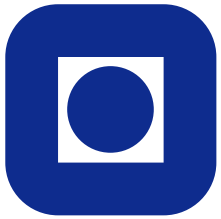


NTNU
Norwegian University of
Science and Technology

Internet voting in Norway

Kristian Gjøsteen

Department of mathematical sciences, NTNU

Luxembourg, May 26, 2011

Innhold

[. . .] mathematical proof can be given that the vote remains unchanged from the time it leaves the voter until it is counted [. . .]

Minister for local government in the Norwegian Parliament, 19.11.2010

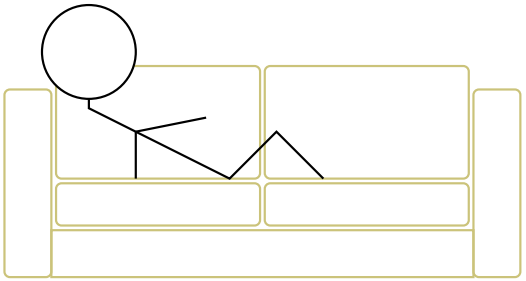
Basic premise

In Norway, we

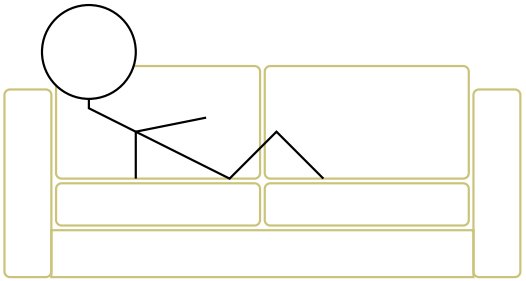
- trust the government not to conspire against us; but
- we do not trust the government not to mess up.

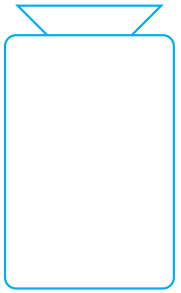
Elections and sofas

Elections and sofas

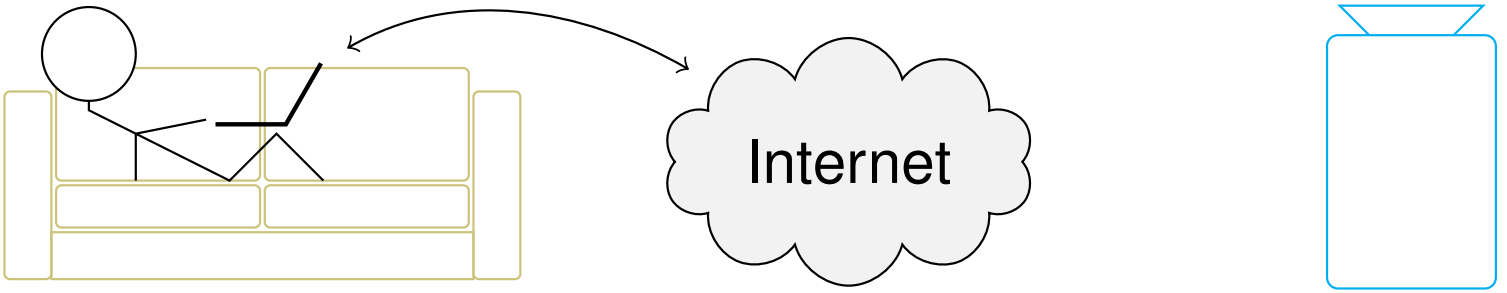


Elections and sofas

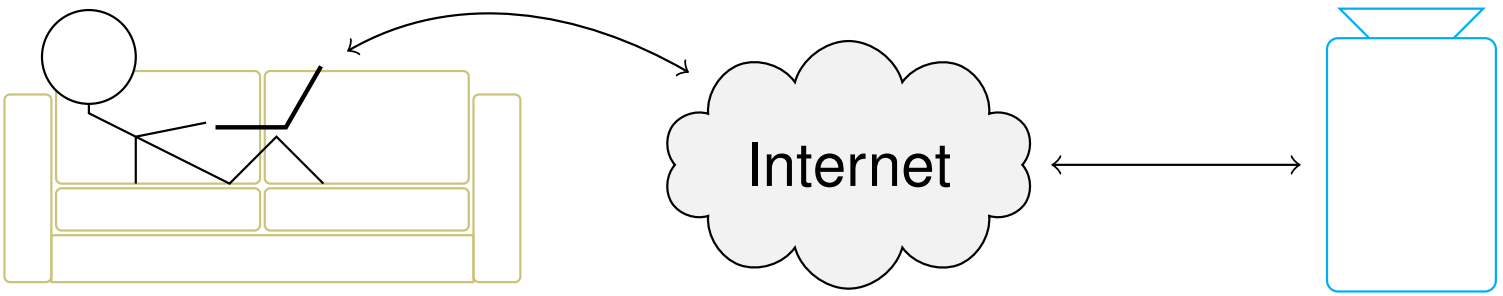




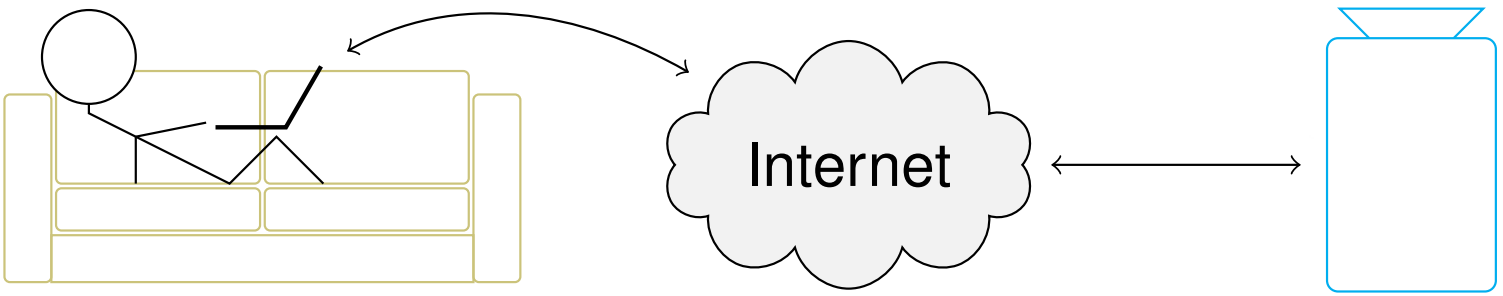
Elections and sofas



Elections and sofas



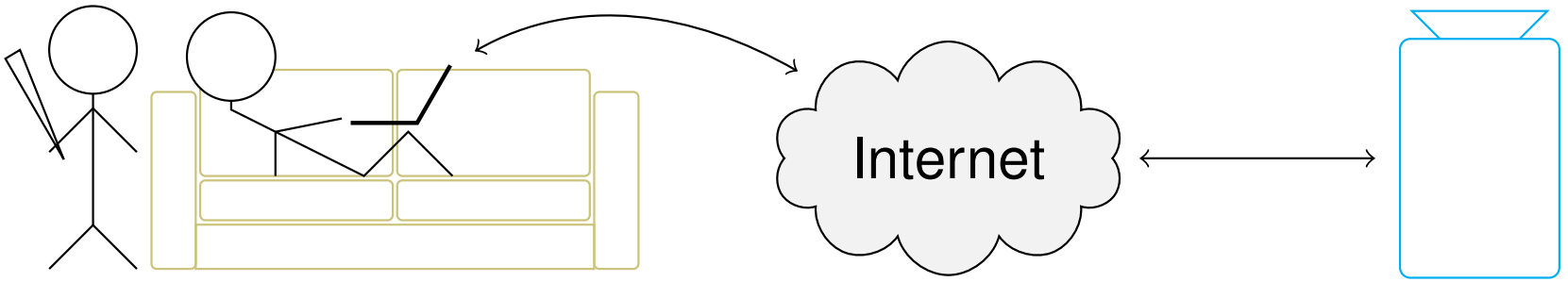
Elections and sofas



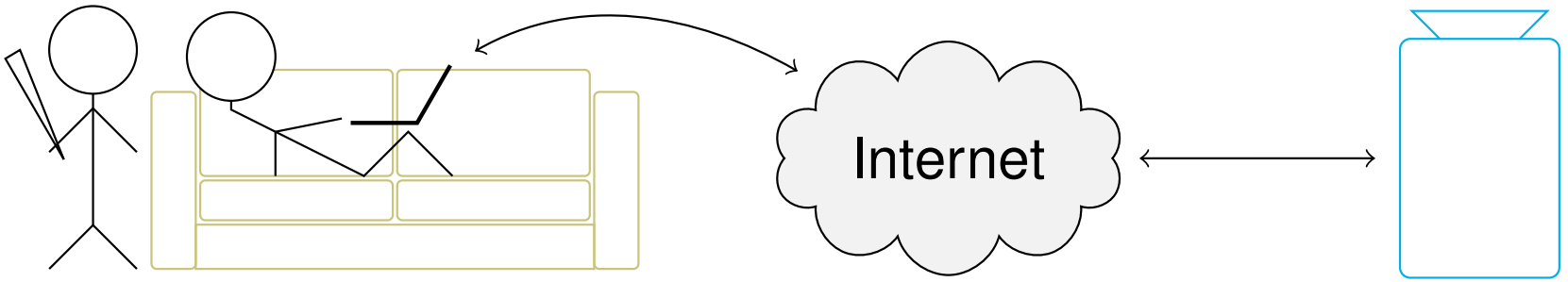
Increase accessibility for voters

- with disabilities
- abroad

Elections and sofas



Elections and sofas



- Only advance voting.
- Electronic revoting allowed.
- Paper vote cancels past *and future* electronic ballots.

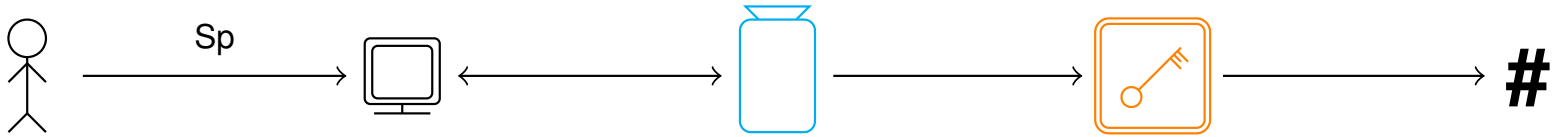
The procurement process

- System source code to be made public.
- A *competitive tender*, where vendors help write the final tender documents.
- Academics and others were also involved.

Eventually three bids were received. Scytl won.

Overview

integrity — secrecy

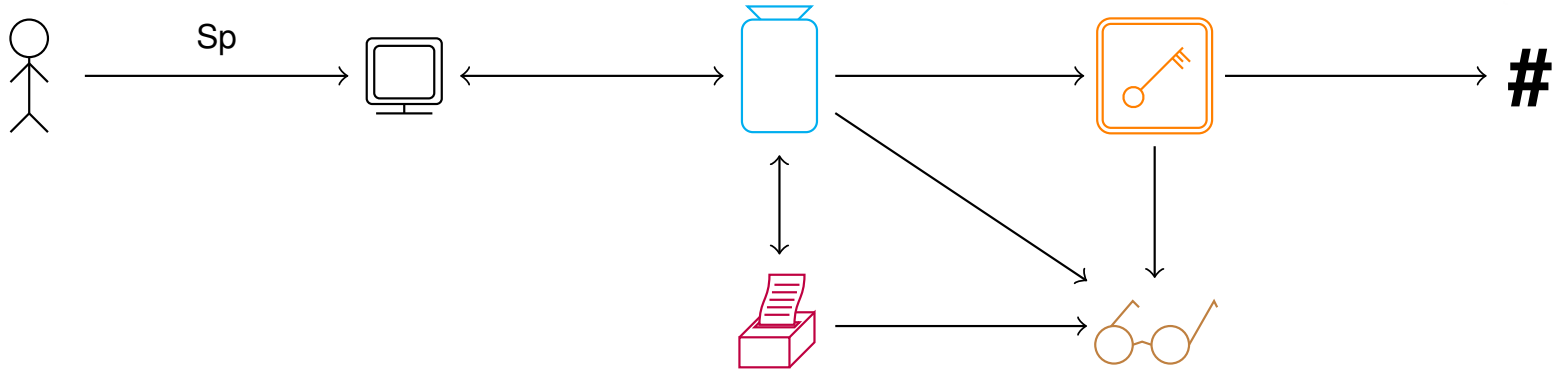


ballot box —

— decryptor —

Overview

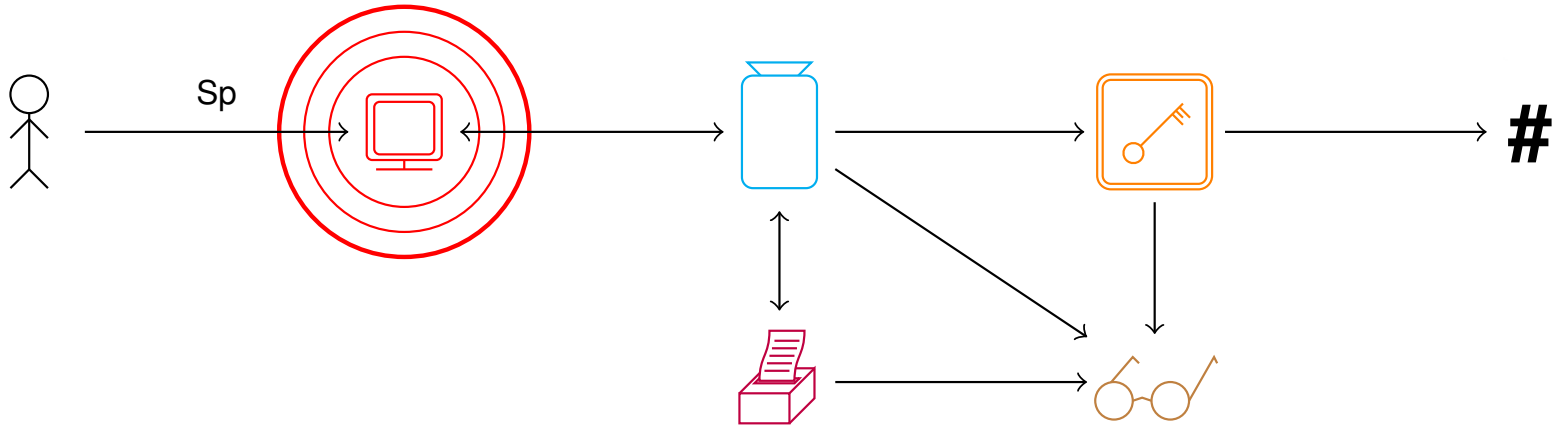
integrity — secrecy



ballot box — receipt generator — decryptor — auditor

Overview

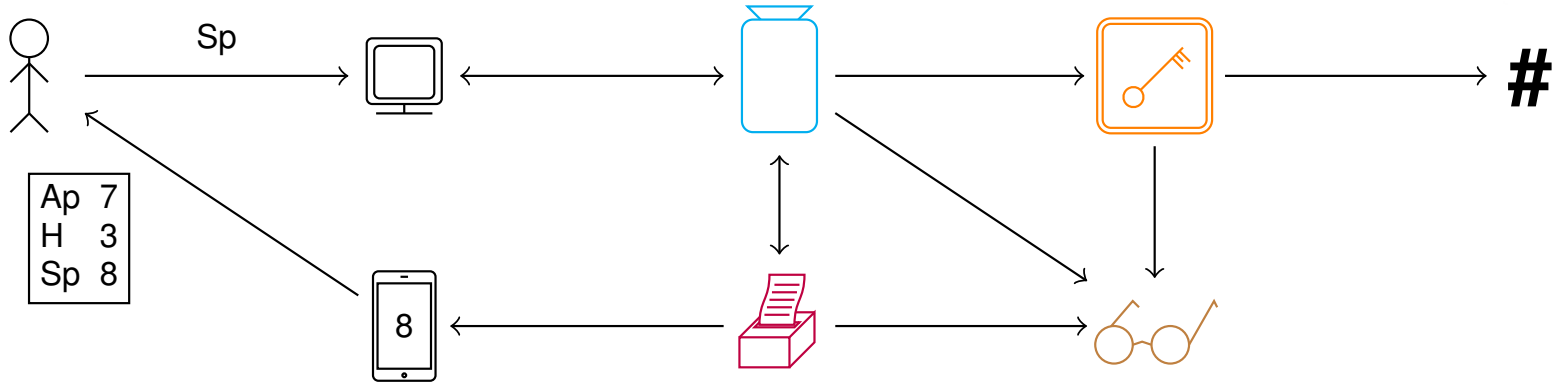
integrity — secrecy



ballot box — receipt generator — decryptor — auditor

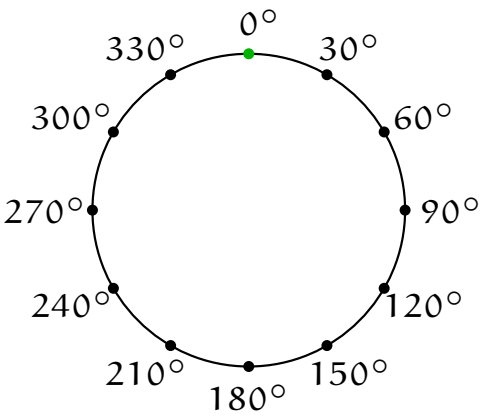
Overview

integrity — secrecy



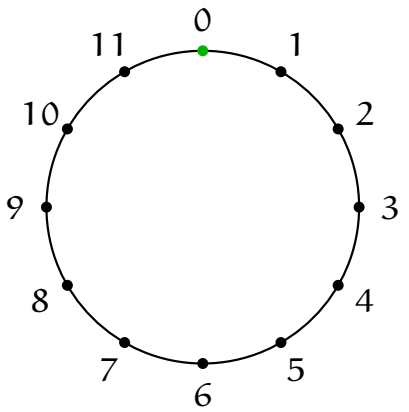
ballot box — receipt generator — decryptor — auditor

Where are we?



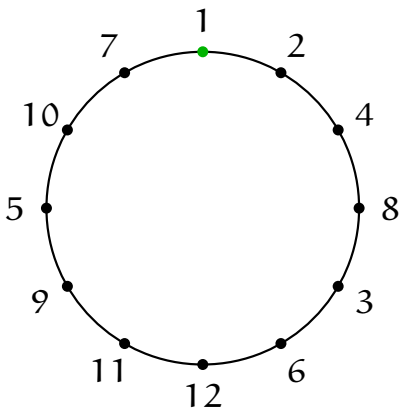
Let G be a prime order finite group.

Where are we?



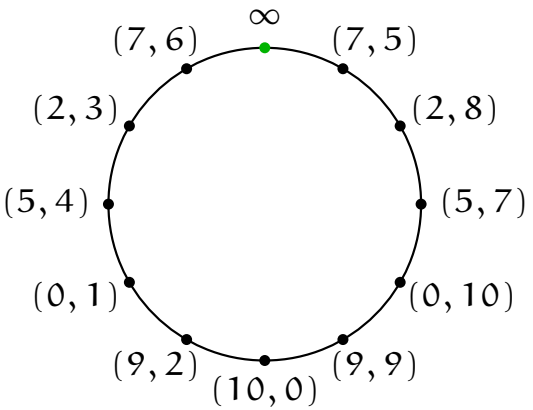
Let G be a prime order finite group.

Where are we?



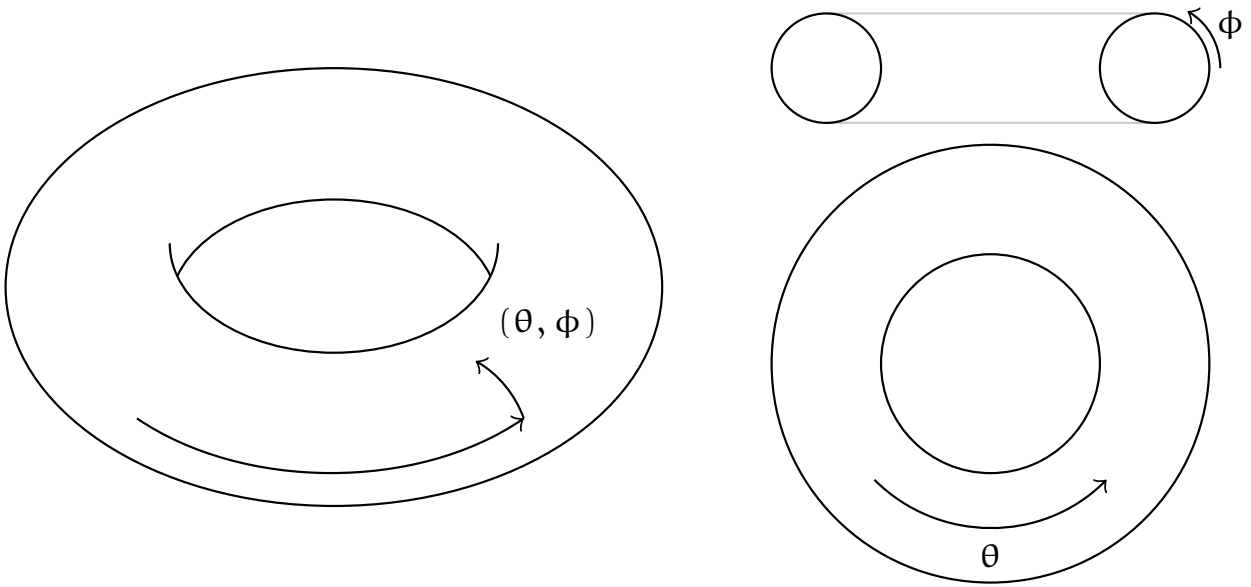
Let G be a prime order finite group.

