

# Private States, Privacy Amplification, and the Uncertainty Principle

Joseph M. Renes  and Jean-Christian Boileau <sup>IQC</sup>



Theoretical Quantum Physics, Institut für Angewandte Physik  
Technische Universität Darmstadt



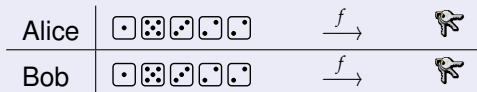
Institute for Quantum Computing, University of Waterloo

DPG Frühjahrstagung  
Düsseldorf  
2007 March 21





# Privacy Amplification

Extract secret key from shared random string



Apply suitable random “hash” function  $f$  to long blocks of shared bits

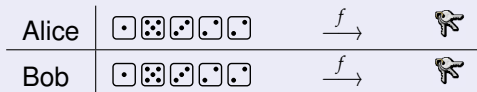
-  Completely random  $n \rightarrow m$  bit functions
-  2-universal hash functions, e.g. linear

Three approaches to *quantum* privacy amplification



- 1 Apply classical methods to the quantum case
- 2 Recast as private state distillation
- 3 Appeal to the uncertainty principle

# Privacy Amplification

## Extract secret key from shared random string



Apply suitable random “hash” function  $f$  to long blocks of shared bits

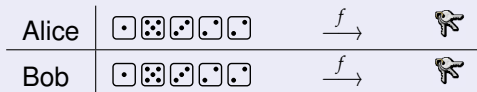
-  Completely random  $n \rightarrow m$  bit functions
-  2-universal hash functions, e.g. linear

## Three approaches to *quantum* privacy amplification

- 1 Apply classical methods to the quantum case
- 2 Recast as private state distillation
- 3 Appeal to the uncertainty principle

# Privacy Amplification

Extract secret key from shared random string



Apply suitable random “hash” function  $f$  to long blocks of shared bits

- ☞ Completely random  $n \rightarrow m$  bit functions
- ☞ 2-universal hash functions, e.g. linear

Three approaches to *quantum* privacy amplification

- 1 Apply classical

**These are really all the same!**

Uncertainty principle connects the various approaches.

uncertainty principle

# Classical approach: $H(Z|E) = 1$

**Goal: create a *perfect key***

$$\kappa_{ABE} = \left( \frac{1}{2} \sum_k |kk\rangle_{AB} \langle kk| \right) \otimes \rho_E$$

Eve's entropy of key:  $H(Z) = 1$

Asymptotic key rate

$$r = 1 - I(A:E) = 1 - \chi(\{1/2, \rho_E^k\})$$

Start with state

$$\rho_{ABE} = \frac{1}{2} \sum_k P_{AB}^{kk} \otimes \rho_E^k,$$

$$P_{AB}^{kk} = |kk\rangle_{AB} \langle kk|$$

Apply  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ :

$$\hat{\rho}_{ABE} = \frac{1}{2^m} \sum_k P_{AB}^{f(k), f(k)} \otimes \hat{\rho}_E^{f(k)},$$

$$\hat{\rho}_E^j = \frac{1}{2^{n-m}} \sum_{k|f(k)=j} \rho_E^k$$

Operator Chernoff bound:  $\hat{\rho}_E^j \approx \hat{\rho}_E$

Eve's state indep. of key  $\Rightarrow \hat{\rho}_{ABE}^{(n)} \approx \kappa_{ABE}$



# Classical approach: $H(Z|E) = 1$

**Goal: create a *perfect key***

$$\kappa_{ABE} = \left( \frac{1}{2} \sum_k |kk\rangle_{AB} \langle kk| \right) \otimes \rho_E$$

