$\text{Abbreviations} \\ \sim X \ 1 = \operatorname{aenc}((\operatorname{groupkey request}, \operatorname{sign}(\operatorname{groupkey request}, \sim M \ 2), \\ -M_3), -M) \\ = \operatorname{aenc}((\operatorname{groupkey request}, \operatorname{sign}(\operatorname{groupkey request}, \operatorname{attsk} \ 2), \operatorname{cert}(\operatorname{attvid} \ 2, \operatorname{pk}(\operatorname{attsk} \ 2), \operatorname{cask} \ 3)), \operatorname{pk}(\\ \operatorname{cask} \ 3)) \\ \sim M_5 = \operatorname{aenc}(((\operatorname{groupkey response}, \operatorname{attvid} \ 2, \operatorname{gsk}(\operatorname{attvid} \ 2, \operatorname{gmsk} \ 4), \operatorname{pk}(\operatorname{gmsk} \ 4), \operatorname{sign}((\operatorname{groupkey response}, \operatorname{attvid} \ 2, \operatorname{gmsk} \ 4), \operatorname{pk}(\operatorname{gmsk} \ 4), \operatorname{pk}(\operatorname{gmsk} \ 4), \operatorname{cask} \ 3)), \operatorname{pk}(\\ \operatorname{attsk} \ 2)) \\ \sim M_6 = \operatorname{aenc}((\operatorname{groupkey response}, \operatorname{vid} \ 7, \operatorname{gmsk} \ 4), \operatorname{gpk}(\operatorname{gmsk} \ 4), \operatorname{gnsk}(\operatorname{groupkey response}, \operatorname{vid} \ 7, \operatorname{gmsk} \ 4), \operatorname{gpk}(\operatorname{gmsk} \ 4), \operatorname{gnsk}(\operatorname{groupkey response}, \operatorname{vid} \ 7, \operatorname{gsk}(\operatorname{vid} \ 7, \operatorname{gmsk} \ 4), \operatorname{gnsk}(\operatorname{groupkey response}, \operatorname{vid} \ 7, \operatorname{gsk}(\operatorname{vid} \ 7, \operatorname{gmsk} \ 4), \operatorname{gnsk}(\operatorname{groupkey response}, \operatorname{vid} \ 7, \operatorname{gsk}(\operatorname{vid} \ 7, \operatorname{gmsk} \ 4), \operatorname{gnsk}(\operatorname{gnoupkey response}, \operatorname{vid} \ 7, \operatorname{gsk}(\operatorname{vid} \ 7, \operatorname{gmsk} \ 4), \operatorname{gnsk}(\operatorname{gnoupkey response}, \operatorname{vid} \ 7, \operatorname{gsk}(\operatorname{vid} \ 7, \operatorname{gmsk} \ 4), \operatorname{gnsk}(\operatorname{gnoupkey response}, \operatorname{vid} \ 7, \operatorname{gsk}(\operatorname{vid} \ 7, \operatorname{gmsk} \ 4), \operatorname{gnsk}(\operatorname{gnoupkey response}, \operatorname{vid} \ 7, \operatorname{gsk}(\operatorname{vid} \ 7, \operatorname{gmsk} \ 4), \operatorname{gnsk}(\operatorname{gnsk} \ 4, \operatorname{gnsk} \ 4, \operatorname{gnsk} \ 4, \operatorname{gnsk} \ 4, \operatorname{gnsk}(\operatorname{gnsk} \ 4, \operatorname{gnsk} \$

