Continuous Variable Cryptography in the Noisy Storage Model

QCrypt, 1.10.2015

Fabian Furrer
NTT Basic Research Lab

Joint work with:
Christian Schaffner @ University of Amsterdam
Stephanie Wehner @ TU Delft

Preliminary & Motivation

Two Party Cryptographic Protocols

Examples:

1) **Oblivious Transfer:** Alice wants to send Bob exclusively one of two messages s_0, s_1 (bits), while Bob can secretly choose which one he wants to learn.

2) **Bit Commitment**

3) **Secure Password Identification**

Preliminary & Motivation

Two Party Cryptographic Protocols

Distrustful Model: Alice does not trust Bob and vice versa

Preliminary & Motivation

Two Party Cryptographic Protocols

Distrustful Model: Alice does not trust Bob and vice versa

Example:

Oblivious Transfer: Alice inputs wants to send Bob exclusively one of two messages s_0, s_1(bits), while Bob can secretly choose which one he wants to learn.

- Alice does not want Bob to learn both messages
- Bob does not want Alice to know which message he learns

Preliminary & Motivation

- **NO GO THEOREM:** No information theoretical security, even with quantum communication [1]!
- **Computational Assumptions (classical crypto)**
  - Issues: no everlasting security (i.e., breaking it in the future retroactively)
- **Relativistic Constraints (time ordering + non-signaling)**
  - Issues: Can be broken once trusted agent can communicate
- **Constraints on the physical devices, e.g., bounded and noisy storage**
  - Because qm memories are expensive and technologically involved, future proof

[1] H-K. Lo and H. F. Chau, *PRL* 78, 3410, 1997 , Dominic Mayers PRL 78, 3414, 1997
[2] Adrian Kent, *PRL* 83, 1447–1450,1999; Adrian Kent, PRL 109, 130501, 2012; J. Kaniewski, M. Tomamichel, E. Hänggi, and S. Wehner. *IEEE Transactions on Information Theory* 2013

Preliminary & Motivation

Bounded and Nosy Storage Model (previous work)

- **Classical Protocols,** memory bound on adversary [1]

- **Quantum Bounded Storage** [2]
  - Cheating party needs O(n) (n=nr of signals) qm memories while honest party don't need any!
  - Quatum part of protocol similar to BB84

- **Noisy (and Bounded) Quantum Storage based on BB84:**
  - individual storage attack [3]
  - General storage attack, related to the classical capacity of the attackers memory channel [4]
  - Very recently: relation to quantum capacities of the attackers memory [5]

[1] U. Maurer, Journal of Cryptology, 5,53,1992. C. Cachin and U. M. Maurer. Proc of CRYPTO 1997
[2] Ivan B Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. *SIAM Journal on Computing*, 37:1865–1890, 2008; Stephanie Wehner, Christian Schaffner, and Barbara M Terhal PRL 100, 220502, 2008
[3] Stephanie Wehner, Christian Schaffner, and Barbara M Terhal, PRL 100,220502,2008
[4] Robert Konig, Stephanie Wehner, and Jürg Wullschleger, IEEE Trans Inf Th, 58:1962–1984,2012
[5] Mario Berta, Omar Fawzi, and Stephanie Wehner, *Adv in Cryptology CRYPTO 2012*, 7417, 776, 2012;F. Dupuis, O. Fawzi, and S. Wehner, IEEE Trans *Inf Th,* 61, 1093, 2015

Our Contribution

- **First Continuous Variable (CV) Protocol** for two party protocol in the noisy storage model
  - **oblivious transfer** and bit commitment
  - Experimentally feasible (requires CV QKD)
- We relate security to the **classical capacity** of the memory channel
- New Continuous Variable Uncertainty Relations for Smooth Min-Entropy

Why CV

- Easy integration in standard telecom systems
- Efficient measurements at high frequencies via homodyne detection
- On-chip implementations

