Zero-Knowledge Made Easy So It Won't Make You Dizzy

A Tale of Transaction Put in Verse
About an Illicit Kind of Commerce

This is an extended version of:
http://link.springer.com/chapter/10.1007%2F978-3-319-44618-9_10

PART I: Warm-up

A Poetical Revenge on Diffie-Hellman Key Exchange

A big mistake on author's side:
This talk includes no outline slide!

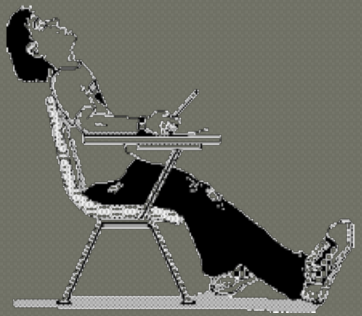
1. Introduction & Motivation

Teaching cryptography can be so boring
That one can hear students snoring
To verify this claim and see
Try introducing them to public key

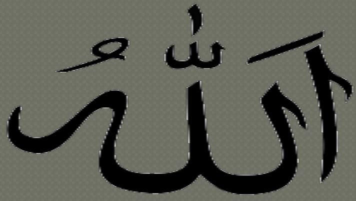
Before we delve into this lecture
We need to first make a conjecture
Perhaps the boredom is caused
By dominance of sleep-inducing prose
We thus attempt to keep the audience alert
By rhymes to which we protocols convert

We start with Diffie-Hellman protocol
Which is by far the simplest one of all
In this description, it isn’t very terse
Since it’s presented entirely in verse

NOTE: As we forward bravely plow
The rhyming tempo changes now

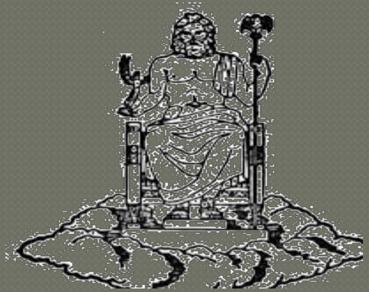


2. The Protocol



2.1 Setup:

Before our Earth was ever trod
Large prime p was picked by God
And if you're a godless atheist
Assume that p was picked by NIST



In the protocol you'll see
All computations are mod p
Then, a generator g was chosen
And thereafter both were frozen

NIST

2. The Protocol (contd.)

2.2 Interaction:

Alice, one of fairer sex,
Computes g to random X
Bob – a sketchy kind of guy
Raises g to chosen Y

Clock synchronization loose
They exchange the residues
Not to spoil all the fun…
But, that's the end of round one

Alice, feeling a bit high
Computes g^X to the Y
Armed with his secret, next
Bob raises g^Y to the X
Now for both the time is ripe
To bootstrap a secure pipe

3. Correctness & Security

$(g^X)^Y$

$(g^Y)^X$

3.1 Correctness

To see that Diffie-Hellman works
Even between two total dorks
Consider that both Bob and Alice
Wind up computing equal values

3.2 Security

A passive eavesdropper can see
How they obtain the shared key
But even best computing toys
Can't help distinguish it from noise

Alas, this claim's no longer true
When adversary changes hue
If Eve adopts an active role
We have a broken protocol

***PART II:** The Real Thing*

ABSTRACT

For any research paper, as all the authors know
An abstract is required to keep the proper flow
An abstract is a lure that must be appetizing
It's typically smeared with shameless aggrandizing

Which brings us to the subject of our seminal result
Its impact on the Zeitgeist will alter the Gestalt
This noble work is prompted by dominance of prose
The reason crypto papers make readers comatose

This paper makes an effort to change the status quo
By showing that crypto poetry is another way to go

1. Introduction

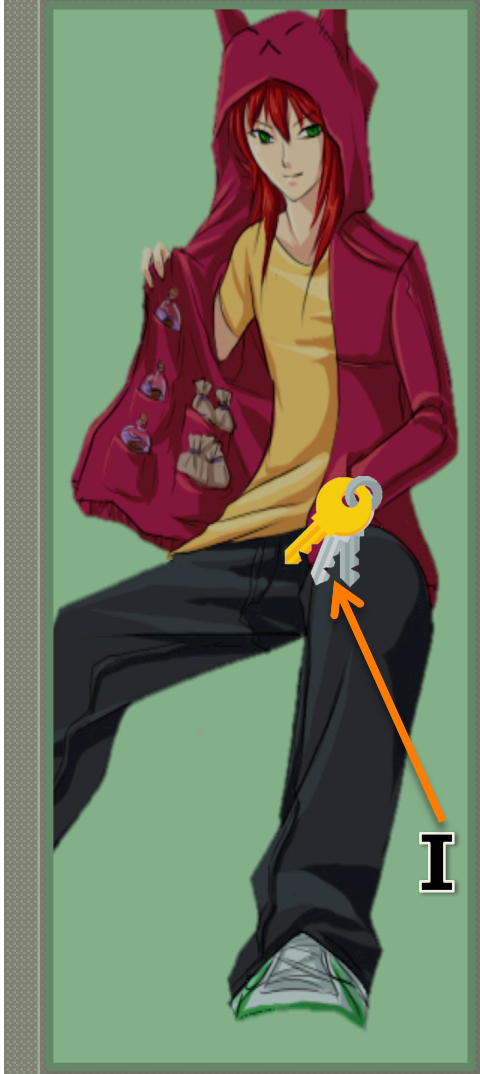
Whoever reads these lines shall have no fear
This rhyming opus will explain Fiat-Shamir
The tricky concept known as Zero Knowledge
Will be as easy to digest as oatmeal porridge
So, now read on and keep one thing in mind
That tortured rhymes are difficult to find

