

Client

Exit Proxy

CDN

(1)

*Generate session
key (skey), append
encrypted session
key as header,
encrypt URL*

GET {foo}_{skey},
{skey}_{PK_exit}

(2)

*Decrypt {skey}_{PK_exit},
decrypt {URL}_{skey}*

GET HMAC_k(foo)

(3)

Retrieve content

{content_{foo}}_k

(4)

*Decrypt {content}_k,
encrypt {content}_{skey}*

{content_{foo}}_{skey}

(5)

*Decrypt
{content}_{skey}*