Secret Sharing Protocols -Publicly Verifiable Secret Sharing with applications

Christopher Foley

Outline

- History
- General Model
- Publicly Verifiable Secret Sharing
- Applications

Disclaimer

- Lots of things in this fields
- Originally wanted to work with Stinson and Wei's paper
- Then Stadler
- Then Gan, et al.
- Then Wu & Tseng
- If I had 2 more weeks then I'd probably do Jeppsen & Lemming (Voting) or probably Chen, et al. (Executing wills online)

History

- 1979 – basic secret sharing schemes proposed
  - Assumed all participants honest
- 1987 – Feldman proposed first Verifiable secret sharing (VSS)
  - Allowed participants to verify their shares but not others
- 1996 – Stadler introduced first Publicly Verifiable Secret Sharing (PVSS)
  - Verify shares held by any participant without revealing own shares

History

- Elliptic Curves
  - Weil pairing in 1993
  - Joux – identity based encryption, signature algorithm (2000)
- Pairing Based cryptography
  - Signatures (2002)
  - Key agreement protocols (2002)
  - Signcryption algorithms (2005)

General Model of PVSS

- Three Phases
  - Initialization phase
  - Distribution Phase
  - Reconstruction Phase

General Model of PVSS

- Initialization Phase
  - All public parameters, private and public keys generated
  - Dealer and Participants Identified

General Model of PVSS

- Distribution Phase
  - Distribution of the shares: Dealer uses participants public keys and public parameters to compute values and the share of the secret to the participants
  - Verification of the shares: Any share may be verified by any party. If all shares are verified then the parties believe that the shares contain the secret and the dealer is uncorrupted. If any share fails, the dealer is corrupted and the scheme aborts.

General Model of PVSS

- Reconstruction:
  - Decryption of shares: participants use private key to decrypt share
  - Reconstruct secret: The secret may be reconstructed from some of the participants.

Pairing-Based PVSS

- $\{U_1, U_2, \ldots, U_n\}$ are participants
- The Dealer, D, wishes to distribute a secret to the participants

Pairing-Based PVSS

Initialization Phase

- The key generation system generates the public parameters $Param=\{G_1,G_2,q,c,P,P_{pub},H\}$
- Each participant chooses a private key $\alpha_i \in \mathbb{Z}_q$ and computes the Public key $P_i=\alpha \cdot P_{pub}$ for i=1..n

Pairing-Based PVSS

Distribution Phase

(Decryption of the shares)

- The dealer chooses a random polynomial

$$f(x) = c + \sum_{j=1}^{t-1} c_i x^j$$

Of degree *t-1* with coefficients in $\mathbb{Z}_q$

Pairing-Based PVSS

Distribution Phase

(Decryption of the shares)

- The dealer selects random numbers $r_i \in \mathbb{Z}_q$
- The dealer then computes $C_j = c_j \cdot P$, $X_i = f(i) \cdot P$, $Y_i = c(P_i, P_{pub})^{f(i)}$, $\alpha_i = r_i \cdot P$, $\beta_i = r_i \cdot P_i$, $h_i = H(P_i, X_i, Y_i, \alpha_i, \beta_i)$, $\gamma_i = (r_i + h_i \cdot f(i)) \cdot P_{pub}$ *for* $j=0,1,..,t-1$ *and* $i=1..n$

Pairing-Based PVSS

Distribution Phase

(Decryption of the shares)

- The dealer then publishes all C_j and $\sigma_i=(Y_i,\alpha_i, \beta_i, \gamma_i)$ to all participants.
- Note: each X_i can be reconstructed from:

$$X_i = f(i)\cdot P = \sum_{j=0}^{t-1} c_j(i^j)\cdot P = \sum_{j=0}^{t-1} (i^j)c_j\cdot P = \sum_{j=0}^{t-1} (i^j)\cdot C_j$$

