Okamoto IDS

We have P and V as in Schnorr.
We will proof that Okamoto in active model is secure.
Prover is an adversary. ~~He knows secret keys a_1, a_2~~
and group generator g_1, g_2 Secret keys a_1, a_2 are randomly chosen.

$g_1 = g$ and $g_2 = g^{\omega}$ ← unknown

$A \xleftarrow{\$}$

$A \leftarrow g_1^{a_1} g_2^{a_2} \left(= g_1^{a_1 + \omega a_2} \right)$

A is of the form $A = g_1^{a_1} g_2^{a_2}$

$\pi \left(P(a_1, a_2, A), V(A) \right) \to 1/0$

Protocol works as follow (security proof): 0° Simulation

$\tilde{P}$		V
$x_1, x_2 \leftarrow_R \mathbb{Z}_q$ $X \leftarrow g_1^{x_1} g_2^{x_2}$	$\xrightarrow{X}$	$c \leftarrow_R \mathbb{Z}_q$
	$\xleftarrow{c}$	
$s_1 = x_1 + a_1 c$ $s_2 = x_2 + a_2 c$	$\xrightarrow{s_1, s_2}$	$g_1^{s_1} g_2^{s_2} = XA^c$ true else false

In order to simulate protocol we just take part in it, since we have a_i's

Many of tuples a_1, a_2, x_1, x_2 can give us $A, X, c, s_1, s_2, \omega$
And now using a rewinding lemma we get different values:

$\tilde{P}$		V
	$\xrightarrow{X}$	
	$\xleftarrow{c'}$	$c' \leftarrow_R \mathbb{Z}_q$
$s_1' = x_1 + a_1 c'$ $s_2' = x_2 + a_2 c'$	$\xrightarrow{s_1', s_2'}$	

Reduction need to be done to compute ω

and break DLP:

?

1. ~~Correctness~~ - jak w Schnorze

2. Security definition

1. Lets define a game of two parties:
$P(SK, PK)$ and active verifier $\tilde{V}(PK)$

We define a view of few active games between them:

$$\bigvee \begin{cases} \Pi^1(P(SK, PK), \tilde{V}(PK)) \rightsquigarrow T_1 \\ \Pi^n(P(SK, P \ldots \end{cases}$$

Secondly, a malicious adversary tries to impersonate the prover

$$Pr\left|\Pi(\mathcal{A}(View, PK), V(PK))^{1}\right| \leq \text{negligible}$$

2) Security property

Let's define a game G_0:

2 parties $\quad P(sk, pk) \quad V(pk)$

Firstly the View ~~of a~~ consisting of several transcripts is created

ParamGen of KeyGen

$$V \begin{cases} \pi\big(P(sk, pk), V(pk)\big) \rightsquigarrow T_1 \\ \quad \text{udaję, żem mam sk, a kurwa nie mam} \\ \pi\big(\qquad \qquad \big) \to T_2 \end{cases}$$

Secondly a malicious adversary tries to impersonate the prover

$$(*) \quad \pi\big(\tilde{P}^{\mathcal{A}}(\text{View}, pk), \mathcal{V}(pk)\big)$$

Protocol is secure if

$$P\big((*) \to 1\big) \leq negl(\lambda)$$