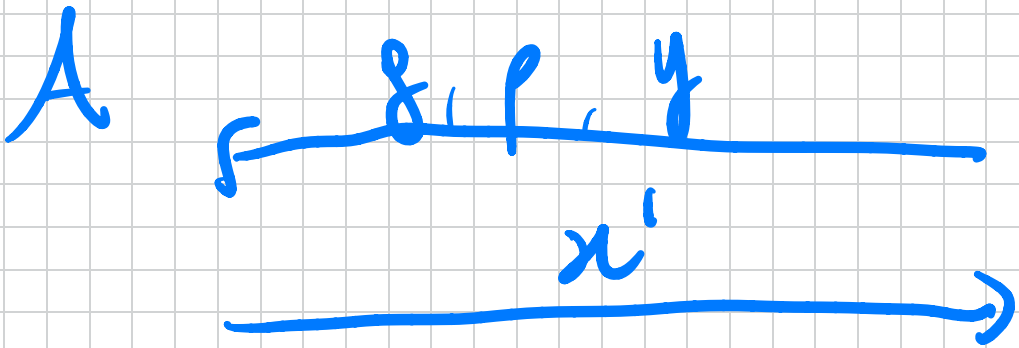
Very popular number-Theoretic assumption:

**DEF (DL Assumption).** Let $p$ be a prime. Then, the following holds $\forall$ PPT $A$:

$$\Pr\left[A(g, p, y) = x : x \leftarrow \mathbb{Z}_{p-1};\ y = g^x \bmod p\right] \leq \mathrm{negl}(\lambda).$$




$\mathcal{C}_{DL}$

$y = g^x \bmod p$

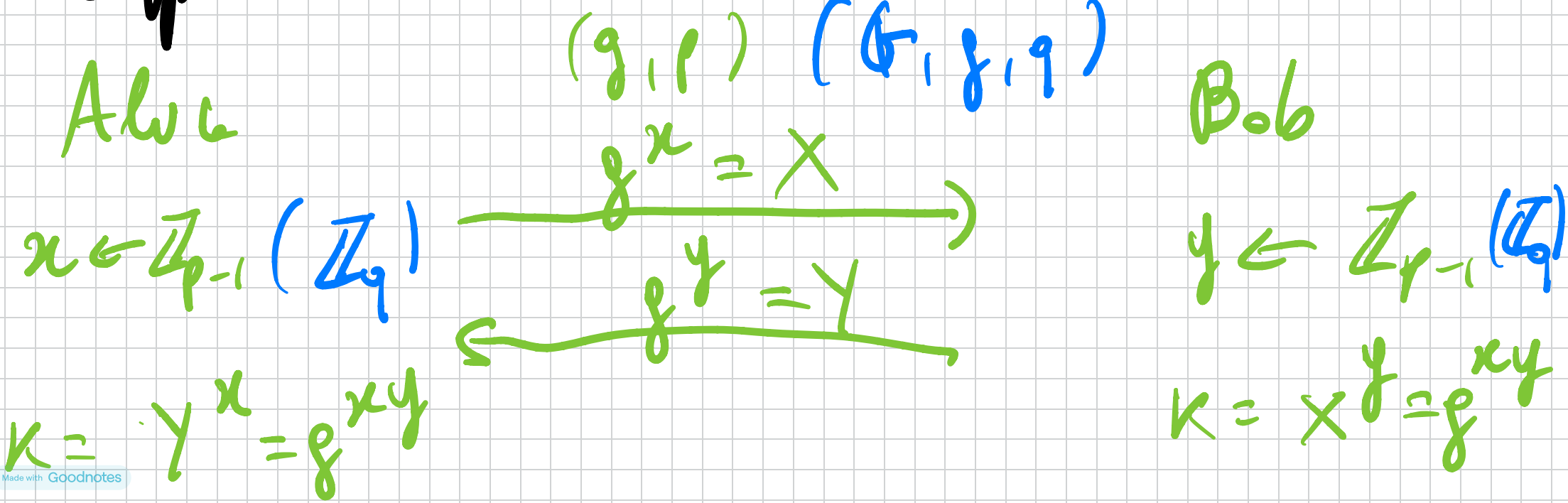
$x \leftarrow \mathbb{Z}_{p-1}$

WIN: $x' = x$.