Eve's entropy of key:  $H(Z) = 1$

Asymptotic key rate

$$r = 1 - I(A:E) = 1 - \chi(\{1/2, \rho_E^k\})$$

Start with state

$$\rho_{ABE} = \frac{1}{2} \sum_k P_{AB}^{kk} \otimes \rho_E^k,$$

$$P_{AB}^{kk} = |kk\rangle_{AB} \langle kk|$$

Apply  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ :

$$\hat{\rho}_{ABE} = \frac{1}{2^m} \sum_k P_{AB}^{f(k), f(k)} \otimes \hat{\rho}_E^{f(k)},$$

$$\hat{\rho}_E^j = \frac{1}{2^{n-m}} \sum_{k|f(k)=j} \rho_E^k$$

Operator Chernoff bound:  $\hat{\rho}_E^j \approx \hat{\rho}_E$

Eve's state indep. of key  $\Rightarrow \hat{\rho}_{ABE}^{(n)} \approx \kappa_{ABE}$



# Classical approach: $H(Z|E) = 1$

**Goal: create a *perfect key***

$$\kappa_{ABE} = \left( \frac{1}{2} \sum_k |kk\rangle_{AB} \langle kk| \right) \otimes \rho_E$$

Eve's entropy of key:  $H(Z) = 1$

Asymptotic key rate

$$r = 1 - I(A:E) = 1 - \chi(\{1/2, \rho_E^k\})$$

Start with state

$$\rho_{ABE} = \frac{1}{2} \sum_k P_{AB}^{kk} \otimes \rho_E^k,$$

$$P_{AB}^{kk} = |kk\rangle_{AB} \langle kk|$$

Apply  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ :

$$\hat{\rho}_{ABE} = \frac{1}{2^m} \sum_k P_{AB}^{f(k), f(k)} \otimes \hat{\rho}_E^{f(k)},$$

$$\hat{\rho}_E^j = \frac{1}{2^{n-m}} \sum_{k|f(k)=j} \rho_E^k$$

Operator Chernoff bound:  $\hat{\rho}_E^j \approx \hat{\rho}_E$

Eve's state indep. of key  $\Rightarrow \hat{\rho}_{ABE}^{(n)} \approx \kappa_{ABE}$



# Classical approach: $H(Z|E) = 1$

**Goal: create a *perfect key***

$$\kappa_{ABE} = \left( \frac{1}{2} \sum_k |kk\rangle_{AB} \langle kk| \right) \otimes \rho_E$$

Eve's entropy of key:  $H(Z) = 1$

**Asymptotic key rate**

$$r = 1 - I(A:E) = 1 - \chi(\{1/2, \rho_E^k\})$$

**Start with state**

$$\rho_{ABE} = \frac{1}{2} \sum_k P_{AB}^{kk} \otimes \rho_E^k,$$

$$P_{AB}^{kk} = |kk\rangle_{AB} \langle kk|$$

**Apply  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ :**

$$\hat{\rho}_{ABE} = \frac{1}{2^m} \sum_k P_{AB}^{f(k), f(k)} \otimes \hat{\rho}_E^{f(k)},$$

$$\hat{\rho}_E^j = \frac{1}{2^{n-m}} \sum_{k|f(k)=j} \rho_E^k$$

**Operator Chernoff bound:  $\hat{\rho}_E^j \approx \hat{\rho}_E$**

**Eve's state indep. of key  $\Rightarrow \hat{\rho}_{ABE}^{(n)} \approx \kappa_{ABE}$**



# Uncertainty Principle

## Entropic form

For qubit system  $H(X) + H(Z) \geq 1$  for  $X$  and  $Z$  measurements

👉 Note this is state independent

## Idea for key distillation:

👉 Instead of arguing that  $H(Z) = 1$ , focus on the  $H(X)$  term

👉 If key  $\approx |+\rangle$ , then  $Z$  measurement unknown.

👉 Distill  $|+\rangle$

## But key has two halves...?

👉 Bob should be able to predict Alice's (hypothetical)  $X$  mmt.

👉 Modify to:  $H(Z|E) + H(X|B) \geq 1$ .



