Appendix A. SAVHO Decryption Function Correctness

The correctness of the decryption function presented in Section 3.1.3 and illustrated by both Eq. 4 and Eq. 5 is explained by the following:

1. Retrieving the S vector elements

   For a given cipher-text $c = [c_0, ..., c_{n-1}]$ where $c_i = \sum_{k=0}^{n-1} p_{ik}(N_k S_k + R_k)$,

$$\begin{aligned}
&\sqrt{2(\sum_{j=0}^{n-1} q_{ij} c_j - R_i) + N_i^2 + S_i^2} - N_i \\
&= \sqrt{2(\sum_{j=0}^{n-1} q_{ij} \sum_{k=0}^{n-1} p_{jk}(N_k S_k + R_k) - R_i) + N_i^2 + S_i^2} - N_i \qquad \text{(A.1)} \\
&= \sqrt{2(\sum_{j=0}^{n-1} \sum_{k=0}^{n-1} q_{ij} p_{jk}(N_k S_k + R_k) - R_i) + N_i^2 + S_i^2} - N_i
\end{aligned}$$

   In order to simplify and avoid the repetition of the computation procedure on all the i's values ($i \in [\ 0, n-1]$), the $\sum_{j=0}^{n-1} \sum_{k=0}^{n-1} q_{ij} p_{jk}(N_k S_k + R_k)$ part is calculated then replaced into Eq. (A.1), respectively for two examples: $i = 0$ and $i = n-1$.

   For $i = 0$,

$$\begin{aligned}
&\sum_{j=0}^{n-1} \sum_{k=0}^{n-1} q_{0j} p_{jk}(N_k S_k + R_k) = q_{00} p_{00}(N_0 S_0 + R_0) + q_{00} p_{01}(N_1 S_1 + R_1) + \\
&\cdots + q_{00} p_{0\,n-1}(N_{n-1} S_{n-1} + R_{n-1}) + q_{01} p_{10}(N_0 S_0 + R_0) + q_{01} p_{11}(N_1 S_1 \\
&+ R_1) + ... + q_{01} p_{1\,n-1}(N_{n-1} S_{n-1} + R_{n-1}) + ... + q_{0\,n-1} p_{n-1\,0}(N_0 S_0 + \\
&R_0) + q_{0\,n-1} p_{n-1\,1}(N_1 S_1 + R_1) + \cdots + q_{0\,n-1} p_{n-1\,n-1}(N_{n-1} S_{n-1} + R_{n-1}) \\
&= (N_0 S_0 + R_0)(q_{00} p_{00} + q_{01} p_{10} + ... + q_{0\,n-1} p_{n-1\,0}) + (N_1 S_1 + R_1)(q_{00} \\
&p_{01} + q_{01} p_{11} + \cdots + q_{0\,n-1} p_{n-1\,1}) + \cdots + (N_{n-1} S_{n-1} + R_{n-1})(q_{00} p_{0\,n-1} \\
&+ q_{01} p_{1\,n-1} + ... + q_{0\,n-1} p_{n-1\,n-1}) \qquad \text{(A.2a)} \\
&= (N_0 S_0 + R_0) \times 1 + (N_1 S_1 + R_1) \times 0 + \cdots + (N_{n-1} S_{n-1} + R_{n-1}) \times 0 \\
&\qquad \text{(A.2b)} \\
&= N_0 S_0 + R_0
\end{aligned}$$

Remark: Passing from (A.2a) to (A.2b) is explained at the last part of this section.

Replacing the latter result in Eq. (A.1), one can obtain:

$\sqrt{2(N_0S_0 + R_0 - R_0) + N_0^2 + S_0^2} - N_0 = \sqrt{2N_0S_0 + N_0^2 + S_0^2} - N_0 = \sqrt{(N_0 + S_0)^2} - N_0 = N_0 + S_0 - N_0 = S_0$

Remark: $\sqrt{(N_0 + S_0)^2} = |N_0 + S_0| = N_0 + S_0$ since $N_0 + S_0$ is a positive number as mentioned in 3.1.2.