Many attempts by mathematicians (for centuries). Trivial in exponential time (try all $x$'s). Many better algorithms: Pollard rho, Baby steps giant steps,

index calculus, .... The complexity of all these algorithms is still subexponential.

The public key revolution: Diffie and Hellman around 1976 proposed public-key crypto. Here is their idea:



$(g^y)^x$ $(g^x)^y$

Minimal requirement for this protocol:
The DL assumption should hold.
Two kinds of attackers:

- Passive: Eavesdrop the communication without changing it.
- Active: Can change protocol messages. (Men-in-the-middle).

Security:

- Hardness of computing $K$
- Or better, The key is indistinguishable from uniformly random.

Let's start with passive security. We make a generalization: instead of running the protocol on $(\mathbb{Z}_p^*, \cdot)$ we now use $(G, \cdot)$ where $G$ is a cyclic

group with generator $g \in G$ and order $q$ (i.e. $g^q = 1$ in $G$).

It is unknown if the key of the DH protocol is hard to compute for passive attackers under the DL assumption.

This motivates:

**DEF (CDH).** The CDH assumption holds if $\forall$ PPT $A$:

$$\Pr[A(\text{params}, g^x, g^y) = g^{xy} : x, y \leftarrow \mathbb{Z}_q]$$

$\leq \text{negl}(\lambda)$.

$$\text{params} = (\mathbb{G}, g, q)$$

Note: CDH $\Rightarrow$ DL. If one can solve DL it can also solve CDH.

But we don't know if DL $\Rightarrow$ CDH.

The CDH assumption is believed to hold in $\mathbb{G} = \mathbb{Z}_p^*$.

If the goal is to obtain a key that is indistinguishable from uniform, we need:

