

## Errata

The following editorial correction has been found in Vol.E104-A, No.9, and should be corrected as follows.

Wrong terms	to be corrected as
p. 1225, Fig. 6, line 18: $\nu := \lceil \xi_1 - \xi_2 \rceil$	p. 1225, Fig. 6, line 18: $\nu := \lceil \xi_2 - \xi_1 \rceil$
p. 1225, Fig. 6, line 23: $\mathbf{h} := \text{MakeHint}_p(-c\mathbf{t}_0, \mathbf{w} - \lceil cs_2 \rceil - \nu + c\mathbf{t}_0, 2\bar{\gamma}_2)$	p. 1225, Fig. 6, line 23: $\mathbf{h} := \text{MakeHint}_p(-c\mathbf{t}_0, \mathbf{w} - \lceil cs_2 \rceil + \nu + c\mathbf{t}_0, 2\bar{\gamma}_2)$
p. 1225, equation (3): $\left\lceil \frac{p}{q} \mathbf{A} \mathbf{z} \right\rceil - c\mathbf{t} = \mathbf{w} - \lceil cs_2 \rceil - \nu$	p. 1225, equation (3): $\left\lceil \frac{p}{q} \mathbf{A} \mathbf{z} \right\rceil - c\mathbf{t} = \mathbf{w} - \lceil cs_2 \rceil + \nu$
p. 1225: $\nu := \lceil \xi_1 - \xi_2 \rceil$	p. 1225: $\nu := \lceil \xi_2 - \xi_1 \rceil$
p. 1225: $\left\lceil \frac{p}{q} \mathbf{A} \mathbf{z} \right\rceil - c\mathbf{t}_1 \cdot 2^d = \mathbf{w} - \lceil cs_2 \rceil - \nu + c\mathbf{t}_0$	p. 1225: $\left\lceil \frac{p}{q} \mathbf{A} \mathbf{z} \right\rceil - c\mathbf{t}_1 \cdot 2^d = \mathbf{w} - \lceil cs_2 \rceil + \nu + c\mathbf{t}_0$
p. 1225: $\mathbf{w}'_1 = \text{UseHint}_p(\mathbf{h}, \mathbf{w} - \lceil cs_2 \rceil - \nu + c\mathbf{t}_0, 2\bar{\gamma}_2) = \text{HighBits}_p(\mathbf{w} - \lceil cs_2 \rceil - \nu, 2\bar{\gamma}_2)$	p. 1225: $\mathbf{w}'_1 = \text{UseHint}_p(\mathbf{h}, \mathbf{w} - \lceil cs_2 \rceil + \nu + c\mathbf{t}_0, 2\bar{\gamma}_2) = \text{HighBits}_p(\mathbf{w} - \lceil cs_2 \rceil + \nu, 2\bar{\gamma}_2)$
p. 1225: $\text{HighBits}_p(\mathbf{w} - \lceil cs_2 \rceil - \nu, 2\bar{\gamma}_2) := \mathbf{r}_1 = \mathbf{w}_1$	p. 1225: $\text{HighBits}_p(\mathbf{w} - \lceil cs_2 \rceil + \nu, 2\bar{\gamma}_2) := \mathbf{r}_1 = \mathbf{w}_1$
p. 1226, Fig. 8, line 17: $\nu := \lceil \xi_1 - \xi_2 \rceil$	p. 1225, Fig. 6, line 17: $\nu := \lceil \xi_2 - \xi_1 \rceil$
p. 1226, Fig. 8, line 18: $(\mathbf{r}_1, \mathbf{r}_0) := \text{Decompose}_p(\mathbf{w} - \lceil cs_2 \rceil - \nu, 2\bar{\gamma}_2)$	p. 1225, Fig. 6, line 18: $(\mathbf{r}_1, \mathbf{r}_0) := \text{Decompose}_p(\mathbf{w} - \lceil cs_2 \rceil + \nu, 2\bar{\gamma}_2)$