Where are we?



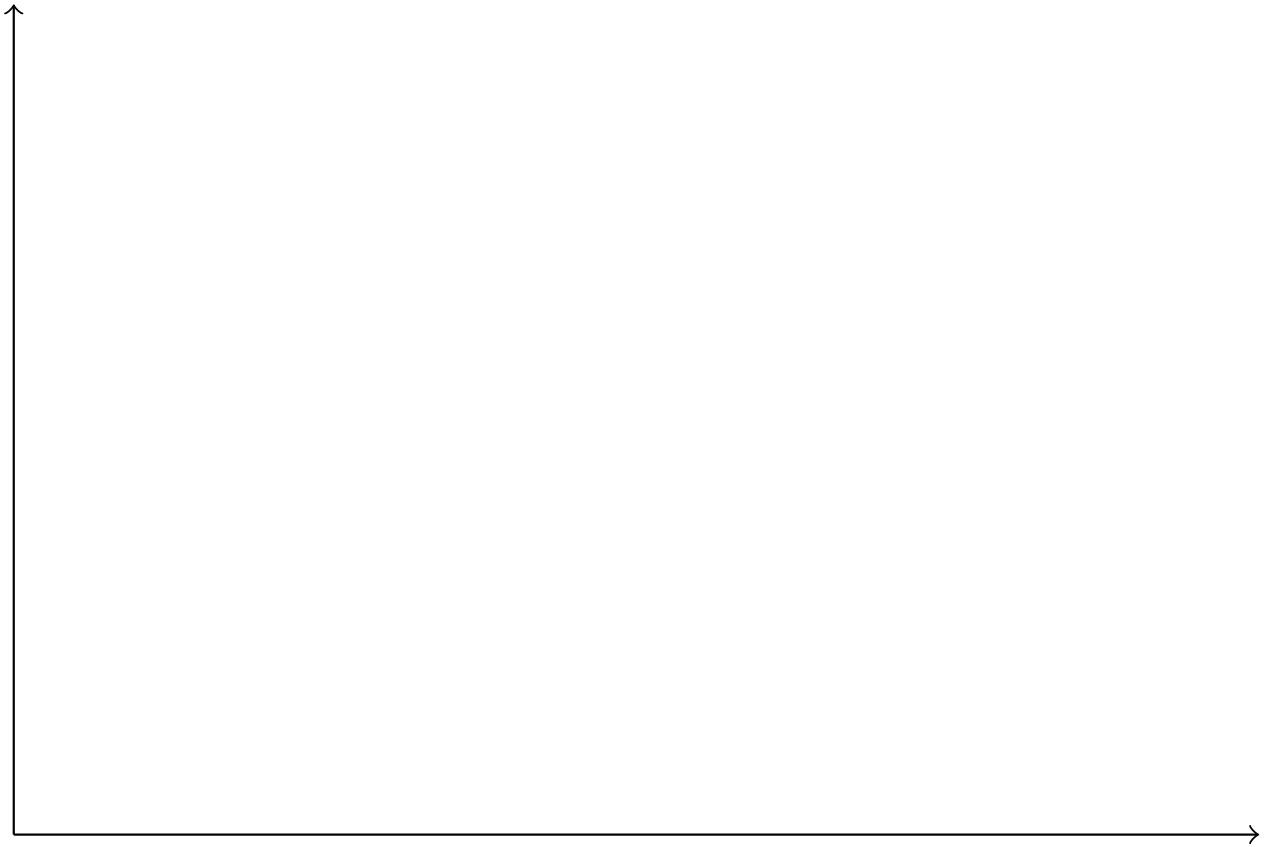
Let G be a prime order finite group.

Where are we?



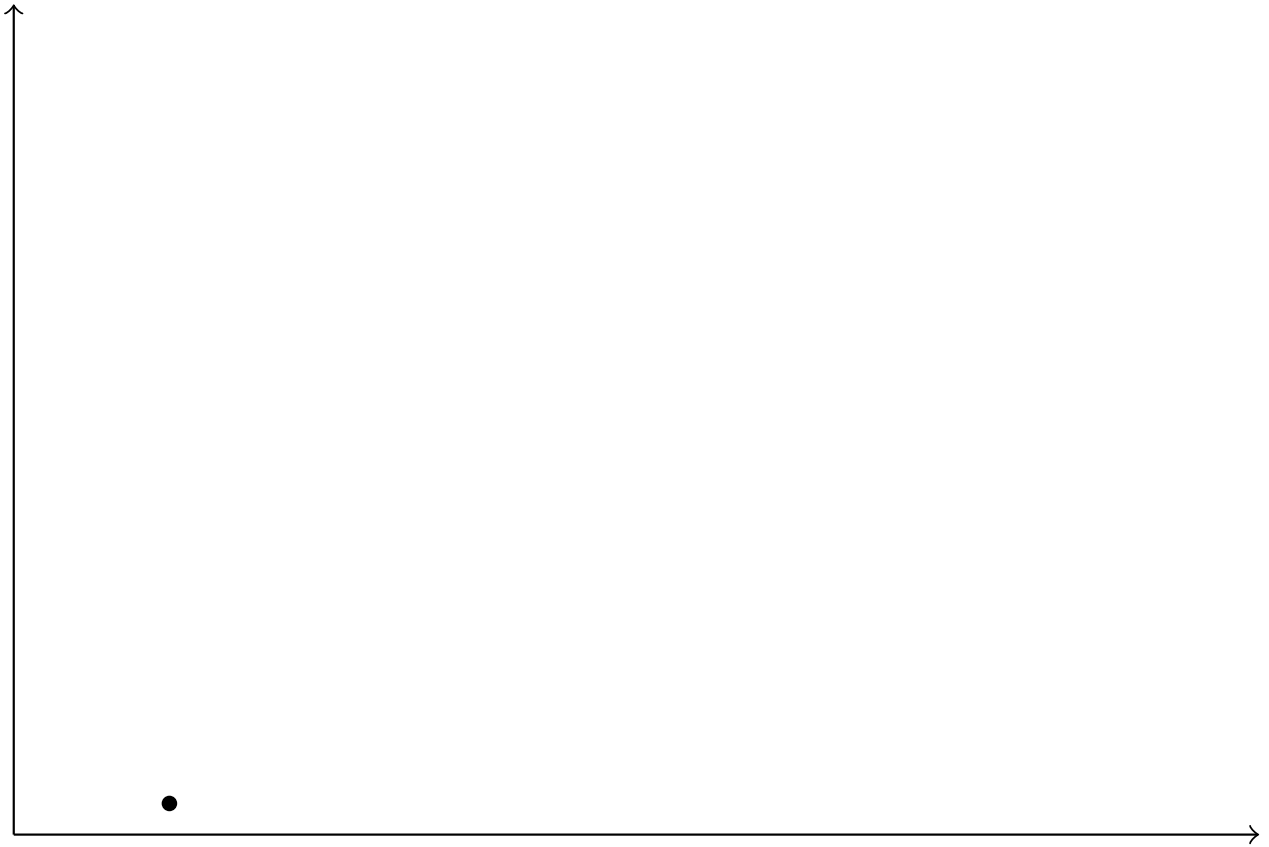
This is $G \times G$.

Properties

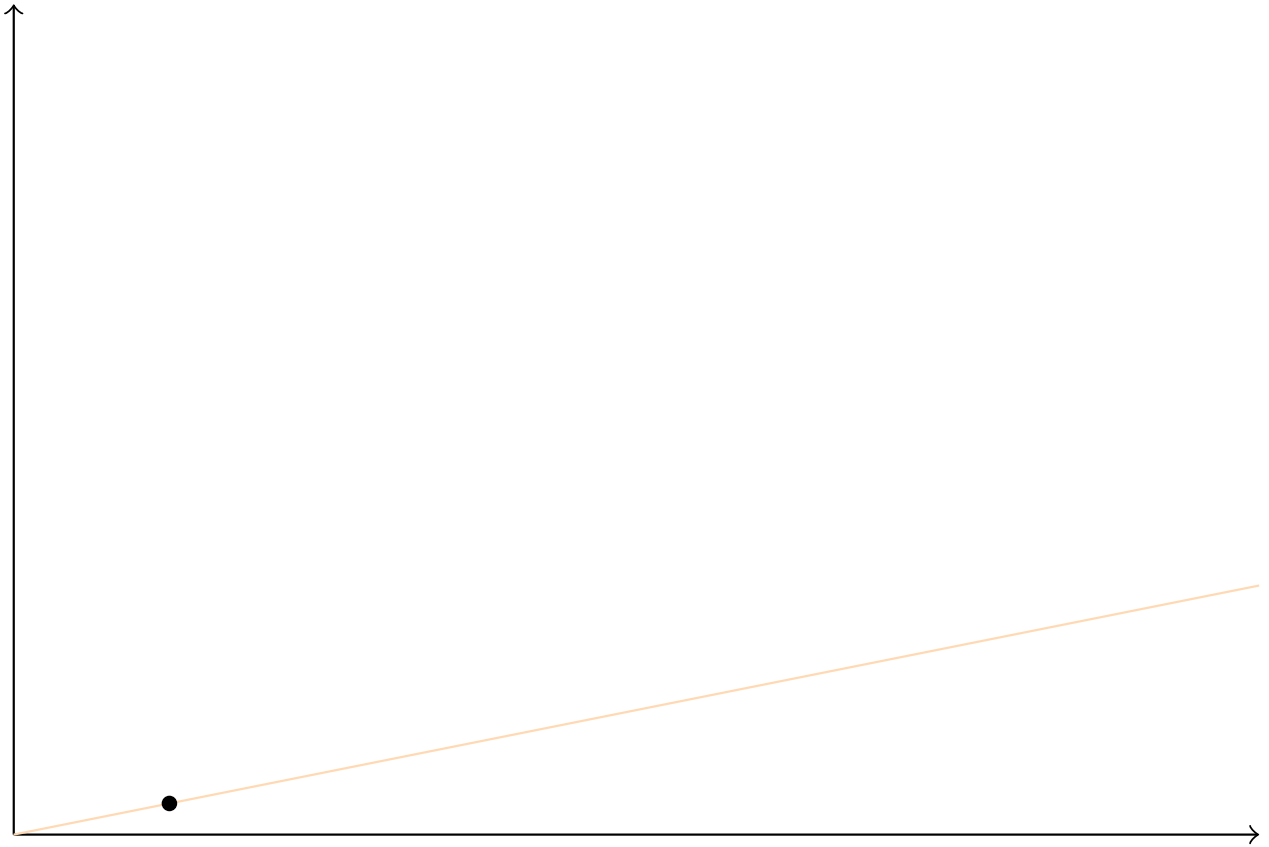


Easier to draw a plane.

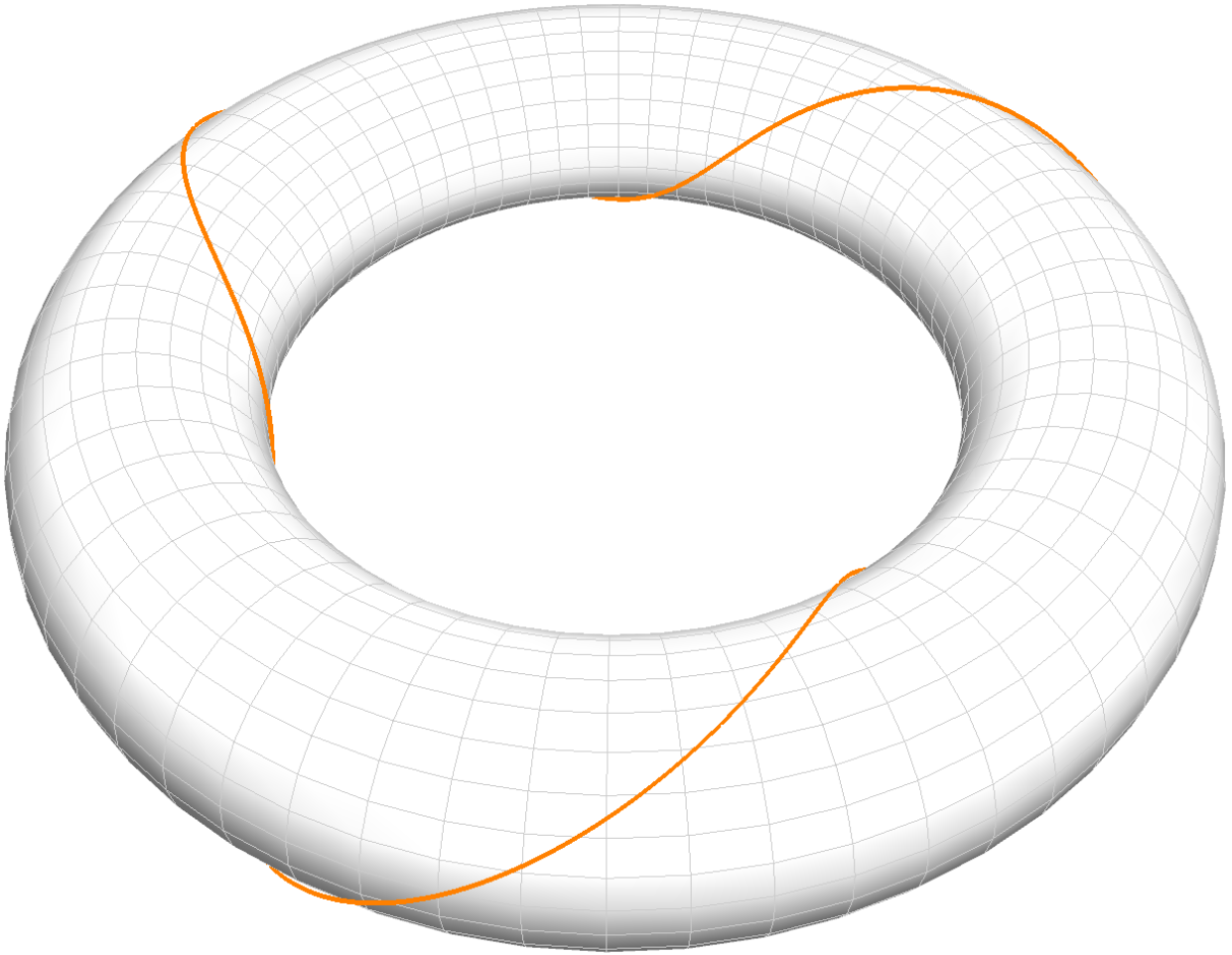
Properties



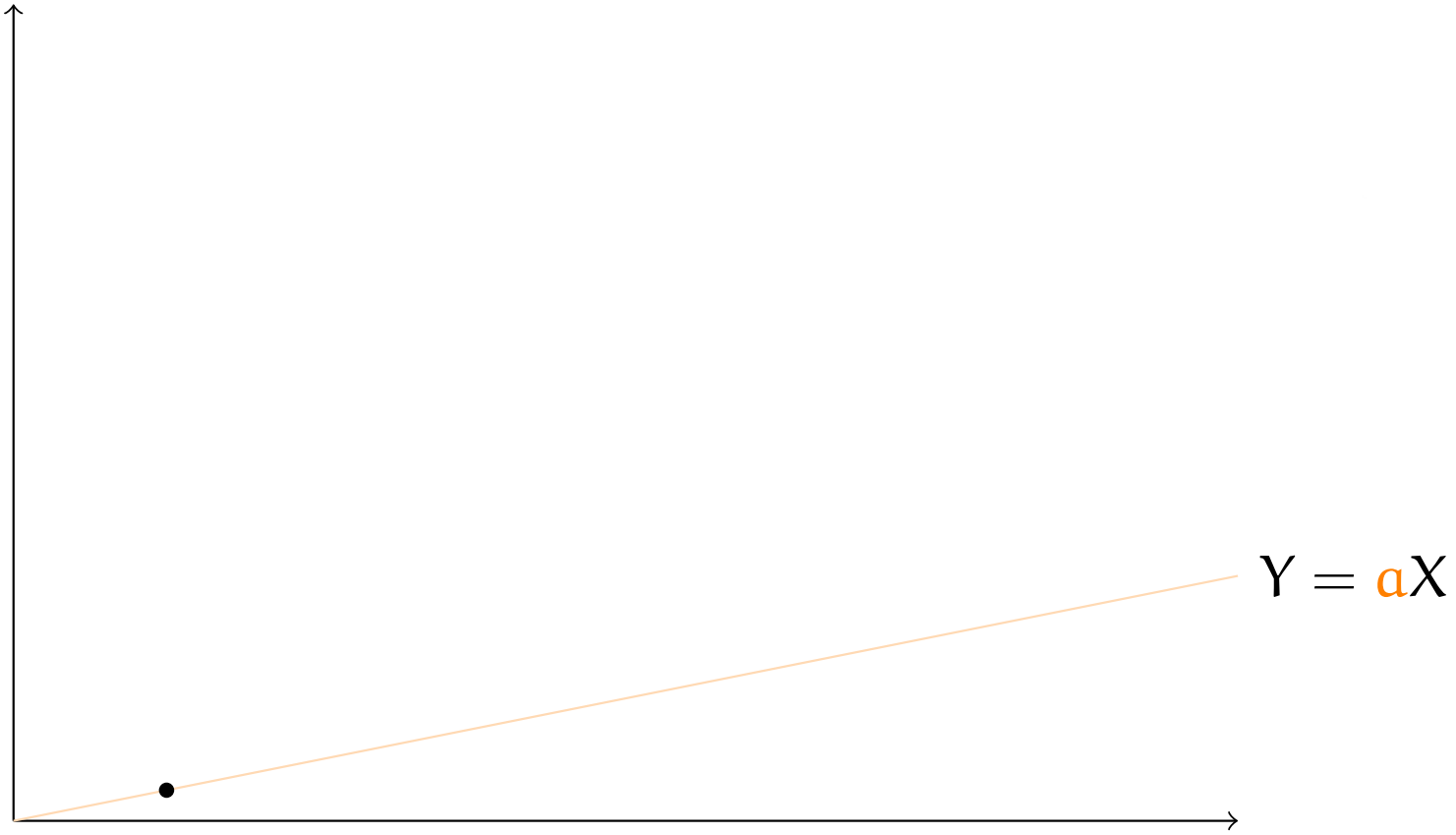
Properties



Lines on donuts

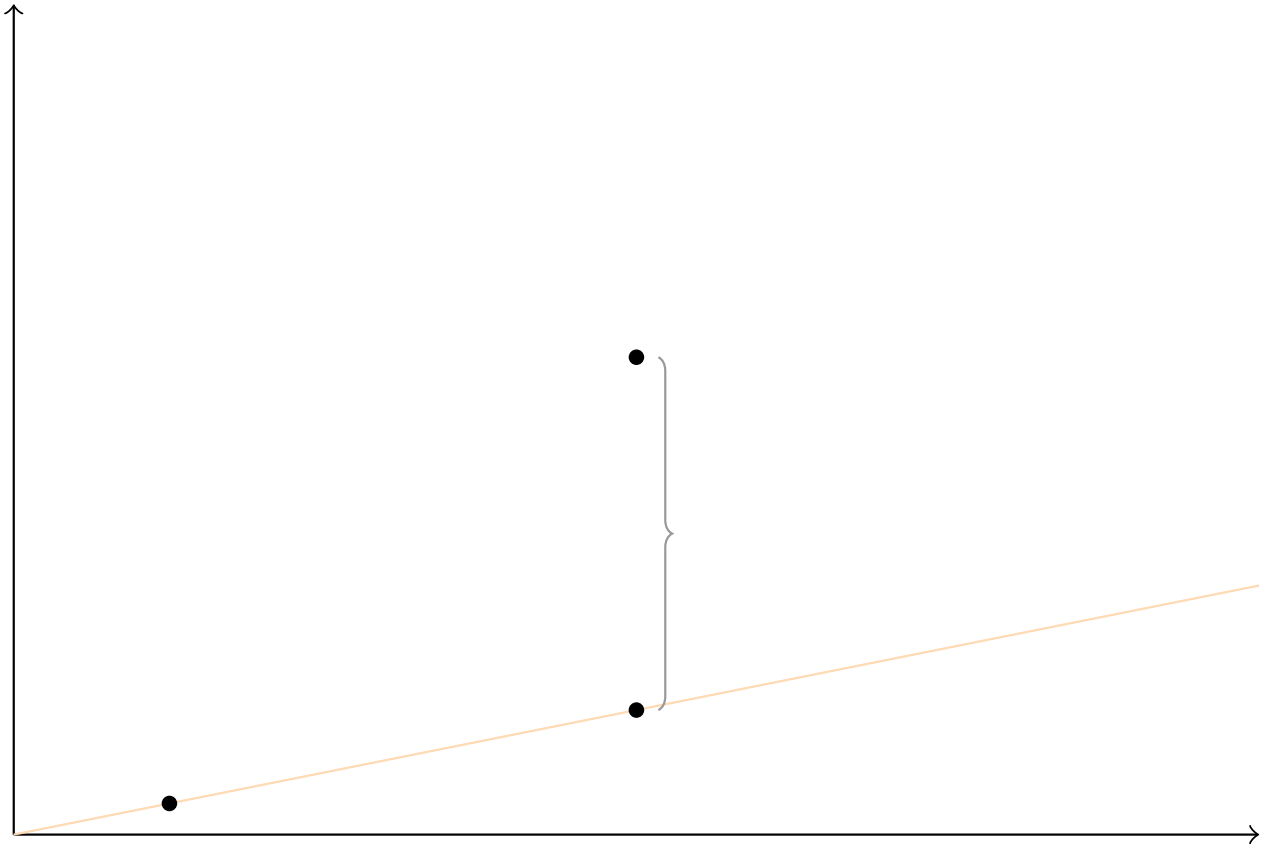


Properties



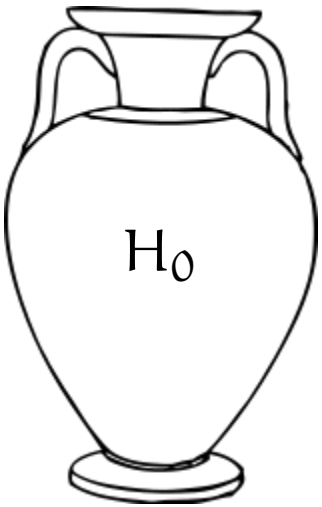
What is the slope of the line? *Discrete logarithms.*