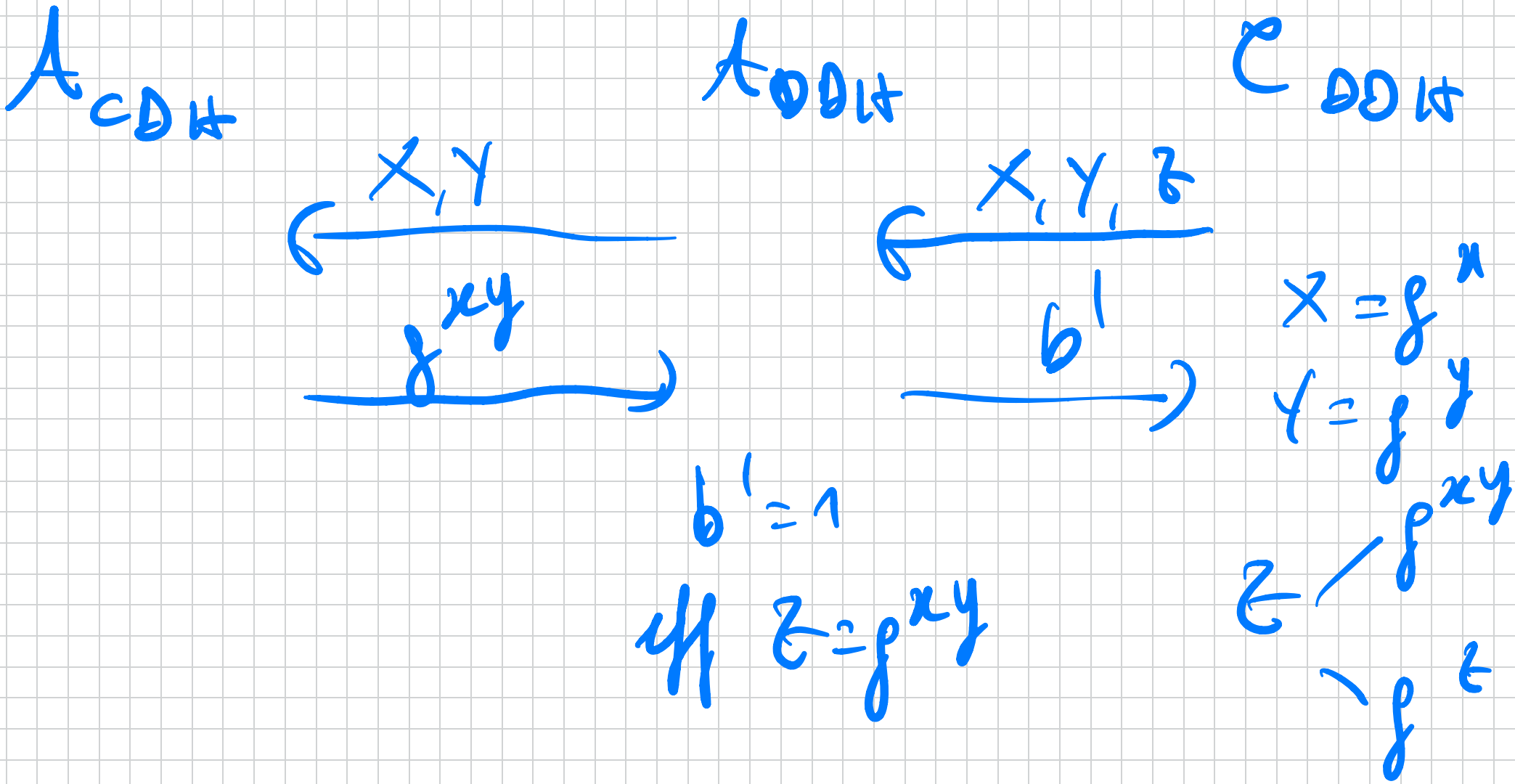
**DEF (DDH assumption).** The DDH assumption holds if:

$$(G, g, q, g^x, g^y, g^{xy}) \overset{c}{\approx} (G, g, q, g^x, g^y, g^z)$$

$$x, y, z \leftarrow \mathbb{Z}_q.$$

$\Rightarrow$ The DH protocol is secure against passive attackers.

As before: DDH $\Rightarrow$ CDH.




However, CDH $\not\Rightarrow$ DDH in general.

Namely, $\exists\ G$ s.t. CDH is believed to hold in $G$, but DDH does not. For instance $G = \mathbb{Z}_p^*$. So we will need a different $G$.

**FACT** DDH does not hold in $\mathbb{Z}_p^*$.

Proof. Consider:

$$QR_p = \{ y : y = x^2 \text{ for } x \in G \}$$

$$= \{ y : y = g^z \text{ for even } z \}$$

On the one hand, we can test if $y \in \mathbb{Q}/R_p$ by checking

$$y^{(p-1)/2} \equiv 1 \mod p.$$

Indeed, if $y = g^{2z'}$ then

$$y^{(p-1)/2} = \left(g^{2z'}\right)^{(p-1)/2}$$

$$= \left(g^{p-1}\right)^{z'} \equiv 1 \mod p$$

Else, $y = g^{2s'+1}$ mod $p$

$$y^{(p-1)/2} = \left(g^{2s'+1}\right)^{(p-1)/2}$$

$$= g^{(p-1)/2} \cdot \underbrace{\left(g^{(p-1)}\right)^{s'}}_{1}$$

$$= g^{(p-1)/2} \neq 1 \bmod p$$

This gives a distinguisher:

- If $Z = g^z$, then $Z$ is a square w.p. $1/2$.
- If $Z = g^{xy}$, then $Z$ is a square w.p. $3/4$ (either $g^x$ is a square or $g^y$ is a square or both).

