Stacked-DRGs / ZigZag Security parameters

irene@protocol.ai

August 9, 2019

Recap for Stacked DRGs (no tapering)

With the following parameters

- conditions: any δ and ϵ such that $\epsilon \leq 0.24$ and $\delta < \epsilon/2$
- number of layers: $\max\left\{\frac{0.68-\epsilon+\delta}{0.12-\delta}, \log_2\left(\frac{1}{3(\epsilon-2\delta)}\right)+\frac{0.12}{0.12-\delta}+1\right\}+1$
- number of offline challenges: $\frac{-\lambda}{\log_2(1-\delta)}$
- number of online challenges: $\frac{-\lambda}{\log_2(2-\epsilon-2\delta)-1}$

we get a PoS with

- space gap: $\epsilon+2\delta$,
- time: $\beta n-1$,
- soundness: $2^{-\lambda}$.

Recap for ZigZag (no tapering)

With the following parameters

- conditions: any δ and ϵ such that $\epsilon+\delta \leq 0.24$ and $\delta < \epsilon/3$ and
- number of layers: $2\log_2\left(\frac{1}{3(\epsilon-2\delta)}\right)+2\frac{0.8-\epsilon+\delta}{0.12-2\delta}+2$
- number of offline challenges: $\frac{-\lambda}{\log_2(1-\delta)}$
- number of online challenges: $\frac{-\lambda}{\log_2(2-\epsilon-3\delta)-1}$

we get a PoS with

- space gap: $\epsilon+3\delta$,
- time: $\beta n-1$,
- soundness: $2^{-\lambda}$.

Notation and definitions

1. **Chung's construction** for a bipartite graph with two layers (each with n nodes) and degree d:

   - Repeat d times the following:
     sample a random permutation $f : \{1, \dots, n\} \to \{1, \dots, n\}$,
     for $i = 1, \dots, n$, add an edge from node i in the top layer to node $f(i)$ in the layer below.

2. Length of a path in a graph = number of edges contained on the path.

3. A directed acyclic graph (DAG) with n nodes is a $(n, 0.80, \beta)$ **DRG** if any set of $0.8n$ nodes contains a path of length $\geq \beta n$ (β is a constant < 0.8).

   Notice, for efficiency we also require small in-degree (*e.g.*, $d = O(\log n)$).

   in-degree = maximum number of incoming edges in a node

   Question: In our implementation we have $d = 5$, is this secure?

4. Definition of **Stacked DRGs graph**: $\mathcal{G}_{\ell,n}$ is a graph with ℓ layers where each layer V_i is a $(n, 0.80, \beta)$ DRG and we add edges in each pair of layers (V_i, V_{i+1}) following the randomized Chung's construction for regular bipartite graphs with degree 8 (edges from layer i to layer $i + 1$).

   Notice: The number of nodes n has to be large enough in order to give negligible probability of failure for Chung's construction and the DRG construction.

   Question: Is $n = 2^{30}$ enough?

5. Definition of **ZigZag graph**: $\mathcal{Z}_{\ell,n}$ is a graph with ℓ layers where each layer V_{2i+1} is a $(n, 0.80, \beta)$ DRG with edges from lower index nodes to higher index nodes and each layer V_{2i} is a $(n, 0.80, \beta)$ DRG with edges from higher index nodes to lower index nodes ($i = 1, 2, \dots$).

   (To construct V_{2i} just take V_{2i+1} and reverse the nodes and the direction of the edges).

   Moreover, for each each pair of layers (V_i, V_{i+1}) add edges following Chung's construction for degree 8 and then project these edges on layer V_{i+1}. Change the direction of these edges following this rule: if $i + 1$ is even then any edge in V_{i+1} has direction from higher to lower indices, if $i + 1$ is odd then any edge in V_{i+1} has direction from lower to higher indices.

