Tato bakalářská práce se zabývá popisem Korelačních útoků na proudové šifry typu kombinačního generátoru. Čtenář je nejdříve zběžně seznámen se základními definicemi z kryptografické teorie potřebné k~porozumění textu. V práci je pak popsán původní článek, který tento druh útoku představuje, a který byl inspirací pro další vylepšení a modifikace. Podrobněji je pak popsána skupina vylepšených útoku nazývaná Rychlé korelační útoky, které jsou mnohem efektivnější, a již plně nahradily původní útok. Závěrem jsou pak popsány některé modifikace Rychlých korelačních útoků.