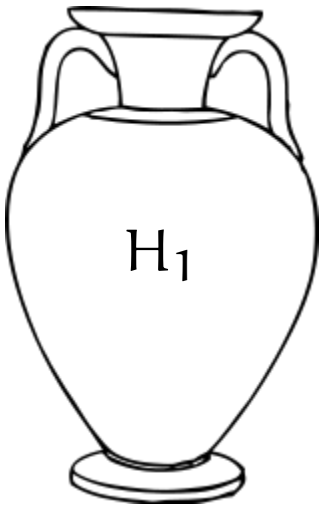
Properties



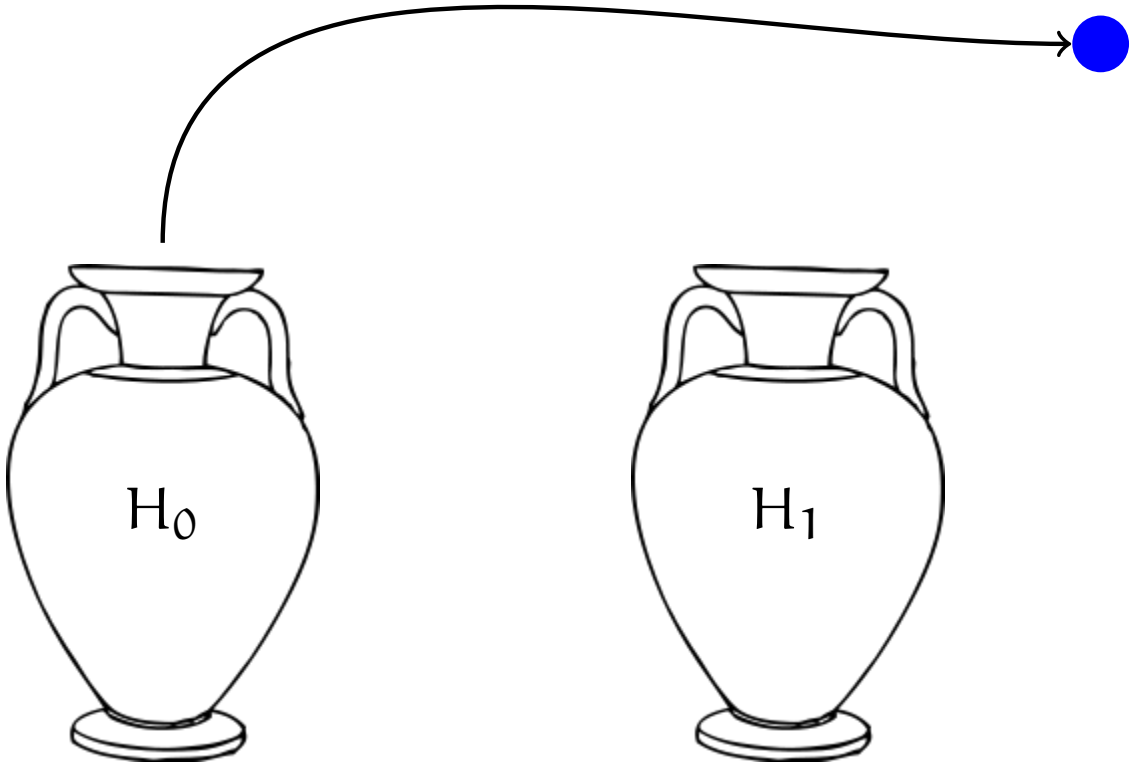
What is the vertical distance from a randomly chosen point down to the line? *Computational Diffie-Hellman*.

Hypothesis testing

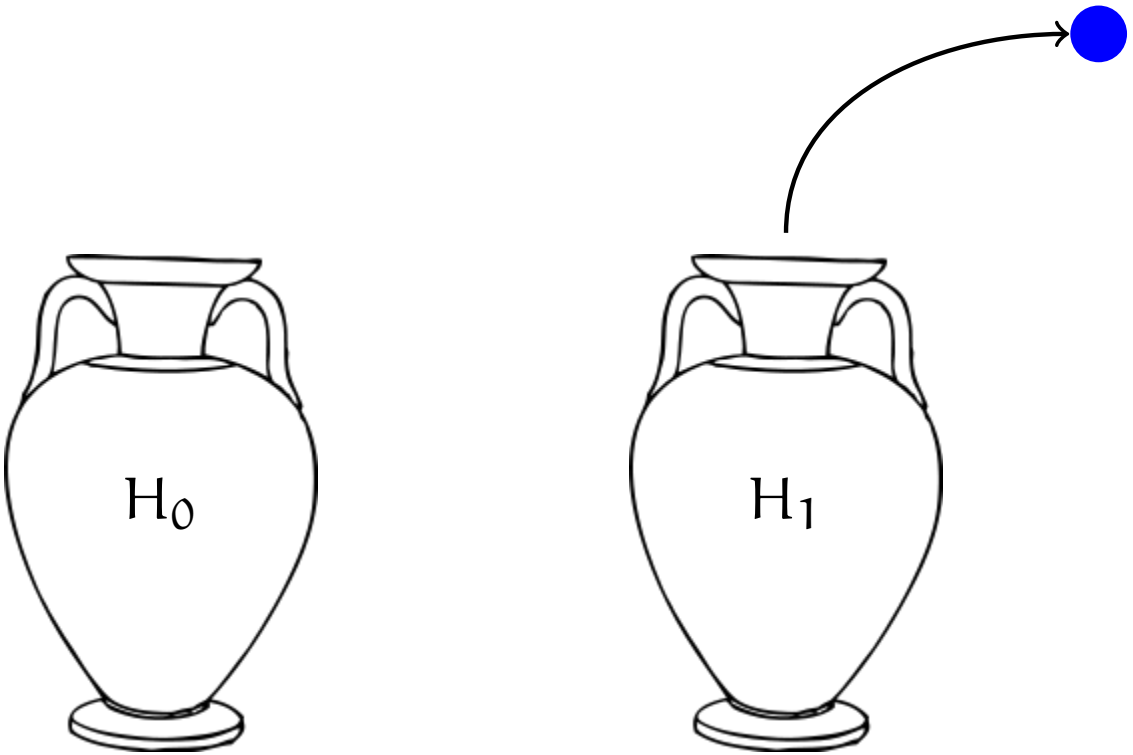




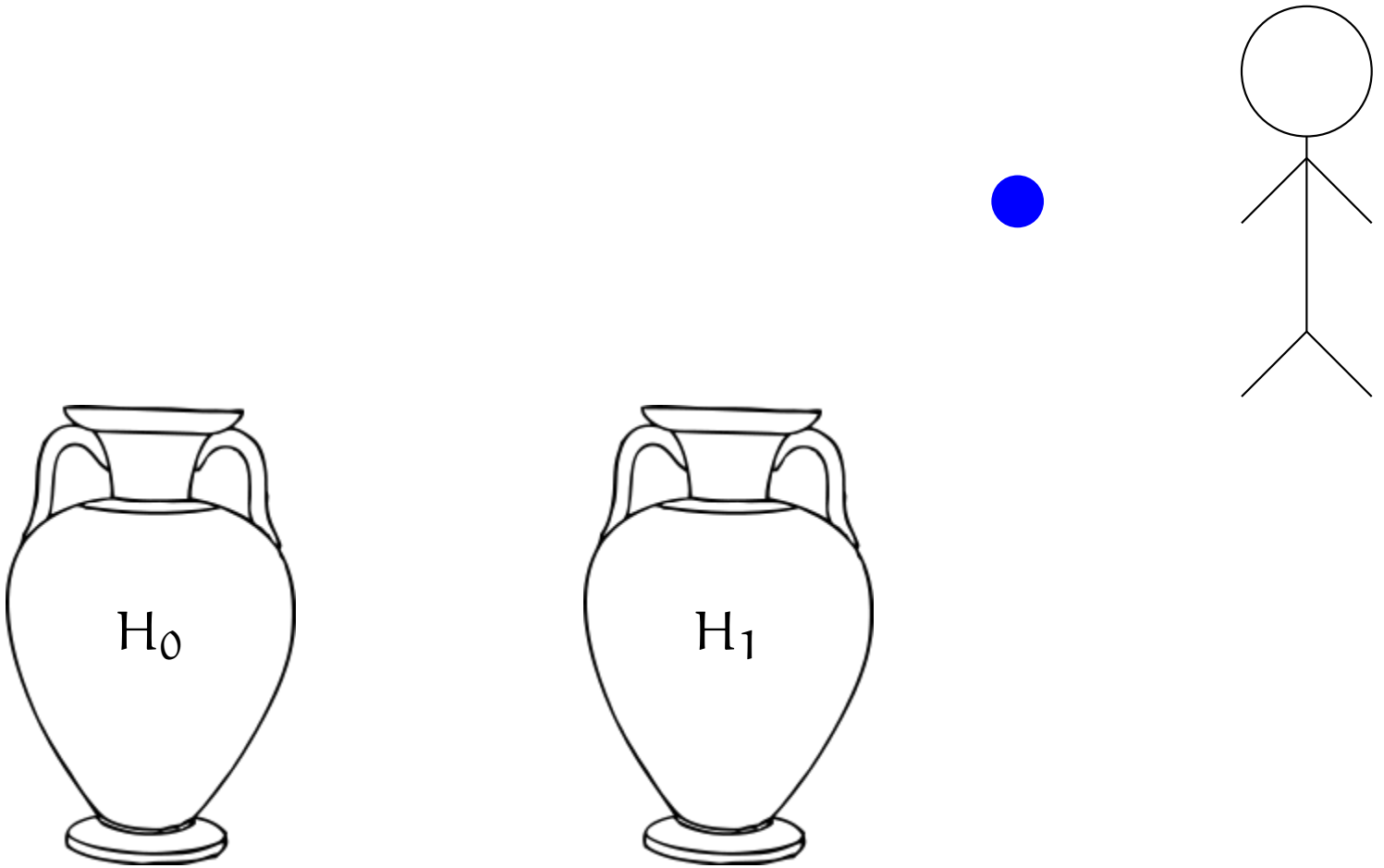
Hypothesis testing



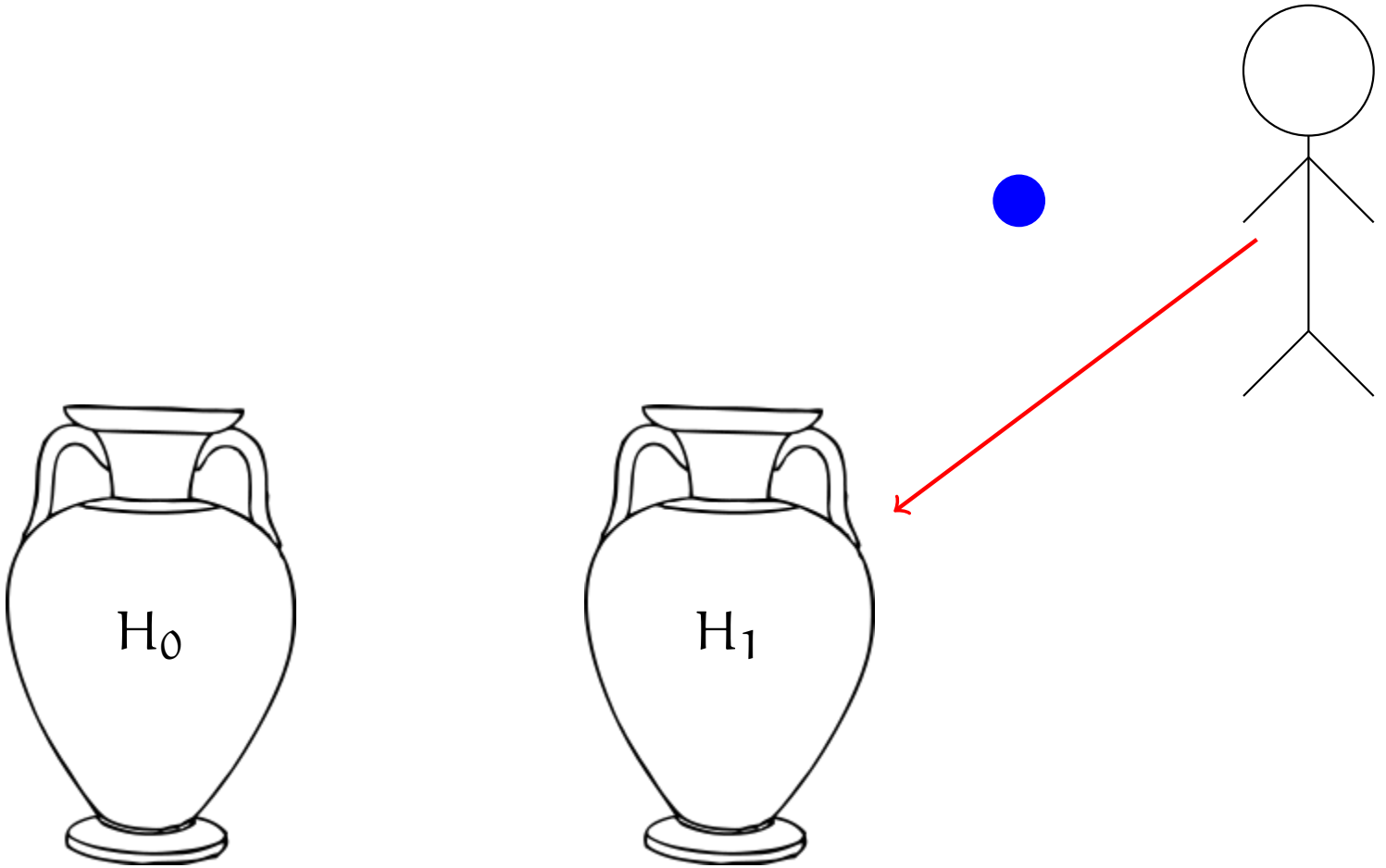
Hypothesis testing



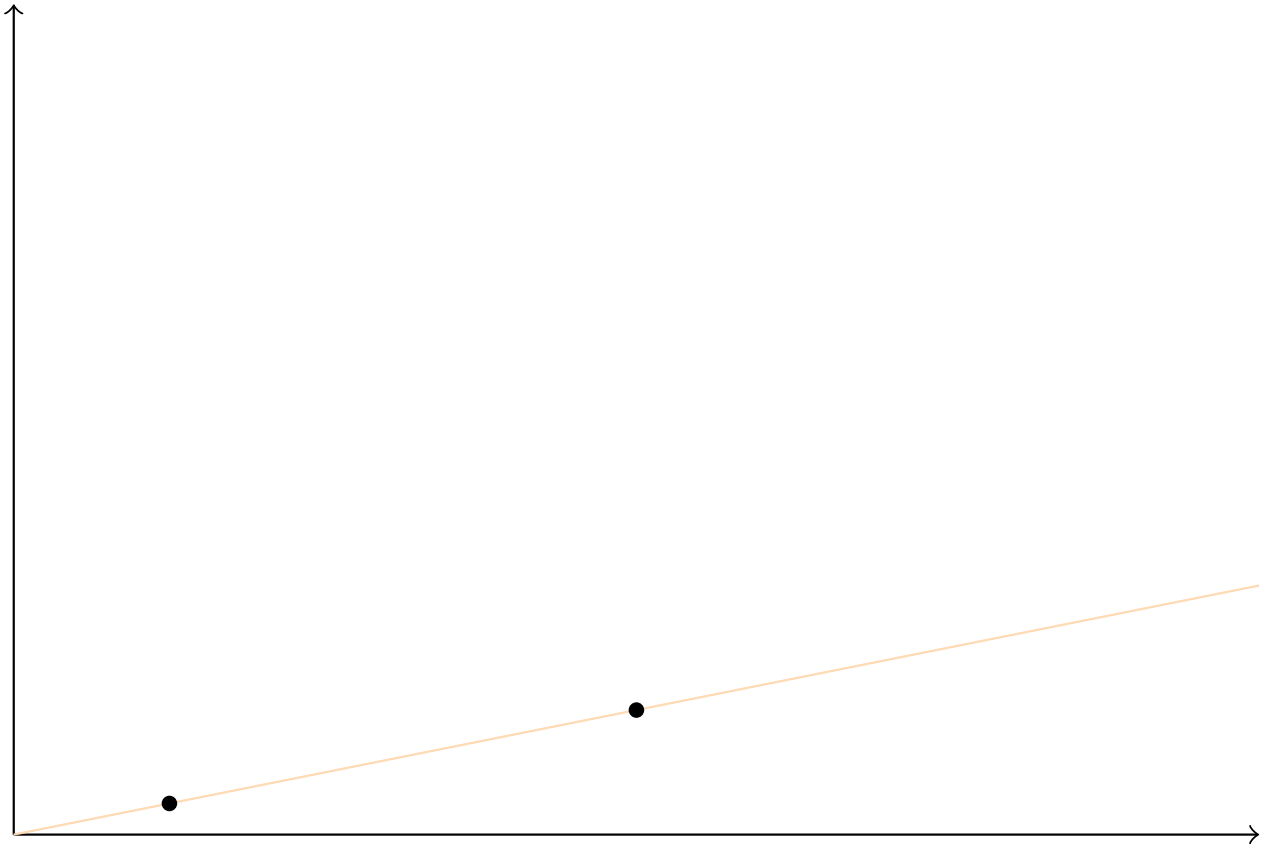
Hypothesis testing



Hypothesis testing

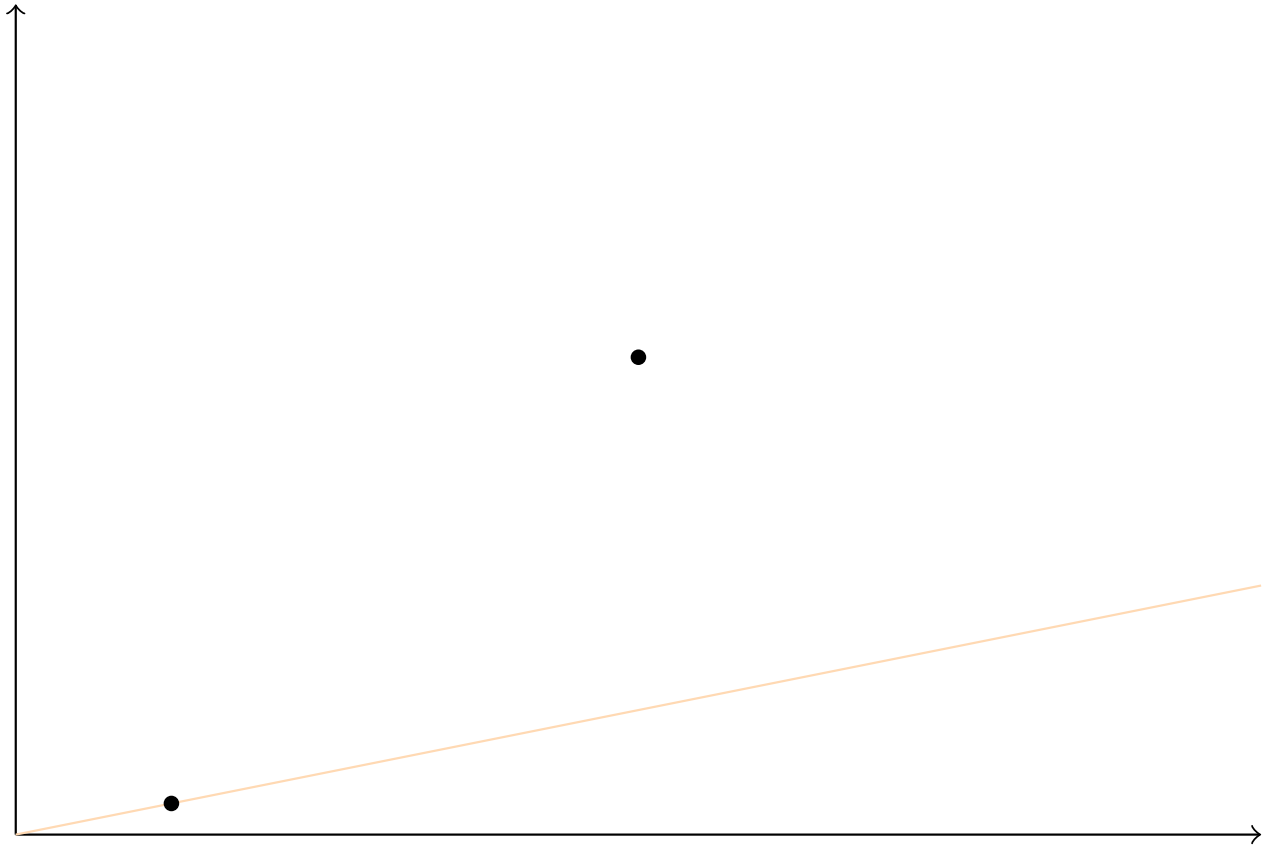


Properties



Is the right-most point sampled at uniform from the line or from the entire plane? *Decision Diffie-Hellman*.

