Quantum Cryptography

Arnav Metrani

IISER Mohali

11th January 2025

Zero-Knowledge Proof

- You have a red cube and a green cube. You (not-colourblind) wish to convince your friend (colourblind) that the cubes are not of the same colour (ie. RR,GG) without them finding out which cube is which. How would you do it?

Zero-Knowledge Proof

- Tell your friend to hold the cubes behind their back (out of sight)

Zero-Knowledge Proof

- Tell your friend to hold the cubes behind their back (out of sight)
- Your friend chooses which cube to show you, and is free to swap the cubes behind their back.

Zero-Knowledge Proof

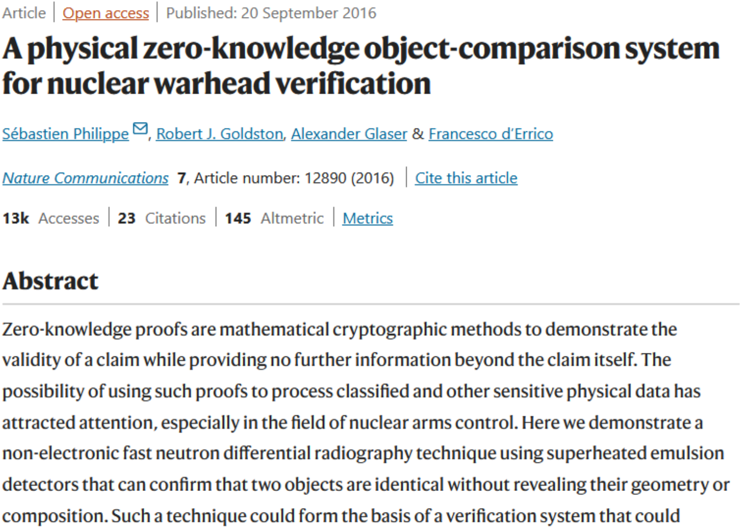
- Tell your friend to hold the cubes behind their back (out of sight)
- Your friend chooses which cube to show you and is free to swap the cubes behind their back as well.
- You (not-colourblind) correctly tell whether the same cube was shown to you as the last time, or if it is a different cube.

Zero-Knowledge Proof

- Tell your friend to hold the cubes behind their back (out of sight)
- Your friend chooses which cube to show you and is free to swap the cubes behind their back as well.
- You (not-colourblind) correctly tell whether the same cube was shown to you as the last time, or if it is a different cube.
- Since your friend knows whether they swapped or not, the probability of you guessing correctly if they were the same colour would be $1/2^n$.

Zero-Knowledge Proof: Applications?

Nuclear disarmament. **(Link)**



Article | Open access | Published: 20 September 2016

A physical zero-knowledge object-comparison system for nuclear warhead verification

Sébastien Philippe ✉, Robert J. Goldston, Alexander Glaser & Francesco d'Errico

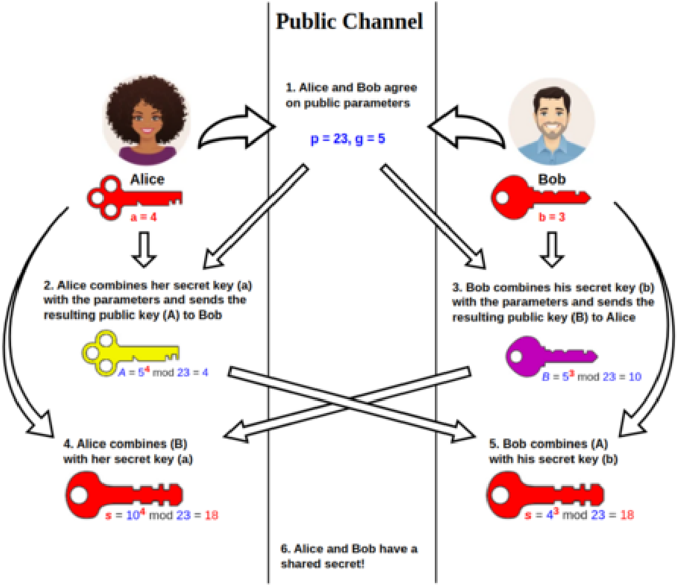
Nature Communications **7**, Article number: 12890 (2016) | Cite this article

