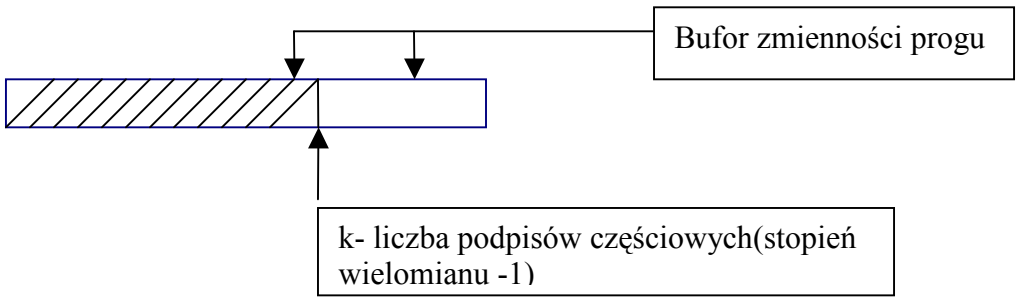
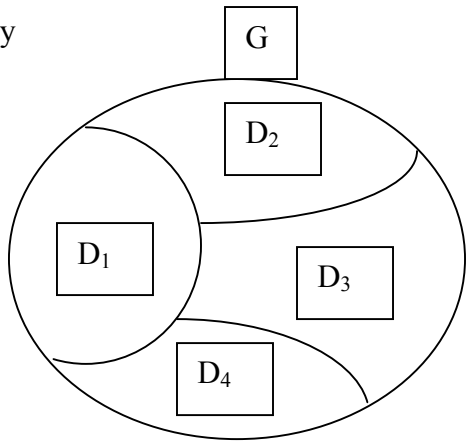
7. Schematy hierarchiczne w grupie Diffie-Hellmana z LUKĄ

Bardziej elastyczna wersja podpisów grupowych (np. zmiana progu)

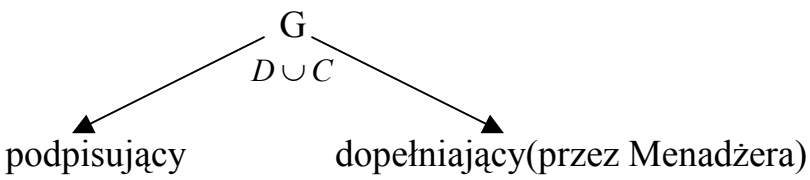


D_i -różne działy



M- zarządza(menadżer kontroluje uzupełnienie podpisów częściowych)

Próg ustalony przez stopień wielomianu, przy zmianie progu wielomian się nie zmienia,ale trzeba go „dopełniać”.



Def.

G nazywamy grupą Diffie-Hellmana z luką, gdy:

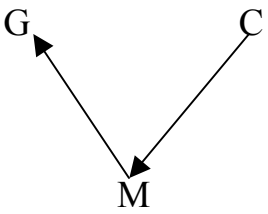
1)Problem obliczeniowy jest trudny w grupie CDH
2)problem decyzyjny D-H jest łatwy w grupie DDH

ad. 1)Dla danych (P, aP, bP) oblicz abp
ad. 2)Dla danej (P, aP, Bp, cP) rozstrzygnij czy c= ab(mod |G|)

Przykład:

Przykładem takiej grupy jest struktura dwuliniowa (G_1, G_2, E_1P), e: $G_1 \rightarrow G_2$ jest iloczynem Weil'a
Wystarczy zauważyć ,że jeśli e(P, cP)=e(aP, bP) to (P, aP, Bp, cP) jest czwórką Diffie-Hellmana

Model komunikacyjny



2 kanały połączeń: poufny i rozgłaszania

Zakładamy, że przeciwnik może „korumpować" t- członków grupy Ct- poziom korupcji

Protokół podpisu(ze zmiennym progiem)

1) generacja kluczy i dzielenie sekretu
2) decyzja Menadżera
3) Podpisywanie:
   a)Członkowie G obliczają podopisy
   b)Delegowany członek G 'skleja' podpisy
4)Weryfikacja