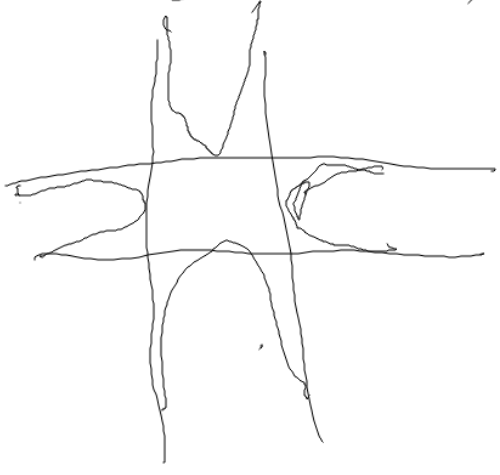
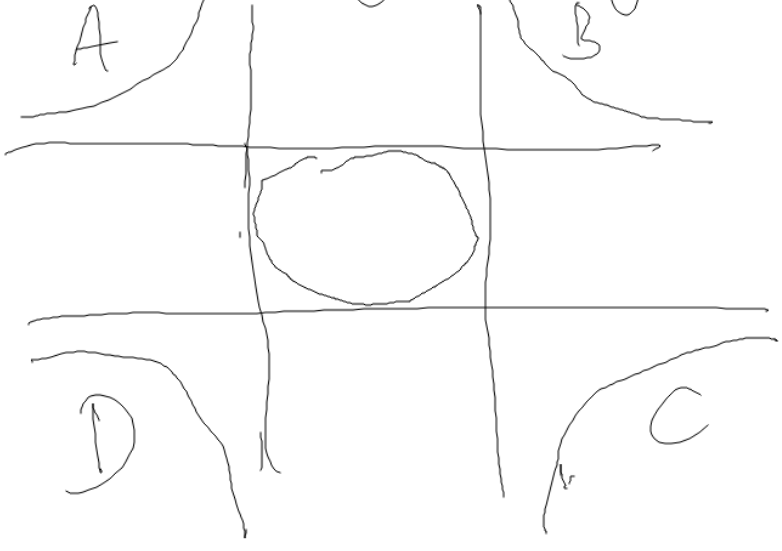
$x^2 + y^2 = 1 + dx^2y^2$

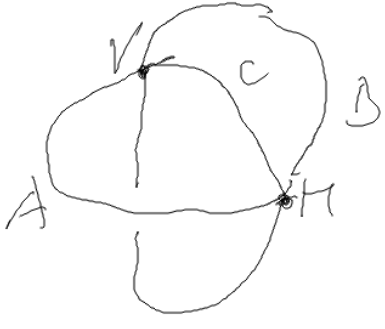
$(1-x^2)(1-y^2) + (d-1)x^2y^2 = 0$

Pokud pracujeme nad $\mathbb{R}$ a $d > 1$, tak nemáme
oba $(1-x^2)$ a $(1-y^2)$ současně kladné

