This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2023.3327304

Errata for "Theory of Communication Efficient Quantum Secret Sharing"

Kaushik Senthoor and Pradeep Kiran Sarvepalli

***Abstract*—Here we give the errata for the paper "Theory of Communication Efficient Quantum Secret Sharing" [1]. As one of the results in this paper, we proposed a construction for universal CE-QTS schemes. However, we recently found an error in this construction. We found that the Vandermonde matrix used for the encoding in this construction leads to a failure in secret recovery. Here we shortly describe why this error occurs and provide a rectification. By replacing the Vandermonde matrix with a Cauchy matrix, the secret recovery in the construction goes through. However, the construction now needs a higher field size. With this rectification, the construction is now correct. The remaining results in the paper remain unaffected.**

In [1, Section V], we gave a construction for $((k, n = 2k-1, *))$ universal CE-QTS schemes based on Staircase codes. For the encoding in this construction, we used an $n \times n$ Vandermonde matrix V given by $[V]_{ij} = x_i^{j-1}$ where $x_1, x_2, \ldots, x_n$ are distinct non-zero constants from $\mathbb{F}_q$ with $q > n$. The secret recovery in this construction involves quantum operations using submatrices of V. Particularly, the matrix W_ℓ in the proof of [1, Lemma 9] is defined as

$$W_\ell = [\, {V_D}^{[\ell,2k-1]^t} \ \underline{w}_{\ell,k+1} \ \underline{w}_{\ell,k+2} \cdots \underline{w}_{\ell,k+i-\ell} \,]^t \tag{E1}$$

for $1 \le \ell \le i-1$ and $1 \le i \le k$. Here $\underline{w}_{\ell,j}$ is a column vector of length $(2k-\ell)$ with one in the jth position and zeros elsewhere. The term V_A^B denotes the submatrix of V with rows given by A and columns given by B. The matrix W_ℓ is a $(2k-\ell) \times (2k-\ell)$ square matrix which can also be written as

$$W_\ell = \left[\begin{array}{c|c|c} V_D^{[\ell,\ell+k-1]} & V_D^{[\ell+k,k+i-1]} & V_D^{[k+i,2k-1]} \\ \hline \mathbf{0}_{(i-\ell)\times k} & I_{(i-\ell)\times(i-\ell)} & \mathbf{0}_{(i-\ell)\times(k-i)} \end{array}\right]. \tag{E2}$$

A. Error

In the proof of [1, Lemma 9] (in page 3177 left column, line 44), it is mentioned that W_ℓ is a full-rank matrix (which is invertible). However, this is not true. The matrix W_ℓ is full rank if and only if the $(2k-i) \times (2k-i)$ square matrix

$$V_D^{[\ell,\ell+k-1] \cup [k+i,2k-1]} \tag{E3}$$

is full rank. However, $V_D^{[\ell,\ell+k-1] \cup [k+i,2k-1]}$ is a submatrix of the Vandermonde matrix V which is not always full rank [2, Chapter 11, Problem 7(a)].

This work was supported by the Department of Science and Technology, Govt. of India, under grant number DST/ICPS/QuST/Theme-3/2019/Q59 and the Mphasis Center for Quantum Information, Communication, and Computing (CQuICC).

The authors are with the Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai 600036, India (email: ee15d042@ee.iitm.ac.in; pradeep@ee.iitm.ac.in).

B. Rectification

This error can be rectified by choosing V to be a Cauchy matrix. In a Cauchy matrix, any square submatrix is of full rank [2, Chapter 11, Problem 7(b)]. This will ensure that the matrix W_ℓ as defined in Eq. (E1) always has full rank. Note that to obtain an $n \times n$ Cauchy matrix with entries from $\mathbb{F}_q$, we need a higher field size of $q \ge 2n$.

C. Text affected

Changing the Vandermonde matrix to Cauchy matrix in the construction needs some minor corrections at the following places in [1].

- Table I
- Example universal CE-QTS scheme given in Section III-A (and later described further in Appendix B)
- Construction for universal CE-QTS schemes in Section V.

The result in these sections hold true after changing the Vandermonde matrix to Cauchy matrix in the encoding. The results in the remaining sections of the paper remain unaffected.

D. Corrections to the original text

We give below the list of corrections to be made in the original text of [1]. These corrections are now made in the latest arXiv version [3] of the paper.

