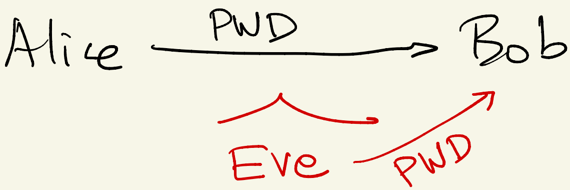
IDENTIFICATION

GOAL: Alice PROVES HER IDENTITY TO Bob

SETUP PHASE
IDENTIFICATION PHASE } PASSWORDS

MODEL



Eve MAY IMPERSONATE Alice

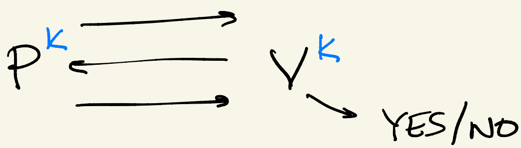
NONINTERACTIVE SCHEMES LIKE PASSWORDS ARE INSECURE

INTERACTIVE PROTOCOLS: Alice AND Bob EXCHANGE MULTIPLE MESSAGES OF PRE-SPECIFIED SIZE IN A GIVEN ORDER.

SECRET-KEY IDENTIFICATION

SETUP PHASE: KEY EXCHANGE $\boxed{K}$ UNKNOWN TO Eve

PROOF OF KNOWLEDGE: Alice = Prover
Bob = Verifier



FUNCTIONALITY: UPON INTERACTING WITH $P(k)$, $V(k)$ ACCEPTS WITH PROB. 1 (FOR ANY KEY k).

SECURITY ?

$$P^k \xrightarrow{M=k} V^k$$

$\downarrow$ ACC IF $M=k$

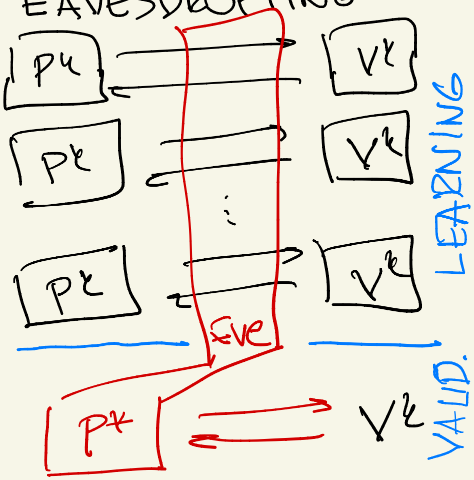
P^*

$$P^* \xrightarrow{\text{GUESS } k} V^k$$

$\Pr[P^* \text{ GUESSES } k] \leq 2^{-k}$

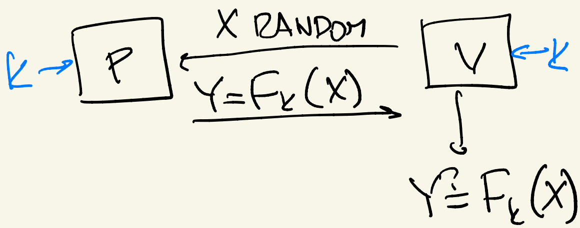
EVEN AFTER 1 EAVESDROP CAN IMPERSONATE.

EAVESDROPPING



(s, q, ε) - EAVESDROPPING SECURITY: P^* OF SIZE s CANNOT PASS VALID. W/P $> \varepsilon$ EVEN AFTER OBSERVING q INTERACTIONS

CHALLENGE-RESPONSE



Eve OBSERVES

$(X_1, F_k(X_1)), \ldots, (X_q, F_k(X_q))$

VALIDATION

$\xleftarrow{\text{NEW } X}$

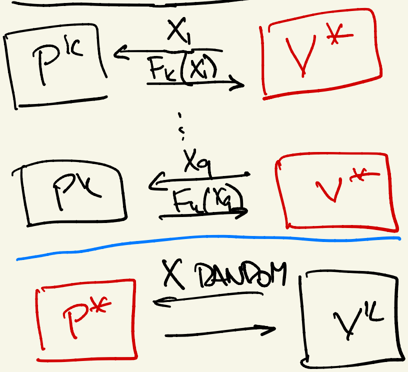
$\xrightarrow{F_k(X)}$

IF $X = X_i$ FOR SOME i CAN GUESS (PROB. $q/2^n$)

IF NOT ADV. $= 2^{-n} + \varepsilon$

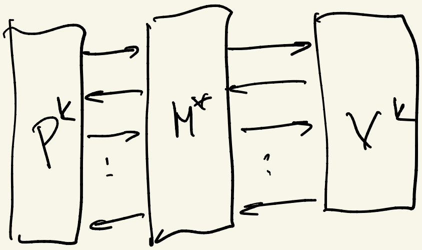
GUESS $F_k(x)$ PRF

IMPERSONATION



(s, q, ε) - SECURE : PASS V^k w/P $\geq \varepsilon$.

