Proof

1 PROOF OF OVERFLOW PROBABILITY

Proof. Let T be the ORAM tree. T is a perfect binary tree of height L, thus having $N = 2^{L+1} - 1$ nodes and $n = 2^L$ leaves. For each node u in T, let X_u be random variable representing the maximal number of blocks it contains during the process. Let $Y_u = \max\{X_u - Z, 0\}$ for any u.

Lemma 1. *For every node x, if p and q be its children. For all $t \in \mathbb{R}$,*

$$\mathbb{E}\left[\exp\left(tY_p\right)\right] \cdot \mathbb{E}\left[\exp\left(tY_q\right)\right] \ge \mathbb{E}\left[\exp\left(t(Y_p + Y_q)\right)\right] \tag{1}$$

Proof. For every node u in T, let b_x be the total number of blocks in the subtree rooting at x. Then $B_u = B_p + B_q$. Given b and t, for any $\beta \ge 0$, let $r_\beta = \mathbb{E}\left[\exp(tY_p) \mid B_p = \beta\right]$, $s_\beta = \mathbb{E}\left[\exp(tY_q) \mid B_q = b - \beta\right]$, $k_\beta = \mathbb{E}\left[B_p = \beta\right] = \mathbb{E}\left[B_q = \beta\right]$ (the second equality comes from symmetry). Since each block is placed independently, s_β is non-decreasing with β, and r_β is non-increasing with β.

Now for any $b \ge 0$,

$$\begin{align}
&\mathbb{E}\left[\exp(t(Y_p + Y_q)) \mid B_u = b\right] \tag{2}\\
=\,&\mathbb{E}\left[\exp(tY_p) \cdot \exp(tY_q) \mid B_p + B_q = b\right] \tag{3}\\
=\,&\sum_{\beta=0}^{b} \mathbb{E}\left[B_p = \beta\right] \notag\\
&\quad \cdot \mathbb{E}\left[\exp(tY_p) \cdot \exp(tY_q) \mid B_p = \beta, B_q = b - \beta\right] \tag{4}\\
=\,&\sum_{\beta=0}^{b} \mathbb{E}\left[B_p = \beta\right] \cdot \mathbb{E}\left[\exp(tY_p) \mid B_p = \beta, B_q = b - \beta\right] \notag\\
&\quad \cdot \mathbb{E}\left[\exp(tY_q) \mid B_p = \beta, B_q = b - \beta\right] \tag{5}\\
=\,&\sum_{\beta=0}^{b} \mathbb{E}\left[B_p = \beta\right] \cdot \mathbb{E}\left[\exp(tY_p) \mid B_p = \beta\right] \notag\\
&\quad \cdot \mathbb{E}\left[\exp(tY_q) \mid B_q = b - \beta\right] \tag{6}\\
=\,&\sum_{\beta=0}^{b} k_\beta r_\beta s_\beta \tag{7}
\end{align}$$

where the equality in (5) and (6) come from the fact that given the number of blocks in a subtree, its distribution of blocks is independent of the blocks in the rest of tree, since all blocks are put independently.

And

$$\begin{align}
&\mathbb{E}\left[\exp(tY_p) \mid B_u = b\right] \tag{8}\\
=\,&\sum_{\beta=0}^{b} \mathbb{E}\left[B_p = \beta\right] \cdot \mathbb{E}\left[\exp(tY_p) \mid B_p = \beta\right] \tag{9}\\
=\,&\sum_{\beta=0}^{b} k_\beta r_\beta \tag{10}
\end{align}$$

Similarly

$$\mathbb{E}\left[\exp(tY_q) \mid B_u = b\right] = \sum_{\beta=0}^{b} k_\beta s_\beta \tag{11}$$

Hence

$$\begin{align}
&\mathbb{E}\left[\exp(Y_p + Y_q) \mid B_u = b\right] \notag\\
&-\mathbb{E}\left[\exp(tY_p) \mid B_u = b\right] \cdot \mathbb{E}\left[\exp(tY_q) \mid B_u = b\right] \tag{12}\\
=\,&\sum_{\beta=0}^{b} k_\beta r_\beta s_\beta - \sum_{\beta=0}^{b} k_\beta r_\beta \cdot \sum_{\beta=0}^{b} k_\beta s_\beta \tag{13}\\
=\,&\sum_{\beta=0}^{b} k_\beta r_\beta s_\beta \sum_{\beta=0}^{b} k_\beta - \sum_{\beta=0}^{b} k_\beta r_\beta \cdot \sum_{\beta=0}^{b} k_\beta s_\beta \tag{14}\\
=\,&\sum_{\beta_1=0}^{b} \sum_{\beta_2=0}^{b} k_{\beta_1} k_{\beta_2} (r_{\beta_1} - r_{\beta_2})(s_{\beta_1} - s_{\beta_2}) \tag{15}\\
\le\,&0 \tag{16}
\end{align}$$

