Cryptanalysis of Grigoriev-Shpilrain Physical Asymmetric Scheme With Capacitors

Nicolas T. Courtois

University College London,
Gower Street, London, UK,
courtois@minrank.org

Abstract. Few days ago Grigoriev and Shpilrain have proposed to build a system for transmission of information without a shared secret, or essentially a sort of public key cryptosystem, based on properties of physical systems [2].
In this paper we show that their second scheme based on capacitors is insecure and extremely easy to break in practice.

Key Words: Public key cryptography, foundations, electrical engineering

1 Introduction

In a paper published few days ago, Grigoriev and Shpilrain propose to build a system for transmission of information without a shared secret, or essentially a sort of public key cryptosystem, based on properties of physical systems [2].

In particular they remark that in cryptography we use hard problems or one way functions, and claim that secure transmission is possible without computationally hard problems. This is an extremely bold (and risky) statement, because the existence of one-way functions is necessary but not sufficient for the existence of public key schemes. Therefore the authors are trying to do something that is probably somewhat substantially more difficult than .... something which already is extremely difficult. In away they are way more ambitious than people who are just trying to invent a new "public key" scheme which extremely few people has ever succeeded doing. This even though it is not meant to be a "public key" scheme in the strict sense of modern cryptography, but rather something which offers a similar functionality in practice with some assumptions.

In this paper we show that the second "public-key" scheme implemented with capacitors is insecure and that the message can be decrypted at the very beginning of the transmission and more easily than by the standard decryption procedure specified by the authors.

2 Background and the Key Idea

In [2] the authors are trying to built a public key scheme based on the following principle: **in order to transmit a message without a shared secret, the recipient needs to participate in the encryption process**. This idea is not new, on the contrary. The idea is very widely known and it is very surprising that the authors do not cite the original inventor cf. Ellis 1970 [1]. It looks like the authors are re-inventing the wheel.

2.1 Related Research

The first person to propose this idea and in this form precisely was James Ellis in 1970. Ellis is known as the senior British government secret service cryptography guru and his work remained classified during his lifetime. Interestingly Ellis has himself explained that he got the idea when studying a very old classified report on a WW2 voice scrambling method. In this invention the recipient of the message was adding noise to the line himself electrically. He therefore was the only person able to remove it and recover the cleartext (unscrambled) signal, see [1]. The original paper however was lost or has not yet been declassified and the earliest written reference available is the Ellis paper from 1970 [1] which was made public only much later in 1997.

However the objective of Ellis was **not** to built another scheme based on the laws of physics. Instead Ellis proposes to replicate this idea in pure cryptography, without any physical assumptions. This leads to the general idea of public-key cryptography which Ellis calls *non-secret encryption*, see [1]. In contrast in [2] is really about a scheme which exploits non-trivial laws of physics and in which the participants take part in the encryption process in a material and physical way.

The paper [2] is not at all the first to try to build a secure communication scheme based on laws of classical physics AND based on the aforementioned principle of the participation of the receiver in the encryption process which we know from Ellis [1]. The authors forget to mention the very well known Quantum Key Distribution.

More importantly we have the works of Laszlo Kish, who is trying to achieve something even more ambitious: a similar sort of secure cryptographic scheme which however does not use "quantum" components only simple electronic components. Kish scheme and the current paper [2] fall in the same category. The Kish scheme was proposed in 2006 Laszlo and is as method for secure key distribution. It is sometimes improperly called Kish cipher, however on its own it does not really provide a functionality of a cipher. The author calls it himself Kirchhoff's-law-Johnson-(like)-noise (KLJN) secure key distribution. Some 20 scientific and popular science papers on this topic have been written since, see [3]. The Kish scheme ressembles a lot the well-known Bennett-Brassard quantum key exchange and is based on resistors with two communicating parties which are connected to a shared electrical wire, and on the fact that the noise on the wire depends on the actions of both participants.

3 A Serious Problem with The Second PK Scheme

A close examination of the second scheme which uses capacitors reveals that it is not secure. In order to break it we do NOT need to fully understand how it works. We are just going to recall the details of the scheme which are necessary for the attack.

In the setup phase we have:

Alice's (sender's) public key: capacitance c_A.

Alice's secret message: electrical charge q_A.

Then it is claimed several times inside the paper that *even an active adversary cannot determine* q_A.

Here is how an active adversary can break the scheme:

1. Eve connects a fast on/off switch between Alice and Bob. She is going to connect the circuit just after Alice does it, with a very short delay.
   Bob cannot possibly detect this, the circuit is just switched on as normal. His view of the events is exactly the same as before.
2. When the encryption starts the circuit is closed and on the Alice side, the voltage between the two wires is $U_A = \frac{q_A}{c_A}$.
3. Eve measures the voltage very quickly with a fast oscilloscope (which is very fast and uses extremely little energy from the capacitor of Alice). Here the oscilloscope essentially acts as a quality voltmeter which is fast and has very high impedance at the entry which makes it nearly impossible to detect.
4. As soon as she has measured the voltage, she connects the circuit immediately for Bob to start receiving his message.
5. She computes the secret key $q_A = c_A \cdot U_A$.
6. It is that easy! It is also the best method Bob to receive his message. The original decryption method does NOT need to be carried.

4 Conclusion

Few days ago Grigoriev and Shpilrain have proposed to build a system for transmission of information without a shared secret, or essentially a sort of public key cryptosystem, based on properties of physical systems [2]. They propose an extremely bold idea that secure transmission of information without one-way functions might be possible, knowing that public key schemes are just much more difficult to built than one-way functions.

However we see that one can find an extremely easy and practical attack such that everyone will agree that the scheme is broken. In this paper we have shown that the second "public-key" scheme of Grigoriev and Shpilrain with capacitors [2] is insecure and can be broken very easily. More precisely we see that the message to be sent can be recovered using an oscilloscope acting essentially as a quality voltmeter. This even before the transmission begins. The adversary can recover the secret message much easier and before Bob.

Moreover Bob can also implement the same attack. He does not need to read it by the method described in the original paper. Bob can also read his secret message before it is ever transmitted in the same way as the attacker can do.

References

1. James H Ellis: *The Possibility of Non-Secret Encryption*, January 1970, 9 pages, declassified in 1997.
2. Dima Grigoriev and Vladimir Shpilrain: *Secure information transmission based on physical principles*, Preprint available at `eprint.iacr.org/2013/261`.
3. Laszlo Kish *et al.*: *Kirchhoff's-law-Johnson-(like)-noise (KLJN) secure key distribution*, also known as *Kish cypher scheme*,web page with links to some 20 scientific and popular science papers, `http://www.ece.tamu.edu/%7Enoise/research_files/research_secure.htm`