Copánkové grupy obsahují několik problémů, které umožňují vytvořit trapdoor funkce pro účely asymetrické kryptografie. Konkrétně conjugacy problem ukazoval potenciál pro tyto účely a vzniklo několik schémat na něm založených. Bohužel se záhy ukázalo, že instance tohoto problému používané v návrzích schémat jsou zranitelné vůči útokům. Cílem této práce bude formálně popsat copánkové grupy a vybudovat teorii pro popis tohoto problému, vybraných odvozených kryptosystémů a útoků na tyto kryptosystémy. V závěru práce pak nahlédneme na další potenciální problémy, které by mohly sloužit k vybudování nového asymetrického kryptosystému.