RESEARCH ARTICLE OPEN ACCESS

QUANTUM CRYPTOGRAPHY COMMUNICATION BETWEEN THE OBJECT IN SPACE AND EARTH

K.Poonguzhali*,D.Kirubasankari**,T.Karthikeyan***

*(Mphil-Research Scholar, Department of Computer Science, Sri Bharathi Womens Arts and Science College, Kunnathoor, Arni.)
**(Assistant Professor, Department of Computer Science, Sri Bharathi Womens Arts and Science College, Kunnathoor, Arni.)
***(Associate Professor, Department of Computer Science, Dr.MGR Chockalingam Arts College, Arni.)

----------**********----------

ABSTRACT

The mobile optical high-speed communication links between diverse platforms for example optical links from aircrafts, UAVs or satellites to ground are based on mobile FSO communication links have gained significant attention over the last years due to their increasing maturity. They are used in point to point links scenarios.

This paper will give an overview on the current and future work of the optical communication regard to quantum communications. Quantum cryptography makes use of the quantum-mechanical behavior of nature for the design and analysis of cryptographic schemes.

Key words: FSO, Quantum Cryptography, Free Space Optical Communication.

----------**********----------

I. INTRODUCTION

Free-space optical communications for mobile applications have become more and more popular during the last couple of years. Especially in applications that require high data rates and power efficiencies, FSO links are a good alternative to state-of-the-art RF links. An additional advantage is the fact that the optical spectrum is unregulated and thus no time-consuming licensing process is necessary.

The Optical Communication Group of German Aerospace Center's Institute of Communication and Navigation is conducting research for a broad variety of possible applications. This includes the demonstration of free-space optical links from stratospheric platforms to ground, aircraft to ground and satellites to ground. Furthermore, challenging topics as adaptive optics systems for highly turbulent atmospheric channels or deep space links for exploration probes are investigated.

II. QUANTUM KEY DISTRIBUTION

Quantum communication allows implementing tasks which are classically impossible. The most prominent example is quantum key distribution where two honest players establish a secure key against an eavesdropper. In the two-party setting however, quantum and classical cryptography often show similar limits.

Oblivious transfer bit commitment and even fair coin tossing are impossible to realize securely both classically and quantumly. On the other hand, quantum cryptography allows for some weaker primitives impossible in the classical world. For example, quantum coin-flipping protocols with maximum bias of $1/\sqrt{2} - 1/2$ against any adversary while remaining impossible based solely on classical communication.

This behavior is indistinguishable from the one specified by the protocol but guarantees

that the joint quantum state held by Alice and Bob at any point during the protocol remains pure. The possibility for players to behave that way in any two-party protocol has important consequences. The impossibility of quantum bit commitment follows from this fact. After the commit phase, Alice and Bob share the pure state| xi 2 HA HB corresponding to the commitment of bit x.

Since a proper commitment scheme provides no information about x to the receiver Bob, it follows that trA | 0ih 0| / trA | 1ih 1|. In this case, the Schmidt decomposition guarantees that there exists a unitary U0,1 acting only on Alice's side such that | 1i / (U0,1IB)| 0i. In other words, if the commitment is concealing then Alice can open the bit of her choice by applying a suitable unitary transform only to her part.

A similar argument allows to conclude that 1-2-ot is impossible. Suppose Alice is sending the pair of bits (b0, b1) to Bob through 1-2-ot. Since Alice does not learn Bob's selection bit, it follows that Bob can get bit b0 before undoing the reception of b0 and transforming it into the reception of b1 using a local unitary transform similar to U0,1 for bit commitment. For both these primitives, privacy for one player implies that local actions by the other player can transform the honest execution with one input into the honest execution with another input.

III. QUANTUM HONEST-BUT-CURIOUS

This quantum honest-but-curious (QHBC) behavior is the natural quantum version of classical HBC behavior. We consider the setting where Alice obtains random variable X and Bob random variable Y according to the joint probability distribution PX,Y .

Any PX,Y models a two-party cryptographic primitive where neither Alice nor Bob provide input. For the purpose of this thesis, this model is general enough since any two-party primitive with inputs can be randomized (Alice and Bob pick their input at random) so that its behavior can be described by a suitable joint probability distribution of PX,Y .

IV. QUANTUM EMBEDDING

Any quantum protocol implementing PX,Y must produce, when both parties purify their actions, a joint pure state | i 2 HAA0 HBB0 that, when subsystems of A and B are measured in the computational basis, leads to outcomes X and Y according the distribution PX,Y .

Notice that the registers A0 and B0 only provide the players with extra working space and, as such, do not contribute to the output of the functionality.

In this paper, we adopt a somewhat strict point of view and define a quantum protocol for PX,Y to be correct if and only if the correct outcomes X, Y are obtained and the registers A0 and B0 do not provide any additional information about Y and X respectively since otherwise would be implementing a different primitive PXX0,Y Y 0 rather than PX,Y .

The sufficient to investigate the cryptographic power of embeddings in order to understand the power of two-party quantum cryptography in the QHBC model.

