

Leaking the secret of Snow White

or “How to explain ring signatures to your children”



This story is based on “How to leak a secret” [RST06] by Rivest, Shamir and Tauman and inspired by “How to explain zero knowledge protocols to your children” [GQ89] by Guillou and Quisquater.

Text: Jan Oliver Ringert
Pictures: Various web sources,
all pictures modified

Leaking the secret of Snow White

Once upon a time in the middle of winter, when the flakes of snow were falling like feathers from the sky, a queen sat at a window sewing, and the frame of the window was made of black ebony. And whilst she was sewing and looking out of the window at the snow, she pricked her finger with the needle, and three drops of blood fell upon the snow. And the red looked pretty upon the white snow, and she thought to herself, would that I had a child as white as snow, as red as blood, and as black as the wood of the window-frame.

Soon after that she had a little daughter, who was as white as snow, and as red as blood, and her hair was as black as ebony, and she was therefore called little snow-white. And when the child was born, the queen died.

...

This is the original beginning of Snow-White's story by the brothers Grimm [GG1812]. If you have heard that tale you know what happened to Snow White. Her wicked step-mother ordered the hunter to kill her. But the hunter led her into the forest and spared her. Because of her righteousness Snow White survived and found the house of seven little dwarfs, who she lived with. The dwarfs were all very nice people and loved Snow White (as far as the brothers Grimm knew). But in fact there was a problem with one of them called Old Grumpy. He was the oldest dwarf and he did not like their new guest. It was by the way illegal for the dwarfs to have contact to humans or even hosting one at their home.

Old Grumpy knew that especially the younger and more adventurous dwarfs liked Snow White a lot and would not want to send her home. The seven dwarfs agreed to keep the existence of Snow-White secret to the Great Council of the mines.

The dwarfs had a big and well organised community with a lot of magic and technology. Only some of them lived in houses deep in the forest. The others lived in the mines way below the roots of the trees. Every dwarf was working in these mines. They normally mined for gold which they really liked a lot. Dwarfs can get very old - many hundreds of years - and all they do is dig for gold. So everything they have and everything they use is made of gold.

You wonder why this was not written in the story of the brothers Grimm? Well Snow White thought it was not important to mention all the gold. Her father was a king and she was used to eat from golden plates and drink from golden cups. So it was not as strange to her as it would be to us if everything was made of gold. She didn't even notice it.

But back to the story:

Old Grumpy wanted to find a way to tell the Great Council that there was a human living with them. But he did not want to do it directly because if the other dwarfs found out that he told their secret they would be very upset. And he did not want them to be angry at him since he was may be a little grumpy, but still liked his friends a lot.

The dwarfs normally use gophers to transmit their messages. But gophers are really unreliable and often make things up.



So if a gopher came to the Great Council and told them about a human living with some dwarfs the council would not believe it.

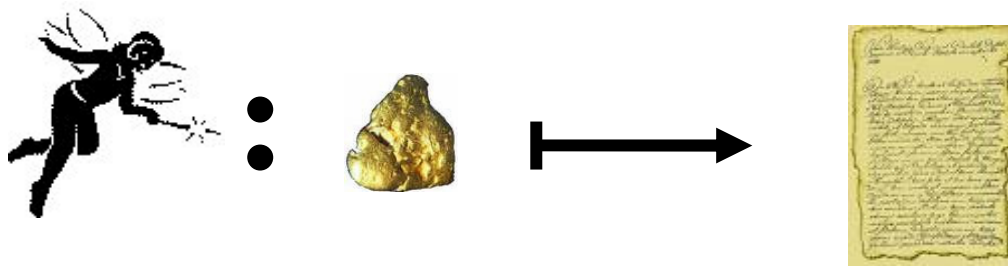
On the left you can see one of those gophers used by the dwarves.

The one in the picture is known to make up a lot of things. You better check if this tale is properly signed or he might have even made up all this.

