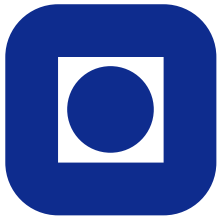


NTNU
Norwegian University of
Science and Technology

The mathematics of Internet voting

Kristian Gjøsteen

Department of mathematical sciences, NTNU

Oslo, September 11, 2011

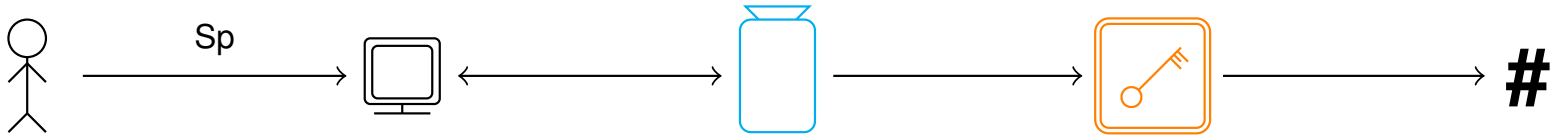
Content

[. . .] 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

Overview

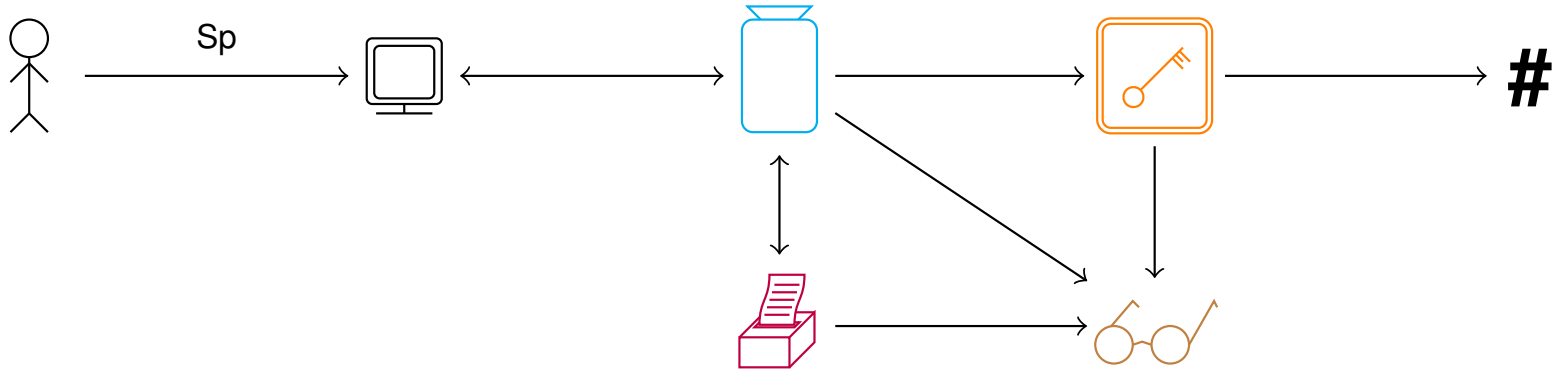
integrity — secrecy



ballot box — — decryptor —

Overview

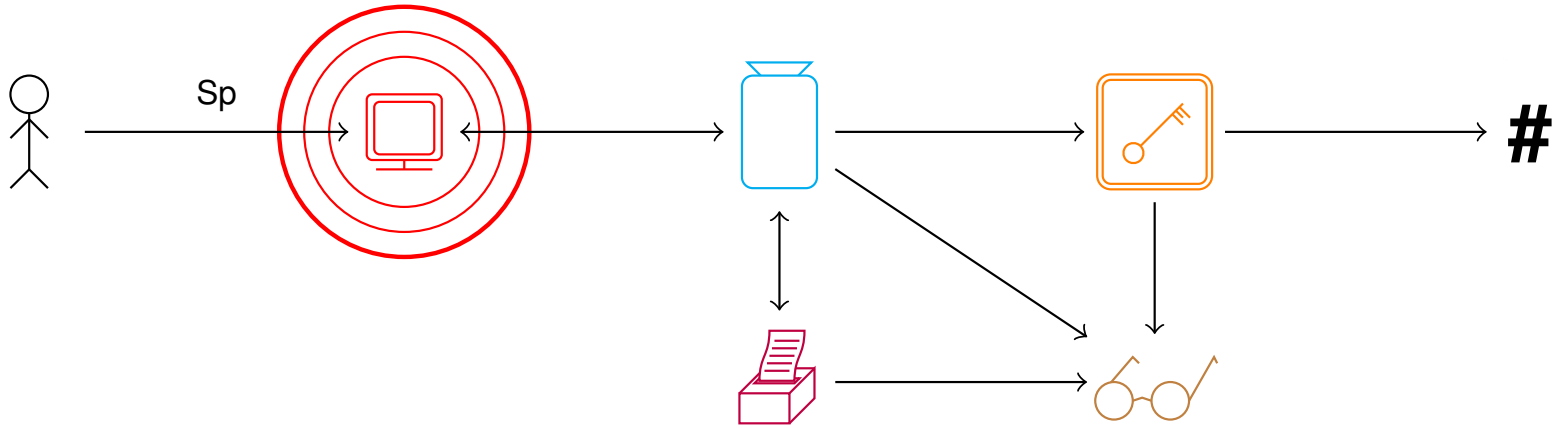
integrity — secrecy



ballot box — return code generator — decryptor — auditor

Overview

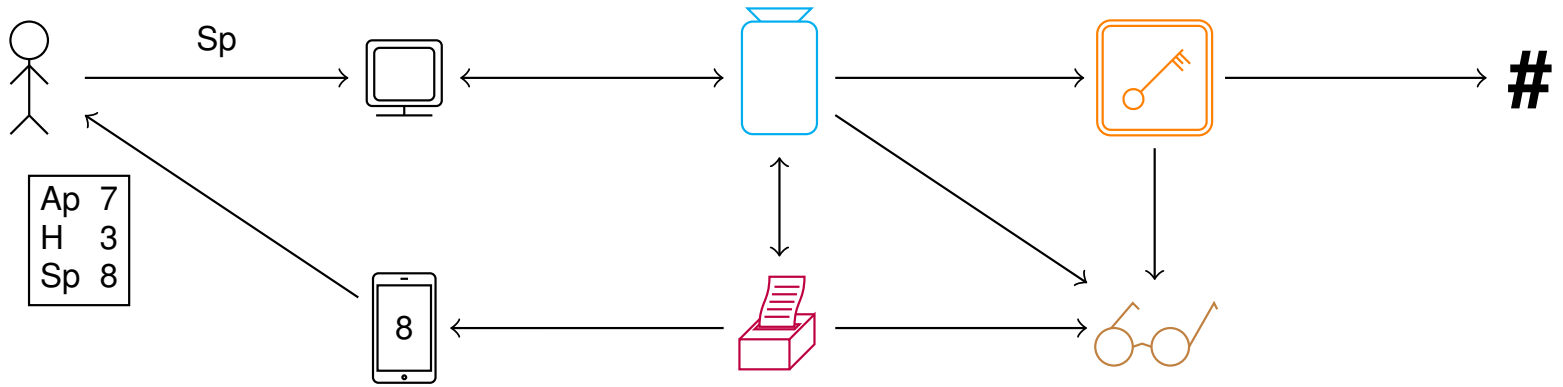
integrity — secrecy



ballot box — return code generator — decryptor — auditor

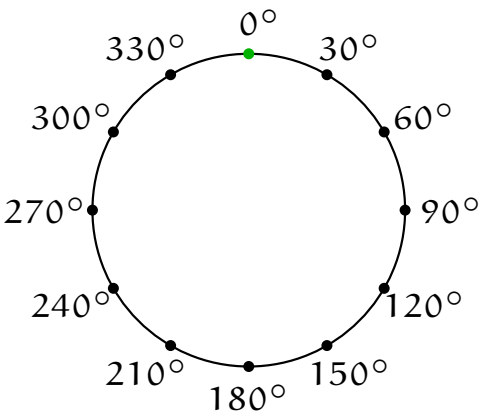
Overview

integrity — secrecy



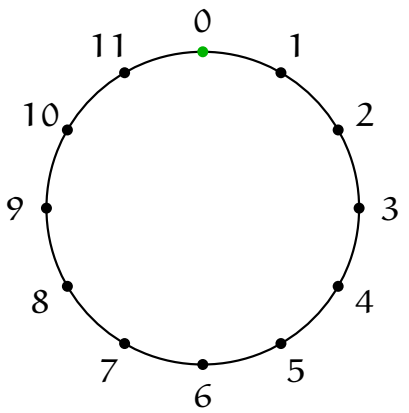
ballot box — return code generator — decryptor — auditor

Where are we?



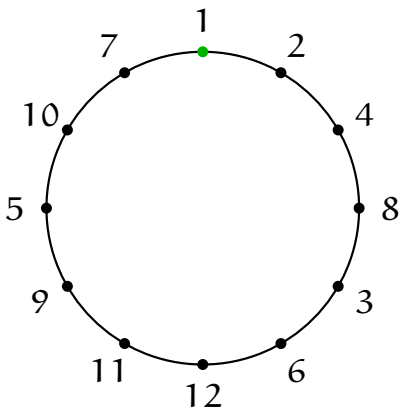
Let G be a prime order finite group.

Where are we?



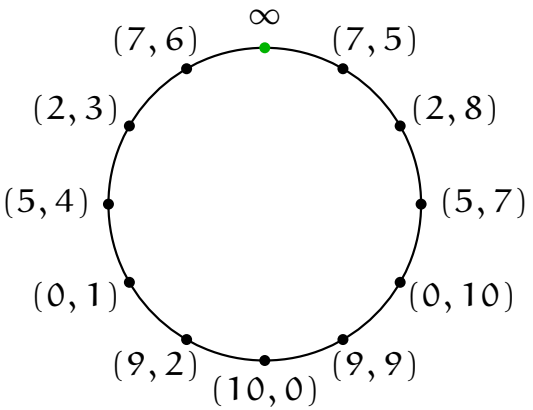
Let G be a prime order finite group.

Where are we?



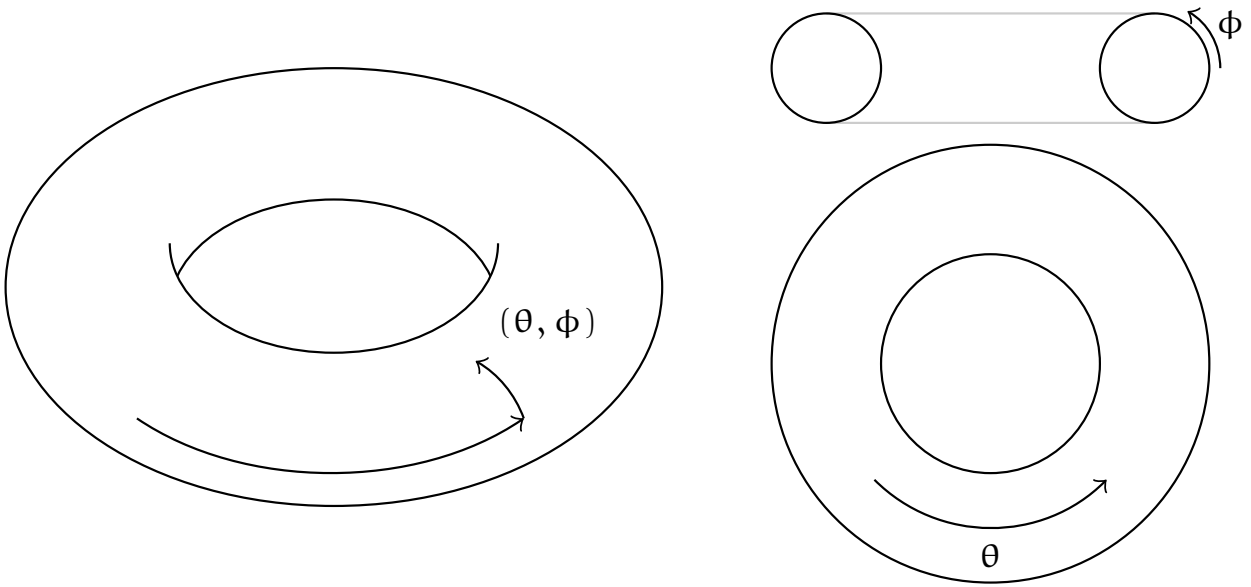
Let G be a prime order finite group.

Where are we?



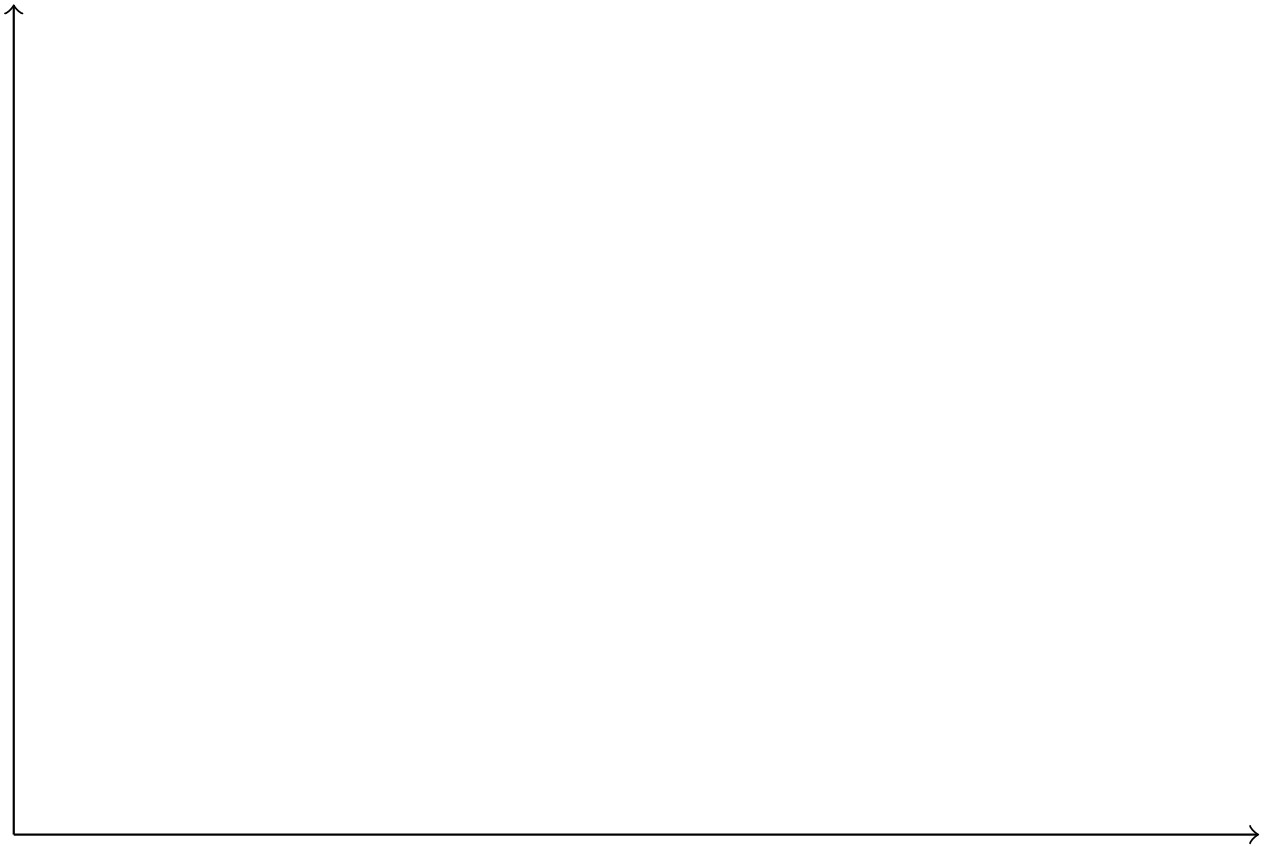
Let G be a prime order finite group.

Where are we?



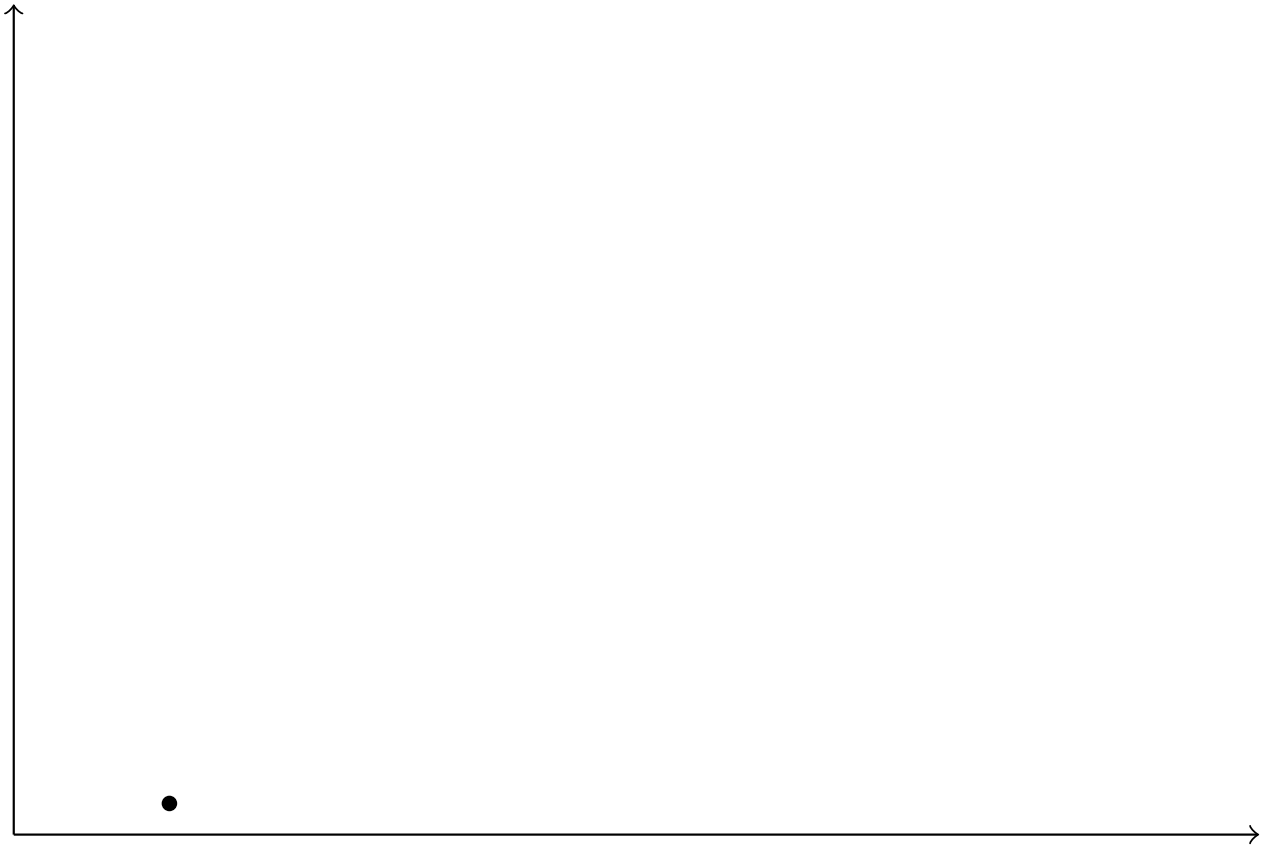
This is $G \times G$.

