Notes on Caulk and Caulk+

arnaucube

February 2023

Abstract

Notes taken while reading about Caulk [1] and Caulk+ [2].

Usually while reading papers I take handwritten notes, this document contains some of them re-written to $LaTeX$.

The notes are not complete, don't include all the steps neither all the proofs.

Contents

1 Preliminaries

1.1 Lagrange Polynomials and Roots of Unity

Let ω denote a root of unity, such that $\omega^N = 1$. Set $\mathbb{H} = \{1, \omega, \omega^2, \ldots, \omega^{N^{-1}}\}$.

Let the i^{th} Lagrange polynomial be $\lambda_i(X) = \prod_{s \neq i-1} \frac{X - \omega^s}{\omega^{i-1} - \omega}$.

Notice that $\lambda_i(\omega^{i-1}) = 1$ and $\lambda_i(w^j) = 0, \ \forall j \neq i-1$.

Let the vanishing polynomial of $\mathbb{H}$ be $z_H(X) = \prod_{i=0}^{N-1}(X - \omega^i) = X^N - 1$.

1.2 KZG Commitments

KZG as a Vector Commitment.

We have vector $\overrightarrow{c} = \{c_i\}_1^n$, which can be interpolated into $C(X)$ through Lagrange polynomials $\{\lambda_i(X)\}$:

$$C(X) = \sum_{i=1}^{n} c_i \cdot \lambda_i(X)$$

so, $C(\omega^{i-1}) = c_i$.

Commitment:

$$C = [C(X)]_1 = \sum_{i=1}^{n} c_i \cdot [\lambda_i(X)]_1$$

Proof of **opening for single value** v at position i:

$$Q(X) = \frac{C(X) - v}{X - \omega^{i-1}}$$

$$\pi_{KZG} = Q = [Q(X)]_1$$

Verification:

$$e(C - [v]_1, [1]_2) = e(\pi_{KZG},\ [X - \omega^{i-1}]_2)$$

unfold

$$e([C(X)]_1 - [v]_1, [1]_2) = e([Q(X)]_1,\ [X - \omega^{i-1}]_2)$$

$$C(X) - v = Q(X) \cdot (X - \omega^{i-1}) \Longrightarrow Q(X) = \frac{C(X) - v}{X - \omega^{i-1}}$$

Proof of **opening for a subset** of positions $I \subset [N]$:

$[H_I]_1$ such that for

$$C_I(X) = \sum_{i \in I} c_i \cdot \tau_i(X)$$

$$z_I(X) = \prod_{i \in I} (X - \omega^{i-1})$$

for $\{\tau_i(X)\}_{i \in I}$ being the Lagrange interpolation polynomials over $\mathbb{H}_I = \{\omega^{i-1}\}_{i \in I}$. *(recall, $z_H(X) = \prod_{i=0}^{N-1}(X - \omega^i) = X^N - 1$))*

$H_I(X)$ can be computed by

$$H_I(X) = \frac{C(X) - C_I(X)}{z_I(X)}$$

So, prover commits to $C_I(X)$ with $C_I = [C_I(X)]_1$, and computes π_{KZG}:

$$\pi_{KZG} = H_I = [H_I(X)]_1$$

Then, verification checks:

$$e(C - C_I, [1]_2) = e(\pi_{KZG}, [z_I(X)]_2)$$

unfold

$$e([C(X)]_1 - [C_I(X)]_1, [1]_2) = e([H_I(X)]_1, [z_I(X)]_2)$$

$$C(X) - C_I(X) = H_I(X) \cdot z_I(X)$$

$$C(X) - C_I(X) = \frac{C(X) - C_I(X)}{z_I(X)} \cdot z_I(X)$$

1.3 Pedersen Commitments

Commitment

$$cm = v[1]_1 + r[h]_1 = [v + hr]_1$$

Prove knowledge of $v,\ r$, Verifier sends challenge $\{s_1, s_2\}$. Prover computes:

$$R = s_1[1]_1 + s_2[h]_1 = [s_1 + hs_2]_1$$

$$c = H(cm, R)$$

$$t_1 = s_1 + vc, \quad t_2 = s_2 + rc$$

Verification:

$$R + c \cdot cm == t_1[1]_1 + t_2[h]_1$$

unfold:

$$R + c \cdot cm == t_1[1]_1 + t_2[h]_1 = [t_1 + ht_2]$$

$$[s_1 + hs_2]_1 + c \cdot [v + hr]_1 == [s_1 + vc + h(s_2 + rc)]_1$$

$$[s_1 + hs_2 + cv + rch]_1 == [s_1 + vc + hs_2 + rch]_1$$

2 Caulk

2.1 Blinded Evaluation

Main idea: combine KZG commitments with Pedersen commitments to prove knowledge of a value v which Pedersen commitment is committed in the KZG commitment.

