CSE 575: Advanced Cryptography
Fall 2024
Lecture 23

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Background: pairing groups
- Polynomial commitment schemes (PCS)
- PCS security
- The Kate-Zaverucha-Goldberg (KZG) construction
- KZG security

Agenda for this lecture

- Announcements
- Background: pairing groups
- Polynomial commitment schemes (PCS)
- PCS security
- The Kate-Zaverucha-Goldberg (KZG) construction
- KZG security

Announcements

- HW4 is out, due 12/6
- Rest of class: no typeset lecture notes.
  - Can get extra credit for typesetting

Agenda for this lecture

- Announcements
- Background: pairing groups
- Polynomial commitment schemes (PCS)
- PCS security
- The Kate-Zaverucha-Goldberg (KZG) construction
- KZG security

Pairing groups

Let G, G_t be cyclic groups of order q

A map $e: G \times G \to G_t$ is bilinear if

$\forall u, v \in G$ and $a, b \in \{0, \ldots, q-1\}$,

$$e(u^a, v^b) = e(u, v)^{ab}$$

- non-degenerate: $e(g, g) \neq 1_{G_t}$
- eff - computable

Note: G has pairing $\Rightarrow$ no DDH ($u, v \in G$, g generator; $u = g^x$, $v = g^y$; $e(u, v) = e(g^x, g^y) = e(g, g)^{xy}$) (Exercise)

Symmetric vs. asymmetric

$e: G_1 \times G_2 \to G_t$

Pairing groups

Example: BLS12-381

$e: G_1 \times G_2 \to G_t$

G_1: 256-bit subgroup of elliptic curve $y^2 = x^3 + 4$ over $\mathbb{F}_p$ for 381-bit p

G_2: same-size subgroup of "$y^2 = x^3 + 4$" over $\mathbb{F}_{p^2}$

G_t: same-size subgroup of $\mathbb{F}_{p^{12}}^{\times}$ (12 = embedding degree)

Evaluate e via "Miller's algorithm"

$\approx$ 10x slower than scalar mult.

Pairing groups

Take "commitment" $Com(x) := g^x$

Given C_x C_y C_z, check $x + y = z$

$$C_x \cdot C_y \stackrel{?}{=} C_z$$

Check $x \cdot y = z$? pairing.

$$e(C_x, C_y) \stackrel{?}{=} e(g, C_z)$$

If $x \cdot y = z$ then

$$e(g^x, g^y) = e(g, g)^{xy} = e(g, g)^z$$

$$= e(g, g^z)$$

Agenda for this lecture

- Announcements
- Background: pairing groups
- Polynomial commitment schemes (PCS)
- PCS security
- The Kate-Zaverucha-Goldberg (KZG) construction
- KZG security

Polynomial commitment schemes

- Setup(n): output pp (n is degree bound)
- Commit(pp, p): output C_p and opening r
- Open(pp, C_p, p, z, r): output π and v s.t. $p(z) = v$
- Verify(pp, C_p, z, v, π): output 0/1

Lots of syntactic variations!

$C_p / \pi \in \mathbb{G}$ $\quad pp \in \{0,1\}^*$

$p \in \mathbb{F}_q[X]$

$z, v, r \in \mathbb{F}_q$

Agenda for this lecture

- Announcements
- Background: pairing groups
- Polynomial commitment schemes (PCS)
- PCS security
- The Kate-Zaverucha-Goldberg (KZG) construction
- KZG security

PCS security

Eval Binding

Hiding: C_p hides p

Correctness: honest (π, v) verifies

$G^{\mathcal{A}}_{PCS,n}$:

$pp \leftarrow Setup(n)$

$p, z, C_p, (\pi_1, v_1), (\pi_2, v_2) \leftarrow \mathcal{A}(pp)$

Ret $Ver(pp, C_p, z, v_1, \pi_1) = 1$

$\wedge\ Ver(pp, C_p, z, v_2, \pi_2) = 1$

$\wedge\ v_1 \neq v_2$

PCS is n-EB if $\forall n, PPT\ \mathcal{A}$,

$Pr[G^{\mathcal{A}}_{PCS,n} = 1] = negl$

Agenda for this lecture

- Announcements
- Background: pairing groups
- Polynomial commitment schemes (PCS)
- PCS security
- The Kate-Zaverucha-Goldberg (KZG) construction
- KZG security

KZG commitments

$\mathbb{F}_q^{<n}[X] \subset$

$p(z) = v \iff p(X) - v = q(X)(X - z)$

$p(X) = q(X)(X - z) + v$

$p(X) - v = q(X)(X - z)$

Main idea: $p(z) = v$ iff $\exists\, q(X)$ s.t.

$$\frac{p(X) - v}{(X - z)} = q(X)$$

KZG commitments

Setup(n):

$\tau \leftarrow \mathbb{F}_q$

Ret $(g, g^{\tau}, g^{\tau^2}, \ldots, g^{\tau^n}) \in \mathbb{G}^{n+1}$

D_1 ||

Commit(pp, P):

Parse P as $a_0, a_1, \ldots, a_n$

Compute $C_P = g^{P(\tau)}$ with pp

$n = 1$

$P(X) = a_1 X + a_0$

D_0 ||, D_1 ||τ

(g, g^{τ})

$P(\tau)$ using a_1, a_0

$D_1^{a_1} \cdot D_0^{a_0}$

$g^{a_1 \tau} \cdot g^{a_0} = g^{a_1 \tau + a_0}$

Multi-scalar Multiplication

Open(pp, C_P, P, z, r := ξ):

- Compute $P(z) := v$
- Compute witness $q(X) = \frac{(P(X) - v)}{(X - z)}$
- Compute C_q as in Commit
- Ret C_q, v

Verify(pp, C_P, z, v, π):

Ret $e(\pi, D_1 / g^z) \stackrel{?}{=} e(g, C_P / g^v)$

Correctness: $\Leftrightarrow e(g^{q(\tau)}, g^{\tau - z}) = e(g, g)^{q(\tau)(\tau - z)} = e(g, g)^{P(\tau) - v} = e(g, C_P / g^v)$

Agenda for this lecture

- Announcements
- Background: pairing groups
- Polynomial commitment schemes (PCS)
- PCS security
- The Kate-Zaverucha-Goldberg (KZG) construction
- KZG security

Security of KZG

Thm: If n-strong DH holds in $\mathbb{G}_1$, KZG is n-EB

n-strong DH:

$\mathcal{G}_n^{\mathcal{A}}$:

$\tau \leftarrow \mathbb{F}_q$; compute $pp := (g, g^{\tau}, g^{\tau^2}, \ldots, g^{\tau^n})$

$(z, h) \leftarrow \mathcal{A}(pp)$

Ret $h \stackrel{?}{=} g^{\frac{1}{\tau - z}}$