Properties

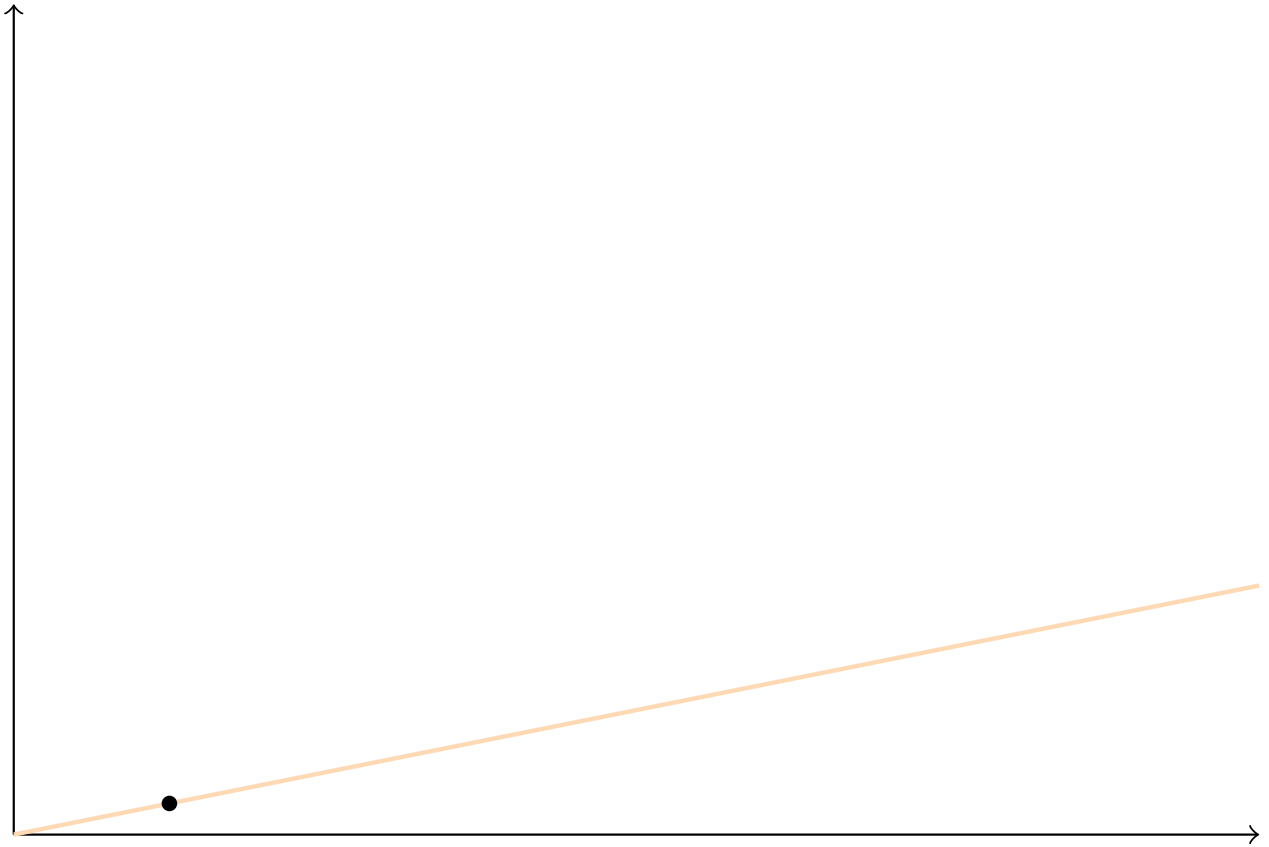


Easier to draw a plane.

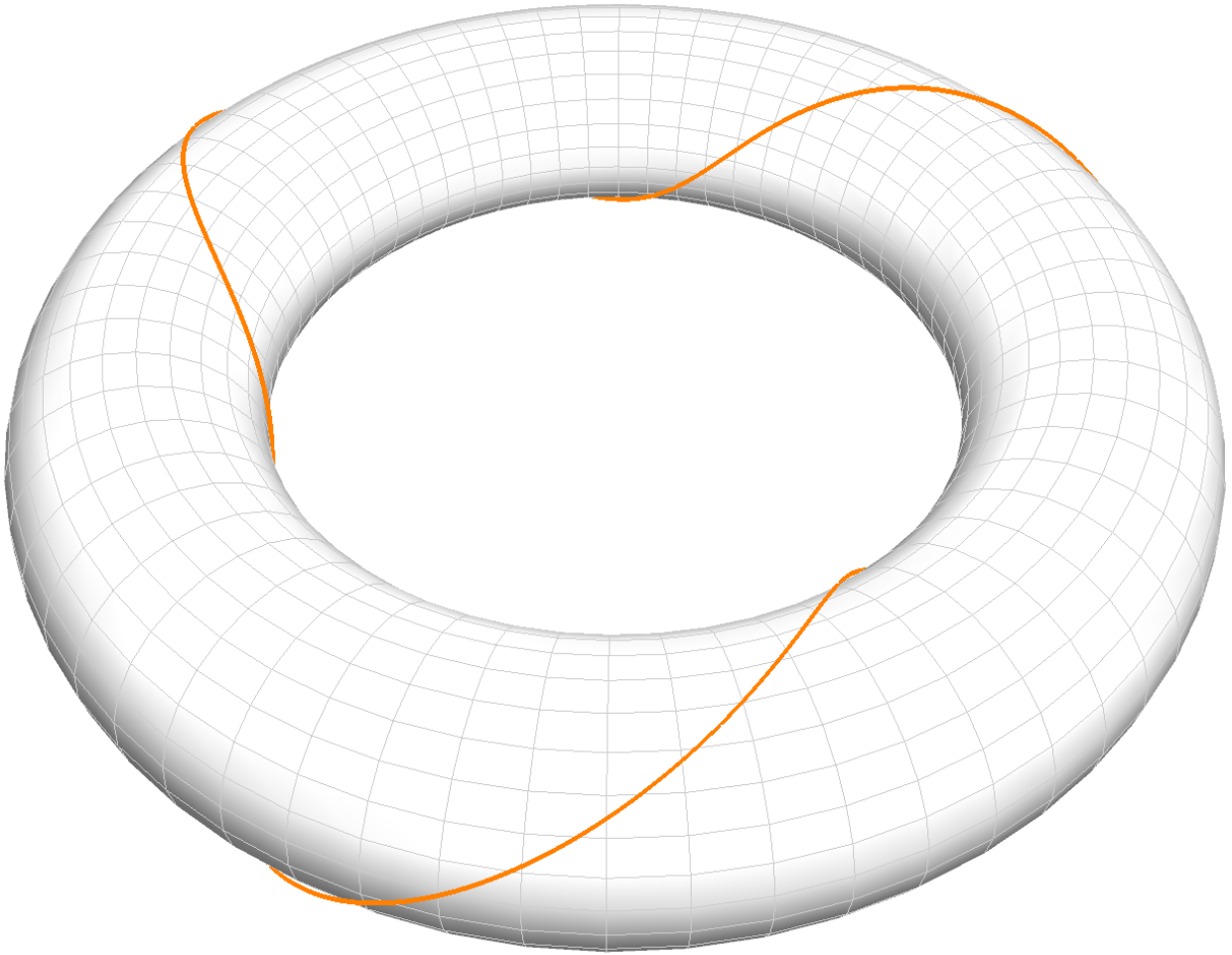
Properties



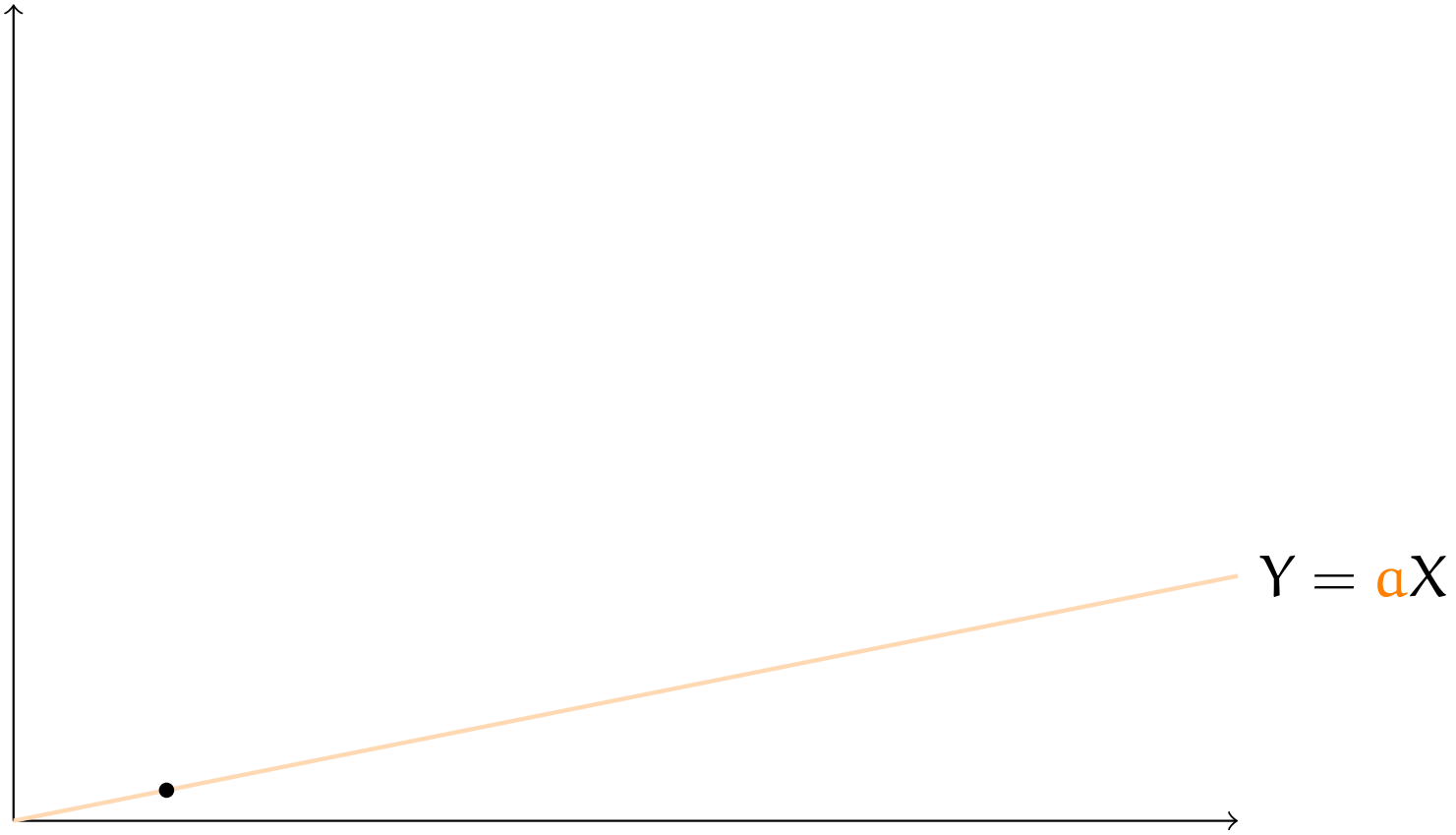
Properties



Lines on donuts

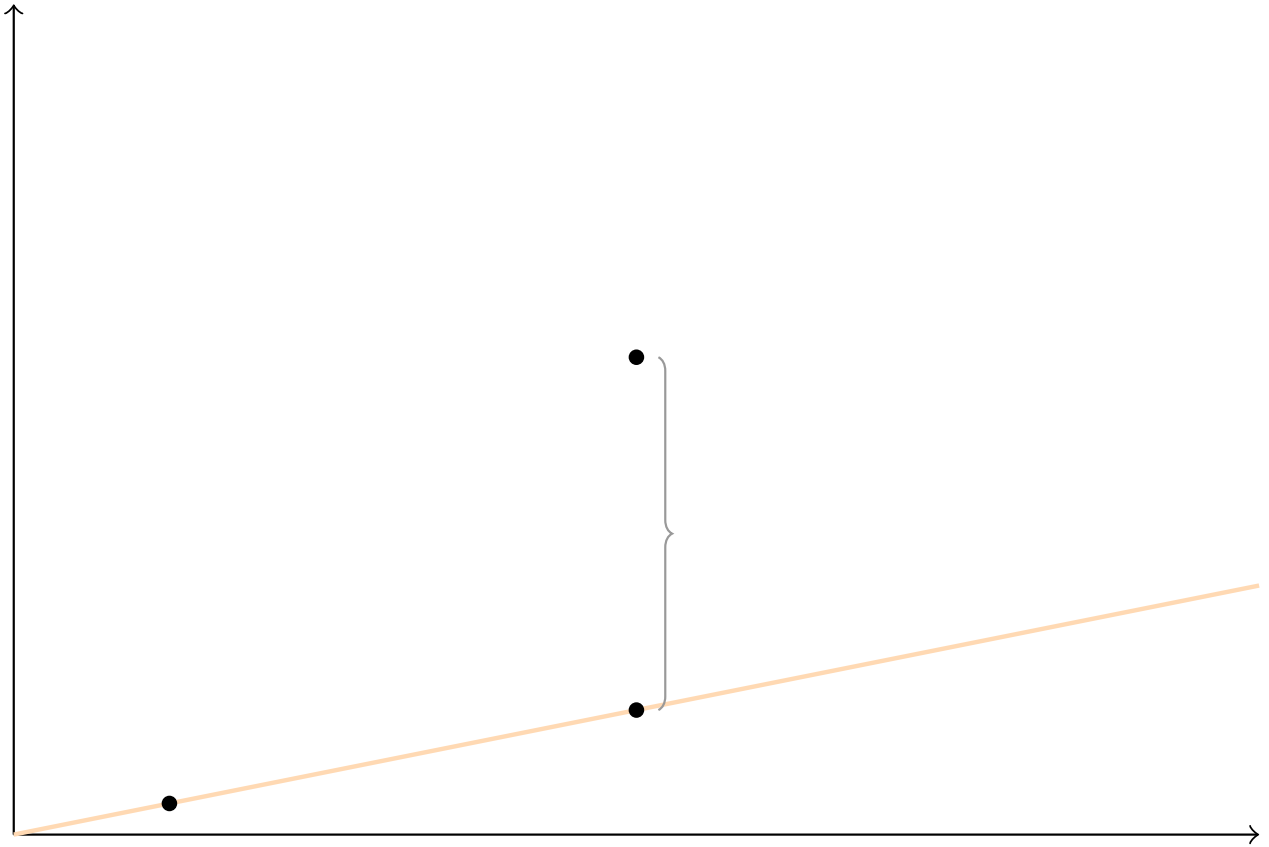


Properties



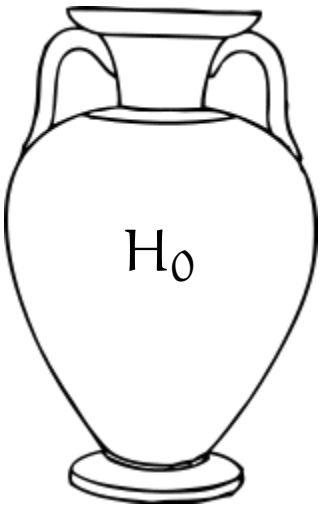
What is the slope of the line? *Discrete logarithms.*

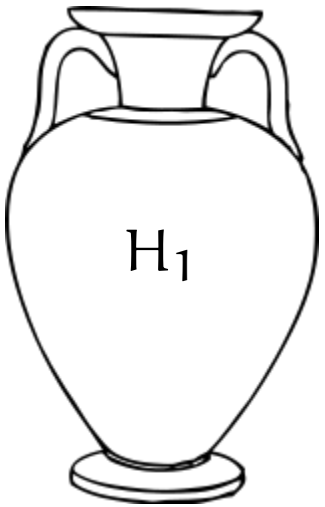
Properties



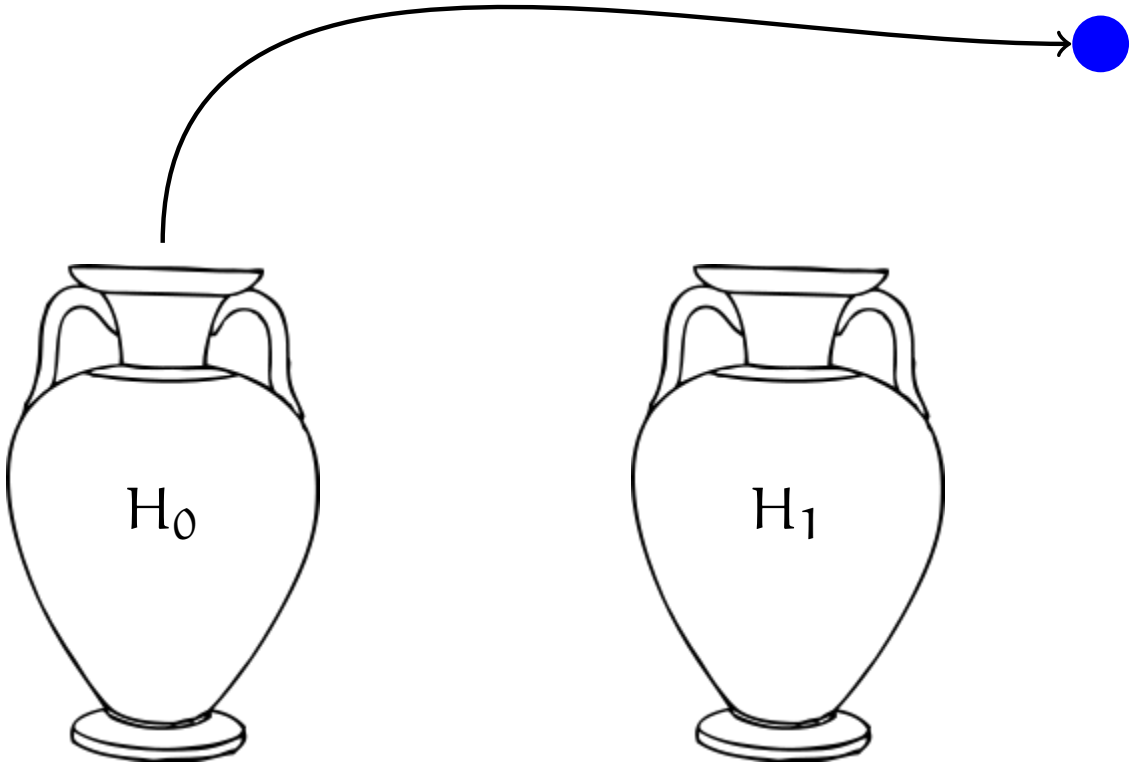
What is the vertical distance from a randomly chosen point down to the line? *Computational Diffie-Hellman*.