$0 < d < 1$, Tedy $x^2 - 1$ $y^2 = 1$ hyperbola



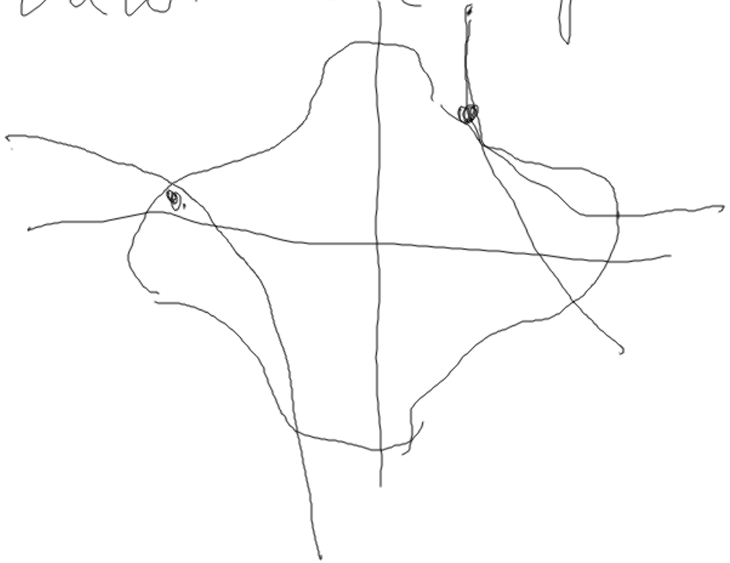




WK — na ní má sčítání geometrický význam. Na přímce leží body, jejichž součet je nula

Na Edw. křivce stejnou roli mají body

$$y = \frac{1 - qx}{1 + px}$$



Základy kryptografie založené na párování

Motivace — Bilineární zobrazení

Ať $(G,+)$ a $(H,\cdot)$ komutativní grupy

$f(a+b,c) = f(a,c)\,f(b,c)$ $\quad a,b \in G \quad f: G\times G \to H$

$f(c,a+b) = f(c,a)\,f(c,b)$

je symetrické $\iff$ $\forall a,b \quad f(a,b) = f(b,a)$ — Gelichart ⇓ symetrické

Pozorování: $\forall n,m \in \mathbb{Z}$ je

$f(na,mb) = f(a,b)^{nm}$ tedy $f(ng,mg) = f(g,g)^{nm}$

Pokud G je cyklická s generátorem g, $= f(mg,ng)$

Definujme $f_a : G \to H$ tak, že $f_a(b) = f(a,b)$

Potom je f_a homomorfismus $G \to H$, neboť

$$f_a(b+c) = f(a,b)f(a,c) = f_a(b)f_a(c)$$

$Hom(G,H) \leftarrow$ grupa všech homomorfismů $G \to H$

$f_a f_b = f_{a+b}$

Je to grupa s operací $g_1, g_2 \in Hom(G,H)$, tak

$$g_1 g_2 : a \mapsto g_1(a) g_2(a)$$

$$g_1g_2(b+c) = g_1(b+c)\,g_2(b+c) = g_1(b)g_1(c)g_2(b)g_2(c) = g_1(b)g_2(b)g_1(c)g_2(c) = g_1g_2(b)\,g_1g_2(c)$$

(Přeformulace biaditivity)

$a \mapsto f_a$ je homomorfismus z G do $Hom(G,H)$

Biaditivní zobrazení je nedegenerované (zleva)

pokud $a \mapsto f_a$ je injektivní homomorfismus grup.

$$\forall a \neq 0 \quad \exists b, \text{ že } f(a,b) \neq 1$$

$$\forall a \neq 0 \quad \exists b, \text{ že } f(b,a) \neq 1$$

nedegenerovanost.

$$f(0,b) = 1 = f(b,0)$$

$$f(0+0,b) = f(0,b) \cdot f(0,b)$$

$$\| \quad f(0,b) \Rightarrow f(0,b) = 1$$

Kolega podrobněji prozkoumá předpoklady vlastnosti f v aplikacích když je třeba, že

předpoklad $f(a,b) = 1 \Rightarrow a = 0$ nebo $b \neq 0$

jde o to, že f_a je vždy bijekce — izomorfismus

$G = \mathbb{Z}_4$ $\quad H = \{-1, 1\}$

$f(a,b) = (-1)^{ab}$ ← biaditivní

$f(2a,b) = 1$ ačkoliv

To co potřebujeme, je $|G| = n$ prvočíslo

a pak $f(P,P) \neq 1 \iff$ nedegenerovanost

Dále budeme předpokládat, že G je cyklická grupa prvočíselného řádu.

Řešit DLP v G znamená ze znalosti
$[n]P$ určit n

v H znamená ze znalosti
2^n určit n

Až G je generována prvkem P
Až H je generována prvkem $f(P,P) = 2$
Pokud řešení DLP v H dává
řešení DLP v G

Proč: Až umím DLP v H
Znám $Q = [n]P$
Spočítám $f(Q,P) = 2^n$
2 DLP v H odvodím n

Dále budeme předpokládat, že G je cyklická grupa prvočíselného řádu.

