A Framework for Unconditionally Secure Public-Key Encryption (with Possible Decryption Errors)

M. Bessonov, D. Grigoriev, V. Shpilrain

NYCCT

May 13, 2018

Unconditionally secure public-key encryption

- Unconditionally secure (i.e., secure without any computational assumptions) public-key encryption is impossible if the legitimate receiver decrypts correctly with probability exactly 1.
- What if this probability is less than 1?
- More precisely, what if the sender transmits a single encrypted bit and the legitimate receiver decrypts it correctly with probability P?

$$1/2 < P < 1$$

The sender advantage

If decryption errors are possible

- sender has an **advantage** over the eavesdropper
- sender knows exactly what the transmitted secret bit is.

Thus, we make the sender guess the receiver's decryption key to gain an advantage.

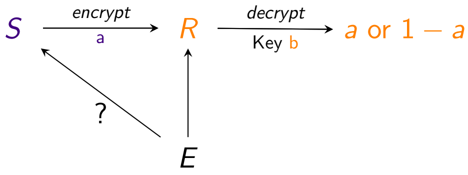
New scheme

Existing schemes: adversary competes with the *receiver*

In our scheme: adversary competes with the **sender**

Goal of the sender: guess receiver's decryption key to decrypt correctly

Goal of the adversary (eavesdropper): guess sender's secret bit correctly.



The scheme

Alice transmits a bit a to Bob

Bob has a private decryption key b

Eve is a computationally unbounded adversary

Proposition

In our scheme, $P_A =$ probability that Alice is successful $> 1/2$

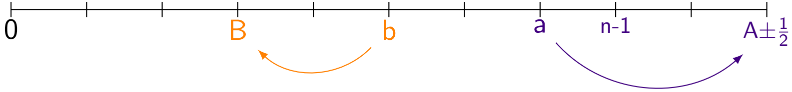
(i.e., to guess Bob's private decryption key b)

$P_E =$ probability that Eve is successful $= 1/2$
(i.e., to guess Alice's bit a)

The scheme

1. Bob selects an integer b from the interval $[0, n-1]$ and performs a random walk with $h(n)$ steps, ending at B. Bob publishes B.

2. Step 2 is repeated by Alice m times. Alice selects an integer a from the interval $[B, n-1]$ and performs a random walk. She selects with probability $1/2$ between $f(n)$ steps and $g(n)$ steps, and her walk ends at A. She adds or subtracts $1/2$ to/from A for her final endpoint.



The scheme

3. Alice groups the m random walks into two groups and selects a group with equal probability:
   Group 1: those with $A < B$
   Group 2: those with $A > B$.

4. From the chosen group in step 2, with equal probability, Alice selects between random walks with $f(n)$ steps and those with $g(n)$ steps. (If empty, go back to Step 2). Alice selects one random walk uniformly at random. Let a_0 be the starting point.

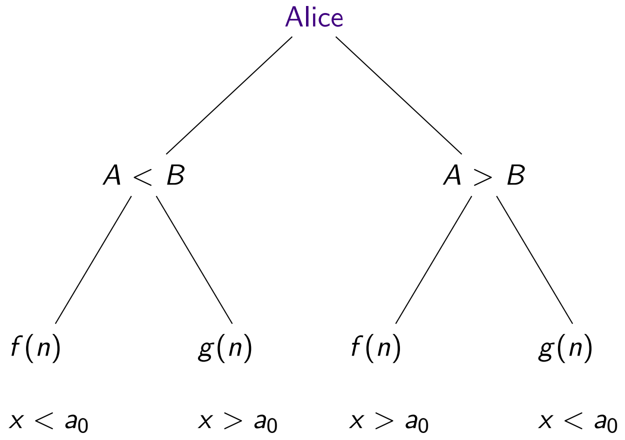
The scheme

5. If the random walk selected is from group
   $f(n)$, $A < B$ or $g(n)$, $A > B$, choose $x < a_0$
   $f(n)$, $A > B$ or $g(n)$, $A < B$, choose $x > a_0$

6. Alice assumes that b is in the interval she selected and encrypts her bit accordingly
   (i.e., labels her selected interval with her secret bit c and the other interval with $1 - c$).
   She sends the a_0 and the above interval labeling to Bob.

7. Bob recovers the bit corresponding to the label of the interval where his b is.

The scheme

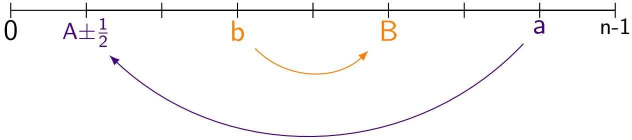


How this works

Suppose $f(n)$ is large and $g(n)$ is small.

$$P\left(b < a \middle| A < B < a\right) \qquad (1)$$

is higher if Alice has $f(n)$ steps



With high probability, Alice's guess of b is correct if she chooses a walk with $f(n)$ steps

But Alice is also trying to confuse Eve, so she may choose a walk with $g(n)$ steps

Still, it is possible to have $P_A > 1/2$, yet $P_E = 1/2$

Experimental results

With $f(n) = 100,000$ steps for Alice, success rate in a single run of the protocol was 76%.

With $g(n) = 2000$ steps for Alice, success rate in a single run of the protocol was 34%.

Thus, $P_A = \frac{1}{2}(0.76 + 0.34) = 0.55$.

At the same time, $P_E = 0.5$.