

Okamoto IDS

We have P and V as in Schnorr.

We will proof that Okamoto in active model is secure.

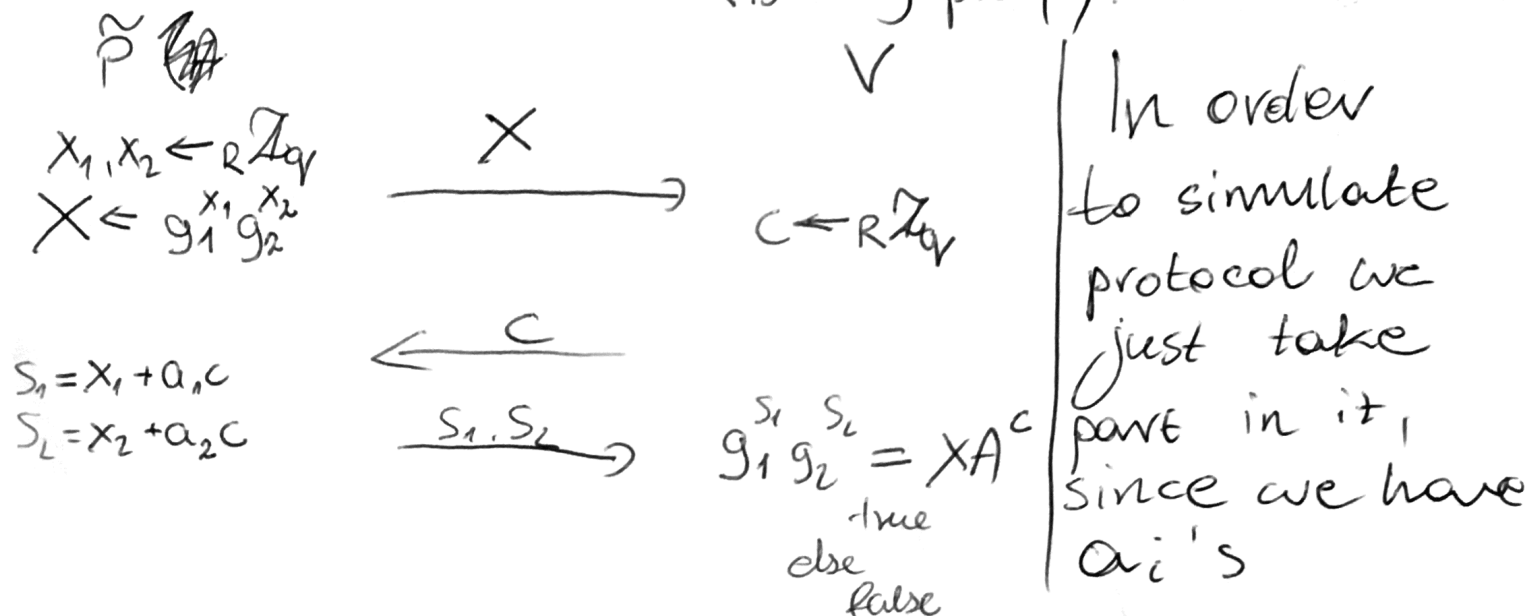
Prover is an adversary. ~~He knows secret keys a_1, a_2~~
 and group generator g_1, g_2 . Secret keys a_1, a_2 are randomly chosen.
 $g_1 = g$ and $g_2 = g^w$ $w \leftarrow \text{unknown}$ $A \leftarrow \mathbb{G}$ chosen.

$$A \leftarrow g_1^{a_1} g_2^{a_2} (= g_1^{a_1 + wa_2})$$

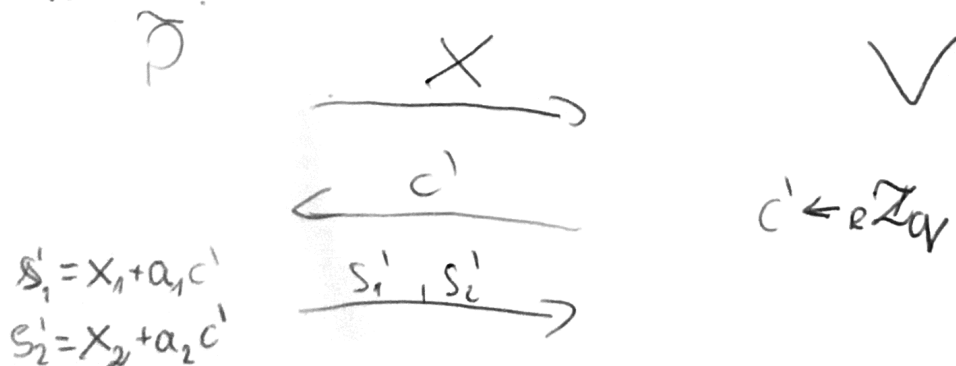
A is of the form $A = g_1^{a_1} g_2^{a_2}$

$$\pi(P(a_1, a_2, A), V(A)) \rightarrow 1/0$$

Protocol works as follow (security proof): \circ Simulation



Many of tuples a_1, a_2, X_1, X_2 can give us A, X, C, S_1, S_2, w
 And now using a rewinding lemma we get different values:



Reduction need to be done to compute w

and break DLP: 2

1. Correctness - jak w Schnorr

2. Security definition

1. let's 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:

$$\bigvee \begin{cases} \pi^1(P(sk, PK), \tilde{V}(PK)) \rightsquigarrow T_1 \\ \pi^n(P(sk, P) \dots \end{cases}$$

Secondly, ~~we~~ a malicious adversary tries to impersonate the prover

$$\Pr \left[\pi^1(\mathcal{A}(\text{View}, PK), \tilde{V}(PK)) \rightsquigarrow T_1 \right] \leq \text{negligible}$$

2) Security property

Let's define a game G_0 :

2 parties

$P(sk, pk)$

$V(pk)$

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

Parameters of
KeyGen

$$V \left\{ \begin{array}{l} \pi(P(sk, pk), V(pk)) \rightsquigarrow T_1 \\ \pi(\text{udaje, zem mam} \\ \text{sk, a kurwa nie mam}) \rightsquigarrow T_2 \end{array} \right.$$

Secondly a malicious adversary
tries to impersonate the prover

$$(*) \pi(P(\text{View}, PK), V(pk))$$

Protocol is secure if

$$P((*) \rightarrow 1) \leq \text{negl}(\lambda)$$