Outlook

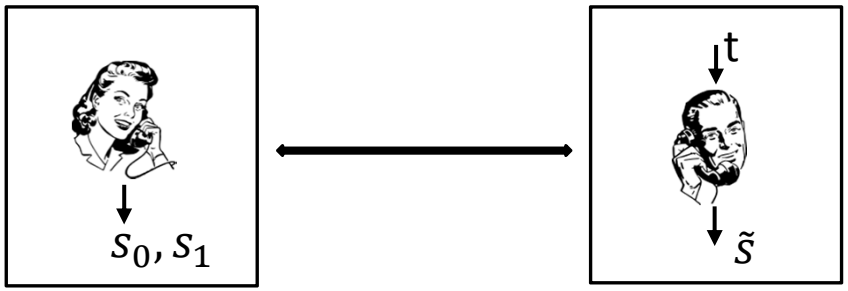
I. Continuous Variable Protocol for Oblivious Transfer (OT) in the noisy storage model

II. Correctness and Security in the noisy storage model

III. Uncertainty Relations for the noisy storage model

IV. Application to Gaussian Bosonic Memory Channel

Oblivious Transfer



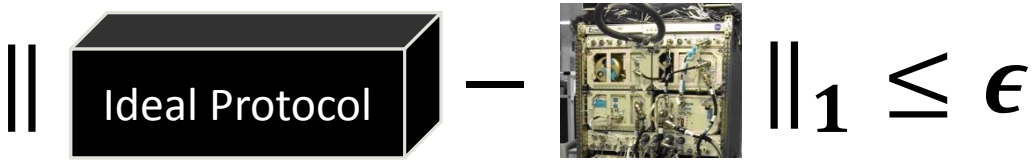
Alice: no input and as output two ℓ-bit strings $s_0, s_1 \in \{0,1\}^\ell$

Bob: input $t \in \{0,1\}$ and output $\tilde{s} \in \{0,1\}^\ell$

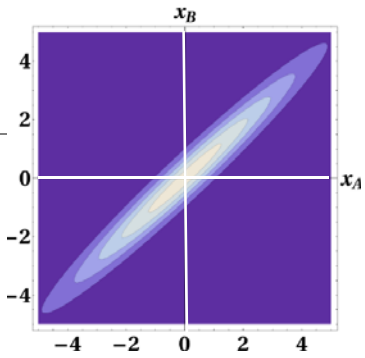
Requirements:

- **Correctness** (both honest): strings s_0, s_1 are random and $\tilde{s} = s_t$
- **Security for Alice** (Alice honest): Bob can only learn one string
- **Security for Bob** (Bob honest): Alice does not learn t

We use **composable security definition** of the above requirements: the protocol is ϵ-indistinguishable from the ideal protocol



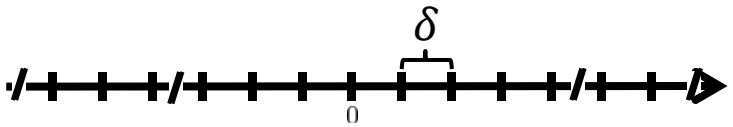
Protocol I: Source & Measurements



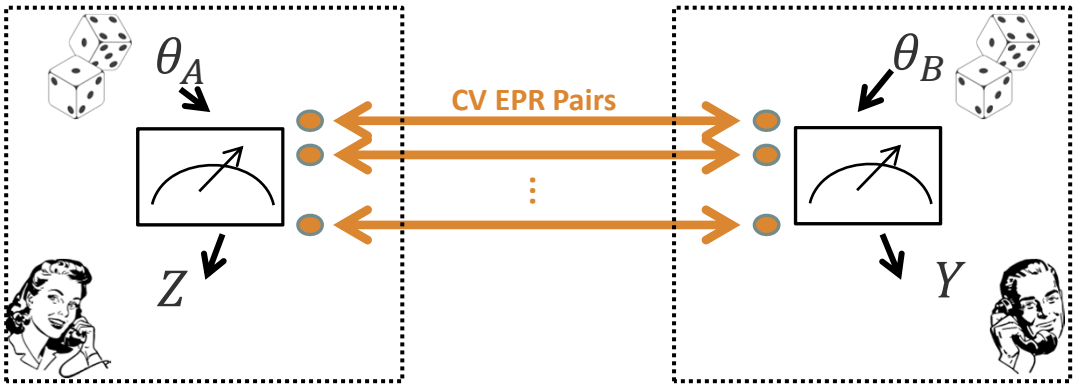
Entanglement based protocol (P&M similar):

