

# Chih-Lun Tsai

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/4313477/publications.pdf>

Version: 2024-02-01

116  
papers

3,770  
citations

117625

34  
h-index

138484

58  
g-index

119  
all docs

119  
docs citations

119  
times ranked

1622  
citing authors

#	ARTICLE	IF	CITATIONS
1	Collusion Attack and Counterattack on the Quantum Key Agreement Via Non-maximally Entangled Cluster States. International Journal of Theoretical Physics, 2021, 60, 331-337.	1.2	1
2	Measure-resend authenticated semi-quantum key distribution with single photons. Quantum Information Processing, 2021, 20, 1.	2.2	5
3	On the Controlled Cyclic Quantum Teleportation of an Arbitrary Two-Qubit Entangled State by Using a Ten-Qubit Entangled State. International Journal of Theoretical Physics, 2020, 59, 200-205.	1.2	25
4	Collective Attack and Improvement on "Mediated Semi-Quantum Key Distribution Using Single Photons". Annalen Der Physik, 2020, 532, 1900493.	2.4	5
5	Efficient semi-quantum private comparison using single photons. Quantum Information Processing, 2019, 18, 1.	2.2	49
6	Improvement on "Cryptanalysis and Improvement of a Multiparty Quantum Direct Secret Sharing of Classical Messages with Bell States and Bell Measurements"™. International Journal of Theoretical Physics, 2019, 58, 2341-2345.	1.2	1
7	Improving the Security of "High-Capacity Quantum Summation with Single Photons in both Polarization and Spatial-Mode Degrees of Freedom"™. International Journal of Theoretical Physics, 2019, 58, 2213-2217.	1.2	10
8	Mediated Semi-Quantum Key Distribution Using Single Photons. Annalen Der Physik, 2019, 531, 1800347.	2.4	26
9	Double CNOT attack on "Quantum key distribution with limited classical Bob". International Journal of Quantum Information, 2019, 17, 1975001.	1.1	8
10	Mediated Semi-Quantum Key Distribution Without Invoking Quantum Measurement. Annalen Der Physik, 2018, 530, 1700206.	2.4	47
11	Statistics attack on "quantum private comparison with a malicious third party"™ and its improvement. Quantum Information Processing, 2018, 17, 1.	2.2	5
12	An Improved Protocol for Controlled Deterministic Secure Quantum Communication Using Five-Qubit Entangled State. International Journal of Theoretical Physics, 2018, 57, 1894-1902.	1.2	0
13	Secure Quantum Communication Scheme for Six-Qubit Decoherence-Free States. International Journal of Theoretical Physics, 2018, 57, 3808-3818.	1.2	2
14	Six-Qubit Decoherence-Free State Measurement Method and its Application to Development of Authenticated Quantum Secure Direct Communication Protocol. International Journal of Theoretical Physics, 2018, 57, 2513-2522.	1.2	3
15	Semi-quantum Key Distribution Robust Against Combined Collective Noise. International Journal of Theoretical Physics, 2018, 57, 3410-3418.	1.2	15
16	Double C-NOT attack and counterattack on "Three-step semi-quantum secure direct communication protocol"™. Quantum Information Processing, 2018, 17, 1.	2.2	34
17	IA-CTR: Integrity-Aware Conventional Counter Mode for Secure and Efficient Communication in Wireless Sensor Networks. Wireless Personal Communications, 2017, 94, 467-479.	2.7	2
18	On "A new quantum blind signature with unlinkability". Quantum Information Processing, 2017, 16, 1.	2.2	9

