High rate quantum cryptography with untrusted relay: Theory and experiment

CARLO OTTAVIANI
Department of Computer Science, The University of York (UK)

1st TWQI Conference – Ann Arbor  27-3 July 2015
In collaboration with:

- Stefano Pirandola
- Sam Braunstein
- Gaetana Spedalieri
- Seth Lloyd
- Christian Weedbrook
- Tobias Gehring
- Christian S. Jacobsen
- Ulrik L. Andersen

Outline

- Measurement-device independence (MDI)
- Protocol with continuous variables (CVs)
  - Reduction of the general attack
  - Secret-key rate and security distances
  - Symmetric configuration
  - Optimal configuration
- Experimental results
- Conclusions and outlook
Measurement-device independence

- Alice: Private space
- Relay (Eve): Random states
- Public channel: Measurement
- Bob: Private space

References:

- Braunstein & Pirandola
  PRL 108, 130502 (2012)
  Arbitrary systems & measurements (quantum instruments)

- Lo, Curty & Qi
  PRL 108, 130503 (2012)
  Qubit regime (decoy states, Bell detection)
Continuous Variables

Next step: MDI quantum cryptography with Continuous Variables

Why?

Cheap quantum sources (amplitude-modulated coherent states)
Efficient homodyne detectors which can also go broadband

High rates compared to discrete variables (qubits)

Working mechanism with CVs

\[ \gamma := \frac{q_- + ip_+}{\sqrt{2}} \]

Two main ingredients:

- Gaussian-modulated coherent states
- CV Bell detection (balanced beamsplitter + homodynes)

Working mechanism with CVs

Relay creates correlations

\[ \gamma = \alpha - \beta^* + \text{noise} \]

Alice and Bob share information

\[ I(\alpha, \beta | \gamma) > 0 \]

Eve cannot eavesdrop from \( \gamma \): \[ I(\alpha | \gamma) = I(\beta | \gamma) = 0 \]
General Attack: Joint on links and relay

Eve cannot eavesdrop from $\gamma$:

$$I(\alpha \mid \gamma) = I(\beta \mid \gamma) = 0$$

For a given observed statistics $p(\alpha, \beta, \gamma)$, Alice and Bob can assume that:

Simulator = Bell detection

(we bound Eve with the Holevo information which is unitarily invariant, so that we can play with $U$)
Reduction of the joint attack: Coherent Gaussian attack

Coherent attack of the links

Gaussian protocol $\rightarrow \mathbf{U}$ Gaussian unitary

(Coherent Gaussian attack)
Coherent Gaussian attack

Realistic attack

\[
V_{E_1,E_1} = \begin{pmatrix}
\omega_A I & G \\
G & \omega_B I
\end{pmatrix}
\]

\[
G = \begin{pmatrix} g \\ g' \end{pmatrix}
\]
Since local detections commute, we can consider the conditional states after the Bell detection of the relay.
Security Analysis

Alice and Bob’s mutual information

\[ I(\alpha : \beta) = \log_2 \frac{\mu}{\chi} \]

- Variance of modulation \( \mu >> 1 \)
- Equivalent noise \( \chi = \chi_L + \epsilon \)

\[ R = \xi I(\alpha : \beta) - I(\alpha : E) \]

Eve’s Holevo information

\[ \Phi_{abE|\gamma}, \rho_{E|\gamma}, \rho_{ab|\gamma} \]

Alice \( \alpha \) (\( a \)) \( \beta \) Bob (\( b \)}
Secret-key rate

\[
R(\tau_A, \tau_B, \chi) = \log_2 \frac{2(\tau_A + \tau_B)}{e |\tau_A - \tau_B| \chi} + h(x) - h(y)
\]

\[
x = \frac{\tau_A \chi}{\tau_A + \tau_B} - 1 \quad y = \frac{\tau_A \tau_B \chi - (\tau_A + \tau_B)^2}{|\tau_A - \tau_B| \tau_A + \tau_B}
\]

\[
\xi = 1
\]