p. 1226, Fig. 8, line 20: $\mathbf{h} := \text{MakeHint}_p(-c\mathbf{t}_0, \mathbf{w} - \lceil cs_2 \rceil - \nu + c\mathbf{t}_0, 2\bar{\gamma}_2)$	p. 1225, Fig. 6, line 20: $\mathbf{h} := \text{MakeHint}_p(-c\mathbf{t}_0, \mathbf{w} - \lceil cs_2 \rceil + \nu + c\mathbf{t}_0, 2\bar{\gamma}_2)$
p. 1226: $\mathbf{r}_1 := \text{HighBits}_p(\mathbf{w} - \lceil cs_2 \rceil - \nu, 2\bar{\gamma}_2) = \text{HighBits}_p(\mathbf{w}, 2\bar{\gamma}_2) := \mathbf{w}_1$	p. 1226: $\mathbf{r}_1 := \text{HighBits}_p(\mathbf{w} - \lceil cs_2 \rceil + \nu, 2\bar{\gamma}_2) = \text{HighBits}_p(\mathbf{w}, 2\bar{\gamma}_2) := \mathbf{w}_1$
p. 1226: $\  \lceil cs_2 \rceil + \nu \ _\infty$	p. 1226: $\  \lceil cs_2 \rceil - \nu \ _\infty$
p. 1227: $\mathbf{h} = \llbracket \text{HighBits}_p(\mathbf{w} - \lceil cs_2 \rceil - \nu + c\mathbf{t}_0, 2\bar{\gamma}_2) \neq \text{HighBits}_p(\mathbf{w} - \lceil cs_2 \rceil - \nu, 2\bar{\gamma}_2) \rrbracket$	p. 1227: $\mathbf{h} = \llbracket \text{HighBits}_p(\mathbf{w} - \lceil cs_2 \rceil + \nu + c\mathbf{t}_0, 2\bar{\gamma}_2) \neq \text{HighBits}_p(\mathbf{w} - \lceil cs_2 \rceil + \nu, 2\bar{\gamma}_2) \rrbracket$
p. 1229, Fig. 9, line 9: $\nu := \lceil \xi_1 - \xi_2 \rceil$	p. 1229, Fig. 9, line 9: $\nu := \lceil \xi_2 - \xi_1 \rceil$
p. 1229, Fig. 9, line 11: $\  \text{LowBits}_p(\mathbf{w} - \lceil cs_2 \rceil - \nu, 2\bar{\gamma}_2) \ _\infty \geq \bar{\gamma}_2 - \beta_2$	p. 1229, Fig. 9, line 11: $\  \text{LowBits}_p(\mathbf{w} - \lceil cs_2 \rceil + \nu, 2\bar{\gamma}_2) \ _\infty \geq \bar{\gamma}_2 - \beta_2$
p. 1229, Fig. 9, line 12: $\mathbf{h} := \text{MakeHint}_p(-c\mathbf{t}_0, \mathbf{w} - \lceil cs_2 \rceil - \nu + c\mathbf{t}_0, 2\bar{\gamma}_2)$	p. 1229, Fig. 9, line 12: $\mathbf{h} := \text{MakeHint}_p(-c\mathbf{t}_0, \mathbf{w} - \lceil cs_2 \rceil + \nu + c\mathbf{t}_0, 2\bar{\gamma}_2)$
p. 1229 $\left\lceil \frac{p}{q} \mathbf{A} \mathbf{z} \right\rceil - c\mathbf{t} = \mathbf{w} - \lceil cs_2 \rceil - \nu$	p. 1229 $\left\lceil \frac{p}{q} \mathbf{A} \mathbf{z} \right\rceil - c\mathbf{t} = \mathbf{w} - \lceil cs_2 \rceil + \nu$
p. 1229 and $\nu := \lceil \xi_1 - \xi_2 \rceil$ .	p. 1229 $\xi_3 := \lceil \frac{p}{q} \mathbf{A}(\mathbf{z} - \mathbf{z}') \rceil - \frac{p}{q} \mathbf{A}(\mathbf{z} - \mathbf{z}')$ , and $\nu := \lceil \xi_1 - \xi_2 - \xi_3 \rceil$ .