G_q Gruppe
g_1, g_2 Erzeuger von G_q
$x, y \in \mathbb{Z}/q\mathbb{Z}$ Eingaben

Alice				Bob
$x_a \in \mathbb{Z}/q\mathbb{Z}$ zufällig $g_a := g_1^{x_a} \neq^! 1$				$x_b \in \mathbb{Z}/q\mathbb{Z}$ zufällig $g_b := g_1^{x_b} \neq^! 1$
	$\leftarrow$	g_a, g_b	$\rightarrow$	
		Schnorr		
	$\leftarrow$	Kenntnis von x_a bzw. x_b	$\rightarrow$	
$g_3 := g_b^{x_a} = g_1^{x_a x_b}$				$g_3 := g_a^{x_b} = g_1^{x_a x_b}$
$a \in \mathbb{Z}/q\mathbb{Z}$ zufällig $P_a := g_3^a = g_1^{a x_a x_b}$ $Q_a := g_1^a g_2^x$				$b \in \mathbb{Z}/q\mathbb{Z}$ zufällig $P_b := g_3^b = g_1^{b x_a x_b}$ $Q_b := g_1^b g_2^y$
	$\leftarrow$	P_a, Q_a, P_b, Q_b	$\rightarrow$	
		Okamoto		
	$\leftarrow$	Kenntnis von a, x bzw. b, y	$\rightarrow$	
$P_a/P_b = g_1^{(a-b)x_a x_b}$ $Q_a/Q_b = g_1^{(a-b)} g_2^{x-y}$ $R_a = (Q_a/Q_b)^{x_a}$				$P_a/P_b = g_1^{(a-b)x_a x_b}$ $Q_a/Q_b = g_1^{(a-b)} g_2^{x-y}$ $R_b = (Q_a/Q_b)^{x_b}$
	$\leftarrow$	R_a, R_b	$\rightarrow$	
		Chaum-Pedersen		
	$\leftarrow$	Bew. der Gleichheit $log_{g_1} g_a = log_{Q_a/Q_b} R_a$ bzw. $log_{g_1} g_b = log_{Q_a/Q_b} R_b$	$\rightarrow$	
$R_{ab} := R_b^{x_a}$				$R_{ab} := R_a^{x_b}$
$R_{ab} =^? P_a/P_b$		VERIFIKATION		$R_{ab} =^? P_a/P_b$