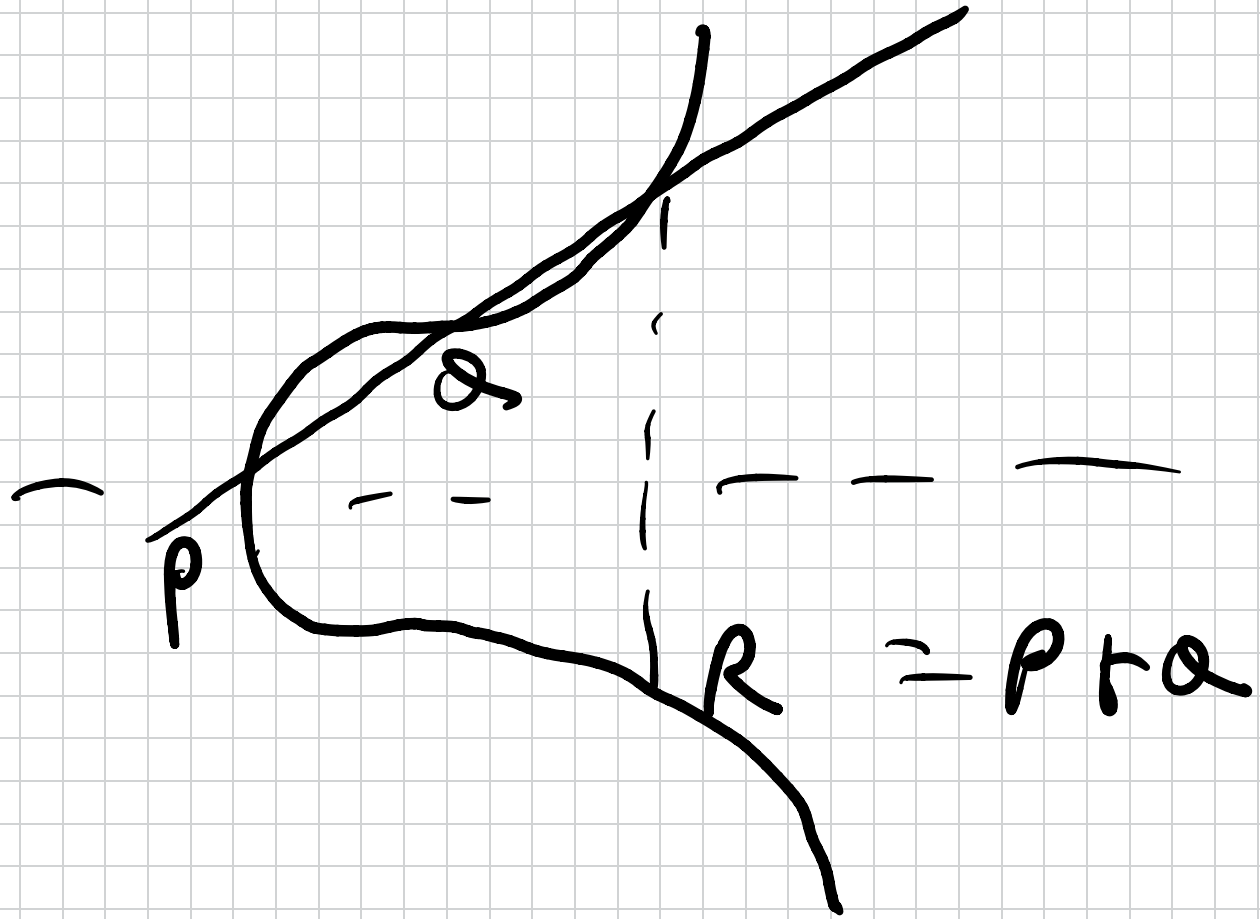
$\Rightarrow$ Can break DDH w.p. $3/4 - 1/2 = 1/4$.

Luckily, there are many $G$'s where DDH is believed to hold:

- Easiest ex: Let $G = \mathbb{Q}R_p$ where $p = 2q+1$, $p, q$ primes. This is cyclic, with order $\frac{p-1}{2} = q$.

