New Directions in Cryptography

CS 303 Alg. Number Theory & Cryptography

Jeremy Johnson

Witfield Diffie and Martin E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. IT-22, No. 6, Nov. 1976.

Classical Cryptography

- Basic problem: Secure communication over an insecure channel
- Solution: private key encryption
  - $\mathbf{m} \rightarrow \mathcal{E}(k,m) = c \rightarrow \mathcal{D}(k,c) = m$

- Shannon provided a rigorous theory of perfect secrecy based on information theory
  - Adversary has unlimited computational resources, but key must be as long as message

Other Cryptographic Problems

- Authentication
  - User Authentication – verify that an individual is who he/she claims
  - Message Authentication – Assure recipient that the message comes from authorized recipient and that the message
  - Message Integrity – Assure that the message has not been modified
- Threat of compromise of the receiver's authentication data
- Threat of dispute

Cryptoanalytic Attacks

- Ciphertext only attack
  - Cryptanalyst possesses only ciphertext
- Known plaintext attack
  - Cryptanalyst possesses substantial quantity of corresponding plaintext and ciphertext
- Chosen plaintext attack
  - Cryptanalyst can submit an unlimited number of plaintext messages of his own choosing and examine the resulting ciphertext

One Time Pad

- Pad = $b_1 \cdots b_n \in \{0,1\}^*$ chosen randomly
- $m = m_1 \cdots m_n$
  - $\mathcal{E}(\text{Pad},m) = c = m \oplus \text{Pad}$
  - $\mathcal{D}(\text{Pad},c) = c \oplus \text{Pad} = (m \oplus \text{Pad}) \oplus \text{Pad} = m$

- $\forall m,c \;\; \Pr_{\text{Pad}}[\mathcal{E}(\text{Pad},m) = c] = 1/2^n$
  - No information gained from seeing c
  - However, $\mathcal{E}(\text{Pad},m) \oplus \mathcal{E}(\text{Pad},m') = m \oplus m'$

Modern Cryptography

- Adversary's resources are computationally bounded
  - Probabilistic polynomial time algorithm
- Impossibility of breaking the encryption system $\rightarrow$ Infeasibility of breaking
- Rely on gap between efficient algorithms for encryption and computational infeasibility of decryption by adversary

Public Key Cryptography

- Let M be a message and let C be the encrypted message (ciphertext). A public key cryptosystem has a separate method E() for encrypting and D() decrypting.
  - D(E(M)) = M
  - Both E() and D() are easy to compute
  - Publicly revealing E() does not make it easy to determine D()
  - E(D(M)) = M - needed for signatures

- The collection of E()'s are made publicly available but the D()'s remain secret. Called a one-way trap-door function (hard to invert, but easy if you have the secret information)

Implementation of PK

- RSA (Integer Factorization)
- El Gamal (Discrete Logarithm)
- Goldwasser-Micali (Quadratic Redisuosity)
  - N = pq, x a non-residue such that $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1$
  - $m = m_1 \cdots m_t$, $m_i \in \{0,1\}$
  - $c = c_1 \cdots c_t$, $c_i = y_i x^{mi} \bmod N$, y_i random quadratic residue

Public Key Distribution

- The goal is for two users to securely exchange a key over an insecure channel. The key is then used in a normal cryptosystem

- Diffie-Hellman Key Exchange
  - $Y = \alpha^X \bmod q$ (q prime, α primitive – all elements are powers of α)
  - $X = \log_\alpha Y \bmod q$ [discrete log]
  - $Y_i = \alpha^{Xi} \bmod q$ [for each user]
  - $K_{ij} = \alpha^{Xi*Xj} \bmod q$ [shared key]
  - $K_{ij} = Y_i^{Xj} \bmod q = Y_j^{Xi} \bmod q$

One-Way Authentication

- One-way functions
  - Computationally easy to apply computationally hard to invert
- "login" problem – capable of judging authenticity of passwords without actually knowing them
  - Enter password (PW) and compute f(PW) and compare with stored value of f(PW) – do not store PW
  - Requires additional encryption
  - True one-way authentication using digital signature
- One-way message authentication
  - $M = (m_1, m_2, \ldots, m_N)$, $m_i \in \{0,1\}$
  - Generate 2N random bits $x_1, X_1, x_2, X_2, \ldots, x_N, X_N$
  - Send $f(x_1), f(X_1), f(x_2), f(X_2), \ldots, f(x_N), f(X_N)$ for authentication
  - Late when M is to be sent, send x_i or X_i depending on whether $m_i = 0$ or 1

Cryptographic Protocol

- A communication protocol with security assurances such as confidentiality, message integrity, anonymity
  - Entity authentication, secure internet communication (TLS/SSL/https/SSH), key exchange, digital signatures, digital cash, electronic voting, …
- Want provably secure protocols
- Key idea
  - Reduce problem to proving $x \in L$ [NP] without revealing any additional knowledge

Coin Tossing Protocol

- Want to flip a coin over the telephone
  - Fair and verifiable
  - Not subject to cheating
- Blum protocol
  - B selects $N = PQ$, $P \equiv 3 \pmod 4$, $Q \equiv 3 \pmod 4$.
  - A selects $x_1,\ldots,x_t$ and send $x_1^2,\ldots,x_t^2$ to B
  - B guesses $b_1,\ldots b_t$ and sends to A
  - A sends $x_1,\ldots,x_t$ to B and B checks $(x_i/n) = b_i$