MAN-IN-MIDDLE



SECURITY IMPOSSIBLE

Claim. C-R PROTOCOL SECURE AGAINST IMPERSONATION

ADDED POWER : V^* GETS TO CHOOSE $x_1, \ldots, x_q$ IN IMPERSONATION PHASE

PRFs HAVE ADAPTIVE SECURITY

$F_k(x)$ COMP. IND. OF $F_k(x_1), \ldots, F_k(x_q)$ UNLESS $x = x_i$ FOR SOME i.

PUBLIC-KEY IDENTIFICATION

SETUP : P GENERATES (sk, pk) & PUBLISHES pk

ID : P NEEDS TO CONVINCE V HE KNOWS sk.

EAVESDROPPING

PUBLIC KEY CHALLENGE-RESPONSE $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$

$$\begin{array}{ccc} \boxed{P^{sk}} & \xleftarrow{C=\mathrm{Enc}(pk,M)} & \boxed{V^{pk}} \\ & \xrightarrow{M'=\mathrm{Dec}(sk,C)} & \downarrow \\ & & M \stackrel{?}{=} M'. \end{array}$$

M RANDOM

EAVESDROPPER OBSERVES

$$(\mathrm{Enc}(pk, M_1), M_1, \mathrm{Enc}(pk, M_2), M_2, \ldots, \mathrm{Enc}(pk, M_q), M_q)$$

NEEDS TO COME UP WITH $\mathrm{Dec}(sk, C)$ FOR $C = \mathrm{Enc}(pk, M)$ FOR RANDOM M.

CAN SIMULATE LEARNING PHASE BY REVERSING ORDER OF RESPONSES AND CHALLENGES

CANNOT PRODUCE $\mathrm{Dec}(sk, C)$ FROM $C = \mathrm{Enc}(pk, M)$ BY SIMULATABILITY

$$\Pr[P^*(pk, \mathrm{Sim}(pk)) = M] \leq 2^{-n} \rightarrow \Pr[P^*(pk, \mathrm{Enc}(pk, M)) = M] \leq 2^{-n} + \varepsilon.$$

PK CR AGAINST IMPERSONATION?

TO ILLUSTRATE PROBLEM ASSUME Enc IS El Gamal

$$(SK, PK) = (X, g^X)$$
$$\mathrm{Enc}(PK, M) = (g^R, PK^R \cdot M)$$
$$\mathrm{Dec}(X, (Y, C)) = Y^{-X} \cdot C$$

$\boxed{P^{SK}}$ $\xleftarrow{(Y,C)}$ V^*

$\xrightarrow{\mathrm{Dec}(SK,(Y,C))}$

$\xleftarrow{(g^X, 1)}$

$\xrightarrow{g^{-X^2}}$

GIVEN g^X, NOT CLEAR HOW TO SIMULATE g^{-X^2} WITHOUT COMPUTING DLOG.

DOES NOT MEAN C-R El Gamal IS <u>INSECURE</u> AGAINST IMPERSONATORS BUT UNCLEAR HOW TO PROVE SECURITY.

THERE EXIST OTHER PKE THAT <u>ARE</u> INSECURE AGAINST IMPERSONATORS AS C-R PROTOCOLS.

SCHNORR'S PROTOCOL

$SK = X$ P $R \xrightarrow{h = g^R}$ V $PK = g^X$ COMMITMENT

$\xleftarrow{C \sim \{0,1\} \;\sim\; \mathbb{Z}_q}$

$\xrightarrow{Y = R + CX}$ $\boxed{PK^C \cdot h \stackrel{?}{=} g^Y}$

FUNCTIONALITY: $(g^X)^C \cdot g^R = g^{R+CX}$ ✓

EAVESDROPPER: OBSERVES (PK, h, C, Y)

$$= (g^X, g^R, C, R+CX)$$

GIVEN g^X, CAN YOU SIMULATE $g^R, C, R+CX$

CHOOSE Y, C AT RANDOM

SIMULATE g^R BY $g^Y \cdot PK^{-C} = g^Y \cdot g^{-CX}$

$$P^* \xrightarrow{\;h\;} V \qquad PK = g^X$$
$$P^* \xleftarrow{\;C\;} V$$
$$P^* \xrightarrow{\;Y\;} V$$

$$\boxed{PK^C \cdot h = g^Y}$$

ARGUMENT: IF $\Pr[PK^C \cdot h = g^Y] \geq \varepsilon$

THEN WE CAN FIND X GIVEN g^X

WITH PROBABILITY $\approx \varepsilon^2$.

