mathbb{G}_2$

Gen: $sk \leftarrow \mathbb{Z}_p$, $pk := sk \cdot G_1 \in \mathbb{G}_1$

S(sk, m): output $\sigma := sk \cdot h(m) \in \mathbb{G}_2$

V(pk, m, σ): accept if $e(G_1, \sigma) \stackrel{?}{=} e(pk, h(m))$

Thm: co-CDH in $\mathbb{G}_1 \times \mathbb{G}_2$ hard $\Rightarrow$ existentially unforgeable (RO model)

co-CDH: $aG_1,\ aG_2,\ bG_2 \not\rightarrow abG_2$

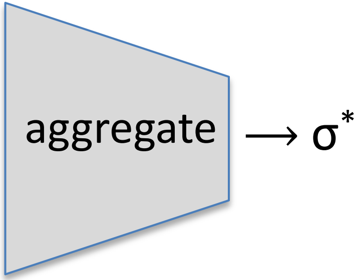
A new property: sig. aggregation [BGLS'03,Bol'03]

Anyone can compress n signatures into one

pk_1 , m_1 $\longrightarrow$ σ_1

⋮

pk_n , m_n $\longrightarrow$ σ_n



$V_{agg}(\overline{\mathbf{pk}} , \overline{\mathbf{m}} , \sigma^*) =$ "accept"

convinces verifier that

for $i = 1, \ldots, n$: user i signed msg m_i

Lots to say about how to aggregate securely:

see [BDN'18] or Boneh-Shoup book

eprint/2018/483 cryptobook.us

Pairing-based sigs. without hashing? [BB'04]

Gen: $sk = (\alpha, \beta \leftarrow \mathbb{Z}_p)$, $pk = (Y = \alpha G_2\,,\ Z = \beta G_2) \in \mathbb{G}_2^2$

S($sk, m \in \mathbb{Z}_p$): $r \leftarrow \mathbb{Z}_p$, $\sigma = \left(\frac{1}{\alpha + r\beta + m}\right) G_1 \in \mathbb{G}_1$, output (r, σ)

m is not hashed!

V$\big(pk, m, (r, \sigma)\big)$: accept if $e(\sigma,\ Y + rZ + mG_2) \stackrel{?}{=} e(G_1, G_2)$

Thm: secure (EUF-CMA) assuming q_S-BDH is hard in $\mathbb{G}_1 \times \mathbb{G}_2$.

q-BDH: $\underbrace{\alpha G_1,\ \alpha^2 G_1,\ \ldots,\ \alpha^q G_1}_{\text{in } \mathbb{G}_1},\ \underbrace{\alpha G_2,\ H,\ \alpha^{q+2} H}_{\text{in } \mathbb{G}_2} \not\Longrightarrow e(G_1, H)^{(\alpha^{q+1})}$

Pairing-based sigs. without hashing? [BB'04]

only used in the security proof

↓

a tower of powers

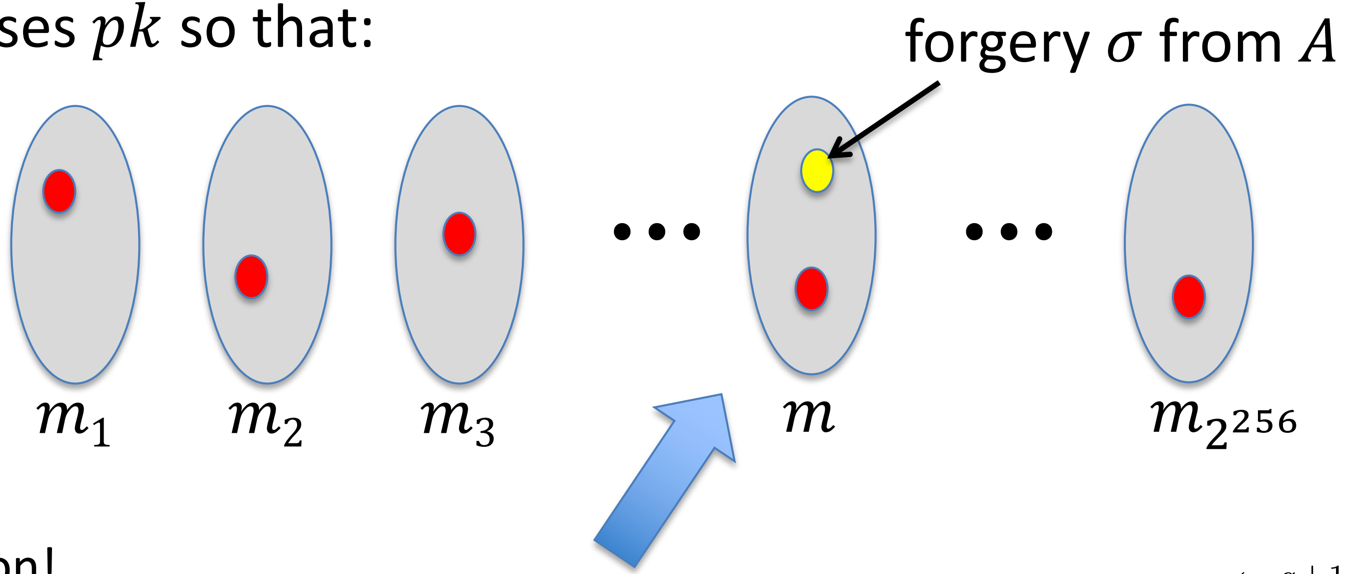
q-BDH: $$\alpha G_1,\ \alpha^2 G_1,\ \ldots,\ \alpha^q G_1$$

(need to account for Brown-Gallant-Cheon algorithm)

The proof strategy

Let A be a sig. forger. We build an algorithm B for q_S-BDH alg.