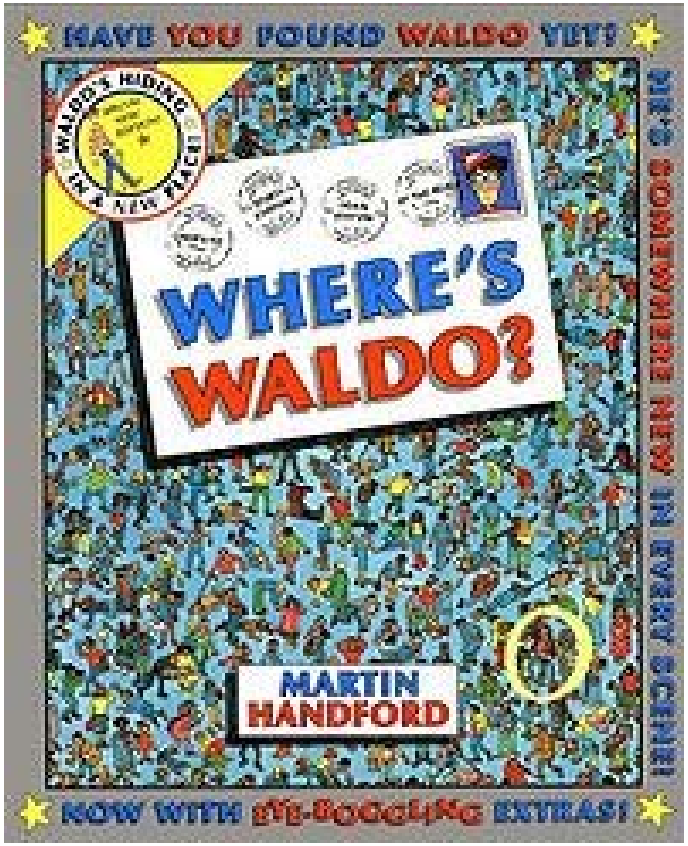
Discussion

- Cryptographic protocols are based on the secrecy of some private information and should preserve this secrecy
- The privacy gives the advantage over adversaries
- Want to prove that the secret is not given away during the protocol which might convey information derived from the secret

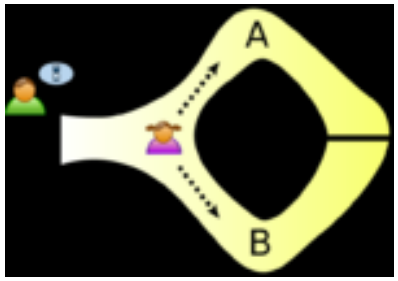
Zero Knowledge Proof

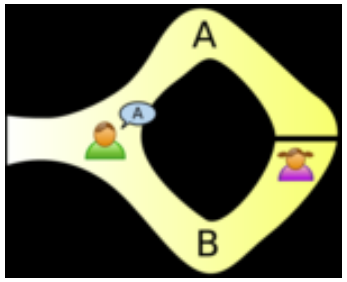
1. Completeness: if the statement is true, the honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.
2. Soundness: if the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.
3. Zero-knowledge: if the statement is true, no cheating verifier learns anything other than this fact. This is formalized by showing that every cheating verifier has some simulator that, given only the statement to be proven (and no access to the prover), can produce a transcript that "looks like" an interaction between the honest prover and the cheating verifier.

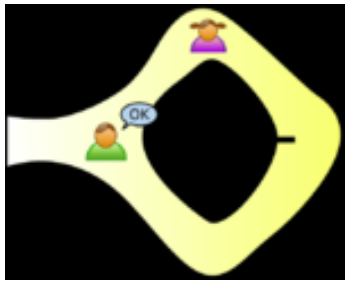
Where’s Waldo



Open Sesame







Jean-Jacques Quisquater, Louis C. Guillou, Thomas A. Berson. How to Explain Zero-Knowledge Protocols to Your Children. *Advances in Cryptology - CRYPTO '89: Proceedings*, v.435, p.628-631, 1990.

Example from GMR

- Quadratic Non-Residuosity
  - L = { x $\in$ $(Z_m)^*$: x is a quadratic non-residue}
  - Verifier generates
    - $\{r_1,\ldots,r_n\}$ random quadratic residues
    - Flips n random coins $\{b_1,\ldots,b_n\}$, $b_i \in \{0,1\}$
    - sends $\{t_1,\ldots,t_n\}$ to prover, $t_i = \begin{cases} r_i^2 \; if \; b_i = 0 \\ x \; r_i^2 \; if \; b_i = 1 \end{cases}$
  - Prover tries to determine b_i

Secure Passwords

- Every users stores a statement of a theorem in a publicly readable directory
- Upon login, the user engages in a zero-knowledge proof of the correctness of the theorem
- If the proof is convincing access is granted
- Guarantees that an adversary who overhears the proof can not learn enough to gain access

Zero Knowledge in Practice

- Trusted Platform Module
  - Secure cryptoprocessor
    - AMD, Hewlett-Packard, IBM, Infineon, Intel, Microsoft, Sun Microsystems, …
  - … Since this left unresolved privacy concerns, version 1.2 of the TPM specification introduced "Direct anonymous attestation": a protocol based on the idea of a zero-knowledge proof which allows a TPM user to receive a certification in such a way that the Privacy CA would not be able to link requests to a single user or platform, while still being able to identify rogue TPMs.