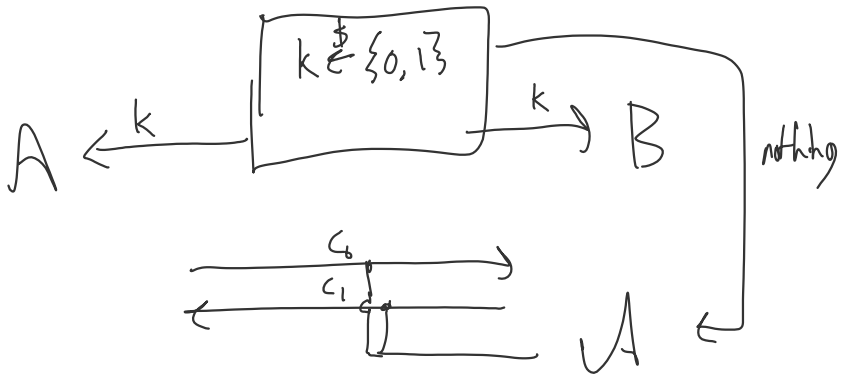
Diffie hellman problems

Thursday, October 3, 2019 12:01 PM

Key exchange



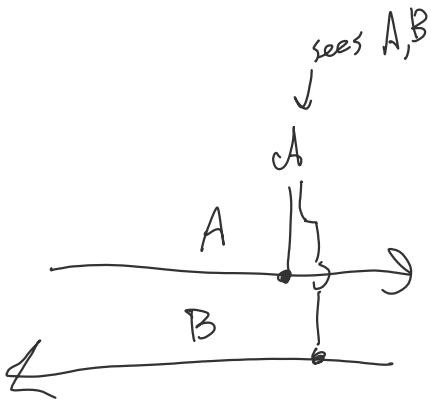
Basic idea:

hardness of computing: g^{ab}, given only

$A = g^a$, $B = g^b$ $\quad g^{a+b} = AB$

$A^b = g^{ab}$

Protocol:



$a \xleftarrow{\$} \mathbb{Z}_p$

$A = g^a$

$b \xleftarrow{\$} \mathbb{Z}_p$

$B = g^b$

$k = H(B^a)$

$k = H(A^b)$

$B^a = A^b = g^{ab}$

↓

Continue using k as shared secret

A sees A, B, and by assumption cannot compute g^{ab}

Dlog: $\forall \mathcal{A}, \Pr\left[X \xleftarrow{\$} G, x \leftarrow \mathcal{A}(X) : g^x = X\right] = \text{negl}$

CDH: $\forall \mathcal{A}, \Pr\left[a \xleftarrow{\$} \mathbb{Z}_p, b \xleftarrow{\$} \mathbb{Z}_p, C \leftarrow \mathcal{A}(g^a, g^b) : C = g^{ab}\right] = \text{negl}$

Computational Diffie Hellman

DDH: Decisional Diffie Hellman

Diffie Hellman triple

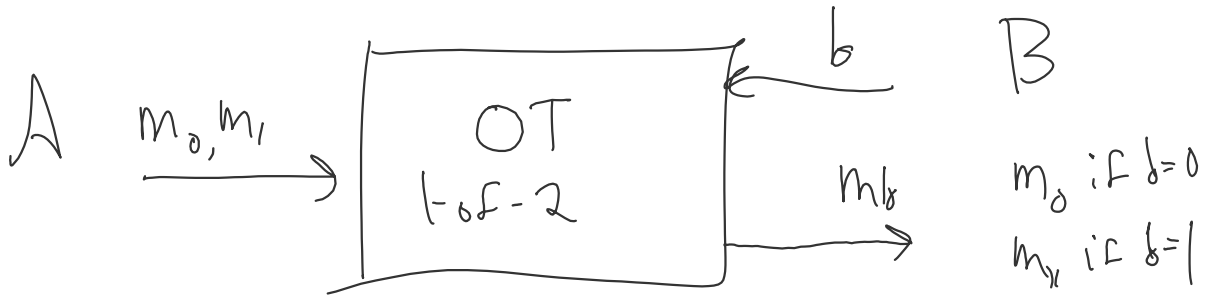
$\left\{a \xleftarrow{\$} \mathbb{Z}_p, b \xleftarrow{\$} \mathbb{Z}_p : (g^a, g^b, g^{ab})\right\}$

$\approx_c \left\{a \xleftarrow{\$} \mathbb{Z}_p, b \xleftarrow{\$} \mathbb{Z}_p, C \xleftarrow{\$} G : (g^a, g^b, C)\right\}$

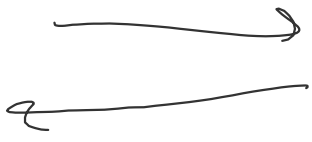
A, B, C

$\mathcal{A}(A, B) \stackrel{?}{=} C$

Oblivious Transfer



SimpleOT



Semi-Honest Simulatability

- Protect Alice from Bob

$\forall m_0, m_1, b, \exists S_B$ for View_B

$$\text{Sim}_B(b, m_b) \approx_c \text{View}_B\left[A(m_0, m_1) \leftrightarrow B(b)\right]$$

- Protect Bob from Alice

$\forall m_0, m_1, b, \exists S_A$ for View_A

$$\text{Sim}_A(m_0, m_1) \approx_c \text{View}_A\left[A(m_0, m_1) \leftrightarrow B(b)\right]$$