sensors

MDPI

Correction

Correction: Witanto et al. Distributed Data Integrity Verification Scheme in Multi-Cloud Environment. *Sensors* 2023, 23, 1623

Elizabeth Nathania Witanto, Brian Stanley and Sang-Gon Lee *

College of Software Convergence, Dongseo University, Busan 47011, Republic of Korea
* Correspondence: nok60@dongseo.ac.kr

The authors make the following corrections to the published paper [1].

The errors appeared in the text because of the explanation in the following.

The original Equation (7):

$$\begin{aligned} e(\delta_k, \omega_k) &= e(\sum_{i\in I} r_i(H(m_i)P + P_{pub}), \sum_{i\in I} r_i Sign_i) \\ &= e(\sum_{i\in I} r_i(H(m_i)+x)P, \sum_{i\in I} r_i(H(m_i)+x)^{-1}P) \\ &= e(P,P)^{\sum_{i\in I} r_i(H(m_i)+x)\cdot\sum_{i\in I} r_i(H(m_i)+x)^{-1}} \\ &= e(P,P) \end{aligned} \tag{7}$$

is complex; thus, the authors made a mistake. The authors misunderstood that the exponential on the 3rd line could be canceled. Then, the authors discovered that the 3rd line of Equation (7) could not be canceled because the authors used a summation. Therefore, the authors have changed it to multiplication instead.

However, this mistake affects Equations (3), (4), (6), (8), and (9), which are strongly related to Equation (7). It also affects explanations in other paragraphs related to computational cost and experiments using our equations. The details of the changes are written in the following.

Changes to Section 5. Proposed Scheme

In Equation (3),

$$\delta_k = \sum_{i\in I} r_i(H(m_i)P + P_{pub}) \tag{3}$$

should be changed to

$$\delta_k = \prod_{i\in I} r_i(H(m_i)P + P_{pub}) \tag{3}$$

In Equation (4),

$$\omega_k = \sum_{i\in I} r_i Sign_i \tag{4}$$

should be changed to

$$\omega_k = \prod_{i\in I} Sign_i {r_i}^{-1} \tag{4}$$

In Equation (6),

$$e(\sum_{k\in K} \delta_k, \sum_{k\in K} \omega_k) = e(P,P) \tag{6}$$

should be changed to

$$e(\prod_{k\in K} \delta_k, \prod_{k\in K} \omega_k) = e(P,P) \tag{6}$$

check for updates

Citation: Witanto, E.N.; Stanley, B.; Lee, S.-G. Correction: Witanto et al. Distributed Data Integrity Verification Scheme in Multi-Cloud Environment. *Sensors* 2023, *23*, 1623. *Sensors* **2023**, *23*, 5566. https://doi.org/10.3390/s23125566

Received: 10 May 2023
Accepted: 22 May 2023
Published: 14 June 2023

Changes to Section 6.1. Correctness

In Equation (7),

$$\begin{aligned} e(\delta_k, \omega_k) &= e(\sum_{i \in I} r_i(H(m_i)P + P_{pub}), \sum_{i \in I} r_i Sign_i) \\ &= e(\sum_{i \in I} r_i(H(m_i) + x)P, \sum_{i \in I} r_i(H(m_i) + x)^{-1}P) \\ &= e(P, P)^{\sum_{i \in I} r_i(H(m_i)+x) \cdot \sum_{i \in I} r_i(H(m_i)+x)^{-1}} \\ &= e(P, P) \end{aligned} \tag{7}$$

should be changed to

$$\begin{aligned} e(\delta_k, \omega_k) &= e(\prod_{i \in I} r_i(H(m_i)P + P_{pub}), \prod_{i \in I} Sign_i {r_i}^{-1}) \\ &= e(\prod_{i \in I} r_i(H(m_i) + x)P, \prod_{i \in I} (r_i(H(m_i) + x))^{-1}P) \\ &= e(P, P)^{\prod_{i \in I} r_i(H(m_i)+x) \cdot \prod_{i \in I} (r_i(H(m_i)+x))^{-1}} \\ &= e(P, P) \end{aligned} \tag{7}$$

In Equation (8),

$$\begin{aligned} e(\sum_{k \in K} \delta_k, \sum_{k \in K} \omega_k) &= e(\sum_{k \in K} \sum_{i \in I} r_{ki}(H(m_{ki})P + P_{pub}), \sum_{k \in K} \sum_{i \in I} r_{ki} Sign_{ki}) \\ &= e(\sum_{k \in K} \sum_{i \in I} r_{ki}(H(m_{ki}) + x)P, \sum_{k \in K} \sum_{i \in I} r_{ki}(H(m_{ki}) + x)^{-1}P) \\ &= e(P, P)^{\sum_{k \in K} \sum_{i \in I} r_{ki}(H(m_{ki})+x) \cdot \sum_{k \in K} \sum_{i \in I} r_{ki}(H(m_{ki})+x)^{-1}} \\ &= e(P, P) \end{aligned} \tag{8}$$