#	ARTICLE	IF	CITATIONS
19	Controlled quantum dialogue using cluster states. Quantum Information Processing, 2017, 16, 1.	2.2	32
20	Comment on "A practical protocol for three-party authenticated quantum key distribution". Quantum Information Processing, 2017, 16, 1.	2.2	1
21	Multiparty quantum private comparison with almost dishonest third parties for strangers. Quantum Information Processing, 2017, 16, 1.	2.2	37
22	Improvement of "Novel Multiparty Quantum Key Agreement Protocol with GHZ States". International Journal of Theoretical Physics, 2017, 56, 3108-3116.	1.2	26
23	Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing. Quantum Information Processing, 2017, 16, 1.	2.2	35
24	Comment on "improving the security of protocols of quantum key agreement solely using bell states and bell measurement", 2017, , .		1
25	Three-party authenticated key agreements for optimal communication. PLoS ONE, 2017, 12, e0174473.	2.5	5
26	A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. IEEE Transactions on Industrial Electronics, 2016, 63, 7124-7132.	7.9	198
27	Forward/Backward Unforgeable Digital Signature Scheme Using Symmetric-Key Crypto-System. , 2016, , .		1
28	Comment on 'Multiparty Quantum Key Agreement with GHZ State'. , 2016, , .		0
29	Quantum dialogue protocols over collective noise using entanglement of GHZ state. Quantum Information Processing, 2016, 15, 2971-2991.	2.2	25
30	Trojan Horse Attack Free Fault-Tolerant Quantum Key Distribution Protocols Using GHZ States. International Journal of Theoretical Physics, 2016, 55, 3993-4004.	1.2	12
31	Authenticated semi-quantum key distributions without classical channel. Quantum Information Processing, 2016, 15, 2881-2893.	2.2	29
32	Controlled quantum dialogue robust against conspiring users. Quantum Information Processing, 2016, 15, 4313-4324.	2.2	30
33	Fault-tolerant controlled deterministic secure quantum communication using EPR states against collective noise. Quantum Information Processing, 2016, 15, 4711-4727.	2.2	4
34	BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network. IEEE Sensors Journal, 2016, 16, 1368-1376.	4.7	519
35	PFC-CTR, PFC-OCB: Efficient stream cipher modes of authencryption. Cryptologia, 2016, 40, 285-302.	0.5	3
36	RT-OCFB: Real-Time Based Optimized Cipher Feedback Mode. Cryptologia, 2016, 40, 1-14.	0.5	5

#	ARTICLE	IF	CITATIONS
37	Quantum entanglement establishment between two strangers. Quantum Information Processing, 2016, 15, 385-403.	2.2	2
38	Multi-Party Quantum Private Comparison Protocol with an Almost-Dishonest Third Party using GHZ States. International Journal of Theoretical Physics, 2016, 55, 2969-2976.	1.2	22
39	An Efficient Quantum Private Comparison of Equality over Collective-Noise Channels. International Journal of Theoretical Physics, 2016, 55, 2125-2138.	1.2	8
40	Authenticated semi-quantum direct communication protocols using Bell states. Quantum Information Processing, 2016, 15, 947-958.	2.2	57
41	Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme With User Anonymity for Secure Communication in Global Mobility Networks. IEEE Systems Journal, 2016, 10, 1370-1379.	4.6	93
42	Enhanced Secure Mutual Authentication and Key Agreement Scheme Preserving User Anonymity in Global Mobile Networks. Wireless Personal Communications, 2015, 82, 2231-2245.	2.7	45
43	Provably secure extended chaotic map-based three-party key agreement protocols using password authentication. Nonlinear Dynamics, 2015, 82, 29-38.	5.2	12
44	Intercept-and-resend attack on controlled bidirectional quantum direct communication and its improvement. Quantum Information Processing, 2015, 14, 3515-3522.	2.2	35
45	Untraceable Sensor Movement in Distributed IoT Infrastructure. IEEE Sensors Journal, 2015, 15, 5340-5348.	4.7	76
46	Probabilistic authenticated quantum dialogue. Quantum Information Processing, 2015, 14, 4631-4650.	2.2	17
47	Multi-party quantum private comparison with an almost-dishonest third party. Quantum Information Processing, 2015, 14, 4225-4235.	2.2	37
48	Multi-controller quantum teleportation with remote rotation and its applications. Quantum Information Processing, 2015, 14, 4615-4629.	2.2	1
49	Controlled probabilistic quantum key distribution using a ground state. Quantum Information Processing, 2015, 14, 989-1003.	2.2	0
50	Authenticated Quantum Dialogue Based on Bell States. International Journal of Theoretical Physics, 2015, 54, 780-786.	1.2	19
51	Attacks and Improvement on "Quantum Direct Communication with Mutual Authentication". International Journal of Theoretical Physics, 2014, 53, 597-602.	1.2	6
52	Arbitrated quantum signature of classical messages without using authenticated classical channels. Quantum Information Processing, 2014, 13, 113-120.	2.2	12
53	Measure-and-Resend Attack and Improvement on "A Scheme to Share Information via Employing Discrete Algorithm to Quantum States". International Journal of Theoretical Physics, 2014, 53, 224-227.	1.2	3
54	Provably Secure Mutual Authentication and Key Exchange Scheme for Expeditious Mobile Communication Through Synchronously One-Time Secrets. Wireless Personal Communications, 2014, 77, 197-224.	2.7	23