- **Source in Alice's Lab:**
  - **CV entangled EPR state** (two mode squeezed states)
  - analog of maximally entangled state for discrete variables
  - X and P quadratures of the two modes are strongly correlated
  - Uncorrelated if the two modes are measured in different quadratures
- **Measurements:**
  - Homodyne detection of the **quadrature X and P** of the em-field:

    $X=a+a^\dagger$, $P=i(a^\dagger-a)$, $[X,P]=2i$
  - **Coarse-graining:** binning into intervals of length δ



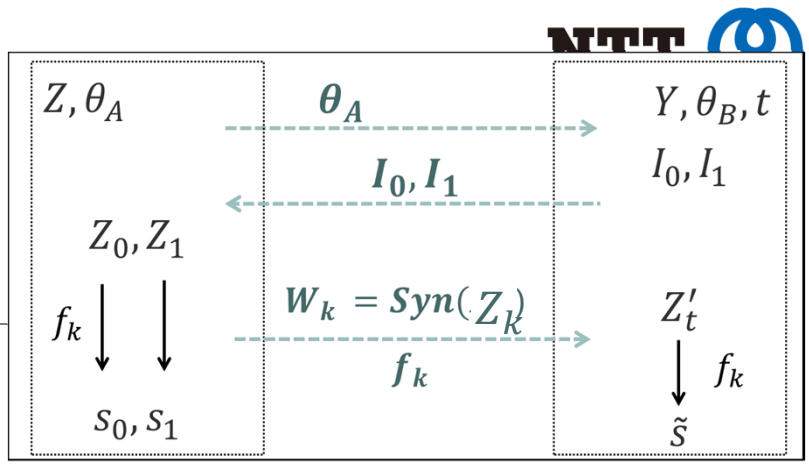
Protocol II: Quantum Part (like QKD)



1) Alice distributes n CV EPR Pairs
2) Alice and Bob measure coarse-grained **X and P uniformly at random** $\boldsymbol{\theta_A} \in_R \{\mathbf{0},\mathbf{1}\}^n$ **and** $\boldsymbol{\theta_A} \in_R \{\mathbf{0},\mathbf{1}\}^n$ **(0 → X and 1 → P)** obtaining outcomes Z and Y, respectively.
3) They **wait time Δt**

Important Property: Outcomes in Z for which Alice's and Bob's measurement choice coincide are highly correlated, and the others are uncorrelated

Protocol III



Classical Part of Protocol[1]:

1) Alice sends θ_A

2) Bob defines $I_t = \{i \,|\theta_A^i = \theta_B^i\}$ and its compliment I_{1-t} and sends I_0, I_1 to Alice

3) Alice divides Z into substrings Z_0, Z_1 according to I_0, I_1

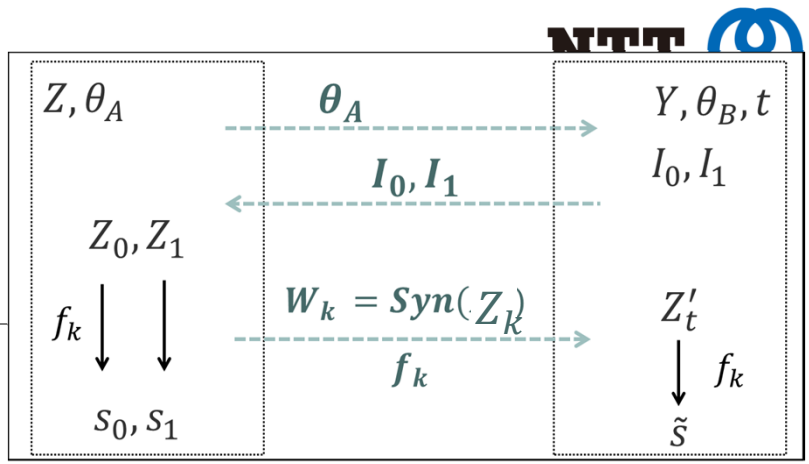
4) Alice sends error correction (EC) syndromes W_0, W_1 for Z_0, Z_1 and Bob corrects Y_t using W_t, to obtain Z'_t $(= Z_t$ with high probability)