$\vdots$

For $i = n - 1$,

$$\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} q_{n-1\,j}p_{jk}(N_kS_k + R_k) = q_{n-1\,0}p_{00}(N_0S_0 + R_0) + q_{n-1\,0}p_{01}(N_1S_1 + R_1) + \cdots + q_{n-1\,0}p_{0\,n-1}(N_{n-1}S_{n-1} + R_{n-1}) + q_{n-1\,1}p_{10}(N_0S_0 + R_0) + q_{n-1\,1}p_{11}(N_1S_1 + R_1) + \cdots + q_{n-1\,1}p_{1\,n-1}(N_{n-1}S_{n-1} + R_{n-1}) + \cdots + q_{n-1\,n-1}p_{n-1\,0}(N_0S_0 + R_0) + q_{n-1\,n-1}p_{n-1\,1}(N_1S_1 + R_1) + \cdots + q_{n-1\,n-1}p_{n-1\,n-1}(N_{n-1}S_{n-1} + R_{n-1})$$

$$= (N_0S_0 + R_0)(q_{n-1\,0}p_{00} + q_{n-1\,1}p_{10} + \cdots + q_{n-1\,n-1}p_{n-1\,0}) + (N_1S_1 + R_1)(q_{n-1\,0}p_{01} + q_{n-1\,1}p_{11} + ... + q_{n-1\,n-1}p_{n-1\,1}) + \cdots + (N_{n-1}S_{n-1} + R_{n-1})(q_{n-1\,0}p_{0\,n-1} + q_{n-1\,1}p_{1\,n-1} + \cdots + q_{n-1\,n-1}p_{n-1\,n-1}) \tag{A.3a}$$

$$= (N_0S_0 + R_0) \times 0 + (N_1S_1 + R_1) \times 0 + \cdots + (N_{n-1}S_{n-1} + R_{n-1}) \times 1 \tag{A.3b}$$

$$= N_{n-1}S_{n-1} + R_{n-1}$$

Remark: Passing from (A.3a) to (A.3b) is explained at the last part of this section.

Replacing the latter result in Eq. (A.1), one can obtain the following:

$$\begin{aligned}
&\sqrt{2(N_{n-1}S_{n-1}+R_{n-1}-R_{n-1})+N_{n-1}^2+S_{n-1}^2}-N_{n-1}\\
&=\sqrt{2N_{n-1}S_{n-1}+N_{n-1}^2+S_{n-1}^2}-N_{n-1}\\
&=\sqrt{(N_{n-1}+S_{n-1})^2}-N_{n-1}\\
&=N_{n-1}+S_{n-1}-N_{n-1}\\
&=S_{n-1}
\end{aligned}$$

Remark: $\sqrt{(N_{n-1}+S_{n-1})^2}=|N_{n-1}+S_{n-1}|=N_{n-1}+S_{n-1}$ since $N_{n-1}+S_{n-1}$ is positive as mentioned in 3.1.2.

2. Retrieving the plain-text m

   After recovering S_i values, the user easily retrieves the plain-text message m by computing $\sum_{i=0}^{n-1} S_i$.

This demonstration affirms that the SAVHO crypto-system is coherent since from which it has been possible to prove that the user always manages, by decrypting c, to find the initial message m.

Before analyzing the homomorphic behavior of SAVHO scheme, we decide to intensively depict the passage we have done from (A.2a) to (A.2b) and from (A.3a) to (A.3b).

Let $P=(p_{ij}\in\mathbb{Z})$ be an invertible matrix of dimension $n\times n$ and $Q=(q_{ij}\in\mathbb{Z})$ represent P^{-1} the inverse matrix of P. Therefore,

$QP=I_{n-1}$

$$\begin{pmatrix} q_{00} & \cdots & q_{0\,n-1}\\ \vdots & \ddots & \vdots\\ q_{n-1\,0} & \cdots & q_{n-1\,n-1}\end{pmatrix}\times\begin{pmatrix} p_{00} & \cdots & p_{0\,n-1}\\ \vdots & \ddots & \vdots\\ p_{n-1\,0} & \cdots & p_{n-1\,n-1}\end{pmatrix}=\begin{pmatrix} 1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & 1\end{pmatrix}$$