1) In page 3166, in fifth row and last column of Table I, "$q > 2k-1$" should be changed to "$q \ge 2(2k-1)$".
2) In page 3169 from Section III-A,
   - in right column, line 21, change "$q = 7$" to "$q = 11$"
   - wherever "$\mathbb{F}_7$" occurs, it should be changed to "$\mathbb{F}_{11}$"
   - in right column, line 34, replace the matrix
   $$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 1 & 2 \\ 1 & 3 & 2 & 6 & 4 \\ 1 & 4 & 2 & 1 & 4 \\ 1 & 5 & 4 & 6 & 2 \end{bmatrix} \text{ with } \begin{bmatrix} 9 & 3 & 4 & 6 & 1 \\ 2 & 9 & 3 & 4 & 6 \\ 8 & 2 & 9 & 3 & 4 \\ 7 & 8 & 2 & 9 & 3 \\ 5 & 7 & 8 & 2 & 9 \end{bmatrix}$$
   - in right column, line 37, replace the text "Here $v_i()$ indicates the polynomial evaluation given by
   $$v_i(f_1, f_2, f_3, f_4, f_5) = f_1 + f_2.x_i + f_3.x_i^2 + f_4.x_i^3 + f_5.x_i^4$$
   and the expression $v_i(\underline{s}, r_1, r_2)$ denotes $v_i(s_1, s_2, s_3, r_1, r_2)$. Here, we have taken $x_i = i$ for $1 \le i \le 5$." with "Here $v_i()$ indicates the expression
   $$v_i(f_1, f_2, f_3, f_4, f_5) = v_{i1} f_1 + v_{i2} f_2 + \ldots + v_{i5} f_5$$

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2023.3327304

where $v_{ij} = [V]_{ij}$ and the expression $v_i(\underline{s}, r_1, r_2)$ denotes $v_i(s_1, s_2, s_3, r_1, r_2)$. The matrix V is a Cauchy matrix."

3) In page 3170 from Section III-A,
   - wherever "$\mathbb{F}_7$" occurs, it should be changed to "$\mathbb{F}_{11}$".
   - in left column, line 24, replace the text "Then, on applying the operators $L_6 |r_2\rangle |v_1(\underline{s}, r_1, r_2)\rangle$, $L_5 |r_2\rangle |v_2(\underline{s}, r_1, r_2)\rangle$, $L_3 |r_2\rangle |v_3(\underline{s}, r_1, r_2)\rangle$ and $L_3 |r_2\rangle |v_4(\underline{s}, r_1, r_2)\rangle$, ..." with "Then, on applying the operators $L_{10} |r_2\rangle |v_1(\underline{s}, r_1, r_2)\rangle$, $L_5 |r_2\rangle |v_2(\underline{s}, r_1, r_2)\rangle$, $L_7 |r_2\rangle |v_3(\underline{s}, r_1, r_2)\rangle$ and $L_8 |r_2\rangle |v_4(\underline{s}, r_1, r_2)\rangle$, ..."
4) In page 3175, in right column, line 39, "$q > 2k - 1$" should be changed to "$q \geq 2(2k - 1)$".
5) In page 3176,
   - in left column, line 11, replace the text "...V is a $n \times n$ Vandermonde matrix given by

$$V = \begin{bmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ 1 & x_2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \dots & x_n^{n-1} \end{bmatrix}. \quad (26)$$

     where $x_1, x_2, \dots, x_n$ are distinct non-zero constants from $\mathbb{F}_q$." with "...V is an $n \times n$ Cauchy matrix given by

$$[V]_{ij} = \frac{1}{x_i - y_j} \quad (26)$$

     where $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n$ are distinct constants from $\mathbb{F}_q$."
   - in left column, line 24, change "$q = 7$" to "$q = 11$"
   - in right column, line 2, replace the matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 1 & 2 \\ 1 & 3 & 2 & 6 & 4 \\ 1 & 4 & 2 & 1 & 4 \\ 1 & 5 & 4 & 6 & 2 \end{bmatrix} \text{ with } \begin{bmatrix} 9 & 3 & 4 & 6 & 1 \\ 2 & 9 & 3 & 4 & 6 \\ 8 & 2 & 9 & 3 & 4 \\ 7 & 8 & 2 & 9 & 3 \\ 5 & 7 & 8 & 2 & 9 \end{bmatrix}$$

   - in right column, after line 2, insert the sentence "Here V is a Cauchy matrix as defined in (26) with $y_1 = 0$, $y_2 = 1$, $y_3 = 2$, $y_4 = 3$, $y_5 = 4$, $x_1 = 5$, $x_2 = 6$, $x_3 = 7$, $x_4 = 8$, $x_5 = 9$."
6) In page 3177, in the proof of Lemma 9, wherever the phrase "Vandermonde matrix" appears, it should be changed into "Cauchy matrix".
7) In page 3178, the expression "$q > 2k-1$" in the statement of Theorem 3 should be changed to "$q \geq 2(2k - 1)$". Theorem 3 should now read as

   Theorem 3 (*Staircase construction for universal CE-QTS*). The encoding given in (27) gives a $((k, n = 2k - 1, *))$ universal CE-QTS scheme with the following parameters.

$$q \geq 2(2k - 1) \text{ (prime)}$$
$$m = \text{lcm}\{1, 2, \dots, k\}$$
$$w_1 = w_2 = \dots = w_n = m$$
$$\text{CC}_n(d) = \frac{dm}{d - k + 1} \text{ for } d \in \{k, k + 1, \dots, 2k - 1\}$$