6. Let $\mathcal{G}_{\ell,n}[\epsilon, \delta]$ indicate the Stacked DRG graph $\mathcal{G}_\ell$ with the following pebble configuration: $(1 - \epsilon)$ black pebbles overall and δ red pebbles in each layer. We say that $\mathcal{Z}_{\ell,n}[\epsilon, \delta]$ is (t, μ)-hard if t rounds (parallel moves) are required to pebble a fraction μ of nodes in the last layer.

   item Let $\mathcal{Z}_\ell[\epsilon, \delta]$ indicate the ZigZag graph $\mathcal{Z}_\ell$ with the following pebble configuration: $(1 - \epsilon)$ black pebbles overall and δ red pebbles in each layer. We say that $\mathcal{Z}_\ell[\epsilon, \delta]$ is (t, μ)-hard if t rounds of moves that only use "forward steps" are required to pebble a fraction μ of nodes in the last layer.

Proof overview (Stacked DRGs, no tapering)

- Claim 6 says that $\mathcal{G}_\ell[\epsilon, \delta]$ with

$$\ell = \max\left\{\frac{0.68 - \epsilon + \delta}{0.12 - \delta}, \log_2\left(\frac{1}{3(\epsilon - 2\delta)}\right) + \frac{0.12}{0.12 - \delta} + 1\right\} \tag{1}$$

$$\delta < \epsilon/2 \tag{2}$$

  is $(\beta n - 1, 1)$ hard.

- Then using Claim 4 and we can say that $\mathcal{G}_{\ell+1}[\epsilon + 2\delta, \delta]$ with

$$\epsilon \leq 0.24 \tag{3}$$

  is $(\beta n - 1, 1 - \frac{\epsilon+2\delta}{2})$ hard.

- Finally, use Claim 2. Assume that we ask for c independent random challenges in the offline phase (in each layer we open the same c nodes) and k independent random challenges in the online phase (last layer only).

  Using the Stacked DRGs graph with $\ell + 1$ layers with conditions (1), (2), (3) and with

$$c = \frac{-\lambda}{\log_2(1 - \delta)} \tag{4}$$

$$k = \frac{-\lambda}{\log_2(2 - \epsilon - 2\delta) - 1} \tag{5}$$

  gives a PoS with space gap: $\epsilon + 2\delta$, time: $\beta n - 1$ and soundness: $2^{-\lambda}$.

Proof overview (ZigZag, no tapering)

- Claim 11 says that $\mathcal{Z}_\ell[\epsilon, \delta]$ with

$$\ell = 2\log_2\left(\frac{1}{3(\epsilon - 2\delta)}\right) + 2\frac{0.8 - \epsilon + \delta}{0.12 - 2\delta} \tag{6}$$

$$\delta < \min\{0.06, \epsilon/3\} \tag{7}$$

  is $(\beta n - 1, 1)$ hard.

- Then using Claim 9 and we can say that $\mathcal{Z}_{\ell+2}[\epsilon + 3\delta, \delta]$ with

$$\epsilon + \delta \leq 0.24 \tag{8}$$

  is $(\beta n - 1, 1 - \frac{\epsilon+3\delta}{2})$ hard.

- Finally, use Claim 2. Assume that we ask for c independent random challenges in the offline phase (in each layer we open the same c nodes) and k independent random challenges in the online phase (last layer only).

Using the ZigZag graph with $\ell + 2$ layers with conditions (6), (7), (8) and with

$$c = \frac{-\lambda}{\log_2(1-\delta)} \tag{9}$$

$$k = \frac{-\lambda}{\log_2(2-\epsilon-3\delta)-1} \tag{10}$$

gives a PoS with space gap: $\epsilon + 3\delta$, time: $\beta n - 1$ and soundness: $2^{-\lambda}$.

PoS Definition

Public parameters: a graph with ℓ layers and n nodes in each layer (*i.e.*, $\mathcal{Z}_\ell[\epsilon, \delta]$ or $\mathcal{G}_\ell[\epsilon, \delta]$) that is (t, μ)-hard

Input: data blocks $D_1, \ldots, D_n$ with $D_i \in \{0, 1\}^m$

Initialization:

- The prover computes the labels $e_1^{(i)}, \ldots, e_n^{(i)}$ for $i = 1, \ldots, \ell$

Claim 2 (a)

If $\mathcal{G}_\ell[\epsilon, \delta]$ is (t, μ)-hard, then $\mathcal{G}_\ell[\epsilon, \delta]$ is $(t^*, 1 - \epsilon/2)$-hard with $t^* = \min(\beta n - 1, t + 1)$.