5) Alice applies hash functions f_0, f_1 and outputs $s_k = f_k(Z_k)$

6) Bob outputs $\tilde{s} = f_t(X'_t)$

I_t= correlated outcomes
I_{1-t}= uncorrelated outcomes

Correctness



Classical Part of Protocol[1]:

1) Alice sends θ_A

2) Bob defines $I_t = \{i \,|\theta_A^i = \theta_B^i\}$ and its compliment I_{1-t} and sends I_0, I_1 to Alice

3) Alice divides Z into substrings Z_0, Z_1 according to I_0, I_1

4) Alice sends error correction (EC) syndromes W_0, W_1 for Z_0, Z_1 and Bob corrects Y_t using W_t, to obtain Z'_t $(= Z_t$ with high probability)

5) Alice applies hash functions f_0, f_1 and outputs $s_k = f_k(Z_k)$

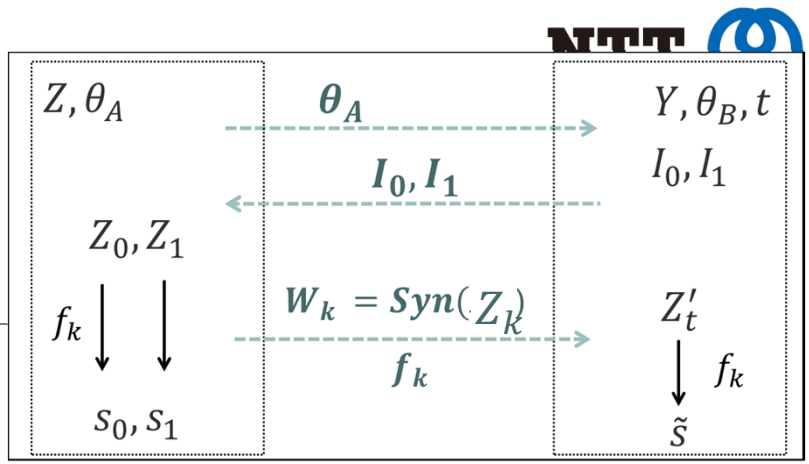
6) Bob outputs $\tilde{s} = f_t(X'_t)$

I_t= correlated outcomes
I_{1-t}= uncorrelated outcomes

Correctness of the Protocol:

- Alice's and Bob's outcomes Z and Y restricted to I_t (i.e., Z_t, Y_t) are highly correlated.
- Given error correction information W_t, Bob can correct Y_t to obtain $Z'_t = Z_t$.
- Hence, $\tilde{S} = f_t(Z'_t) = f_t(Z_t) = S_t$

Security for Bob



Classical Part of Protocol[1]:

1) Alice sends θ_A

2) Bob defines $I_t = \{i \,|\theta_A^i = \theta_B^i\}$ and its compliment I_{1-t} and sends I_0, I_1 to Alice

3) Alice divides Z into substrings Z_0, Z_1 according to I_0, I_1

4) Alice sends error correction (EC) syndromes W_0, W_1 for Z_0, Z_1 and Bob corrects Y_t using W_t, to obtain Z'_t $(= Z_t$ with high probability)

