Quantum Private Broadcasting


A. Broadbent, C. González-Guillén

arXiv:2107.11474

Private Broadcasting

Proposed Solutions

Quantum Private Broadcasting

Comparison

Private Broadcasting

One message, multiple recipients

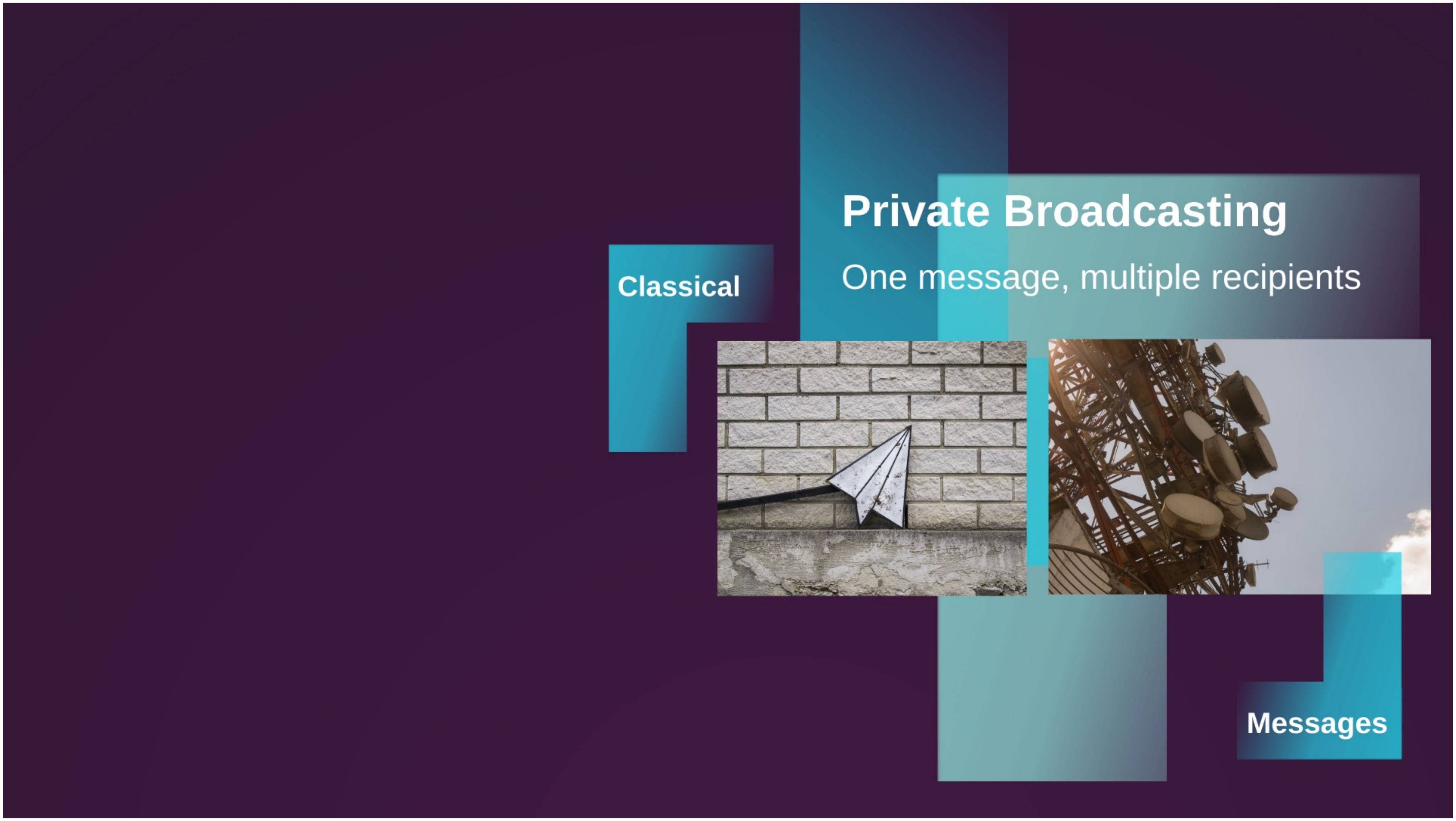
Classical

Messages

Sending Messages

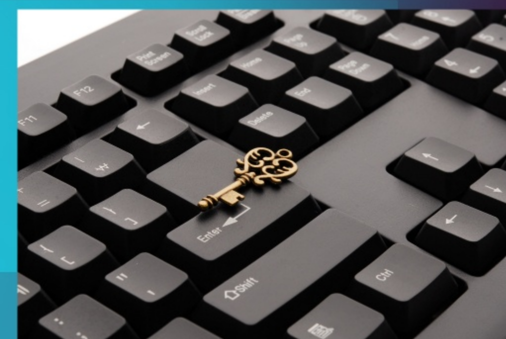
Insecure channels

Solution: Encryption


Private Broadcasting
One message, multiple recipients
Classical
Messages

Classical Broadcasting

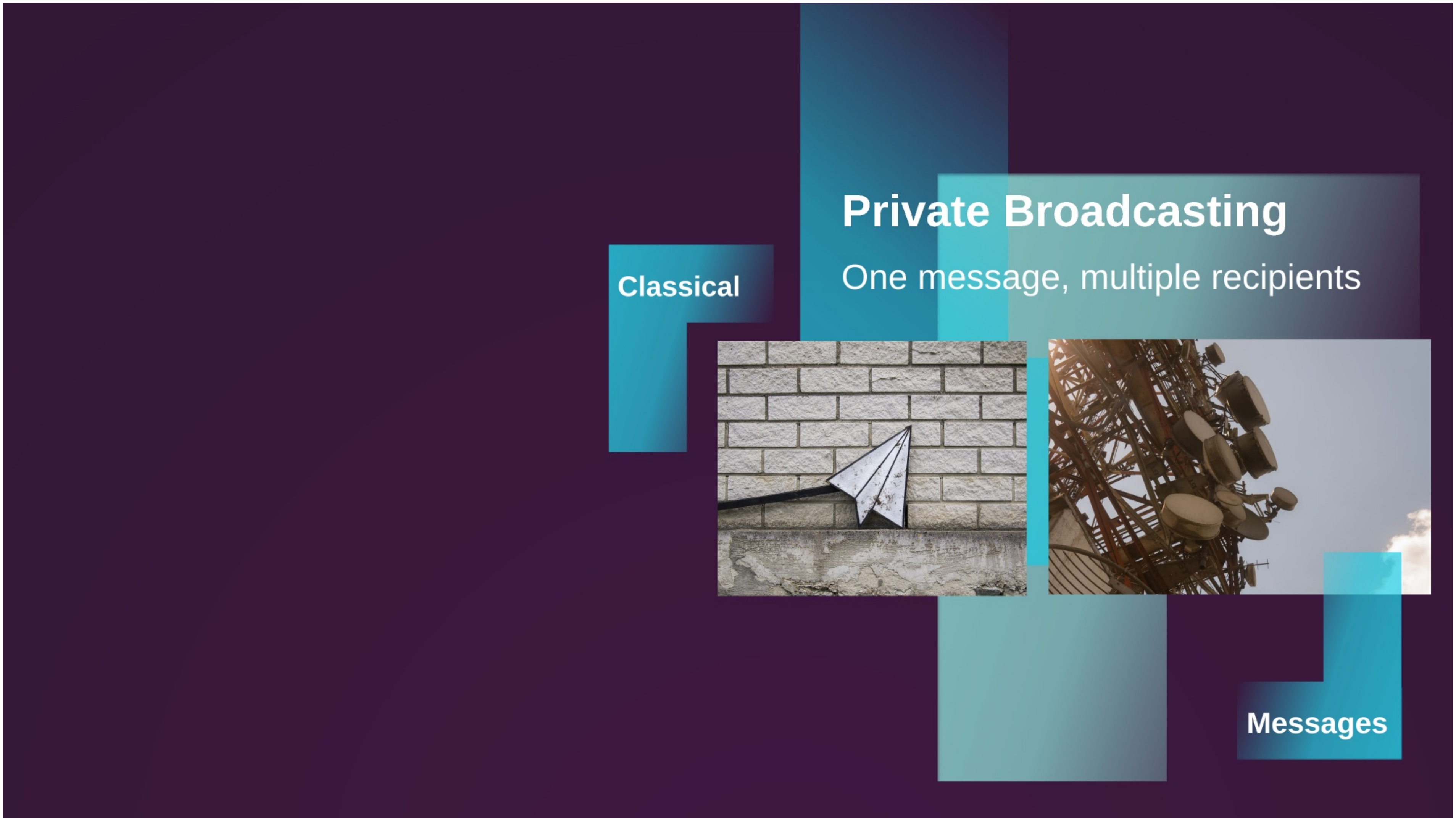
Copy message, same encryption key



Ex. One-Time Pad

$$t\left\{\begin{array}{ccccc} m & \oplus & k & = & c \\ m & \oplus & k & = & c \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m & \oplus & k & = & c \end{array}\right.$$

$$
t \left\{ \begin{array}{ccccc} m & \oplus & k & = & c \\ m & \oplus & k & = & c \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m & \oplus & k & = & c \end{array} \right.
$$


Private Broadcasting
One message, multiple recipients
Classical
Messages

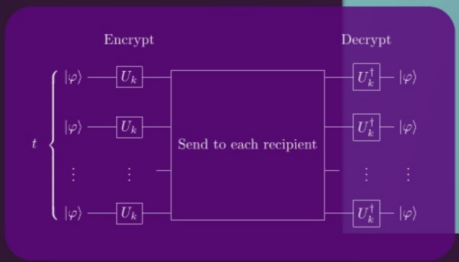

Private Broadcasting
Proposed Solutions
Quantum Private Broadcasting
Comparison
Quantum Private Broadcasting
A. Broadbent, C. González-Guillén
arXiv:2107.11474