should be changed to

$$\begin{aligned} e(\prod_{k \in K} \delta_k, \prod_{k \in K} \omega_k) &= e(\prod_{k \in K} \prod_{i \in I} r_{ki}(H(m_{ki})P + P_{pub}), \prod_{k \in K} \prod_{i \in I} Sign_{ki} {r_{ki}}^{-1}) \\ &= e(\prod_{k \in K} \prod_{i \in I} r_{ki}(H(m_{ki}) + x)P, \prod_{k \in K} \prod_{i \in I} (r_{ki}(H(m_{ki}) + x))^{-1}P) \\ &= e(P, P)^{\prod_{k \in K} \prod_{i \in I} r_{ki}(H(m_{ki})+x) \cdot \prod_{k \in K} \prod_{i \in I} (r_{ki}(H(m_{ki})+x))^{-1}} \\ &= e(P, P) \end{aligned} \tag{8}$$

Changes to Section 6.2. Unforgeability

In Equation (9),

$$\delta' = \sum_{i \in I, i \neq j} r_i H(m_i)P + r_j H(m_b)P \tag{9}$$

should be changed to

$$\delta' = \prod_{i \in I, i \neq j} r_i H(m_i)P + r_j H(m_b)P \tag{9}$$

Changes to Section 7.1. Computation Cost

In paragraph 1, the sentence "The cost of the CSP is $(c \times (2Mul + Add + Hash)) + SIGN + 2VER$ with the bracket showing the cost for generating proof δ, while the cost of the verifier is $((c \times Mul) + (c \times P)) + 2SIGN + 2VER$ with the bracket showing the cost for generating proof ω and bilinear pairing of proofs δ, ω in the verification process. The last is the cost of CO, $((t \times Add) + P) + 3SIGN + 3VER$ with the bracket showing the cost for the batch verification process." should be changed to:

"The cost of the CSP is $(c \times (3Mul + Add + Hash)) + SIGN + 2VER$ with the bracket showing the cost for generating proof δ, while the cost of the verifier is

$((c \times Mul \times Inv) + (c \times P)) + 2SIGN + 2VER$ with the bracket showing the cost for generating proof ω and bilinear pairing of proofs δ, ω in the verification process. The last is the cost of CO, $((t \times Mul) + P) + 3SIGN + 3VER$, with the bracket showing the cost for the batch verification process."

Table 2 "Computation costs of each actor" was shown in the text as:

Table 2. Computation costs of each actor.

Actor	Computation Cost
User	$(n \times (Inv + Add + Mul + Hash)) + 2SIGN + VER$
CSP	$(c \times (2Mul + Add + Hash)) + SIGN + 2VER$
Verifier	$((c \times Mul) + (c \times P)) + 2SIGN + 2VER$
CO	$((t \times Add) + P) + 3SIGN + 3VER$

$c = n/a$, Inv = inverse, Add = addition, Mul = multiplication, P = bilinear pairing, $SIGN$ = digital signature, VER = verification of digital signature.

It should be changed to

Table 2. Computation costs of each actor.

Actor	Computation Cost
User	$(n \times (Inv + Add + Mul + Hash)) + 2SIGN + VER$
CSP	$(c \times (3Mul + Add + Hash)) + SIGN + 2VER$
Verifier	$((c \times Mul \times Inv) + (c \times P)) + 2SIGN + 2VER$
CO	$((t \times Mul) + P) + 3SIGN + 3VER$

$c = n/a$, Inv = inverse, Add = addition, Mul = multiplication, P = bilinear pairing, $SIGN$ = digital signature, and VER = verification of digital signature.

Changes to Section 7.3. Experiment Results

In paragraph 1, the sentence "CSP reaches time 5.6 s for generating proof δ of 2000 data blocks and the user 2.6 s for generating ZSS signature of the same amount of data blocks. CSP needs a longer time because as shown in Equation (3), it needs two multiplication operations. Different from the user that only needs one multiplication operation in Equation (2)." should be changed to:

"The CSP reaches time 5.3 s for generating proof δ of 2000 data blocks and the user 2.6 s for generating the ZSS signature of the same amount of data blocks. The CSP needs a longer time because, as shown in Equation (3), it needs three multiplication operations. Different from the user that only needs one multiplication and one inverse operation in Equation (2)."

In the original article, due to the correction to Equation (3), a change is required to Figure 5. The corrected Figure 5 appears below.