5) Alice applies hash functions f_0, f_1 and outputs $s_k = f_k(Z_k)$

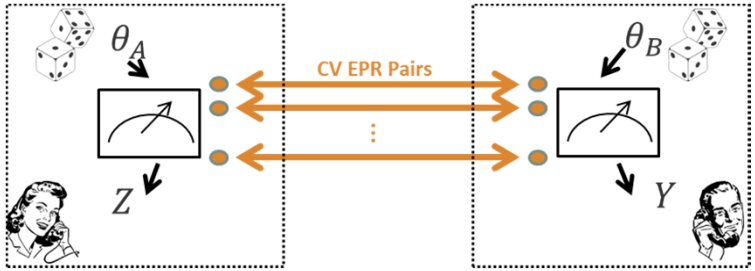
6) Bob outputs $\tilde{s} = f_t(X'_t)$

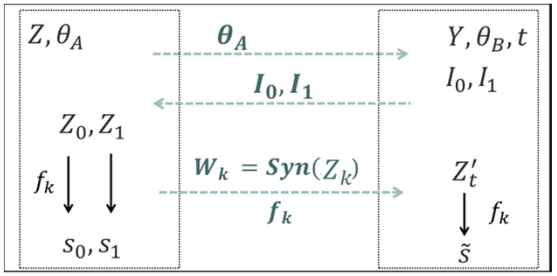
I_t= correlated outcomes
I_{1-t}= uncorrelated outcomes

Security for Bob:

- The only classical and quantum information Bob sends to Alice during the protocol is I_0, I_1 which are uncorrelated to t

Security for Alice

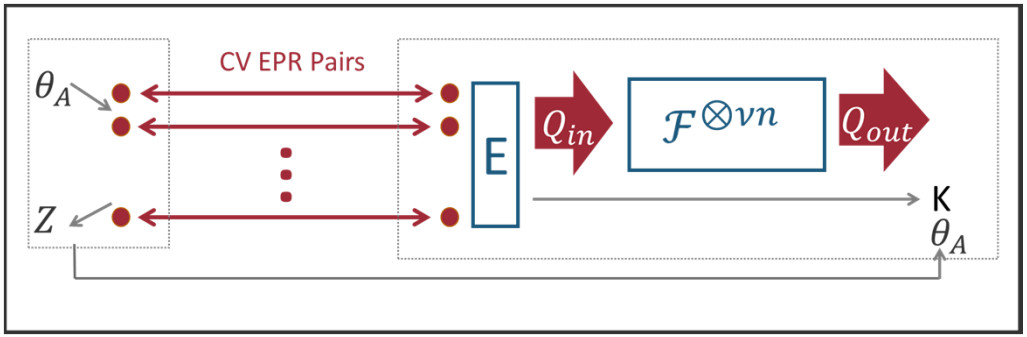




Observation:

- If Bob can measure all his signals in the same basis as Alice, he learns both strings s_0, s_1
- He can do this if he has a quantum memory to store all n modes over a time Δt until he receives Alice's measurement choices θ_A.
- **But what if Bob has only a limited quantum memory capacity, i.e., in the noisy storage model?**

Attacks in the Noisy Memory Model



Assumption:

- Bob has νn quantum channels $\mathcal{F}$
- E is an encoding that is assumed in the following to be either
  - an arbitrary quantum channel
  - a Gaussian quantum channel
  - a quantum channel that acts identical and individual on the signals (or a very limited number of signals)
- After time Δt Bob receives Alice's measurement choice θ_A

Result I

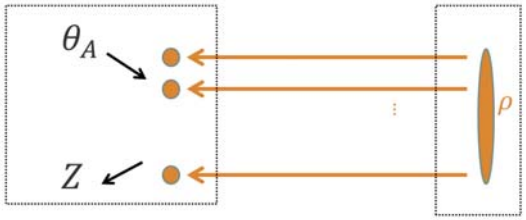
We show security of the OT protocol depending on [1]:

- The **classical strong converse capacity** of Bob's memory $C_{SC}(\mathcal{F})$

> $C_{SC}(\mathcal{F})$ is the rate above which the probability to successfully send classical information through $\mathcal{F}$ decays exponentially (decay rate ξ): $P_{succ}^{\mathcal{F}}(nR) \leq 2^{-n\xi(R-C_{SC}(\mathcal{F}))}$

- The **uncertainty rate** $\lambda^{\epsilon}(n,\delta)$ that can be generated by CV measurements in terms of the smooth min-entropy (n = number of signals, δ=spacing of homodyne meas.)