# Uncertainty Principle

## Entropic form

For qubit system  $H(X) + H(Z) \geq 1$  for  $X$  and  $Z$  measurements

👉 Note this is state independent

## Idea for key distillation:

👉 Instead of arguing that  $H(Z) = 1$ , focus on the  $H(X)$  term

👉 If key  $\approx |+\rangle$ , then  $Z$  measurement unknown.

👉 Distill  $|+\rangle$

## But key has two halves...?

👉 Bob should be able to predict Alice's (hypothetical)  $X$  mmt.

👉 Modify to:  $H(Z|E) + H(X|B) \geq 1$ .



# Private States: Purification of $\kappa_{ABE}$

Private state  $\gamma_{ABSE}$  has form

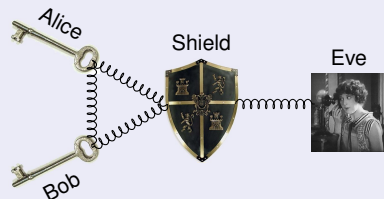
$$\frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB} V_S^k |\xi\rangle_{SE} = U_{ABS} |\Phi\rangle_{AB} |\xi\rangle_{SE}$$

- Unitaries  $V_S^k$  and state  $|\xi\rangle_{SE}$  arbitrary
- $|\Phi\rangle_{AB}$  maximally entangled

Twisting operator:  $U_{ABS} = \sum_{j,k} P_{AB}^{j,k} \otimes V_S^{j,k}$

Shield owned by AB, but not part of key

Shield deflects AB correlations from E



$H(Z|E) = 1$ :  $\gamma_{ABSE}$  a private state iff:

- 1  $p_{j,k} = \text{Tr}[\gamma_{ABSE} P_{AB}^{j,k}] = \frac{1}{2} \delta_{j,k}$ ,
- 2  $\gamma_E^j = \gamma_E^k$  for all  $j, k$ ,

where  $\gamma_E^k = 2 \langle k, k | \gamma_{ABE} | k, k \rangle_{AB}$ .

$H(X|B) = 0$ :  $\gamma_{ABSE}$  a private state iff:

- 1  $p_{j,k} = \text{Tr}[\gamma_{ABSE} P_{AB}^{j,k}] = \frac{1}{2} \delta_{j,k}$ ,
- 2  $\sigma_{BS}^j \sigma_{BS}^k = 0$  for all  $j \neq k$ ,

where  $\sigma_{BS}^x = 2 \langle \tilde{x} | \gamma_{ABS} | \tilde{x} \rangle_A$

Two characterizations related by uncertainty principle!



# Private States: Purification of $\kappa_{ABE}$

Private state  $\gamma_{ABSE}$  has form

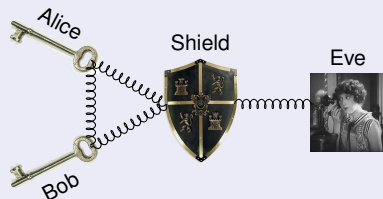
$$\frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB} V_S^k |\xi\rangle_{SE} = U_{ABS} |\Phi\rangle_{AB} |\xi\rangle_{SE}$$

- Unitaries  $V_S^k$  and state  $|\xi\rangle_{SE}$  arbitrary
- $|\Phi\rangle_{AB}$  maximally entangled

Twisting operator:  $U_{ABS} = \sum_{j,k} P_{AB}^{j,k} \otimes V_S^{j,k}$

Shield owned by AB, but not part of key

Shield deflects AB correlations from E



$H(Z|E) = 1$ :  $\gamma_{ABSE}$  a private state iff:

- 1  $p_{j,k} = \text{Tr}[\gamma_{ABSE} P_{AB}^{j,k}] = \frac{1}{2} \delta_{j,k}$ ,
- 2  $\gamma_E^j = \gamma_E^k$  for all  $j, k$ ,

where  $\gamma_E^k = 2 \langle k, k | \gamma_{ABE} | k, k \rangle_{AB}$ .