13k Accesses | **23** Citations | **145** Altmetric | Metrics

Abstract

Zero-knowledge proofs are mathematical cryptographic methods to demonstrate the validity of a claim while providing no further information beyond the claim itself. The possibility of using such proofs to process classified and other sensitive physical data has attracted attention, especially in the field of nuclear arms control. Here we demonstrate a non-electronic fast neutron differential radiography technique using superheated emulsion detectors that can confirm that two objects are identical without revealing their geometry or composition. Such a technique could form the basis of a verification system that could

Diffie–Hellman key exchange



1. Alice and Bob agree on public parameters

2. Alice combines her secret key (a) with the parameters and sends the resulting public key (A) to Bob

3. Bob combines his secret key (b) with the parameters and sends the resulting public key (B) to Alice

4. Alice combines (B) with her secret key (a)

5. Bob combines (A) with his secret key (b)

6. Alice and Bob have a shared secret!

One-time pad

Let us say that A wants to send the message $M \in \{0,1\}^x$ to B.
A and B share a completely random bitstring $K \in \{0,1\}^y$.
Ensuring that x=y, A encodes its message into the cipher text $C = M \oplus K$.
B receives the cipher text and applies the same bitwise XOR operation.
Since $C \oplus K = K \oplus M \oplus K = M$, B is able to decode the message.

One time pad: Security

This system is perfectly secret if knowing the ciphertext gives out no information about the message. We can quantify this in the following manner:

Let us say that A can transmit any of the plaintexts m as a message M, and the probability of A transmitting the plaintext m is given by $P(M = m)$.

Now, if we wish to transmit a plaintext m and choose a random key k, then the ciphertext will be $c = m \oplus k$ $(C = c)$.

We can now restate the earlier statement on perfect security as

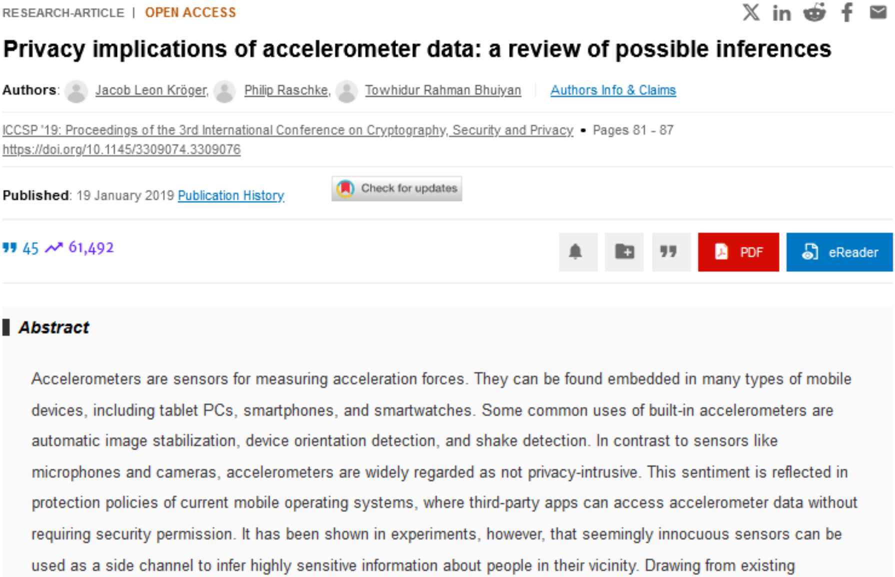
$$P(M = m|C = c) = P(M = m)$$

SEND
CASH

TEMPEST

(Link)

(Link)



Privacy implications of accelerometer data: a review of possible inferences

Authors: Jacob Leon Kröger, Philip Raschke, Towhidur Rahman Bhuiyan | Authors Info & Claims

ICCSP '19: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy • Pages 81 - 87
https://doi.org/10.1145/3309074.3309076

Published: 19 January 2019 Publication History

Abstract

Accelerometers are sensors for measuring acceleration forces. They can be found embedded in many types of mobile devices, including tablet PCs, smartphones, and smartwatches. Some common uses of built-in accelerometers are automatic image stabilization, device orientation detection, and shake detection. In contrast to sensors like microphones and cameras, accelerometers are widely regarded as not privacy-intrusive. This sentiment is reflected in protection policies of current mobile operating systems, where third-party apps can access accelerometer data without requiring security permission. It has been shown in experiments, however, that seemingly innocuous sensors can be used as a side channel to infer highly sensitive information about people in their vicinity. Drawing from existing

No-Cloning Theorem

The no-cloning theorem states that it is impossible to create an independent copy of an unknown state.