IDEA. RUN (P^*, V) PROTOCOL TWICE

TO GET "2 EQUATIONS" FROM

WHICH WE CAN SOLVE FOR X.

$$P^* \xrightarrow{\;h\;} V \qquad \text{IDENTICAL} \qquad P^* \xrightarrow{\;h\;} V$$
$$P^* \xleftarrow{\;C\;} V \qquad\qquad\qquad P^* \xleftarrow{\;C'\;} V$$
$$P^* \xrightarrow{\;Y\;} V \qquad \text{INDEPENDENT} \qquad P^* \xrightarrow{\;Y'\;} V$$

$$PK^C \cdot h = g^Y \qquad\qquad PK^{C'} \cdot h = g^{Y'}$$

$$\left.\begin{array}{l} PK^{c}\cdot h = g^{Y} \\ PK^{c'}\cdot h = g^{Y'} \end{array}\right\} \longrightarrow \begin{array}{l} PK^{c-c'} = g^{Y-Y'} \\ PK = g^{(Y-Y')/(c-c')} \end{array}$$

$\dfrac{Y-Y'}{\boxed{C-C'}}$ MUST BE THE DLOG OF PK.

$$\Pr[g^{Y} = h\cdot PK^{C} \text{ AND } g^{Y'} = h\cdot PK^{C'}]$$

$$= E[\Pr[g^{Y} = h\cdot PK^{C}, g^{Y'} = h\cdot PK^{C'}] \mid h, PK]$$

CONDITIONALLY INDEPENDENT

$$= E[\Pr[g^{Y} = h\cdot PK^{C}]^2 \mid h, PK]$$

$$\geq E[\Pr[g^{Y} = h\cdot PK^{C}]]^2$$ CAUCHY-SCHWARZ (NONNEG. OF VARIANCE)

$$= \Pr[g^{Y} = h\cdot PK^{C}]^2 = \varepsilon^2$$

BUT $C-C'$ COULD BE ZERO!

$\Pr[C=C'] = \frac{1}{2}$

Prob OF P^* FOOLING V IS SOME CONSTANT LARGER THAN ½ BUT BOUNDED AWAY FROM 1.

CAN IMPROVE BY CHOOSING C FROM LARGER CHALLENGE SPACE, OR BY REPEATING THE PROTOCOL INDEPENDENTLY.

THIS WILL HANDLE IMPERSONATION ATTACKS

$SK = X$ $\quad$ $PK = g^X$

$P \xrightarrow{\boxed{R}\ h = g^R} V^*$ $\qquad$ COMMITMENT

$P \xleftarrow{C^*} V^*$

$P \xrightarrow{Y = R + CX} V^*$ $\qquad$ $\boxed{PK^C \cdot h \stackrel{?}{=} g^Y}$

V^* IS A CHEATING VERIFIER

C^* CAN DEPEND ON PK AND ON h

WANT TO ARGUE EVEN SUCH A V^* CAN SIMULATE HIS VIEW (GIVEN PK)

$(PK = g^X,\ h = g^R,\ \underline{Y} = R + \underline{C}^* X)$

MIGHT NOT BE INDEPENDENT

<u>Sim</u>: GUESS C, Y AT RANDOM

SET $h = g^Y PK^{-C}$

CALCULATE $C^*(PK, h)$

IF $C = C^*$ OUTPUT (PK, h, Y)

IF NOT TRY AGAIN

<u>GIVEN $C^* = C$</u>, Sim OUTPUT IDENTICALLY DISTRIBUTED TO V^*'S VIEW

$\Pr[C = C^* \mid PK] = \frac{1}{2}$ SO $\Pr[\text{Sim OUTPUTS}] = \frac{1}{2}$.

REPEAT q TIMES $\rightarrow$ $\Pr = 1 - 2^{-q}$.

$\boxed{2^{-q}\text{-CLOSE TO } V^*\text{'S VIEW.}}$