Relativistic Effects Can Keep Data Secret: A Simple Scheme

Vladik Kreinovich

Department of Computer Science
University of Texas at El Paso
El Paso, Texas 79968, USA
vladik@utep.edu

1. Computer Security without Physics

- Most existing computer security schemes rely on the computational complexity of certain computing tasks.
- For example, RSA relies on the difficulty of factoring large integers.
- These schemes use sophisticated algorithms.
- However, these schemes operate within standard computational devices.
- These devices are based on classical – non-quantum, non-relativistic – physics.

2. Computer Security and Physics

- In the 1990s, it was shown that quantum effects can be successfully used for secure communications.
- Quantum communications have indeed been used to make communications secure.
- E.g., supposedly there is a quantum communication link between the White House and the Pentagon.
- A 2016 Geneva experiment showed that relativistic effects can also be used to secure communications.

3. Main Idea

- The corresponding schemes use the fact that:
  - according to relativity theory,
  - all communication speeds are limited by the speed of light.
- These schemes are related to the problem of bit commitment in situations when:
  - the two parties do not trust each other
  - and there is no third person whom both parties trust.
- The simplest scheme involves the situation when two companies bid for the same job.
- The smallest bid wins.
- So, if one party learns about the bid of a competitor, it can offer a slightly smaller amount and win.

4. Newtonian vs. Relativistic Bidding

- Thus, if one party submits a bid earlier, the other party may learn this bid and win.
- Even if they submit simultaneously, one may submit slightly earlier and the other will learn the bid.
- Relativistic effects enable to make bidding safe:
  - if both parties submit their bids at the same time but from the different Earth locations,
  - then it takes a few milliseconds for each signal to reach the other party,
  - so no one can cheat.
- This idea can be extended to cases when we need to preserve a secret bid for up to 24 hours.

5. Relativistic Bit Commitment: Setting of the First Algorithm

- Suppose that Alice wants to select a bid B and keep it secret for time t.
- In the computer, all information is stored as 0s and 1s.
- It is thus sufficient to consider each bit d from the bid.
- Alice does not want Bob to learn the bit until time t.
- Bob wants to make sure that this bit d stays the same.
- Alice and Bob do not trust each other.
- However, Alice has a trusted friend Amy.
- At first, all three on them are at the same location.

6. Relativistic Bit Commitment: First Algorithm

- Alice selects (and shares with Amy):
  - a bit d and
  - a random integer a from 1 to N.
- After this, Amy moves to a faraway location, at a distance $r > c \cdot t$.
- After that, Bob generated a random integer $b \in \{1, \ldots, N\}$, and sends it to Alice.
- Alice replies with $r = a + b \cdot d \bmod N$.
- So, Bob gets either a or $a + b$.
- Then, Amy sends a to Bob.
- Once Bob gets a, he compares a with Alice's answer:
  - if $r = a$, this means that $d = 0$;
  - if $r = a + b$, this means that $d = 1$.

7. Why This Works

- Bob cannot find d:
  - all he knows is a random number,
  - without knowing a, we cannot tell whether it is a or $a + b$.
- Amy cannot cheat:
  - from the moment Alice learns b,
  - it takes Alice at least time t to send b to Amy, and at least as long to send the reply to Bob,
  - so a b-dependent reply cannot get to Bob before time t.

8. Limitations of This Algorithm

- This algorithm is guaranteed to store a secret bit for time $t = r/c$.
- For Earth locations, this time is limited to milliseconds.
- To store a secret for a second, Amy needs to move to the Moon.
- To store a secret for 24 hours, Amy must go beyond Solar systems.
- This is good for the future, but we cannot do it yet.
- So, to store a bit for longer than milliseconds, we need a different algorithm.

9. Second Algorithm

- In the second algorithm, Bob also has a trusted friend Brian.
- At first, Alice and Amy select a sequence of random numbers $a_1, \ldots, a_m$.
- Simultaneously, Bob and Brian select their sequence of random numbers $b_1, \ldots, b_m$.
- Then, Amy and Brian jointly move away to a distance $r > c \cdot \Delta t$.
- First, Bob sends b_1 to Alice, she replies with

$$r_1 = a_1 + b_1 \cdot d.$$

- After time Δt, Brian sends b_2 to Amy, she replies with

$$r_2 = a_2 + b_2 \cdot a_1.$$

10. Second Algorithm (cont-d)

- Since $r > c \cdot \Delta t$, neither Amy not Brian have information about the first exchange.
- After time Δt, Bob sends b_3 to Alice, she replies with

$$r_3 = a_3 + b_3 \cdot a_2, \text{ etc.}$$

- At each cycle m, Bob or Brian send b_m, and get

$$r_m = a_m + b_m \cdot a_{m-1}.$$

- At the end, Amy and/or Alice reveal a_m and d.
- Based on a_m and $r_m = a_m + b_m \cdot a_{m-1}$, Bob and Brain can compute $b_m \cdot a_{m-1}$.
- Since they know b_m, they can compute a_{m-1}.
- Similarly, from a_{m-1} and $r_{m-1} = a_{m-1} + b_{m-1} \cdot a_{m-2}$, we can compute $b_{m-1} \cdot a_{m-2}$ hence a_{m-2}, etc.

11. Second Algorithm: Discussion

- Eventually, based on $r_1 = a_1 + b_1 \cdot d$, a_1, and b_1, Bob and Brian can compute d.
- So, Bob and Brian have:
  - the value d that was officially disclosed by Amy and
  - the value d that was used originally – that they can calculate.
- So, Bob and Brian can then check that it is the same d as before.
- If we have m pairs of random numbers, we can keep a secret during time $m \cdot \Delta t$.
- The larger m, the longer we can keep a secret.
- In Geneve, Switzerland, the secret was kept for 24 hours.

12. References

- A. Kent, *Phys. Rev. Lett.* 83, 1447 (1999).
  http://dx.doi.org/10.1103/PhysRevLett.83.1447
- T. Lunghi et al., *Phys. Rev. Lett.* 115, 030502 (2015).
  http://dx.doi.org/10.1103/PhysRevLett.115.030502
- K. Chakraborty, A. Chailloux, A. Leverrier, *Phys. Rev. Lett.* 115, 250501 (2015).
  http://dx.doi.org/10.1103/PhysRevLett.115.250501
- S. Fehr and M. Fillinger, in: M. Fischlin and J.-S. Coron, (eds.), *Proceedings of the 35th Annual International Conference on Advances in Cryptology Eurocrypt'2016*, Springer (2016), Pt. II, p. 477.
- E. Verbanis et al., *Phys. Rev. Lett.* 117, 140506 (2016).
  http://dx.doi.org/10.1103/PhysRevLett.117.140506