This proof shows that no such unitary operation exists for a pure state.

Let there exist a unitary operation s.t.

$$U\,|\psi\rangle|\,E\rangle = |\psi\rangle|\,\psi\rangle$$

Then $U\,|0\rangle|\,E\rangle = |0\rangle|\,0\rangle$, $U\,|1\rangle|\,E\rangle = |1\rangle|\,1\rangle$.
Now let $|\psi\rangle = \alpha|\,0\rangle + \beta\,|1\rangle, |\,\alpha\,|^2 + |\,\beta|^2 = 1$.
Applying this unitary cloning operator gives:

$$U\,(\alpha\,|0\rangle + \beta|\,1\rangle)\,|E\rangle = \alpha\,|00\rangle + \beta|\,11\rangle$$

However:

$$|\psi\rangle|\,\psi\rangle = \alpha^2\,|00\rangle + \alpha\beta|\,01\rangle + \alpha\beta\,|10\rangle + \beta^2|\,11\rangle$$

If α and β are non-zero, we get a contradiction. Thus proven.

Purification

Given a mixed state ρ_S, by coupling with another system T we can obtain a pure state in $\mathcal{H}_S \otimes \mathcal{H}_T$.
Let $\rho_S = \sum_i p_i \left|i_S\right\rangle\!\left\langle i_S\right|$.

Then $\Big|ST\Big\rangle = \sum_i \sqrt{p_i}\Big|\, i_S\Big\rangle\Big|i_T\Big\rangle$ will be a pure state.

We can obtain the mixed state back by taking the partial trace of system T $tr_T\left(|ST\rangle\langle ST|\right)$.
If we assume that there exists a unitary cloning operator for mixed states $U\left(\rho_{system} \otimes \rho_{env}\right) U^{\dagger} = \rho_{system} \otimes \rho_{system}$, then we should be able to couple the system with another system R to purify it, thus obtaining a universal unitary cloning operator for pure states. But since we have shown it's impossible for pure states, we get a contradiction.

Stinespring Dilation

Given a quantum operation $\mathcal{E}(\rho)$ which need not be unitary, by coupling it with the environment we can define the quantum operation as a unitary operator in the combined space, and since we assume the environment does not interact with the system after the operation we can get the state of the system by tracing out the environment.

$\mathcal{E}(\rho) = tr_{env}\left[U\left(\rho_{system} \otimes \rho_{env}\right)U^{\dagger}\right].$

If we assume that there exists a non-unitary cloning operator, via Stinespring Dilation we can convert the non-unitary operator to a unitary one by coupling a ‘dummy’ system to our qubit system. After this, the proof by contradiction follows for the mixed states.

Indistinguishability of non-orthogonal states on measurement

Given $|\psi\rangle$ and $|\phi\rangle$, if $\langle\psi|\phi\rangle \neq 0$, then we cannot deterministically tell which state we have received.
(Helstrom measurement)

Non-orthogonal states cannot be distinguished without disturbance

Let us assume we want to obtain information regarding the non-orthogonal states $|\psi\rangle$ and $|\varphi\rangle$. We could do this by devising a unitary operator which does the following:

$$U\left(|\psi\rangle|E\rangle\right) = |\psi\rangle|v\rangle, U\left(|\varphi\rangle|E\rangle\right) = |\varphi\rangle|v'\rangle$$

Where $|E\rangle$ is a pre-defined state from our 'interceptor' system. Since the unitary operator results in different independent states for each of the non-orthogonal states, we can then analyse the states separately.