Řešit DLP v G znamená ze znalosti
$[n]P$ určit n

v H znamená ze znalosti
2^n určit n

Až G je generována prvkem P
Až H je generována prvkem $f(P,P) = 2$
Pokud řešení DLP v H dává
řešení DLP v G

Proč: Až umím DLP v H
Znám $Q = [n]P$
Spočítám $f(Q,P) = 2^n$
2 DLP v H odvodím n

Bilineární

Ve dvojici když $|G| = n = |H|$ prvočíslo tak vlastně pracuji nad tělesem $\mathbb{Z}_n$

Platí $f(\lambda a, b) = \lambda f(a, b)$ pro všechna $a, b \in G$, $\lambda \in \mathbb{Z}_n$

UMĚT DHP v H STAČÍ $\mathbb{Z}, 2^x, 2^y \to 2^{xy}$

Bilineární Diffie-Hellmanův problém nad f

$P, [a]P, [b]P, [c]P \to [abc]P$

$\Downarrow$ určí 2^{abc}

ZNÁM $2, 2^a, 2^b, 2^c, 2^{ab}, 2^{bc}, 2^{ac}$ — 2^{abc}

$c = 1$

POKUD UMÍŠ BILINEÁRNÍ DHP

$\Downarrow$

STAND ALONE DHP

DHP

$P, [a]P, [b]P$

$\Downarrow ?$

$[ab]P$

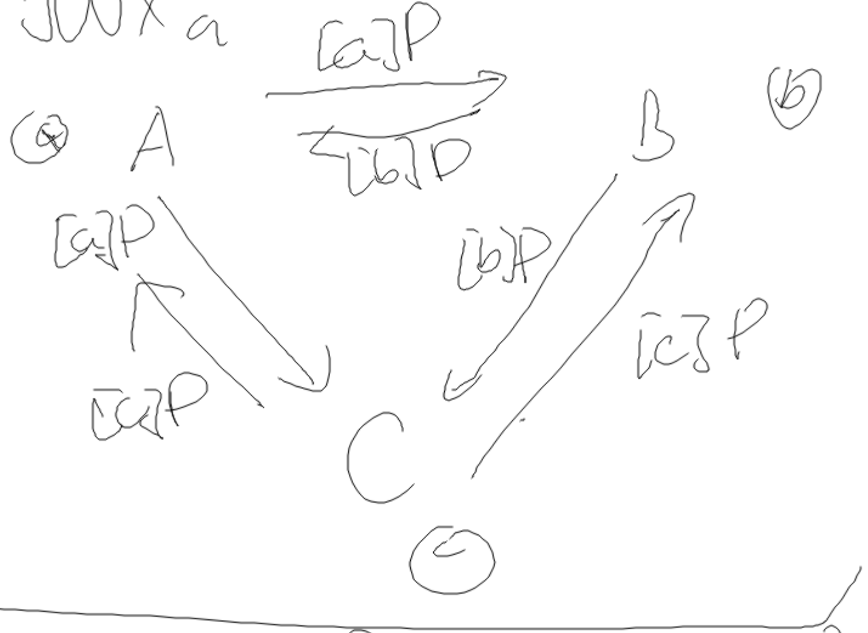
$A \xrightarrow{[a]P} B$

$A \xleftarrow{[b]P} B$

(a) (b)

Oba znají $[ab]P$

PROTOKOL JOUX



$$f([b]P,[c]P)^{a} = f(P,P)^{abc}$$

SDÍLENÉ TAJEMSTVÍ

DH-čtveřice (P, aP, bP, cP), kde $cP = abP$

[illegible], že lze ověřit, že se jedná o DH-čtveřice ze znalosti f, neboť $f(aP,bP) = f(P,P)^{ab} = f(P,cP)$