A Note on "Secure and Distributed IoT Data Storage in Clouds Based on Secret Sharing and Collaborative Blockchain"

Zhengjun Cao, Lihua Liu

Abstract. We show that the data storage scheme [IEEE/ACM Trans. Netw., 2023, 31(4), 1550-1565] is flawed due to the false secret sharing protocol, which requires that some random 4×4 matrixes over the finite field F_p (a prime p) are invertible. But we find its mathematical proof for invertibility is incorrect. To fix this flaw, one needs to check the invertibility of all 35 matrixes so as to generate the proper 7 secret shares.

Keywords: Secure data storage, secret sharing, invertible matrix, determinant.

1 Introduction

Recently, Wang et al. [1] have presented a distributed internet of things (IoT) data cloud storage scheme based on secret sharing and blockchain. In the considered scenario, each node acts as a data storage node, a blockchain node, and a data retrieval server. The scheme uses a new (4, 7)-secret sharing scheme as a building block, in which a message is mapped to 7 shares, and distributed to 7 cloud nodes. Any 4 nodes or more can collaborate to recover the message. In this note, we show that the correctness of Wang et al.'s secret sharing scheme is falsely claimed. Its mathematical proof neglects the difference between the real numbers field and the finite field F_p (a prime p). We also suggest a revising method.

2 Review of the Wang et al.'s secret sharing scheme

Let p be a big prime with length ℓ, V_e be the target secret.

Share-generation. The IoT device splits V_e into four parts with an equal length less than ℓ, i.e., $V_e = x_1 \| x_2 \| x_3 \| x_4$. Randomly pick three different integers $a, b, c \in \{2, 3, \cdots, p-1\}$. Construct the 7 secret shares $s_1, s_2, \cdots, s_7$ such that

$$s_i \equiv x_1 + a^{i-1} x_2 + b^{i-1} x_3 + c^{i-1} x_4 \bmod p \tag{1}$$

Distribute the pairs (i, s_i) and the parameters a, b, c to the target 7 nodes.

Z. Cao is with Department of Mathematics, Shanghai University, China. L. Liu is with Department of Mathematics, Shanghai Maritime University, Shanghai, China. Email: liulh@shmtu.edu.cn

Retrieval. Let $s_i, s_j, s_k, s_l, 1 \le i < j < k < l \le 7$ be the pooled four shares. Solve the equations

$$\begin{pmatrix} s_i \\ s_j \\ s_k \\ s_l \end{pmatrix} = \begin{pmatrix} 1 & a^{i-1} & b^{i-1} & c^{i-1} \\ 1 & a^{j-1} & b^{j-1} & c^{j-1} \\ 1 & a^{k-1} & b^{k-1} & c^{k-1} \\ 1 & a^{l-1} & b^{l-1} & c^{l-1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \tag{2}$$

to recover x_1, x_2, x_3, x_4.

3 The false mathematical proof

In order to prove the correctness of Wang et al.'s secret sharing scheme, it suffices to show that the determinant

$$D = \begin{vmatrix} 1 & a^{i-1} & b^{i-1} & c^{i-1} \\ 1 & a^{j-1} & b^{j-1} & c^{j-1} \\ 1 & a^{k-1} & b^{k-1} & c^{k-1} \\ 1 & a^{l-1} & b^{l-1} & c^{l-1} \end{vmatrix} \neq 0 \tag{3}$$

over the finite filed F_p, not the real numbers field $\mathbb{R}$. But we find the original mathematical argument neglects the basic requirement. The defined function (page 1555, [1])

$$f(t) = \frac{\frac{t^\alpha - 1}{t-1} - \frac{\tau^\alpha - 1}{\tau - 1}}{\frac{t^\beta - 1}{t-1} - \frac{\tau^\beta - 1}{\tau - 1}}$$

where $\alpha > \beta, t > \tau$, is NOT a monotonically increasing function over F_p.

In fact, it is very difficult to mathematically prove

$$\begin{aligned} D =& \frac{1}{a^4 b^4 c^4}(a^{i+3}b^{k+3}c^{j+3} - a^{i+3}b^{j+3}c^{k+3} - a^{j+3}b^{k+3}c^{i+3} \\ &+ a^{j+3}b^{i+3}c^{k+3} + a^{k+3}b^{j+3}c^{i+3} - a^{k+3}b^{i+3}c^{j+3} \\ &- a^{i+3}b^{l+3}c^{j+3} + a^{i+3}b^{j+3}c^{l+3} + a^{j+3}b^{l+3}c^{i+3} \\ &- a^{j+3}b^{i+3}c^{l+3} - a^{l+3}b^{j+3}c^{i+3} + a^{l+3}b^{i+3}c^{j+3} \\ &+ a^{i+3}b^{l+3}c^{k+3} - a^{i+3}b^{k+3}c^{l+3} - a^{k+3}b^{l+3}c^{i+3} \\ &+ a^{k+3}b^{i+3}c^{l+3} + a^{l+3}b^{k+3}c^{i+3} - a^{l+3}b^{i+3}c^{k+3} \\ &- a^{j+3}b^{l+3}c^{k+3} + a^{j+3}b^{k+3}c^{l+3} + a^{k+3}b^{l+3}c^{j+3} \\ &- a^{k+3}b^{j+3}c^{l+3} - a^{l+3}b^{k+3}c^{j+3} + a^{l+3}b^{j+3}c^{k+3}) \\ &\not\equiv 0 \bmod p \end{aligned} \tag{4}$$

for different integers $a, b, c \in F_p \backslash \{0, 1\}$, and different indexes $i, j, k, l \in \{1, 2, \cdots, 7\}$.