However, if we now take the inner products of the inputs and the outputs:

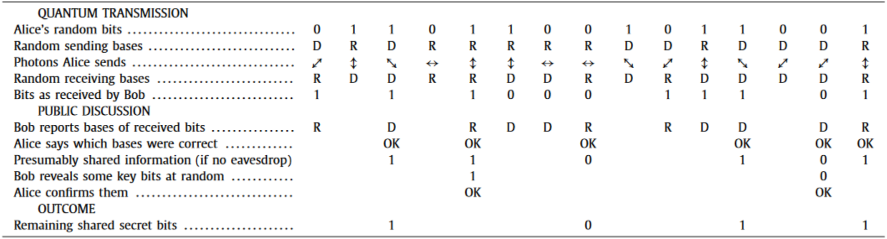
$$\left(\langle\varphi|\langle E|\right) U^\dagger U\left(|\psi\rangle|E\rangle\right) = \langle\varphi|\psi\rangle\langle E|E\rangle = \langle\varphi|\psi\rangle\langle v'|v\rangle$$
$$\langle E|E\rangle = \langle v'|v\rangle$$

Which implies $|v\rangle$ and $|v'\rangle$ but be identical, giving us no information. We can use Stinespring dilation to extend this proof to non-unitary quantum operations.

Holy trinity of QKD no-go theorems

- You can't make copies.
- States which share similaries cannot be differentiated.
- You can't know a state without disturbing it.

BB84 Protocol



QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Weak Coherent Pulses (WCP)

$$p\left(\text{k photons in pulse}\right) = \frac{e^{-\mu}\mu^k}{k!}$$

(Link)

Differential Phase Shift QKD

(Paper link)

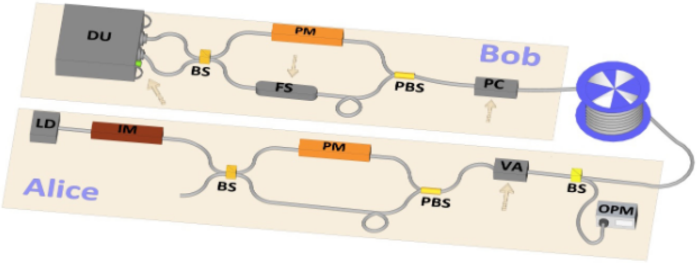
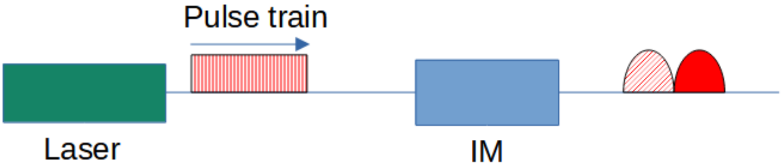
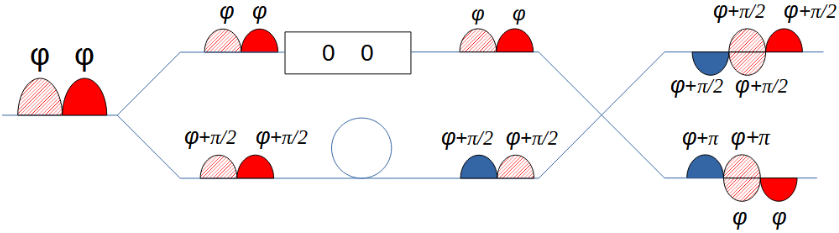


Fig. 1. Experimental setup for the T12 protocol. In Alice's layout, light pulses are emitted by a 1550 nm laser diode (LD), pulsed at 1 GHz, and transmitted through an intensity modulator (IM) and an unbalanced Mach-Zehnder interferometer. This is composed by a fibre-integrated beam-splitter (BS), a phase modulator (PM) and a final polarising BS (PBS). A variable attenuator (VA) is used to set the intensity of the pulses at the desired level. An optical power meter (OPM) measures the total flux in the fibre and adjust the VA in real-time in order to keep it constant. After a fibre spool of different lengths, the light passes through a polarization control (PC) and a second interferometer that matches Alice's. In one arm, a fibre-stretcher (FS) is used to match the arms length between the two distant interferometers, thus generating interference at the final BS. Pulses are eventually measured by a detection unit (DU).

