One-time security (unconditional)

Thm: the one-time MAC on the previous slide satisfies (L=msg-len)

$$\forall m_1 \neq m_2, t_1, t_2: \quad \Pr_{a,b}\left[S((a,b), m_1) = t_1 \;\middle|\; S((a,b), m_2) = t_2 \right] \leq L/q$$

Proof: $\forall m_1 \neq m_2,\ t_1,\ t_2$:

(1) $\Pr_{a,b}\left[S((a,b), m_2) = t_2 \right] = \Pr_{a,b}\left[P_{m_2}(a)+b=t_2 \right] = 1/q$

(2) $\Pr_{a,b}\left[S((a,b), m_1) = t_1 \text{ and } S((a,b), m_2) = t_2 \right] =$

$$\Pr_{a,b}\left[P_{m_1}(a)-P_{m_2}(a)=t_1-t_2 \text{ and } P_{m_2}(a)+b=t_2 \right] \leq L/q^2 \quad \blacksquare$$

$\Rightarrow$ given valid (m_2,t_2), adv. outputs (m_1,t_1) and is right with prob. $\leq L/q$