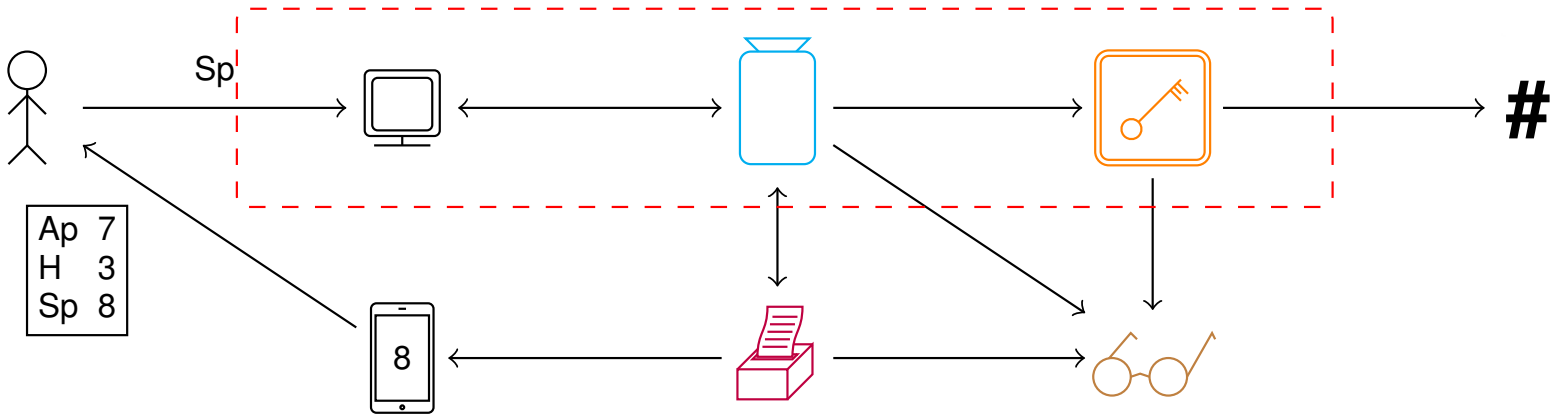
Properties



Is the right-most point sampled at uniform from the line or from the entire plane? *Decision Diffie-Hellman*.

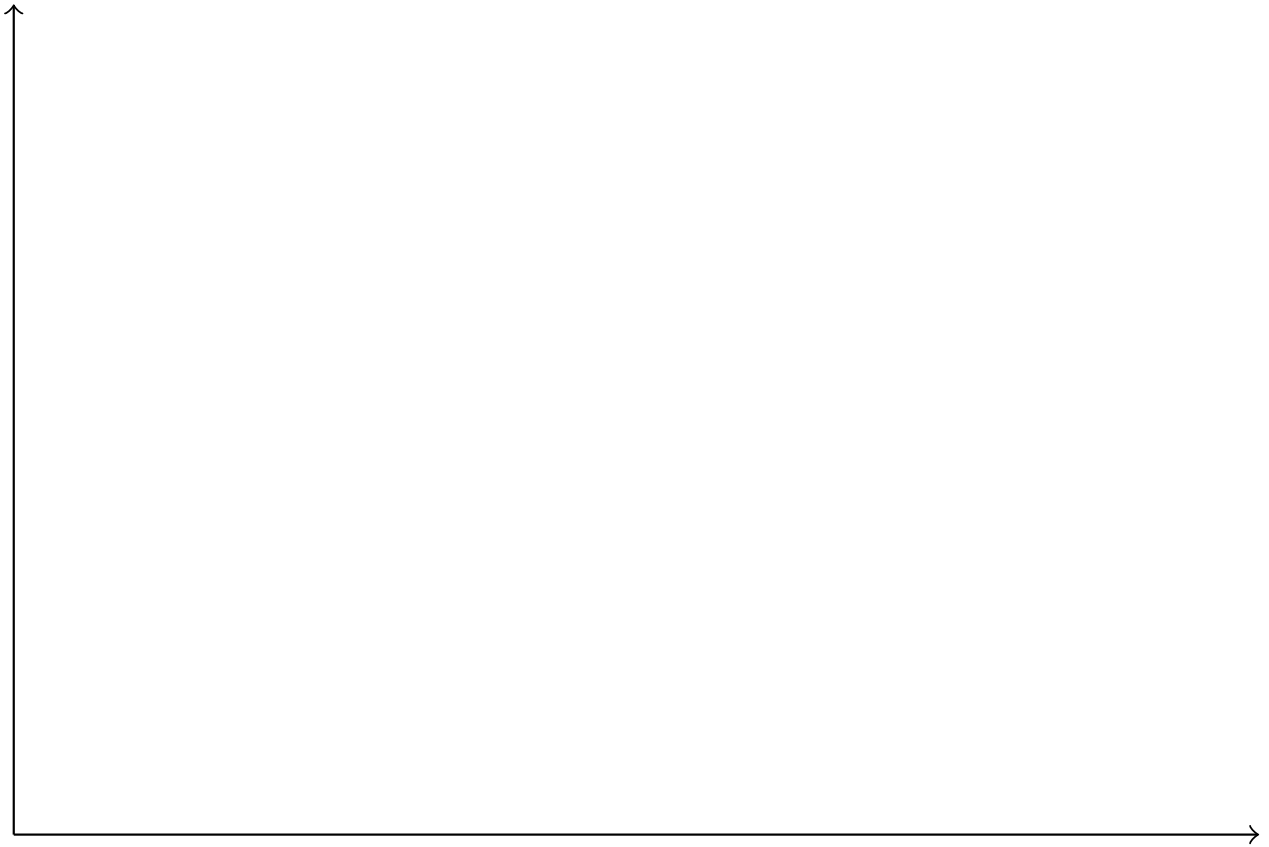
Overview

integrity — secrecy



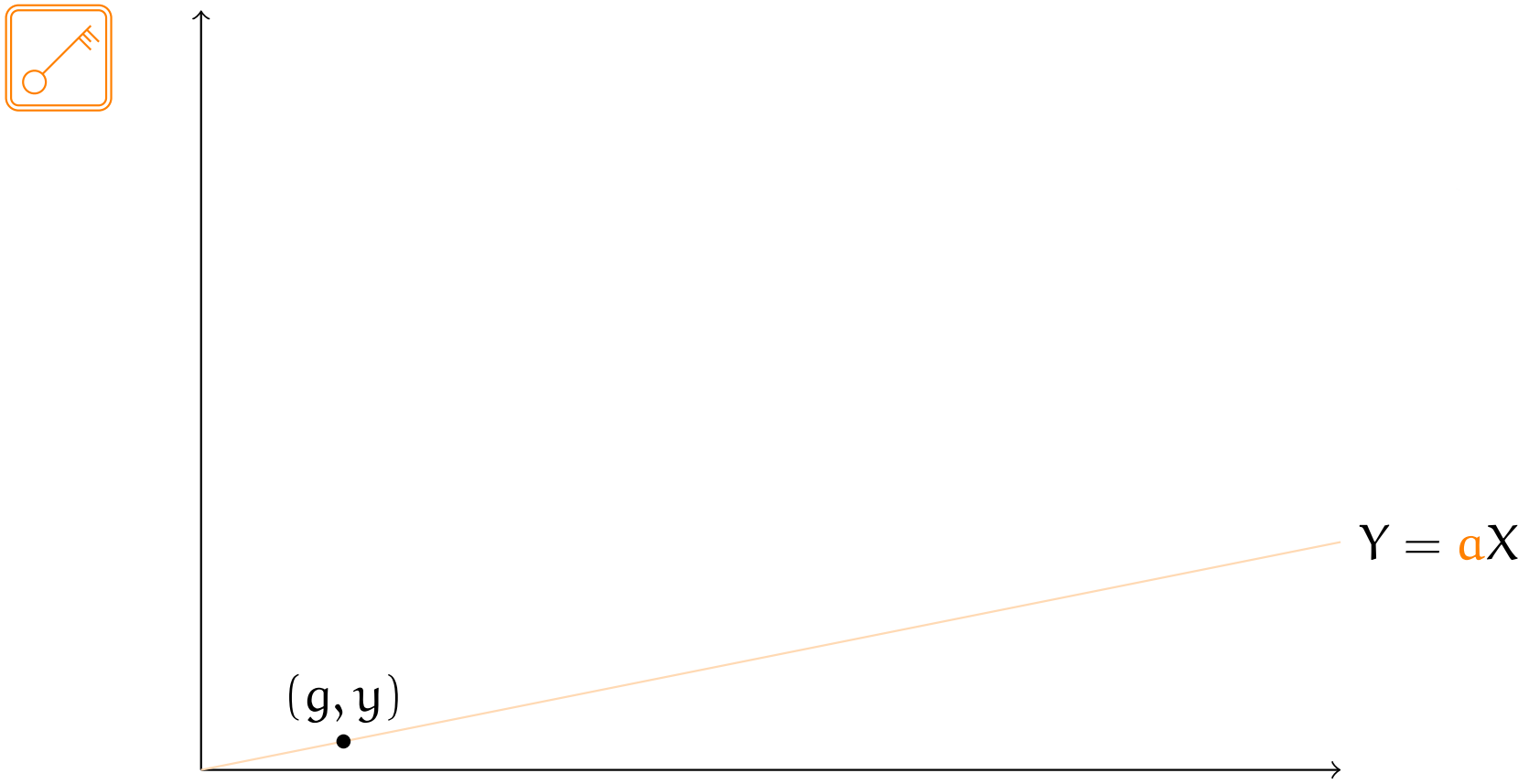
ballot box — receipt generator — decryptor — auditor

ElGamal encryption



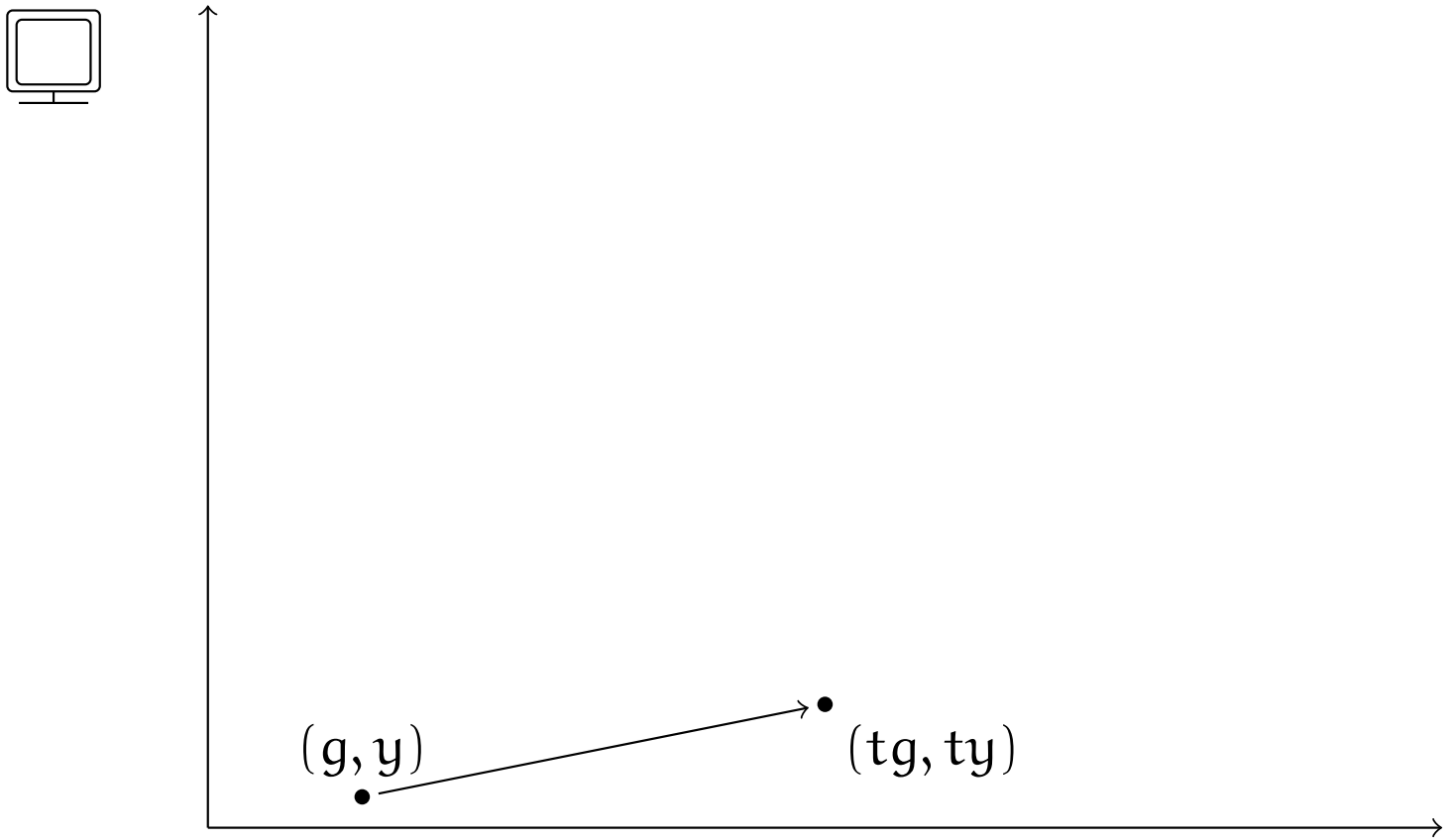
How to encrypt a ballot v?

ElGamal encryption



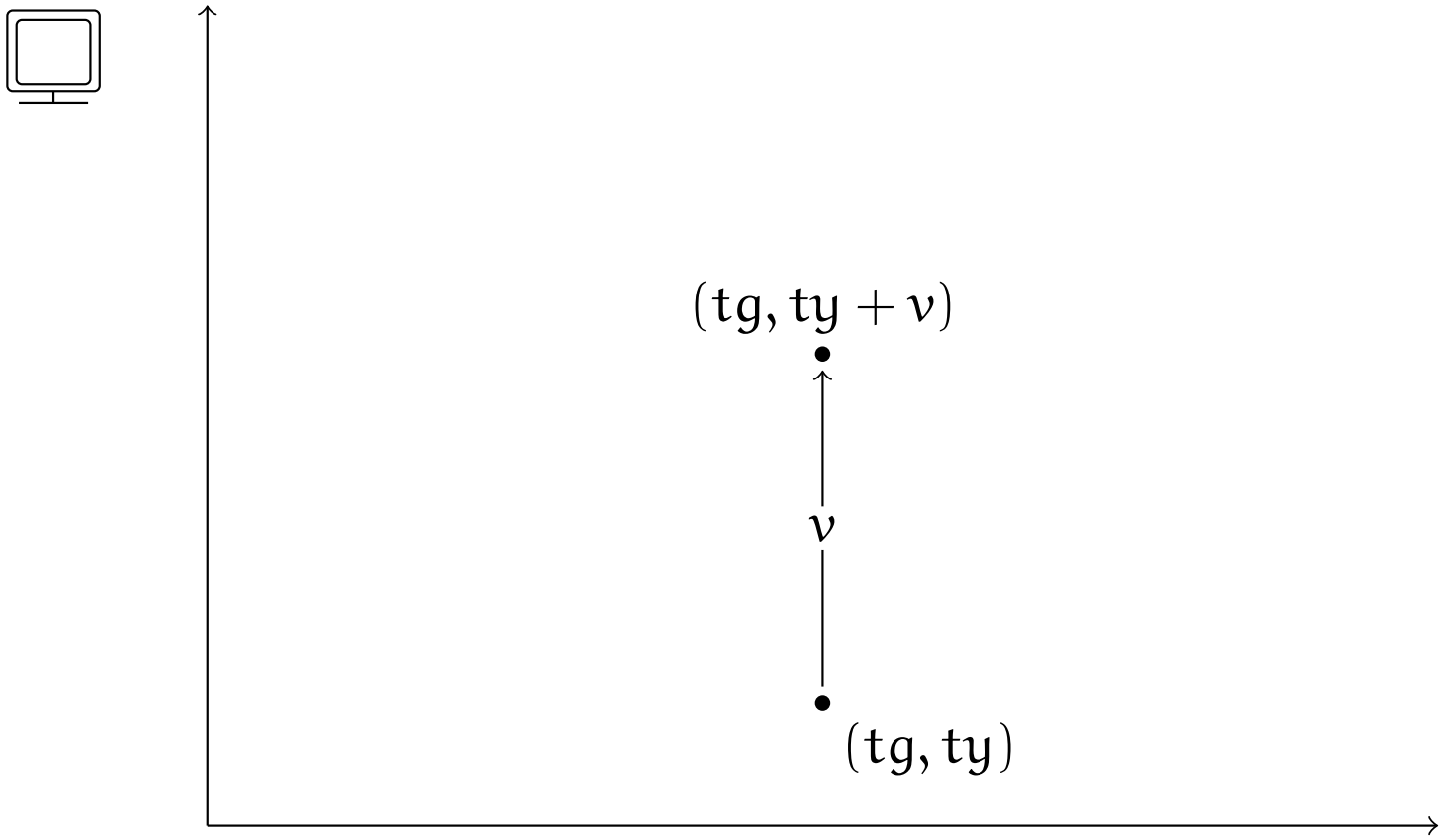
The electoral board selects a slope a and a point (g, y) on the line $Y = aX$.

ElGamal encryption



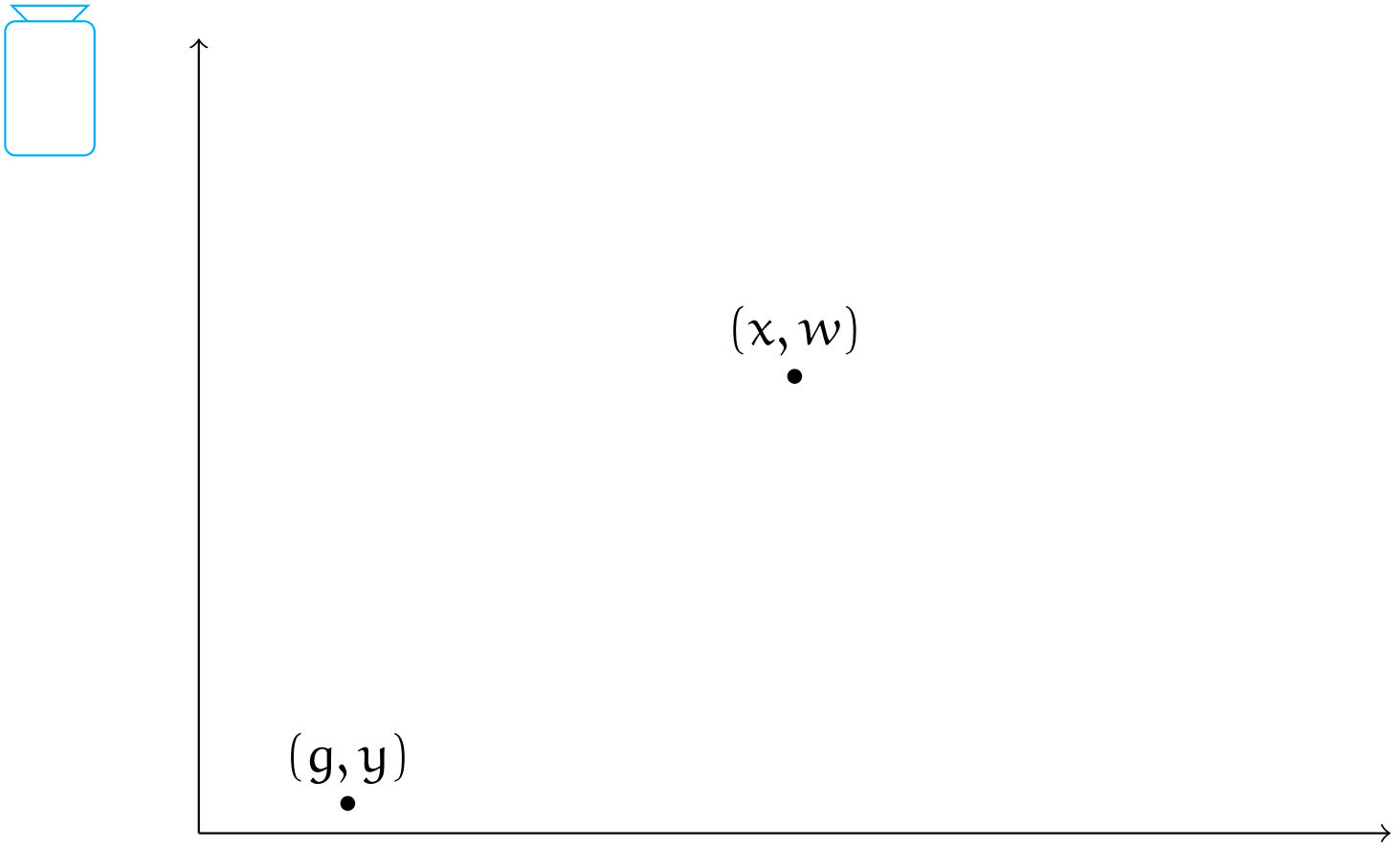
The voter's computer selects a random point on the line through (g, y).