$\frac{1}{n} H_{min}^{\epsilon}(Z|\theta_A) \geq \lambda^{\epsilon}(n,\delta)$, where



[1] Robert Konig, Stephanie Wehner, and Jürg Wullschleger, IEEE Trans Inf Th, 58:1962–1984,2012; Christian Schaffner, *PRA* 82, 032308, 2010

Result I

Security for Alice can be achieved for sufficiently large n if

$$r_{OT} := 1/2(\lambda^{\epsilon}(n,\delta) - r_{EC}) - \nu C_{SC}(\mathcal{F}) > 0$$

Moreover, the length of the string $\ell = |S_0| = |S_1|$ is given by

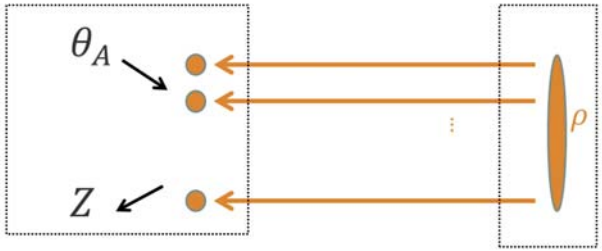
$$\ell = n\xi r_{OT} - \mathcal{O}(\log 1/\epsilon)$$

- $C_{SC}(\mathcal{F})$= strong converse rate
- $\lambda^{\epsilon}(\mathrm{n},\delta)$ = uncertainty rate
- $r_{EC} = \frac{1}{n}\log|W_0 W_1|$ = error correction rate
- ϵ is of the order of the composable security parameter

Take Home Message:

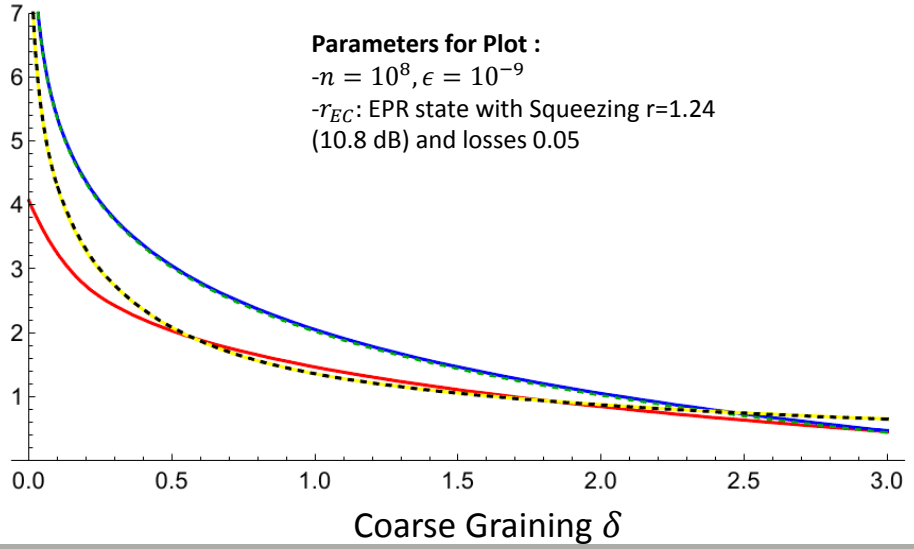
uncertainty rate – error correction rate > 2 x effective classical capacity

Uncertainty Rate (Result II)



We derive 3 different Uncertainty Relations: $H_{min}^{\epsilon}(Z|\theta_A) \geq n\lambda^{\epsilon}(n,\delta)$

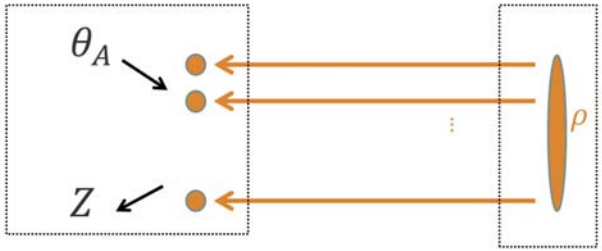
1) No assumptions: using majorization techniques similar to [1]
2) For Gaussian states (i.e., Gaussian encoding attacks) : based on continuous approximations
3) For tensor product states (IID) (i.e. individual encodings): using the asymptotic equipartition property [2]



