IDENTIFICATION

GOAL: Alice PROVES HER IDENTITY to Bob

SETUP PHASE

IDENTIFICATION PHASE

MODEL

Alice $\xrightarrow{\text{PWD}}$ Bob

Eve $\xrightarrow{\text{PWD}}$

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 $[k]$ unknown to Eve

PROOF OF KNOWLEDGE: Alice = Prover

Bob = Verifier

$P^k \xleftarrow{} Y^k \xrightarrow{} \text{YES/NO}$
**FUNCTIONALITY:** Upon interacting with $P(k), V(k)$ accepts with probability 1 (for any key $k$).

Security question?

\[
P^k \xrightarrow{M=k} V^k \xrightarrow{\text{ACC if } M=k} \]

$P^*$ guesses $k$ with $V^k$

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

Even after (eavesdropping can impersonate).

---

**Eavesdropping**

\[P^k \xrightarrow{\text{Eve}} V^k \]

\[P^k \xrightarrow{\text{Eve}} V^k \]

\[P^k \xrightarrow{\text{Eve}} V^k \]

\[P^k \xrightarrow{\text{Eve}} V^k \]

(s, q, e) - Eavesdropping security: $P^k$ of size $s$ cannot pass valid with $p > \varepsilon$ even after observing $q$ interactions.

---

**Challenge-Response**

\[k \rightarrow P \xrightarrow{X \text{ random}} y = F_k(x) \xrightarrow{\text{Eve observes}} (x_1, F_k(x_1), \ldots, (x_q, F_k(x_q))) \]

Validation

\[\text{NEW } X \xleftarrow{\text{F_k(x)}} \rightarrow \]

If $X = x_i$ for some $i$, can guess (prob. $q/2^m$).

If not adv. $= 2^{-m} + \varepsilon$ guess $F_k(x) \rightarrow \text{pre}$. 
Claim. C-R Protocol Secure Against Impersonation

Added Power: \( V^* \)
Gets to choose \( X_1, \ldots, X_9 \)
In Impersonation Phase

PRFs Have Adaptive Security

\( F_k(X) \) Comp. Ind. of \( F_k(X_1), \ldots, F_k(X_9) \) 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 (Gen, Enc, Dec)

\[
\begin{array}{c}
S_k \quad \text{(P)} \\
C = \text{Enc}(P_k, M) \\
M! = \text{Dec}(S_k, C) \\
V \quad \text{(V)}
\end{array}
\]

M RANDOM

EAVESDROPPER OBSERVES

\[
(\text{Enc}(P_k, M_1), M_1, \text{Enc}(P_k, M_2), M_2, \ldots, \text{Enc}(P_k, M_q), M_q)
\]

NEEDS TO COME UP WITH \(\text{Dec}(S_k, C)\) FOR \(C = \text{Enc}(P_k, M)\) FOR RANDOM M.

CAN SIMULATE LEARNING PHASE BY REVERSING ORDER OF RESPONSES AND CHALLENGES

CANNOT PRODUCE \(\text{Dec}(S_k, C)\) FROM \(C = \text{Enc}(P_k, M)\) BY SIMULATABILITY

\[
\Pr [ P^* (P_k, \text{Sim}(P_k)) = M ] \leq 2^{-m} \quad \Rightarrow \quad \Pr [ P^* (P_k, \text{Enc}(P_k, M)) = M ] \leq 2^{-m + \epsilon}
\]
PK CR AGAINST IMPERSONATION?

TO ILLUSTRATE PROBLEM ASSUME Enc IS El Gamal

\[(SK, PK) = (X, g^x)\]

\[Enc(PK, M) = (g^2, PK^2 \cdot M)\]

\[Dec(X, (Y, C)) = Y^{-X} \cdot C\]

GIVEN \(g^x\), NOT CLEAR HOW TO SIMULATE \(g^{-x^2}\) WITHOUT COMPUTING DLOG.