Hypothesis testing

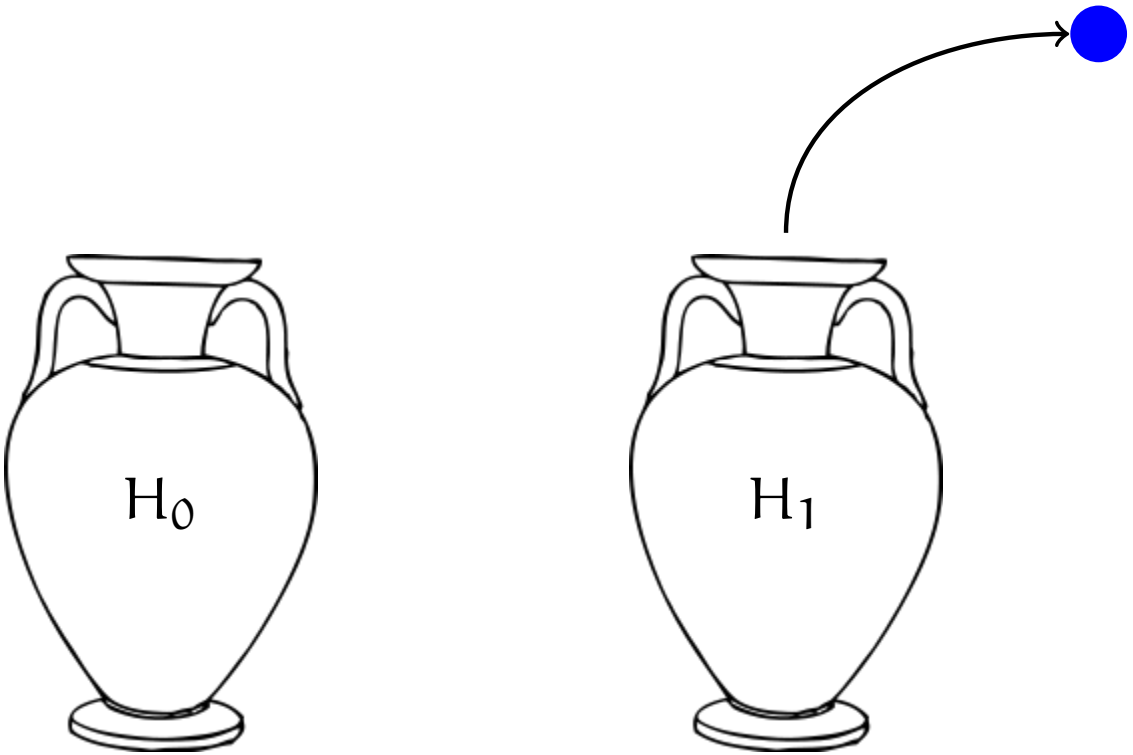




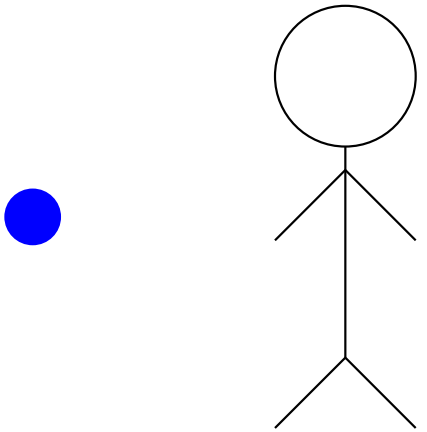
Hypothesis testing

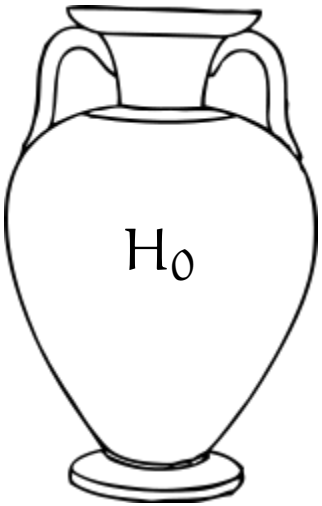


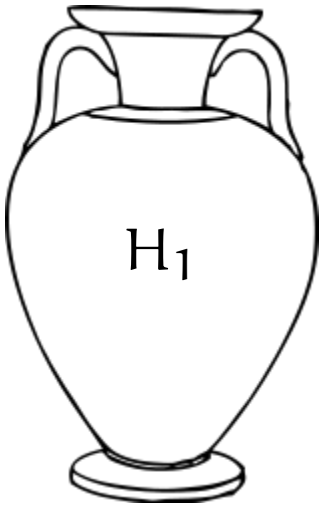
Hypothesis testing



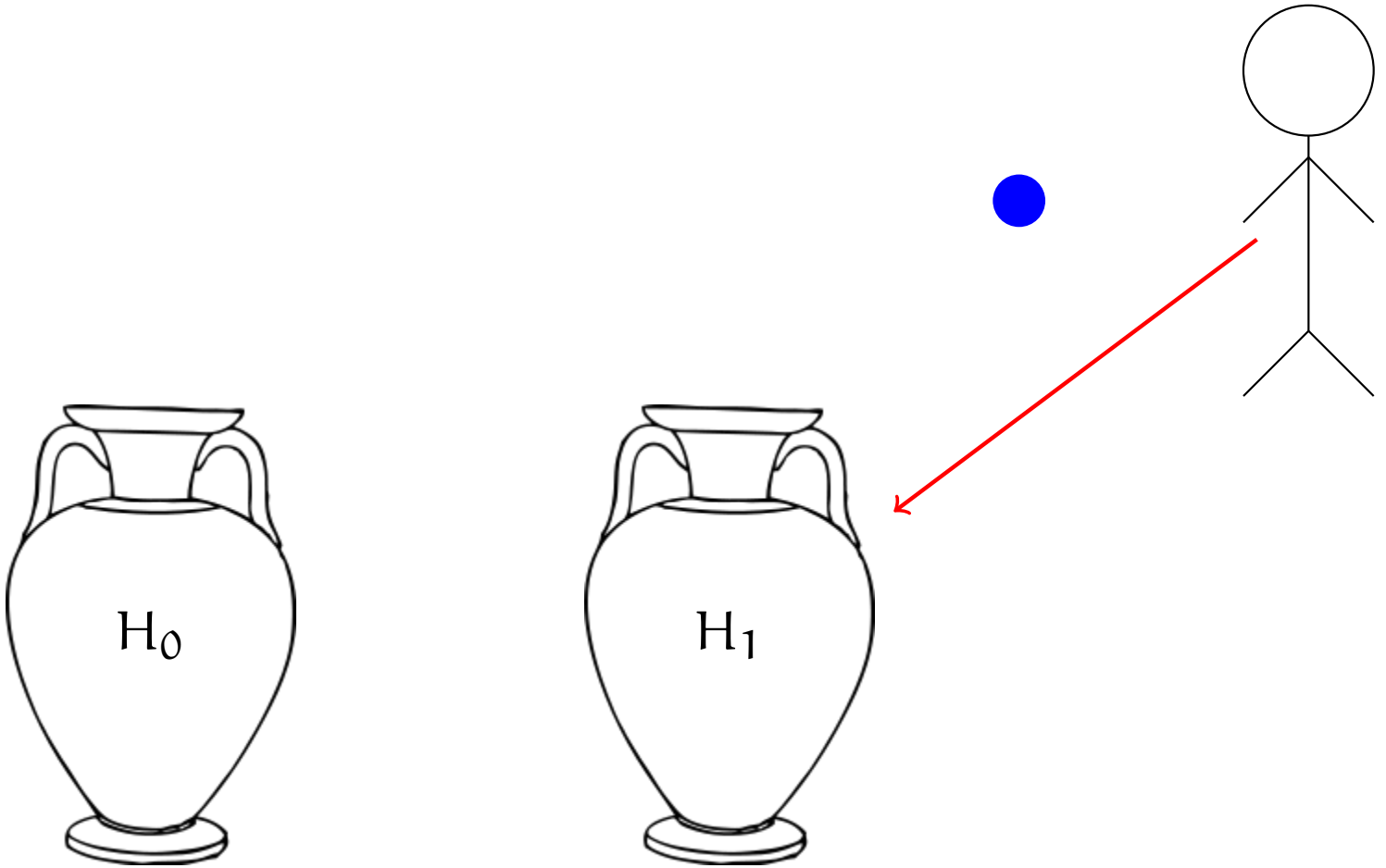
Hypothesis testing



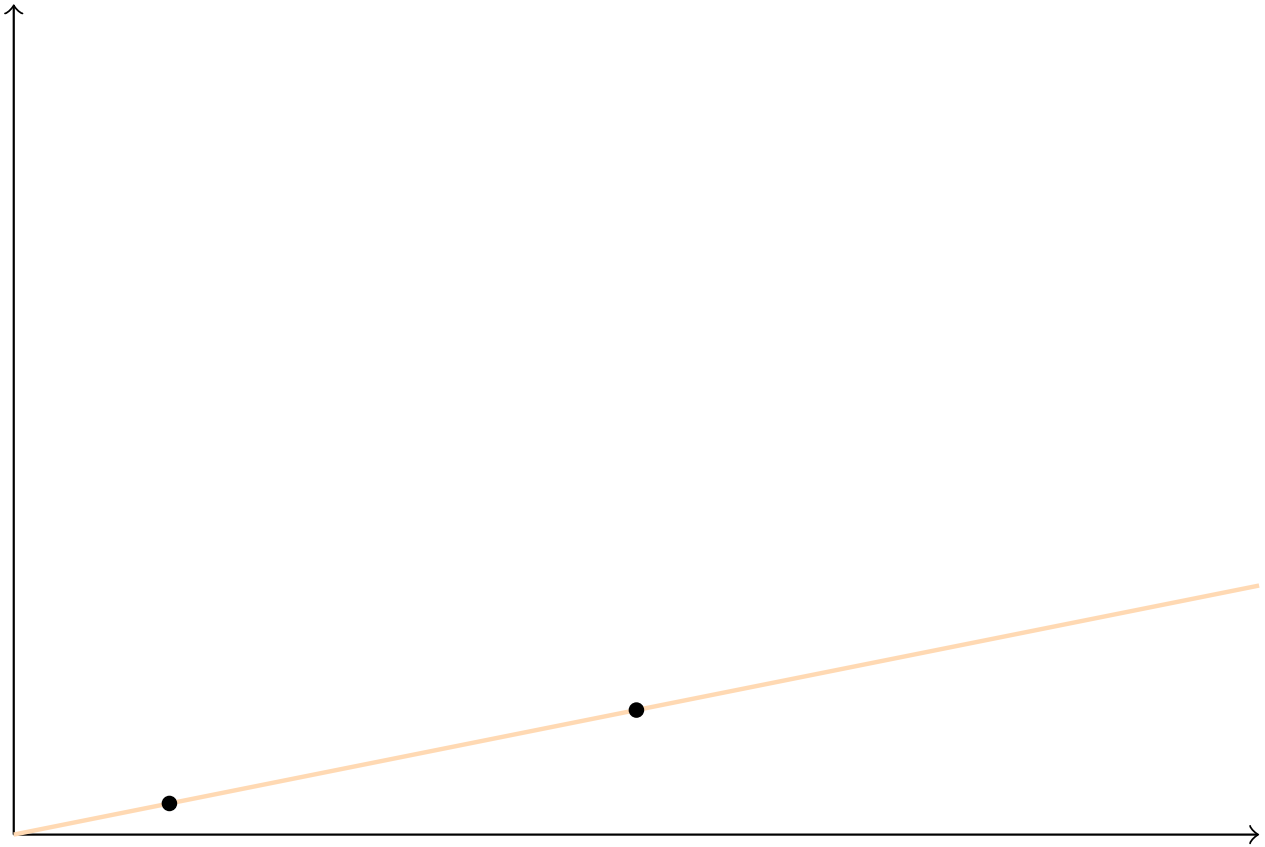




Hypothesis testing

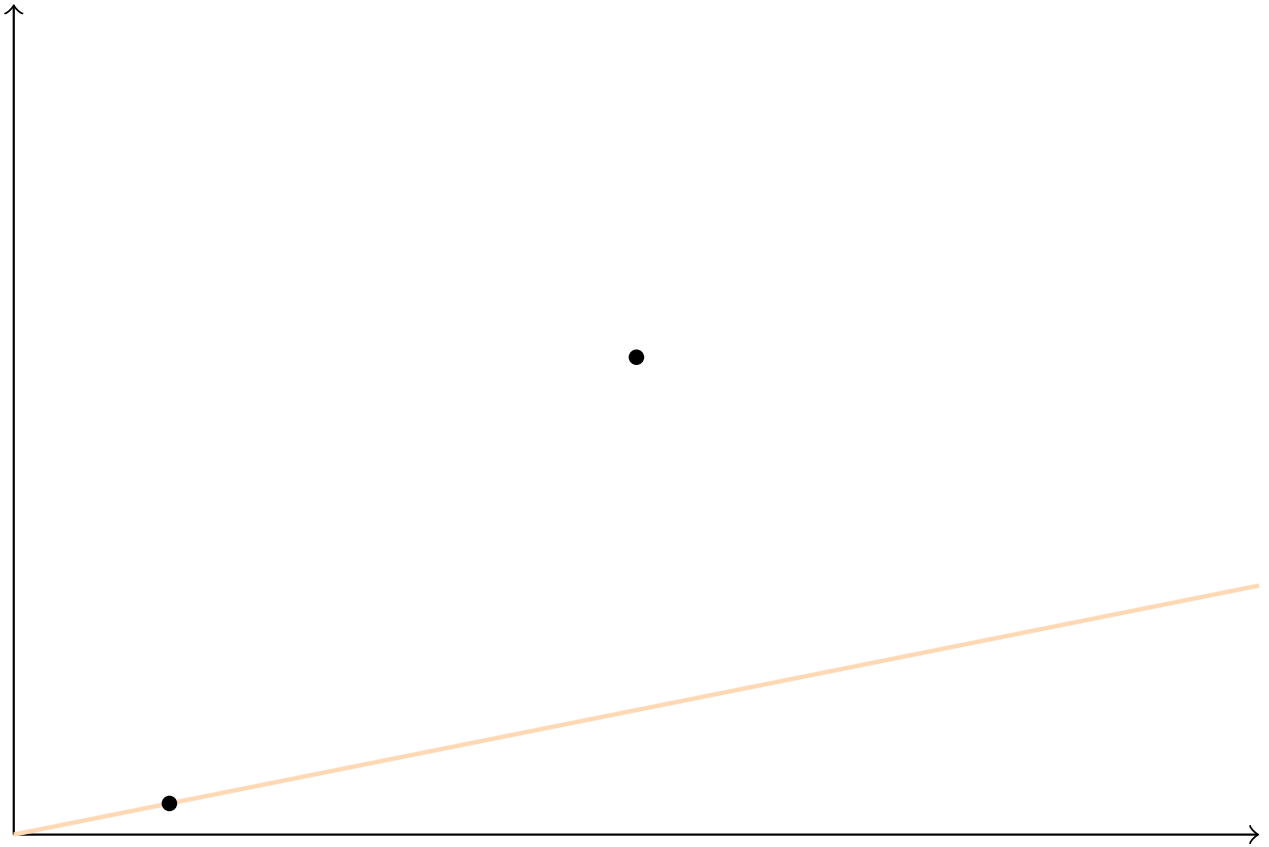


Properties



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

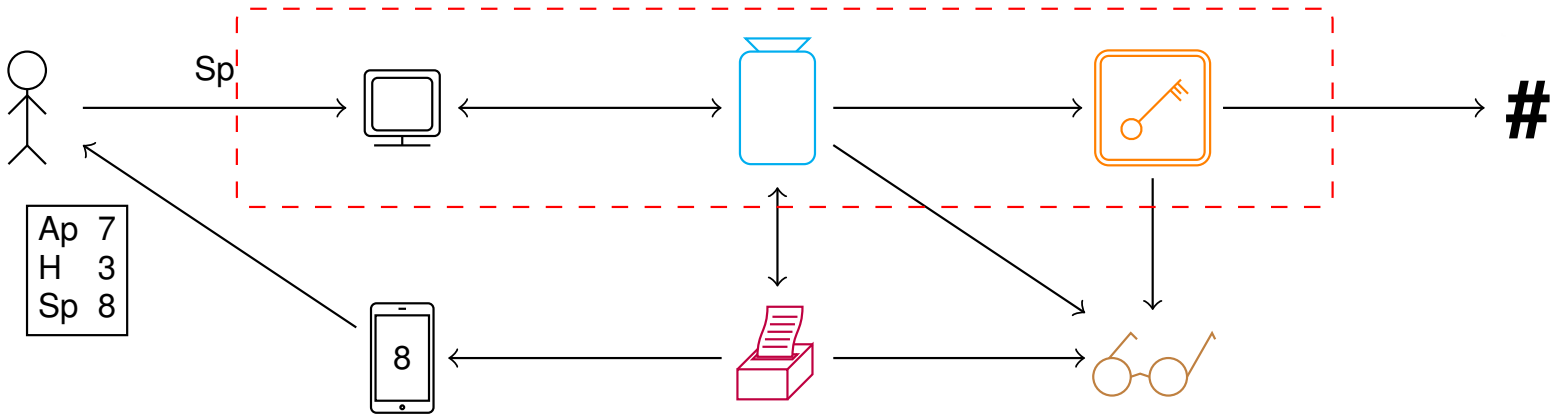
