Lecture Notes on SECRET SHARING
Exposition by Bill Gasarch

1 Introduction

Zelda has a secret s which is a string of bits. She has associates Alice and Bob. She wants to give SOME info to Alice and SOME info to Bob such that

- Alice alone has NO IDEA what the secret is (info-theoretic security).
- Bob alone has NO IDEA what the secret is (info-theoretic security).
- If Alice and Bob share their information then they can both learn the secret.

This problem can be generalized to Zelda having three friends and any TWO cannot uncover the secret, but all three CAN.

This problem can be generalized further: Zelda has n friends and if only $n-1$ share information they learn NOTHING, but if all of them get together, then they can learn.

This problem can be generalized further: Zelda has n friends and if only $k-1$ share information they learn NOTHING, but if any k get together, then they can learn. (k is some parameter.)

We will show how all of these things can be done.

2 Zelda, Alice, and Bob

We give TWO methods for Zelda to share here secret so that Alice and Bob cannot obtain is separately, but can if they work together.

2.1 Method One

Def 2.1 If b and c are bits (elements of $\{0,1\}$ then $\otimes$ (pronounced "x-or") is defined as follows

b	c	$b \otimes c$
0	0	0
0	1	1
1	0	1
1	1	0

Note that $b \otimes c \otimes c = b$.

METHOD ONE

1. Zelda's secret is a string of sits $s_1 s_2 \cdots s_L$.
2. Zelda generates a RANDOM SEQUENCE OF L sits: $a_1 a_2 \cdots a_L$.
3. Zelda computes $b_1 = s_1 \otimes a_1$,

   $b_2 = s_2 \otimes a_2$,

   $\cdots$,

   $b_L = s_L \otimes a_L$.
4. Zelda gives Alice $a_1 a_2 \cdots a_L$.
5. Zelda gives Alice $b_1 b_2 \cdots b_L$.

Alice alone has $a_1 \cdots a_L$ which is a RANDOM sequence of bits. NO information.
Bob alone has $b_1 \cdots b_L$ which is a RANDOM sequence of bits. NO information.
But if they get together then they can XOR the strings bitwise to obtain
$s_1 = a_1 \otimes b_1$
$s_2 = a_2 \otimes b_2$
$\cdots$
$s_L = a_L \otimes b_L$

2.2 Method Two

METHOD TWO

1. Zelda's secret is a string of sits $s_1 s_2 \cdots s_L$. Zelda finds a PRIME that is at least 2^L. NOW view Zelda's secret as an element $s \in \{0, 1, 2, \ldots, p-1\}$. We will do arithmetic mod p.
2. Zelda picks random $m \in \{0, \ldots, p-1\}$. Let f be the function $f(x) = mx + s$.
3. Zelda gives Alice $(1, f(1))$ and gives Bob $(2, f(2))$. Note that these are two points on the line $f(x) = mx + b$.

If Alice and Bob get together then they have two points of the line $f(x) = mx + s$. Hence they can determine the line and hence s.

Separately all they has is one point from a line. This tells them NOTHING.

3 Zelda, Alice, Bob, and Carol

We give TWO methods for Zelda to share here secret so that Alice and Bob CANNOT obtain the secret, Alice and Carol CANNOT obtain the secret, Bob and Carol CANNOT obtain the secret, BUT Alice, Bob, and Carol together CAN!

3.1 Method One

METHOD ONE

1. Zelda's secret is a string of sits $s_1 s_2 \cdots s_L$.
2. Zelda generates a RANDOM SEQUENCE OF L sits: $a_1 a_2 \cdots a_L$.
3. Zelda generates another RANDOM SEQUENCE OF L sits: $b_1 b_2 \cdots b_L$.
4. Zelda computes $c_1 = s_1 \otimes a_1 \otimes b_1$,
   $c_2 = s_2 \otimes a_2 \otimes b_2$,
   $\cdots$,
   $c_L = s_L \otimes a_L \otimes c_L$.
5. Zelda gives Alice $a_1 a_2 \cdots a_L$.
6. Zelda gives Alice $b_1 b_2 \cdots b_L$.
7. Zelda gives Alice $c_1 c_2 \cdots c_L$.

Alice alone has $a_1 \cdots a_L$ which is a RANDOM sequence of bits. NO information.
Bob alone has $b_1 \cdots b_L$ which is a RANDOM sequence of bits. NO information.
Carol alone has $c_1 \cdots c_L$ which is a RANDOM sequence of bits. NO information.
But if they get together then they can XOR the strings bitwise to obtain
$s_1 = a_1 \otimes b_1 \otimes c_1$
$s_2 = a_2 \otimes b_2 \otimes c_2$
$\cdots$
$s_L = a_L \otimes b_L \otimes c_L$.