Let $C(X) = \sum_{i=1}^{N} c_i \lambda_i(X)$, where $\overrightarrow{c} = \{c_i\}_{i \in I}$. In normal KZG, prover would compute $Q(X) = \frac{C(X)-v}{X-\omega^{i-1}}$, and send $[Q(X)]_1$ as proof. We will obfuscate the commitment:

rand $a \in \mathbb{F}$, blind commit to $z(X) = aX - b = a(X - \omega^{i-1})$, where $\omega^{i-1} = b/a$. Denote by $[z]_2$ the commitment to $[z(X)]_2$.

Prover computes:

i. π_{ped}, Pedersen proof that cm is from v, r (section 1.3)

ii. π_{unity} (see 2.1.1)

iii. For random s computes:

$$T(X) = \frac{Q(X)}{a} + hs \longrightarrow [T]_1 = [T(X)]_1$$

$$S(X) = -r - s \cdot z(X) \longrightarrow [S]_2 = [S(X)]_2$$

i, ii, iii defines the *zk proof of membership*, which proves that (v, r) is a opening of cm, and v opens C at ω^{i-1}.

Verifier checks proofs $\pi_{ped}, \ \pi_{unity}$ (i, ii), and checks

$$e(C - cm, [1]_2) == e([T]_1, [z]_2) + e([h]_1, [S]_2)$$

unfold:

$$\begin{aligned}
C(X) - cm &== T(X) \cdot z(X) + h \cdot S(X) \\
C(X) - v - hr &== (\frac{Q(X)}{a} + sh) \cdot z(X) + h(-r - s \cdot z(X)) \\
C(X) - v &== hr + (\frac{Q(X)}{a})z(X) + sh \cdot z(X) - hr - sh \cdot z(X) \\
C(X) - v &== \frac{Q(X)}{a} \cdot z(X) \\
C(X) - v &== \frac{Q(X)}{a} \cdot a(X - \omega^{i-1}) \\
C(X) - v &== Q(X) \cdot (X - \omega^{i-1})
\end{aligned}$$

Which matches with the definition of $Q(X) = \frac{C(X)-v}{X-\omega^{i-1}}$.

2.1.1 Correct computation of $z(x)$, π_{unity}

Want to prove that prover knows a, b such that $[z]_2 = [aX - b]_2$, and $a^N = b^N$.

To prove $\frac{a}{b}$ is inside the evaluation domain (ie. $\frac{a}{b}$ is a N^{th} root of unity), proves (in $log(N)$ time) that its N^{th} is one ($\frac{a}{b} = 1$).

Conditions:

i. $f_0 = \frac{a}{b}$

ii. $f_i = f_{i-1}^2, \ \forall \ i = 1, \ldots, log(N)$

iii. $f_{log(N)} = 1$

Redefine i, and from there, redefine ii, iii:

i.

$$
\begin{aligned}
f_0 &= z(1) = a - b \\
f_1 &= z(\sigma) a\sigma - b \\
f_2 &= \frac{f_0 - f_1}{1-\sigma} = \frac{a(1-\sigma)}{1-\sigma} = a \\
f_3 &= \sigma f_2 - f_1 = \sigma a - a\sigma + b = b \\
f_4 &= \frac{f_2}{f_3} = \frac{a}{b}
\end{aligned}
$$

ii. $f_{5+i} = f_{4+i}^2, \quad \forall i = 0, \ldots, log(N) - 1$

iii. $f_{4+log(N)} = 1$

Lemma 1. Let $z(X)$ $deg = 1$, $n = log(N) + 6$, σ such that $\sigma^n = 1$.
If $\exists\ f(X) \in \mathbb{F}[X]$ such that

1. $f(X) = z(X)$, for $1, \sigma$
2. $f(\sigma^2)(1-\sigma) = f(1) - f(\sigma)$
3. $f(\sigma^3) = \sigma f(\sigma^2) - f(\sigma)$
4. $f(\sigma^4) f(\sigma^3) = f(\sigma^2)$
5. $f(\sigma^{4+i+1}) = f(\sigma^{4+i})^2, \quad \forall i = 0, \ldots, log(N) - 1$
6. $f(\sigma^{5+log(N)} \cdot \sigma^{-1}) = 1$

then, $z(X) = aX - b$, where $\frac{b}{a}$ is a Nth root of unity.