Parameters for Plot :
-$n = 10^8, \epsilon = 10^{-9}$
-r_{EC}: EPR state with Squeezing r=1.24 (10.8 dB) and losses 0.05

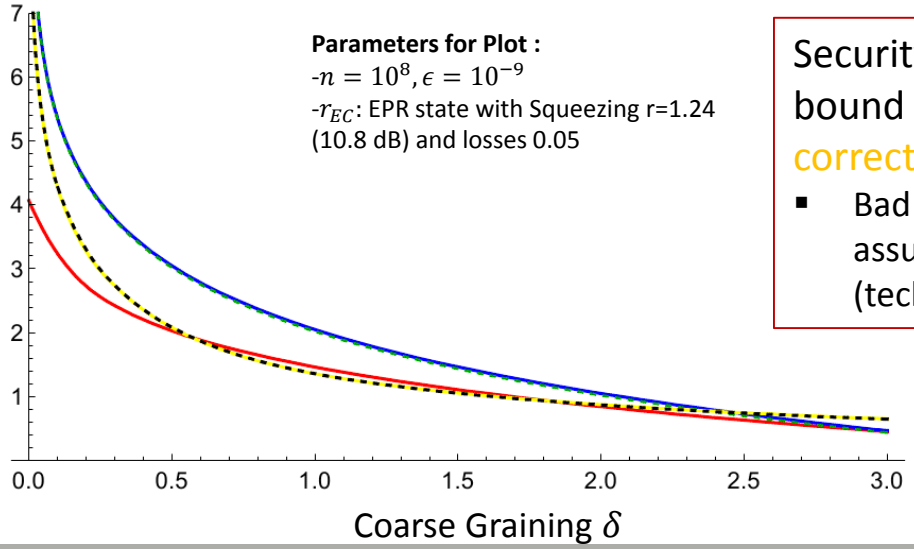
[1] Ł. Rudnicki, PRA 91, 032123,2015
[2] FF, J. Aberg, and R. Renner, CMP 306, 165,2011

Uncertainty Rate (Result II)



We derive 3 different Uncertainty Relations: $H_{min}^{\epsilon}(Z|\theta_A) \geq n\lambda^{\epsilon}(n,\delta)$

1) No assumptions: using majorization techniques similar to [1]
2) For Gaussian states (i.e., Gaussian encoding attacks) : based on continuous approximations
3) For tensor product states (IID) (i.e. individual encodings): using the asymptotic equipartition property [2]



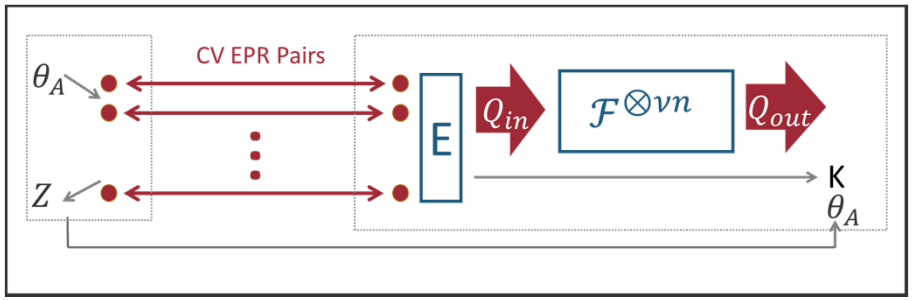
Parameters for Plot :
-$n = 10^8, \epsilon = 10^{-9}$
-r_{EC}: EPR state with Squeezing r=1.24 (10.8 dB) and losses 0.05

Security for OT: if the uncertainty bound is above the yellow line (error correction rate)

- Bad memories required without any assumptions on the memory attacks (technical problem)

[1] Ł. Rudnicki, PRA 91, 032123,2015
[2] FF, J. Aberg, and R. Renner, CMP 306, 165,2011