Alg. B chooses pk so that:



A tight reduction!

reveals q_S-BDH solution $e(G_1, H)^{(\alpha^{q+1})}$

What if tower of powers is part of scheme?

A new primitive: **functional commitments** [LRY'16]

- An interesting primitive in its own right
- Used for building succinct proof systems

Fix a function family $\mathcal{F} = \{ f : X \to Y \}$

$\text{Setup}(1^\lambda, \mathcal{F}) \to (pp, vp)$

$\text{Commit}(pp, f \in \mathcal{F}) \to \mathrm{com}$

$\text{Eval}(pp, f, x) \to (f(x), \pi)$ $\text{Verify}(vp, \mathrm{com}, x, y, \pi) \to 0/1$

Security: function binding

The committer can only "open" a commitment in a way that is consistent with <u>some</u> $f \in \mathcal{F}$

<u>Def</u>: the commitment scheme is **function binding** if $\forall$ PPT $\mathcal{A}$:

$$\Pr\left[\begin{array}{l} \forall i \in [n]: \ \text{Verify}(vp, \text{com}, x_i, y_i, \pi_i) = 1, \\ \text{but } \nexists f \in \mathcal{F} \text{ s.t. } \forall i \in [n]: \ f(x_i) = y_i \end{array} : \begin{array}{l} (pp, vp) \leftarrow\$ \ \text{Setup}(1^\lambda, \mathcal{F}) \\ \big(\text{com}, (x_i, y_i, \pi_i)_{i=1}^n\big) \leftarrow\$ \ \mathcal{A}(pp) \end{array}\right]$$

is negligible.

Committing to a polynomial in $\mathbb{F}_p^{<d}[X]$ [KZG'10]

Goal: commitment scheme for $\mathcal{F} = \{ f \in \mathbb{F}_p[X], \quad \deg(f) < d \}$

Lemma: Let $f \in \mathbb{F}_p[X]$. Then

$$f(u) = v \quad \text{iff} \quad q(X) := \frac{f(X) - v}{X - u} \in \mathbb{F}_p[X]$$

i.e. $f(X) - v$ is in the ideal $(X - u)$

Committing to a polynomial in $\mathbb{F}_p^{<d}[X]$ [KZG'10]

Goal: commitment scheme for $\mathcal{F} = \{ f \in \mathbb{F}_p[X], \quad \deg(f) < d \}$

Lemma: Let $f \in \mathbb{F}_p[X]$. Then

$$f(u) = v \quad \text{iff} \quad q(X) := \frac{f(X)-v}{X-u} \in \mathbb{F}_p[X]$$

Setup$(1^\lambda, d)$: $\alpha \leftarrow \mathbb{Z}_p, \quad pp = (\alpha G_1, \alpha^2 G_1, \dots, \alpha^{d-1} G_1), \quad vp = \alpha G_2$

Commit$(pp, f = \sum_{i=0}^{d-1} c_i X^i) \rightarrow f(\alpha) \cdot G_1 = \sum_{i=0}^{d-1} c_i \cdot \alpha^i G_1 \in \mathbb{G}_1$

Eval$(pp, f, u) \rightarrow (v = f(u), \ \pi = q(\alpha) \cdot G_1)$

Why is this secure?

Verify π: use pairing to check that $q(\alpha) \cdot (\alpha - u) = f(\alpha) - v$

Verify$(vp, \text{com}, u, v, \pi)$: $e(\pi,\ \alpha G_2 - uG_2) \stackrel{?}{=} e(com - vG_1,\ G_2)$

Thm: This scheme is function binding for $\mathbb{F}_p^{<d}[X]$
if q_d–BDH is hard in $\mathbb{G}_1 \times \mathbb{G}_2$, in the AGM

(or under ARSDH assumption w/o AGM [LPS'24,CGKY'25])

- Dory [L'20]: no secrets in pp, vp, but proof size is $O(\log d)$
- KZG generalizes to $\mathbb{F}_p^{\leq 1}[X_1, \ldots, X_k]$, but proof π is k group elements.

… see Mercury [EG'25] for a fast constant-size proof.

Applications of univariate poly-commit

Example 1: to **commit to a set** $S = \{u_1, \dots, u_n\} \subseteq \mathbb{F}_p$

commit to polynomial $f(X) := (X - u_1) \cdots (X - u_n) \in \mathbb{F}_p[X]$

Later: prove $u \in S$ by proving that $f(u) = 0$

Example 2: to **commit to a vector** $v = (v_1, \dots, v_n) \in \mathbb{F}_p^n$

commit to a polynomial $g \in \mathbb{F}_p[X]$ s.t. $g(i) = v_i, \quad i \in [n]$

Later: prove $v[i] = v_i$ by proving $g(i) = v_i$

Batch open: open many committed poly. at t points using a single proof

Verkle trees and more …

Many more applications to univariate and multilinear polynomial commitment schemes

Most succinct constructions use pairings

… and all was good

Then came the quantum computer

National Security Memorandum 10 (NSM-10) establishes the year 2035 as the primary target for completing the migration to PQC across Federal systems [NSM10]:

> "Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a Cryptographically Relevant Quantum Computer (CRQC). To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."

Open: is there a post-quantum BLS? (aggregation, threshold, DKG)

post-quantum KZG? (short proofs)

Finally: why stop at pairings?

An important open problem: **multilinear maps** [BS'02]

Find a mapping $e: G_1 \times \cdots \times G_n \to G_T$ s.t.

- e is a non-degenerate n-linear map,
- e is computable in poly-time, and
- DLOG in $G_1, \cdots, G_n, G_T$ is hard.

Open for $n \geq 3$. Powerful applications in cryptography.

THE END