QPB

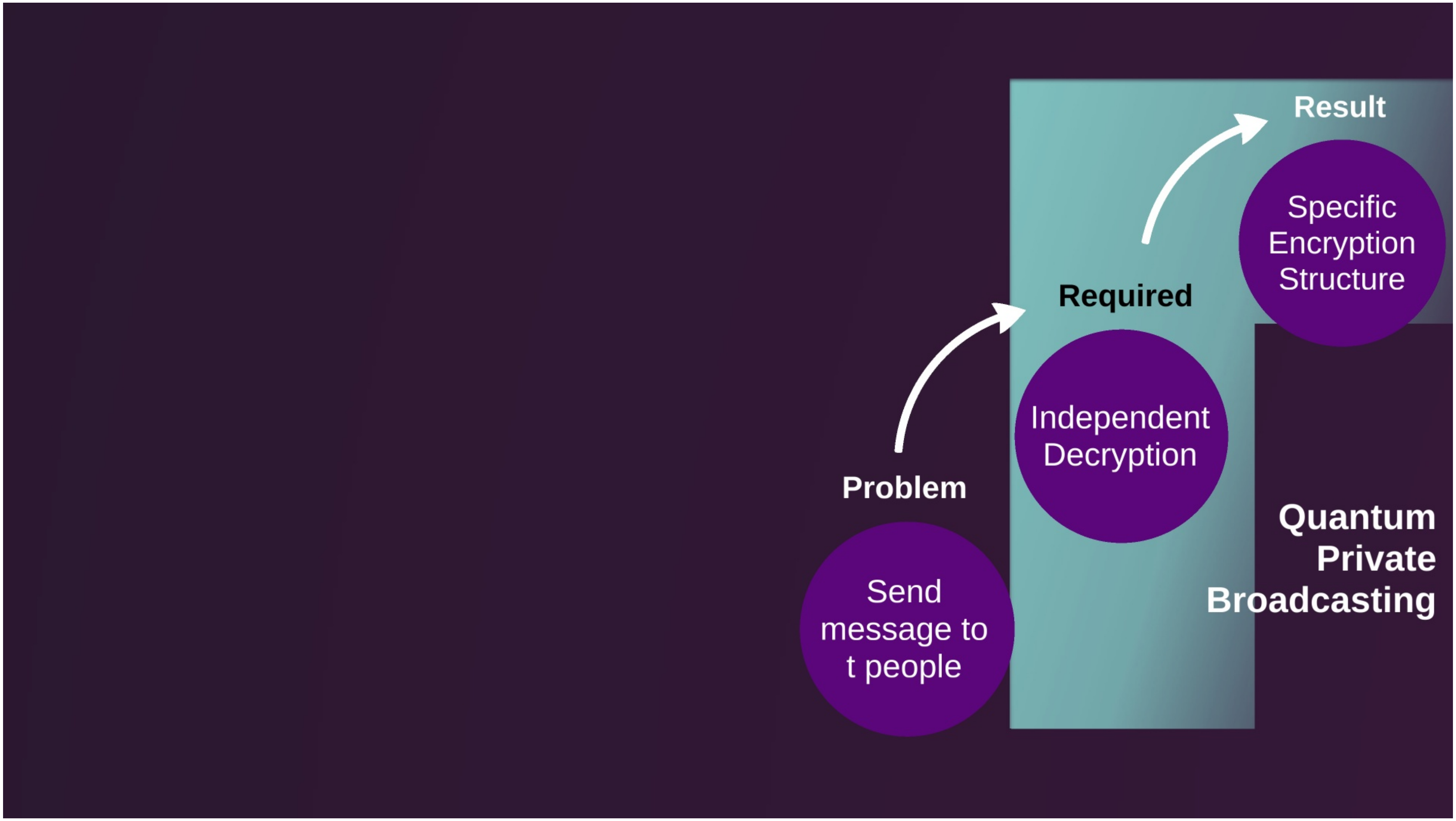
Quantum Private Broadcasting

Message: pure quantum state

No contact between recipients



Restrictions

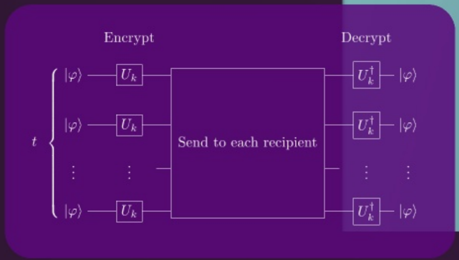

Result
Specific Encryption Structure
Required
Independent Decryption
Problem
Send message to t people
Quantum Private Broadcasting