Notice that if X and Y were provided privately to Alice and Bob through a trusted third party for instance then the expected amount of information one party gets about the other party's output is minimal and can be quantified by the Shannon mutual information I(X; Y) between X and Y . Assume that | i 2 HAA0 HBB0 is the embedding of PX,Y produced by a correct quantum protocol. We define the leakage of | i as

$$\Delta = \max \{S(X; BB0) - I(X; Y) , S(Y ;AA0) - I(Y ;X) \} ,$$

where S(X;BB0) (resp. S(Y ;AA0)) is the information the quantum registers BB0 (resp. AA0) provide about the output X (resp. Y). That is, the leakage is the maximum amount of extra information about the other party's output given the quantum state held by one party.

It turns out that S(X;BB0) = S(Y ;AA0) holds for all embeddings, exhibiting a symmetry similar to its classical counterpart I(X; Y) = I(Y ;X) and therefore, the two quantities we are taking the maximum of (in the definition of leakage above) coincide.

V.CONTRIBUTIONS

Our first contribution establishes that the notion of leakage is well behaved. We show that the leakage of any embedding for PX,Y is lower bounded by the leakage of some regular embedding of the same primitive. Thus, in order to lower bound the leakage of any correct implementation of a given primitive, it success to minimize the leakage over all its regular embeddings.

We also show that the only non-leaking embeddings are the ones for trivial primitives, where a primitive PX,Y is said to be (cryptographically) trivial if it can be generated by a classical protocol against HBC adversaries5.

This extends known impossibility results for two-party primitives to all non-trivial primitives. Embeddings of primitives arise from protocols where Alice and Bob have full control over the environment. Having in mind that any embedding of a non-trivial primitive leaks information, it is natural to investigate what tasks can be implemented without leakage with the help of a trusted third party.

In general, this is not an easy task since it requires to find the Eigen values of the reduced density matrix A = trB | ih | (or equivalently B = trA | ih |). As far as we know, no known results allow us to obtain a non-trivial lower bound on the leakage (which is the difference between the mutual information and accessible information) of non-trivial primitives.

Finally, we note that our lower bounds on the leakage of the randomized primitives also lower bound the minimum leakage for the standard versions of these primitives7 where the players choose their inputs uniformly at random. While we focus on the typical case where the primitives are run with uniform inputs, the same reasoning can be applied to primitives with arbitrary distributions of inputs.

VI.RELATED WORK

Our framework allows quantifying the minimum amount of leakage whereas standard impossibility proofs as the ones of do not in general provide such quantification since they usually assume privacy for one player in order to show that the protocol must be totally insecure for the other player. By contrast, we derive lower bounds for the leakage of any correct implementation.

At first glance, our approach seems contradictory with standard impossibility proofs since embeddings leak the same amount towards both parties.

Our results complement the ones obtained by Callback for the setting where Alice and Bob have inputs and obtain identical outcomes called single-function computations. Shows that in any correct implementation of primitives.We show that only trivial distributions can be implemented securely in the QHBC model. Furthermore, we introduce a quantitative measure of protocol-insecurity that lets us answer which embedding allows the least effective cheating. Another notion of privacy in quantum protocols, generalizing its classical counterpart is proposed by Klauck.

There in two-party quantum protocols with inputs for computing a function f : X × Y ! Z, where X and Y denote Alice's and Bob's respective input spaces, and privacy against QHBC adversaries are considered. Privacy of a protocol is measured in terms of privacy loss, defined for each round of the protocol and fixed distribution of inputs PX0,Y 0 by S(B;X|Y) = H(X|Y) - S(X|B, Y), where B denotes Bob's private working register, and X := (X0, f(X0, Y 0)), Y := (Y 0, f(X0, Y 0)) represent the complete views of Alice and Bob, respectively. Privacy loss of the entire protocol is then defined as the supreme over all joint input distributions, protocol rounds, and states of working registers.

In our framework, privacy loss corresponds to S(X; Y B)-I(X; Y) from Alice points of view and S(Y ;XA)-I(X; Y) from Bob's point of view. Privacy loss is therefore very similar to our definition of leakage except that it requires the players to get their respective honest outputs. As a consequence, the protocol implementing PX,Y by asking one party to prepare a regular embedding of PX,Y before sending her register to the other party would have no privacy loss.

Moreover, the scenario analyzed is restricted to primitives which provide the same output f(X, Y) to both players. Another difference is that since privacy loss is computed over all rounds of a protocol, a party is allowed to abort which is not considered QHBC in our setting. In conclusion, the model of different from ours even though the measures of privacy loss and leakage are similar.

Provides interesting results concerning trade between privacy loss and communication complexity of quantum protocols, building upon similar results of [CK91,Kus92] in the classical scenario. It would be interesting to know whether a similar operational meaning can also be assigned to the new measure of privacy.

VII. THE RECENT RESULT

A recent result by Kunzler et al. shows that two-party functions that are securely computable against active quantum adversaries form a strict subset of the set of functions which are securely computable in the classical HBC model. This complements our result that the sets of securely computable functions in both HBC and QHBC models are the same roadmap.

We introduce the cryptographic and information-theoretic notions and concepts used throughout the paper. We define, motivate, and analyze the generality of modeling two-party quantum protocols by embeddings and define triviality of primitives and embeddings.

We define the notion of leakage of embeddings, show basic properties and argue that it is a reasonable measure of privacy. We explicitly lower bound the leakage of some universal two-party primitives. Finally, We discuss possible directions for future research and open questions.

VIII.PRELIMINARIES

Quantum Information Theory Let | iAB 2 HAB be an arbitrary pure state of the joint systems A and B. The states of these subsystems are A = trB | ih | and B = trA | ih |, respectively. We denote by S(A) := S(A) and S(B) := S(B) the von Neumann entropy of subsystem A and B respectively.