Let's see the relations between the conditions and the Lemma 1:

$$Conditions \longrightarrow Lemma\ 1$$

$$\begin{matrix} f_0 = z(1) = a - b \\ f_1 = z(\sigma) a\sigma - b \end{matrix} \longrightarrow 1.\ f(X) = z(X), for 1, \sigma$$

$$f_2 = \frac{f_0 - f_1}{1-\sigma} = \frac{a(1-\sigma)}{1-\sigma} = a \longrightarrow 2.\ f(\sigma^2)(1-\sigma) = f(1) - f(\sigma)$$

$$f_3 = \sigma f_2 - f_1 = \sigma a - a\sigma + b = b \longrightarrow 3.\ f(\sigma^3) = \sigma f(\sigma^2) - f(\sigma)$$

$$f_4 = \frac{f_2}{f_3} = \frac{a}{b} \longrightarrow 4.\ f(\sigma^4) f(\sigma^3) = f(\sigma^2)$$

$$f_{5+i} = f_{4+i}^2, \quad \forall i = 0, \ldots, log(N) - 1 \longrightarrow 5.\ f(\sigma^{4+i+1}) = f(\sigma^{4+i})^2,\ \forall i = 0, \ldots, log(N) - 1$$

$$f_{4+log(N)} = 1 \longrightarrow 6.\ f(\sigma^{5+log(N)} \cdot \sigma^{-1}) = 1$$

For succintness: aggregate $\{f_i\}$ in a polynomial $f(X)$, whose coefficients in Lagrange basis associated to $\mathbb{V}_n$ are the f_i (ie. s.t. $f(\omega^i) = f_i$).

$$
\begin{aligned}
f(X) &= (a-b)\rho_1(X) + (a\sigma - b)\rho_2(X) + a\rho_3(X) + b\rho_4(X) + \sum_{i=0}^{log(N)} (\frac{a}{b})^{2^i} \rho_{5+i}(X) \\
&= f_0\rho_1(X) + f_1\rho_2(X) + f_2\rho_3(X) + f_3\rho_4(X) + \sum_{i=0}^{log(N)} (f_4)^{2^i} \rho_{5+i}(X)
\end{aligned}
$$

Prover shows that $f(X)$ by comparing $f(\sigma^i)$ with the corresponding constraints from Lemma 1:

For rand α (set by Verifier), set $\alpha_1 = \sigma^{-1}\alpha,\ \alpha_2 = \sigma^{-2}\alpha$, and send $v_1 = f(\alpha_1),\ v_2 = f(\alpha_2)$ with corresponding proofs of opening.

Given v_1, v_2, shows that $p_\alpha(X)$, which proves the constraints from Lemma 1, evaluates to 0 at α (ie. $p_\alpha(\alpha) = 0$).

$$\begin{aligned} p_\alpha(X) = &- h(X) z_{V_n}(\alpha) + [f(X) - z(X)] \cdot (\rho_1(\alpha) + \rho_2(\alpha)) \\ &+ [(1-\sigma) f(X) - f(\alpha_2) + f(\alpha_1)] \rho_3(\alpha) \\ &+ [f(X) + f(\alpha_2) - \sigma f(\alpha_1)] \rho_4(\alpha) \\ &+ [f(X) f(\alpha_1) - f(\alpha_2)] \rho_5(\alpha) \\ &+ [f(X) - f(\alpha_1) f(\alpha_1)] \prod_{i \notin [5, \ldots, 4+log(N)]} (\alpha - \sigma^i) \\ &+ [f(\alpha_1) - 1] \rho_n(\alpha) \end{aligned}$$

2.1.2 NIZK argument of knowledge for R_{unity} and $deg(z) \leq 1$

Prover:

$$r_0, r_1, r_2, r_3 \leftarrow^{\$} \mathbb{F}, \quad r(X) = r_1 + r_2 X + r_3 X^2$$

$$\begin{aligned} f(X) = &(a-b)\rho_1(X) + (a\sigma - b)\rho_2(X) + a\rho_3(X) + b\rho_4(X) + \sum_{i=0}^{log(N)} (\frac{a}{b})^{2^i} \rho_{5+i}(X) \\ &+ r_0 \rho_{5+log(N)}(X) + r(X) z_{V_n}(X) \end{aligned}$$

$$\begin{aligned} p(X) = &[f(X) - (aX - b)](\rho_1(X) + \rho_2(X)) \\ &+ [(1-\sigma) f(X) - f(\sigma^{-1}X) + f(\sigma^{-1}X)] \rho_3(X) \\ &+ [f(X) + f(\sigma^{-2}X) - \sigma f(\sigma^{-1}X)] \rho_4(X) \\ &+ [f(X) f(\sigma^{-1}X) - f(\sigma^{-2}X)] \rho_5(X) \\ &+ [f(X) - f(\sigma^{-1}X) f(\sigma^{-1}X)] \prod_{i \notin [5, 4+log(N))]} (X - \sigma^i) \\ &+ [f(\sigma^{-1}X) - 1] \rho_n(X) \end{aligned}$$

Set

$$h'(X) = \frac{p(X)}{z_{V_n}(X)}, \quad h(X) = h'(X) + X^{d-1} z(X)$$

output $([F]_1 = [f(X)]_1,\ [H]_1 = [h(x)]_1)$.