Function of the transmissivities and the equivalent noise

\[
h(x) = \frac{x+1}{2} \log_2 \frac{x+1}{2} - \frac{x-1}{2} \log_2 \frac{x-1}{2}
\]

\[ \omega_A = \omega_B = \omega \quad \tau_A = \tau_B = \tau \]

\[ R = \log_2 \frac{\tau^2}{\sqrt{\lambda \lambda'(\tau + \lambda)(\tau + \lambda')}} + h \left[ \frac{\sqrt{(\tau + 2\lambda)(\tau + 2\lambda')}}{\tau} \right] \]

\[ \lambda = (1 - \tau)(\omega - g) + \frac{1 - \eta}{\eta} \]
\[ \lambda = (1 - \tau)(\omega + g') + \frac{1 - \eta'}{\eta'} \]

CO, G. spedalieri, S.L. Braunstein, S. Pirandola, PRA 91, 022320 (2015)
Joint symmetric attacks

Collective Attacks:
(1) $g' = g = 0$

Separable Attacks:
(2), (3), (4) $g' = g = \pm (\omega - 1)$

EPR Attacks:
(5), (6) $g' = -g = \pm \sqrt{\omega^2 - 1}$

(6) is optimal!
EPR attack, (6), is optimal!

CO et al., PRA 91, 022320 (2015)
Maximum Performance: pure loss

\[ R(\tau_A, \tau_B) = \log_2 \left[ \frac{\tau_A \tau_B}{e |\tau_A - \tau_B|} \right] + h \left( \frac{2}{\tau_B} - 1 \right) - h \left( \frac{2 - \tau_A - \tau_B}{|\tau_A - \tau_B|} \right) \]

\[ R(\tau_A, \tau_B) = \log_2 \left[ \frac{\tau_A \tau_B}{e |\tau_A - \tau_B|} \right] + h \left( \frac{2}{\tau_B} - 1 \right) - h \left( \frac{2 - \tau_A - \tau_B}{|\tau_A - \tau_B|} \right) \]

See also Preprint arXiv:1312.4104
Robustness to excess noise

\[ \chi = \chi_L + \epsilon \]

- \( \epsilon = 0 \)
- \( \epsilon = 0.1 \)

\( d \) (km)

Max distance

Insecure \( (R<0) \)

(\( R>0 \))

Experimental Setup
(Christian S. Jacobsen, Tobias Gehring, Ulrik L. Andersen)

see also arXiv:1312.4104
Experimental Results

Parameters: Excess noise 0.01; $\varphi = 60$ SNU

- Figure a: (i) $\tau_A = 0.98$
- Figure b: (ii) $\tau_A = 0.975$
- Figure c: (iii) $\tau_A = 0.935$

Nature Photonics, 9, 397-402, (2015)
Few points on CV experiments I

- Cheap room temperature components (optical modulators ad homodyne detections)
- Regime of parameters easily achievable in practice
- Gaussian modulation ~ 60 shot noise units (easy)
- CV Bell detection efficiency routinely high ($\eta \sim 98\%$) and can be done in free space
- Reconciliation efficiency $\xi \sim 97\%$ state-of-the-art
- Excess-noise in our experiment is $\varepsilon \sim 0.01$

arXiv:1506.06748 for more visit Stefano’s Poster
• Our experimental rate is a lower bound

• The theoretical rate is optimal

• Finite-size effects and composable security support our experimental results

• The relay doesn’t need to be in Alice’s Lab

• Interfering signals from independent laser sources is no longer a security issue or major experimental challenge in CV-QKD

• Fast time-resolved homodyne detectors are available with bandwidths of 100MHz and more

arXiv:1506.06748 for more visit Stefano’s Poster
A comparison CVs-DVs

arXiv:1506.06748 for more visit Stefano’s Poster
Typical network topology

Mobile device connecting to a public access point
Conclusions

A conceptual advance

Untrusted relays versus the trusted relays used in the current network prototypes (SECOQC, Tokyo network…)

Our untrusted relay performs cheap operations with all the complexity left to the end-users

First steps towards the realization of the end-to-end principle in a quantum network over metropolitan distances

Outlook:

• More complex structures with less trusted nodes
• Extension to thermal-QKD: to use different frequencies for mixed technology platforms (microwave/infrared)
Thx for your attention