Since the joint system is in a pure state, it follows from the Schmidt decomposition that S(A) = S(B) (see e.g. [NC00]). Analogously to their classical counterparts, we can define quantum conditional entropy S(A|B) := S(AB) - S(B), and quantum mutual information S(A;B) := S(A)+S(B)-S(AB) = S(A)-S(A|B). Even though in general, S(A|B) can be negative, S(A|B) 0 is always true if A is a classical register.

Let R = {(PX(x), x R}x2X be an ensemble of states x R with prior probability PX(x). The average quantum state is R = Px2X PX(x)x R. The famous result by Holevo upper-bounds the amount of classical information about X that can be obtained by measuring R: Theorem 2 (Holevo bound [Hol73,Rus02]).*Let* Y be the random variable describing the outcome of some measurement applied to R *for* R = {PX(x), x R}x2X.

Then, I(X; Y) S(R) -Px PX(x)S(xR), where equality can be achieved if and only if {x R}x2X are simultaneously diagonalizable.

Definition: 1 (Dependent part). *For two random variables* X, Y , *let* fX(x) : = PY |X=x. *Then the* dependent part of X with respect to Y *is defined as* X & Y := fX(X).

The dependent part X & Y is the minimum random variable among the random variables computable from X for which X $ X & Y $ Y forms a Markov chain. In other words, for any random variable K = f(X) such that X $ K $

Y is a Markov chain, there exists a function g such that g(K) = X & Y . Immediately from the definition we get several other properties of X & Y [WW04]: H(Y |X & Y) = H(Y |X), I(X; Y) = I(X & Y ; Y), and X & Y = X & (Y & X). The second and the third formula yield I(X; Y) = I(X & Y ; Y & X).

The notion of dependent part has been further investigated. Wullschleger and Wolf have shown that quantities H(X & Y |Y) and H(Y & X|X) are monotones for two-party computation. That is, none of these values can increase during classical two-party protocols. In particular, if Alice and Bob start a protocol from scratch then classical two-party protocols can only produce (X, Y) such that: H(X & Y |Y) = H(Y & X|X) = 0,since H(X & Y |Y) > 0 if and only if H(Y & X|X) > 0. Conversely, any primitive satisfying H(X & Y |Y) = H(Y & X|X) = 0 can be implemented securely in the honest-but-curious (HBC) model.

The operations to be executed from the random outcome are then performed quantumly without fixing the random outcomes. For example, suppose a protocol instructs a party to pick with probability p state |0iC and with probability 1-p state |1iC before sending it to the other party through the quantum channel C.

The purified version of this instruction looks as follows: Prepare a quantum register in state pp|0iR + p1 - p|1iR holding the random process. Add a new register initially in state |0iC before applying the unitary transform U : |riR|0iC 7! |riR|_riC for r 2 {0, 1}, send register C through the quantum channel and keep register R.

From the receiver's point of view, the purified behavior is indistinguishable from the one relying upon a classical source of randomness because in both cases, the state of register C is p|0ih0| + (1 - p)|ih1|. All operations invoking classical randomness can be purified similarly.

The result is that measurements are postponed as much as possible and only extract information required to run the protocol in the sense that only when both players need to know a random outcome.

We investigate the leakage of several universal cryptographic two-party primitives. By universality we mean that any two-party secure function evaluation can be reduced to them. We investigate the completely randomized versions where players do not have inputs but receive randomized outputs instead.

IX.TWO-PARTY PROTOCOLS AND THEIR CORRECTNESS

We consider cryptographic primitives providing X to honest player Alice and Y to honest player Bob according to a joint probability distribution PX,Y . The goal of this section is to define when a protocol correctly implements the primitive PX,Y . The first natural requirement is that once the actions of are purified by both players, measurements of registers A and B in the computational basis10 provide joint outcome (X, Y) = (x, y) with probability PX,Y (x, y).

Protocol can use extra registers A0 on Alice's and B0 on Bob's side providing them with working space. The purification of all actions of therefore generates a pure state | i 2 HAB HA0B0. A second requirement for the correctness of the protocol is that these extra registers are only used as working space, i.e. the final state | iABA0B0 is such that the content of Alice's working register A0 does not give her any further information about Bob's output Y than what she can infer from her honest output X and vice versa for B0. Formally, we require that S(XA0; Y) = I(X; Y) and S(X; Y B0) = I(X; Y) or equivalently, that A0 $ X $ Y and X $ Y $ B0 form Markov chains11.

Definition :2 A protocol for PX,Y is correct if measuring registers A and B of its final state in the computational basis yields outcomes X and Y with distribution PX,Y and the final state satisfies S(X; Y B0) = S(XA0; Y) = I(X; Y) where A0 and B0 denote the extra working registers of Alice and Bob. The state | i 2 HAB HA0B0 is called an embedding of PX,Y if it can

be produced by the purification of a correct protocol for PX,Y .

We would like to point out that our definition of correctness is stronger than the usual classical notion which only requires the correct distribution of the output of the honest players. For example, the trivial classical protocol for the primitive PX,Y in which Alice samples both player's outputs XY , sends Y to Bob, but keeps a copy of Y for herself, is not correct according to our definition, because it implements a fundamentally deferent primitive, namely PXY,Y .

