11/7/2025: Tree Based Group Diffie-Hellman

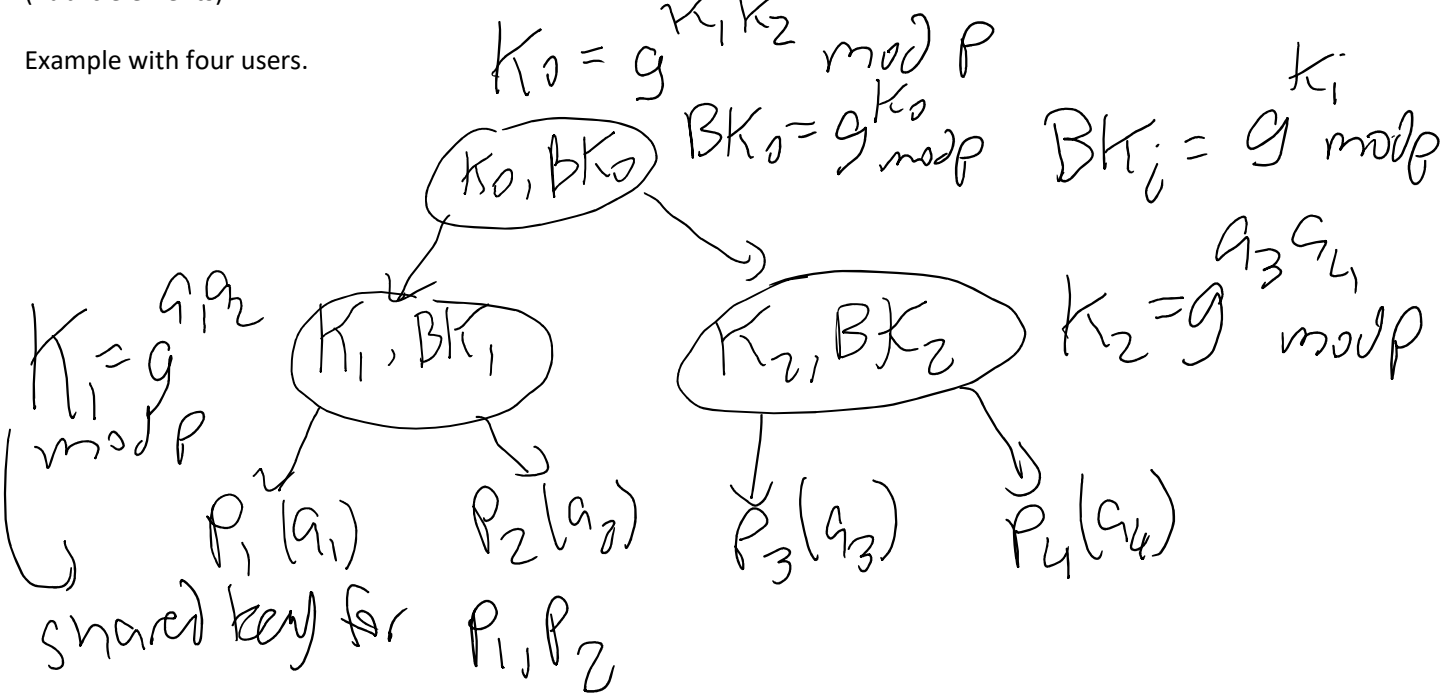
Thursday, October 30, 2025 8:13 PM

Key Management: You might have different groups, and want each group to have a shared key.

Example with four users and sharing keys via key exchange, essentially using Diffie-Hellman.

Whole company/Big Group picks a public prime number p and a generator, g. (Public elements)

Example with four users.