8) In page 3178, left column last line, replace the sentence "Though the scheme based on Staircase codes gives a better bound on the dimension of the qudits, the concatenated construction could give a smaller secret size for $n < 2k - 1$." with "However, the concatenated construction could give a smaller secret size for $n < 2k - 1$."
9) In page 3184 from Appendix B,
   - in right column, line 16, change "$q = 7$" to "$q = 11$"
   - in right column, lines 22 and 31, change "$\mathbb{F}_7$" to "$\mathbb{F}_{11}$"
   - in right column, line 34, replace the matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 1 & 2 \\ 1 & 3 & 2 & 6 & 4 \\ 1 & 4 & 2 & 1 & 4 \\ 1 & 5 & 4 & 6 & 2 \end{bmatrix} \text{ with } \begin{bmatrix} 9 & 3 & 4 & 6 & 1 \\ 2 & 9 & 3 & 4 & 6 \\ 8 & 2 & 9 & 3 & 4 \\ 7 & 8 & 2 & 9 & 3 \\ 5 & 7 & 8 & 2 & 9 \end{bmatrix}$$

   - in right column, line 32, replace the text "$v_i()$ indicates the polynomial evaluation given by

$$v_i(f_1, f_2, f_3, f_4, f_5) = f_1 + f_2.x_i + f_3.x_i^2 + f_4.x_i^3 + f_5.x_i^4$$

     and the expression $v_i(\underline{s}, r_1, r_2)$ denotes $v_i(s_1, s_2, s_3, r_1, r_2)$. Here, we have taken $x_i = i$ for $1 \leq i \leq 5$." with "$v_i()$ indicates the expression

$$v_i(f_1, f_2, f_3, f_4, f_5) = v_{i1} f_1 + v_{i2} f_2 + \dots + v_{i5} f_5$$

     where $v_{ij} = [V]_{ij}$ and the expression $v_i(\underline{s}, r_1, r_2)$ denotes $v_i(s_1, s_2, s_3, r_1, r_2)$. The matrix V is a Cauchy matrix."
10) In page 3185 from Appendix B,
    - wherever "$\mathbb{F}_7$" occurs, it should be changed to "$\mathbb{F}_{11}$".
    - in left column, line 24, replace the text "Then, on applying the operators $L_6 |r_3\rangle |v_1(0,r_1,r_2,r_3,r_4)\rangle$, $L_6 |r_3\rangle |v_2(0,r_1,r_2,r_3,r_4)\rangle$ and $L_1 |r_3\rangle |v_3(0, r_1, r_2, r_3, r_4)\rangle$, ..." with "Then, on applying the operators $L_5 |r_3\rangle |v_1(0,r_1,r_2,r_3,r_4)\rangle$, $L_7 |r_3\rangle |v_2(0,r_1,r_2,r_3,r_4)\rangle$ and $L_8 |r_3\rangle |v_3(0, r_1, r_2, r_3, r_4)\rangle$, ..."

We earlier presented the results on universal CE-QTS schemes from [1] in a conference [4]. A revised version of [4] including the above corrections is available in [5].

REFERENCES

[1] K. Senthoor and P. K. Sarvepalli, "Theory of communication efficient quantum secret sharing," *IEEE Trans. Inform. Theory*, vol. 68, no. 5, pp. 3164–3186, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9674910

[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Elsevier, 1977, vol. 16.

[3] K. Senthoor and P. K. Sarvepalli, "Theory of communication efficient quantum secret sharing," *e-print quant-ph/2101.12419*, 2020. [Online]. Available: https://arxiv.org/abs/2101.12419

[4] ——, "Universal communication efficient quantum threshold secret sharing schemes," in *Proc. 2020 IEEE Information Theory Workshop (ITW), Riva del Garda, Italy*, 2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9457576

[5] ——, "Universal communication efficient quantum threshold secret sharing," *e-print quant-ph/2002.09229*, 2020. [Online]. Available: https://arxiv.org/abs/2002.09229

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2023.3327304

Kaushik Senthoor graduated with a PhD in Electrical Engineering from the Indian Institute of Technology Madras, India in July 2023. He has a Masters degree from the Indian Institute of Science, Bangalore in Telecommunication Engineering and a Bachelors degree from Amrita School of Engineering, Coimbatore in Electronics and Communication Engineering. After finishing his Masters degree, he worked as an Engineer in Ittiam Systems, Bangalore. He will be joining Delft University of Technology, Netherlands as a postdoctoral researcher in November 2023. His research interests include classical and quantum error control codes, information theory, distributed storage and signal processing.

Pradeep Kiran Sarvepalli is an Associate Professor at the Indian Institute of Technology Madras. He graduated with a PhD in Computer Science from Texas A&M University. He also holds a Masters degree in Electrical Engineering from Texas A&M University and a B.Tech. degree in Electrical Engineering from Indian Institute of Technology Madras. He held Postdoctoral Fellowships in the University of British Columbia and Georgia Institute of Technology. He also worked as an IC Design Engineer in Texas Instruments India, Bangalore. His research interests are quantum and classical error correcting codes, quantum cryptography, quantum computation, and distributed storage.