A Cryptographic Solution to the Problems of Social Dating

Orr Dunkelman

Faculty of Mathematics and Computer Science
Weizmann Institute of Science
P.O. Box 26, Rehovot 76100, Israel
orr.dunkelman@weizmann.ac.il

Abstract. One of the problems encountered by many couples in today's social dating world is the issue of commitment. This problem arises whenever one of the involved persons is willing to commit to a long term relationship, while the other person is not yet willing to commit to the same goal.

In this short note we show a simple craptographic solution to the problem, that we believe may reduce the issue of this problem significantly, and would allow today's couples to address more burning issues, namely, whether the toilet seat should be always left in the sitting position.

1 A Quick Introduction

In a recent survey held in the EU, it was found out that many young couples find themselves in a vicious (and famous) deadlock. This deadlock follows the fact that at some point of time, one of the members of the couple feels that he (or she) is willing to commit to the relationship (e.g., moving to live under the same roof, getting married, bringing kids to the world), while the other person is still not willing to commit to the same action.

This problem is extremely acute in instances where the person who is still unwilling to commit, remains indecisive for a long period of time. As the person willing to commit is usually disappointed with the lack of commitment from the unyielding person, this gap is usually very stressful for the relationship, and may even lead to the (quite expected) end of the relationship.

In this work, we suggest a solution to the problem, and prove its completeness under the Diffie-Hellman gap. The suggested construction is both efficient and easy to follow, and from experiments we conducted on 100 lab rats, have extended the length of relationships by a factor of π (mostly because the rats were trying to understand why their partner was discussing cryptography with them).

2 Notations

In this paper we use the following notations:

- $\mathcal{A}$ — stands for Alex, who is willing to commit,

- $\mathcal{B}$ — stands for the partner of $\mathcal{A}$ who has commitment issues, and cannot really see how wonderful $\mathcal{A}$ is.
- $\mathcal{C}$ — $\mathcal{A}$'s friend who has a secret crush on $\mathcal{A}$, and waits for $\mathcal{A}$ to throw $\mathcal{B}$ out the windows, so he (or she) could date $\mathcal{A}$.
- $\mathcal{D}$ — the normal distribution (also referred to as $\mathcal{N}(0,1)$).

3 The Proposed Solution

Our proposed solution is quite simple. Once $\mathcal{A}$ reaches the level that he (or she) is willing to commit to $\mathcal{B}$, then $\mathcal{A}$ announces this to $\mathcal{B}$. At this point usually one of three scenarios is unfolded:

- $\mathcal{B}$ announces his (or her) eternal love to $\mathcal{A}$, leading to a happy relationship, and an increase in the expected revenue of divorce lawyers in $\mathcal{A}$ and $\mathcal{B}$'s country (of about 33% of the expected cost of a divorce).
- $\mathcal{B}$ feels threatened by the show of feelings from $\mathcal{A}$, and as he (or she, even though, it is usually he) thought that the main purpose of the relationship was to hang around in $\mathcal{A}$'s apartment and watch cartoons, runs away screaming.
- $\mathcal{B}$ enters a catatonic shock and retreats from the world for a period of time which is distributed according to $\mathcal{D}$.

Of course, none of these scenarios may use our solution. But in the rare case where $\mathcal{B}$ may be willing to commit at the future, he (or she) invokes the following craptographic commitment schemes:

1. $\mathcal{B}$ picks a large prime number p at random and a generator g of Z_p^*.
2. $\mathcal{B}$ picks a string x, which is related to the commitment (the human commitment) in a manner we describe below.
3. $\mathcal{B}$ computes a commitment $c = g^x \bmod p$ and offers this as the craptographic commitment to $\mathcal{A}$.

The string x is of course the secret of this commitment, and it is to be chosen according to the related human commitment at hand. For example, if the discussed commitment is marriage, then x is chosen to be a date, a location, and the number of attendees in the ceremony (and where applicable, the length of the reception, and whether formal dress code is required). When the discussed commitment is bringing a child to the world, then x obviously contains a list of agreed names to the newborn. It is left as an exercise to the reader to define x for other commitment issues.

At this point $\mathcal{A}$ has received what is known as a *weak commitment*, i.e., a proof that $\mathcal{B}$ may consider a real commitment later, but that $\mathcal{B}$ believes that he (or she) will offer the full commitment in the future, thus bridging the gap between the expectations of $\mathcal{A}$ and $\mathcal{B}$ from the relationship.

To open the commitment, there are two possible scenarios:

- $\mathcal{B}$ comes to his (or her) senses, and identifies $\mathcal{A}$ either as the best thing that ever happened to him (or her) or not. In the first case, $\mathcal{B}$ reveals his (or her) secret string x, and the commitment is done. In the latter, $\mathcal{A}$ is devastated, and may have a rebound relationship with $\mathcal{C}$, just to find out that $\mathcal{C}$ was advising at the same time to $\mathcal{B}$ to leave $\mathcal{A}$ [2,3].
- $\mathcal{A}$ succeeds to solve the commitment, i.e., to find an x' such that $c \equiv g^{x'} \bmod p$. In this case, $\mathcal{A}$ learns on $\mathcal{B}$ intentions, and may decide to end the relationship as the bastard was willing to get married only in 2100, or as once reported "when hell freezes over". On the other hand, such a success can show that $\mathcal{A}$ can read the mind of $\mathcal{B}$, proving that this pairing should take place, thus encouraging $\mathcal{B}$ to offer a true commitment.