Then,

$q_{00}p_{00}+q_{01}p_{10}+...+q_{0\,n-1}p_{n-1\,0}=1$

$q_{00}p_{01}+q_{01}p_{11}+...+q_{0\,n-1}p_{n-1\,1}=0$

$q_{00}p_{0\,n-1}+q_{01}p_{1\,n-1}+...+q_{0\,n-1}p_{n-1\,n-1}=0$

$\vdots$

$q_{n-1\,0}p_{00}+q_{n-1\,1}p_{10}+...+q_{n-1\,n-1}p_{n-1\,0}=0$

$q_{n-1\,0}p_{01}+q_{n-1\,1}p_{11}+...+q_{n-1\,n-1}p_{n-1\,1}=0$

$q_{n-1\,0}p_{0\,n-1} + q_{n-1\,1}p_{1\,n-1} + ... + q_{n-1\,n-1}p_{n-1\,n-1} = 1$

The first three equations are used in the passage from (A.2a) to (A.2b) and the last three ones in the passage from (A.3a) to (A.3b).

Appendix B. SAVHO Homomorphic Addition Correctness

The correctness of the homomorphic addition given in Section 3.2.1 and illustrated by Eq. 6 is explained in details as follows:

Let $c = (c_i)_{0\leq i\leq n-1}$ and $c^{'} = (c^{'}_i)_{0\leq i\leq n-1}$ be two cipher-texts corresponding respectively to two plain-texts m and m'.

According to SAVHO crypto-system $c_i = \sum_{m=0}^{n-1} p_{im}(N_m S_m + R_m)$ and $c^{'}_i = \sum_{k=0}^{n-1} p_{ik}(N^{'}_k S^{'}_k + R^{'}_k)$.

Therefore, the sum of these cipher-texts is given by:

$c_{add} = c+c^{'} = (\sum_{m=0}^{n-1} p_{im}(N_m S_m+R_m))_{0\leq i\leq n-1}+(\sum_{k=0}^{n-1} p_{ik}(N^{'}_k S^{'}_k+R^{'}_k))_{0\leq i\leq n-1}$.

The next part shows that retrieving the $m+m'$ value can be done by decrypting c_{add}.

1. Retrieving the $S + S'$ vector elements

   $\forall\ i \in [0, n-1]$,

$$
\begin{aligned}
&(2(\sum_{j=0}^{n-1} q_{ij}(\sum_{m=0}^{n-1} p_{jm}(N_m S_m + R_m) + \sum_{k=0}^{n-1} p_{jk}(N^{'}_k S^{'}_k + R^{'}_k)) - (R_i + R^{'}_i)) + N_i^2 \\
&+ N_i^{'2} + S_i^2 + S_i^{'2} + 2(N_i + S_i)(N^{'}_i + S^{'}_i))^{\frac{1}{2}} - N_i - N^{'}_i \\
&= (2(\sum_{j=0}^{n-1} q_{ij} \sum_{m=0}^{n-1} p_{jm}(N_m S_m + R_m) + \sum_{j=0}^{n-1} q_{ij} \sum_{k=0}^{n-1} p_{jk}(N^{'}_k S^{'}_k + R^{'}_k) - (R_i + \\
&R^{'}_i)) + N_i^2 + N_i^{'2} + S_i^2 + S_i^{'2} + 2(N_i + S_i)(N^{'}_i + S^{'}_i))^{\frac{1}{2}} - N_i - N^{'}_i \\
&= (2(\sum_{j=0}^{n-1}\sum_{m=0}^{n-1} q_{ij}p_{jm}(N_m S_m + R_m) + \sum_{j=0}^{n-1}\sum_{k=0}^{n-1} q_{ij}p_{jk}(N^{'}_k S^{'}_k + R^{'}_k) - (R_i + \\
&R^{'}_i)) + N_i^2 + N_i^{'2} + S_i^2 + S_i^{'2} + 2(N_i + S_i)(N^{'}_i + S^{'}_i))^{\frac{1}{2}} - N_i - N^{'}_i
\end{aligned}
\tag{B.1}
$$

   Proceeding in the same way as in the previous proof:

   $\sum_{j=0}^{n-1}\sum_{m=0}^{n-1} q_{ij}p_{jm}(N_m S_m + R_m) = N_0 S_0 + R_0$

$\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} q_{ij}p_{jk}(N_k^{'}S_k^{'}+R_k^{'}) = N_0^{'}S_0^{'}+R_0^{'}$ for $i=0$ and they are equal respectively to $N_{n-1}S_{n-1}+R_{n-1}$ and $N_{n-1}^{'}S_{n-1}^{'}+R_{n-1}^{'}$ for $i=n-1$.