ElGamal encryption



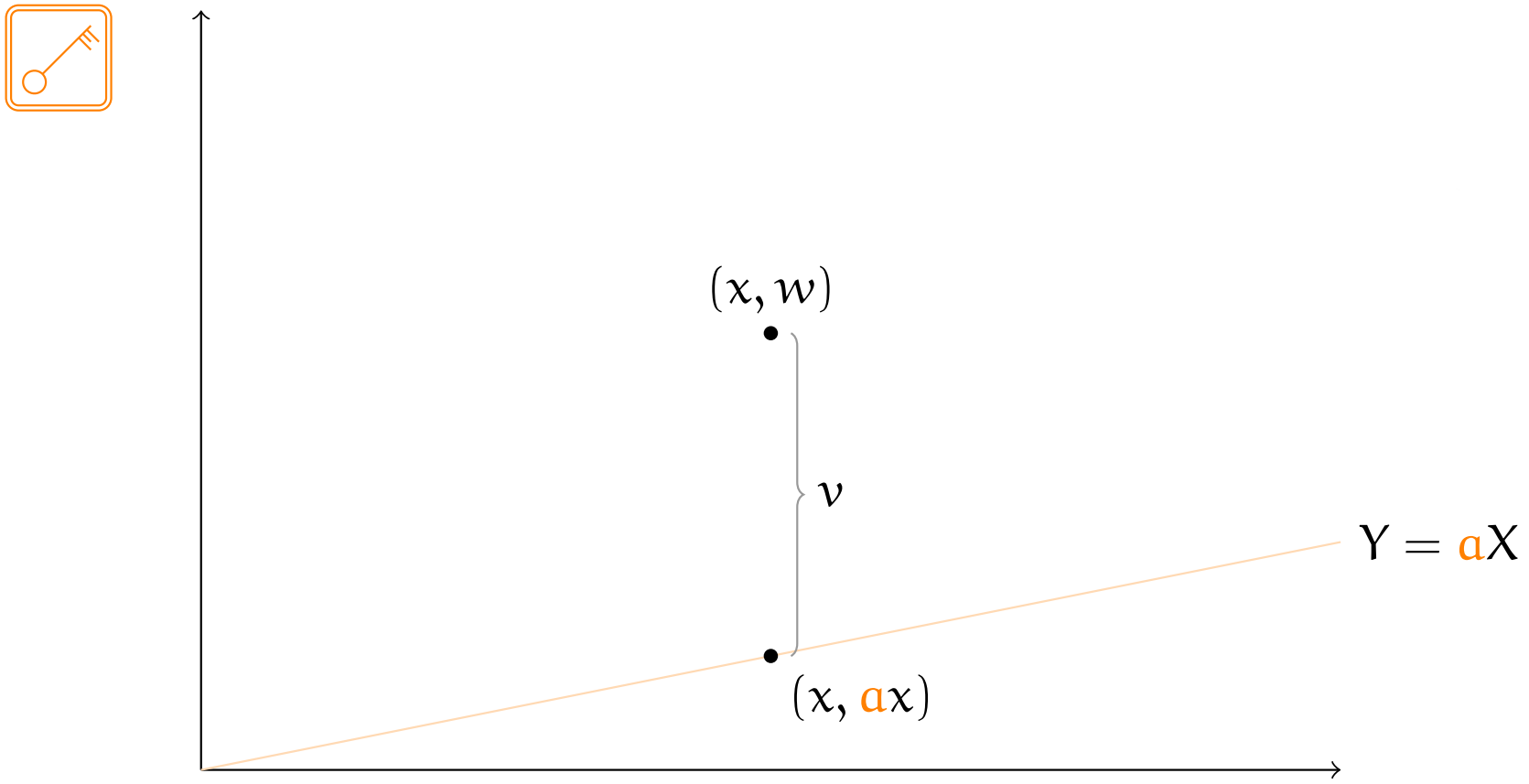
The computer shifts the point upwards by v.

ElGamal encryption



The ballot box gets the ciphertext (x, w).

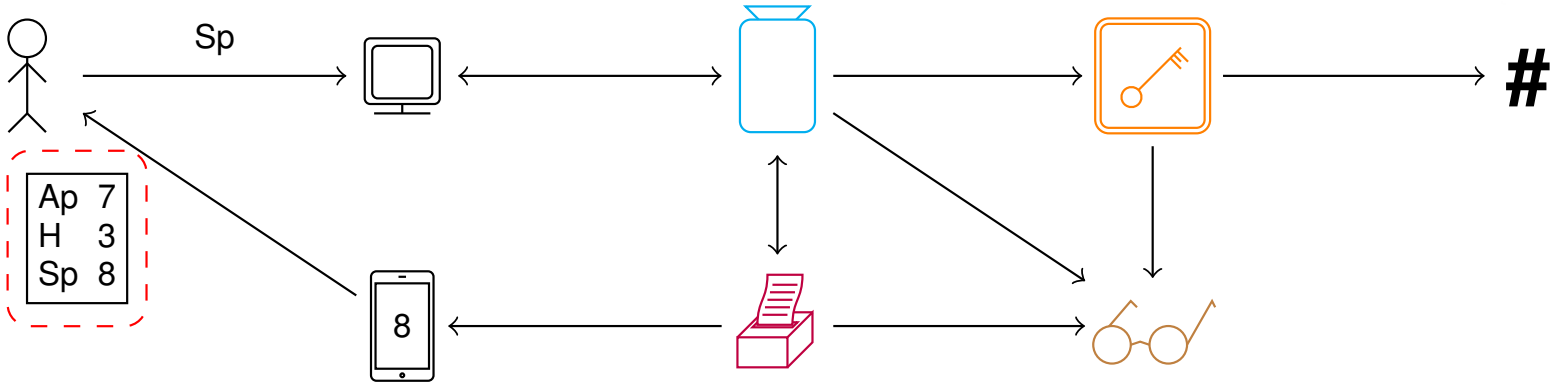
ElGamal encryption



The electoral board gets the ciphertext and recovers v.

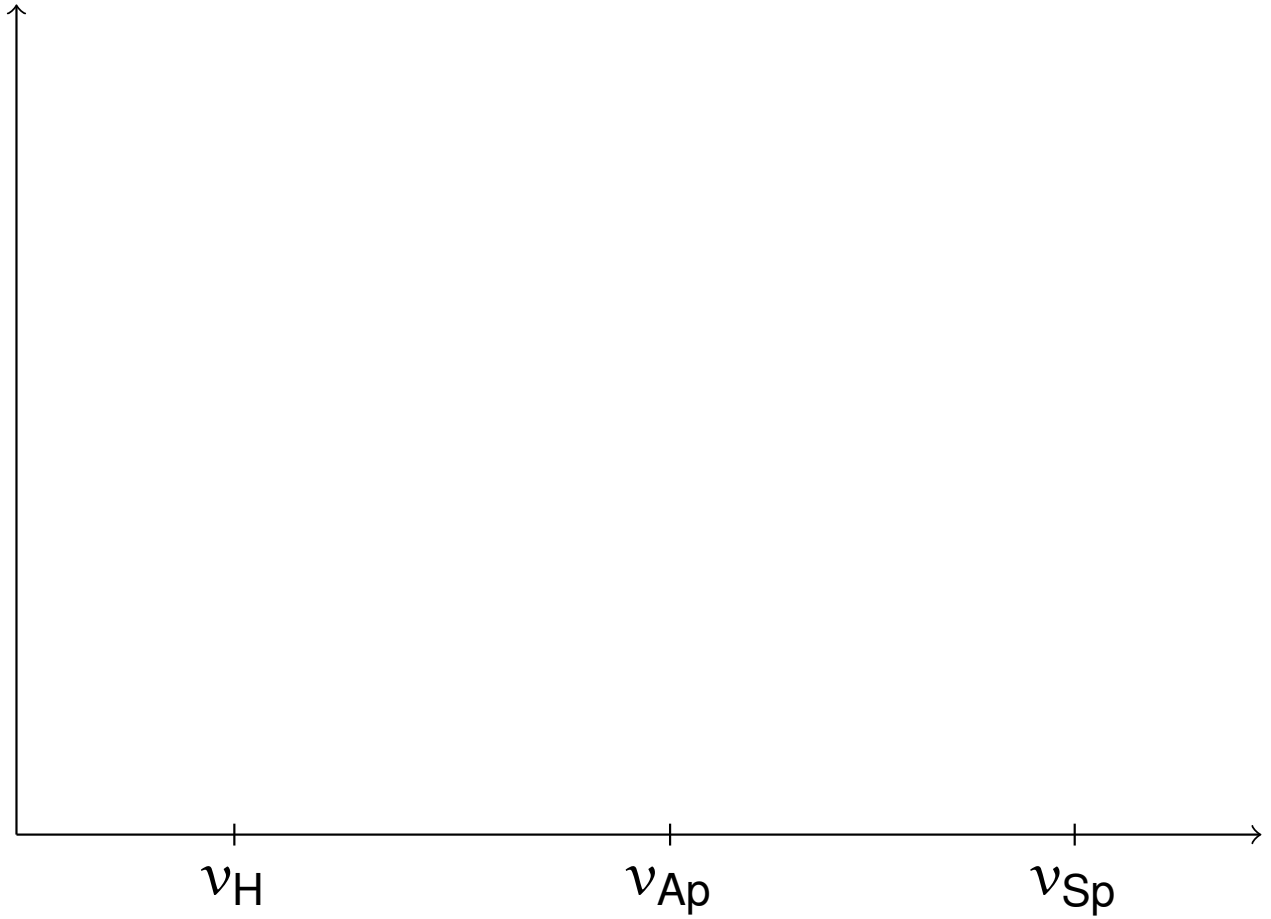
Overview

integrity — secrecy



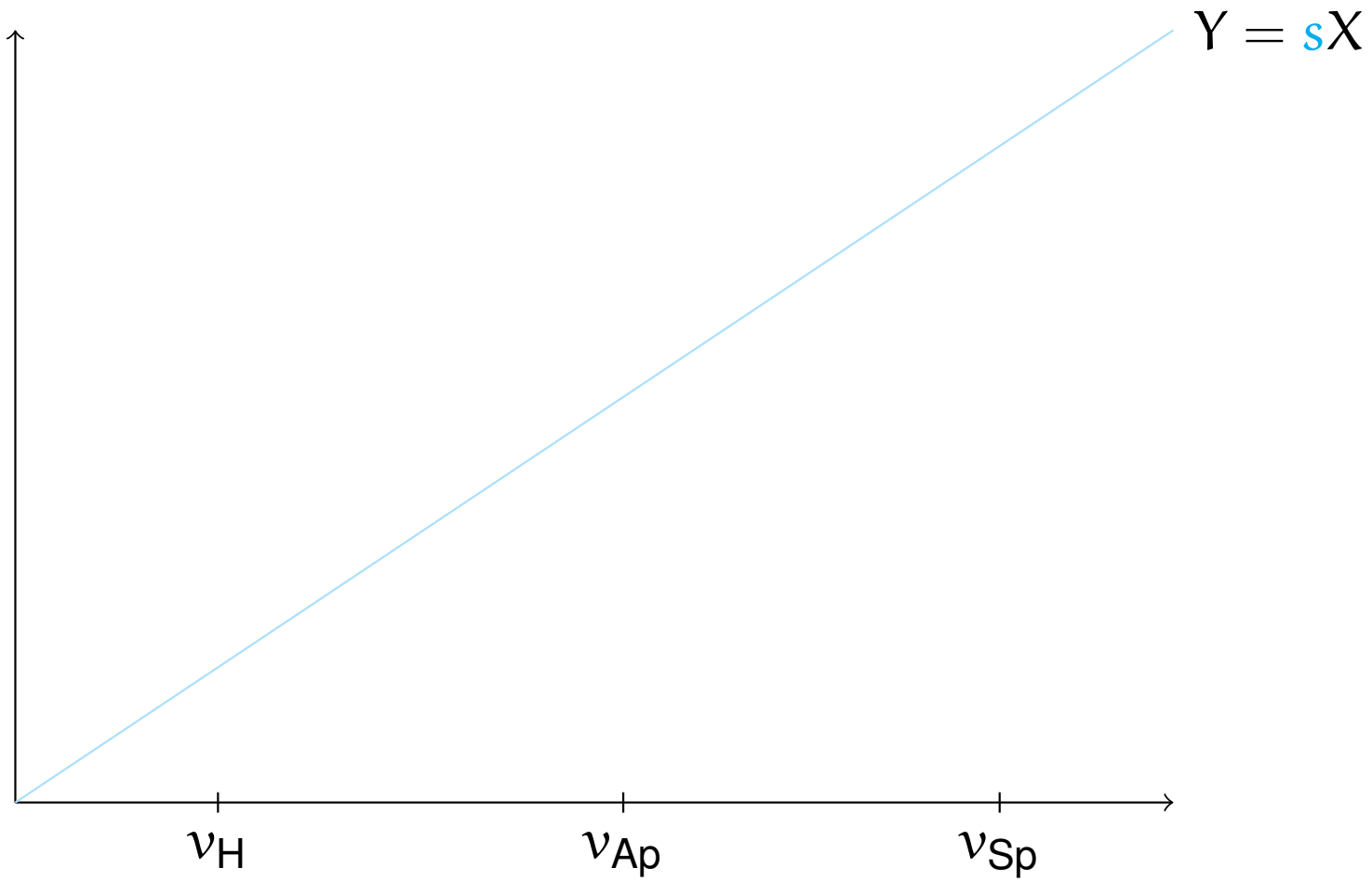
ballot box — receipt generator — decryptor — auditor

Receipt codes



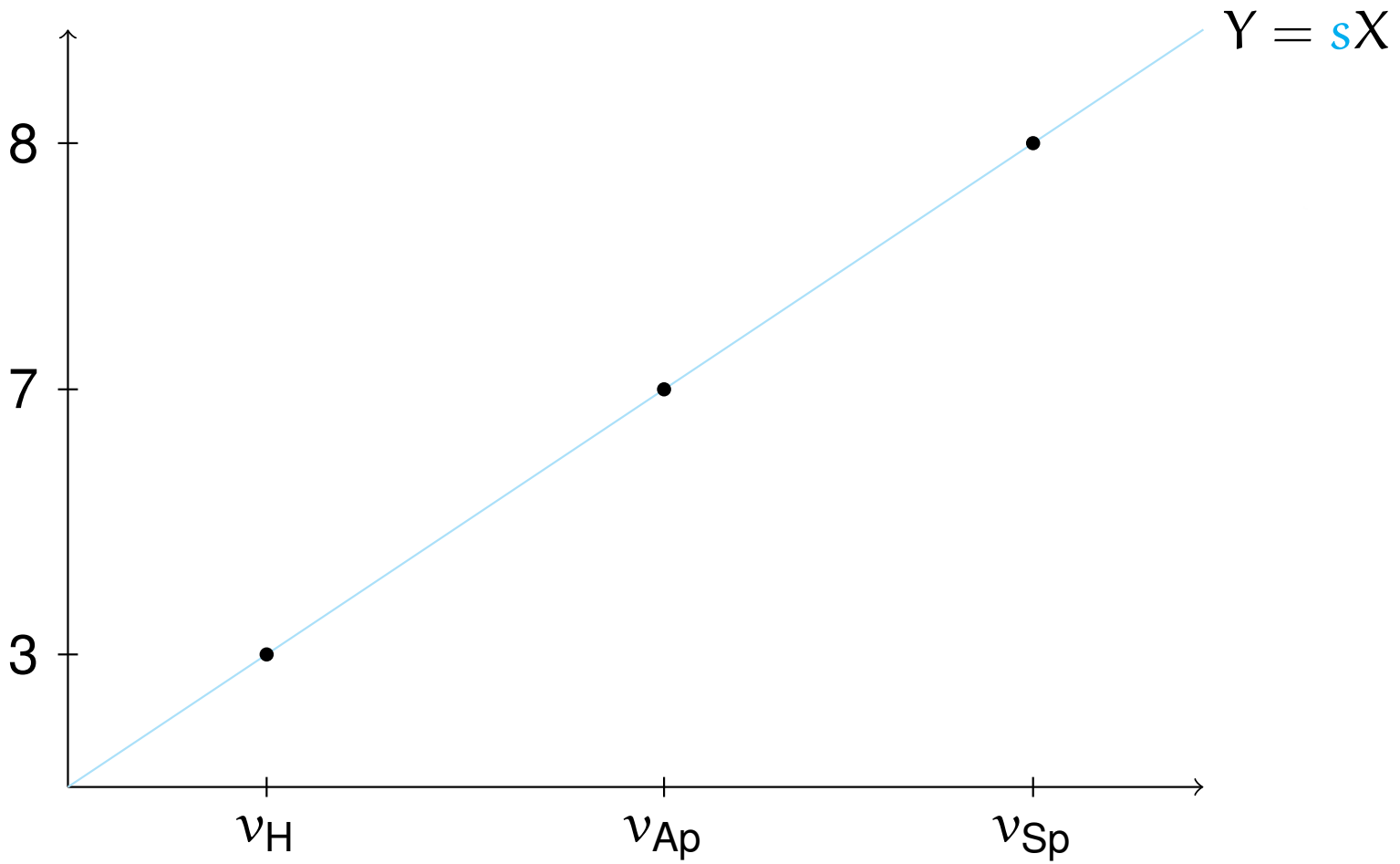
We must code parties as group elements.

Receipt codes



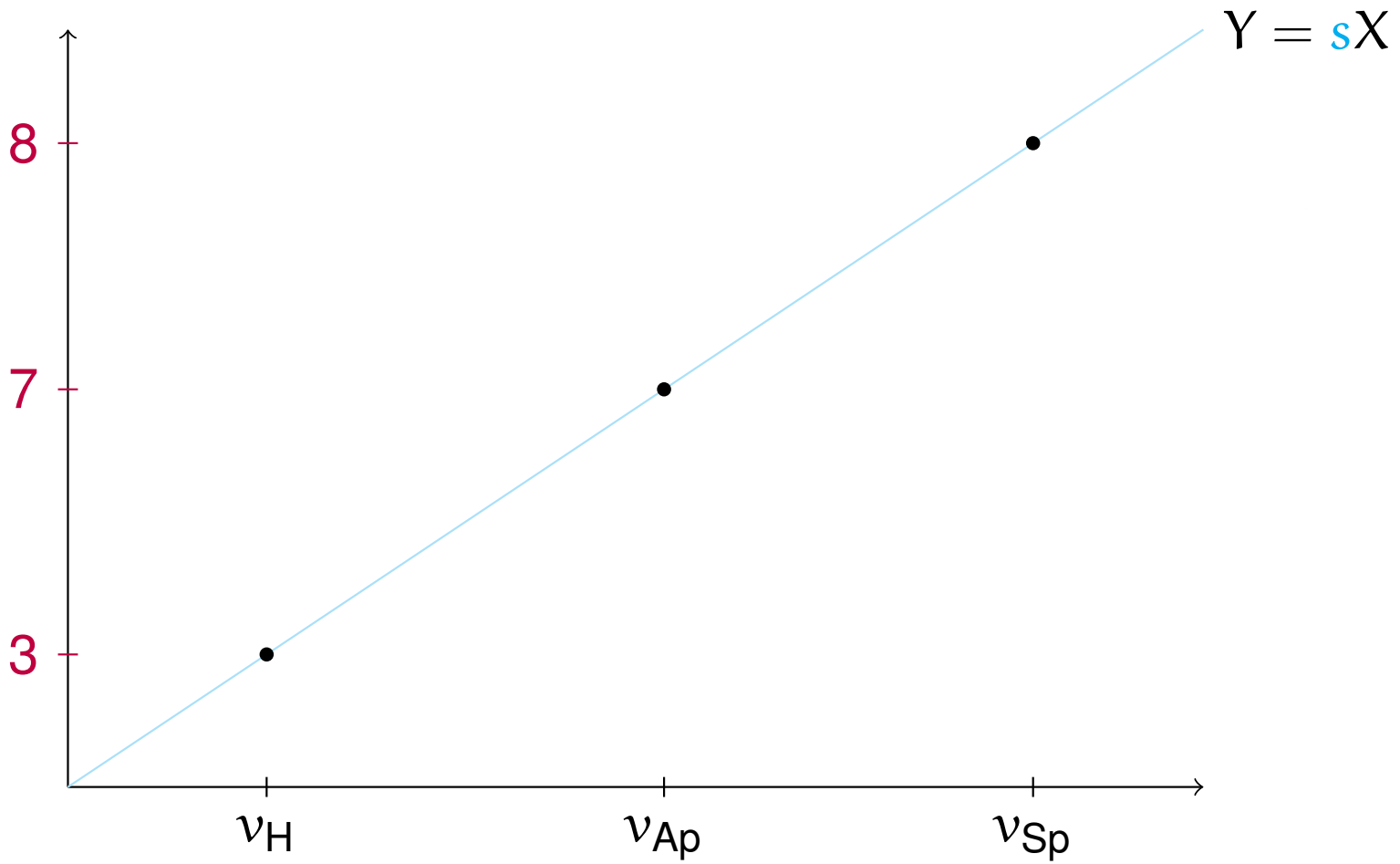
The electoral board assigns a random number s to each voter.