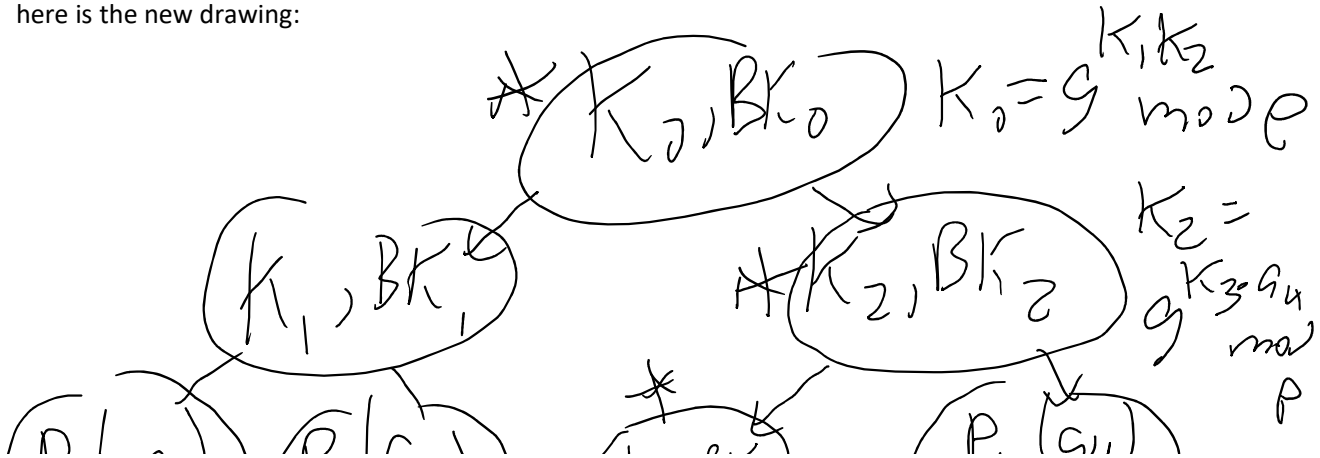


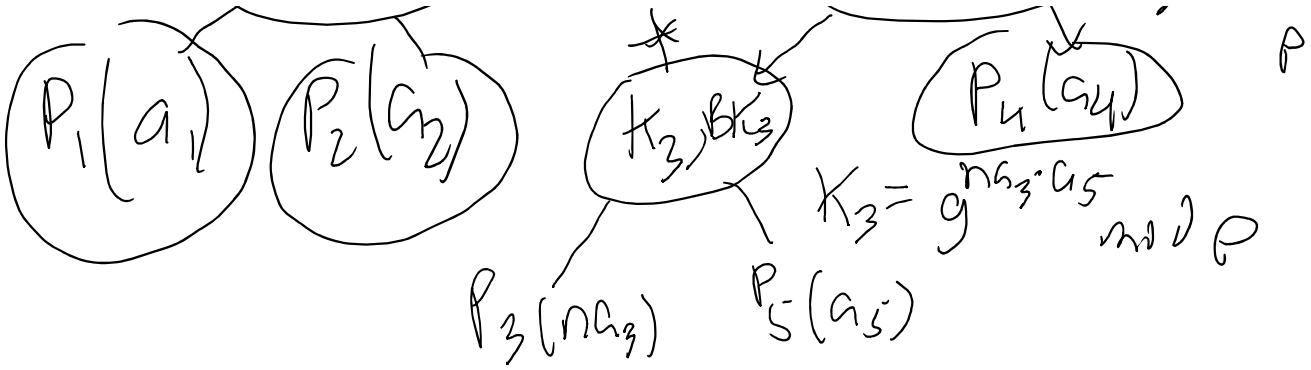
Not allowing for arbitrary groups, the groups have to fit in this sort of tree structure.

How do we add a user?

Let's say that we have a new person P5 and their sponsor is P3 (all people are at leaf nodes so basically when we add someone, we will change a leaf node into an internal node and have both the new person and the sponsor as children of that new internal node.

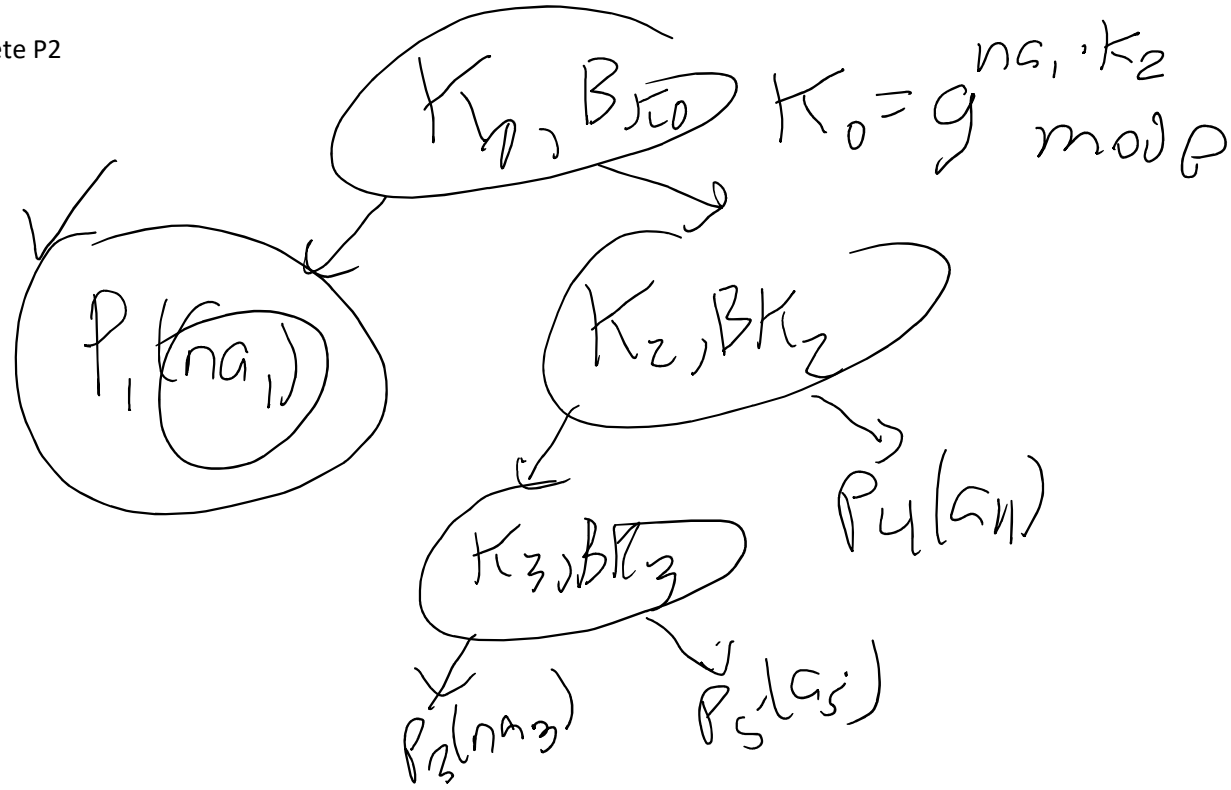
To do this P3 picks a new secret key na3, P5 picks their secret key a5, here is the new drawing:





Delete: Pretty similar to insert. Any node can be deleted fairly easily since all people are leaf nodes.

Let's delete P2



Sample

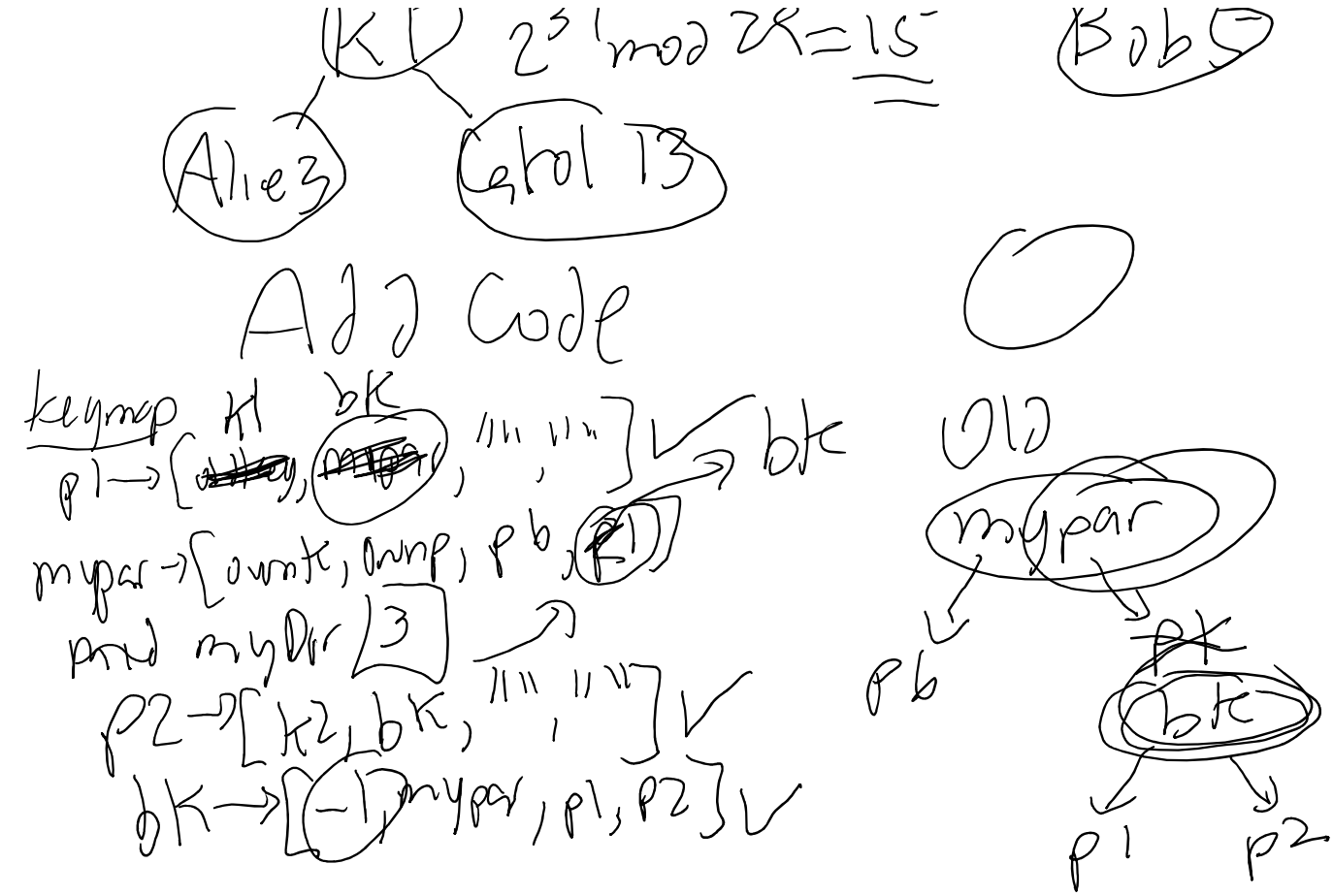
$K0 = 2^{35} = 12 \bmod 29$

Alice 7 Bob 5

next

$K0 = 3^{15 \times 5} = 3^{75} \bmod 29 = 18$

KD $2^{39} \bmod 29 = 15$ Bob 5


KE
Alice
Carol
Bob
Adj Code
keymap
p1
bk
mypar
pb
p2
OLD