Claim 2 (b)

If $\mathcal{G}_{\ell-1}[\epsilon - 2\delta, \delta]$ is $(t, 1)$-hard and $0 < \epsilon - 2\delta \leq 0.24$, then $\mathcal{G}_\ell[\epsilon, \delta]$ is $(t^*, 1 - \epsilon/2)$-hard with $t^* = \min(\beta n - 1, t + 1)$.

Correct Claim 4

If $\mathcal{G}_{\ell-1}[\epsilon - 2\delta, \delta]$ is $(t, 1)$-hard and $0 < \epsilon - 2\delta \leq 0.24$, then $\mathcal{G}_\ell[\epsilon, \delta]$ is $(t^*, 1 - \epsilon/2)$-hard with $t^* = \min(\beta n - 1, t + 1)$.

Alternative Claim 4

If $\delta < \epsilon/2$ and $\mathcal{G}_{\ell-1}[\epsilon/2 - \delta, \delta]$ is $(t, 1)$-hard, then $\mathcal{G}_\ell[\epsilon, \delta]$ is $(t^*, 1 - \epsilon/2)$-hard with $t^* = \min(\beta n - 1, t + 1)$.

Proof. Let S be a subset of nodes from the last layer in $\mathcal{G}_\ell[\epsilon, \delta]$ with size $(1 - \epsilon/2)n$, we need to show that t^* rounds are required to pebble S. Let X be the subset of S of unpebbled nodes, it is enough to show that X requires t^* rounds to be pebbled. Let $|X| = \alpha^* n$ and notice that $\alpha^* \geq \alpha_\ell - \epsilon/2 \geq \epsilon/2 - \delta > 0$.

Now, consider two cases:

1. If $\alpha^* \geq 0.8$, then $\beta n - 1$ rounds are required to pebble X (this is because V_ℓ is a $(n, 0.8, \beta)$ DRG, so X contains a path of length βn).

2. If $\epsilon/2 - \delta < \alpha^* < 0.8$, then we have that the nodes in X are connected to β^* nodes in layer $\ell - 1$ with $\beta^* > 1.17\alpha^*$ (because of the table in Figure 2.2 in ePrint 2018/702).

   ToDo: Check this!

   Among these nodes, at least $\alpha' \geq \beta^* - \rho_{\ell-1} - \delta$ are unpebbled. From this,

   $$\alpha' \geq \beta^* - \rho_{\ell-1} - \delta = \beta^* + (\gamma_{\ell-1} - \gamma + \rho_\ell) - \delta$$

   And therefore

   $$\begin{aligned}
   \alpha' - \gamma_{\ell-1} &\geq \beta^* - \gamma + (1 - \alpha_\ell - \delta) - \delta \\
   &\geq \beta^* - \gamma + (1 - \alpha^* - \epsilon/2) - 2\delta \\
   &> (1.17 - 1)\alpha^* + \epsilon/2 - 2\delta \\
   &> 0.17(\epsilon/2 - \delta) + \epsilon/2 - 2\delta = 1.17(\epsilon/2 - \delta) - \delta \\
   &> (\epsilon/2 - \delta) - \delta
   \end{aligned} \tag{11}$$

   The last inequality is because $\delta < \epsilon/2$ implies $1.17(\epsilon/2 - \delta) > \epsilon/2 - \delta$. Now, consider the graph $\mathcal{G}_{\ell-1}[\epsilon', \delta]$ with $\epsilon' = \epsilon/2 - \delta$ and the following constrain in its pebble configuration: the number of black pebbles from layer 1 to layer $\ell - 2$ is $\gamma_{\ell-1} n$ (the same number as in $\mathcal{G}_\ell[\epsilon, \delta]$). Then, (11) says that we can apply Claim 3 from ePrint 2018/702, and therefore the fact that $\mathcal{G}_{\ell-1}[\epsilon', \delta]$ is $(t, 1)$-hard implies that at least t rounds are required to pebble the unpebbled nodes among the $\beta^* n$ dependency of X. Finally, X needs $t + 1$ rounds to be pebbled in in $\mathcal{G}_\ell[\epsilon, \delta]$.

