SCHNORR IDS

We have two parties - P; V which denotes prover and verifier. Protocol is successful if correctness ~~equation~~ condition is fulfilled.

We start with initialization:

ParamGen() → params

KeyGen(params) → SK, PK where SK - secret key, PK - public key

Having SK and PK we can start a protocol, which, if ~~accepts~~ is correct, ~~fulfill the following equation~~ accepts honest P(SK, PK) with p-ty 1

$$Pr\left[\Pi(P(PK,SK), V(PK) \to 1)\right] = 1$$

~~where KeyGen() → (SK, PK)~~

d(PK, View), V(PK)

Schnorr IDS is secure if $adv(t) = \max P[\Pi(\dots) \to 1]$ is negligible, where $View = \{t_1, t_2, \dots t_m\}$

How protocol works:

We have a dLP (discrete logarithm problem) to break: $DL_g A = \alpha$

P(sk, $A = g^\alpha$) — pk — V(A)

Adversary is trying to guess a

$x \leftarrow_R Z_q$, $X = g^x$ — X → — $c \leftarrow_R Z_q$

$s = x + ac$ — ← c —

— s → — if $g^s = XA^c$ true else false

1 The prover needs to simulate transcription

X

c

s

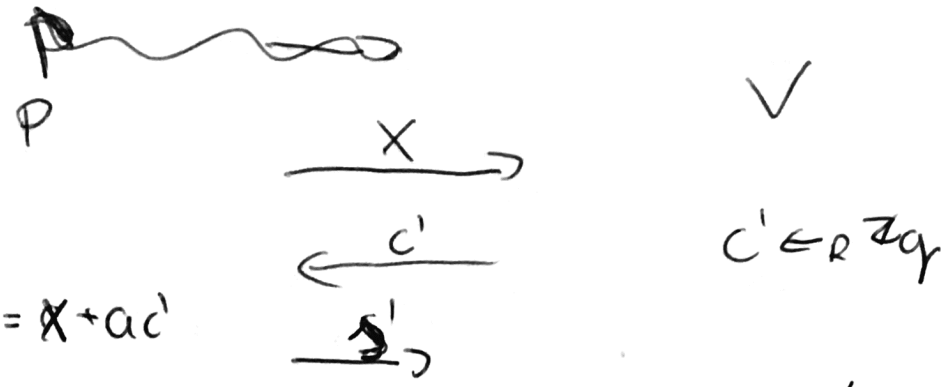
s ← $

c ← $

$X = \frac{g^s}{A^c}$

And now, we assume that adversary can rewind to X. Now ~~he sends the~~ the same X is reused ~~to verifier~~ but ~~gets~~

~~modified C changes and so does~~ ~~C, C' and s computes~~ or $s(s')$ ~~and~~, $c' \neq c, s \neq s'$



Now, by solving the equations we can guess a, what results in breaking DLP:

$$s = ax + x$$
$$s' = ac' + x$$

$$s - \hat{s} = a(c - c')$$
$$a = \frac{s - s'}{c - c'}$$

Conclusion:

~~While adversary cannot rewind to the same~~ ~~he cannot obtain such s' and c' which will be~~ Adversary cannot learn anything from observing transcripts that he could not compute himself. The key idea is ~~that~~ that order of generating transcripts doesn't matter. Schnorr IDS is secure against eavesdropping.

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

ParamGen, KeyGen

V { $\Pi(P(sk,pk), V(pk)) \rightarrow T_1$ (udaje, że mam sk, a kurwa nie mam)

$\Pi($ $) \rightarrow T_2$

Secondly a malicious adversary tries to impersonate the prover

(*) $\Pi(\tilde{P}(View, PK), V(pk))$

Protocol is ~~it~~ Secure if

$$P((*) \rightarrow 1) \leq negl(\lambda)$$