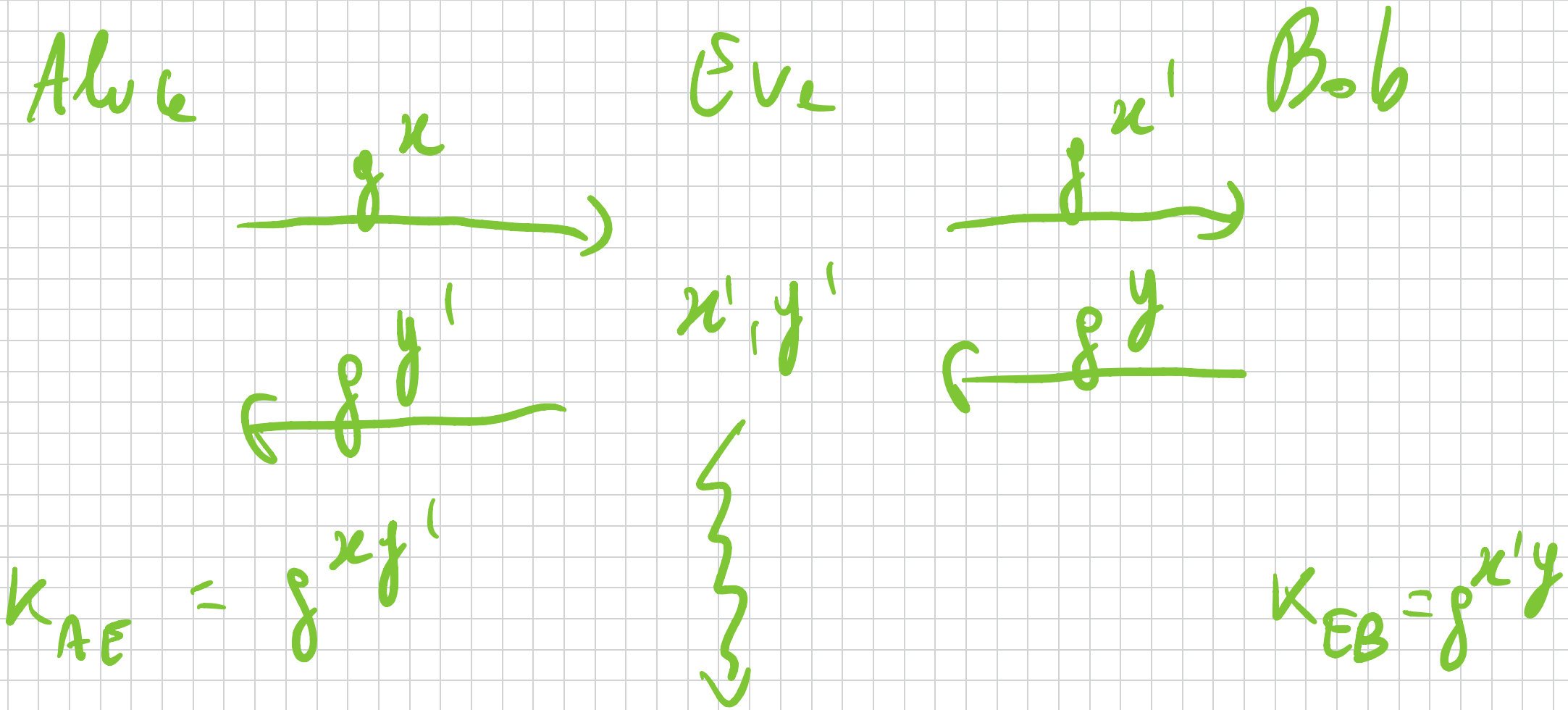
- Elliptic curve groups. These are groups defined by the points of an elliptic curve $Y = X^3 + aX^2 + bX + c$

modulo $e$ primo.

