Computer Science 308-547A
Cryptography and Data Security

Claude Crépeau

These notes are, largely, transcriptions by Anton Stiglic of class notes from the former course *Cryptography and Data Security (308-647A)* that was given by prof. Claude Crépeau at McGill University during the autumn of 1998-1999. These notes are updated and revised by Claude Crépeau.

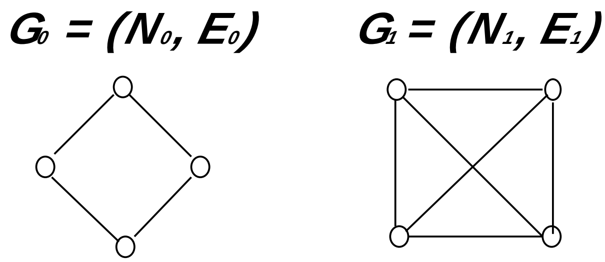
17 Zero-Knowledge Proofs

17.1 Interactive Proofs

The statement is valid ⇒ Verifier will accept.
The statement is invalid ⇒ Verifier will reject with high probability.

Zero-Knowledge: Whatever strategy the Verifier uses, all the data that he gets from the prover could have been generated by himslef, alone, aussimg that he knew the validity/invalidity of the statement.

17.1.1 ZK proof for graph isomorphism.



P wants to prove that $G_0 \cong G_1$. $G_0 = \tilde{\Pi}(G_1)$.

Prover		*Verifier*
$\Pi \in_R S_{N_1}$, $G \leftarrow \Pi(G_0)$		
	$\xrightarrow{G}$	
		$b \in_R \{0, 1\}$
	$\xleftarrow{b}$	
$\Pi_0 \leftarrow \Pi$, $\Pi_1 \leftarrow \Pi \cdot \tilde{\Pi}$		
	$\xrightarrow{\Pi_b}$	
		$verify\ G = \Pi_b(G_b)$

Definition 17.1 (Interactive Proof) *An interactive proof (I, P) is a two party game between:*

P: all-powerful prover, and
V: the verifier (probabilistic polynomial time verifier),
such that

$$\forall_{x\in L} Pr(V\ accepts\ x\ after\ talking\ to\ P) \geq \frac{2}{3}$$
$$\forall_{x\notin L} \forall_{P'} Pr(V\ accepts\ x\ after\ talking\ to\ P') < \frac{1}{3}$$

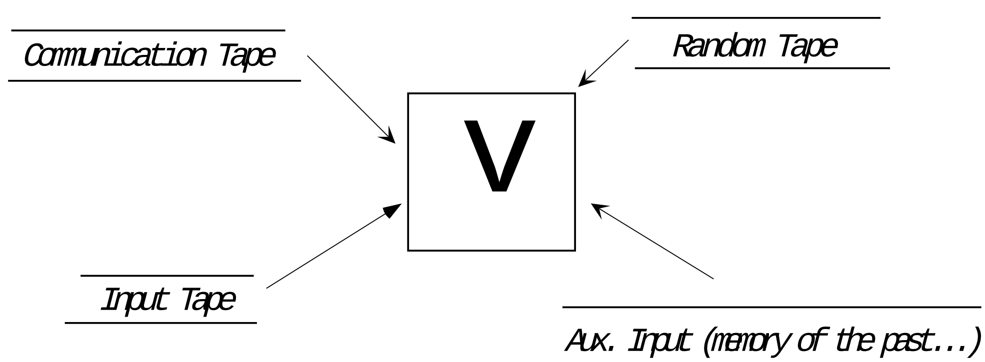
where P' is an arbitraly behaviored and all powerfull (can decide any language in constant time).

Note: "Talking to P" does not mean "invoking P'", because V has to be probabilistic polynomial time bounded.

For the above graph isomorphism proof to be an IP, one must execute two rounds of it. We will give a 1 round IP for this problem latter on.

17.1.2 Definiton of ZK-ness

definition of the *Verifier*:



$View(V)$ = a computation history of V on some input.

Definition 17.2 *An IP (P, V) is ZK if*

$$\forall_{V'}, \exists_{S_{V'}} : \forall_{x\in L} View(V', (P, V'), x) = S'(x).$$

where V' is an arbitrary behavior of V that is probabilistic and polynomialy time bounded and $S_{V'}$ is a simulator, also probabilistic polynomial time bounded.

Example 17.1 (graphs isomorphism:) *An IP for graph isomorphism in 1 round that is ZK:*

$$G_0 \cong G_1$$

$$\begin{array}{rcl}
P & & V \\
\Pi \leftarrow_R S_n, & & \\
\sigma \leftarrow_R S_n, & & \\
G \leftarrow \Pi(G_0) & & \\
G' \leftarrow \sigma(G_0) & & \\
 & \xrightarrow{G,G'} & \\
 & & b, b' \leftarrow_R \{0,1\} \\
 & \xleftarrow{b,b'} & \\
G = \Pi_b(G_b), & & \\
G' = \sigma_{b'}(G_{b'}) & & \\
 & \xrightarrow{\Pi_b,\sigma_{b'}} & \\
 & & verify: \\
 & & \textbf{if } G = \Pi_b(G_b) \textbf{ and } G' = \sigma_{b'}(G_{b'}) \\
 & & \textbf{then } \textit{accept} \\
 & & \textbf{else } reject.
\end{array}$$

Variations on ZK:
$View_{V'}(x) = S'(x)$ (distributions are the same): ZK is **perfect**.
$View_{V'}(x) \approx S'(x)$ (statistical indistinguishability): ZK is **statistical**.
$View_{V'}(x) \approx_P S'(x)$ (computational indistinguish.): ZK is **computational**.