#	ARTICLE	IF	CITATIONS
55	Quantum Teleportation with Remote Rotation on a GHZ State. International Journal of Theoretical Physics, 2014, 53, 1233-1238.	1.2	9
56	Quantum authentication: one-step authenticated quantum secure direct communications for off-line communicants. Quantum Information Processing, 2014, 13, 925-933.	2.2	27
57	Trojan horse attack free fault-tolerant quantum key distribution protocols. Quantum Information Processing, 2014, 13, 781-794.	2.2	9
58	CNOT extraction attack on "quantum asymmetric cryptography with symmetric keys". Science China: Physics, Mechanics and Astronomy, 2014, 57, 1001-1003.	5.1	5
59	Quantum private comparison of equality protocol without a third party. Quantum Information Processing, 2014, 13, 239-247.	2.2	34
60	Efficient quantum dialogue using single photons. Quantum Information Processing, 2014, 13, 2451-2461.	2.2	28
61	Forgery attack on one-time proxy signature and the improvement. Quantum Information Processing, 2014, 13, 2007-2016.	2.2	13
62	Comment on the "Quantum Private Comparison Protocol Based on Bell Entangled States". International Journal of Theoretical Physics, 2014, 53, 837-840.	1.2	9
63	Authenticated semi-quantum key distribution protocol using Bell states. Quantum Information Processing, 2014, 13, 1457-1465.	2.2	104
64	Controlled remote state preparation protocols via AKLT states. Quantum Information Processing, 2014, 13, 1639-1650.	2.2	41
65	Multiparty quantum remote control. Quantum Information Processing, 2013, 12, 3545-3552.	2.2	8
66	Fault tolerant authenticated quantum direct communication immune to collective noises. Quantum Information Processing, 2013, 12, 3495-3509.	2.2	6
67	Fault tolerant quantum key distributions using entanglement swapping of GHZ states over collective-noise channels. Quantum Information Processing, 2013, 12, 3207-3222.	2.2	19
68	Comment on "Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise". Quantum Information Processing, 2013, 12, 2871-2875.	2.2	5
69	Fault tolerant deterministic quantum communications using GHZ states over collective-noise channels. Quantum Information Processing, 2013, 12, 3043-3055.	2.2	18
70	Multiparty controlled quantum secure direct communication based on quantum search algorithm. Quantum Information Processing, 2013, 12, 3791-3805.	2.2	16
71	Deterministic quantum communication using the symmetric W state. Science China: Physics, Mechanics and Astronomy, 2013, 56, 1903-1908.	5.1	17
72	Modification Attack on QSDC with Authentication and the Improvement. International Journal of Theoretical Physics, 2013, 52, 2230-2234.	1.2	20

#	ARTICLE	IF	CITATIONS
73	Bell state entanglement swappings over collective noises and their applications on quantum cryptography. Quantum Information Processing, 2013, 12, 1089-1107.	2.2	22
74	Intercept-Resend Attacks on Semi-quantum Secret Sharing and the Improvements. International Journal of Theoretical Physics, 2013, 52, 156-162.	1.2	41
75	Enhancement on "quantum blind signature based on two-state vector formalism". Quantum Information Processing, 2013, 12, 109-117.	2.2	65
76	Dynamic quantum secret sharing. Quantum Information Processing, 2013, 12, 331-344.	2.2	82
77	New circular quantum secret sharing for remote agents. Quantum Information Processing, 2013, 12, 685-697.	2.2	59
78	Multi-user private comparison protocol using GHZ class states. Quantum Information Processing, 2013, 12, 1077-1088.	2.2	104
79	Quantum dialogue protocols immune to collective noise. Quantum Information Processing, 2013, 12, 2131-2142.	2.2	78
80	EFFICIENT KEY CONSTRUCTION ON SEMI-QUANTUM SECRET SHARING PROTOCOLS. International Journal of Quantum Information, 2013, 11, 1350052.	1.1	46
81	Cryptanalysis and improvement of controlled secure direct communication. Chinese Physics B, 2013, 22, 060308.	1.4	10
82	Provably secure mutual authentication and key agreement scheme with user anonymity. , 2013, , .		1
83	Improved "bidirectional quantum secure communication protocol based on a shared private Bell state"; , 2012, , .		0
84	Comment on: Supervisory Asymmetric Deterministic Secure Quantum Communication. International Journal of Theoretical Physics, 2012, 51, 3868-3875.	1.2	5
85	Improved QSDC Protocol over a Collective-Dephasing Noise Channel. International Journal of Theoretical Physics, 2012, 51, 3941-3950.	1.2	57
86	On "controlled quantum teleportation and secure direct communication"; , 2012, , .		2
87	Comment on "Security analysis and improvements of arbitrated quantum signature schemes". Physical Review A, 2012, 85, .	2.5	37
88	Multi-party quantum secret sharing based on two special entangled states. Science China: Physics, Mechanics and Astronomy, 2012, 55, 460-464.	5.1	27
89	Controlled Deterministic Secure Quantum Communication Based on Quantum Search Algorithm. International Journal of Theoretical Physics, 2012, 51, 2447-2454.	1.2	17
90	New quantum private comparison protocol using EPR pairs. Quantum Information Processing, 2012, 11, 373-384.	2.2	184