X.REGULAR EMBEDDINGS

We call an embedding | iABA0B0 regular if the working registers A0, B0 are empty. Formally, let n, m = {{0, 1}n ?{0, 1}m ! [0 . . . 2)} Be the set of functions mapping bit-strings of length m+ n to real numbers between 0 and 2.

Definition: 3 For a joint probability distribution PX,Y where X 2 {0, 1}n and Y 2 {0, 1}m, we define the set

$$\mathcal{E}(P_{X,Y}) := \left\{ |\psi\rangle \in \mathcal{H}_{AB} : |\psi\rangle = \sum_{x\in\{0,1\}^n, y\in\{0,1\}^m} e^{i\theta(x,y)} \sqrt{P_{X,Y}(x,y)} |x,y\rangle_{AB}, \theta \in \Theta_{n,m} \right.$$

and call any state | i 2 E(PX,Y) a regular embedding of the joint probability distribution PX,Y .

Clearly, any | i 2 E(PX,Y) produces (X, Y) with distribution PX,Y since the probability that Alice measures x and Bob measures y in the computational basis is |h |x, yi|2 = PX,Y (x, y).

In order to specify a particular regular embedding one only needs to give the description of the phase function(x, y). We denote by | i 2 E(PX,Y) the quantum embedding of PX,Y with phase function.

The constant function (x, y) := 0 for all x 2 {0, 1}n, y 2 {0, 1}m corresponds to what we call canonical embedding | 0i := Px,yp PX,Y (x, y)|x, yiAB . In Lemma below we show that every primitive PX, Y has a regular embedding which is in some sense the most secure among all embeddings of PX, Y.

XI. TRIVIAL CLASSICAL PRIMITIVES AND TRIVIAL EMBEDDINGS

In this section, we define triviality of classical primitives and bipartite embeddings. We show that for any non-trivial classical primitive, its canonical quantum embedding is also non-trivial. Intuitively, a primitive PX,Y is trivial if X and Y can be generated by Alice and Bob from scratch in the classical honest-but-curious (HBC) model12.

Definition: 4 A primitive PX,Y is called trivial if it satisfies H(X & Y |Y) = 0, or equivalently, H(Y & X|X) = 0. Otherwise, the primitive is called non-trivial.

Definition: 5 A regular embedding | iAB 2 E(PX,Y) is called trivial if either S(X & Y |B) = 0 or S(Y & X|A) = 0. Otherwise, we say that | iAB is non-trivial.

Let | i 2 E(PX,Y) be trivial and assume without loss of generality that S(Y & X|A) = 0. Intuitively, this means that Alice can learn everything possible about Bob's outcome Y (Y could include some private coin-flips on Bob's side, but that is "filtered out" by the dependent part). More precisely, Alice holding register A can measure her part of the shared state to completely learn a realization of Y & X, specifying PX|Y=y. She then chooses X according to the distribution PX|Y=y. An equivalent way of trivially generating (X,Y) classically is the following classical protocol.

Alice samples PX|Y=y0 from distribution PY&X and announces its outcome to Bob. She samples x from the distribution PX|Y =y0.

Bob picks y with probability PY |Y&X=PX|Y =y0. Of course, the same reasoning applies in case S(X & Y |B) = 0 with the roles of Alice and Bob reversed. In fact, the following lemma (proven in Appendix B) shows that any

non-trivial primitive PX,Y has a non-trivial embedding.

Lemma: 1 If PX,Y is a non-trivial primitive then the canonical embedding | 0i 2 E(PX,Y) is also non-trivial.

XII.THE LEAKAGE OF QUANTUM EMBEDDINGS

We formally define the leakage of embeddings and establish properties of the leakage. A perfect implementation of PX,Y simply provides X to Alice and Y to Bob and does nothing else. The expected amount of information that one random variable gives about the other is I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y |X) = I(Y ;X). Intuitively, we define the leakage of a quantum embedding | iABA0B0 *of* PX,Y as the larger of the two following quantities the extra amount of information Bob's quantum registers BB0 provide about X and the extra amount Alice's quantum state in AA0 provides about Y respectively in comparison to the minimum amount I(X; Y).

Definition: 6 Let | i 2 HABA0B0 be an embedding of PX,Y . We define the leakage | i as _ (PX,Y) := max {S(X;BB0) - I(X; Y) , S(AA0; Y) - I(X; Y)} . Furthermore, we say that | i is -leaking if (PX,Y).

It is easy to see that the leakage is non-negative since S(X;BB0) _ S(X; ˜ B) for ˜ B the result of a quantum operation applied to BB0. Such an operation could be the trace over the extra working register B0 and a measurement in the computational basis of each cubit of the part encoding Y , yielding S(X; ˜ B) = I(X; Y).

Notice that S(X;B) = S(X) + S(B) - S(X,B) = H(X) + S(B) - H(X) = S(B) and because | i is pure, S(A) = S(B). Therefore, S(X;B) = S(A; Y) and the two quantities coincide. The following lemma states that this actually happens for all embeddings and hence, the definition of leakage is symmetric with respect to both players.

Lemma: 2 (Symmetry). *Let* | i 2 HABA0B0 be an embedding of PX,Y . Then (PX,Y) = S(X;BB0) - I(X; Y) = S(AA0; Y) - I(X; Y) .

The next lemma shows that the leakage of an embedding of a given primitive is lower-bounded by the leakage of some regular embedding of the same primitive, which simplifies the calculation of lower bounds for the leakage of embeddings.

