Nella crittografia simmetrica, le funzioni di round utilizzate come elementi costitutivi per i cifrari a blocchi iterati sono ottenuti come la composizione di diversi layer che agiscono come una sequenza di trasformazioni biunivoche che forniscono un aumento globale di complessità. Lo studio delle condizioni su tali layer che rendono il gruppo generato dalle funzioni di round di un cifrario a blocchi un gruppo primitivo è stato affrontato negli anni passati, sia nel caso di Substitution Permutation Networks che di Feistel Networks, dando ai progettisti di cifrari a blocchi la ricetta per evitare l'attacco di imprimitività, che sfrutta l'invarianza di alcuni sottospazi durante la cifratura. Nel caso degli schemi Lai-Massey, in cui sia i Substitution Permutation Networks che le reti di Feistel sono combinati, la resistenza agli attacchi di imprimitività è un problema aperto di vecchia data. In questo seminario mostriamo una generalizzazione di tale schema e dimostriamo la sua resistenza contro l'attacco di imprimitività. La nostra soluzione è ottenuta come conseguenza di un più risultato generale in cui il problema di dimostrare la primitività di uno schema di Lai-Massey generalizzato si riduce a quello più semplice di dimostrare la primitività del gruppo generato dalle funzioni di round di una SPN strettamente correlata. Mostriamo come questo implichi una riduzione del costo computazionale della ricerca in sottospazio invariante."