Since above inequality holds for any b, we conclude that

$$\mathbb{E}\left[\exp(Y_p + Y_q)\right] - \mathbb{E}\left[\exp(tY_p)\right] \cdot \mathbb{E}\left[\exp(tY_q)\right] \ge 0 \tag{17}$$

Thus completing the proof of the lemma. □

For leaves c in T, since X_c follows $(1/n, nZ)$-Bernoulli distribution, we have

$$\mathbb{E}\left[\exp\left(tX_c\right)\right] = \left(1 + \frac{1}{n}(e^t - 1)\right)^{nZ} \tag{18}$$

Then if u has two children p, q, we have

$$X_u = \max\{p - Z, 0\} + \max\{q - Z, 0\} = Y_p + Y_q. \tag{19}$$

Then for any $t > 0$,

$$\begin{align}
&\mathbb{E}\left[\exp\left(tX_u\right)\right] \tag{20}\\
=\,&\mathbb{E}\left[\exp\left(t(Y_p + Y_q)\right)\right] \tag{21}\\
\le\,&\mathbb{E}\left[\exp\left(tY_p\right)\right] \cdot \mathbb{E}\left[\exp\left(tY_q\right)\right] \tag{22}\\
=\,&\mathbb{E}\left[\exp\left(t\max\{X_p - Z, 0\}\right)\right] \notag\\
&\cdot \mathbb{E}\left[\exp\left(t\max\{X_p - Z, 0\}\right)\right] \tag{23}\\
\le\,&\left(1 + e^{-Zt}\mathbb{E}\left[\exp\left(tX_p\right)\right]\right)\left(1 + e^{-Zt}\mathbb{E}\left[\exp\left(tX_q\right)\right]\right) \tag{24}
\end{align}$$

Lemma 2. *For $0 < p < 1/4$, the sequence $\{a_n\}_{n\ge0}$ defined by $a_{n+1} = (1 + pa_n)^2$ converges to $\frac{2}{1-2p+\sqrt{1-4p}}$ if $0 < a_0 < \frac{1-2p+\sqrt{1-4p}}{2p^2}$.*

Proof. Notice that

$$\alpha = \frac{2}{1 - 2p + \sqrt{1 - 4p}} \tag{25}$$

$$\beta = \frac{1 - 2p + \sqrt{1 - 4p}}{2p^2} \tag{26}$$

are two solutions of the equation $(1 + px)^x = x$ on x. By the monotonicity of quadratic polynomial, for all $\alpha \le x < \beta$, $\alpha < (1 + px)^2 < x$. And for all $0 < x \le \alpha$, $x \le (1 + px)^2 \le \alpha$.

Therefore if $\alpha \leq a_0 < \beta$, for all n, $\alpha < a_{n+1} < a_n < \beta$. Applying monotone convergence theorem, $\{a_n\}$ has a limit L. Since $L = \lim_{n\to\infty}(1+pa_n)^2 = (1+pL)^2$, L must be α (it cannot be β because $a_n < a_0 < \beta$).

If $0 < a_0 \leq \alpha$, for all n, $0 < a_n \leq a_{n+1} < \alpha$. Similarly we deduce that $\{a_n\}$ tends to α by applying monotone convergence theorem. □

Take c_d be any node in the $(L-d)$-th level of the tree. Then

$$\mathbb{E}\left[\exp\left(tX_{c_0}\right)\right] = \left(1 + \frac{1}{n}(e^t - 1)\right)^{nZ} < e^{Z(e^t-1)} \tag{27}$$

Consider the sequence $\{a_n\}_{n\geq 0}$ defined by $a_0 = e^{Z(e^t-1)}$, $a_{n+1} = (1+e^{-Zt}a_n)^2$. Since $\mathbb{E}\left[\exp\left(tX_{c_0}\right)\right] < a_0$, applying inequality (24), we deduce by induction that $\mathbb{E}\left[\exp\left(tX_{c_d}\right)\right] < a_d$ for every $d \geq 0$.

According to lemma 2, the sequence $\{a_n\}_{n\geq 0}$ converges if

$$e^{Z(e^t-1)} < \frac{1}{2}e^{2Zt}(1 - 2e^{-Zt} + \sqrt{1-4e^{-Zt}}) \tag{28}$$

$$\iff e^{Z(e^t-2t-1)} < \frac{1}{2}(1 - 2e^{-Zt} + \sqrt{1-4e^{-Zt}}) \tag{29}$$

When $t = 1$, the left hand side of (29) is smaller than 0.6, the right hand side is larger than 0.7. For sufficiently large t, the left hand side tends to infinity but the right hand side is smaller to 1. Thus we can take $\gamma_Z > 1$ to be the maximal value of t such that the inequality (29) holds.