Properties



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

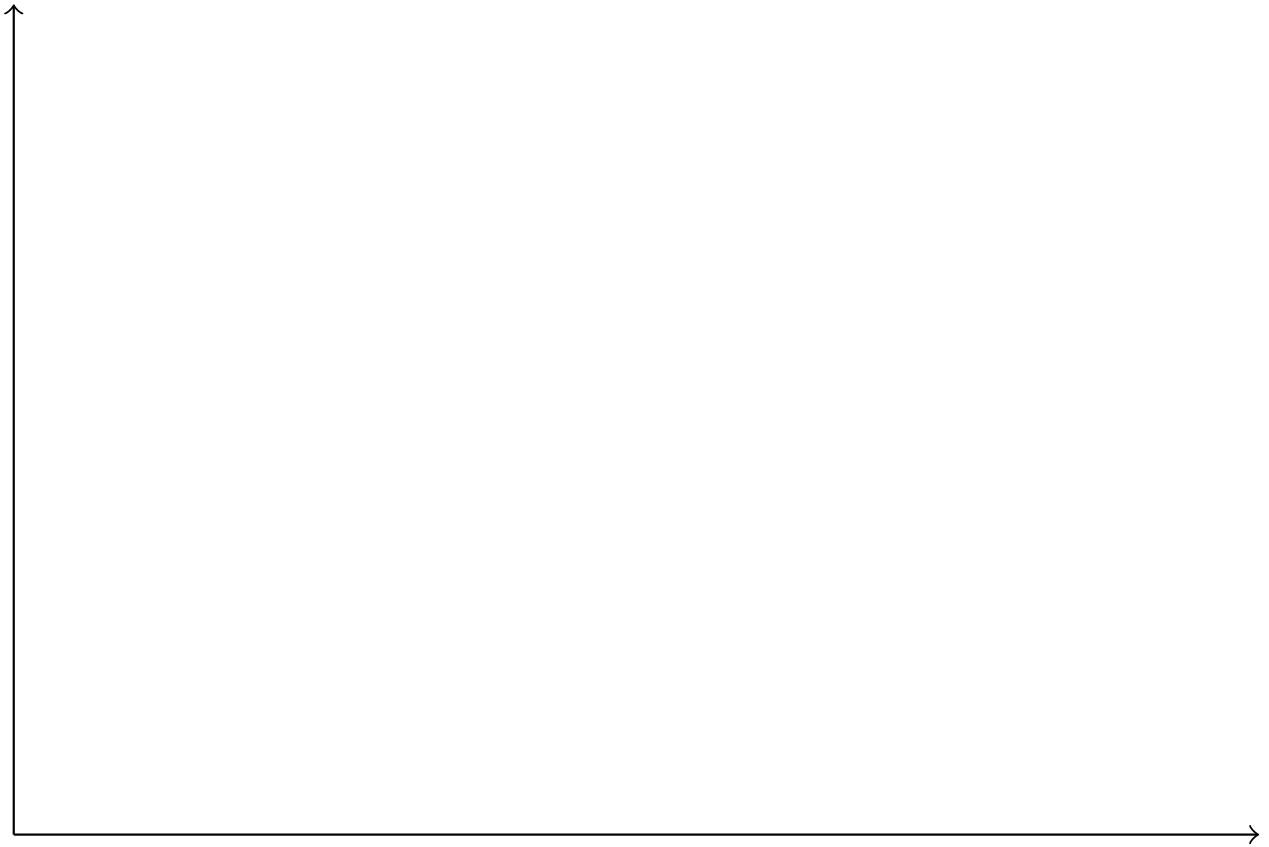
Overview

integrity — secrecy



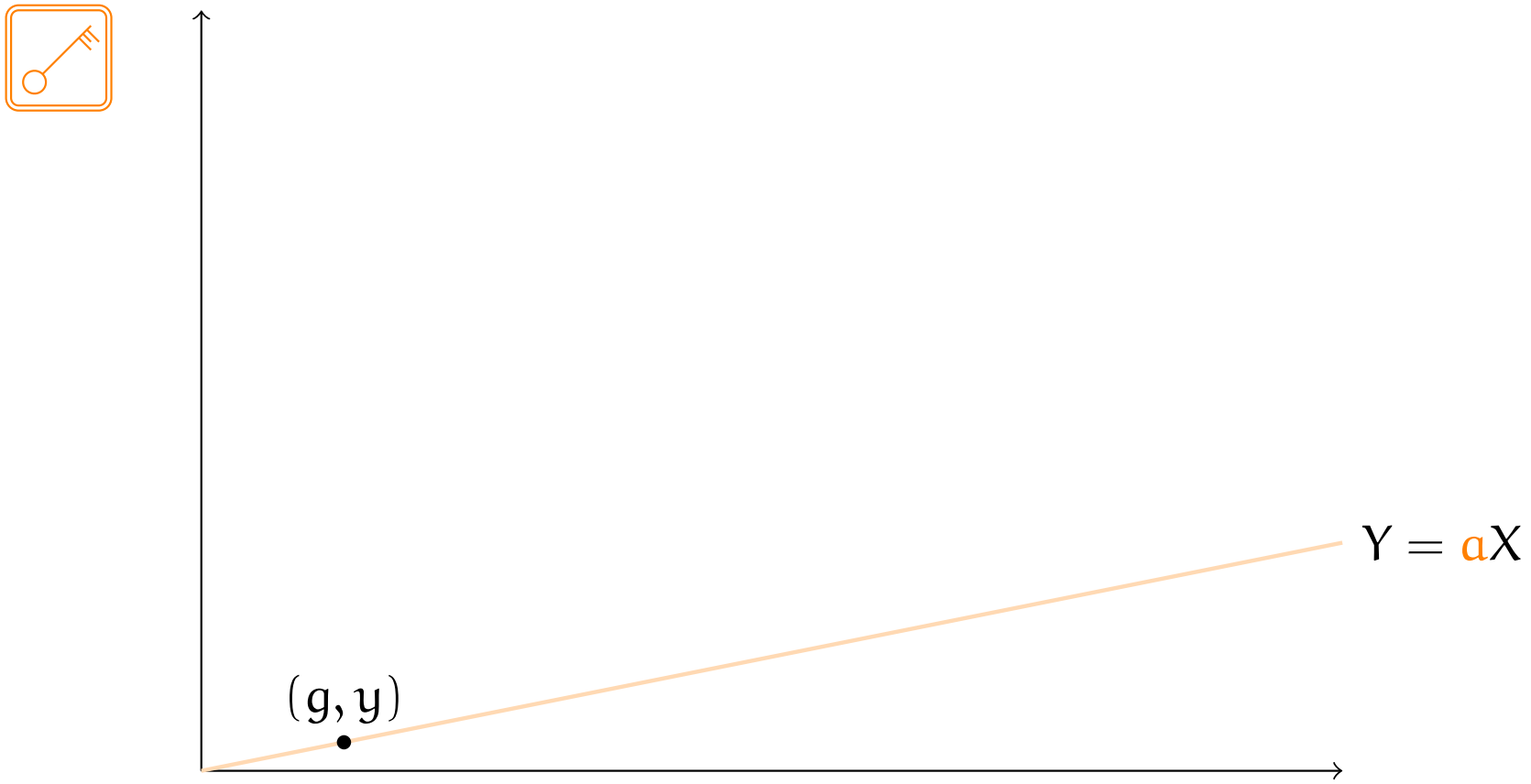
ballot box — return code generator — decryptor — auditor

ElGamal encryption



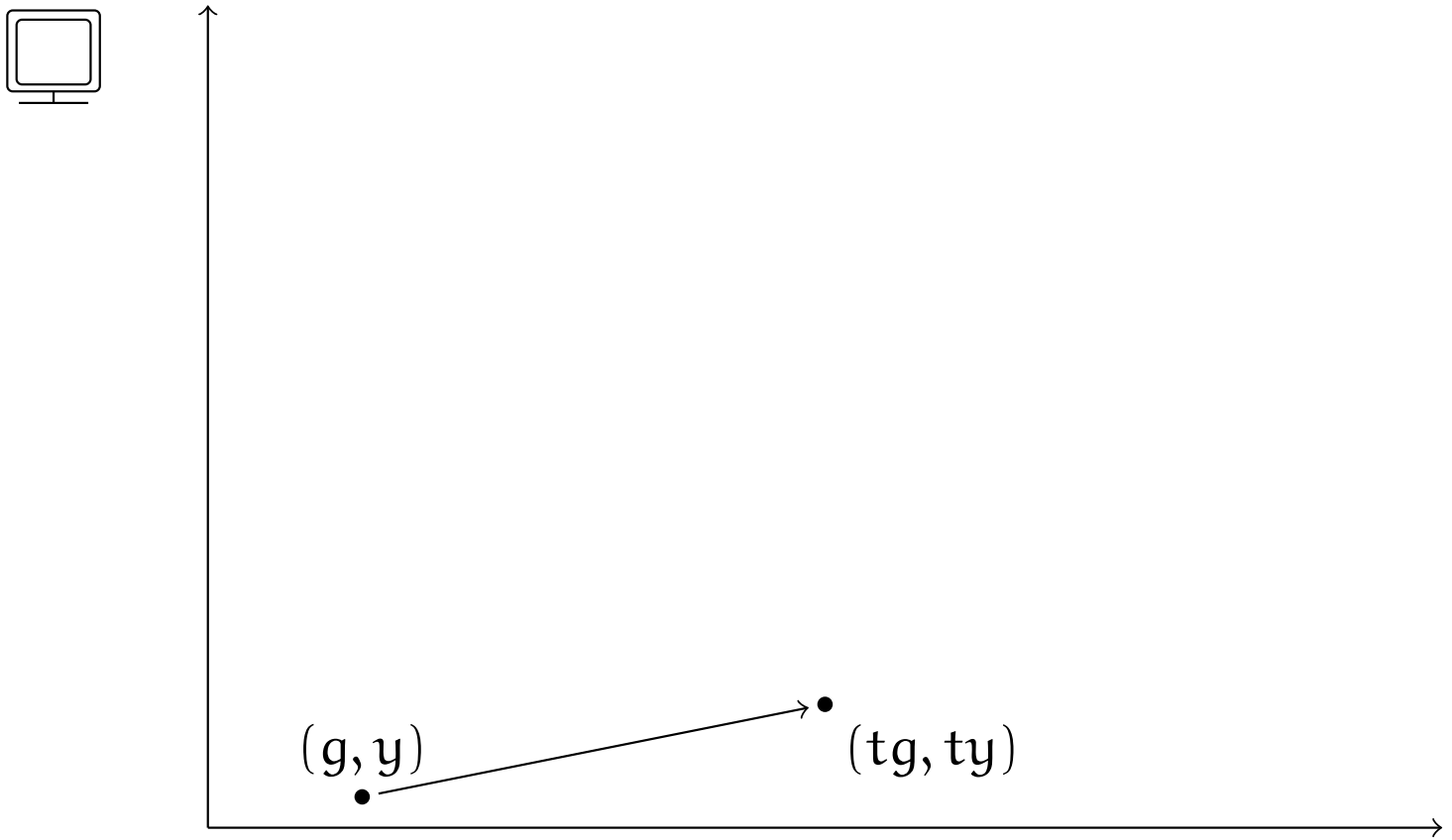
How to encrypt a ballot v?

ElGamal encryption



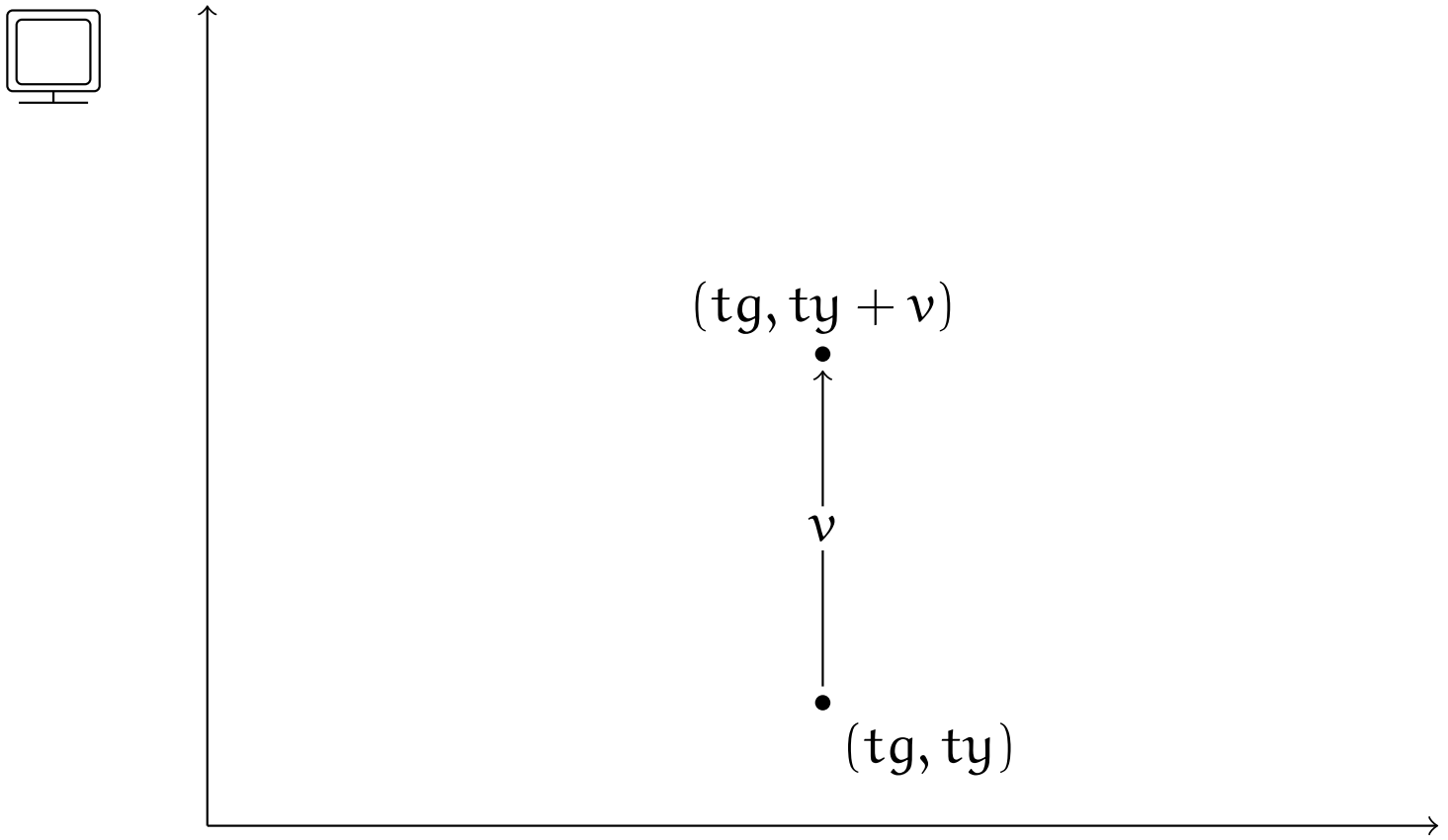
The electoral board selects a slope a and a point (g, y) on the line $Y = aX$.