Lemma: 3 For every embedding | i of a primitive PX,Y , there is a regular embedding | 0i of

PX,Y such that (PX,Y)0(PX,Y).

Definition: 7 We define the leakage of a primitive PX,Y as the minimal leakage among all

protocols correctly implementing PX,Y. Formally, PX,Y := min | I (PX,Y) , where the minimization is over all embeddings | i of PX,Y.

Notice that the minimum in the previous definition is well-defined, because by Lemma, it is sufficient to minimize over regular embeddings | i 2 E(PX,Y). Furthermore, the function (PX,Y) is continuous on the compact (i.e. closed and bounded) set [0, 2]|X| of complex phases corresponding to elements |x, yiAB in the formula for | iAB 2 E(PX,Y) and therefore it achieves its minimum.

Theorem: 1. For any primitive PX,Y , PX,Y PX&Y,Y&X. Proof *(*Sketch*).* The proof idea is to pre-process the registers storing X and Y in a way allowing.

Alice and Bob to convert a regular embedding of PX,Y into a regular embedding of PX&Y,Y&X by measuring parts of these registers. It follows that on average, the leakage of the resulting regular embedding of PX&Y,Y&X is at most the leakage of the embedding of PX,Y the players started with. Hence, there must be a regular embedding of PX&Y,Y&X leaking at most as much as the best embedding of PX,Y .

Theorem: 2 If a two-party quantum protocol provides the correct outcomes of PX,Y to the players without leaking extra information, then PX,Y must be a trivial primitive.

Proof. Theorem implies that if there is a 0–leaking embedding of PX,Y than there is also a leaking embedding of PX&Y,Y&X.

Let us therefore assume that | i is a non-leaking embedding of PX,Y such that X = X & Y and Y = Y & X. We can write | i in the form | i = PxpPX(x)|xi|'xi and get B = Px PX(x)|'xih'x|. For the leakage of | i we have: (PX,Y) = S(X;B) - I(X; Y) = S(B) - I(X; Y) = 0. From the Holevo bound (Theorem 2) follows that the states {|'xi}x form an orthonormal basis of their span (since X = X & Y , they are all different) and that Y captures the result of a measurement in this basis, which therefore is the computational basis. Since Y = Y & X, we get that for each x, there is a single yx 2 Y such that |'xi = |yxi.

The primitives PX&Y,Y&X and PX,Y are therefore trivial this result can be seen as a quantum extension of the corresponding characterization for the cryptographic power of classical protocols in the HBC model. Whereas classical two-party protocols cannot achieve anything non-trivial, their quantum counterparts necessarily leak information when they implement non-trivial primitives.. A special case of such protocols are the ones where the players are allowed one call to a black box for a certain non-trivial primitive.

Theorem: 3 Suppose that primitives PX,Y and PX_0,Y_0 satisfy $H(X_0 \& Y_0|Y_0) > H(X \& Y |Y)$ or $H(Y_0 \& X_0|X_0) > H(Y \& X|X)$. Then any implementation of PX_0,Y_0 using just one call to the ideal functionality for PX,Y leaks information.

XIII.REDUCIBILITY OF PRIMITIVES AND THEIR LEAKAGE

The two primitives PX,Y and PX_0,Y_0 such that PX,Y is reducible to PX_0,Y_0 , what is the relationship between the leakage of PX,Y and the leakage of PX_0,Y_0? We use the notion of reducibility in the following sense.

We say that a primitive PX,Y is reducible in the HBC model to a primitive PX_0, Y_0 if PX,Y can be securely implemented in the HBC model from a secure implementation of PX_0,Y_0.

Notice that the answer, even if we assume perfect reducibility, is not captured in our previous result from Lemma, since an embedding of PX_0,Y_0 is not necessarily an embedding of PX,Y.

XIV. THE IMPORTANCE OF CRYPTOGRAPHY

At a time when the reliance upon electronic data transmission and processing is becoming every day more prevalent, unauthorized access to proprietary information is a real threat. In 2004, 53% of the respondents of the CSI/FBI Computer Security and Crime Survey admitted having been subjected to unauthorized use of computer systems. These attacks caused a total loss of more than 140 million USD for the respondents of the survey.

Last but not least, the way an organization protects its information assets increasingly impacts the image projected to customers. Protecting Information Efficiently protecting critical information within an organization requires the definition and the implementation of a consistent information security policy.

Such a policy describes which processes and means must be applied within the company to achieve this goal. It puts into practice technologies such as biometrics or smartcards, for instance, to control access to the data processing and storage infrastructures whether electronic or not and guarantee the physical security of the information.

It also resorts to solutions such as Intrusion Prevention and Detection systems, Firewalls and Antivirus Software to defend a secure perimeter around the internal computer

network of the organization and prevent hackers from penetrating it. Finally, it defines measures to protect information transmission between remote sites. This last aspect of information security is often overlooked.

XV. CRYPTOGRAPHY

Cryptography is the art of rendering information exchanged between two parties unintelligible to any unauthorized person. Although it is an old science, its scope of applications remained mainly restricted to military and diplomatic purposes until the development of electronic and optical telecommunications.

In the past twenty-five years, cryptography evolved out of its status of "classified" science and offers now solutions to guarantee the secrecy of the ever expanding civilian telecommunication networks.