For some small $\delta > 0$, let $t \in \gamma_Z - \delta$. Now $\{a_n\}_n$ converges to $2(1 - 2e^{-Zt} + \sqrt{1-4e^{-Zt}})$. Thus for sufficiently large L,

$$a_L < \frac{2}{1 - 2e^{-Zt} + \sqrt{1-4e^{-Zt}}} + \epsilon \tag{30}$$

.

The stash overflows if and only if the root contains more than $Z + R$ blocks. By Markov's Inequality,

$$p_{\text{overflow}} = \Pr\left[X_{c_L} > Z + R\right] \tag{31}$$

$$= \Pr\left[\exp(tX_{c_L}) \geq e^{t(Z+R+1)}\right] \tag{32}$$

$$\leq e^{-t(Z+R+1)}\mathbb{E}\left[\exp\left(tX_{c_L}\right)\right] \tag{33}$$

$$\leq e^{-(\gamma_Z-\delta)(Z+R+1)}H_Z \tag{34}$$

$$= C_Z\alpha_Z^R \tag{35}$$

where

$$H_Z = \left(\frac{2}{1 - 2e^{-Z(\gamma_Z-\delta)} + \sqrt{1-4e^{-Z(\gamma_Z-\delta)}}} + \epsilon\right) \tag{36}$$

$$C_Z = e^{-(\gamma_Z-\delta)(Z+1)}H_Z \tag{37}$$

$$\alpha_Z = e^{-(\gamma_Z-\delta)} \tag{38}$$

which is the desired upper bound of overflow probability.

In particular, take sufficiently small δ and ϵ,

$$C_2 < 0.038, \quad \alpha_2 < 0.310 \tag{39}$$

$$C_3 < 0.008, \quad \alpha_3 < 0.288 \tag{40}$$

$$C_4 < 0.002, \quad \alpha_4 < 0.286 \tag{41}$$

□

2 PROOF OF CORRECTNESS ABOUT OBLIVIOUS PLACEMENT

First we will formalize the process of Oblivious Placement. Without loss of generality, let 0 denotes the invalid key. Let $n = 2^k$, the outmost loop of Oblivious Placement is looped by k times. In the r ($r = 1, 2, \ldots, k$) time, the variable $T = 2^{k-r}$. The operations executed when $T = 2^{k-r}$ is denoted as the r-th round. Let $a^{(r)}$ be the array addr at the end of the r-th loop. In particular, $a^{(0)}$ is original array. In the r-th round, for any $M = 0, 2T, \ldots, n - 2T$ and $i \in [M, M+T)$, if $0 < a^{(r)}_{M+T+i} < M+T$ or $a^{(r)}_{M+i} \geq M+T$, $a^{(r)}_{M+T+i}$ and $a^{(r+1)}_{M+i}$ are swapped in $a^{(r+1)}$, otherwise they are kept unchanged in $a^{(r+1)}$.

To prove the correctness of Oblivious Placement, we need to prove that $a^{(k)}_i = i$ for any i appearing in a_0, and $a^{(k)}_i = 0$ for all other i.

Proof. We will prove that for each $r \in \{0, 1, \ldots, k\}$ (again define $T = 2^{k-r}$), and for each $M = \{0, 2T, \ldots, M - 2T\}$, the subarray $a^{(r)}_{[M,M+2T)}$ satisfies the following properties:

Property 1. Nonzero elements are in the same range of indices of the subarray. Formally speaking, if the indices of subarray takes in the interval $[a, b)$ (in this case $a = M, b = M + 2T$), any nonzero element lies in the interval $x \in [a, b)$.

Property 2. We can rotate the elements such that the indices of all nonzero elements are continuous and strictly increasing. Formally speaking, there exists some u, v ($u \in [a, b)$) such that $a^{(r)}_u < a^{(r)}_{u+1} < \cdots < a^{(r)}_v$, or $a^{(r)}_u < a^{(r)}_{u+1} < \cdots < a^{(r)}_{b-1} < a^{(r)}a < a^{(r)}_{a+1} < \cdots < a^{(r)}_v$; and any other elements in $a^{(r)}$ is zero. Notice that the subarray may only contain zeros, which is included in the case $u > v$.

If a subarray satisfies above properties, say it is (u, v)-cyclic, or cyclic in short, where u, v are taken the same value as they are in property 2.