4 Security

The security of the proposed solution is mostly based on the gap between $\mathcal{A}$ and $\mathcal{B}$. For example, if $\mathcal{A}$ has access to the computer used by $\mathcal{B}$ to generate the commitment, he (or she) can use this access to reveal x without putting too much effort into the problem. This is obviously a weakness of the human relationship model, and it has to be addressed in a wider framework of universal compostability, which we leave as an open problem.

Going back to the security of the proposed solution, one can easily see that as long as there is a gap between Diffie and Hellman, they cannot come together to think about how to help $\mathcal{A}$ solving the challenge. Of course the use of algorithms like baby-step-kid-step-adolescent-step should be used only when the commitment required is about bearing kids.

5 Possible Extensions

In some scenarios $\mathcal{A}$ may wish to produce a weak commitment himself (or herself). In this case, $\mathcal{A}$ may still feel the lack of a similar action from $\mathcal{B}$ is as devastating as in the case of a true commitment. Hence, $\mathcal{B}$ can offer a *weaker commitment*, which is a commitment to the event of giving a weak commitment (where x is the date of giving that weak commitment). Of course, $\mathcal{A}$ may wish to offer the same weaker commitment first, for which, $\mathcal{B}$ must offer the *even weaker commitment*, and so forth.

In some scenarios, the above protocol becomes a multiparty protocol. For example, if $\mathcal{B}$ has a secret affair with $\mathcal{A}_1$ who awaits the moment $\mathcal{B}$ ditches $\mathcal{A}$ in his (or her) favor. In such a case, $\mathcal{B}$ is required to give both $\mathcal{A}$ and $\mathcal{A}_1$ the same commitment, stating the date of choosing between the two. Of course, $\mathcal{B}$ may choose to give two different commitments which collide, hence, offering a collision attack between the commitments. While a simple Weil pairing can be used to solve the case of $\mathcal{A}$ and $\mathcal{A}_1$, following Joux's multicollision attack, we are afraid that the multiple problem of s entities $\{\mathcal{A}_i\}$ (for $i = 1, \ldots, s$), requires the use of stronger mathematical assumptions.

For example, it is well known that in order to have three $\mathcal{A}_i$, $\mathcal{B}$ must use untraceable operations (as otherwise, $\mathcal{A}_1$ may learn on the existence of $\mathcal{A}_2$). The assumptions needed to prove the security (and the safety) of $\mathcal{B}$ in these settings are still under research (e.g., [1]).

Another potential research direction concerns the lack of hiding in our proposed commitment scheme. Namely, if $\mathcal{A}$ suspects that the commitment he (or she) has received from $\mathcal{B}$ has something to do with their future marriage, he (or she) can verify that it does not include statements of the form "On (date) I shall choose between $\mathcal{A}$ and $\mathcal{A}_1$ according to a coin flip". Given the fact that love should be blind as well, it seems extremely important to blind the commitments themselves, thus preventing such weaknesses.

Finally, we note that commitments related to moving in together must take into consideration the "key exchange" problem that must ensue if $\mathcal{A}$ moves in with $\mathcal{B}$ (or vice versa). In some cases, this key exchange takes place before any commitment phase, which ensures both the hardness of the protocol, as well as its completeness (if only $\mathcal{A}$ gives a key to $\mathcal{B}$, one can only assume what will happen to the relationship in the presence of $\mathcal{C}$).

6 Concluding Remarks

Modern times lead to modern problems. This can be seen by the fact that the problem studied in this note did not exist 100 years ago, where a different pairing model was used. As it is easier to travel and meet more candidates for social dating, the problem of random pairing has become important.

It is worth mentioning that following recent trends, future researchers will have to incorporate a three-way commitment scheme (between $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ who started recently to find $\mathcal{B}$ attractive), or even the general problem of multi-party dating protocols.

Acknowledgements

We would like to thank the following people for their constructive remarks and fruitful discussions: Dan and Tanja Lange and Bernstein, Claudia Diaz, Sebastiaan Indesteege, Raphael C.-W. Phan, Nigel Smart, Diffie and Hellman, and Rivest, Shamir and Adelman.

References

1. Bogetoft, P., Christensen, D.L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J.D., Nielsen, J.B., Nielsen, K., Pagter, J., Schwartzbach, M.I., Toft, T.: Secure Multiparty Computation Goes Live. In Dingledine, R., Golle, P., eds.: Financial Cryptography. Volume 5628 of Lecture Notes in Computer Science., Springer (2009) 325–343

2. Lamberger, M., Mendel, F., Rechberger, C., Rijmen, V., Schläffer, M.: Rebound Distinguishers: Results on the Full Whirlpool Compression Function. In Matsui, M., ed.: ASIACRYPT. Volume 5912 of Lecture Notes in Computer Science., Springer (2009) 126–143
3. Mendel, F., Rechberger, C., Schläffer, M., Thomsen, S.S.: The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl. In Dunkelman, O., ed.: FSE. Volume 5665 of Lecture Notes in Computer Science., Springer (2009) 260–276