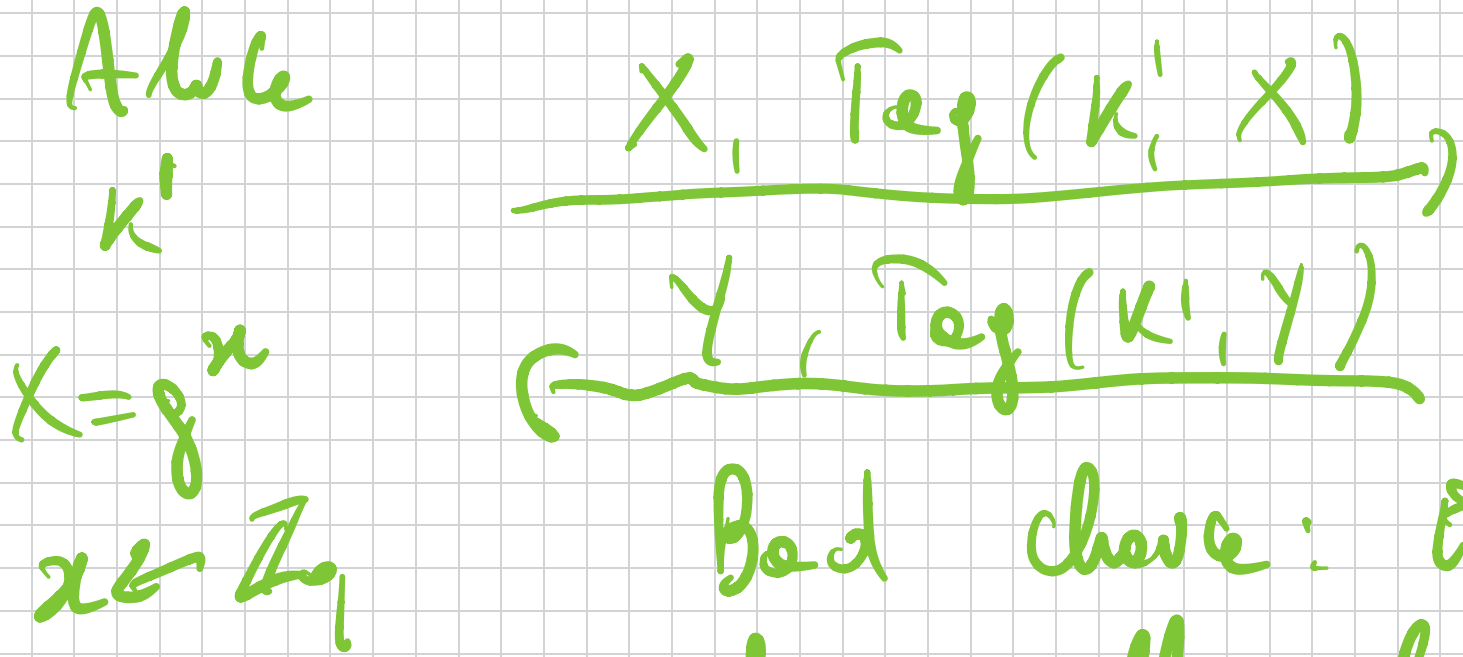



$G = E(\mathbb{Z}_p)$ , "+"