Discussion of Security for Gaussian Memory Channels

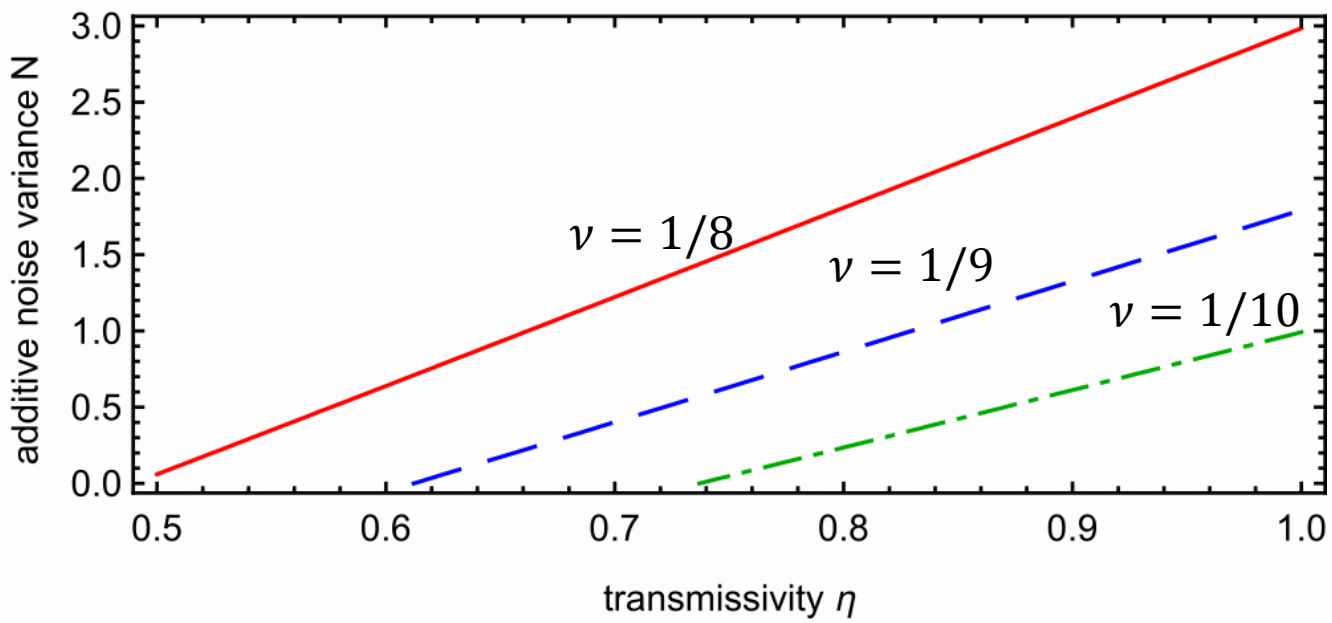


- $\mathcal{F}$ **= one mode bosonic Gaussian channel:** loss channel with **transmissivity** τ and additive Gaussian **noise with variance** V_N
- Strong converse classical capacity for phase insensitive one mode Gaussian channel known (recent results [1])
- Requires a maximal photon number constraint N_{max} (i.e., each encoding has only non negligible support on subspace with less than N_{max} photons)[2]

[1] V. Giovannetti, A. Holevo, and R. Garcia-Patron, arXiv:1312.2251 (2013), V. Giovannetti, R. Garcia-Patron, N. Cerf, and A. Holevo, arXiv:1312.6225 (2013)
[2]

Security under Gaussian Memory Attacks

Left side of the lines are secure regions (plots = equality in condition)



- EPR state with squeezing of 10.8 dB and 5% losses on Bob's mode.
- Error Correction Efficiency 0.96
- Nmax = 30
- Protocol Parameters: $n = 10^8$, $\epsilon_s = 10^{-9}$

Summary

- Protocol for OT (and BC) based on optical CV systems (exper. feasible, needs no quantum memory)
- Security in the noisy storage model:

uncertainty rate – error correction rate > 2 x effective classical capacity

- New Uncertainty Relations for CV Systems
- Discussion of security for practical memory channels

Open Problems

- Need better uncertainty relations without assumptions
- Reduction to quantum capacities of the memory channels