3.2 Method Two

METHOD TWO

1. Zelda's secret is a string of sits $s_1 s_2 \cdots s_L$. Zelda finds a PRIME that is at least 2^L. NOW view Zelda's secret as an element $s \in \{0, 1, 2, \ldots, p-1\}$. We will do arithmetic mod p.

2. Zelda picks random $a, b \in \{0, \ldots, p-1\}$. Let f be the function $f(x) = ax^2 + bx + s$.

3. Zelda gives Alice $(1, f(1))$, Bob $(2, f(2))$ and Carol $(3, f(3))$. Note that these are three points on the parabola $f(x) = ax^2 + bx + s$.

If Alice, Bob, and Carol get together then they have three points of the parabola $f(x) = ax^2 + bx + s$ (we'll show how in the next section). Hence they can determine the parabola line and hence s.

Separately all they has is one point from a parabola. This tells them NOTHING.

If two of them get together all they have ae two points from a parabola. This tells them NOTHING.

4 Given Three Points on a Parabola, Find It

In the problem above we need to go from $(1, f(1))$ and $(2, f(2))$, and $(3, f(3))$ to the parabola they come from. We will do this, but note that what we do applies to ANY three points.

Since we are given $(1, f(1))$ we know that

$$a \times 1^2 + b \times 1 + s = f(1)$$

Since we are given $(2, f(2))$ we know that

$$a \times 2^2 + b \times 2 + s = f(2)$$

Since we are given $(3, f(3))$ we know that

$$a \times 3^2 + b \times 3 + s = f(2)$$

We rewrite this:

$$\begin{aligned} a + b + s = &\quad f(1) \\ 4a + 2b + s = &\quad f(2) \\ 9a + 3b + s = &\quad f(3) \end{aligned}$$

We HAVE $f(1), f(2), f(3)$ and we want to FINE a, b, s. This is three linear equations in three variables. This is a standard problem from linear algebra, and we could bring in matrices and such, but we'll just SOLVE IT as is.

We want to take the first two equations and eliminate a from it. Multiply the first equation by 4 so that we can then subtract and get rid of the a

$$\begin{aligned} 4a + 4b + 4s = &\quad f(1) \\ 4a + 2b + s = &\quad f(2) \end{aligned}$$

Subtract to get

$2b + 3s = f(1) - f(2)$

We now do the same thing with the last two equations. This will be a bit harder— we will multiply the second equation by 9 and the third by 4 (we want to avoid fractions)

$$\begin{aligned} 36a + 18b + 9s = &\quad f(2) \\ 36a + 12b + 4s = &\quad f(3) \end{aligned}$$

Subtract to get

$6b + 5s = f(2) - f(3)$

We NOW look at the two equations in b, s:

$$\begin{aligned} 2b + 3s = &\quad f(1) - f(2) \\ 6b + 5s = &\quad f(2) - f(3) \end{aligned}$$

Multiply the first equation by 3 to get

$$\begin{aligned} 6b + 9s = &\quad 3(f(1) - f(2)) \\ 6b + 5s = &\quad f(2) - f(3) \end{aligned}$$

Subtract to get
$5s = 3(f(1) - f(2)) - (f(2) - f(3))$
From this we can get s. From that we can get b and then a.

This method is quite general- given $d + 1$ points of a degree d polynomial you can set up a $d + 1$ linear equations in $d + 1$ variables and solve them to get all of the coefficients. Our job is a bit easier since all we want is the constant term s.

5 Zelda and Her n Friends

Using methods similar to those in the prior sections we COULD give TWO methods for Zelda to share her secret so that if any set of $n - 1$ of her friends get together they CANNOT obtain her secret, but if they ALL get together, they can.

6 Zelda and her Friends Alice, Bob, Carol, Donna Revisited

Zelda wants so share her secret with Alice, Bob, Carol, and Donna so that if any TWO get together they can uncover the secret, but no ONE can.

For this there is NO $\otimes$ type solution. But there is still a polynomial solution.

1. Zelda's secret is a string of sits $s_1 s_2 \cdots s_L$. Zelda finds a PRIME that is at least 2^L. NOW view Zelda's secret as an element $s \in \{0, 1, 2, \ldots, p - 1\}$. We will do arithmetic mod p.

2. Zelda picks random $m \in \{0, \ldots, p - 1\}$. Let f be the function $f(x) = mx + s$.

3. Zelda gives Alice $(1, f(1))$, Bob $(2, f(2))$, Carol $(3, f(3))$ and Donna $(4, f(4))$. Note that these are four points on the line $f(x) = mx + b$.

If any two get together they have two points of the line and they can crack it.

Any one person doesnt' have much.

This generalizes nicely- that will be a HW.