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

THERE EXIST OTHER PKE THAT ARE INSECURE AGAINST IMPERSONATORS AS C-R PROTOCOLS.

SCHNORR'S PROTOCOL

\[SK = x\]

\[P \rightarrow h = g^2 \quad PK = g^x\] COMMITMENT

\[C \sim \{0, 1\}^q \sim Z_q\]

\[Y = R + CX\]

\[PK^C \cdot h = g^Y\]

FUNCTIONALITY: \((g^x)^C \cdot g^2 = g^{R + CX}\)
EAVESDROPPER observes $(P_L, h, C, Y) = (g^x, g^r, C, R + CX)$

Given $g^x$, can you simulate $g^r$ of PKC

Choose $Y, C$ at random
Simulate $g^r$ by $g^y . PK-C = g^y . g^{-CX}$

\[
\begin{align*}
P^* & \xrightarrow{h} C \\
C & \xrightarrow{v} P_L = g^x \\
Y & \xrightarrow{p^*} PKC . h = g^y
\end{align*}
\]

ARGUMENT: If $Pr[PKC . h = g^y] \geq \epsilon$
then we can find $X$ given $g^x$ with probability $\approx \epsilon^2$.

IDEA. Run $(P^*, V)$ protocol twice to get "2 equations" from which we can solve for $X$.

\[
\begin{align*}
P^* & \xrightarrow{h} C \\
C & \xrightarrow{v} IDENTICAL \\
Y & \xrightarrow{p^*} PKC . h = g^y
\end{align*}
\]

\[
\begin{align*}
P^* & \xleftarrow{h} C \\
C & \xleftarrow{v} INDEPENDENT \\
Y' & \xleftarrow{p^*} PKC' . h = g^{y'}
\end{align*}
\]
\[ \text{Pr}[g^y = h \cdot PK^c \text{ and } g^{y'} = h \cdot PK^{c'}] \]

\[ = E \left[ \text{Pr}[g^y = h \cdot PK^c, g^{y'} = h \cdot PK^{c'}] \mid h, PK \right] \]

\[ \text{CONDITIONALLY INDEPENDENT} \]

\[ = E \left[ \text{Pr}[g^y = h \cdot PK^c]^2 \mid h, PK \right] \]

\[ \geq E \left[ \text{Pr}[g^y = h \cdot PK^c] \right]^2 \quad \text{(CAUCHY-SCHWARZ, NONNEG. OF VARIANCE)} \]

\[ = \text{Pr}[g^y = h \cdot PK^c]^2 = \epsilon^2 \]

\[ \text{BUT } C - C' \text{ COULD BE ZERO!} \]

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

The probability of \( P^* \) fooling \( V \) is some constant larger than \( \frac{1}{2} \) but bounded away from 1. Can improve by choosing \( C \) from a larger challenge space, or by repeating the protocol independently. This will handle impersonation attacks.
$SK = x \overset{P}{\rightarrow} \begin{array}{c} h = g^x \\ C^x \end{array} \overset{V^*}{\rightarrow} \begin{array}{c} PK = g^x \\ \end{array}$

$Y = R + CX \quad \overset{PK^C \cdot h = g^Y}{\rightarrow}$

$V^*$ IS A CHEATING VERIFIER

$C^x$ CAN DEPEND ON $PK$ AND ON $h$

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

$(PK = g^x, h = g^R, Y = R + C^x X)$

MIGHT NOT BE INDEPENDENT

Sim: GUESS $C, Y$ AT RANDOM

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

CALCULATE $C^x(PK, h)$

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

IF NOT TRY AGAIN

GIVEN $C^x = C$, Sim OUTPUT IDENTICALLY DISTRIBUTED TO $V^*$'S VIEW

$Pr[C = C^x|PK] = \frac{1}{2}$  so $Pr[\text{Sim outputs}] = \frac{1}{2}.$

REPEAT $q$ TIMES $\Rightarrow Pr = 1 - 2^{-q}$ \textit{2^{-q}-CLOSE TO V^*'S VIEW.}