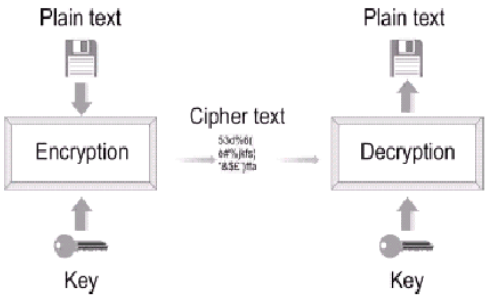
The way cryptography works is illustrated in figure Before transmitting sensitive information, the sender combines the plain text with a secret key, using some encryption algorithm, to obtain the cipher text.

The more bits the key contains, the better the security. The DES algorithm – Data Encryption Standard –played an important role in the security of electronic communications. It was adopted as a standard by the US federal administration in 1976.

The length of its keys is however only 56 bits. Since it can nowadays be cracked in a few hours, it is not considered secure any longer. It has been replaced recently by the Advanced Encryption Standard AES which has a minimum key length of 128 bits.

The more often a key is changed, the better the security. The encryption algorithm is disclosed, the secrecy of such a scheme basically depends on the fact that the key is secret.

Truly random numbers must thus be used for the key. Second, it must not be possible for a third party to intercept the key during its exchange between the sender and the recipient. This so-called key distribution problem. Is very central in cryptography.



Principle of cryptography

XVI. HIGH ALTITUDE PLATFORM-TO-GROUND LINKS

A very interesting and promising application for free-space optical links is the interconnection of airships placed in the stratosphere, so called High Altitude Platforms (HAPs). Equipped with RF-systems for the connection to users on ground and optical terminals for building up a network among them, HAPs over a cost-effective solution for offering broadband data access in regions where only little terrestrial infrastructure exists or where it would be too expensive to build it up.

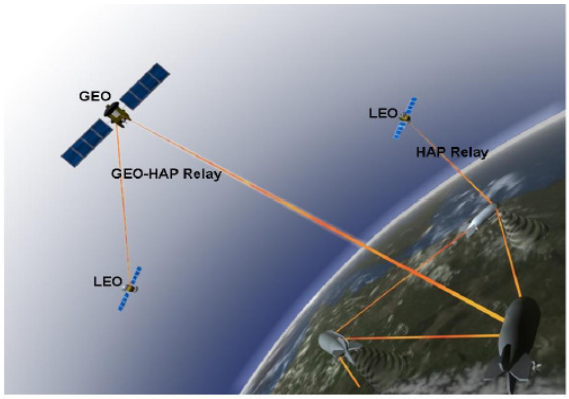


Fig. 1. Artist's Impression of a network including High Altitude Platforms

(HAPs) in the stratosphere. Users can connect through weather-insensible RF communication links, while optical Inter-HAP links serve as backbone. Further applications are the use of

HAPs as data relay for LEO- and GEO-satellites.

As the operating altitude of HAPs is above the height of clouds, no link blockings for the Inter-HAP-links can be expected due to clouds. At the same time, the RF user links can operate through the clouds, also during bad weather conditions. Furthermore, HAPs can be used as data-relay for optical downlinks from satellites.

DLR has developed an FSO terminal for stratospheric applications, and demonstrated its functionality in the framework of the EU funded project CAPANINA. A downlink from a stratospheric balloon with a height of up to 25km with a data rate of 1;25 Gbit=s over a distance of 64km has been performed. Figure 2 shows pictures of the development. A periscope-type Coarse Pointing Assembly (CPA) was used for the terminal.

Fig. 2. Freespace Experimental Laser Terminal (FELT) that has been developed for the CAPANINA Trial

The validation trial was carried out at the ESRANGE facilities in Kiruna, Sweden. Figure 3 shows a picture of the ballon launch. The payload was mounted in a compartment at the bottom of the ballon.

Fig. 3. Launch of the stratospheric ballon carrying the FELT payload

Data was transmitted at rates of 622 Mbit=s and 1:25 Gbit=s. Figure 4 shows an eye pattern and a Bit Error Rate (BER) that has been measured during the trial. Virtually error free data communication could be achieved with both data rates.

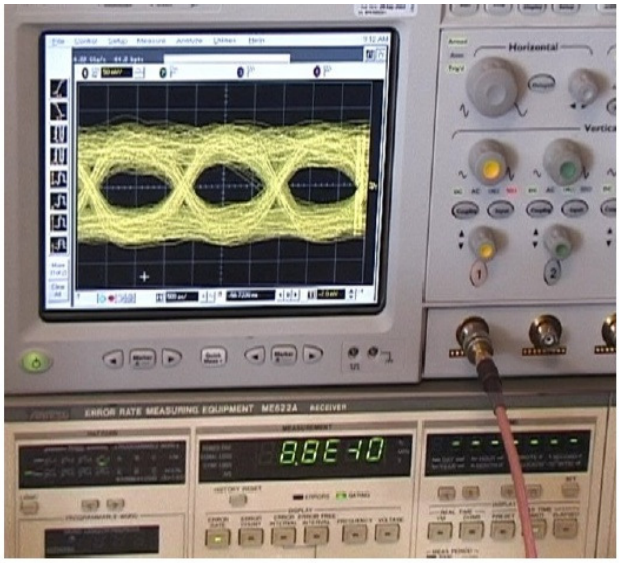


Fig. 4. Eye at the receiver and BER measured for a data rate of 622 Mbit=s during the CAPANINA trial

XVII.AIRCRAFT-TO-GROUND LINKS

Optical Downlinks from aircraft have recently been demonstrated in DLR's AR-GOS project. The ARGOS project (airborne wide area high altitude monitoring system) is meant to develop a platform to supply decision makers during mass or even catastrophic events with real-time reconnaissance data of the current situation.