Note that

$$\begin{aligned} h(x) &= h'(X) + X^{d-1} z(X) \\ &= \frac{p(X)}{z_{V_n}(X)} + X^{d-1} z(X) \longrightarrow p(X) + X^{d-1} z(X) = z_{V_n}(X) h(X) \end{aligned}$$

Verifier sets challenge $\alpha \in^{\$} \mathbb{F}$ (hash of transcript by Fiat-Shamir).

$$\begin{aligned}
p_\alpha(X) = &- h(X)z_{V_n}(\alpha) \\
&+ [f(X) - z(X)] \cdot (\rho_1(\alpha) + \rho_2(\alpha)) \\
&+ [(1-\sigma)f(X) - f(\alpha_2) + f(\alpha_1)]\rho_3(\alpha) \\
&+ [f(X) + f(\alpha_2) - \sigma f(\alpha_1)]\rho_4(\alpha) \\
&+ [f(X)f(\alpha_1) - f(\alpha_2)]\rho_5(\alpha) \\
&+ [f(X) - f(\alpha_1)f(\alpha_1)] \prod_{i \notin [5,\ldots,4+log(N)]} (\alpha - \sigma^i) \\
&+ [f(\alpha_1) - 1]\rho_n(\alpha)
\end{aligned}$$

Note: for the check that $[z]_1$ has degree 1, we add $-h(X)z_{V_n}(\alpha)$, to include the term $X^{d-1}z(X)$ in $h(X)$. Later the Verifier will compute $[P]_1$ without the terms including $z(X)$ (ie. without $-X^{d-1}z(X)z_{V_n}(\alpha) - z(X)[\rho_1(\alpha) + \rho_2(\alpha)]$), which the Verifier will add via the pairing:

$$\begin{aligned}
&-X^{d-1}z(X)z_{V_n}(\alpha) - z(X)(\rho_1(\alpha) + \rho_2(\alpha)) \\
=\ &(-X^{d-1}z_{V_n}(\alpha) - (\rho_1(\alpha) + \rho_2(\alpha))) \cdot z(X) \\
\longrightarrow\ &e(-(\rho_1(\alpha) + \rho_2(\alpha)) - z_{V_n}(\alpha)[X^{d-1}]_1, [z]_2)
\end{aligned}$$

Prover then generates KZG proofs

$$((v_1, v_2), \pi_1) \leftarrow KZG.Open(f(X), (\alpha_1, \alpha_2))$$
$$(0, \pi_2) \leftarrow KZG.Open(p_\alpha(X), \alpha)$$

prover's output: (v_1, v_2, π_1, π_2).
Verify: set $\alpha_1 = \sigma^{-1}\alpha,\ \alpha_2 = \sigma^{-2}\alpha$,
(notice that $f(X) \rightarrow [F]_1$, and $f(\alpha_1) = v_1,\ f(\alpha_2) = v_2$)

$$\begin{aligned}
[P]_1 = &- z_{V_n}(\alpha)[H]_1 + [F]_1(\rho_1(\alpha) + \rho_2(\alpha)) \\
&+ [(1-\sigma)[F]_1 - v_2 + v_1]\rho_3(\alpha) \\
&+ [[F]_1 + v_2 - \sigma v_1]\rho_4(\alpha) \\
&+ [[F]_1 v_1 - v_2]\rho_5(\alpha) \\
&+ [[F]_1 - v_1^2] \prod_{i \notin [5,\ldots,4+log(N)]} (\alpha - \sigma^i) \\
&+ [v_1 - 1]\rho_n(\alpha)
\end{aligned}$$

$$KZG.Verify((\alpha_1, \alpha_2), (v_1, v_2), \pi_1)$$
$$e([P]_1, [1]_2) + e(-(\rho_1(\alpha) + \rho_2(\alpha)) - z_{V_n}(\alpha)[x^{d-1}]_1, [z]_2) = e(\pi_2, [x - \alpha]_2)$$

3 Caulk+

WIP

References

[1] Arantxa Zapico, Vitalik Buterin, Dmitry Khovratovich, Mary Maller, Anca Nitulescu, and Mark Simkin. Caulk: Lookup arguments in sublinear time. Cryptology ePrint Archive, Paper 2022/621, 2022. `https://eprint.iacr.org/2022/621`.

[2] Jim Posen and Assimakis A. Kattis. Caulk+: Table-independent lookup arguments. Cryptology ePrint Archive, Paper 2022/957, 2022. `https://eprint.iacr.org/2022/957`.