Differential Phase Shift QKD



Differential Phase Shift QKD



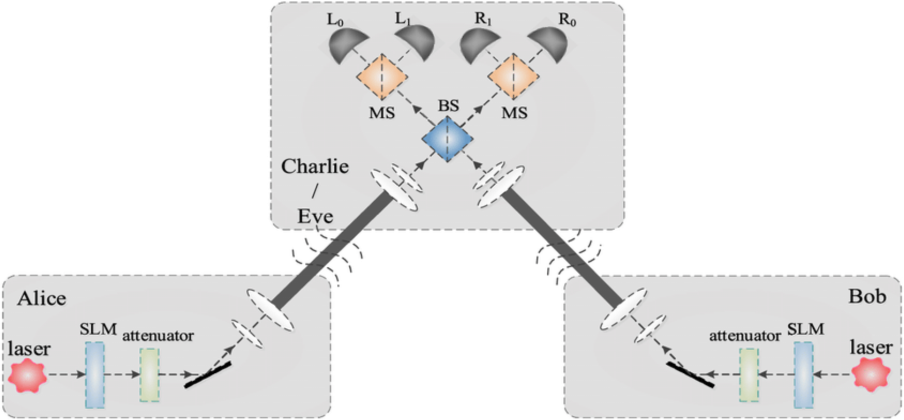
Post-processing

- Error Correction
- Parameter Estimation
- Privacy Amplification

Measurement Device Independent QKD

(Detector attacks)

MDI-QKD Protocol:



Measurement Device Independent QKD

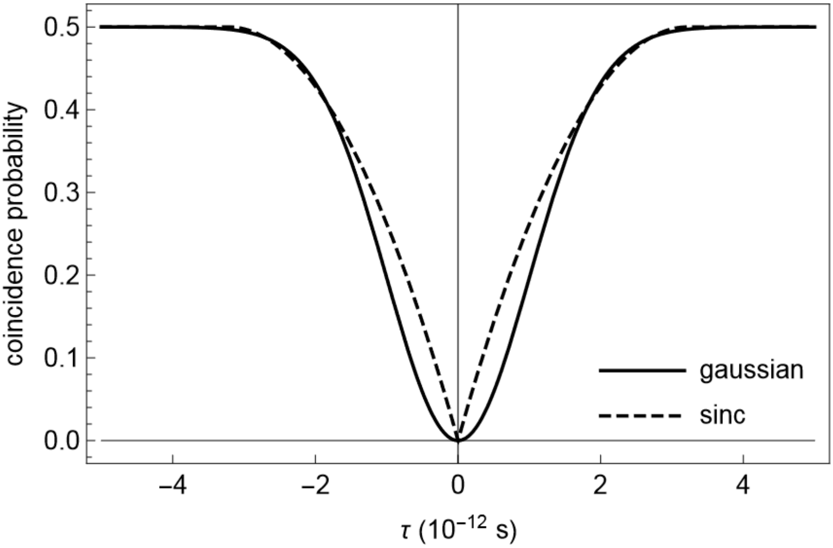
HOM effect:

$$|1\rangle_A|1\rangle_B = \hat{a}_A^\dagger \hat{a}_B^\dagger|0\rangle_A|0\rangle_B = \frac{1}{2}\left[i\hat{a}_C^\dagger\hat{a}_C^\dagger + \hat{a}_C^\dagger\hat{a}_D^\dagger - \hat{a}_D^\dagger\hat{a}_C^\dagger + i\hat{a}_D^\dagger\hat{a}_D^\dagger\right]|0\rangle_c|0\rangle_D$$

$$= \frac{i}{\sqrt{2}}|2\rangle_c|0\rangle_D + |0\rangle_C|2\rangle_D]$$

This only holds if the input photons are indistinguishable (polarization, temporally, spatially).