The available sensors include a visible camera system and synthetic aperture radar. An optical downlink of the gathered data to a transportable optical ground station, placed at the operations center, is foreseen to obtain real-time data access. In the frame of the project, an Airborne Optical Terminal for one of DLR's research aircraft has been developed.

Its operability was shown over a link distance of up to 90km. The data rate for the system was driven by project requirements, and has been chosen to the rather low value of 125 Mbit=s. Although this is a moderate data rate for FSO links, it is sufficient for the project requirements, and still greatly outperforms typical microwave links (30:::40 Mbit=s).

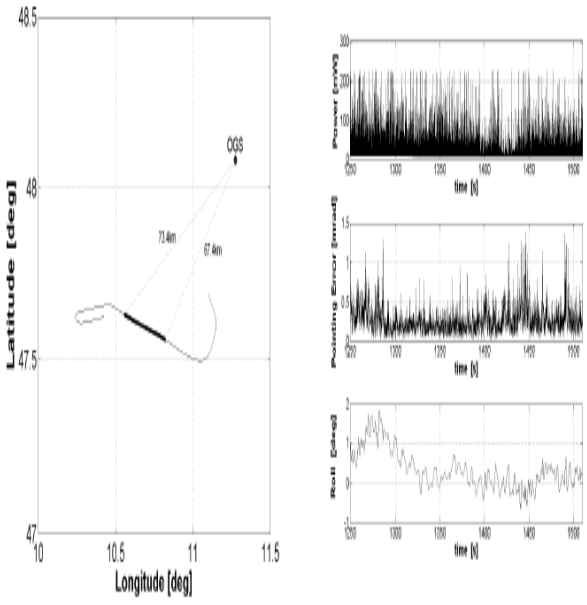


Fig. 7. Left: Flight Path example during validation fight. Right: Measurement data in the beacon-uplink for the thick painted line; Top: Received Power at Airborne Terminal, Middle: Pointing Error of Airborne Terminal, Bottom: Roll Angle of aircraft.

Considering the beam divergence of 2 m rad, and taking into account the forward error correction that is applied to the sent data, an error free communication link can be established with this setup.

The new developments will be varied by further flight testing campaigns. The ultimate goal of the project is to demonstrate an optical link over a distance higher than 100km with a data rate of over 1 G bits.

XVIII.SATELLITE-T0-GROUND LINKS

Also for the downlink of earth observation data gathered by LEO satellites, optical links to ground stations or High Altitude Platforms (HAPs) can be a solution for the increasing amount of downlink volume. Typical RF Systems for high data rates in the X- and/or Ka-Band require tens to hundreds of Watts of electrical power and antenna diameters of several to tens of centimeters onboard the satellite.

Furthermore, antenna dishes with several meters diameter are necessary on ground station side. It is believed that optical downlink terminals for LEO satellites can be built with lower power consumptions (< 50W) and smaller telescope diameters (few centimeters). Furthermore, ground station telescope diameters in the range from 10 cm to 40 cm are sufficient and available at reasonable prices.

VIX. FUTURE EXPERIMENTS

The data-rate was around 50 M bits. In 2006, a total of eight trials have been performed to which five were successful, while the others failed due to cloudy weather.

As an example, Figure 9 shows the received power during KIODO Trial 3. It is visible that the power level increases while the fading gets lower during the trial. This is for the fact that the link distance through the

atmosphere gets lower for higher elevation angles, resulting in a less turbulent communication channel and, of course, a higher power due to the shorter link distance. The visible signal breaks are characterstic of the laser terminal onboard OICETS, and don't appear due to mispointing of the telescope.

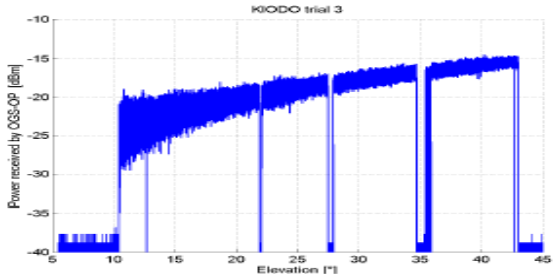


Fig. 9. Received Power during KIODO Trial 03

Figure 10 shows the Bit Error Rate results that have been obtained during a selection of the KIODO trials. It is visible that the Bit Error Rates get lower for higher elevation angles, as the received power increases and the scintillation due to atmospheric turbulence gets lower. Further trials with OICETS were carried out during a seconds campaign in the summer of 2009.

The parameters of the receiver can be optimized for the purpose of designing an optimal receiver front end for the turbulent atmospheric channel. However, again a number of links failed due to cloudy weather. Figure 11 show OGS-OP during the KIODO 2009 trials.