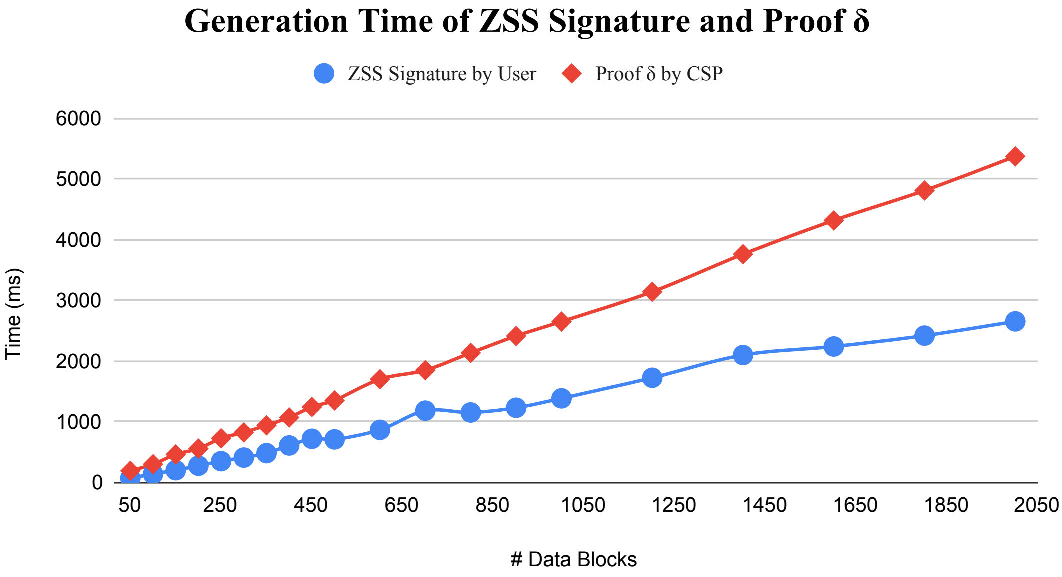

Figure 5. Generation time of Signature and Proof Delta.

In paragraph 3, the sentence "It needs 10 s to verify 2000 data blocks. However, the case of multi-verifiers (5, 10, 15, and 20 verifiers) reduces the time consumption significantly with results of 1.9 s, 1 s, 0.6 s, and 0.5 s, respectively, for the same amount of data blocks." should be changed to:

"It needs 7.3 s to verify 2000 data blocks. However, the case of multi-verifiers (5, 10, 15, and 20 verifiers) significantly reduces the time consumption with results of 1.5 s, 0.7 s, 0.5 s, and 0.4 s, respectively, for the same amount of data blocks."

In the original article, due to the correction to Equation (4), a change is required to Figure 6. The corrected Figure 6 appears below.

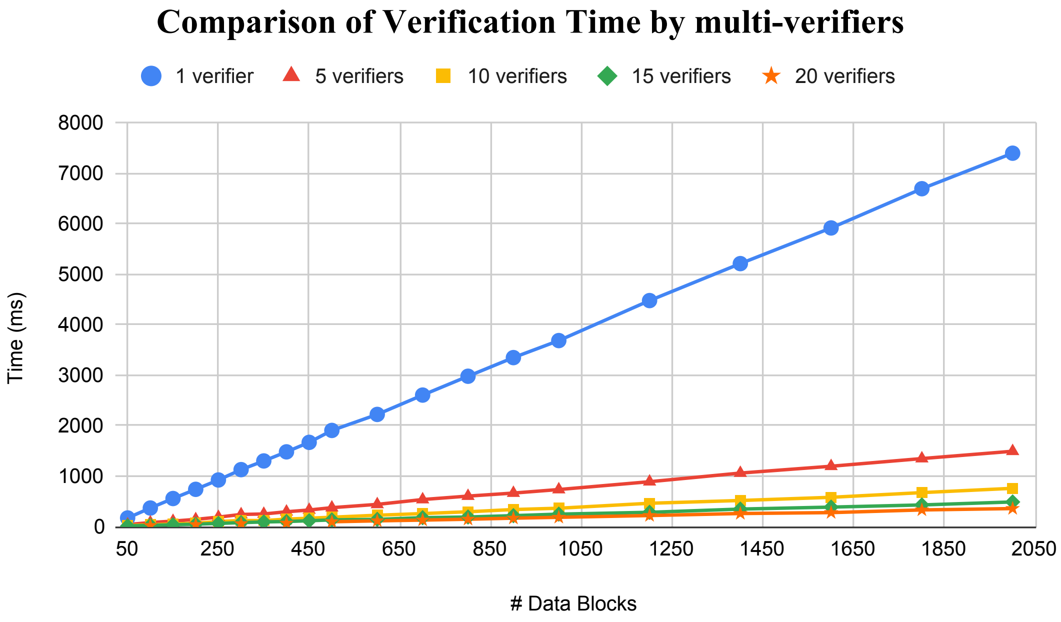

Figure 6. Comparison of verification time using multi-verifiers.

The authors apologize for any inconvenience caused and state that the scientific conclusions are unaffected. The original article has been updated.

References

1. Witanto, E.N.; Stanley, B.; Lee, S.G. Distributed Data Integrity Verification Scheme in Multi-Cloud Environment. *Sensors* **2023**, *23*, 1623. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.