

Hyperencryption & Quantum Cryptography: The End Of Snooping?

Synopsis:

Data security and privacy have become major concerns in the present times. It's a dangerous world out there. Hardly a day goes by without our newspaper headlines screaming about the lack of security of data. Almost all organizations have reported losses due to unauthorized interception of data.

The largest threat is eavesdropping. The only thing to counter this threat is to reduce eavesdropping or make it entirely impossible. Practically, it is impossible to ensure that no eavesdropping occurs. Here cryptography comes in handy. Cryptography has the property that the defender has an enormous advantage over the passive eavesdropper or the malicious attacker. The amount possible damage done by unauthorized interception of data is reduced. Still, the cycle continues. People demand newer methods of safe-guarding their data, newer methods are created which claim to be fool-proof for some limited time and then some crackers get together and find out some loophole. Security is a 40 year old discipline, yet things are getting worse every day. The question is; where does this end?

The answer is; right here.

Two groups of people, working independently have come up with two technologies definitely worth more than a look.

The first is **hyperencryption**. The pet project of Prof. Michael Rabin & his PhD. student Yan Zong Ding at Harvard University Laboratories is a new avatar of the fundamentally secure one-time pad. This is still an experimental technology; the researchers have yet to write a paper on it. A detailed explanation is expected in the IEEE Transactions soon.

The second technology which is covered in this paper has been implemented. Research on **quantum cryptography** has been going on in Los Alamos National Laboratories under Dr. Hughes since the late 1980's. This research is being undertaken alongside research on quantum computing.

Both these technologies use different techniques to overcome the threat posed by attackers. But will this be enough? This paper asks the same question. Hopefully, the question mark at the end of the name of this paper gives us a positive answer.

Some may ask, does a layman need this much security? Yes. People maybe surfing the internet at home, discussing some new market strategy over a WAN or having an affair. Or they may be living in a place where privacy rights of citizens are non-existent. For whatever reasons, the data and communications are personal and private information and nobody else's business. A person has every right to defend his privacy.

These two technologies help him to do just that.

By

M. Habibullah Pagarkar

Third Year Information Technology

V.E.S.I.T

Phone number: 3000661/659