Receipt codes



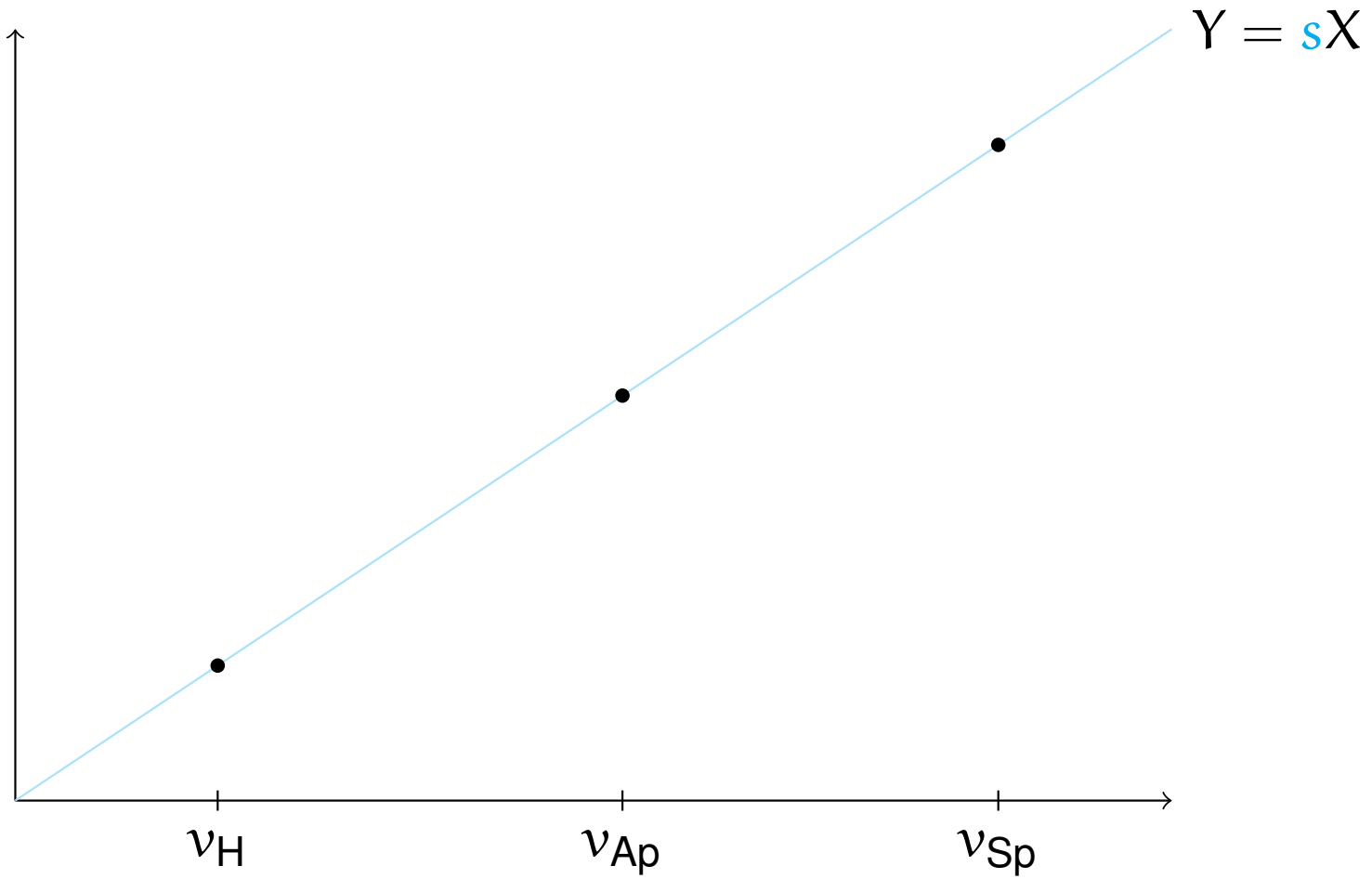
This voter's receipt code for party v will be sv.

Receipt codes



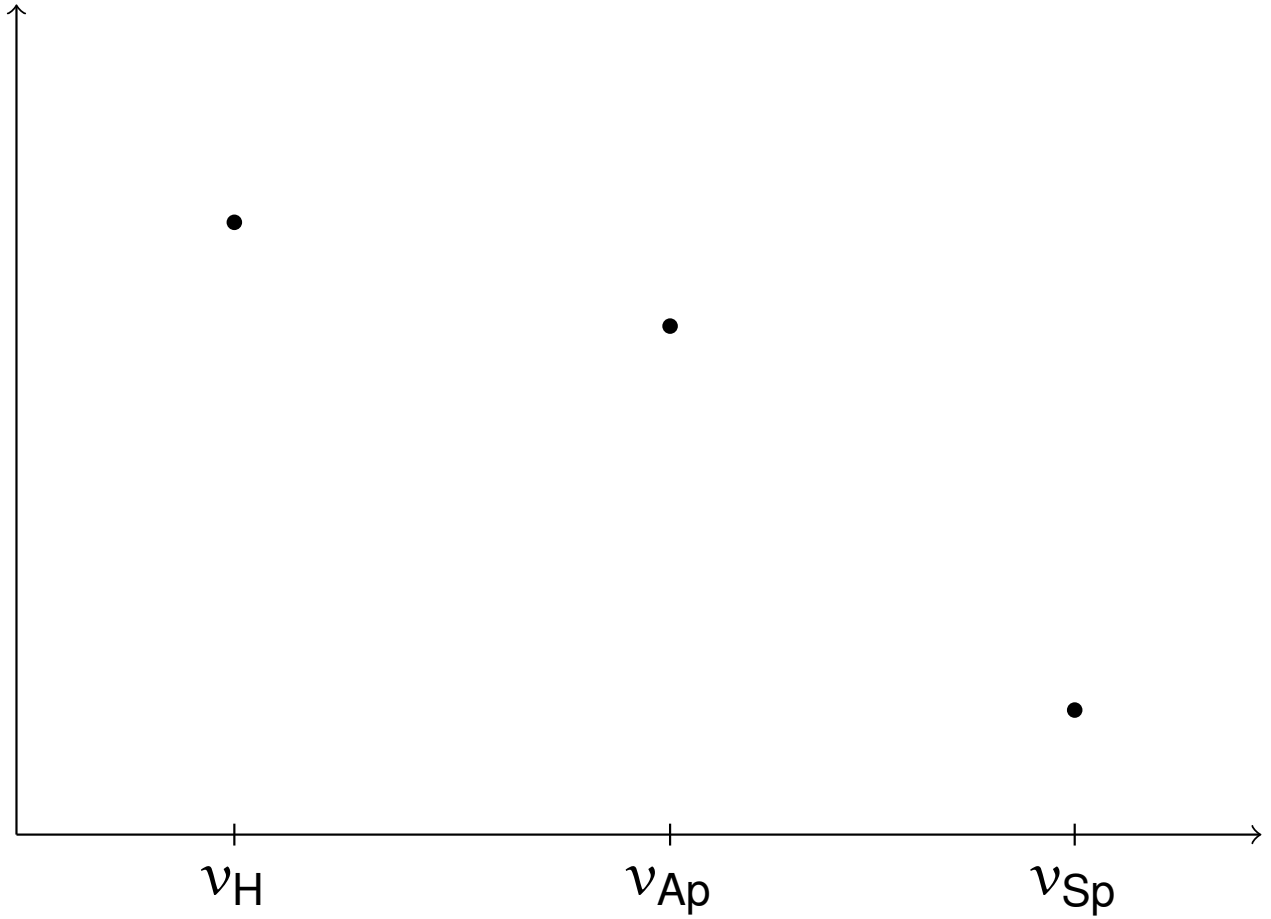
The receipt generator sees the receipt codes.

Receipt codes



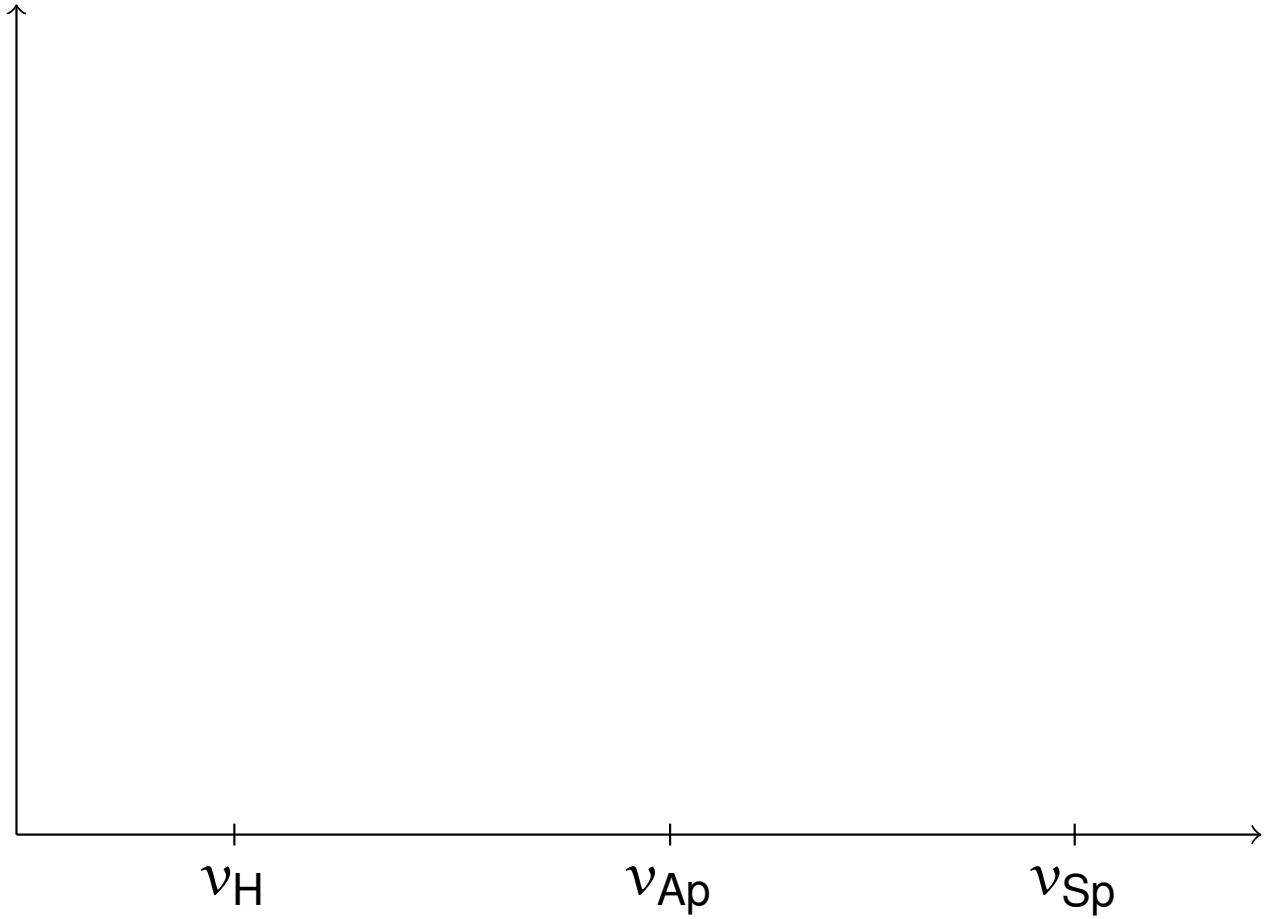
Are the points on a line or are they all over the plane?

Receipt codes



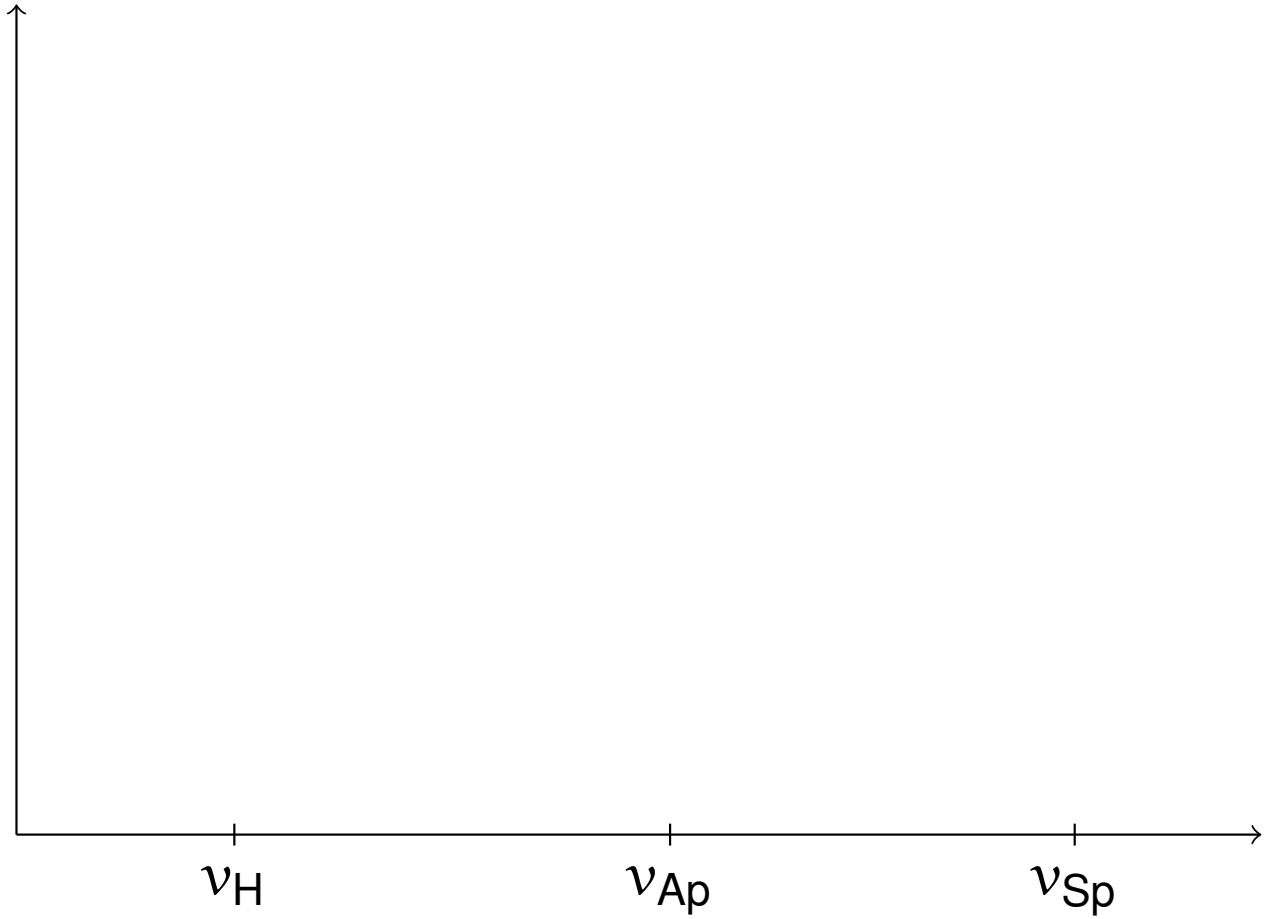
Are the points on a line or are they all over the plane?

Receipt codes



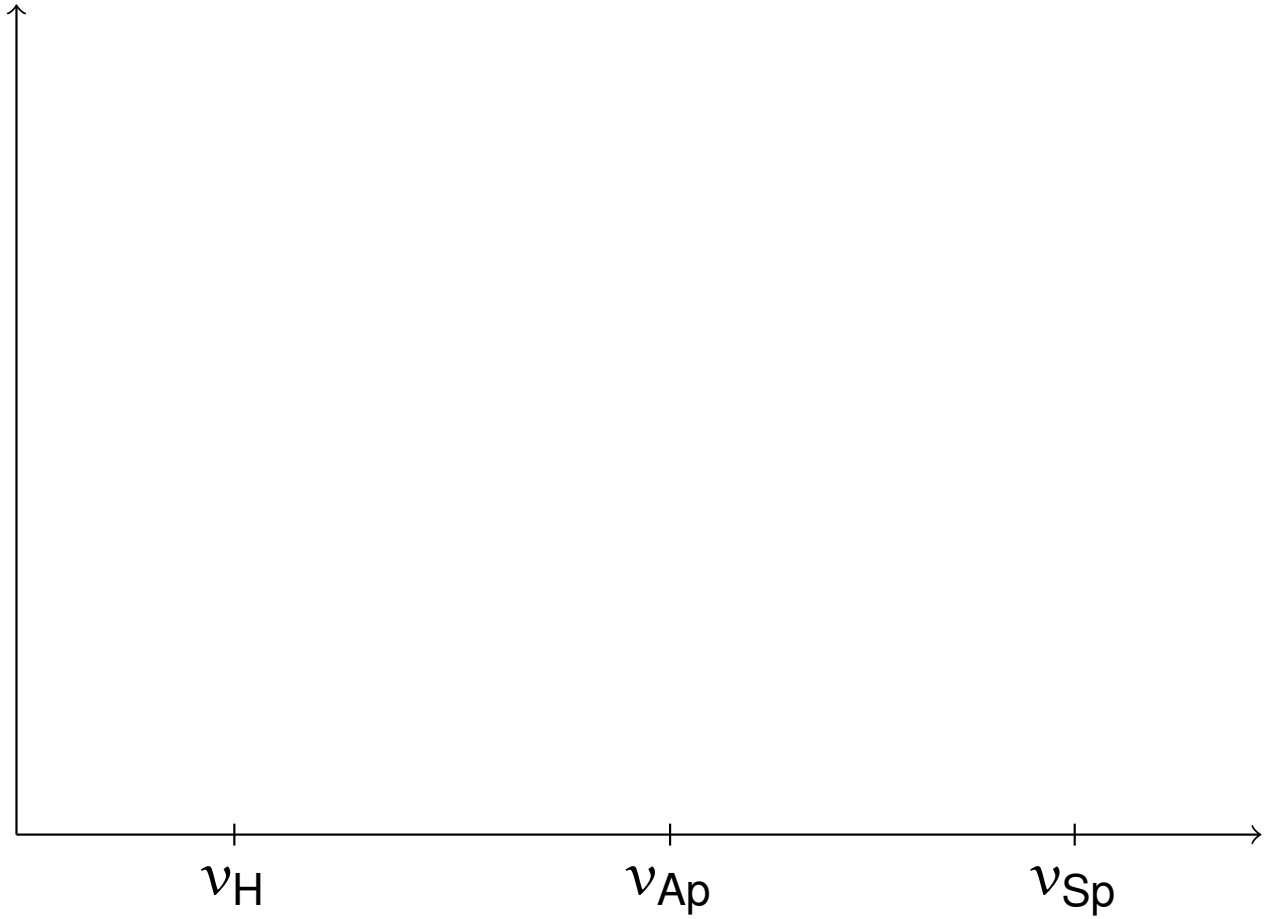
How we code parties as group elements is important!

Receipt codes



Random coding works well (DDH).

Receipt codes



Efficiency dictates non-random coding.

Points on a line?

$G \subset \mathbb{F}_p^*$, parties are coded as small primes $\ell_1, \ldots, \ell_n$.

Are the points $(\ell_1, r_1), \ldots, (\ell_n, r_n)$ on a line?

Points on a line?

$G \subset \mathbb{F}_p^*$, parties are coded as small primes $\ell_1, \ldots, \ell_n$.

Are the points $(\ell_1, r_1), \ldots, (\ell_n, r_n)$ on a line?