2. Setup & Preliminaries

Computed safely, back in ancient times
Is number N – a product of two primes
About its origin there isn't much to say
Assume (or pray) that it was not the NSA

To make the protocol description very clear
All computations are mod N in Fiat-Shamir

2.1 The Cast

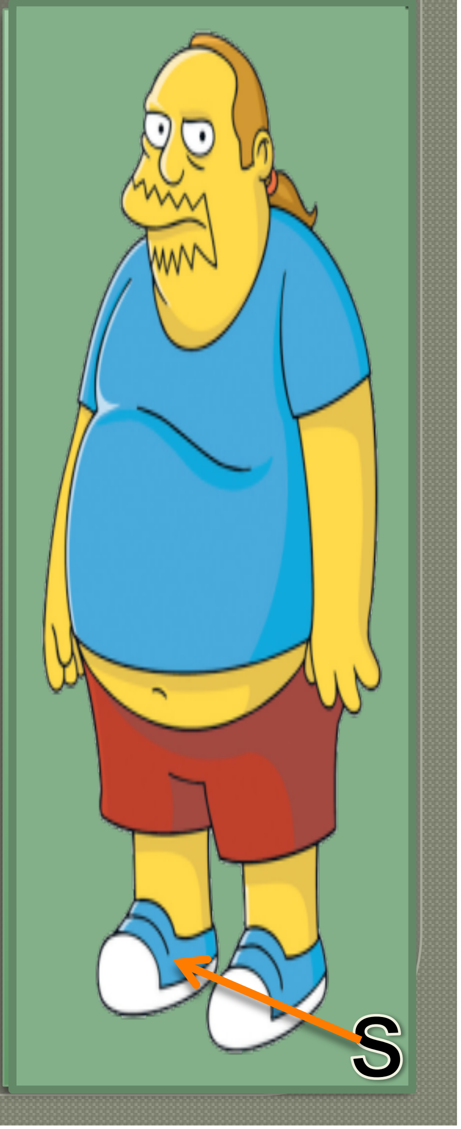


The protocol involves a dweeb, called Bob
A lazy, nerdy and socially-awkward slob
Like many of his bored and geeky kind
Bob smokes a lot of weed to numb his mind

His dealer, Alice, is crafty trailer trash
Who offers pot, ecstasy, and high-grade hash
Like any merchant wanting customers' respect
She has integrity and stature to protect
For each transaction, Alice wants her client
To be completely Fiat-Shamir-compliant

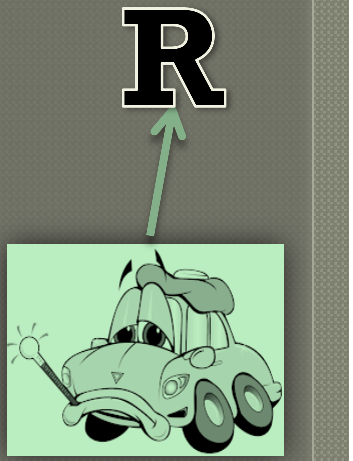
2.2 Assumptions

To circumvent some simple online dangers
Suppose that Bob and Alice aren't strangers
Thus, we assume that I – Bob's ID string
Already hangs on Alice's public-key ring
Meanwhile, its secret square root, called S
Bob had tattooed on his right foot, no less
NOTE: Due to consuming large quantities of pot
Bob's long-term memory is unfortunately shot

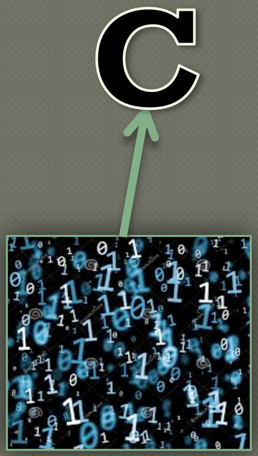


3. Interaction

The online phase begins with round one
When Bob's supply of cannabis is gone
Sneezing and coughing like a decrepit car
Bob generates a random number we'll call R
Squaring it mod N yields a value X
Which he then sends to Alice all in hex



Having received and stored X, she is content
Since there is merchandise for her to vend
Next, from her private random numbers pit
Alice selects a brand new challenge bit
It is referred to as C from here on
She forwards it to Bob over the phone



