Let $F_{BIG}: \mathbf{K} \times \mathbf{X} \longrightarrow \mathbf{Y}$ be a PRF that has the extension property

$$F_{BIG}(k, x) = F_{BIG}(k, y) \quad \Rightarrow \quad F_{BIG}(k, \mathbf{x\|w}) = F_{BIG}(k, \mathbf{y\|w})$$

Generic attack on the derived MAC:

step 1: issue $|Y|^{1/2}$ message queries for rand. messages in X.

obtain (m_i, t_i) for $i = 1 ,\dots, |Y|^{1/2}$

step 2: find a collision $t_u = t_v$ for $u \neq v$ (one exists w.h.p by b-day paradox)

step 3: choose some w and query for $t := F_{BIG}(k, \mathbf{m_u\|w})$

step 4: output forgery $(\mathbf{m_v\|w},\ \mathbf{t})$. Indeed $t := F_{BIG}(k, \mathbf{m_v\|w})$