This can be proven by induction. The case when $r = 0$ is just a restatement of the assumption for elements in $a^{(0)}$. It suffices to prove the $(r+1)$-case if smaller cases are proved. Again let $T = 2^{k-r}$, for each $M \in \{0, 2T, \ldots, M - 2T\}$, the subarray $B = a^{(r-1)}_{[M,M+2T)}$ will be separated into two subarrays $C_1 = a^{(r)}_{[M,M+T)}$ and $C_2 = a^{(r)}_{[M+T,M+2T)}$ after the $(r+1)$-th loop.

For index $u \in [M, M+T)$, if $a^{(r)}_u \geq M+T$, say u is raised; for index $u \in [M+T, M+2T)$, if $0 < a^{(r)}_u < M+T$, say u is sunk. According to the induction hypothesis, B is (u, v)-cyclic for some u, v. We will discuss every possible cases of u and v, and prove that under all cases, both C_1 and C_2 are cyclic.

Case 1. $u > v$, i.e. all elements in B are zero. Then all elements in C_1 and C_2 are also zero.

Case 2. $M \leq v < M + 2T$. Because nonzero elements in B are strictly increasing, it is impossible that both sunk and raised u exists.

If there is neither sunk nor raised elements, then B is unchanged from a_r to a_{r+1}. According to the definition of sunk/raised, property 1 is automatically satisfied for C_1 and C_2. Furthermore the continuous set of indices of nonzero elements, after cutting by half, is still two continuous set of indices. Hence property 2 are also satisfied.

If there is some indices that is raised or sunk, according to the symmetry, we may assume there is some sunk indices without loss of generality.

If $u < M+T$, there is some $w \in [M+T, v]$ s.t. $M+T, M+T+1, \dots, w$ are all sunk elements. Because $a_w^{(r)} \le M+T$, $a_w^{(r)} \ge a_u^{(r)} + w - u$ and $a_w^{(r)} < M + 2T$ we have $u > w - T$. Therefore C_1 is $(w - T, u)$-cyclic and C_2 is $(w + 1, v)$-cyclic.

If $u \ge M + T$. Then there is some $w \in [u, v]$ s.t. $w, w + 1, \dots, v$ are all sunk elements. Therefore C_1 is $(u - T, w - T)$-cyclic and C_2 is $(w + 1, v)$-cyclic.

Case 3. $v \ge M + 2T$. If there is neither sunk nor raised elements, then B is unchanged from a_r to a_{r+1}. Again property 1 is automatically satisfied for C_1 and C_2. The nonzero elements in C_2 is still continuous, and the nonzero elements in C_1 is either continuous or continuous after rotating. In both cases C_1 and C_2 are both cyclic.

If there exists some sunk or raised elements, we will consider three subcases.

(1) $a_M^{(r)} < M + T$. Then there exists some $w \in [M + 1, v + 1]$ s.t. $w, w+1, \dots, v$ are all raised indices. Then $a_u^{(r)} < a_M^{(r)} < M + T$, implying $[u, M + 2T)$ are all indices being sunk. Because $(w - 1 + 2T) - u \le a_{w-1}^{(r)} - a_u^{(r)} \le (M + T - 1) - M = T - 1$, we have $w - 1 < u - T$. Thus C_1 is $(u - T, w - 1)$-cyclic and C_2 is $(w + T, v + T)$-cyclic.

(2) $a_M^{(r)} \ge M + T$ and $u \ge M + T$. Then all indices in $[M, v]$ are raised. And for some $w \in [u, M + 2T]$, $[u, w]$ are all indices being sunk ($u = M+2T$ means no indices are sunk). Because $(v+2T) - (w+1) \le a_u^{(r)} - a_{w+1}^{(r)} \le (M+2T-1) - (M+T) = T-1$, we have $w+1 > v+T$. Thus C_1 is $(u-T, w-T)$-cyclic and C_2 is $(w + 1, v + T)$-cyclic.

(3) $a_M^{(r)} \ge M + T$ and $u < M + T$. Again all indices in $[M, u]$ are raised. For some $w \in [M + T, M + 2T]$, $[M + T, w]$ are all indices being sunk. $(v + 2T) - (w + 1) \le a_v^{(r)} - a_w^{(r)} \le (M + 2T - 1) - (M + T) = T - 1$ hence $w + 1 > v + T$. $w-u \le a_w^{(r)} - a_u^{(r)} \le (M+T-1) - M = T-1$ hence $u > w+T$. Thus C_1 is $(u, w - T)$-cyclic and C_2 is $(w + 1, v + T)$-cyclic.

From all cases discussed above, for each r, each one in corresponding subarrays are cyclic. Particularly, when $r = k$, each subarray is of length 1. According to property 1, the element is either equal to its index, either be zero. Because during the rounds the elements are only swapped, every nonzero elements in the original array still appears in the result array. Thus our proof is complete. □