Secure Cloud Computing for Medical Data

Daniel J. Bernstein, Carl Ellison, Tanja Lange, Kristin Lauter, Victor Miller,
Michael Naehrig, and Eran Tromer

Abstract. We answer a recent challenge by Benaloh, Lauter, Horvitz, and Chase [1] concerning patient privacy in electronic medical records. Our approach offers strong privacy and confidentiality, and enables autonomous delegation of priviliges in a distributed setting. We instantiate our constructions using the recent results of Gentry [4] via a framework already known in the early sixties [3].

1 Introduction

C G C G

2 Lyrics

```
C                                              G
Does your doctor know the full importance of encryption?
G                                 G7           C
If your data were revealed you'd suffer a conniption.
C                                   C7                  F
But now you can prevent him from disclosing your prescription
F               C                 G             C
with fully homomorphic lattice-based secure encryption!

C                        G
Um diddle diddle diddle, um diddle ay.
C                        G
Um diddle diddle diddle, um diddle ay.

C                                          G
Fully homomorphic lattice-based secure encryption
G                                   G7         C
pulls together several keys in layers for ignition.
C                                   C7         F
Then wraps itself recursively with clever repetition.
F                   C           G                C
Other steps are evident - who needs good exposition?

C                        G
Um diddle diddle diddle, um diddle ay.
C                        G
Um diddle diddle diddle, um diddle ay.
```

```
C                                                   G
Cloud computing lets you spread your data with precision,
G                                   G7              C
Merging different servers: German, Welsh, perhaps Egyptian.
C                                       C7                F
But when you finally run the scheme you end up with frustration.
F             C               G          C
Doing just 2 bits per round limits the adoration.

C                        G
Um diddle diddle diddle, um diddle ay.
C                        G
Um diddle diddle diddle, um diddle ay.

C                                          G
Fully homomorphic lattice-based secure encryption
G                           G7           C
pulls together several keys in layers for ignition.
C                                  C7       F
Then wraps itself recursively with clever repetition.
F               C              G               C
Other steps are evident - who needs good exposition?
```

3 Acknowledgement

We are grateful to the numerous anonymous craptologous reviewers, the anonymous chairs of the Crapto 2009 Rump Session for giving us the opportunity to present our anonymous craptologic work in authentic unanonymous craptologic environment [2]. We also thank the anonymous cinematographers, who cinematographically preserved our craptographic research presentation [2], as well as the International Association for Craptologic and Cinematographic Research (IAC^{2}R) for making the video of our presentation [2] available for the public, and in particular for future cinematographic and craptologic research.

References

1. Josh Benaloh, Melissa Chase, Eric Horvitz, and Kristin Lauter. Patient controlled encryption: ensuring privacy of electronic medical records. In *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 103–114, New York, NY, USA, 2009. ACM.
2. Daniel J. Bernstein, Carl Ellison, Tanja Lange, Kristin Lauter, Victor Miller, Michael Naehrig, and Eran Tromer. Secure cloud computing for medical data, 2009. Presentation at Crypto 2009 Rump Session, `http://www.iacr.org/conferences/crypto2009/videos/27_Rump_Session_Part_3.html`, at 1:07:30.
3. The Sherman Brothers. Supercalifragilisticexpialidocious. In *Mary Poppins*. Walt Disney, 1964.
4. Craig Gentry. Fully homomorphic encryption using ideal lattices. In *STOC '09: Proceedings of the 41st annual ACM symposium on Theory of computing*, pages 169–178, New York, NY, USA, 2009. ACM.