ElGamal encryption



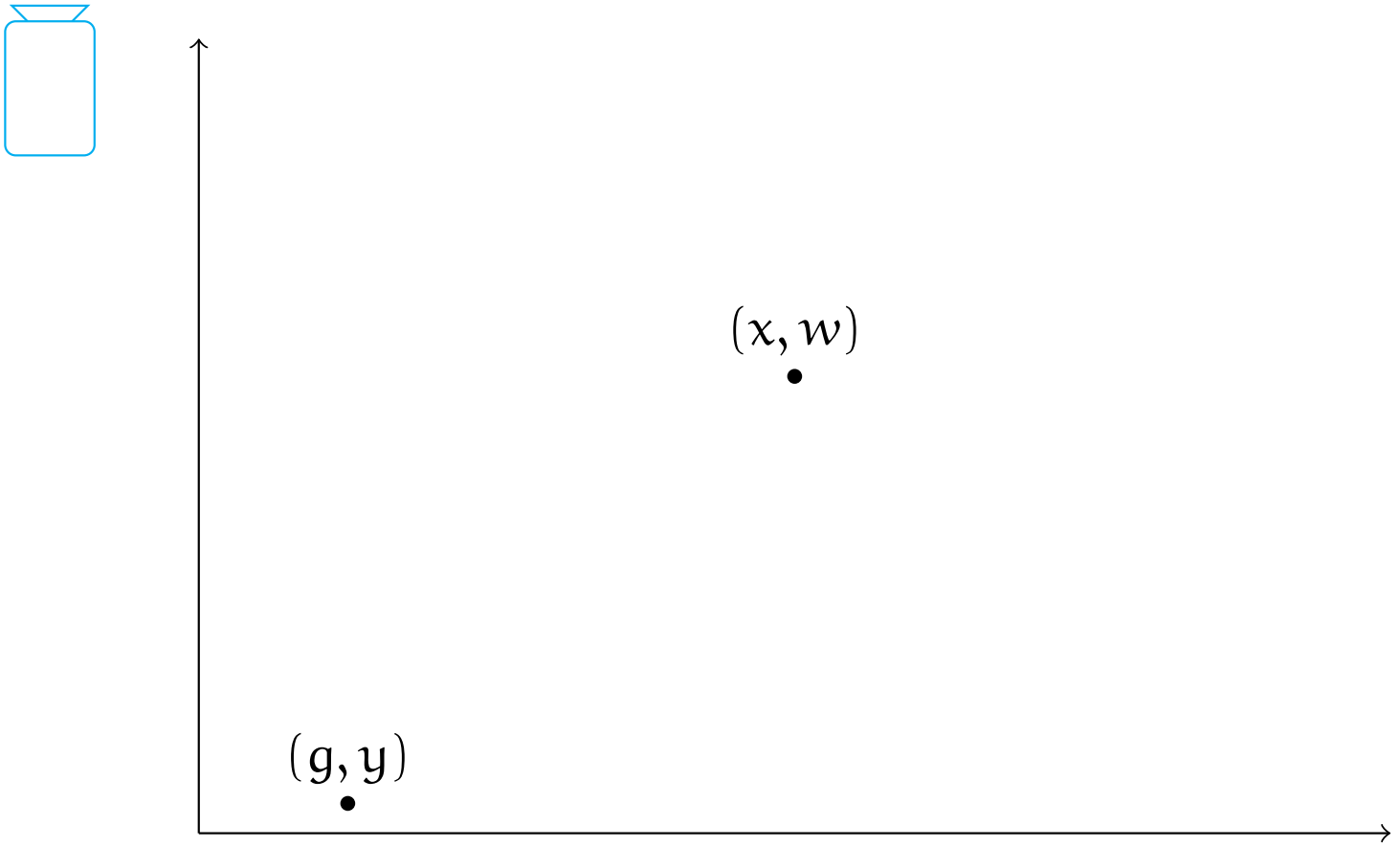
The voter's computer selects a random point on the line through (g, y).

ElGamal encryption



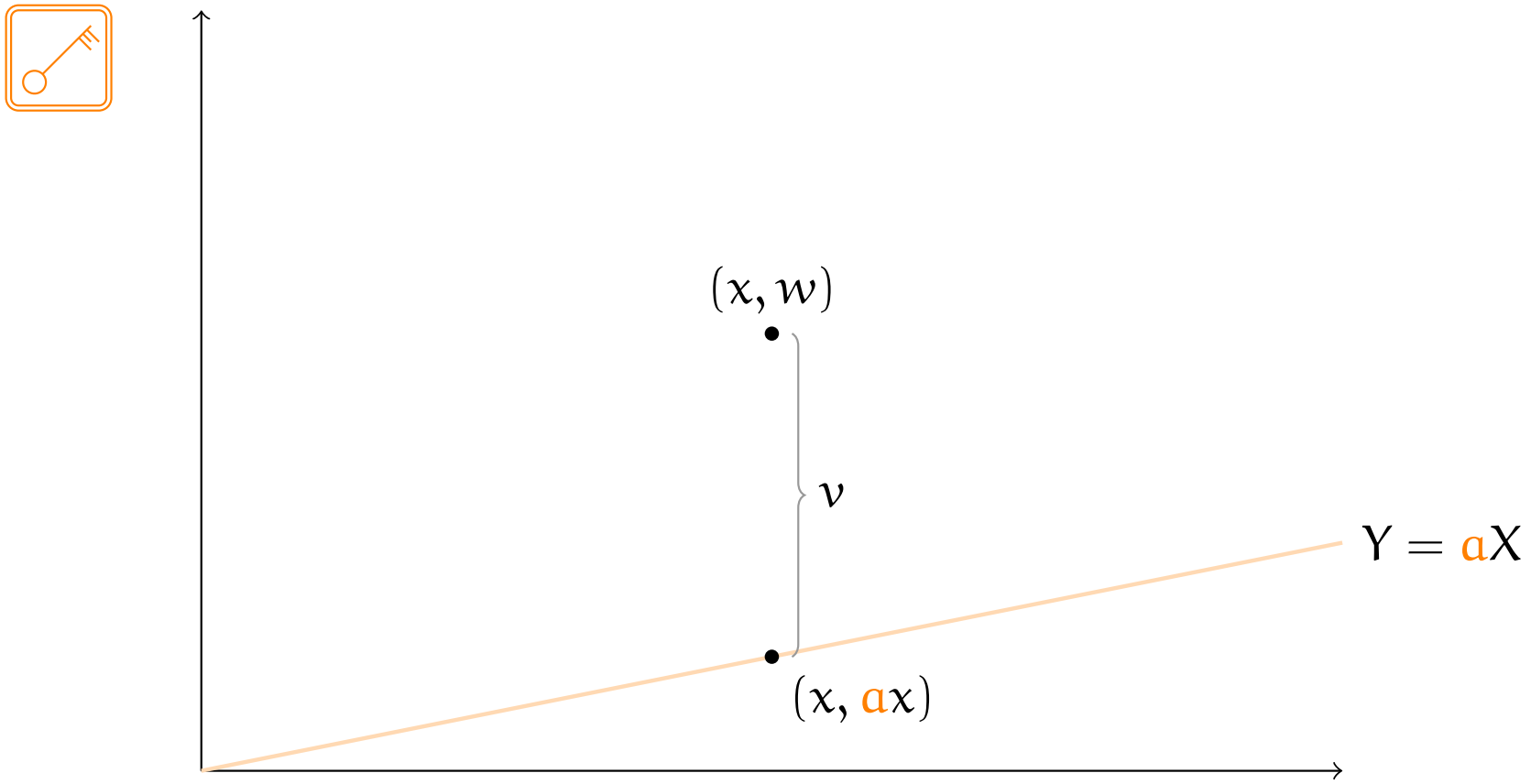
The computer shifts the point upwards by v.

ElGamal encryption



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

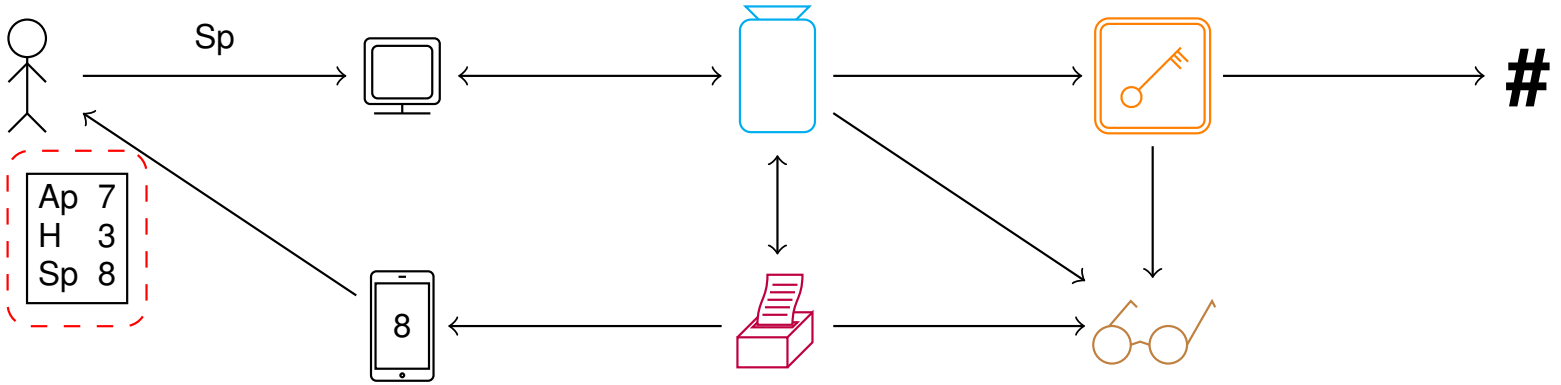
ElGamal encryption



The electoral board gets the ciphertext and recovers v.

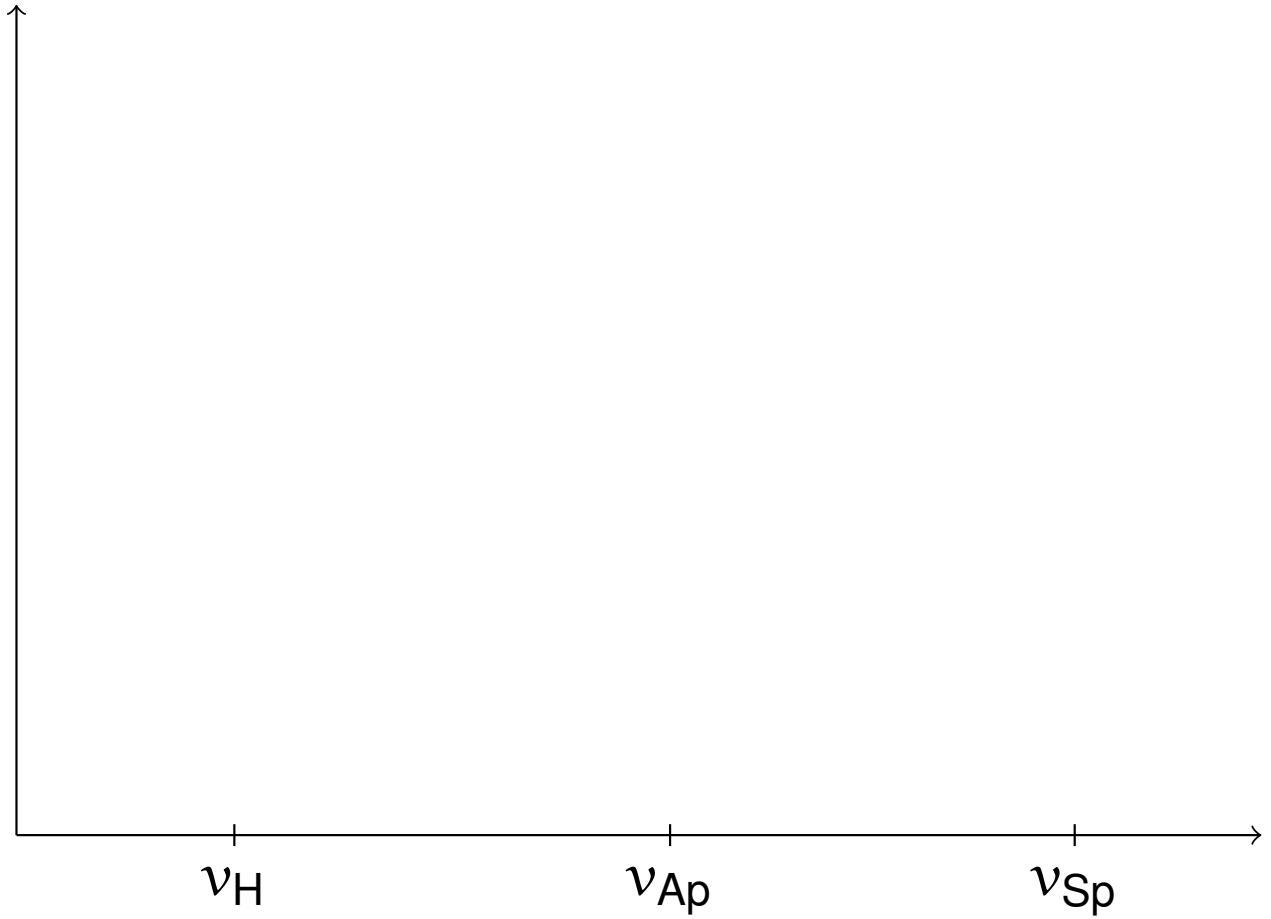
Overview

integrity — secrecy



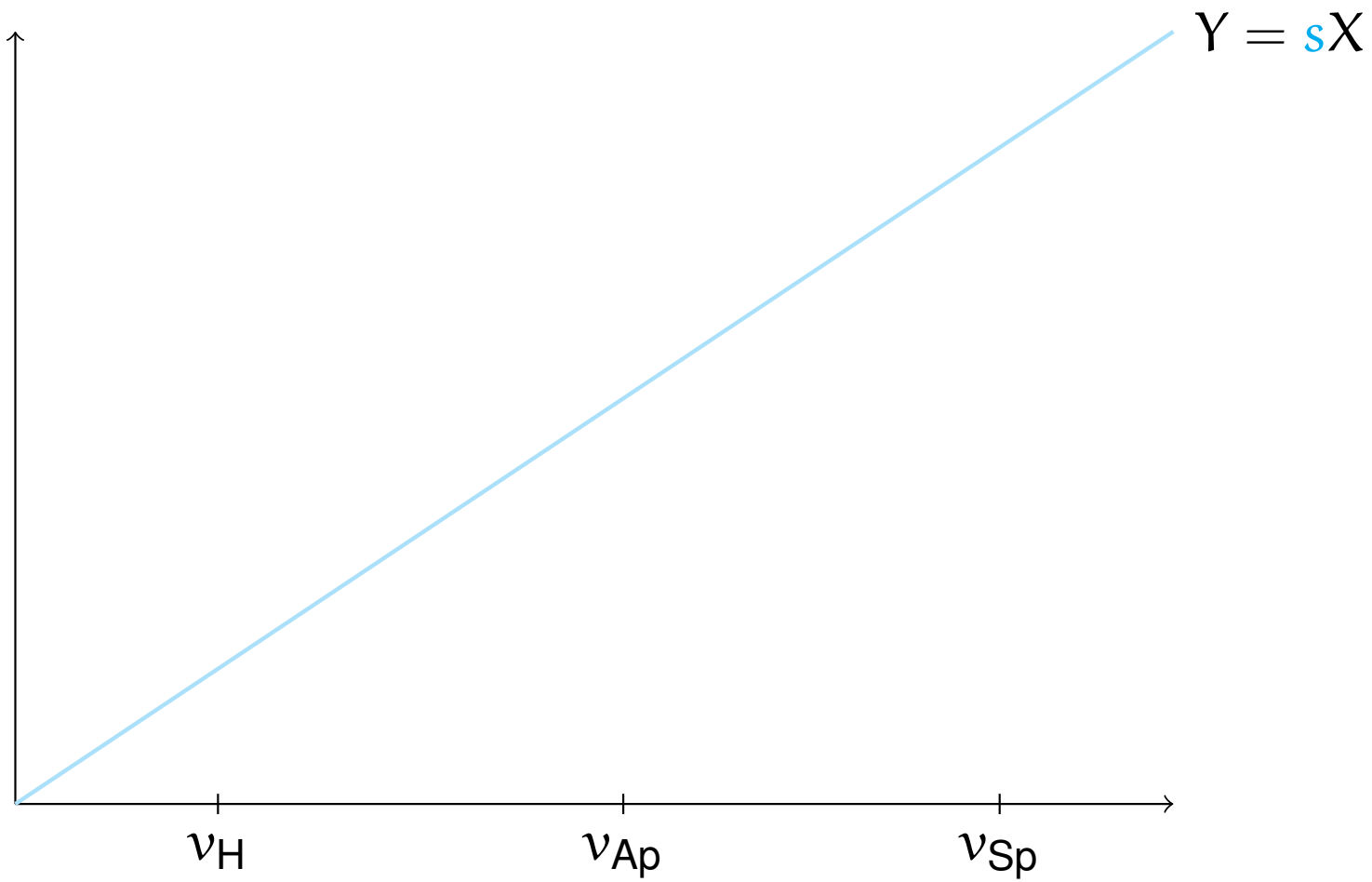
ballot box — return code generator — decryptor — auditor

Return Codes



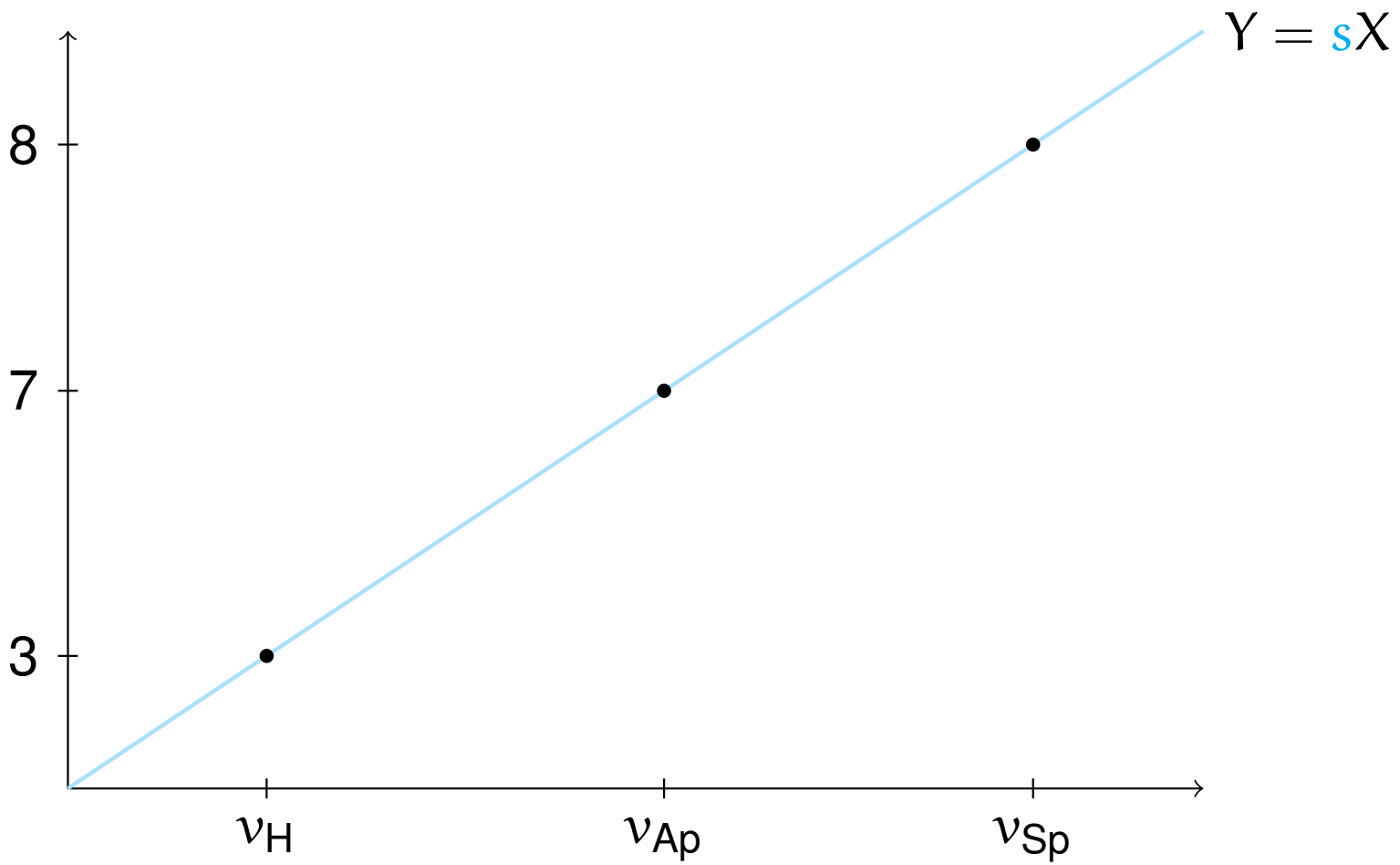
We must code parties as group elements.