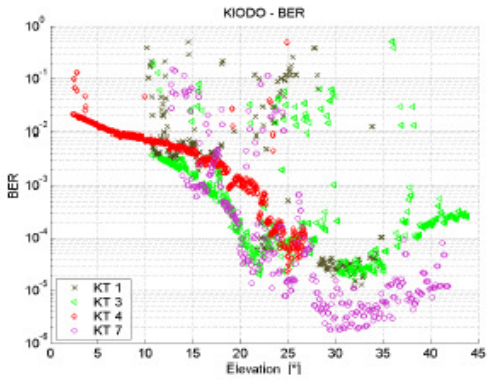


Fig. 10. Bit Error Rate Results for different elevation angles

Fig. 11. Optical Ground Station Oberpfaffenhofen (OGS-OP) during the KIODO 2009 trials. Visible on the infrared picture is the beacon laser's backscatter due to haze.

The possibility of optical LEO downlinks for the transmission of earth sensing data using state-of-the art 1550 nm components is currently investigated at DLR. Figure 12 shows an example link budget for a downlink from a LEO satellite to the Optical Ground Station in Oberpfaffenhofen (OGS-OP) for two different aperture diameters with direction limited radiation from the satellite.

XX.APPLICABILITY OF QUANTUM CRYPTOGRAPHY TO STANDARD FSO LINKS

The communication subsystems of the mentioned optical terminals can be modified for using them in quantum communication applications. A possible design of a combined optical transceiver for traditional FSO- and quantum communications using state-of-the art technology has been proposed.

Common FSO terminals for communication purposes operate at a wavelength of 1550 nm. The atmospheric transmission at this wavelength is more beneficial than for shorter wavelengths in the 800nm region, as they are typical for quantum communication systems. This effect is illustrated in Figure 13 for the example of an aircraft-to-ground link.

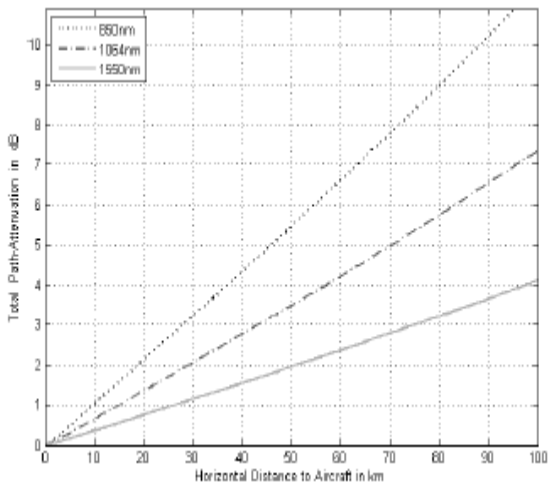


Fig. 13. Different atmospheric attenuations for an aircraft-to-ground link.

For the relatively short link distances of optical aircraft-to-ground links, there is no need to design the communication system close to the direction limit. Instead, larger beam divergences can still fulfill the project requirements in terms of free-space loss and thus data-rate, with the advantage that the requirements for the tracking system can be relaxed and a less accurate tracking system is sufficient. Furthermore, many mature and low prized shelf components are available in the 1550 nm range.

XXI. FURTHER DEVELOPMENTS

The research held of free-space optical communications offers still many open questions that are worth investigating them. One topic that is currently researched at DLR is an adaptive optics system fitted to the particular needs of FSO systems operating in the turbulent atmosphere.

A system consisting of a wave front sensor and a deformable mirror can be used to mitigate the influences of the atmosphere on the communication beam. A first lab-setup of this challenging development is intended to be operational in 2010.

Currently, development and qualification actions are carried out for the purpose of developing a small and lightweight optical terminal for the deployment on small- and micro- LEO satellites.

XXII. CONCLUSIONS

Optical Free-Space Communications offer a solution for the continuously increasing demand of higher data rates in many applications.

The feasibility of FSO links has been shown for diverse spectra of applications. This includes the execution of validation trials from stratospheric platforms, aircrafts and satellites.

BIBLIOGRAPHY

1. Bennett, C. H. & Brassard, G. (1984). *Quantum cryptography: Public key distribution And coin tossing*. Proceedings of IEEE International Conference on Computers Systems Signal Processing, Bangalore India, December 1984.

2. Bennett, Charles H., Gilles Brassards, and Jean-Marc Roberts, (1988), *Privacy amplification by public discussions*, Siam J. Comput, Vol 17, No. 2, April 1988.

3. B. Mayer et al. Dlr-internal electronic data base of atmospheric absorption coefficients. In DLR internal, 2002.

4. D. Giggenbach and J. Horwath. Optical free-space communications downlinks from stratospheric platforms - overview on stropex, the optical communications experiment of capanina. In IST Summit Dresden, 2005.

5. M. Pfennigbauer et al. Satellite-based quantum communication terminal employing state-of- the-art technology. Journal of Optical Networking (JON), 4, 2005.

6. M. Knapek et al. Optical high-capacity satellite downlinks via high-altitude plat-form relays. In Proceedings of the SPIE, 2006.

7. J. Horwath et al. Broadband backhaul communication for stratospheric platforms: The

stratospheric optical payload experiment (stropex). In Proceedings of the SPIE, 2006. 14 C.Fuchs, D. Giggenbach.

8. M. Knapek et al. The DLR ground station in the optical payload experiment (stropex) – results of the atmospheric measurement instruments. In Proceedings of the SPIE, 2006.

9. M. Toyoshima et al. Ground-to-octets laser communication experiments. In Proceedings of the SPIE, 2006.

10. Y. Takayama et al. Tracking and pointing characteristics of oicets optical terminal in communication demonstrations with ground stations. In Proceedings of the SPIE, 2007.