Therefore, for $i=0$, the Eq. (B.1) computation is given by the following:

$$(2(N_0S_0+R_0+N_0^{'}S_0^{'}+R_0^{'}-(R_0+R_0^{'}))+N_0^2+N_0^{'2}+S_0^2+S_0^{'2}+2(N_0$$
$$+S_0)(N_0^{'}+S_0^{'}))^{\frac{1}{2}}-N_0-N_0^{'}$$
$$=(2(N_0S_0+R_0+N_0^{'}S_0^{'}+R_0^{'}-R_0-R_0^{'})+N_0^2+N_0^{'2}+S_0^2+S_0^{'2}+2(N_0+$$
$$+S_0)(N_0^{'}+S_0^{'}))^{\frac{1}{2}}-N_0-N_0^{'}$$
$$=(2N_0S_0+2N_0^{'}S_0^{'}+N_0^2+N_0^{'2}+S_0^2+S_0^{'2}+2(N_0+S_0)(N_0^{'}+S_0^{'}))^{\frac{1}{2}}-N_0$$
$$-N_0^{'}$$
$$=\sqrt{(N_0+S_0)^2+(N_0^{'}+S_0^{'})^2+2(N_0+S_0)(N_0^{'}+S_0^{'})}-N_0-N_0^{'}$$
$$=\sqrt{(N_0+S_0+N_0^{'}+S_0^{'})^2}-N_0-N_0^{'}$$
$$=N_0+S_0+N_0^{'}+S_0^{'}-N_0-N_0^{'}$$
$$=S_0+S_0^{'}$$

Remark: $\sqrt{(N_0+S_0+N_0^{'}+S_0^{'})^2}=|N_0+S_0+N_0^{'}+S_0^{'}|=N_0+S_0+N_0^{'}+S_0^{'}$ since $N_0+S_0>0$ and $N_0^{'}+S_0^{'}>0$ as mentioned in 3.1.2.

$\vdots$

For $i=n-1$, the Eq. (B.1) computation is given by the following:

$$(2(N_{n-1}S_{n-1}+R_{n-1}+N_{n-1}^{'}S_{n-1}^{'}+R_{n-1}^{'}-(R_{n-1}+R_{n-1}^{'}))+N_{n-1}^2+$$
$$N_{n-1}^{'2}+S_{n-1}^2+S_{n-1}^{'2}+2(N_{n-1}+S_{n-1})(N_{n-1}^{'}+S_{n-1}^{'}))^{\frac{1}{2}}-N_{n-1}-N_{n-1}^{'}$$
$$=(2(N_{n-1}S_{n-1}+R_{n-1}+N_{n-1}^{'}S_{n-1}^{'}+R_{n-1}^{'}-R_{n-1}-R_{n-1}^{'})+N_{n-1}^2+$$
$$N_{n-1}^{'2}+S_{n-1}^2+S_{n-1}^{'2}+2(N_{n-1}+S_{n-1})(N_{n-1}^{'}+S_{n-1}^{'}))^{\frac{1}{2}}-N_{n-1}-N_{n-1}^{'}$$
$$=(2N_{n-1}S_{n-1}+2N_{n-1}^{'}S_{n-1}^{'}+N_{n-1}^2+N_{n-1}^{'2}+S_{n-1}^2+S_{n-1}^{'2}+2(N_{n-1}$$
$$+S_{n-1})(N_{n-1}^{'}+S_{n-1}^{'}))^{\frac{1}{2}}-N_{n-1}-N_{n-1}^{'}$$
$$=((N_{n-1}+S_{n-1})^2+(N_{n-1}^{'}+S_{n-1}^{'})^2+2(N_{n-1}+S_{n-1})(N_{n-1}^{'}+S_{n-1}^{'}))^{\frac{1}{2}}$$
$$-N_{n-1}-N_{n-1}^{'}$$
$$=\sqrt{(N_{n-1}+S_{n-1}+N_{n-1}^{'}+S_{n-1}^{'})^2}-N_{n-1}-N_{n-1}^{'}$$