4 A counter-example

Wang et al. have presented one illustrative example (see page 1555, [1]) for the new secret sharing scheme, where $p = 13, a = 2, b = 3, c = 4$. But they failed to make a thorough investigation of all 35 determinants. It is easy to check the below Mathematica code and the outputs.

```
a=2; b=3; c=4; A=Subsets[Range[7],{4}];
d=Det[{{1, a^(i-1), b^(i-1), c^(i-1)},
  {1, a^(j-1), b^(j-1), c^(j-1)},
  {1, a^(k-1), b^(k-1), c^(k-1)},
  {1, a^(u-1), b^(u-1), c^(u-1)}}];
For[s=1, s<36, s++, Clear[i,j,k,u];
 indexChoice = Normal[AssociationThread[
            {i, j, k, u}, A[[s]]]];
 v= d /. indexChoice;
 Print[indexChoice, "---", v]]

-------------------------------------

{i->1,j->2,k->3,u->4}---12
{i->1,j->2,k->3,u->5}---120
{i->1,j->2,k->3,u->6}---780
{i->1,j->2,k->3,u->7}---4200
{i->1,j->2,k->4,u->5}---420
{i->1,j->2,k->4,u->6}---3600
{i->1,j->2,k->4,u->7}---21588
{i->1,j->2,k->5,u->6}---8700
{i->1,j->2,k->5,u->7}---68880
{i->1,j->2,k->6,u->7}---143220
{i->1,j->3,k->4,u->5}---600
{i->1,j->3,k->4,u->6}---5712
{i->1,j->3,k->4,u->7}---36120
{i->1,j->3,k->5,u->6}---18120
{i->1,j->3,k->5,u->7}---151200
{i->1,j->3,k->6,u->7}---348600
{i->1,j->4,k->5,u->6}---19920
{i->1,j->4,k->5,u->7}---184800
{i->1,j->4,k->6,u->7}---560112
{i->1,j->5,k->6,u->7}---561120
{i->2,j->3,k->4,u->5}---288
{i->2,j->3,k->4,u->6}---2880
{i->2,j->3,k->4,u->7}---18720
{i->2,j->3,k->5,u->6}---10080
{i->2,j->3,k->5,u->7}---86400
{i->2,j->3,k->6,u->7}---208800
{i->2,j->4,k->5,u->6}---14400
```

```
{i->2,j->4,k->5,u->7}---137088
{i->2,j->4,k->6,u->7}---434880
{i->2,j->5,k->6,u->7}---478080
{i->3,j->4,k->5,u->6}---6912
{i->3,j->4,k->5,u->7}---69120
{i->3,j->4,k->6,u->7}---241920
{i->3,j->5,k->6,u->7}---345600
{i->4,j->5,k->6,u->7}---165888
```

Clearly, $780 \equiv 0 \bmod 13$, $18720 \equiv 0 \bmod 13$. We conclude that the shares $\{s_1, s_2, s_3, s_6\}$ and $\{s_2, s_3, s_4, s_7\}$ cannot be used to recover the original secret.

5 A revision

Notice that the modulus p is a public system parameter. To retrieve the original secret, there are 35 matrixes for the $(4, 7)$ secret sharing scheme once the three integers a, b, c are chosen. So, the exhaustive calculation is more suitable for the case, unlike the usual Shamir's secret sharing [2]. The new share-generation can be described as follows.

Share-generation. The IoT device splits V_e into four parts with an equal length less than ℓ, i.e., $V_e = x_1 \| x_2 \| x_3 \| x_4$. Randomly pick different integers $a, b, c \in \{2, 3, \cdots, p-1\}$. For all 35 tuples $(i, j, k, l), 1 \le i < j < k < l \le 7$, compute the determinants

$$\begin{vmatrix} 1 & a^{i-1} & b^{i-1} & c^{i-1} \\ 1 & a^{j-1} & b^{j-1} & c^{j-1} \\ 1 & a^{k-1} & b^{k-1} & c^{k-1} \\ 1 & a^{l-1} & b^{l-1} & c^{l-1} \end{vmatrix}$$

and check that they are not divisible by the prime p. Otherwise, rechoose integers a, b, c until all 35 determinants are not divisible by p. Then construct the 7 secret shares $s_1, s_2, \cdots, s_7$ such that $s_i \equiv x_1 + a^{i-1}x_2 + b^{i-1}x_3 + c^{i-1}x_4 \bmod p$, and distribute the shares to 7 nodes.

6 Conclusion

We show that the Wang et al.'s data storage scheme should be revised owing to its flawed share-generation mechanism. We hope the findings in this note could be helpful for the future work on designing such schemes.

References

[1] N. Wang, et al., "Secure and Distributed IoT Data Storage in Clouds Based on Secret Sharing and Collaborative Blockchain", *IEEE/ACM Trans. Netw.*, vol. 31, no. 4, pp. 1550-1565, 2023.

[2] A. Shamir, "How to Share a Secret," *Commun. ACM*, vol. 22, no. 11, pp. 612-613, 1979.