17.2 RSA

P wants to prove that he knows m such that $c = m^e \bmod n$, where e, n and c are given publicly.

$$
\begin{array}{rcl}
\underline{Prover} & & \underline{Verifier} \\
m' \in_R Z_n^*, & & \\
c' \leftarrow m'^e \bmod n & & \\
 & \xrightarrow{c'} & \\
 & & b \in_R \{0,1\} \\
 & \xleftarrow{b} & \\
\hat{m} \leftarrow m^b m' \bmod n & & \\
 & \xrightarrow{\hat{m}} & \\
 & & verify\ c^b c' = \hat{m}^e \bmod n
\end{array}
$$

17.3 ElGammal

P wants to prove that he knows m such that $c = (\alpha^k \bmod p, m\beta^k \bmod p)$, for some k where $p, \alpha.\beta$ and c are given publicly.

$$
\begin{array}{rcl}
\underline{Prover} & & \underline{Verifier} \\
m' \in_R Z_p^*, & & \\
k' \in_R Z_{p-1}, & & \\
c' \leftarrow (\alpha^{k'} \bmod p, m'\beta^{k'} \bmod p) & & \\
 & \xrightarrow{c'} & \\
 & & b \in_R \{0,1\} \\
 & \xleftarrow{b} & \\
\hat{m} \leftarrow m^b m' \bmod p & & \\
\hat{k} \leftarrow bk + k' \bmod p-1 & & \\
 & \xrightarrow{\hat{m},\hat{k}} & \\
 & & verify\ c^b c' = (\alpha^{\hat{k}} \bmod p, \hat{m}\beta^{\hat{k}} \bmod p)
\end{array}
$$

17.4 Factoring

P wants to prove that he knows the factorization of n. The Verifier provides some quadratic residue x the Prover shows that a knows a square root r.

$$
\begin{array}{rcl}
\underline{Prover} & & \underline{Verifier} \\
r' \in_R Z_n^*, & & \\
y \leftarrow r'^2 \bmod n & & \\
 & \xrightarrow{y} & \\
 & & b \in_R \{0,1\} \\
 & \xleftarrow{b} & \\
\hat{r} \leftarrow r^b r' \bmod n & & \\
 & \xrightarrow{\hat{r}} & \\
 & & verify\ x^b y = \hat{r}^2 \bmod n
\end{array}
$$

17.5 Discrete log

P wants to prove that he knows a such that $\beta = \alpha^a \bmod p$, where p, α, β.

$$
\begin{array}{rcl}
\underline{Prover} & & \underline{Verifier} \\
a' \in_R Z_{p-1}, & & \\
\beta' \leftarrow \alpha^{a'} \bmod p & & \\
 & \xrightarrow{\beta'} & \\
 & & b \in_R \{0,1\} \\
 & \xleftarrow{b} & \\
\hat{a} \leftarrow ba + a' \bmod p-1 & & \\
 & \xrightarrow{\hat{a}} & \\
 & & verify\ \beta^b \beta' = \alpha^{\hat{a}} \bmod p
\end{array}
$$

References

[BB88] Pierre Beauchemin and Gilles Brassard. A generalization of hellman's extension of shannon's approach to cryptography. In Carl Pomerance, editor, *Proc. CRYPTO 87*, pages 461–461. Springer-Verlag, 1988. Lecture Notes in Computer Science No. 293.

[BS93] E. Biham and A. Shamir. *A Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, 1993.

[dB88] Bert den Boer. Cryptanalysis of F.E.A.L. In Christoph G. Günther, editor, *Advances in Cryptology—EUROCRYPT 88*, volume 330 of *Lecture Notes in Computer Science*, pages 293–299. Springer-Verlag, 25–27 May 1988.

[Hel80] M. E. Hellman. A cryptanalytic time-memory trade off. *IEEE Transactions on Information Theory*, IT-26:401–406, 1980.

[Mat94] M. Matsui. Linear cryptanalysis method for DES cipher. *Lecture Notes in Computer Science*, 765:386–397, 1994.

[Mur90] S. Murphy. The cryptoanalysis of FEAL-4 with 20 chosen plaintexts. *Journal of Cryptology*, 2:145–154, 1990.

[MVV97] A. J. (Alfred J.) Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. The CRC Press series on discrete mathematics and its applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 1997.

[NBS93] Data encryption standard (des). Technical Report FIPS PUB 46-2, National Bureau of Standards, 1993.

[NIS80] Des modes of operation. Technical Report FIPS PUB 81, National Institute of Standards and Technology, december 1980.

[NIS99] http://www.nist.gov/aes/, 1999.

[Sha48] C. E. Shannon. A mathematical theory of communication. volume 27, pages 379–423, 623–656, 1948.

[Sta99] William Stallings. *Cryptography and network security: principles and practice*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, second edition, 1999.

[Sti95] Douglas R. Stinson. *Cryptography Theory and Practice.* CRC Press, Boca Raton, 1995.

[VK84] V. L. Voydock and S. T. Kent. Security mechanisms in a transport layer protocol. *Computer Networks*, 8:433–450, 1984.