$= N_{n-1} + S_{n-1} + N'_{n-1} + S'_{n-1} - N_{n-1} - N'_{n-1}$

$= S_{n-1} + S'_{n-1}$

Remark: $\sqrt{(N_{n-1} + S_{n-1} + N'_{n-1} + S'_{n-1})^2} = |N_{n-1} + S_{n-1} + N'_{n-1} + S'_{n-1}| = N_{n-1} + S_{n-1} + N'_{n-1} + S'_{n-1}$ since $N_{n-1} + S_{n-1} > 0$ and $N'_{n-1} + S'_{n-1} > 0$ as mentioned in 3.1.2.

2. Retrieving $m + m'$

   $m + m'$ is given by summing the result of the previous calculation i.e $S_0 + S'_0 + \cdots + S_{n-1} + S'_{n-1}$ which is equal to $S_0 + ... + S_{n-1} + S'_0 + ... + S'_{n-1}$.

Appendix C. SAVHO Homomorphic Average Correctness

The correctness of the homomorphic average given in Section 3.2.2 and illustrated by Eq. 7 is explained in details as follows:

Suppose that $c = (c_i)_{0 \le i \le n-1} = (\sum_{m=0}^{n-1} p_{im}(N_m S_m + R_m))_{0 \le i \le n-1}$ and $c' = (c'_i)_{0 \le i \le n-1} = (\sum_{k=0}^{n-1} p_{ik}(N'_k S'_k + R'_k))_{0 \le i \le n-1}$ represent two cipher-texts in SAVHO crypto-system. To obtain the average over plain-texts i.e $\frac{m+m'}{2}$ while operating on cipher-texts the user must decrypt $c_{Average} = \frac{c+c'}{2} = (\sum_{m=0}^{n-1} p_{im}(N_m \frac{S_m}{2} + \frac{R_m}{2}))_{0 \le i \le n-1} + (\sum_{k=0}^{n-1} p_{ik}(N'_k \frac{S'_k}{2} + \frac{R'_k}{2}))_{0 \le i \le n-1}$.

1. Retrieving the $\frac{S+S'}{2}$ vector elements

   $\forall\ i \in [0, n-1]$,

$$(2(\sum_{j=0}^{n-1} q_{ij}(\sum_{m=0}^{n-1} p_{jm}(N_m \frac{S_m}{2} + \frac{R_m}{2}) + \sum_{k=0}^{n-1} p_{jk}(N'_k \frac{S'_k}{2} + \frac{R'_k}{2})) - (\frac{R_i}{2} + \frac{R'_i}{2}))$$

$$+ N_i^2 + N_i'^2 + (\frac{S_i}{2})^2 + (\frac{S'_i}{2})^2 + 2(N_i + \frac{S_i}{2})(N'_i + \frac{S'_i}{2}))^{\frac{1}{2}} - N_i - N'_i$$

$$= (2(\sum_{j=0}^{n-1} q_{ij} \sum_{m=0}^{n-1} p_{jm}(N_m \frac{S_m}{2} + \frac{R_m}{2}) + \sum_{j=0}^{n-1} q_{ij} \sum_{k=0}^{n-1} p_{jk}(N'_k \frac{S'_k}{2} + \frac{R'_k}{2}) - (\frac{R_i}{2}$$

$$+ \frac{R'_i}{2})) + N_i^2 + N_i'^2 + (\frac{S_i}{2})^2 + (\frac{S'_i}{2})^2 + 2(N_i + \frac{S_i}{2})(N'_i + \frac{S'_i}{2}))^{\frac{1}{2}} - N_i - N'_i$$

$$= (2(\sum_{j=0}^{n-1} \sum_{m=0}^{n-1} q_{ij} p_{jm}(N_m \frac{S_m}{2} + \frac{R_m}{2}) + \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} q_{ij} p_{jk}(N'_k \frac{S'_k}{2} + \frac{R'_k}{2}) - (\frac{R_i}{2}$$

$$+\frac{R_i^{'}}{2})) + N_i^2 + N_i^{'2} + (\frac{S_i}{2})^2 + (\frac{S_i^{'}}{2})^2 + 2(N_i + \frac{S_i}{2})(N_i^{'} + \frac{S_i^{'}}{2}))^{\frac{1}{2}} - N_i - N_i^{'} \tag{C.1}$$