Measurement Device Independent QKD



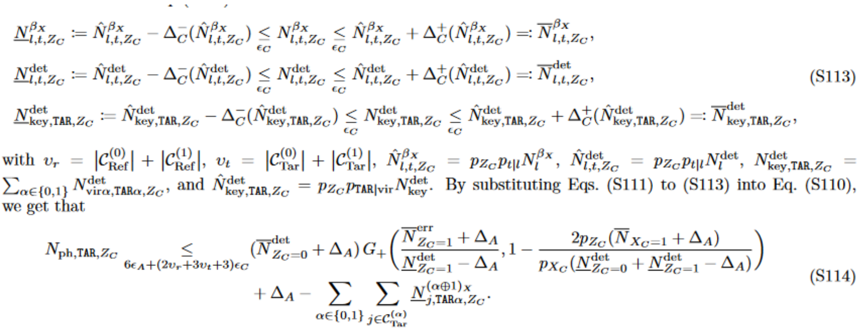
Open Problems

$$r' = H_\xi\left(X|E\right) - \frac{\mathsf{leak}_{EC} + \Delta}{n}$$

Where $\Delta = 2\lg(\frac{1}{2\left[\varepsilon - \overline{\varepsilon} - \varepsilon_{EC}\right]}) + 7\sqrt{n\lg(\frac{2}{\overline{\varepsilon} - \overline{\varepsilon}'})}$

$$H_\xi\left(X|E\right) = \min_{\sigma_{\overline{XE}} \in \Gamma_\xi} H\left(\overline{X}|\overline{E}\right)$$

Open Problems

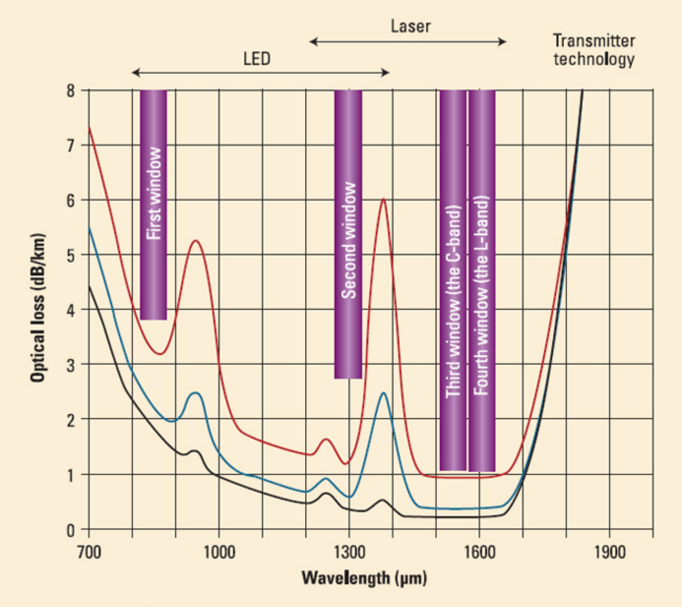


$$\begin{aligned}
\underline{N}^{\beta x}_{l,t,Z_C} &\coloneqq \hat{N}^{\beta x}_{l,t,Z_C} - \Delta^{-}_{C}(\hat{N}^{\beta x}_{l,t,Z_C}) \underset{\epsilon_C}{\leq} N^{\beta x}_{l,t,Z_C} \underset{\epsilon_C}{\leq} \hat{N}^{\beta x}_{l,t,Z_C} + \Delta^{+}_{C}(\hat{N}^{\beta x}_{l,t,Z_C}) \eqqcolon \overline{N}^{\beta x}_{l,t,Z_C}, \\
\underline{N}^{\mathrm{det}}_{l,t,Z_C} &\coloneqq \hat{N}^{\mathrm{det}}_{l,t,Z_C} - \Delta^{-}_{C}(\hat{N}^{\mathrm{det}}_{l,t,Z_C}) \underset{\epsilon_C}{\leq} N^{\mathrm{det}}_{l,t,Z_C} \underset{\epsilon_C}{\leq} \hat{N}^{\mathrm{det}}_{l,t,Z_C} + \Delta^{+}_{C}(\hat{N}^{\mathrm{det}}_{l,t,Z_C}) \eqqcolon \overline{N}^{\mathrm{det}}_{l,t,Z_C}, \\
\underline{N}^{\mathrm{det}}_{\mathrm{key},\mathtt{TAR},Z_C} &\coloneqq \hat{N}^{\mathrm{det}}_{\mathrm{key},\mathtt{TAR},Z_C} - \Delta^{-}_{C}(\hat{N}^{\mathrm{det}}_{\mathrm{key},\mathtt{TAR},Z_C}) \underset{\epsilon_C}{\leq} N^{\mathrm{det}}_{\mathrm{key},\mathtt{TAR},Z_C} \underset{\epsilon_C}{\leq} \hat{N}^{\mathrm{det}}_{\mathrm{key},\mathtt{TAR},Z_C} + \Delta^{+}_{C}(\hat{N}^{\mathrm{det}}_{\mathrm{key},\mathtt{TAR},Z_C}) \eqqcolon \overline{N}^{\mathrm{det}}_{\mathrm{key},\mathtt{TAR},Z_C},
\end{aligned} \tag{S113}$$