Return Codes



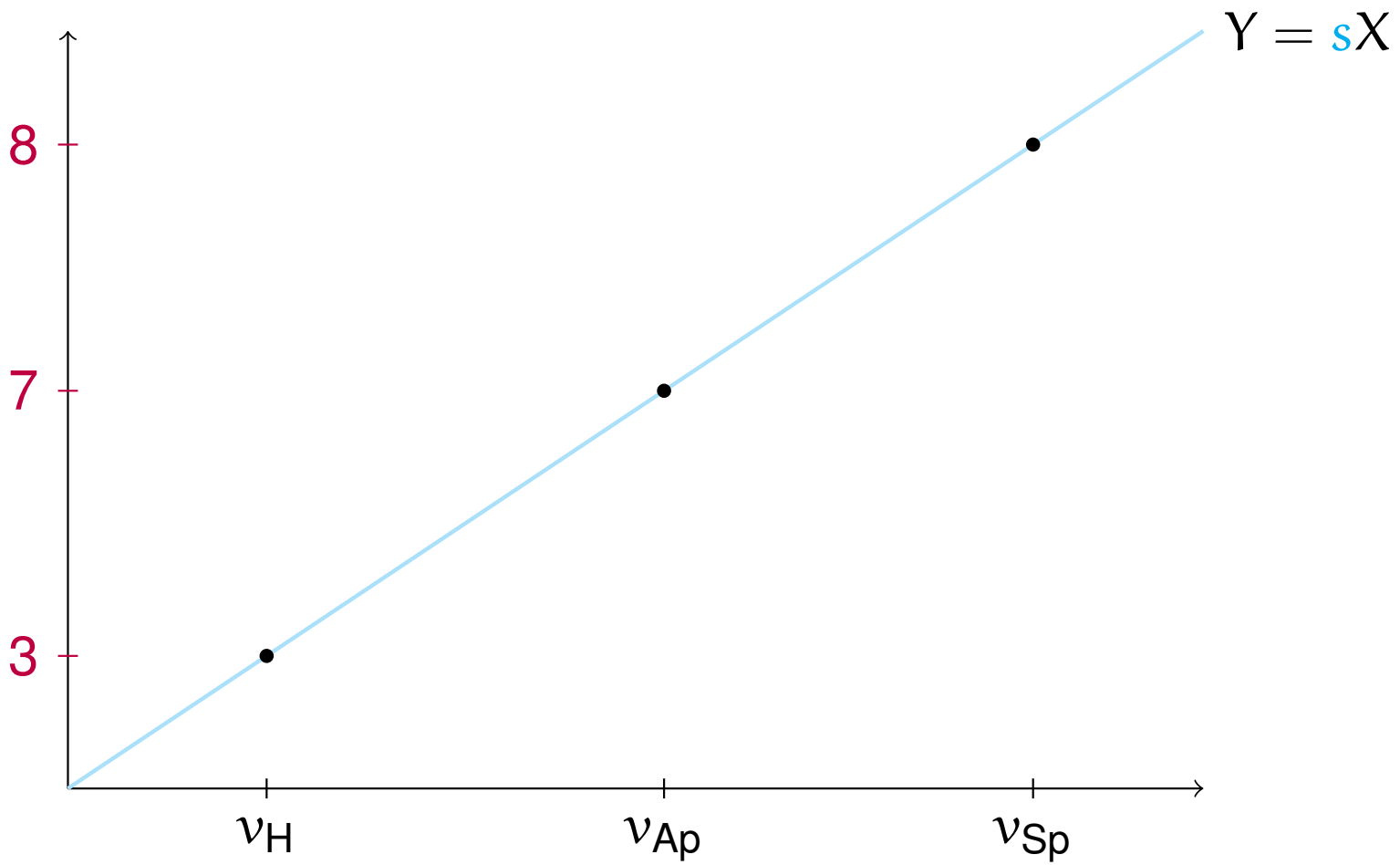
The electoral board assigns a random number s to each voter.

Return Codes



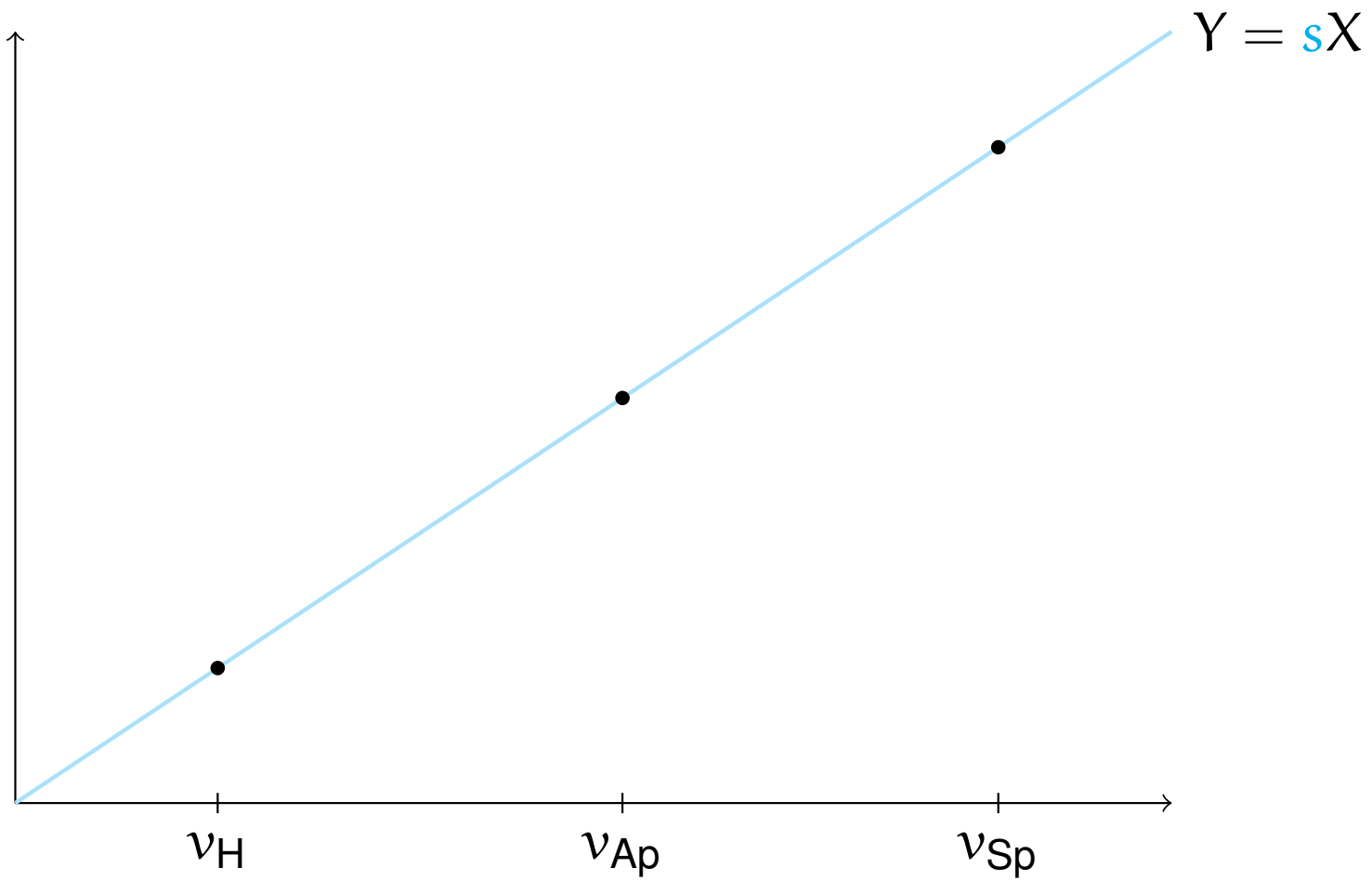
This voter's return code for party v will be sv.

Return Codes



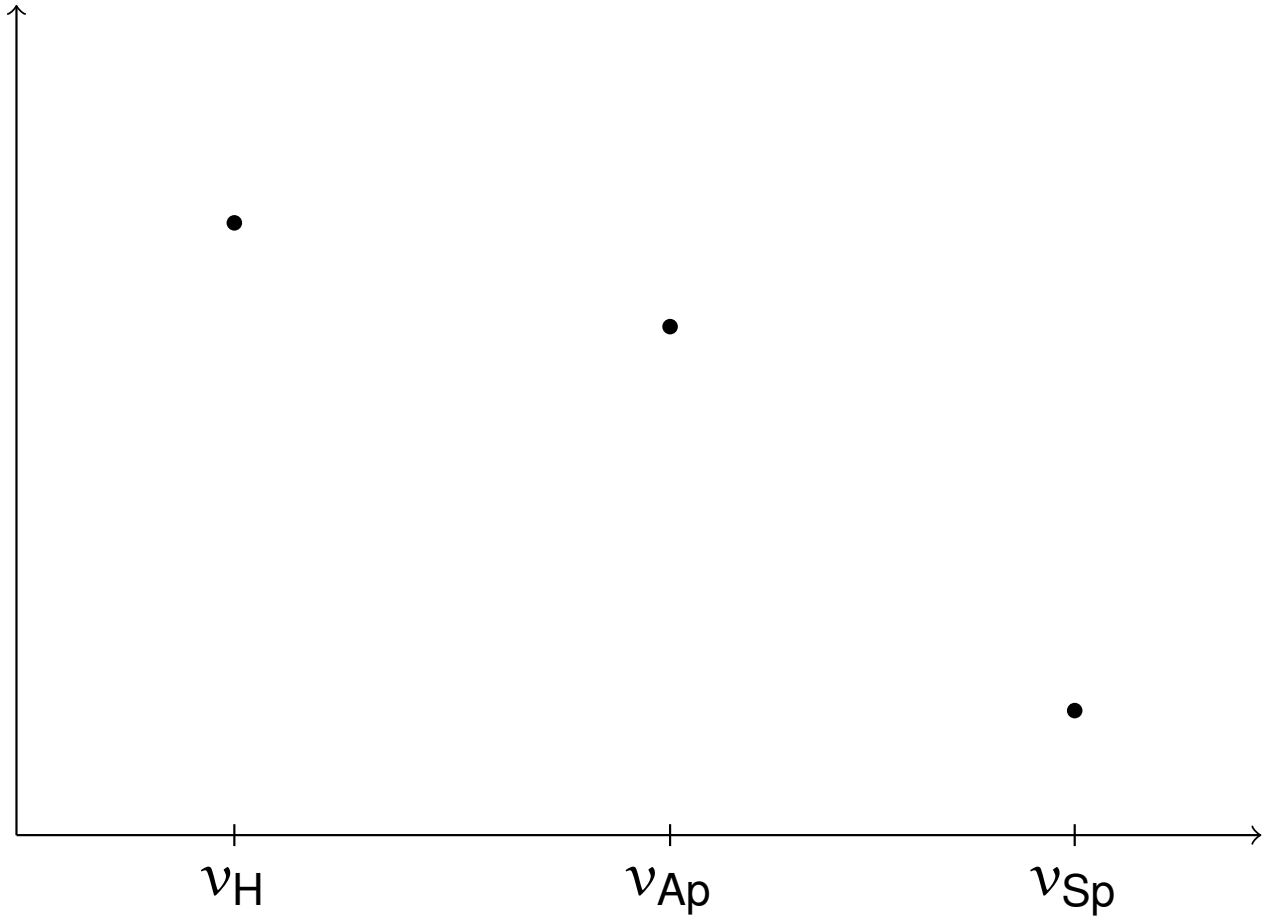
The return code generator sees the return codes.