QPB

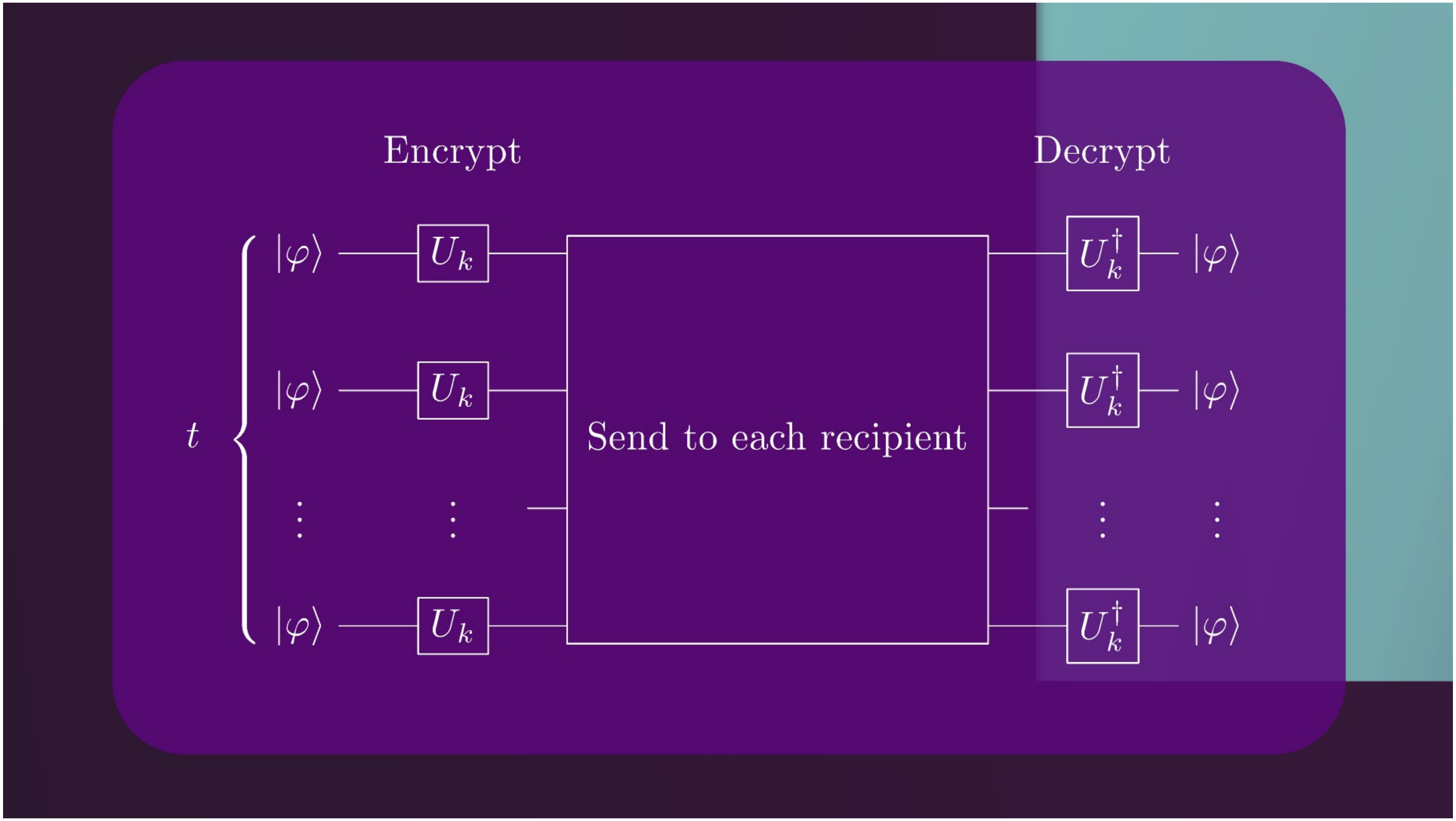
Quantum Private Broadcasting

Message: pure quantum state

No contact between recipients



Restrictions

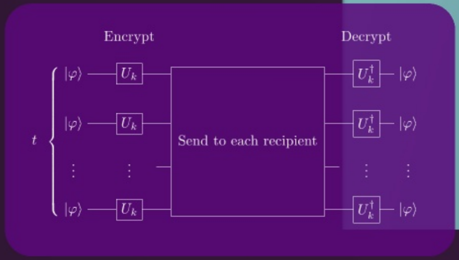

Encrypt
Decrypt
t
$|\varphi\rangle$
U_k
$U_k^\dagger$
Send to each recipient

QPB

Quantum Private Broadcasting

Message: pure quantum state

No contact between recipients



Restrictions

Correctness

δ-correct, t-recipient QPB

$$\mathsf{Enc}_k : \mathcal{H}_M^{\otimes t} \to \mathcal{H}_C^{\otimes t}$$
$$\mathsf{Dec}_k : \mathcal{H}_C \to \mathcal{H}_M$$

$$\left\| (\mathsf{Dec}_k^{\otimes t} \circ \mathsf{Enc}_k)\big|_{\mathrm{Sym}(d^t)} - \mathbb{1}_{\mathrm{Sym}(d^t)} \right\|_\diamond \leq 1 - \delta$$

$$\mathrm{Sym}(d^t) := \{ |\phi\rangle \in (\mathcal{H}_d)^{\otimes t} : P_d(\pi)\,|\phi\rangle = |\phi\rangle, \forall \pi \in S_t \}$$
$$P_d(\pi) = \sum_{i_1,\ldots,i_t \in [d]} |i_{\pi^{-1}(1)}, \ldots, i_{\pi^{-1}(t)}\rangle\langle i_1, \ldots, i_t|$$

$$\mathsf{Enc}_k : \mathcal{H}_M \to \mathcal{H}_C$$

$$\mathsf{Dec}_k : \mathcal{H}_C \to \mathcal{H}_M$$

$$\left\| \left(\mathsf{Dec}_k^{\otimes t} \circ \mathsf{Enc}_k\right)\Big|_{\mathrm{Sym}(d^t)} - \mathbb{1}_{\mathrm{Sym}(d^t)} \right\|_\diamond \leq 1 - \delta$$

$$\mathrm{Sym}(d^t) := \{\left|\phi\right\rangle \in (\mathcal{H}_d)^{\otimes t} : P_d(\pi)\left|\phi\right\rangle = \left|\phi\right\rangle, \forall \pi \in S_t\}$$

$$P_d(\pi) = \sum_{i_1,\ldots,i_t \in [d]} \left|i_{\pi^{-1}(1)}, \ldots, i_{\pi^{-1}(t)}\right\rangle\!\left\langle i_1, \ldots, i_t\right|$$