Proceeding in the same way as in appendix A:
$\sum_{j=0}^{n-1}\sum_{m=0}^{n-1} q_{ij}p_{jm}(N_m\frac{S_m}{2}+\frac{R_m}{2})$ must be equal to $N_0\frac{S_0}{2}+\frac{R_0}{2}$ and $N_{n-1}\frac{S_{n-1}}{2}+\frac{R_{n-1}}{2}$ respectively for $i=0$ and $i=n-1$.
while, $\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} q_{ij}p_{jk}(N_k^{'}\frac{S_k^{'}}{2}+\frac{R_k^{'}}{2})$ must be equal to $N_0^{'}\frac{S_0^{'}}{2}+\frac{R_0^{'}}{2}$ for $i=0$ and $N_{n-1}^{'}\frac{S_{n-1}^{'}}{2}+\frac{R_{n-1}^{'}}{2}$ for $i=n-1$.
Therefore, for $i=0$, the Eq. (C.1) computation is analyzed as following:

$$(2(N_0\frac{S_0}{2} + \frac{R_0}{2} + N_0^{'}\frac{S_0^{'}}{2} + \frac{R_0^{'}}{2} - (\frac{R_0}{2} + \frac{R_0^{'}}{2})) + N_0^2 + N_0^{'2} + (\frac{S_0}{2})^2 + (\frac{S_0^{'}}{2})^2$$
$$+ 2(N_0 + \frac{S_0}{2})(N_0^{'} + \frac{S_0^{'}}{2}))^{\frac{1}{2}} - N_0 - N_0^{'}$$
$$= (2(N_0\frac{S_0}{2} + \frac{R_0}{2} + N_0^{'}\frac{S_0^{'}}{2} + \frac{R_0^{'}}{2} - \frac{R_0}{2} - \frac{R_0^{'}}{2}) + N_0^2 + N_0^{'2} + (\frac{S_0}{2})^2 +$$
$$(\frac{S_0^{'}}{2})^2 + 2(N_0 + \frac{S_0}{2})(N_0^{'} + \frac{S_0^{'}}{2}))^{\frac{1}{2}} - N_0 - N_0^{'}$$
$$= (2N_0\frac{S_0}{2} + 2N_0^{'}\frac{S_0^{'}}{2} + N_0^2 + N_0^{'2} + (\frac{S_0}{2})^2 + (\frac{S_0^{'}}{2})^2 + 2(N_0 + \frac{S_0}{2})(N_0^{'}+$$
$$\frac{S_0^{'}}{2}))^{\frac{1}{2}} - N_0 - N_0^{'}$$
$$= \sqrt{(N_0 + \frac{S_0}{2})^2 + (N_0^{'} + \frac{S_0^{'}}{2})^2 + 2(N_0 + \frac{S_0}{2})(N_0^{'} + \frac{S_0^{'}}{2})} - N_0 - N_0^{'}$$
$$= \sqrt{(N_0 + \frac{S_0}{2} + N_0^{'} + \frac{S_0^{'}}{2})^2} - N_0 - N_0^{'}$$
$$= N_0 + \frac{S_0}{2} + N_0^{'} + \frac{S_0^{'}}{2} - N_0 - N_0^{'}$$
$$= \frac{S_0}{2} + \frac{S_0^{'}}{2}$$

Remark: $\sqrt{(N_0 + \frac{S_0}{2} + N_0^{'} + \frac{S_0}{2}^{'})^2} = |N_0 + \frac{S_0}{2} + N_0^{'} + \frac{S_0^{'}}{2}| = N_0 + \frac{S_0}{2} + N_0^{'} + \frac{S_0^{'}}{2}$ since $N_0 + \frac{S_0}{2} > 0$ and $N_0^{'} + \frac{S_0^{'}}{2} > 0$ as mentioned in 3.1.2.