Return Codes



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

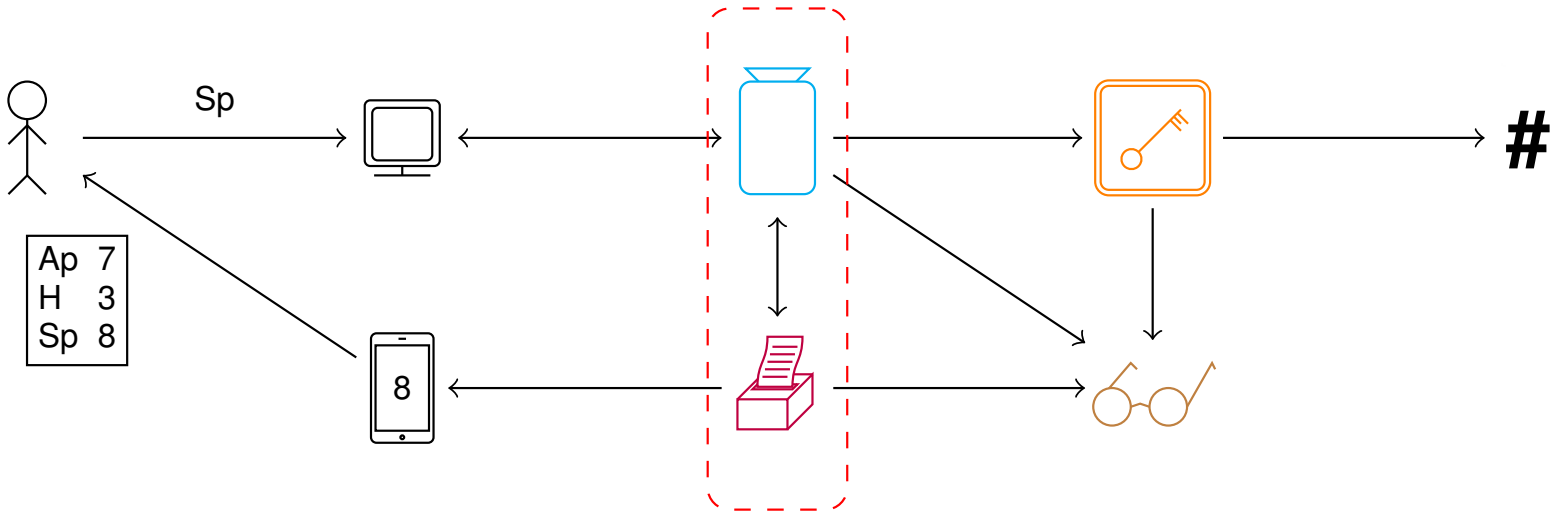
Return Codes



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

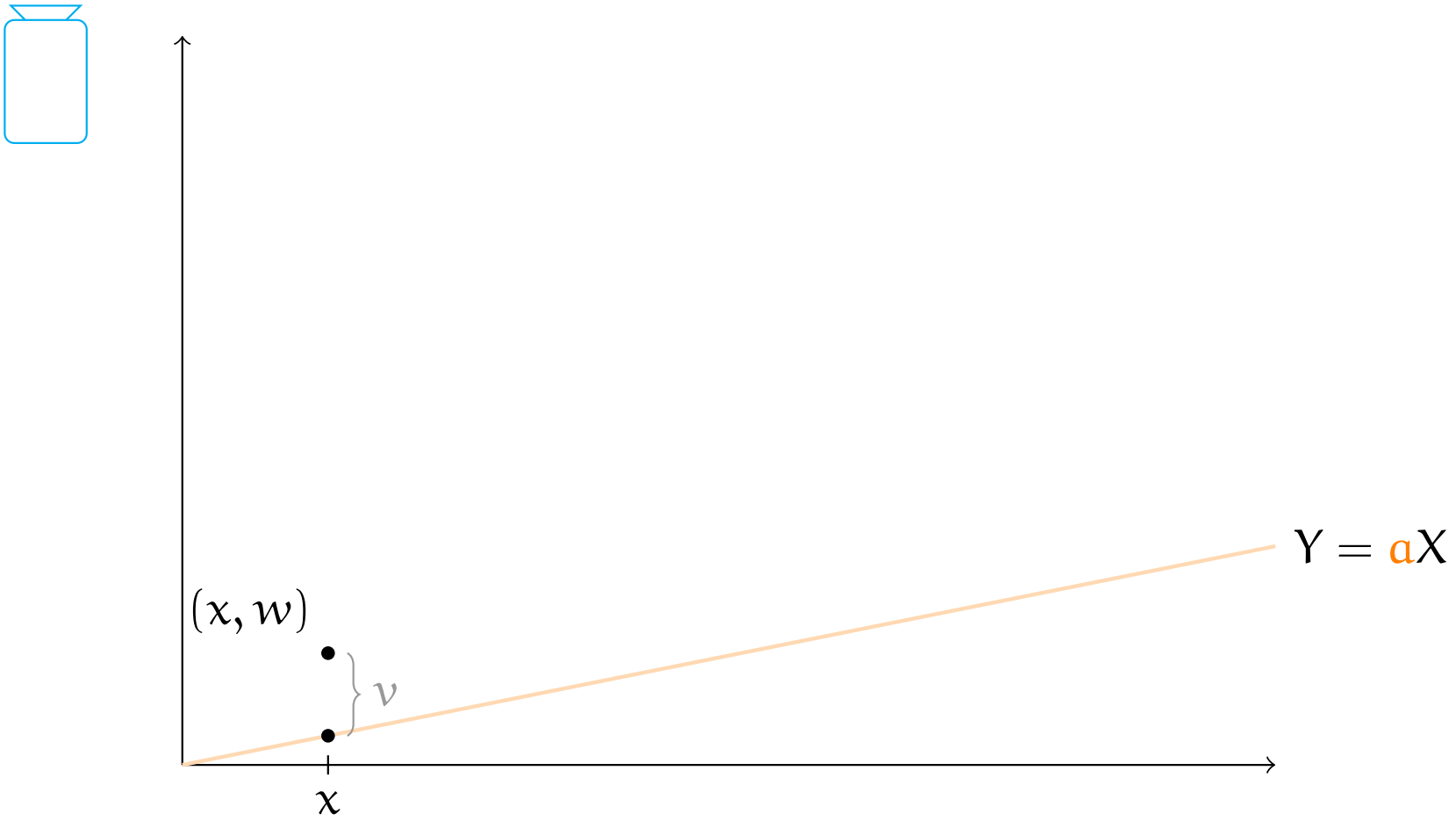
Overview

integrity — secrecy



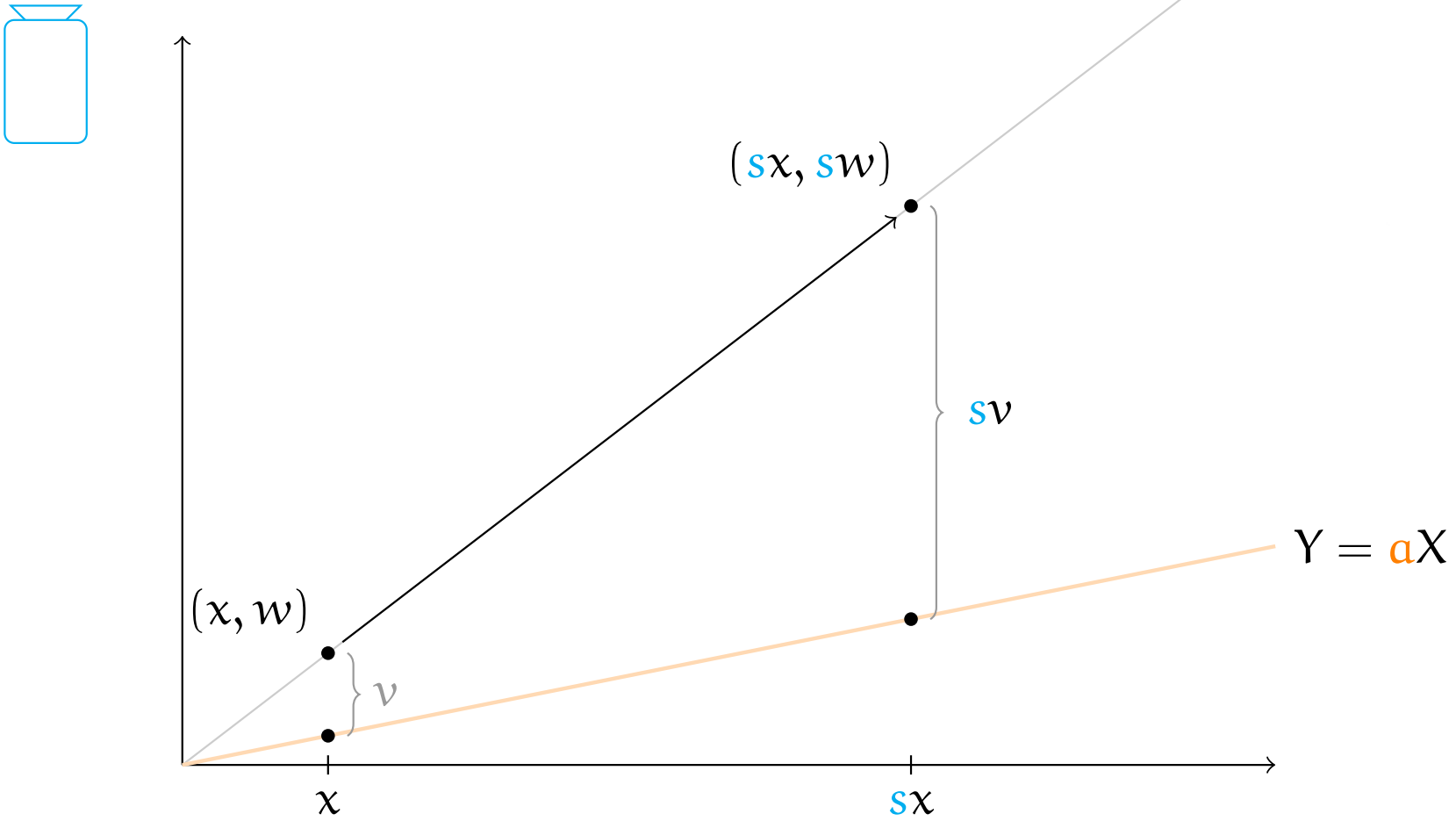
ballot box — return code generator — decryptor — auditor

Return Codes II

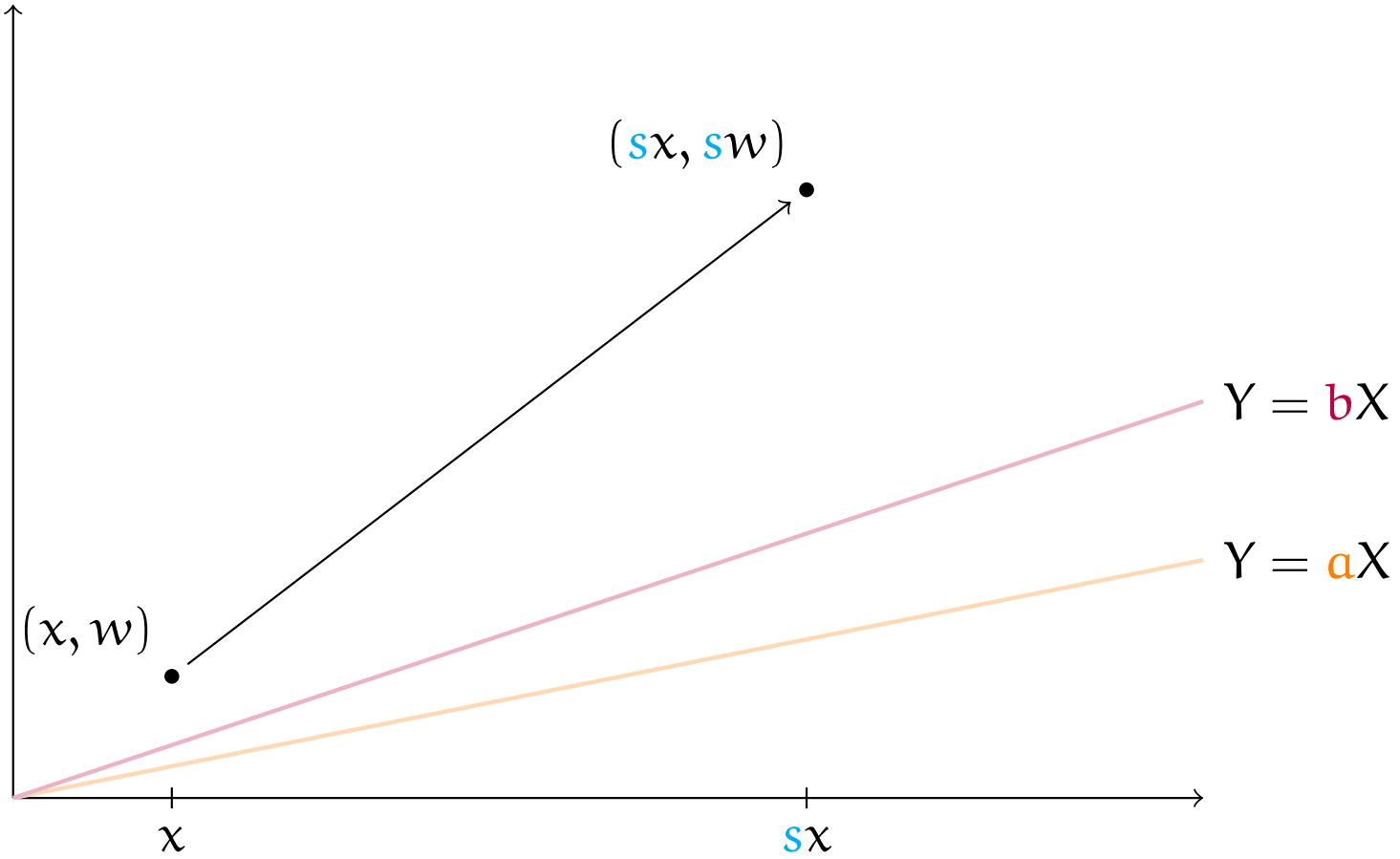


The ballot box has the ciphertext.

Return Codes II

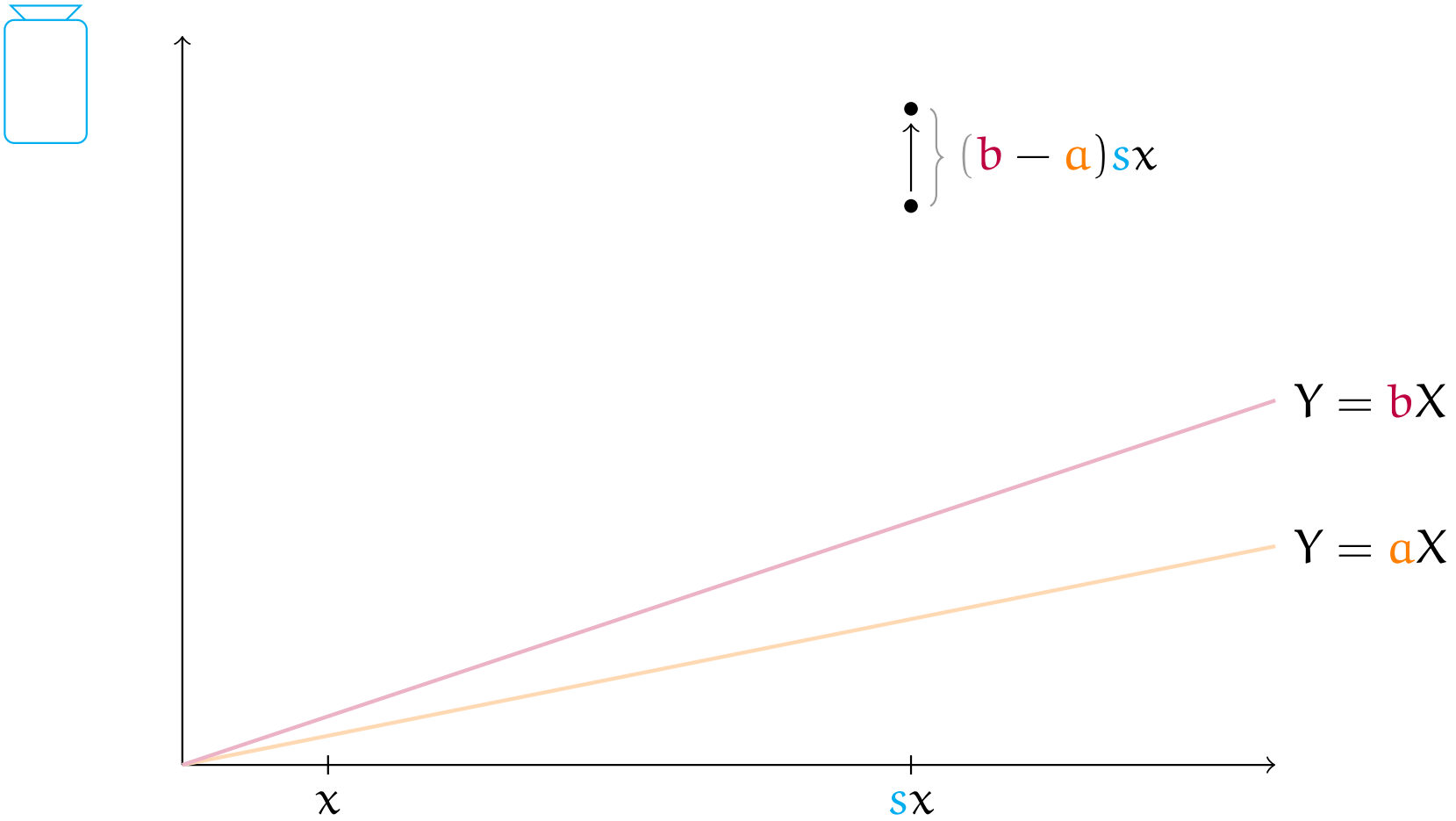


Return Codes II



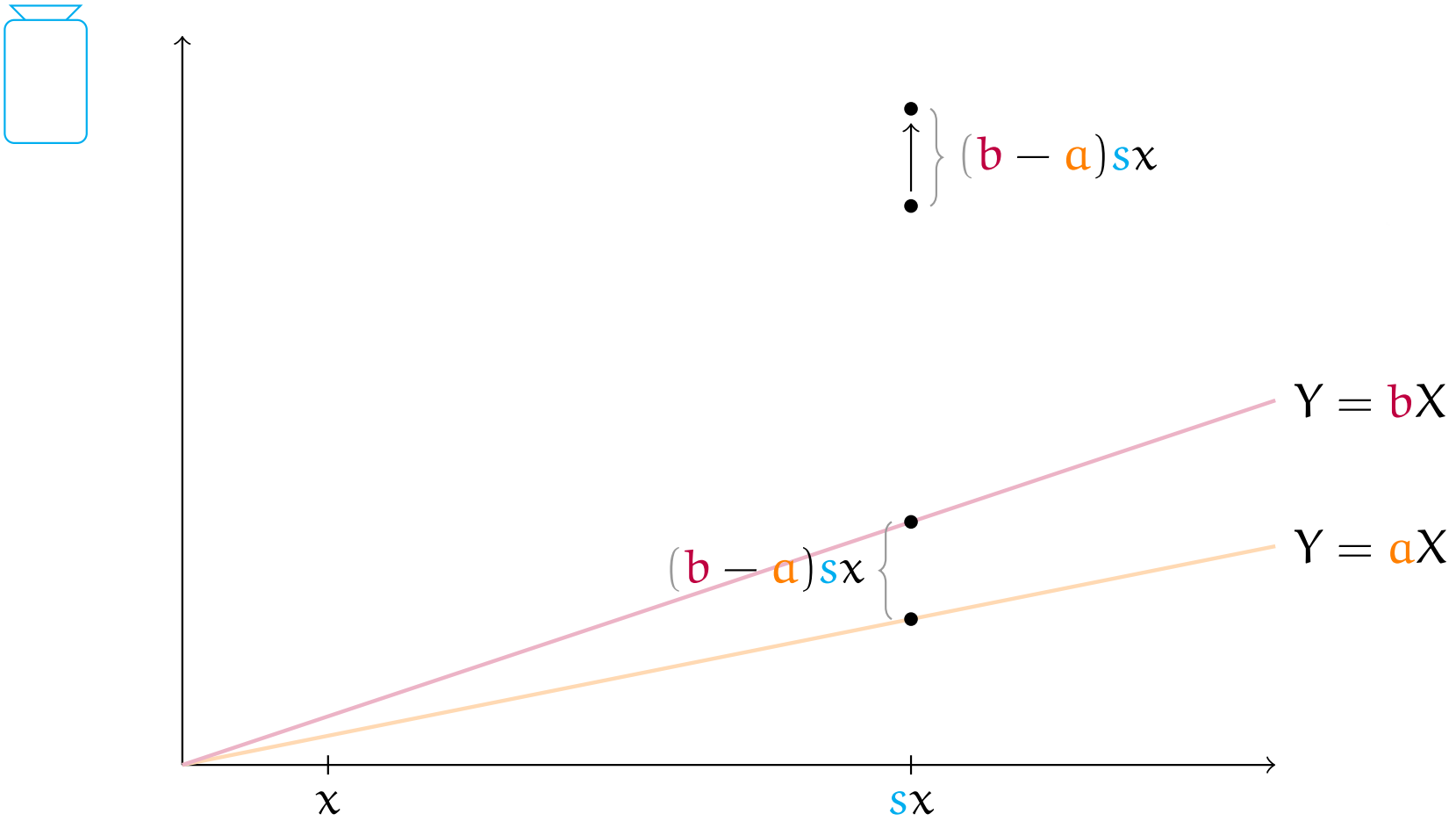
The return code generator has a line of its own.