with $v_r = |\mathcal{C}^{(0)}_{\mathrm{Ref}}| + |\mathcal{C}^{(1)}_{\mathrm{Ref}}|$, $v_t = |\mathcal{C}^{(0)}_{\mathrm{Tar}}| + |\mathcal{C}^{(1)}_{\mathrm{Tar}}|$, $\hat{N}^{\beta x}_{l,t,Z_C} = p_{Z_C} p_{t|l} N^{\beta x}_{l}$, $\hat{N}^{\mathrm{det}}_{l,t,Z_C} = p_{Z_C} p_{t|l} N^{\mathrm{det}}_{l}$, $N^{\mathrm{det}}_{\mathrm{key},\mathtt{TAR},Z_C} = \sum_{\alpha\in\{0,1\}} N^{\mathrm{det}}_{\mathrm{vir}\alpha,\mathtt{TAR}\alpha,Z_C}$, and $\hat{N}^{\mathrm{det}}_{\mathrm{key},\mathtt{TAR},Z_C} = p_{Z_C} p_{\mathtt{TAR}|\mathrm{vir}} N^{\mathrm{det}}_{\mathrm{key}}$. By substituting Eqs. (S111) to (S113) into Eq. (S110), we get that

$$\begin{aligned}
N_{\mathrm{ph},\mathtt{TAR},Z_C} \underset{6\epsilon_A+(2v_r+3v_t+3)\epsilon_C}{\leq} & (\overline{N}^{\mathrm{det}}_{Z_C=0} + \Delta_A)\, G_{+}\left(\frac{\overline{N}^{\mathrm{err}}_{Z_C=1} + \Delta_A}{\underline{N}^{\mathrm{det}}_{Z_C=1} - \Delta_A}, 1 - \frac{2p_{Z_C}(\overline{N}_{X_C=1} + \Delta_A)}{p_{X_C}(\underline{N}^{\mathrm{det}}_{Z_C=0} + \underline{N}^{\mathrm{det}}_{Z_C=1} - \Delta_A)}\right) \\
& + \Delta_A - \sum_{\alpha\in\{0,1\}} \sum_{j\in\mathcal{C}^{(\alpha)}_{\mathrm{Tar}}} \underline{N}^{(\alpha\oplus 1)x}_{j,\mathtt{TAR}\alpha,Z_C}.
\end{aligned} \tag{S114}$$

Open Problems



Supplementary: Indistinguishability of non-orthogonal states on measurement

Although this proof uses POVM formalism, it can be done for generalised measurement operators as well.
Let us assume a set of measurement operators exist $\{M_1, M_2\}$ ($\{M_j\}$ for general purposes) which can differentiate $|\psi_1\rangle, |\, \psi_2\rangle$ ($\{|\psi_i\rangle\}$ for generalisation) by giving a measurement result j when M_j is applied.

We assume that once the result is obtained there exists some rule $f(j)$ that allows us to map the result to the state.
For example, if $|\psi_i\rangle$ is prepared then we will get $f(j) = 1$, and never $f(j) = 2$.

Supplementary: Indistinguishability of non-orthogonal states on measurement

A simple setup could be:
Given states $|\psi_1\rangle, |\,\psi_2\rangle$, we can construct projective measurement operators $P_0 = |\psi_1\rangle\langle\psi_1|\,, P_1 = |\psi_2\rangle\langle\psi_2|$ and the rule $f(0) = 1, f(1) = 2$. Now if we naïvely model the P_0 operator with the '0" detector and similarly with P_1, then on measuring state $|\psi_1\rangle$ the probability of the '0" detector clicking will be 1 the obtained state will be $|\psi_1\rangle$.