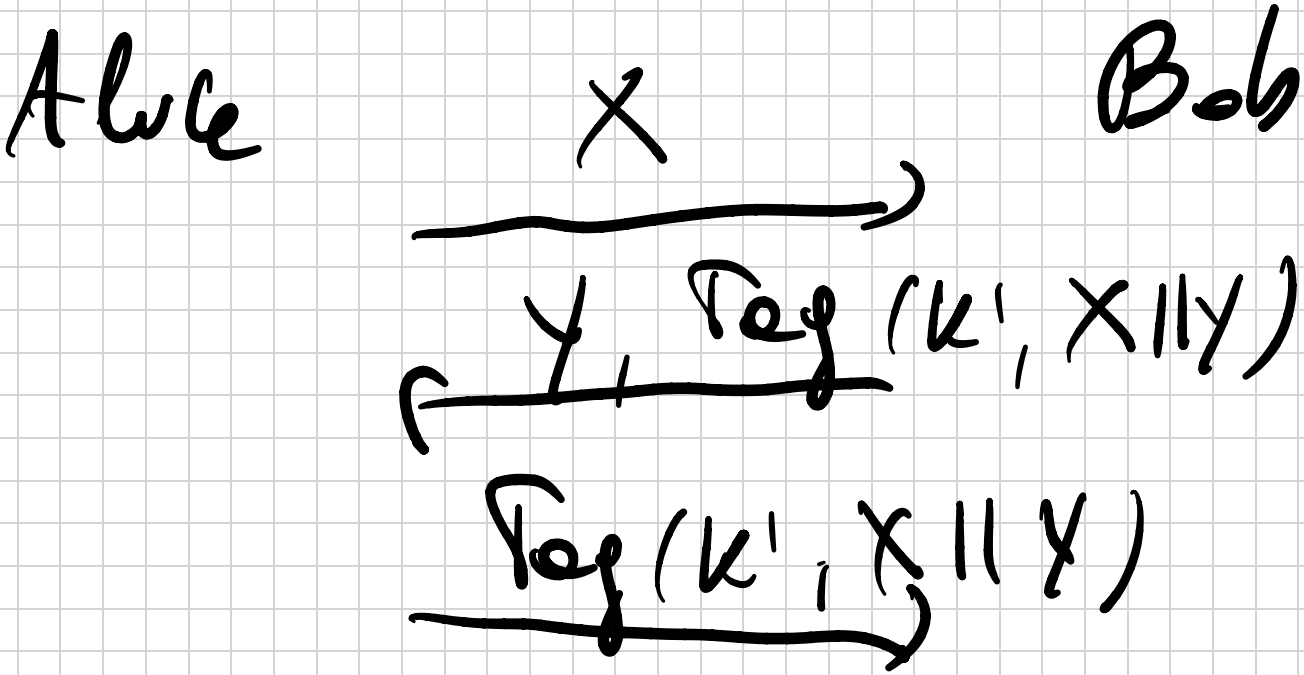
# What about active security?



Bottom line: We need MASTER KEYS to authenticate communication using either MACs or DIGITAL SIGNATURES (we will study this later).



A better protocol:



Let's show that DDH easily implies what we studied so far:

PRGs

$$(G, g, q) = \text{params}.$$

$$x, y \leftarrow \mathbb{Z}_q$$

$$G_{\text{params}}(x, y) = G(x, y)$$

$$= (g^x, g^y, g^{xy})$$

$$G : \mathbb{Z}_q^2 \to \mathbb{G}^3$$

so it has pseudo sketch. Also:

$$(g^x, g^y, g^{xy}) \approx_c (g^x, g^y, g^z)$$

$\hookrightarrow$ UNIFORM over $\mathbb{G}^3$.

We can also improve the sketch:

$$G(x, y_1, \dots, y_t) = (g^x, g^{y_1}, g^{xy_1}, \dots$$

$$x, y_i \in \mathbb{Z}_q \qquad \dots, g^{y_t}, g^{xy_t})$$

$$G : \mathbb{Z}_q^{t+1} \to G^{2t+1}$$

**Exercise** : This is PRF under DDH.

PRFs. Apply GGM with a particular PRG. We get:

$$\mathcal{F} = \left\{ F_{\vec{a}} : \{0,1\}^n \to G \right\}_{\vec{a} \in \mathbb{Z}_q^{n+1}}$$

$$F_{\vec{a}}(x_1, \ldots, x_n) = \left( g^{a_0} \right)^{\prod_{i=1}^{n} a_i^{x_i}}$$

The above is GRM with following PRG:

$$G_a(g^b) = (g^b, g^{ab})$$

$$= G_0(g^b) \| G_1(g^b)$$