$\vdots$

For $i = n-1$, the Eq. (C.1) computation is given by the following:

$$(2(N_{n-1}\frac{S_{n-1}}{2} + \frac{R_{n-1}}{2} + N'_{n-1}\frac{S'_{n-1}}{2} + \frac{R'_{n-1}}{2} - (\frac{R_{n-1}}{2} + \frac{R'_{n-1}}{2})) + N^2_{n-1} + N'^2_{n-1}$$
$$+ (\frac{S_{n-1}}{2})^2 + (\frac{S'_{n-1}}{2})^2 + 2(N_{n-1} + \frac{S_{n-1}}{2})(N'_{n-1} + \frac{S'_{n-1}}{2}))^{\frac{1}{2}} - N_{n-1} - N'_{n-1}$$
$$= (2(N_{n-1}\frac{S_{n-1}}{2} + \frac{R_{n-1}}{2} + N'_{n-1}\frac{S'_{n-1}}{2} + \frac{R'_{n-1}}{2} - \frac{R_{n-1}}{2} - \frac{R'_{n-1}}{2}) + N^2_{n-1}$$
$$+ N'^2_{n-1} + (\frac{S_{n-1}}{2})^2 + (\frac{S'_{n-1}}{2})^2 + 2(N_{n-1} + \frac{S_{n-1}}{2})(N'_{n-1} + \frac{S'_{n-1}}{2}))^{\frac{1}{2}}$$
$$- N_{n-1} - N'_{n-1}$$
$$= (2N_{n-1}\frac{S_{n-1}}{2} + 2N'_{n-1}\frac{S'_{n-1}}{2} + N^2_{n-1} + N'^2_{n-1} + (\frac{S_{n-1}}{2})^2 + (\frac{S'_{n-1}}{2})^2 + 2(N_{n-1}$$
$$+ \frac{S_{n-1}}{2})(N'_{n-1} + \frac{S'_{n-1}}{2}))^{\frac{1}{2}} - N_{n-1} - N'_{n-1}$$
$$= ((N_{n-1} + \frac{S_{n-1}}{2})^2 + (N'_{n-1} + \frac{S'_{n-1}}{2})^2 + 2(N_{n-1} + \frac{S_{n-1}}{2})(N'_{n-1} + \frac{S'_{n-1}}{2}))^{\frac{1}{2}}$$
$$- N_{n-1} - N'_{n-1}$$
$$= \sqrt{(N_{n-1} + \frac{S_{n-1}}{2} + N'_{n-1} + \frac{S'_{n-1}}{2})^2} - N_{n-1} - N'_{n-1}$$
$$= N_{n-1} + \frac{S_{n-1}}{2} + N'_{n-1} + \frac{S'_{n-1}}{2} - N_{n-1} - N'_{n-1}$$
$$= \frac{S_{n-1}}{2} + \frac{S'_{n-1}}{2}$$

Remark: $\sqrt{(N_{n-1} + \frac{S_{n-1}}{2} + N'_{n-1} + \frac{S'_{n-1}}{2})^2} = |N_{n-1} + \frac{S_{n-1}}{2} + N'_{n-1} + \frac{S'_{n-1}}{2}| = N_{n-1} + \frac{S_{n-1}}{2} + N'_{n-1} + \frac{S'_{n-1}}{2}$ since $N_{n-1} + \frac{S_{n-1}}{2} > 0$ and $N'_{n-1} + \frac{S'_{n-1}}{2} > 0$ as mentioned in 3.1.2.

2. Retrieving $\frac{m+m'}{2}$

   Summing the result of the previous computations i.e $\frac{S_0}{2} + \frac{S'_0}{2} + \cdots + \frac{S_{n-1}}{2} + \frac{S'_{n-1}}{2}$ which is equal to $\frac{S_0}{2} + ... + \frac{S_{n-1}}{2} + \frac{S'_0}{2} + ... + \frac{S'_{n-1}}{2}$ gives $\frac{m+m'}{2}$ as result.