Security

ϵ-indistinguishable ciphertexts

$$\left\| (\mathbb{E}_{k\in K} \mathsf{Enc}_k - \langle\sigma\rangle)|_{\mathrm{Sym}(d^t)} \right\|_{1\to 1} \leq \epsilon$$

ϵ-indistinguishable ciphertexts against adversaries with side information

$$\left\| (\mathbb{E}_{k\in K} \mathsf{Enc}_k - \langle\sigma\rangle)|_{\mathrm{Sym}(d^t)} \right\|_{\diamond} \leq \epsilon$$

Security

ϵ-indistinguishable ciphertexts

$$\left\| \left(\mathbb{E}_{k\in K} \mathsf{Enc}_k - \langle\sigma\rangle\right)\big|_{\mathrm{Sym}(d^t)} \right\|_{1\to 1} \leq \epsilon$$

ϵ-indistinguishable ciphertexts against adversaries with side information

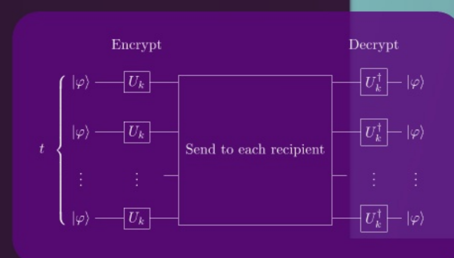
$$\left\| \left(\mathbb{E}_{k\in K} \, \mathsf{Enc}_k - \langle\sigma\rangle\right)\big|_{\mathrm{Sym}(d^t)} \right\|_\diamond \leq \epsilon$$

QPB

Quantum Private Broadcasting

Message: pure quantum state

No contact between recipients



Restrictions


Private
Broadcasting
Proposed
Solutions
Quantum
Private
Broadcasting
Comparison
Quantum Private
Broadcasting
A. Broadbent, C. González-Guillén
arXiv:2107.11474

Solutions to t-QPB

We consider 3 solutions
- Focus on key length in terms of classical bits
- i.e. taking logarithm of unitaries needed

QOTP

Unitary t-designs

Symmetric t-designs

Quantum One-Time Pad

For t-QPB

$$\mathsf{dQOTP}_{a,b}(\rho \otimes \rho) = \underbrace{X^a Z^b \rho Z^b X^a} \otimes \underbrace{X^a Z^b \rho Z^b X^a}$$

$$\left\| \left(\mathbb{E}_{a,b}\, \mathsf{dQOTP}_{a,b} - \langle \sigma \rangle \right) \Big|_{\mathrm{Sym}(2^2)} \right\|_{1 \to 1} \geq \frac{1}{2}$$

Ex. $\rho_0 = |0\rangle\langle 0| \otimes |0\rangle\langle 0|, \ \rho_1 = |+\rangle\langle +| \otimes |+\rangle\langle +|$

Solution

$$\mathsf{dQOTP}_{a,b}(\rho \otimes \rho) = \underbrace{X^a Z^b \rho Z^b X^a}_{} \otimes \underbrace{X^a Z^b \rho Z^b X^a}_{}$$

$$\left\| \left(\mathbb{E}_{a,b}\, \mathsf{dQOTP}_{a,b} - \langle \sigma \rangle \right) \Big|_{\mathrm{Sym}(2^2)} \right\|_{1 \to 1} \geq \frac{1}{2}$$

Ex. $\rho_0 = |0\rangle\langle 0| \otimes |0\rangle\langle 0|,\ \rho_1 = |+\rangle\langle +| \otimes |+\rangle\langle +|$

Secure QOTP for t-QPB

Separate keys
for each copy

Key length:

$$\log_2(4^t) = 2t$$

Quantum One-Time Pad

For t-QPB

$$\mathsf{dQOTP}_{a,b}(\rho \otimes \rho) = \underbrace{X^a Z^b \rho Z^b X^a}_{} \otimes \underbrace{X^a Z^b \rho Z^b X^a}_{}$$

$$\left\| \left(\mathbb{E}_{a,b}\, \mathsf{dQOTP}_{a,b} - \langle \sigma \rangle \right)\Big|_{\mathrm{Sym}(2^2)} \right\|_{1\to 1} \geq \frac{1}{2}$$

Ex. $\rho_0 = |0\rangle\langle 0| \otimes |0\rangle\langle 0|,\ \rho_1 = |+\rangle\langle +| \otimes |+\rangle\langle +|$

Solution

Solutions to t-QPB

We consider 3 solutions
- Focus on key length in terms of classical bits
- i.e. taking logarithm of unitaries needed

