6.857 Recitation 5

Cheng Chen

March 10, 2017

1 Administrivia

Pset 2 due on Gradescope this Monday 3/13

2 t-out-of-n Secret Sharing

Goal: The dealer wants to distribute a secret s amongst $P_1, \ldots, P_n$ such that P_i has a share s_i of the secret.

1. $\geq t$ players can reconstruct s
2. $< t$ players can not

Shamir's Scheme:

1. Distribution: The dealer picks a random polynomial f of degree $t-1$ such that $f(0) = s$. He computes $s_i = f(i)$.
2. Reconstruction: Any t players can reconstruct f by applying Lagrange interpolation. They recover the secret by computing $f(0)$.

Correctness: There is a 1-to-1 correspondance between t pairs of $(i, f(i))$ and a polynomial f.

Perfect security: Say the attacker has $t-1$ shares $\{f(i)\}$ wlog. Sampling coefficients of f is equivalent to sampling $f(0), \{f(i)\}$. That is, $\forall r \Pr[s, \{f(i)\}] = \Pr[r, \{f(i)\}]$. Therefore $\Pr[s \mid \{f(i)\}] = \Pr[r \mid \{f(i)\}]$.

Shamir's secret sharing is related to error-correcting codes. In error-correcting codes, a message of length k is extended by $n-k$ 'redundant' bits. The resulting n bits are sent over a noisy channel, where the receiver might not correctly receive the value of all bits (although the order is unchanged). Then, the receiver uses the redundant information to repair the message. The original idea of Reed-Solomon codes was to oversample a polynomial of degree k at $n > k+1$ points and to use interpolation techniques to repair the message afterwards (although this view is not used in practice anymore). This is identical to Shamir Secret Sharing, but rather than reconstructing the secret from only partial information, the secret (polynomial) is used to reconstruct rest of the shares.

As a result, Shamir Secret Sharing can handle the input of 'wrong' shares, as these correspond to wrongly transmitted bits in the error-correcting code setting. However, more shares are needed in this case, which leads to the condition $t < n/3$.

Visual secret sharing? [2]

3 Meet-In-The-Middle (MITM) Attack

We've seen DES in the class. DES has key size 56 bits and block size 64 bits. The key space of DES is too small. If we want to make it more secure (larger key space), can we just encrypt the message twice with independent keys? No, MITM attack!

The Meet-in-the-Middle attack (MITM) is a generic space–time tradeoff cryptographic attack against encryption schemes which rely on performing multiple encryption operations in sequence.

Goal: chosen plaintext key recovering

$$C = Enc_{k_2}(Enc_{k_1}(P))$$

Find k_1 and k_2.

The naive algorithm is to enumerate all pairs of k_1, k_2. This takes $O(2^{2k})$ time and $O(1)$ space.

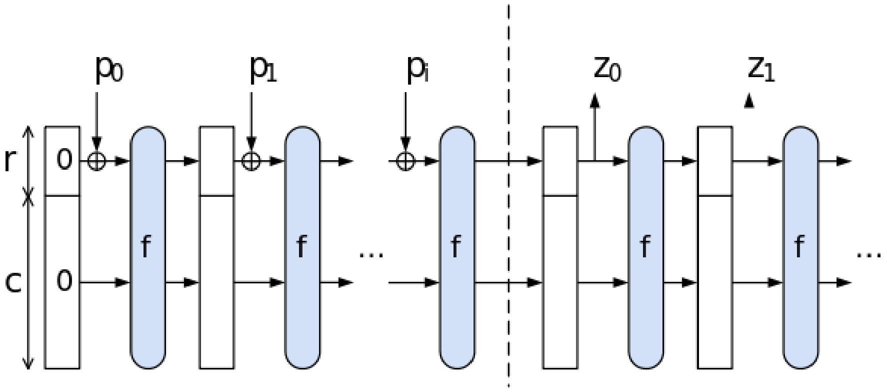
It is equivalent to find k_1, k_2 such that

$$Dec_{k_2}(C) = Enc_{k_1}(P)$$

MITM computes $Dec_{k_2}(C)$ for all k_2 and $Enc_{k_1}(P)$ for all k_1. Use a hash table to find k_1, k_2 pairs. This takes time $O(2^{k+1})$ and space $O(2^k)$.

4 Keccak (SHA3) Sponge Construction

SHA-3 uses the sponge construction in which data is "absorbed" into the sponge, then the result is "squeezed" out. In the absorbing phase, message blocks are XORed into a subset of the state, which is then transformed as a whole. In the "squeeze" phase, output blocks are read from the same subset of the state, alternated with state transformations.



- d =output hash size in bits$\in \{224, 256, 384, 512\}$
- $c = 2d$ bits
- state size= $25w$ where w =word size (e.g. $w = 64$)
- $c + r = 25w$
- $r \geq d$ (so hash can be first d bits of z_0)
- Input padding with 10*1 until length is a multiple of r
- f has 24 rounds (for $w = 64$), not quite identical (round constant)
- f is public, efficient, invertible function from $\{0,1\}^{25w} \to \{0,1\}^{25w}$

Example parameters: $d = 256, c = 512, r = 1088, w = 64$

NIST announcement controversy? [4]

5 References

1. https://www.cs.bris.ac.uk/~nigel/FHE-MPC/Lecture7.pdf
2. http://tau-crypto-f16.wdfiles.com/local--files/course-schedule/Crypto2016_12.pdf
3. https://en.wikipedia.org/wiki/Meet-in-the-middle_attack
4. https://en.wikipedia.org/wiki/SHA-3#NIST_announcement_controversy