Supplementary: Indistinguishability of non-orthogonal states on measurement

The proof is as follows:
Given states $|\psi_1\rangle, |\,\psi_2\rangle$, we have $\{M_j\}$. Constructing $E_i = \sum_{j:f(j)=i} M_j^\dagger M_j$, we can say

$$\langle\psi_1\,|E_1|\,\psi_1\rangle = 1, \langle\psi_2\,|E_2|\,\psi_2\rangle = 1$$

Since $\sum_i E_i = \mathbb{I}$,

$$\langle\psi_1\,|E_2|\,\psi_1\rangle = 0, \langle\psi_2\,|E_1|\,\psi_2\rangle = 0$$

$\langle\psi_1\,|E_2|\,\psi_1\rangle = \langle\psi_1\,\left|\sqrt{E_2}\sqrt{E_2}\right|\,\psi_1\rangle = \langle\phi|\phi\rangle = 0$, which is only possible if $\sqrt{E_2}|\psi_1\rangle = |\phi\rangle$ is the zero vector.

Supplementary: Indistinguishability of non-orthogonal states on measurement

To make the states non-orthogonal, let $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\psi_{1\perp}\rangle$ and $|\beta|^2 < 1$.

$$\langle\psi_2 \,|E_2|\, \psi_2\rangle = |\alpha|^2\langle\psi_1 \,|E_2|\, \psi_1\rangle + |\beta|^2\langle\psi_{1\perp} \,|E_2|\, \psi_{1\perp}\rangle = |\beta|^2\langle\psi_{1\perp} \,|E_2|\, \psi_{1\perp}\rangle$$

But since $\langle\psi_{1\perp} \,|E_2|\, \psi_{1\perp}\rangle \leq \sum_i\langle\psi_{1\perp} \,|E_i|\, \psi_{1\perp}\rangle = 1$ (Since the state must resolve to *some* value on measurement/sum of probabilities is 1.), the results we obtain are contradictory, since we get:

$$\langle\psi_2 \,|E_2|\, \psi_2\rangle = 1\text{AND}\langle\psi_2 \,|E_2|\, \psi_2\rangle = |\beta|^2\langle\psi_{1\perp} \,|E_2|\, \psi_{1\perp}\rangle \leq |\beta|^2 < 1$$

Thus proved.

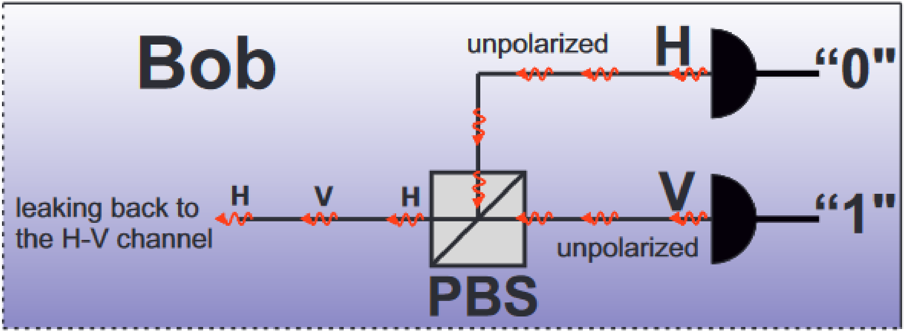
Supplementary: Error correction

With the simplest error correction protocol, Alice randomly chooses pairs of bits and announces their XOR value (i.e. their sum modulo 2). Bob replies either "accept" if he has the same XOR value for his corresponding bits, or "reject" if not. In the first case, Alice and Bob keep the first bit of the pair and eliminate the second one, while in the second case they eliminate both bits.

Supplementary: Privacy Amplification

Alice again randomly chooses pairs of bits and computes their XOR value. But, contrary to error correction she does not announce this XOR value. She only announces which bits she chose (e.g. bit number 103 and 537). Alice and Bob then replace (sic) the two bits by their XOR value. In this way 7 they shorten their key while keeping it error free, but if Eve has only partial information on the two bits, her information on the XOR value is even lower. Consider for example that Eve knows only the value of the first bit, and nothing about the second one. Then she has no information at all on the XOR value.

Supplementary: Backflash


Bob
unpolarized
H
"0"
leaking back to the H-V channel
H
V
H
PBS
V
"1"
unpolarized