QOTP

Unitary t-designs

Symmetric t-designs

Security

Unitary t-designs

Unitary appears Haar-random when used up to t times

$$\sum_{k\in K} p(U_k) \cdot U_k^{\otimes t} \rho (U_k^{\dagger})^{\otimes t} = \int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^{\dagger})^{\otimes t} dU$$

Key Length

$$\sum_{k\in K} p(U_k)\cdot U_k^{\otimes t}\rho(U_k^{\dagger})^{\otimes t}$$

$$= \int_{\mathcal{U}(d)} U^{\otimes t}\rho(U^{\dagger})^{\otimes t} dU$$

Designs & t-QPB Security

- Schmidt decomposition
- Re-writing twirling of states
- Collapses to twirling of state in symmetric subspace

$$|\psi\rangle \in \mathcal{H}_A \otimes \mathrm{Sym}(d^t)$$

$$|\psi\rangle = \sum_{i=1}^{D} \lambda_i \, |a_i\rangle \otimes |\varphi_i\rangle$$

$$|\psi\rangle\langle\psi| = \sum_i \sum_j \lambda_i \lambda_j^* \, |a_i\rangle\langle a_j| \otimes |\varphi_i\rangle\langle\varphi_j|$$

$$\rho_0 = \frac{\mathbb{1}}{2} \otimes \frac{\mathbb{1}}{2}, \rho_1 = \tau_{\mathrm{Sym}}$$

$$\int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} dU = \mathrm{tr}(\Pi_{\mathrm{Sym}} \rho \Pi_{\mathrm{Sym}}) \tau_{\mathrm{Sym}} + \sum_b \mathrm{tr}(\Pi_b \rho \Pi_b) \tau_b$$

$$|\psi\rangle \in \mathcal{H}_A \otimes \mathrm{Sym}(d^t)$$

$$|\psi\rangle = \sum_{i=1}^{D} \lambda_i \, |a_i\rangle \otimes |\varphi_i\rangle$$

$$|\psi\rangle\langle\psi| = \sum_i \sum_j \lambda_i \lambda_j^* \, |a_i\rangle\langle a_j| \otimes |\varphi_i\rangle\langle\varphi_j|$$

$$= \tau_{\mathrm{Sym}}$$

$$|\psi\rangle = \sum_{i=1}^{D} \lambda_i \, |a_i\rangle \otimes |\varphi_i\rangle$$

$$|\psi\rangle\langle\psi| = \sum_i \sum_j \lambda_i \lambda_j^* \, |a_i\rangle\langle a_j| \otimes |\varphi_i\rangle\langle\varphi_j|$$

$$\int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} dU = \mathrm{tr}(\Pi_{\mathrm{Sym}} \rho \Pi_{\mathrm{Sym}}) \tau_{\mathrm{Sym}} + \sum_b \mathrm{tr}(\Pi_b \rho \Pi_b) \tau_b$$

Designs & t-QPB Security

- Schmidt decomposition
- Re-writing twirling of states
- Collapses to twirling of state in symmetric subspace

$$|\psi\rangle \in \mathcal{H}_A \otimes \mathrm{Sym}(d^t)$$

$$|\psi\rangle = \sum_{i=1}^{D} \lambda_i |a_i\rangle \otimes |\varphi_i\rangle$$

$$|\psi\rangle\langle\psi| = \sum_i \sum_j \lambda_i \lambda_j^* |a_i\rangle\langle a_j| \otimes |\varphi_i\rangle\langle\varphi_j|$$

$$\rho_0 = \frac{\mathbb{1}}{2} \otimes \frac{\mathbb{1}}{2}, \rho_1 = \tau_{\mathrm{Sym}}$$

$$\int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} dU = \mathrm{tr}(\Pi_{\mathrm{Sym}} \rho \Pi_{\mathrm{Sym}}) \tau_{\mathrm{Sym}} + \sum_b \mathrm{tr}(\Pi_b \rho \Pi_b) \tau_b$$

$$\rho_0 = \frac{\mathbb{1}}{2} \otimes \frac{\mathbb{1}}{2}, \rho_1 = \tau_{\mathrm{Sym}}$$

Security

Unitary t-designs

Unitary appears Haar-random when used up to t times

$$\sum_{k \in K} p(U_k) \cdot U_k^{\otimes t} \rho (U_k^{\dagger})^{\otimes t}$$
$$= \int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^{\dagger})^{\otimes t} dU$$

Key Length

Lower & Upper Bounds

Translate to key length bounds

	Lower	**Upper**
Weighted	$\binom{d^2+t-1}{t} \in \Omega(t^{d^2-1})$	$\binom{d^2+t-1}{t}^2 \in O(t^{2(d^2-1)})$
Unweighted	$\binom{d^2+t-1}{t} \in \Omega(t^{d^2-1})$	$\left(\frac{e(d^2+t-1)}{t}\right)^{2t}$

Key length d=2:

$$\log_2\left(\frac{1}{6}\left(t^3 + 6t^2 + 11t + 6\right)\right)$$

Translate to key length bounds

	Lower	Upper
Weighted	$\binom{d^2+t-1}{t} \in \Omega(t^{d^2-1})$	$\binom{d^2+t-1}{t}^2 \in O(t^{2(d^2-1)})$
Unweighted	$\binom{d^2+t-1}{t} \in \Omega(t^{d^2-1})$	$\left(\frac{e(d^2+t-1)}{t}\right)^{2t}$