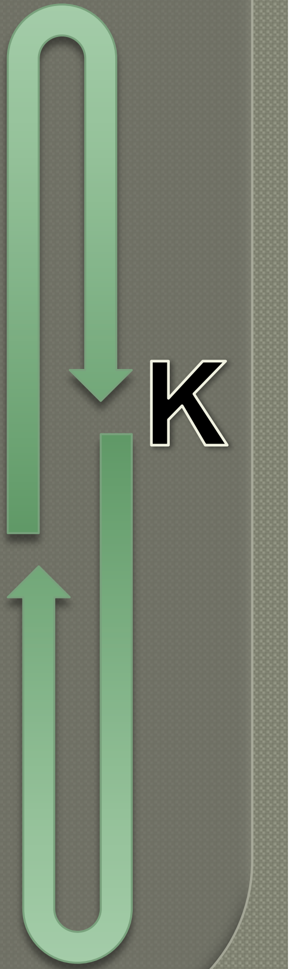
In round three, Bob readies his reply
Of course, it must on challenge C rely
Accordingly, it's R if C is zero,
Else, R times S is sent by our hero

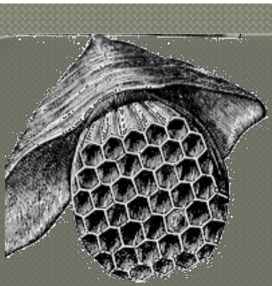
3. Interaction (contd.)

For C of zero, Alice squares the reply and checks
Whether it matches Bob's prior commitment X
She otherwise compares X times I
With square mod N of Bob's previous reply

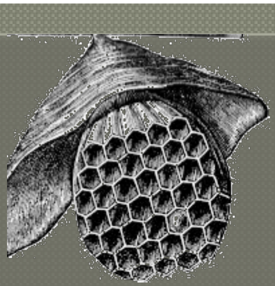
Should she encounter any kind of error
Alice drops everything and runs away in terror
For this behavior, there is a solid reason:
She simply doesn't want to land in prison

Assuming all goes well, it should be clear
That much remains to do in Fiat-Shamir
Though it is fast, simple and discrete
There is a 50-50 chance that Bob can cheat
Thus, online phase must be re-run K times
Because of difficulty of coming up with rhymes





4. Epilog



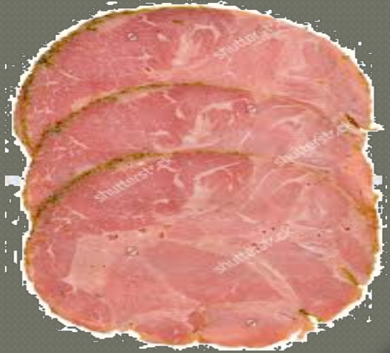
Once the transaction is finally complete
Both parties hurry to get off the street
The dealer Alice now proactively decides
That time is right to re-stock the merchandise
Eager to sample freshly purchased hash
Bob rushes home while clutching his new stash

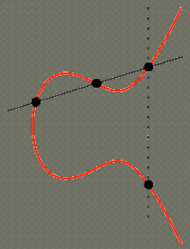
5. Security Proof (Sketch)

This is a mere sketch, no need to get excited
A real proof, as usual, will never be provided
As for security, there is but one direction
It's plainly evident by cursory inspection

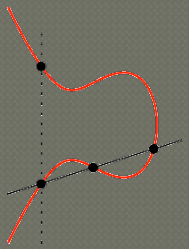
6. Related Work

While feeling pride and yet not seeking fame
Having explored the literature, we claim
That this attempt at crypto-poetry is first
Which might result in stirring up a hornet's nest
Thus triggering a crypto-lyrical tsunami
Which sadly rhymes only with pastrami





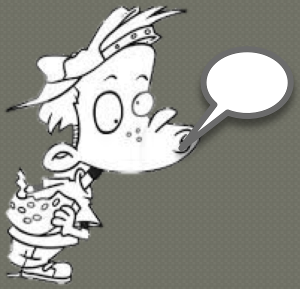
7. Future Work



Before tapping this poem with a verbal cork
We summarize directions for the future work

俳句

Our research isn’t finished and much is left to do
For instance, proving theorems completely in haiku
Devising crypto protocols for alpine cows to yodel
That are proven secure in the standard crypto model



How to take advantage of symmetric crypto tricks
To build one-way functions that spit out limericks
How to create lyrics, music and dance moves
That praise the shapely beauty of elliptic curves

These are just examples and challenges abound
For any eager student open problems can be found

8. Conclusions

This paper demonstrated with obvious finesse
The awesome teaching power of pithy crypto-verse
Our research took advantage of a lucky trick
By picking Fiat-Shamir as its guinea pig

In sheer simplicity this method has no peer
Even a total idiot can comprehend Fiat-Shamir
To understand it, there's no need to go to college
Its only purpose is advancing Zero Knowledge

We've reached the end and it's time for a beer
Let's drink at least K rounds as in Fiat-Shamir
And if we drink too much and feel a bit delirious
Everyone we meet should be honest-but-curious

9. Disclaimer & Acknowledgments

Despite severe pressure from his poetic muse
The author of this poem doesn't advocate drug use
This literary effort was made possible in part
By generous funding from Endowment for the Art
We finally acknowledge, with self-important flair
Helpful comments by reviewers and the Program Chair