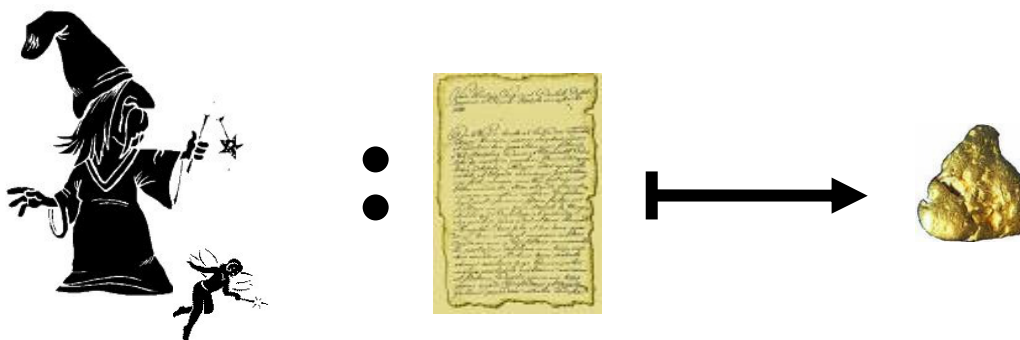
Since nobody could believe what those gophers said, the dwarfs had designed a complex system to prove that their messages were real. It was something like a signature:

The dwarfs' way to prove they sent a message

As the most common material for the dwarfs is gold, they take a big gold nugget and engrave their message on it. When they have done that, they give the gold to their private alchemist-fairy. This alchemist-fairy is a special kind of fairy. And every dwarf has exactly one of them from the day that he is born. These fairies are really important to the dwarfs and so they keep them secret. They keep them in a little bag on their belt. The brothers Grimm did not know this since it is a good kept secret of the dwarfs. What this fairy does is take the gold nugget with the message on it apart till there is only a little bit of gold dust left. The way they crumble down the nugget is their private secret and it is different from every other fairy. But to be able to reconstruct the nugget and the message they write notes how to reassemble the gold. These notes are the real messages that are transported by the gophers.



When another dwarf gets one of those notes he can call a public-chemist-wizard. They run around everywhere and when they see the note they now exactly how to reconstruct the gold nugget. The only thing they need to know is which fairy took the gold apart. If they reassemble gold taken apart by another fairy, a completely different nugget would be the result.



Since the result would be completely different for different fairies, no dwarf can forge a message and make the others believe that somebody else engraved it on the nugget.

Old Grumpy could have used this method to make the council believe that the message came from a reputable source. But then everybody could have seen that it was him who leaked the secret. It was Old Grumpy's task to create a way he could send a special message. This message should make the Great Council believe that one of the seven dwarfs sent it but should make it impossible to find out which one.

It took some time but finally he had an idea. The idea involved the legendary gold-smiths that to my mind have not been mentioned yet in history. People did not really like those guys, since they were not easy to deal with. They did excellent work at no question, but there were a few things that made working with them difficult:

- They normally take a few gold nuggets and make jewellery or ornaments out of it. They are really sensitive with their working material. That means if you give them a handful of nuggets and tell them you want something, they decide on every single nugget, how that something will look. That means, if you replace one of the nuggets you hand them, the crafts piece will look completely different.
- They are really consistent in their work. Once they find the perfect way of forging the nuggets, they will exactly reproduce that piece of art for the same nuggets. (Normally you could not give them a nugget twice. But remember that the alchemist-wizards can produce the same nugget over and over again from the same message.)



Old Grumpy once had a gold-smith forge a ring with a big diamond on it. And he remembered the fact:

- The smith was so taken by the look of the diamond that he designed the ring not only by the different nuggets, but also by the diamond. This had the effect that the smith needed one gold nugget more to finish the ring because he wanted it bigger. The gold-smith needed a nugget that exactly fit his description. He would not take any other nugget. Another nugget would not close the ring.

Finding a nugget at this special size was not really hard for a dwarf so it was ok. Old Grumpy's idea for a signature - he calls ring signature - and that satisfies his needs was:

1. Look for a diamond and write on it that Snow White stays at their house.
2. Create six random notes that look like notes created by alchemist-fairies.
3. Give those notes to an alchemist-wizard and tell him they come each from another dwarf. The wizard then produces six gold nuggets.
4. Give the diamond and the six nuggets to the gold-smith. He will then ask for a seventh nugget to finish his work.
5. Find that nugget and tell the private alchemist-fairy to produce a note as when sending a message.
6. Reconstruct a copy of the nugget and give it to the gold-smith who then finishes the ring.