Key length d=2:

Lower & Upper Bounds

Translate to key length bounds

	Lower	**Upper**
Weighted	$\binom{d^2+t-1}{t} \in \Omega(t^{d^2-1})$	$\binom{d^2+t-1}{t}^2 \in O(t^{2(d^2-1)})$
Unweighted	$\binom{d^2+t-1}{t} \in \Omega(t^{d^2-1})$	$\left(\frac{e(d^2+t-1)}{t}\right)^{2t}$

Key length d=2:

$$\log_2\left(\frac{1}{6}\left(t^3+6t^2+11t+6\right)\right)$$

Security

Unitary t-designs

Unitary appears Haar-random when used up to t times

$$\sum_{k\in K} p(U_k)\cdot U_k^{\otimes t}\rho(U_k^{\dagger})^{\otimes t}$$
$$= \int_{\mathcal{U}(d)} U^{\otimes t}\rho(U^{\dagger})^{\otimes t}dU$$

Key Length

Solutions to t-QPB

We consider 3 solutions
- Focus on key length in terms of classical bits
- i.e. taking logarithm of unitaries needed

QOTP

Unitary t-designs

Symmetric t-designs

Key Length

Symmetric Unitary t-designs

- Relaxation of unitary t-design
- Mimics action of Haar-measure in symmetric subspace
- Security of designs for t-QPB applies to symmetric designs

Exact Symmetric Bounds

Lower bound:

- 1-design in $\mathcal{U}(\mathrm{Sym}(d^t))$
- Resulting lower bound of d_{Sym}^2

Upper bound:

$$A = \{U^{\otimes t} \otimes (\overline{U})^{\otimes t}|_{\mathrm{Sym}(d^t)\otimes\mathrm{Sym}(d^t)} : U \in \mathcal{U}(d)\}$$
$$B = \{V \otimes \overline{V} : V \in \mathcal{U}(\mathrm{Sym}(d^t))\}$$

- Applying Carathéodory's Theorem

$$d_{\mathrm{Sym}}^4 - 2d_{\mathrm{Sym}}^2 + 3 \in O(d_{\mathrm{Sym}}^4)$$

Approximate

- Resulting lower bound of d_{S}

Upper bound:

$$A = \{U^{\otimes t} \otimes (\overline{U})^{\otimes t}|_{\mathrm{Sym}(d^t)\otimes \mathrm{Sym}(d^t)} : U \in \mathcal{U}(d)\}$$

$$B = \{V \otimes \overline{V} : V \in \mathcal{U}(\mathrm{Sym}(d^t))\}$$

- Applying Carathéodory's Theorem

Exact Symmetric Bounds

Lower bound:

- 1-design in $\mathcal{U}(\mathrm{Sym}(d^t))$
- Resulting lower bound of d_{Sym}^2

Upper bound:

$A = \{U^{\otimes t} \otimes (\overline{U})^{\otimes t}|_{\mathrm{Sym}(d^t)\otimes\mathrm{Sym}(d^t)} : U \in \mathcal{U}(d)\}$
$B = \{V \otimes \overline{V} : V \in \mathcal{U}(\mathrm{Sym}(d^t))\}$

- Applying Carathéodory's Theorem

$$d_{\mathrm{Sym}}^4 - 2d_{\mathrm{Sym}}^2 + 3 \in O(d_{\mathrm{Sym}}^4)$$

Approximate

Approximate Bounds

Lower Bound:

$$(d_{\mathrm{Sym}})^{(1-\epsilon)}$$

Upper Bound:

$$\alpha \frac{d_{\mathrm{Sym}}}{\epsilon^2} \log(d_{\mathrm{Sym}})^6 \log(1/\epsilon^2)$$

Exact Symmetric Bounds

Lower bound:

- 1-design in $\mathcal{U}(\mathrm{Sym}(d^t))$
- Resulting lower bound of d_{Sym}^2

Upper bound:

$$A = \{U^{\otimes t} \otimes (\overline{U})^{\otimes t}|_{\mathrm{Sym}(d^t)\otimes\mathrm{Sym}(d^t)} : U \in \mathcal{U}(d)\}$$
$$B = \{V \otimes \overline{V} : V \in \mathcal{U}(\mathrm{Sym}(d^t))\}$$

- Applying Carathéodory's Theorem

$$d_{\mathrm{Sym}}^4 - 2d_{\mathrm{Sym}}^2 + 3 \in O(d_{\mathrm{Sym}}^4)$$

Approximate

Key Length

Symmetric Unitary t-designs

- Relaxation of unitary t-design
- Mimics action of Haar-measure in symmetric subspace
- Security of designs for t-QPB applies to symmetric designs

Solutions to t-QPB

We consider 3 solutions
- Focus on key length in terms of classical bits
- i.e. taking logarithm of unitaries needed