$H(X|B) = 0$ :  $\gamma_{ABSE}$  a private state iff:

- 1  $p_{j,k} = \text{Tr}[\gamma_{ABSE} P_{AB}^{j,k}] = \frac{1}{2} \delta_{j,k}$ ,
- 2  $\sigma_{BS}^j \sigma_{BS}^k = 0$  for all  $j \neq k$ ,

where  $\sigma_{BS}^x = 2 \langle \tilde{x} | \gamma_{ABS} | \tilde{x} \rangle_A$

Two characterizations related by uncertainty principle!



# Private State Distillation: $H(X|B) = 0$

- 👉 Start with  $|\psi\rangle_{ABSE} = \frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB} |\varphi^k\rangle_{SE}$  (purification of  $\rho_{ABE}$ )
- 👉 Bob has incomplete info:  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) < 1$
- 👉 Simple distillation idea: Alice narrows possible  $x$  by public announcement so Bob can distinguish remaining  $\sigma_{BS}^x$ .
- 👉  $\approx$  Classical comm. over quantum channel  $\Rightarrow$  use HSW theorem
- 👉 Pretend Alice measures  $X_A$  on  $|\psi\rangle_{ABSE}^{\otimes n}$  and then computes  $n[1 - \chi]$  random parities
- 👉 Bob can reliably distinguish between the remaining  $2^{n\chi}$  possibilities. **Result is a private state.**
- 👉 Parities correspond to  $X^{\mathbf{u}}$  for some random strings  $\mathbf{u}$ .  
Key given by  $Z^{\mathbf{v}}$  for  $\mathbf{v}$ 's such that  $\mathbf{v} \cdot \mathbf{u} = 0$  for all  $\mathbf{u}$
- 👉 Just as well measure  $Z$  individually and reconstruct key as  $Z^{\mathbf{v}}$
- 👉 Resulting rate =  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) = 1 - I(A:E)$



# Private State Distillation: $H(X|B) = 0$

- Start with  $|\psi\rangle_{ABSE} = \frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB} |\varphi^k\rangle_{SE}$  (purification of  $\rho_{ABE}$ )
- Bob has incomplete info:  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) < 1$
- Simple distillation idea: Alice narrows possible  $x$  by public announcement so Bob can distinguish remaining  $\sigma_{BS}^x$ .
- $\approx$  Classical comm. over quantum channel  $\Rightarrow$  use HSW theorem
- Pretend Alice measures  $X_A$  on  $|\psi\rangle_{ABSE}^{\otimes n}$  and then computes  $n[1 - \chi]$  random parities
- Bob can reliably distinguish between the remaining  $2^{n\chi}$  possibilities. **Result is a private state.**
- Parities correspond to  $X^{\mathbf{u}}$  for some random strings  $\mathbf{u}$ .  
Key given by  $Z^{\mathbf{v}}$  for  $\mathbf{v}$ 's such that  $\mathbf{v} \cdot \mathbf{u} = 0$  for all  $\mathbf{u}$
- Just as well measure  $Z$  individually and reconstruct key as  $Z^{\mathbf{v}}$
- Resulting rate =  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) = 1 - I(A:E)$



# Private State Distillation: $H(X|B) = 0$

- Start with  $|\psi\rangle_{ABSE} = \frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB} |\varphi^k\rangle_{SE}$  (purification of  $\rho_{ABE}$ )
- Bob has incomplete info:  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) < 1$
- Simple distillation idea: Alice narrows possible  $x$  by public announcement so Bob can distinguish remaining  $\sigma_{BS}^x$ .
- $\approx$  Classical comm. over quantum channel  $\Rightarrow$  use HSW theorem
- Pretend Alice measures  $X_A$  on  $|\psi\rangle_{ABSE}^{\otimes n}$  and then computes  $n[1 - \chi]$  random parities
- Bob can reliably distinguish between the remaining  $2^{n\chi}$  possibilities. **Result is a private state.**
- Parities correspond to  $X^{\mathbf{u}}$  for some random strings  $\mathbf{u}$ .  
Key given by  $Z^{\mathbf{v}}$  for  $\mathbf{v}$ 's such that  $\mathbf{v} \cdot \mathbf{u} = 0$  for all  $\mathbf{u}$
- Just as well measure  $Z$  individually and reconstruct key as  $Z^{\mathbf{v}}$
- Resulting rate =  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) = 1 - I(A:E)$