□

Correct Claim 9

Now we want to prove that: If $\mathcal{Z}_{\ell-2}[\epsilon-3\delta,\delta]$ is $(t,1)$-hard and $\epsilon-2\delta \leq 0.24$, then $\mathcal{Z}_\ell[\epsilon,\delta]$ is $(t^*, 1-\epsilon/2)$-hard with $t^* = \min(\beta n - 1, t+2)$.

Proof. Let S be a subset of nodes from the last layer in $\mathcal{Z}_\ell[\epsilon,\delta]$ with size $(1-\epsilon/2)n$, we need to show that t^* rounds are required to pebble S (assuming we have $(1-\epsilon)n$ black pebbles overall and δ red pebbles in each layer).

Let X be the subset of S of unpebbled nodes, it is enough to show that X requires t^* rounds to be pebbled starting from the same configuration of pebbles stated before. Notice that $|X| \geq (\alpha_\ell - \epsilon/2)n$, and if $(\alpha_\ell - \epsilon/2)n > 0.8$ then $\beta n - 1$ rounds are required to pebble X because the last layer is a DRG.

Define $\alpha^* = (\alpha_\ell - \epsilon/2) - \rho_{i-1} - \rho_{i-2}$ ($\alpha_\ell n$ defined as the number of unpebbled nodes that in the last layer of $\mathcal{Z}_\ell[\epsilon,\delta]$, $\rho_j n$ defined as the number of black pebbles in layer j in $\mathcal{Z}_\ell[\epsilon,\delta]$), define Z as the set of *forward dependencies* of X in layer V_{i-2}, and $\alpha' = |Z|/n$. Because of Lemma 6 we split the proof in two cases:

1. $\alpha^* \leq 1/3$: in this case we have that $\alpha' \geq 2\alpha^* - 2\delta$. This implies that

$$\alpha' - \gamma_{\ell-2} \geq \epsilon - 4\delta \tag{12}$$

   ($\gamma_{\ell-2}n$ defined as the number of black pebbles from layer 1 to layer $\ell-3$ in $\mathcal{Z}_\ell[\epsilon,\delta]$).

   Now, consider the graph $\mathcal{Z}_{\ell-2}[\epsilon-3\delta,\delta]$ with the following specific constrain in its pebble configuration: the number of black pebbles from layer 1 to layer $\ell-3$ is $\gamma_{\ell-2}n$ (the same number as in $\mathcal{Z}_\ell[\epsilon,\delta]$). Then, (12) says that we can apply Claim 3, and therefore the fact that $\mathcal{Z}_{\ell-2}[\epsilon-3\delta,\delta]$ is $(t,1)$-hard implies that Z needs at least t rounds in order to be pebbled in $\mathcal{Z}_{\ell-2}[\epsilon-3\delta,\delta]$ (note that this implies that Z needs at least t round in $\mathcal{Z}_\ell[\epsilon,\delta]$ too). Therefore, X needs $t+2$ rounds to be pebbled in in $\mathcal{Z}_\ell[\epsilon,\delta]$.

2. $\alpha^* > 1/3$: in this case we have that $\alpha' \geq 0.12 + \alpha_\ell - \epsilon/2 - 2\delta - \rho_{\ell-1} - \rho_{\ell-2}$. This implies that

$$\alpha' - \gamma_{\ell-2} \geq 0.12 - 3\delta + \epsilon/2 \tag{13}$$

   If $\epsilon - 2\delta \leq 0.24$, then $0.12 - 3\delta + \epsilon/2 \geq \epsilon - 4\delta$ and we can conclude as before.

□