Idea 1: Find a relation $\prod \ell_i^{t_i} = 1$, then $\prod r_i^{t_i} = 1$ holds if the points are on a line.

Points on a line?

$G \subset \mathbb{F}_p^*$, parties are coded as small primes $\ell_1, \ldots, \ell_n$.

Are the points $(\ell_1, r_1), \ldots, (\ell_n, r_n)$ on a line?

Idea 1: Find a relation $\prod \ell_i^{t_i} = 1$, then $\prod r_i^{t_i} = 1$ holds if the points are on a line.

Too few primes!

Points on a line?

$G \subset \mathbb{F}_p^*$, parties are coded as small primes $\ell_1, \ldots, \ell_n$.

Are the points $(\ell_1, r_1), \ldots, (\ell_n, r_n)$ on a line?

Idea 1: Find a relation $\prod \ell_i^{t_i} = 1$, then $\prod r_i^{t_i} = 1$ holds if the points are on a line.

Idé 2: Choose an extra prime ℓ_{n+1} and find two relations:

$$\ell_{n+1} \prod \ell_i^{t_i} = 1, \qquad \ell_{n+1} \prod \ell_i^{t_i'} = 1.$$

Points on a line?

$G \subset \mathbb{F}_p^*$, parties are coded as small primes $\ell_1, \ldots, \ell_n$.

Are the points $(\ell_1, r_1), \ldots, (\ell_n, r_n)$ on a line?

Idea 1: Find a relation $\prod \ell_i^{t_i} = 1$, then $\prod r_i^{t_i} = 1$ holds if the points are on a line.

Natural extension:

1. Choose many extra primes $\ell_{n+1}, \ldots, \ell_N$.
2. Find many relations of the form $\prod \ell_i^{t_{ij}} = 1$.
3. Use linear algebra to eliminate $\ell_{n+1}, \ldots, \ell_N$ to get a single relation.

Points on a line?

$G \subset \mathbb{F}_p^*$, parties are coded as small primes $\ell_1, \ldots, \ell_n$.

Are the points $(\ell_1, r_1), \ldots, (\ell_n, r_n)$ on a line?

Idea 1: Find a relation $\prod \ell_i^{t_i} = 1$, then $\prod r_i^{t_i} = 1$ holds if the points are on a line.

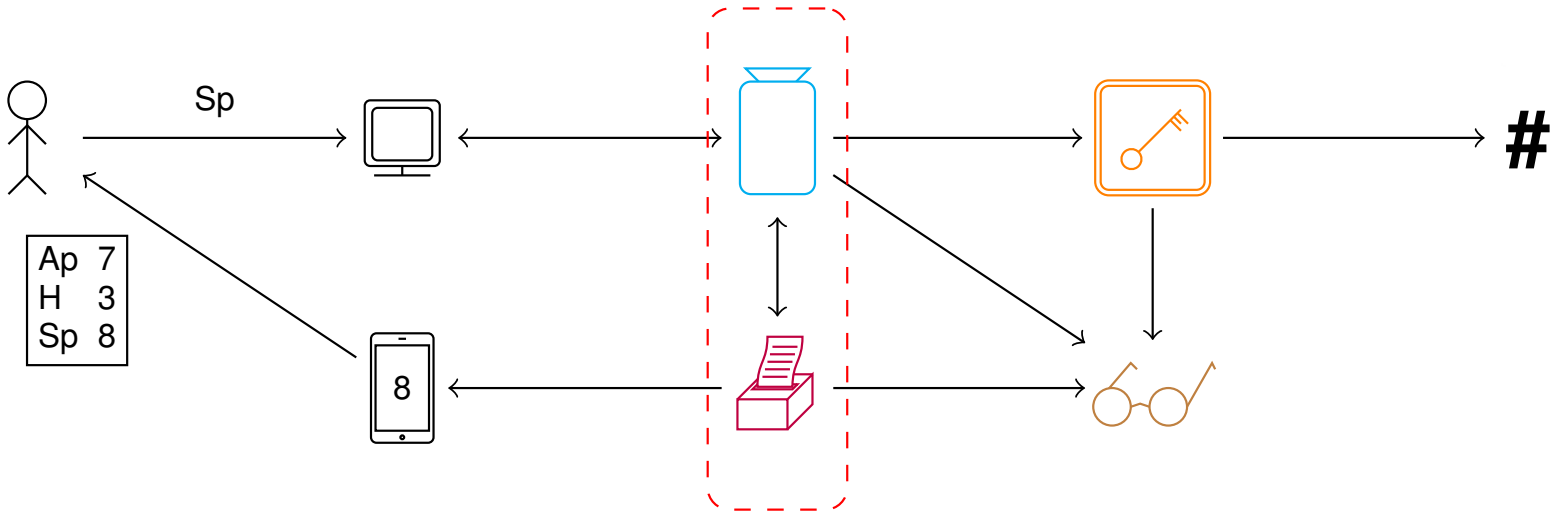
Natural extension:

1. Choose many extra primes $\ell_{n+1}, \ldots, \ell_N$.
2. Find many relations of the form $\prod \ell_i^{t_{ij}} = 1$.
3. Use linear algebra to eliminate $\ell_{n+1}, \ldots, \ell_N$ to get a single relation.

If p is large, this approach does not work.

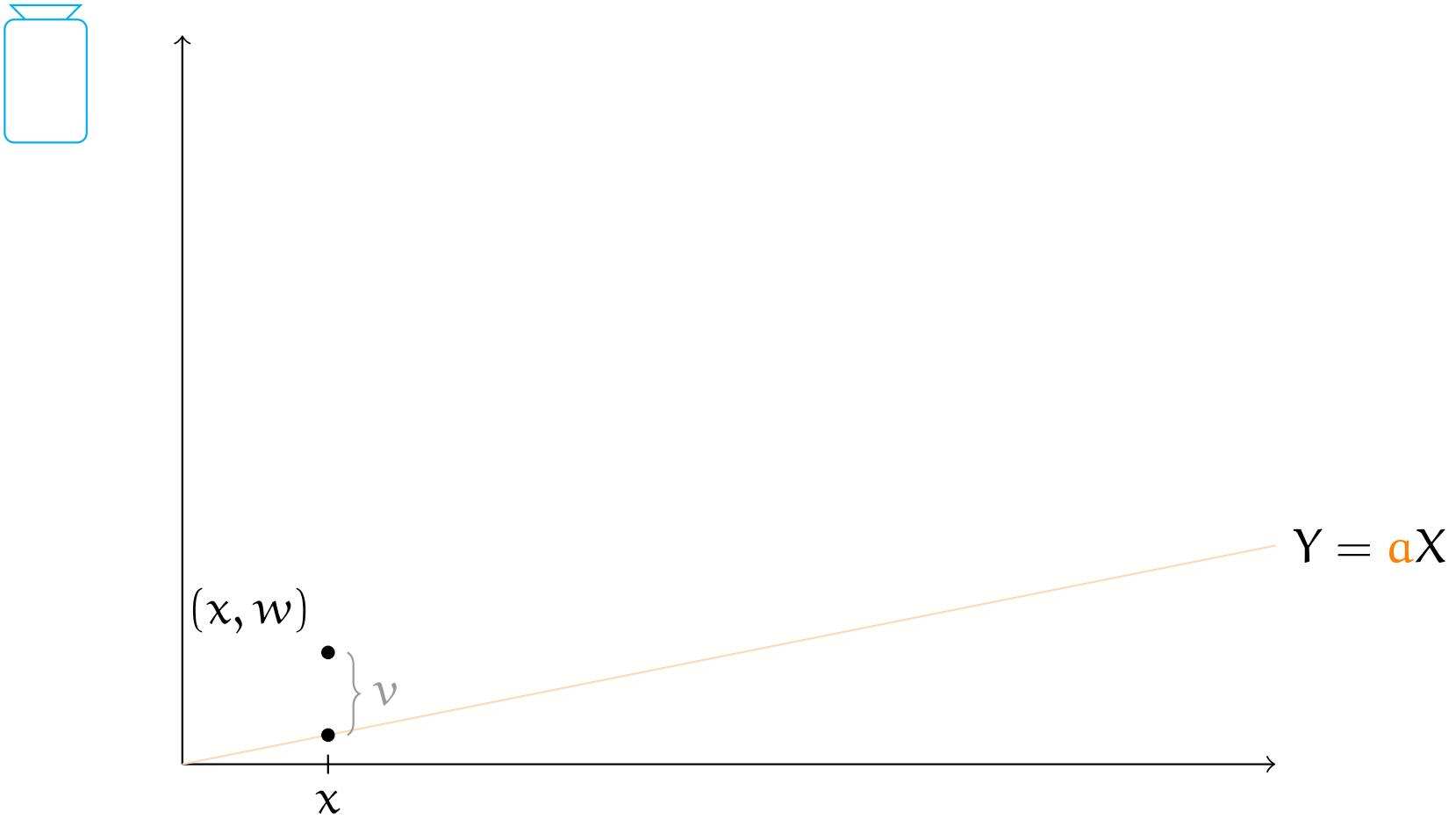
Overview

integrity — secrecy



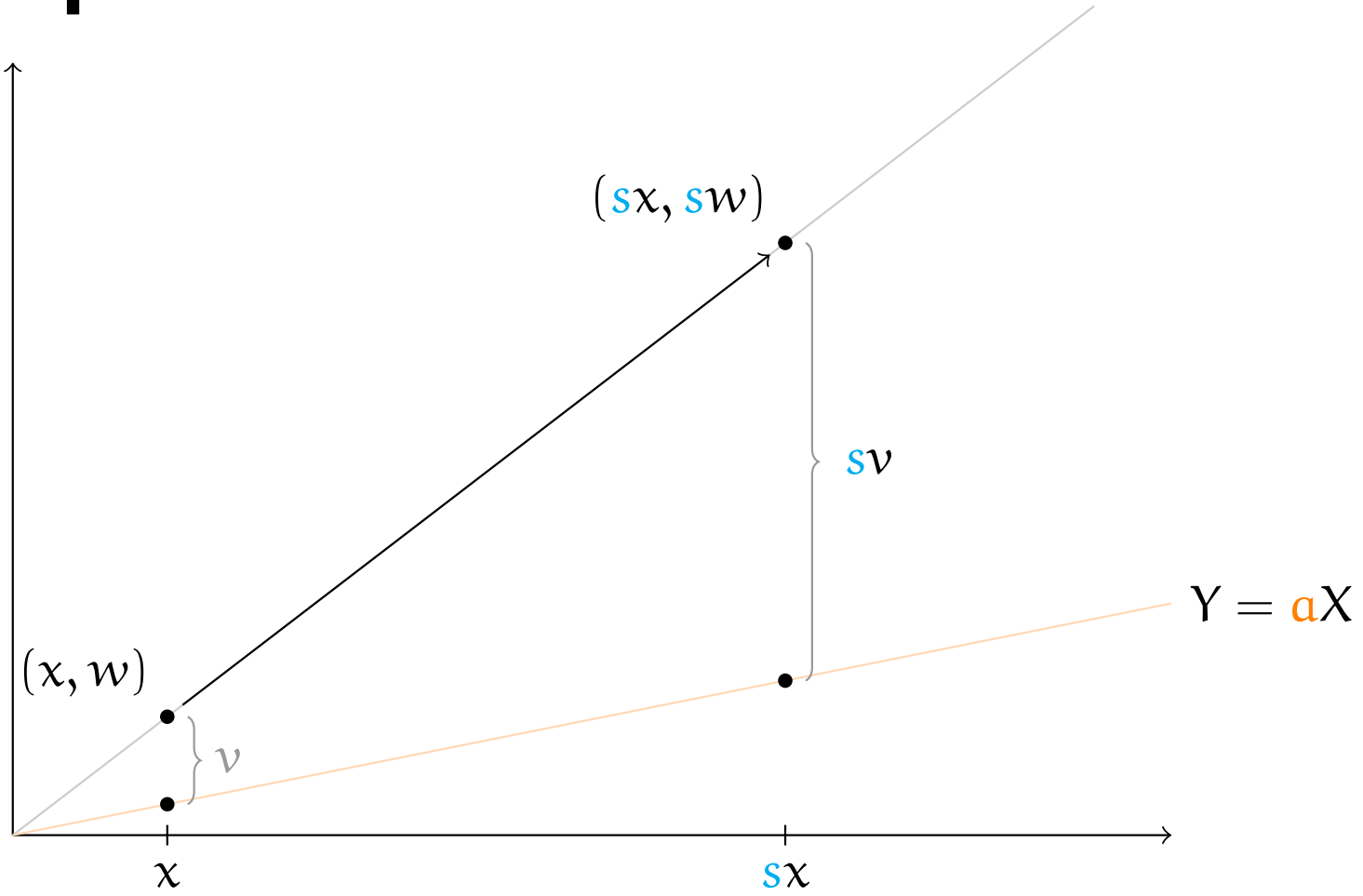
ballot box — receipt generator — decryptor — auditor

Receipt codes II

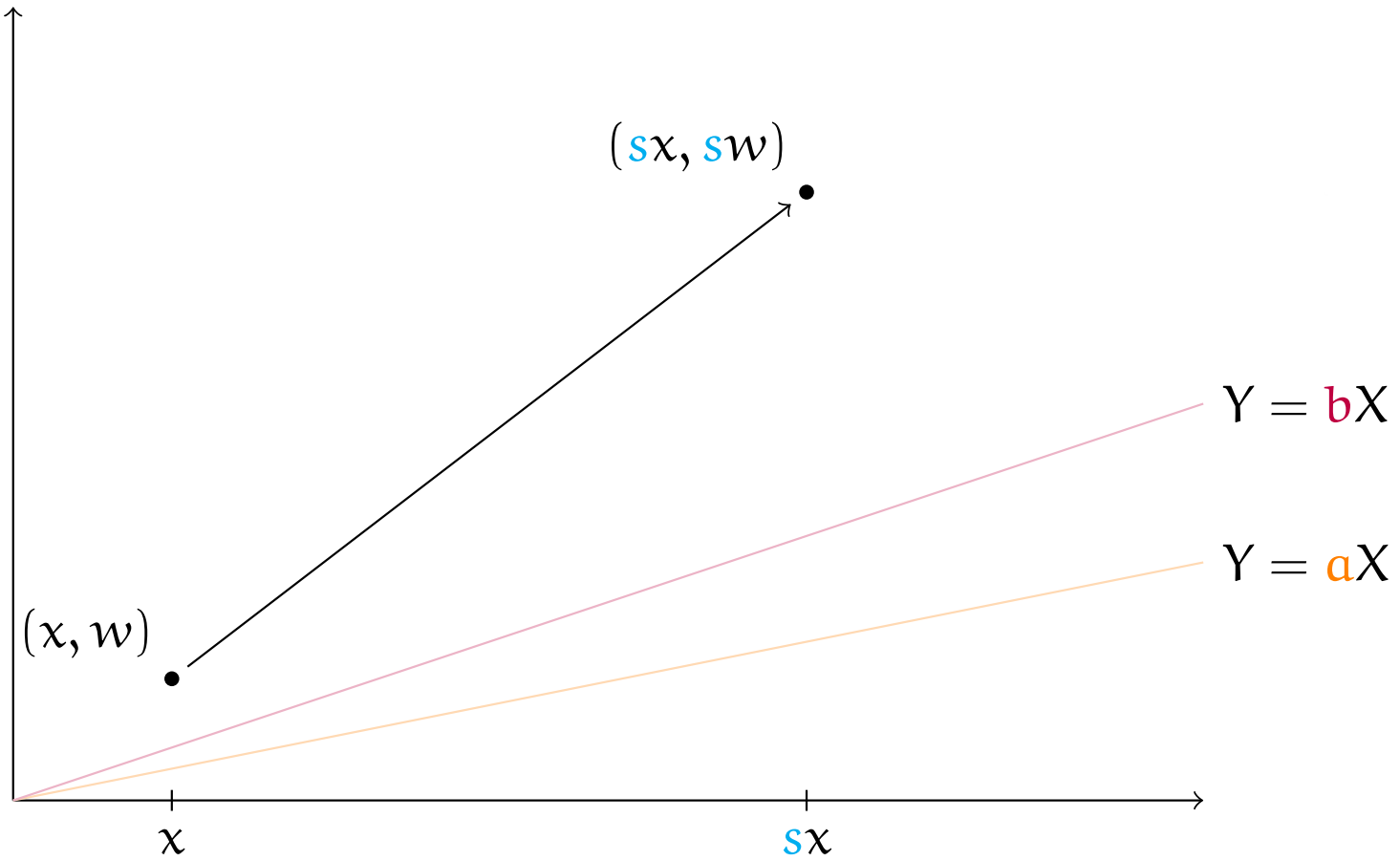


The ballot box has the ciphertext.