The signature consists of:

- the seven notes on how to construct the nuggets
- the corresponding names of the dwarves (since the alchemist-wizard needs those)
- the diamond

To check this signature the Great council will:

1. Construct the nuggets from the notes.
2. Give the nuggets and the diamond to a gold-smith.
3. Retrieve a ring if the signature was correct or be asked by the gold-smith for a further nugget to finish the ring.

If the message was changed on the diamond, the gold-smith would be inspired another way and produce a different ring.

If somebody else tried to produce the signature whose name is not on the list, he could not close the ring – since he would not be able to construct the seventh note that looked like Old Grumpy's note. He cannot guess that note, since a little change in the note changes the outcome of the transformation to the nugget by the alchemist-wizard.

Old Grumpy was really happy that he had discovered a way to get rid of Snow White. He engraved the message to the diamond, created the ring and was getting ready to send it. The instance that the gopher appeared he heard the other dwarves scream in terror. They had

discovered that Snow White was dead. She was poisoned by an apple from her evil step-mother.

At that point Old Grumpy realized how much indeed he had come to like Snow White. During the time they all lived together, he had learned that sometimes a few changes aren't that bad. And that even humans can be nice to have around.

As you can see in the Disney's movie Old Grumpy was the one who finally led the charge to save Snow White from the wicked queen [WWW].

About this story

As I mentioned on the cover page: This story is based on "How to leak a secret" [RST06] by Rivest, Shamir and Tauman and inspired by "How to explain zero knowledge protocols to your children" [GQ89] by Guillou and Quisquater. Last semester I attended a lecture about cryptography. When I was studying for the exam, I flipped through the pages of the book written by my professor [Wät03]. I looked through his sources and saw the mentioned paper written by Guillou and Quisquater. I read it and thought it was a fun idea. About three months later I applied to hold a seminar about ring signatures. I tried to understand the ideas behind it and how it all worked. I have to give a talk on the paper [RST06] for about 75 minutes. That means I have to explain it as simple as possible (almost like explaining it to a child).

Well, why not explain it to a child? This is the reason of the creation of this paper. It cost me some hours that I better had invested in the "real" paper for my seminar :-). But ...

Further work to be done:

Rethink the whole stuff about the signatures.

Check if the combining function (gold-smith) is close enough to the original combining function:

- it is said to a permutation for each input (nugget)
- it is efficiently solvable for any missing nugget, since they lie around everywhere in the mines
- it should be infeasible to solve if the private alchemist-fairy is not at hand

The message (on the diamond) affects the permutation...

There are a lot of things to think about, but it is now about 72 hours before my talk and I only have half of the slides and no hand-outs yet.

How come I used "Snow White and the seven dwarfs" as the base of this paper?

I will answer this question by first answering another question: "How would you describe a dwarf?"

- light colour of skin (from working in the mines)
- often a full beard
- grey hair or bald

Now read those answers again carefully as the answer to another question: "What do most of the famous cryptographers look like?".

For most of them the criteria meet. But the description does not fit at all to one of the authors of the original paper “How to leak a secret”. This problem could be solved by bringing Snow White into the story.

I am just curious: “Did you even notice that the cover picture was not taken from the original Disney’s movie? In fact: I modified it!”

Cast

Snow White	Yael Tauman
Dwarf 1	Leonard Adleman
Dwarf 2 (sleeping)	Adi Shamir
Dwarf 3	Michael O. Rabin
Dwarf 4	Whitfield Diffie
Dwarf 5	Ronald Rivest
Dwarf 6	Martin Hellman
Dwarf 7	Ralph Merkle
Gopher	Jan Oliver Ringert
Gold smith	Automatix

Dwarfs numbered from left to right.

Sources

- [RST06] R. Rivest, A. Shamir, and Y. Tauman
“How to Leak a Secret: Theory and Applications of Ring Signatures.”
- [GQ89] Guillou, Quisquater
“How to Explain Zero-Knowledge Protocols to Your Children”
- [GG1812] J. Grimm, W. Grimm
“Snow White and the Seven Dwarfs”
(<http://www.cs.cmu.edu/~spok/grimtmp/042.txt>)
- [WWW] Disney,
Explanation of the characters of the seven dwarfs (1937)
(<http://disney.go.com/vault/archives/characters/sevendwarfs/sevendwarfs.html>)
- [Wät03] D. Wätjen
„Kryptographie. Grundlagen, Algorithmen, Protokolle.“