# Private State Distillation: $H(X|B) = 0$

- Start with  $|\psi\rangle_{ABSE} = \frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB} |\varphi^k\rangle_{SE}$  (purification of  $\rho_{ABE}$ )
- Bob has incomplete info:  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) < 1$
- Simple distillation idea: Alice narrows possible  $x$  by public announcement so Bob can distinguish remaining  $\sigma_{BS}^x$ .
- $\approx$  Classical comm. over quantum channel  $\Rightarrow$  use HSW theorem
- Pretend Alice measures  $X_A$  on  $|\psi\rangle_{ABSE}^{\otimes n}$  and then computes  $n[1 - \chi]$  random parities
- Bob can reliably distinguish between the remaining  $2^{n\chi}$  possibilities. **Result is a private state.**
- Parities correspond to  $X^{\mathbf{u}}$  for some random strings  $\mathbf{u}$ .  
Key given by  $Z^{\mathbf{v}}$  for  $\mathbf{v}$ 's such that  $\mathbf{v} \cdot \mathbf{u} = 0$  for all  $\mathbf{u}$
- Just as well measure  $Z$  individually and reconstruct key as  $Z^{\mathbf{v}}$
- Resulting rate =  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) = 1 - I(A:E)$



# Private State Distillation: $H(X|B) = 0$

- Start with  $|\psi\rangle_{ABSE} = \frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB} |\varphi^k\rangle_{SE}$  (purification of  $\rho_{ABE}$ )
- Bob has incomplete info:  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) < 1$
- Simple distillation idea: Alice narrows possible  $x$  by public announcement so Bob can distinguish remaining  $\sigma_{BS}^x$ .
- $\approx$  Classical comm. over quantum channel  $\Rightarrow$  use HSW theorem
- ☞ Pretend Alice measures  $X_A$  on  $|\psi\rangle_{ABSE}^{\otimes n}$  and then computes  $n[1 - \chi]$  random parities
- Bob can reliably distinguish between the remaining  $2^{n\chi}$  possibilities. **Result is a private state.**
- Parities correspond to  $X^{\mathbf{u}}$  for some random strings  $\mathbf{u}$ .  
Key given by  $Z^{\mathbf{v}}$  for  $\mathbf{v}$ 's such that  $\mathbf{v} \cdot \mathbf{u} = 0$  for all  $\mathbf{u}$
- Just as well measure  $Z$  individually and reconstruct key as  $Z^{\mathbf{v}}$
- Resulting rate =  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) = 1 - I(A:E)$



# Private State Distillation: $H(X|B) = 0$

- Start with  $|\psi\rangle_{ABSE} = \frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB} |\varphi^k\rangle_{SE}$  (purification of  $\rho_{ABE}$ )
- Bob has incomplete info:  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) < 1$
- Simple distillation idea: Alice narrows possible  $x$  by public announcement so Bob can distinguish remaining  $\sigma_{BS}^x$ .
- $\approx$  Classical comm. over quantum channel  $\Rightarrow$  use HSW theorem
- Pretend Alice measures  $X_A$  on  $|\psi\rangle_{ABSE}^{\otimes n}$  and then computes  $n[1 - \chi]$  random parities
- Bob can reliably distinguish between the remaining  $2^{n\chi}$  possibilities. **Result is a private state.**
- Parities correspond to  $X^{\mathbf{u}}$  for some random strings  $\mathbf{u}$ .  
Key given by  $Z^{\mathbf{v}}$  for  $\mathbf{v}$ 's such that  $\mathbf{v} \cdot \mathbf{u} = 0$  for all  $\mathbf{u}$
- Just as well measure  $Z$  individually and reconstruct key as  $Z^{\mathbf{v}}$
- Resulting rate =  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) = 1 - I(A:E)$