#	ARTICLE	IF	CITATIONS
91	Thwarting intercept-and-resend attack on Zhang's quantum secret sharing using collective rotation noises. Quantum Information Processing, 2012, 11, 113-122.	2.2	28
92	Improvement on "Quantum Key Agreement Protocol with Maximally Entangled States". International Journal of Theoretical Physics, 2011, 50, 1793-1802.	1.2	91
93	Comment on "Quantum Key Distribution and Quantum Authentication Based on Entangled State". International Journal of Theoretical Physics, 2011, 50, 2703-2707.	1.2	15
94	Revisiting Deng et al.'s Multiparty Quantum Secret Sharing Protocol. International Journal of Theoretical Physics, 2011, 50, 2790-2798.	1.2	19
95	Fault tolerant two-step quantum secure direct communication protocol against collective noises. Science China: Physics, Mechanics and Astronomy, 2011, 54, 496-501.	5.1	78
96	On "a simple three-party password-based key exchange protocol". International Journal of Communication Systems, 2011, 24, 1520-1532.	2.5	13
97	New arbitrated quantum signature of classical messages against collective amplitude damping noise. Optics Communications, 2011, 284, 3144-3148.	2.1	12
98	The enhancement of three-party simultaneous quantum secure direct communication scheme with EPR pairs. Optics Communications, 2011, 284, 515-518.	2.1	41
99	Intercept-resend attacks on Chen et al.'s quantum private comparison protocol and the improvements. Optics Communications, 2011, 284, 2412-2414.	2.1	72
100	On "multiparty quantum secret sharing with Bell states and Bell measurements". Optics Communications, 2010, 283, 4405-4407.	2.1	13
101	Teleportation of a Pure EPR State via GHZ-like State. International Journal of Theoretical Physics, 2010, 49, 1969-1975.	1.2	59
102	Quantum key agreement protocol based on BB84. Optics Communications, 2010, 283, 1192-1195.	2.1	177
103	Simple password-based three-party authenticated key exchange without server public keys. Information Sciences, 2010, 180, 1702-1714.	6.9	39
104	THE ENHANCEMENT OF ZHOU <i>et al.</i> 's QUANTUM SECRET SHARING PROTOCOL. International Journal of Modern Physics C, 2009, 20, 1531-1535.	1.7	43
105	New Efficient Three-Party Quantum Key Distribution Protocols. IEEE Journal of Selected Topics in Quantum Electronics, 2009, 15, 1602-1606.	2.9	53
106	Enhanced delegation-based authentication protocol for PCSs. IEEE Transactions on Wireless Communications, 2009, 8, 2166-2171.	9.2	24
107	SECURITY OF "ASYMMETRICAL QUANTUM KEY DISTRIBUTION PROTOCOL". International Journal of Modern Physics C, 2007, 18, 157-161.	1.7	3
108	Comment on "Quantum secret sharing between multiparty and multiparty without entanglement". Physical Review A, 2006, 73, .	2.5	28

#	ARTICLE	IF	CITATIONS
109	Private Authentication Techniques for the Global Mobility Network. Wireless Personal Communications, 2005, 35, 329-336.	2.7	15
110	Security of park-lim key agreement schemes for vsat satellite communications. IEEE Transactions on Vehicular Technology, 2003, 52, 465-468.	6.3	3
111	Security analysis of the generalized key agreement and password authentication protocol. IEEE Communications Letters, 2001, 5, 462-463.	4.1	11
112	Privacy and non-repudiation on pay-TV systems. IEEE Transactions on Consumer Electronics, 2000, 46, 20-27.	3.6	24
113	On the security of Park et al.'s key distribution protocol for digital mobile communications. , 0, , .		1
114	(t+1,n) threshold and generalized DSS signatures without a trusted party. , 0, , .		1
115	Anonymous Proof of Membership with Ring Signature. , 0, , .		1
116	Network Security. , 0, , 509-585.		1