Return Codes II

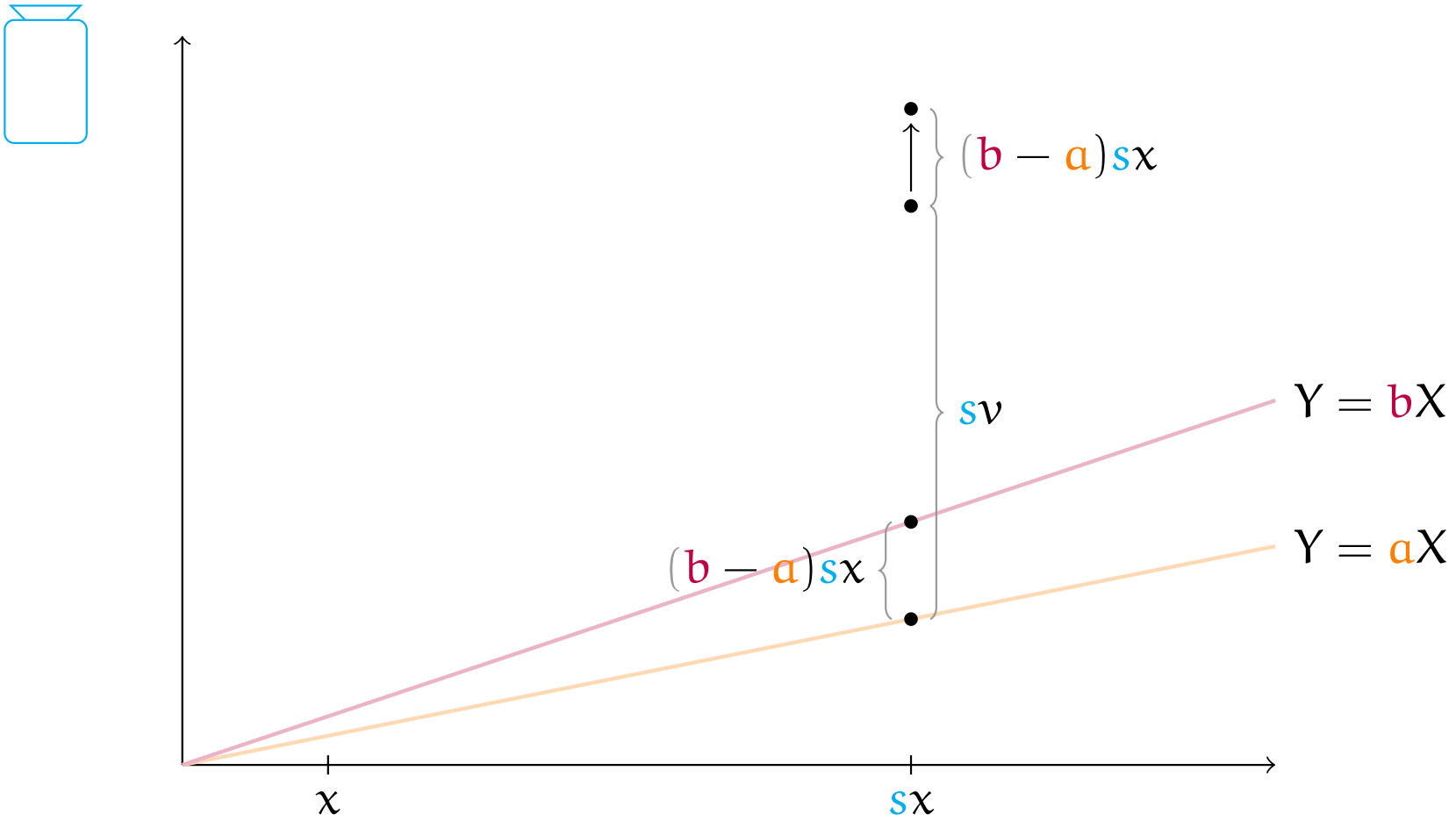


The ballot box has the difference between the two slopes.

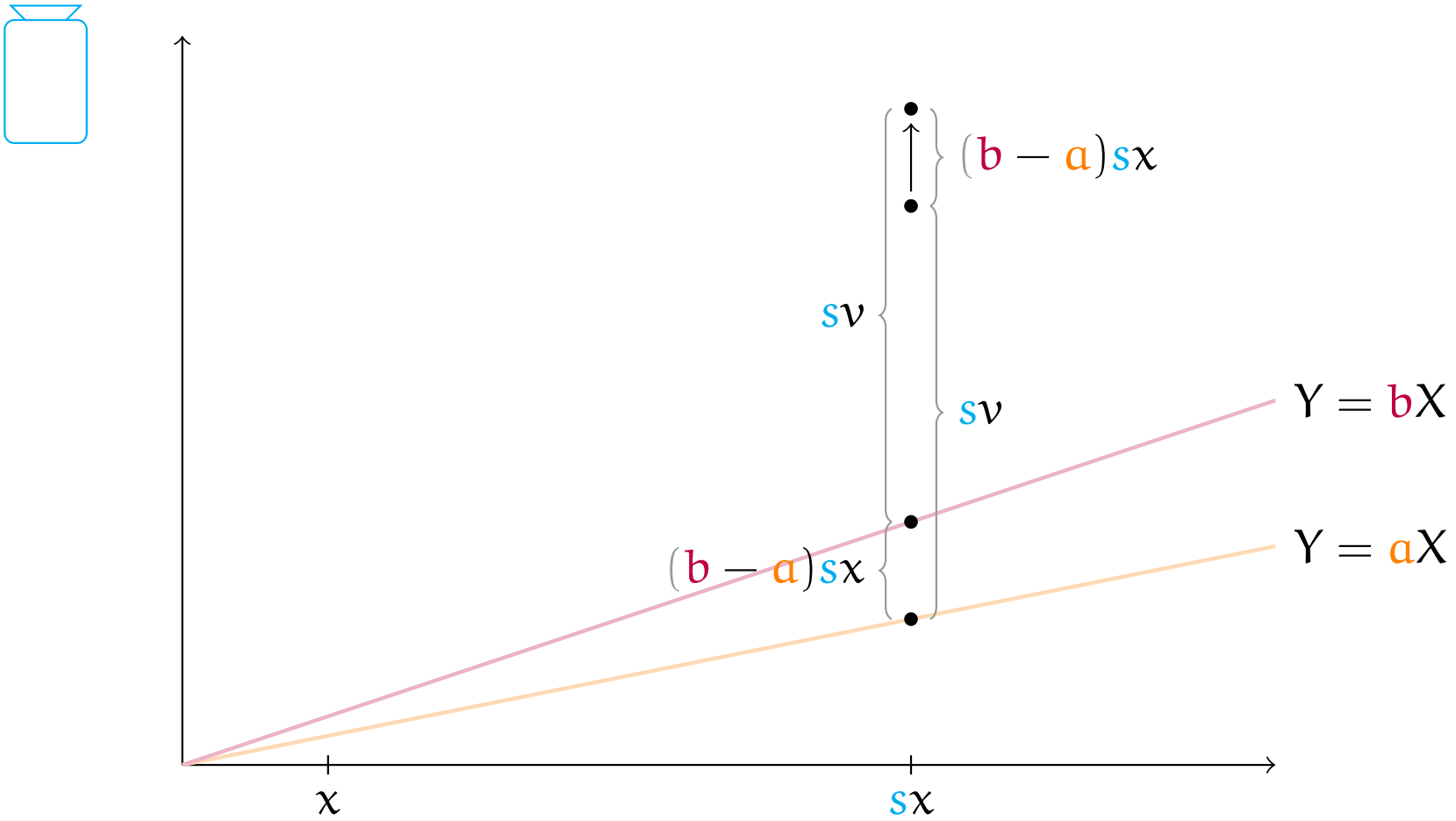
Return Codes II



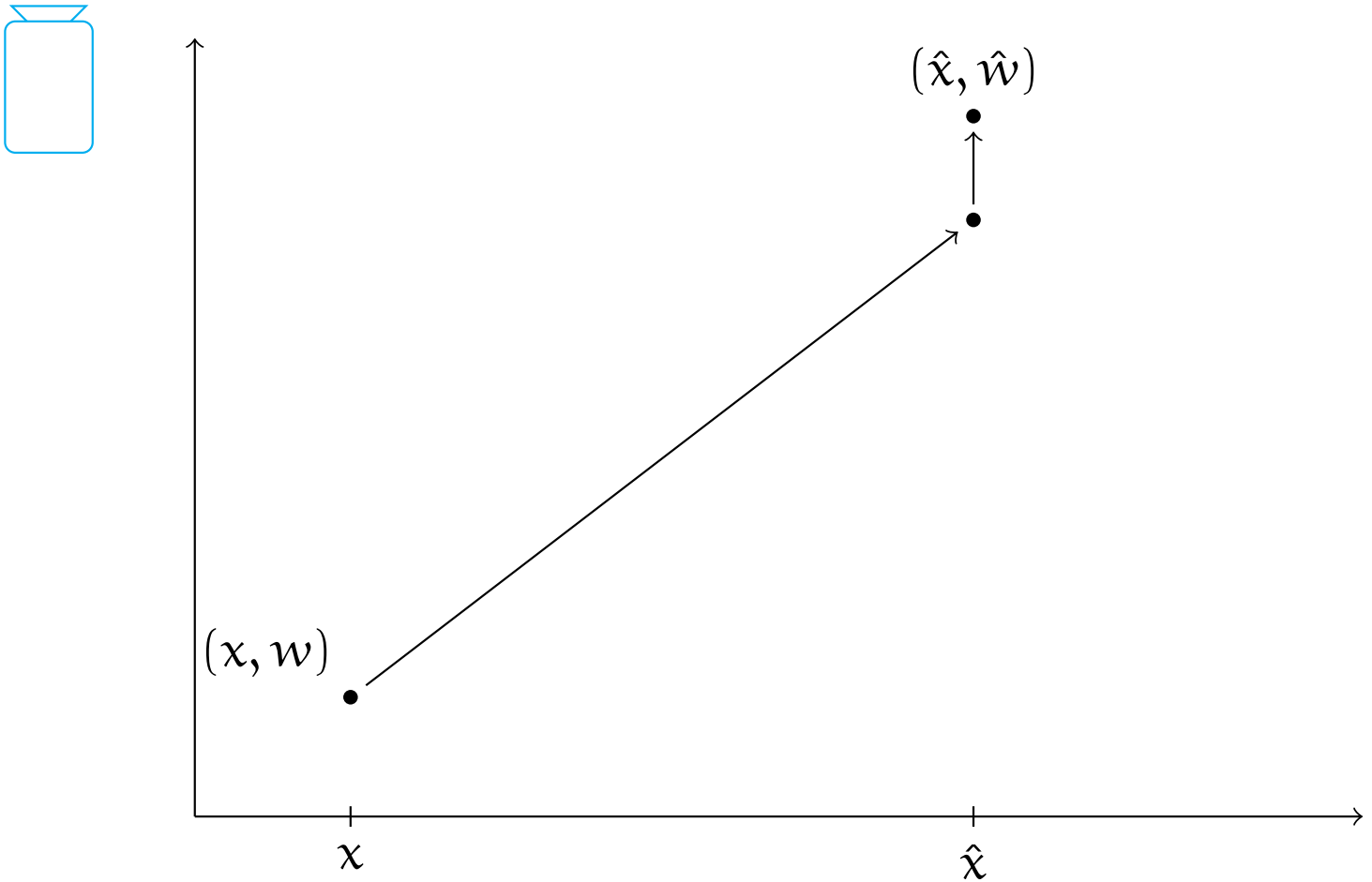
Return Codes II



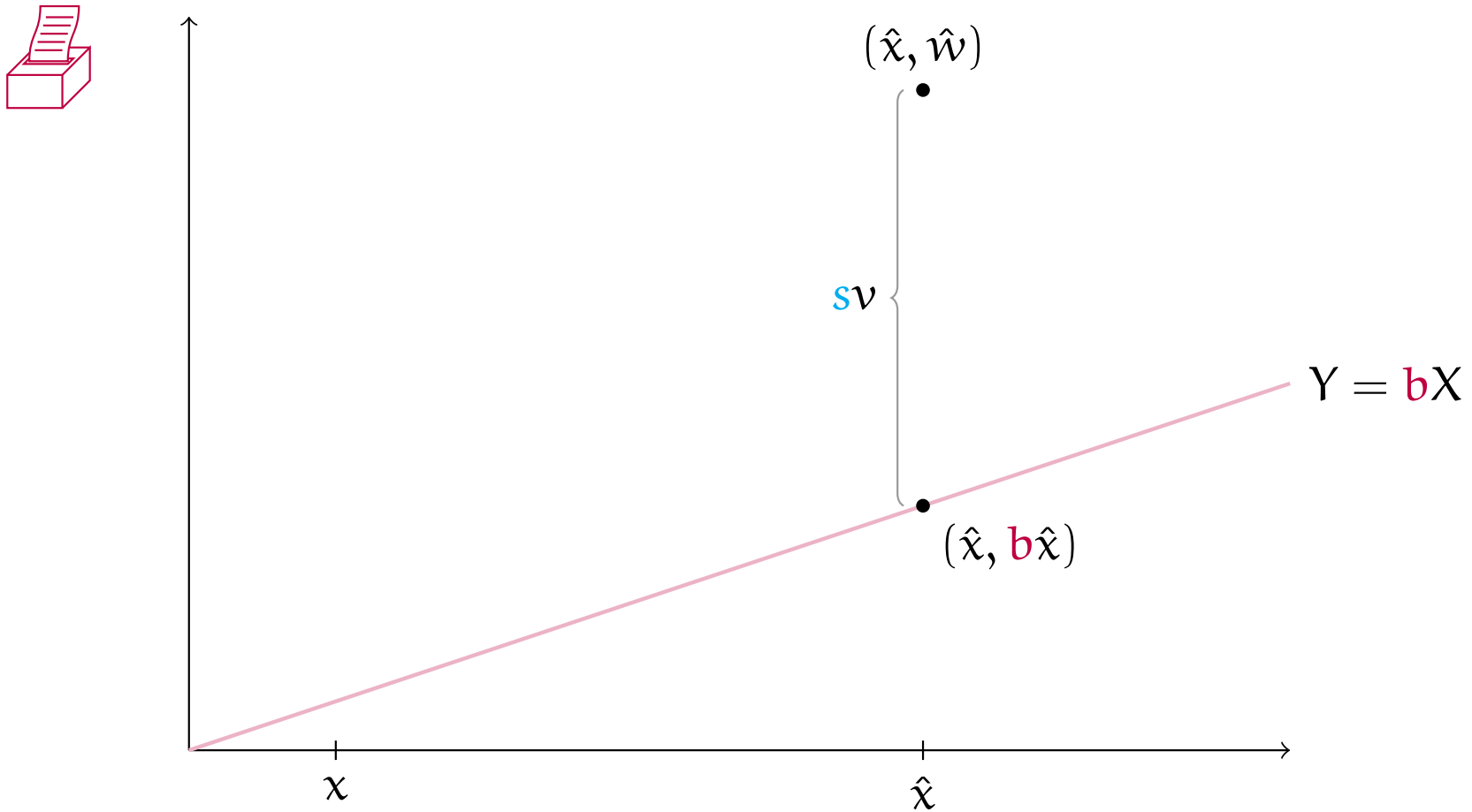
Return Codes II



Return Codes II

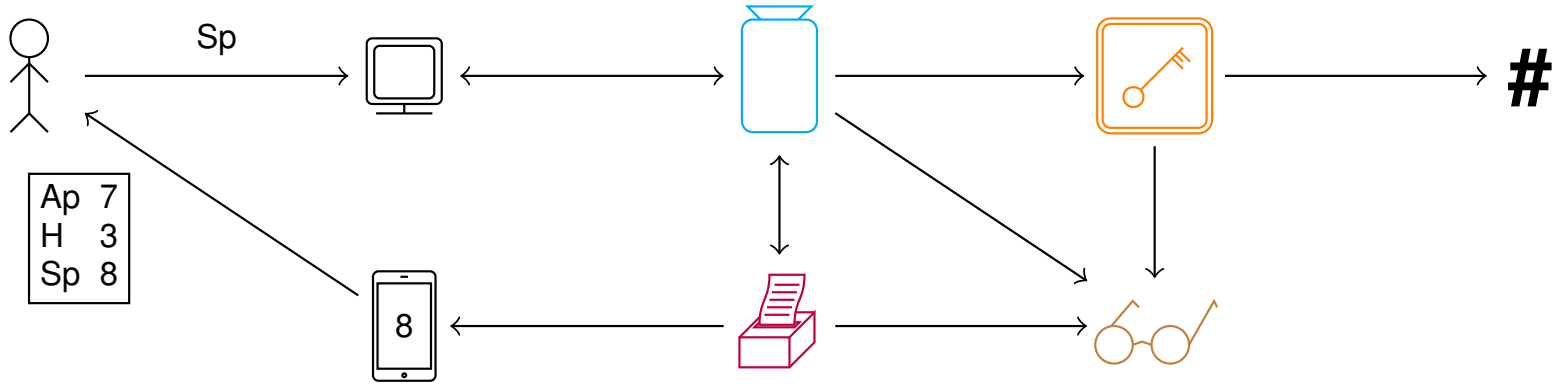


Return Codes II



Overview

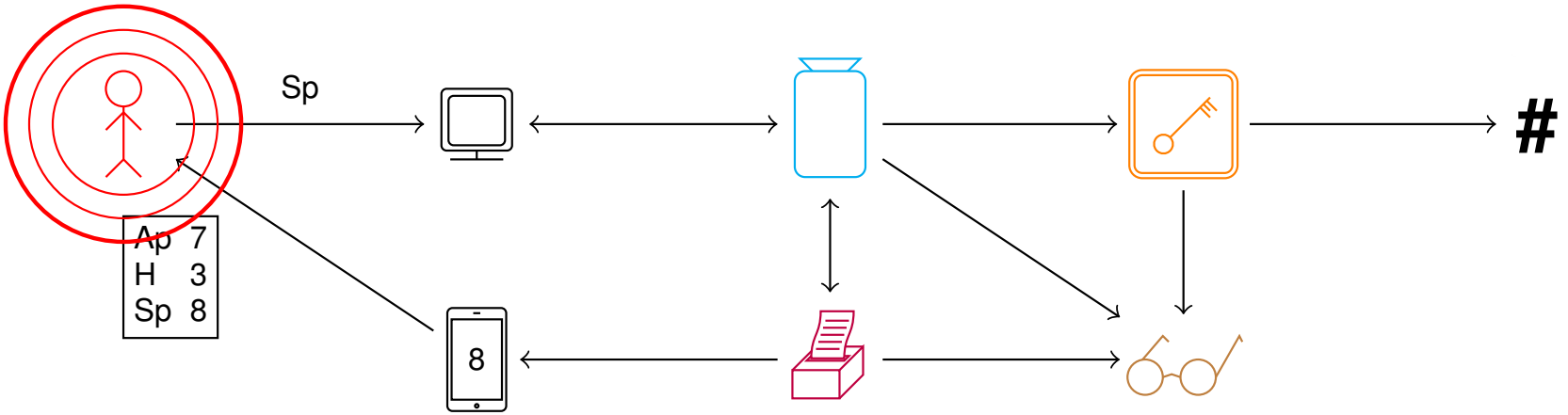
integrity — secrecy



ballot box — return code generator — decryptor — auditor

Overview

integrity — secrecy



ballot box — return code generator — decryptor — auditor