# Private State Distillation: $H(X|B) = 0$

- Start with  $|\psi\rangle_{ABSE} = \frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB} |\varphi^k\rangle_{SE}$  (purification of  $\rho_{ABE}$ )
- Bob has incomplete info:  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) < 1$
- Simple distillation idea: Alice narrows possible  $x$  by public announcement so Bob can distinguish remaining  $\sigma_{BS}^x$ .
- $\approx$  Classical comm. over quantum channel  $\Rightarrow$  use HSW theorem
- Pretend Alice measures  $X_A$  on  $|\psi\rangle_{ABSE}^{\otimes n}$  and then computes  $n[1 - \chi]$  random parities
- Bob can reliably distinguish between the remaining  $2^{n\chi}$  possibilities. **Result is a private state.**
- Parities correspond to  $X^{\mathbf{u}}$  for some random strings  $\mathbf{u}$ .  
Key given by  $Z^{\mathbf{v}}$  for  $\mathbf{v}$ 's such that  $\mathbf{v} \cdot \mathbf{u} = 0$  for all  $\mathbf{u}$
- Just as well measure  $Z$  individually and reconstruct key as  $Z^{\mathbf{v}}$
- Resulting rate =  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) = 1 - I(A:E)$



# Private State Distillation: $H(X|B) = 0$

- Start with  $|\psi\rangle_{ABSE} = \frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB} |\varphi^k\rangle_{SE}$  (purification of  $\rho_{ABE}$ )
- Bob has incomplete info:  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) < 1$
- Simple distillation idea: Alice narrows possible  $x$  by public announcement so Bob can distinguish remaining  $\sigma_{BS}^x$ .
- $\approx$  Classical comm. over quantum channel  $\Rightarrow$  use HSW theorem
- Pretend Alice measures  $X_A$  on  $|\psi\rangle_{ABSE}^{\otimes n}$  and then computes  $n[1 - \chi]$  random parities
- Bob can reliably distinguish between the remaining  $2^{n\chi}$  possibilities. **Result is a private state.**
- Parities correspond to  $X^{\mathbf{u}}$  for some random strings  $\mathbf{u}$ .  
Key given by  $Z^{\mathbf{v}}$  for  $\mathbf{v}$ 's such that  $\mathbf{v} \cdot \mathbf{u} = 0$  for all  $\mathbf{u}$
- Just as well measure  $Z$  individually and reconstruct key as  $Z^{\mathbf{v}}$
- Resulting rate =  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) = 1 - I(A:E)$



# Private State Distillation: $H(X|B) = 0$

- Start with  $|\psi\rangle_{ABSE} = \frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB} |\varphi^k\rangle_{SE}$  (purification of  $\rho_{ABE}$ )
- Bob has incomplete info:  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) < 1$
- Simple distillation idea: Alice narrows possible  $x$  by public announcement so Bob can distinguish remaining  $\sigma_{BS}^x$ .
- $\approx$  Classical comm. over quantum channel  $\Rightarrow$  use HSW theorem
- Pretend Alice measures  $X_A$  on  $|\psi\rangle_{ABSE}^{\otimes n}$  and then computes  $n[1 - \chi]$  random parities
- Bob can reliably distinguish between the remaining  $2^{n\chi}$  possibilities. **Result is a private state.**
- Parities correspond to  $X^{\mathbf{u}}$  for some random strings  $\mathbf{u}$ .  
Key given by  $Z^{\mathbf{v}}$  for  $\mathbf{v}$ 's such that  $\mathbf{v} \cdot \mathbf{u} = 0$  for all  $\mathbf{u}$
- Just as well measure  $Z$  individually and reconstruct key as  $Z^{\mathbf{v}}$
- Resulting rate =  $\chi(\{\frac{1}{2}, \sigma_{BS}^x\}) = 1 - I(A:E)$