QOTP

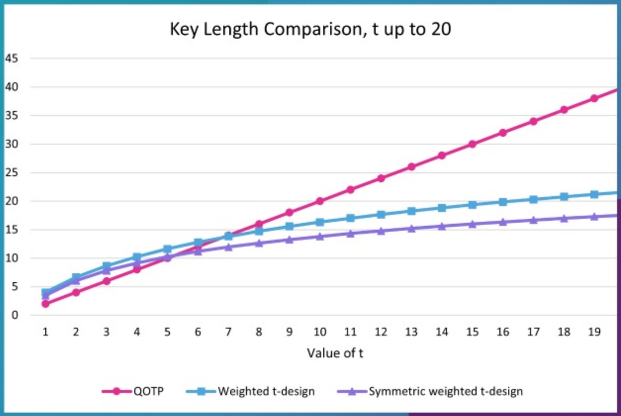
Unitary t-designs

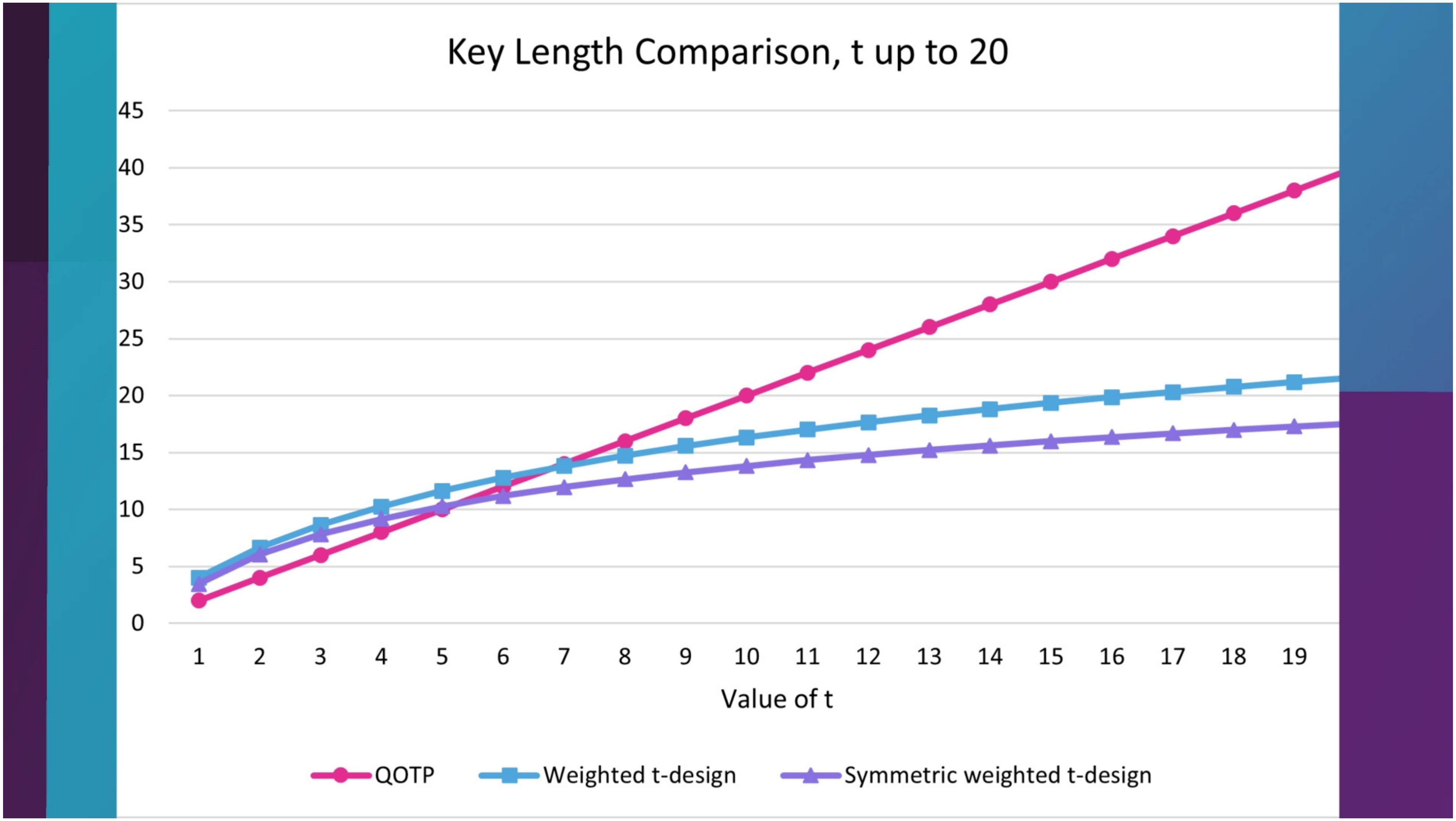
Symmetric t-designs


Private
Broadcasting
Proposed
Solutions
Quantum
Private
Broadcasting
Comparison
Quantum Private
Broadcasting
A. Broadbent, C. González-Guillén
arXiv:2107.11474

Comparison of Solutions

Taking d=2, letting t vary




Key Length Comparison, t up to 20
45
40
35
30
25
20
15
10
5
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
Value of t
QOTP
Weighted t-design
Symmetric weighted t-design


Private
Broadcasting
Proposed
Solutions
Quantum
Private
Broadcasting
Comparison
Quantum Private
Broadcasting
A. Broadbent, C. González-Guillén
arXiv:2107.11474