Receipt codes II

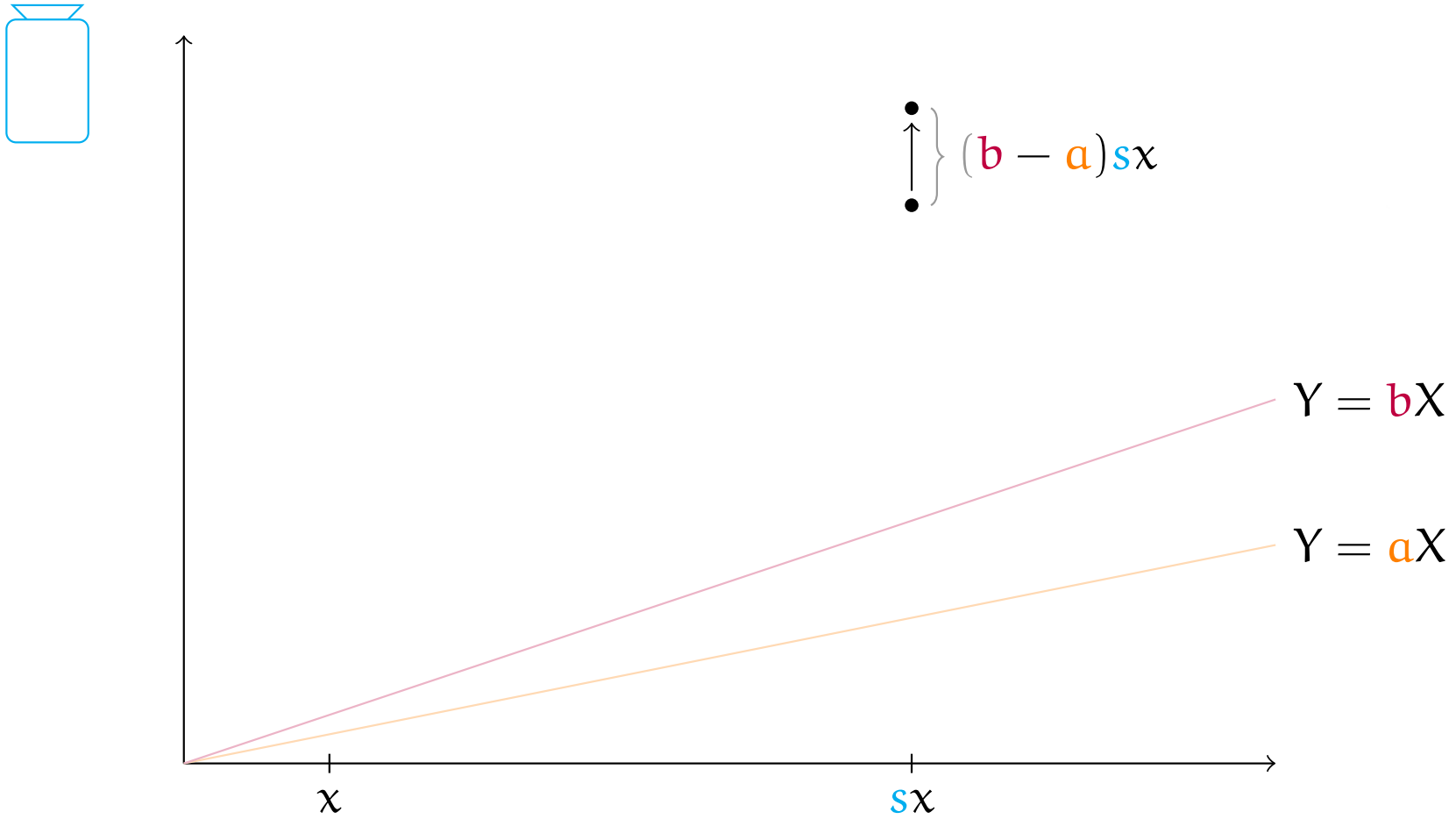


Receipt codes II



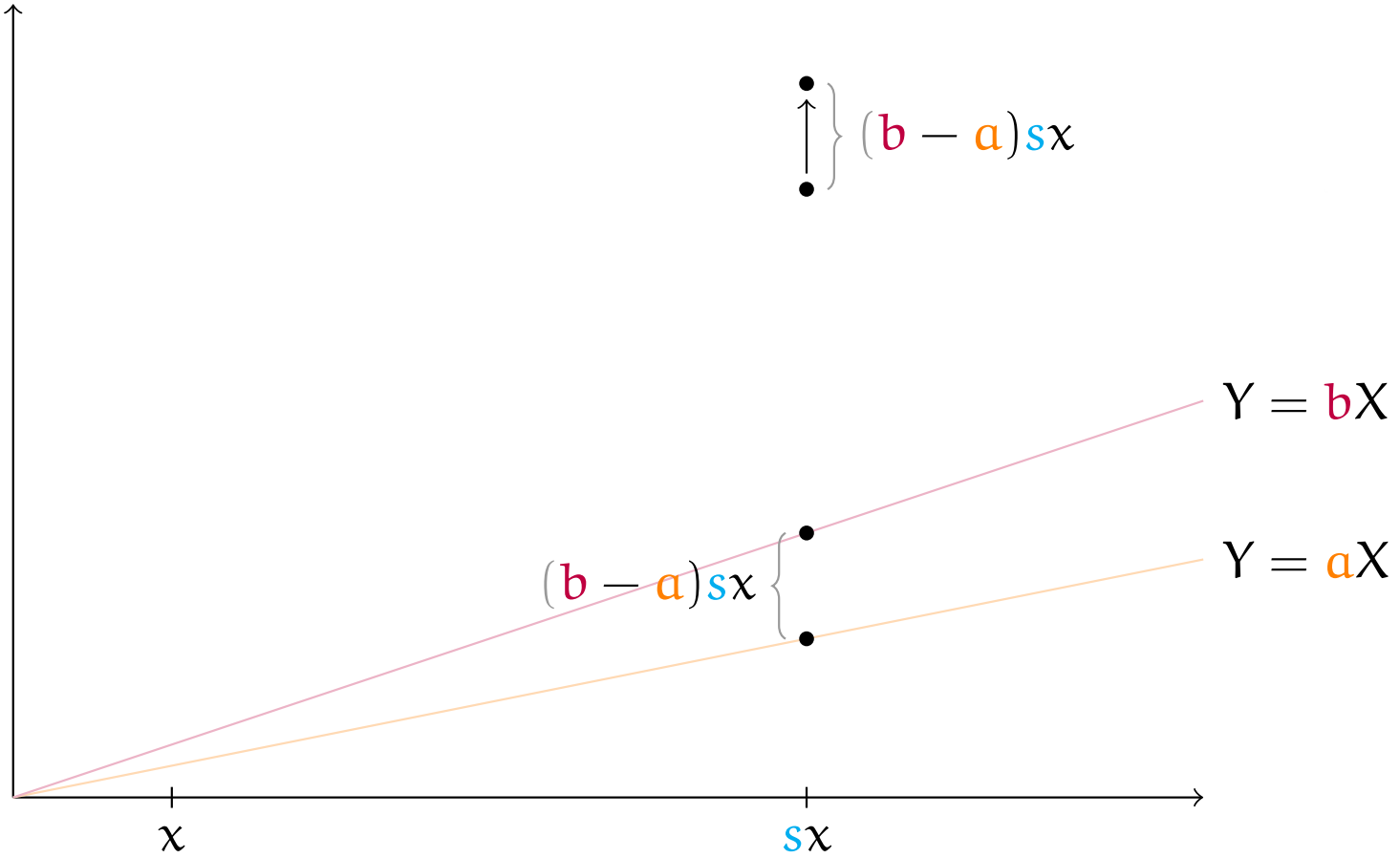
The receipt generator has a line of its own.

Receipt codes II

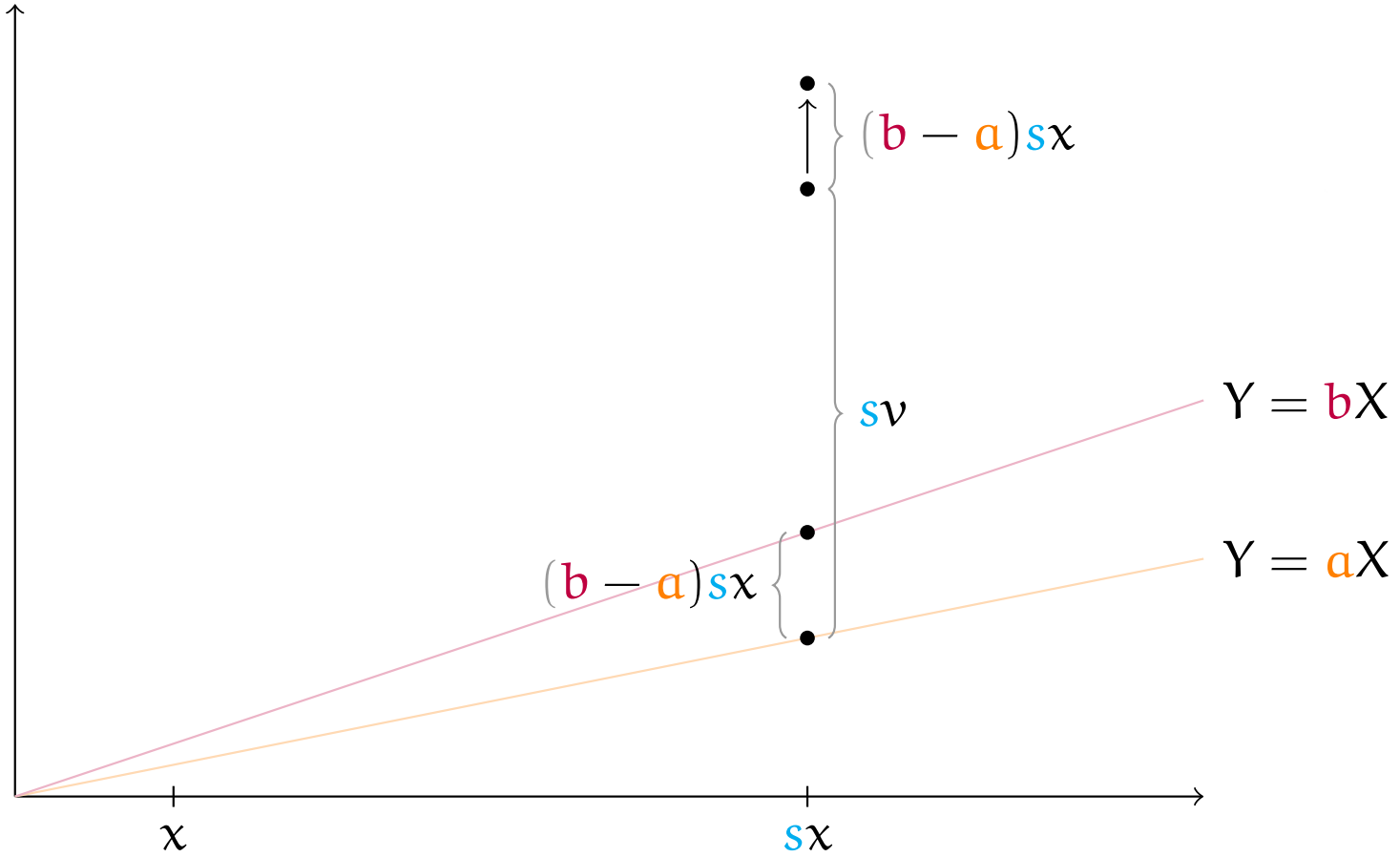


The ballot box has the difference between the two slopes.

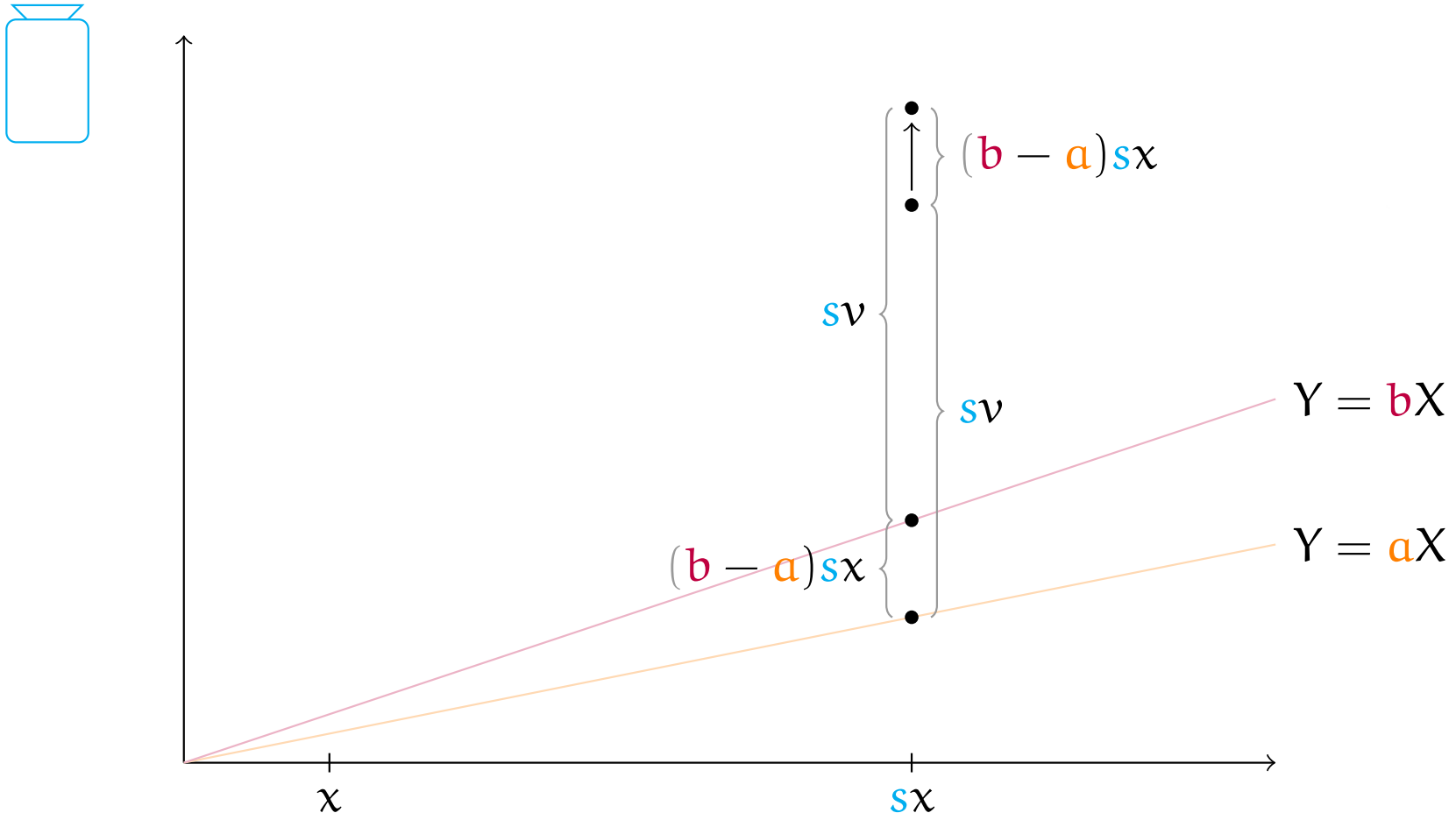
Receipt codes II



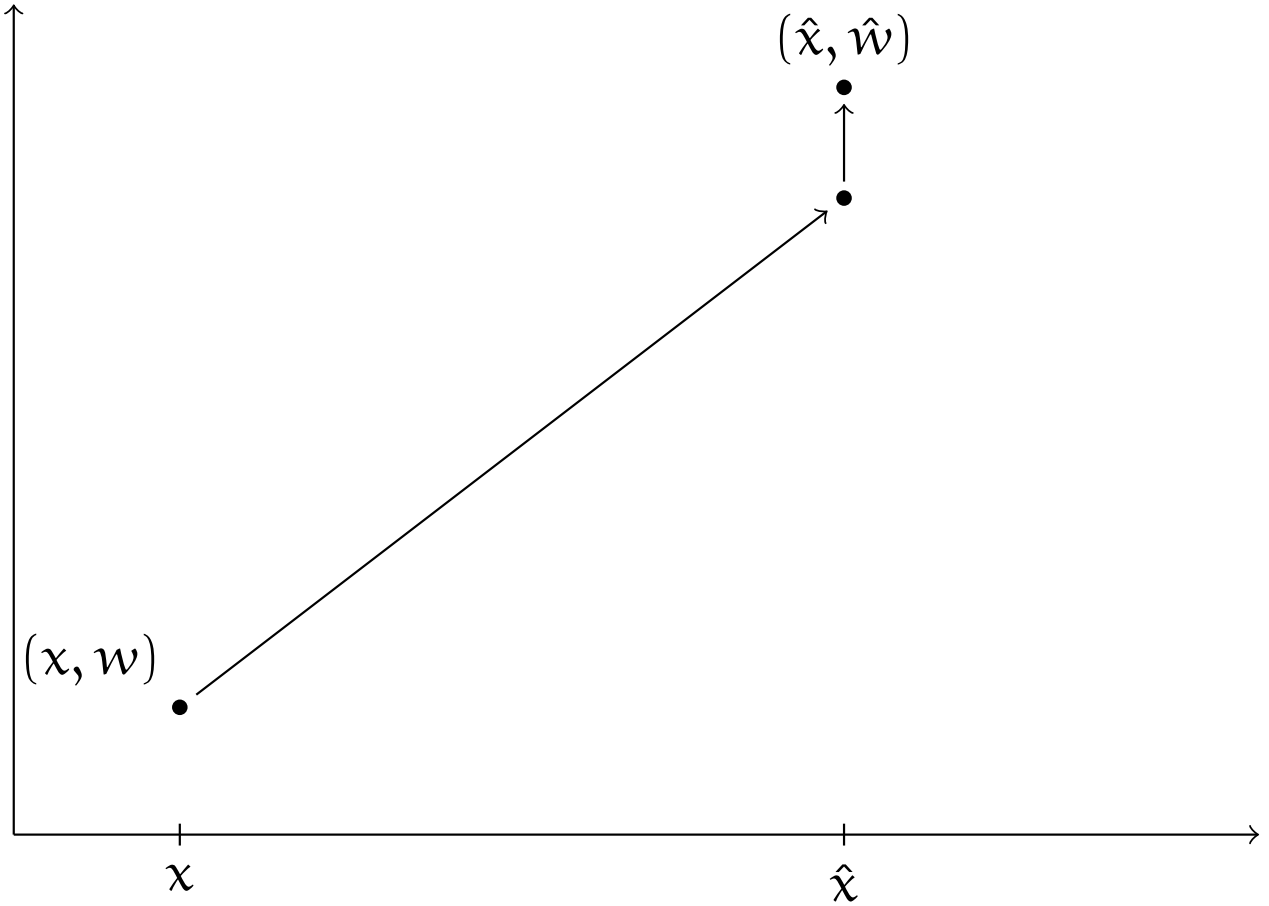
Receipt codes II



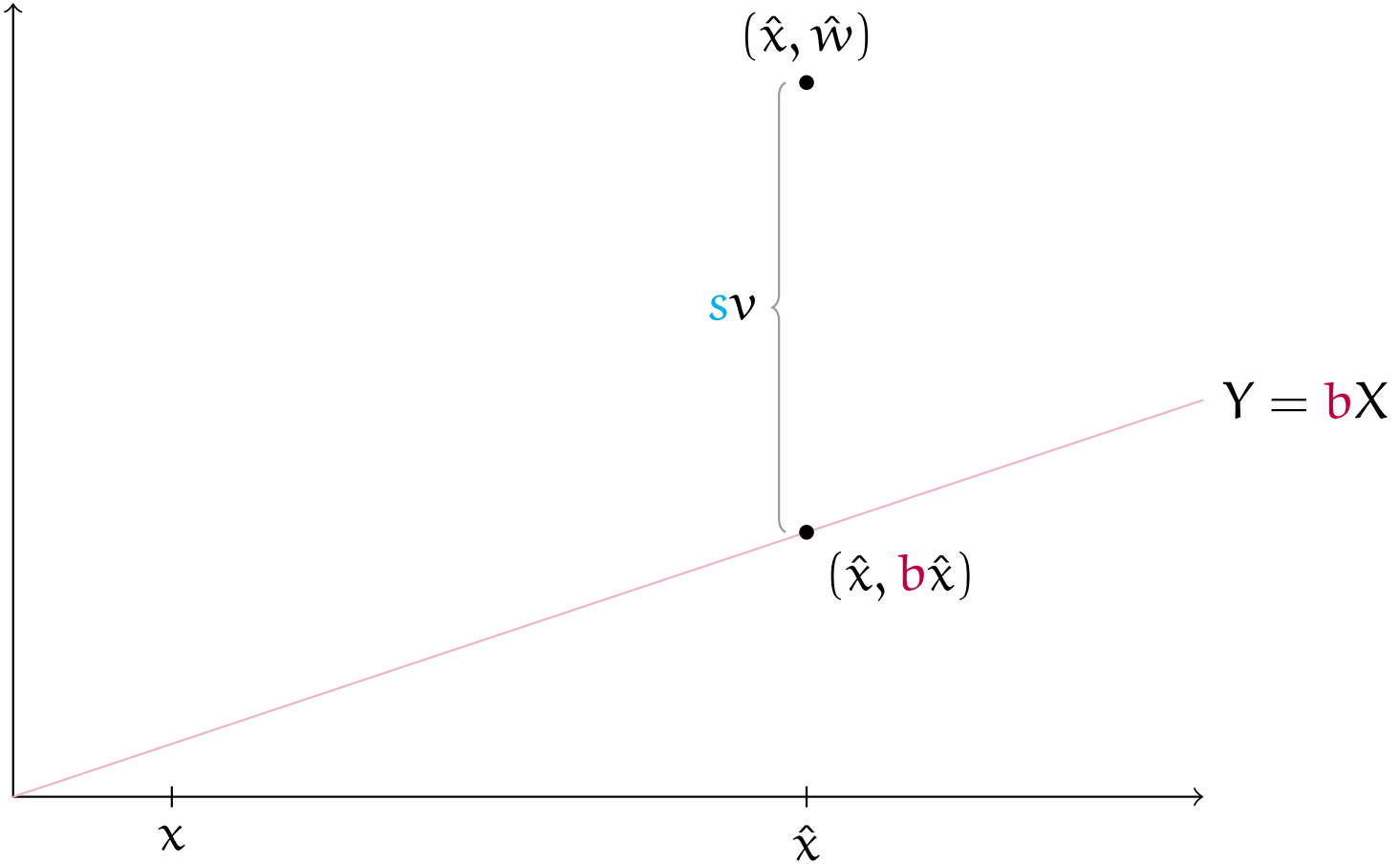
Receipt codes II



Receipt codes II



Receipt codes II



Full system

Add digital signatures and NIZK proofs all over the place to get something that is «secure» even if

- the ballot box and any number of computers; *or*
- the receipt generator; *or*
- the decryptor; *or*
- the auditor

are corrupt.

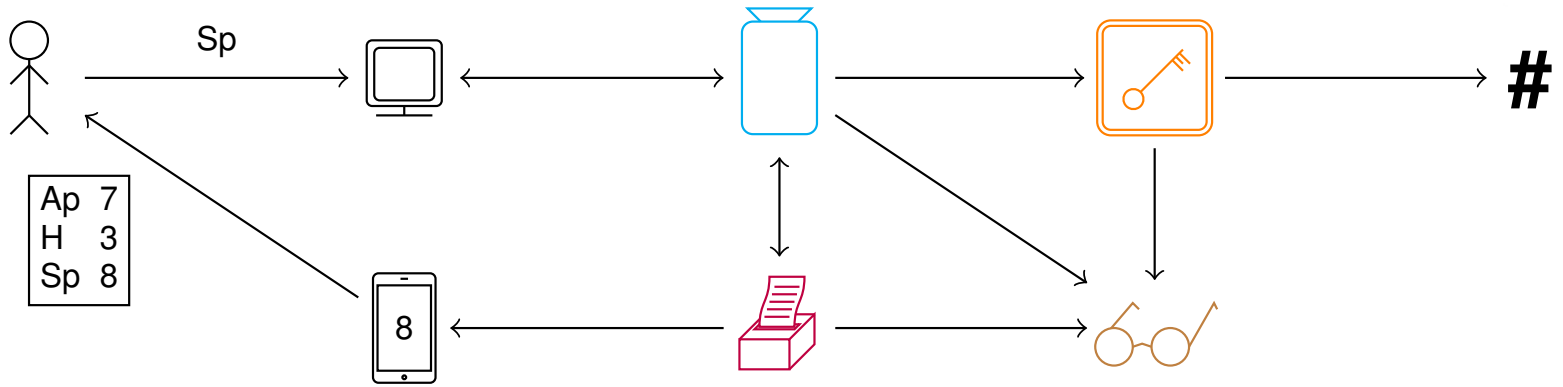
Future improvements

This is work done by two of my masters students.

- The encoded ballot consists of many group elements. The current system uses many independent ElGamal encryptions. A more efficient solution is to use an ElGamal variant that can encrypt more than one group element.
- It is problematic that the ballot box and the receipt generator share the election decryption key. It is possible to fix this.
- The decryption can be done by a verifiable combined shuffle and decryption, based on Groth's verifiable shuffle.

Overview

integrity — secrecy



ballot box — receipt generator — decryptor — auditor