Pairing-Based PVSS

Distribution Phase

Verification of the shares

- Participants recover $X_i = \sum_{j=0}^{t-1} (i^j) \cdot C_j$ then checks two equations:

$$c\left(P, \sum_{t=1}^{n} \gamma_i\right) = c\left(P_{pub}, \sum_{i=1}^{n} \left(\alpha_i + h_i \cdot X_i\right)\right)$$ and

$$\prod_{t=1}^{n} c\left(P_i, \gamma_i\right) = c\left(\sum_{t=1}^{n} \beta_i, P_{pub}\right) \cdot \prod_{i=1}^{n} Y_i^{h_i}$$

Pairing-Based PVSS

Distribution Phase

Verification of the shares

- If these checks do not fail, the participants may assume that the shares distributed by the dealer are uncorrupted.

Pairing-Based PVSS

Reconstruction Phase

Decryption of shares:

- Each participant uses their private key to decrypt their share

$$Y^{\alpha_i^{-1}} = c\left(P_i, P_{pub}\right)^{f(i)\alpha_i^{-1}} = c\left(\alpha_i P_{pub}, P_{pub}\right)^{f(i)\alpha_i^{-1}} = c\left(P_{pub}, P_{pub}\right)^{f(i)} = S_i$$

Pairing-Based PVSS

Reconstruction Phase

Interpolation

- Any t shareholders U_i with shares S_i may join to reconstruct the secret

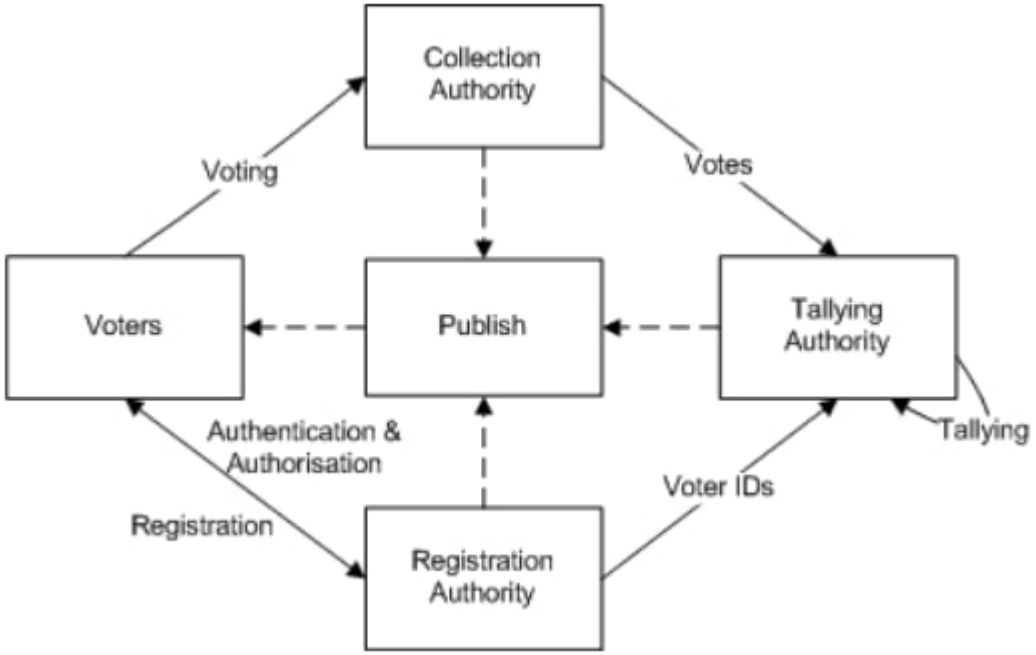
$$\prod_{i=1}^{t} S_j^{\lambda_i} = c\left(P_{pub}, P_{pub}\right)^c, where\ \lambda_i = \prod_{i \neq j} \frac{i}{j-1}$$

Applications Overview

- PVSS has had numerous applications discussed in literature
  - Key/Code Escrow systems
  - Commerce
    - Anonymous cash exchange
  - Signature authentication
  - Revocable authority
  - Electronic voting
  - Authentication of Last Will and Testament

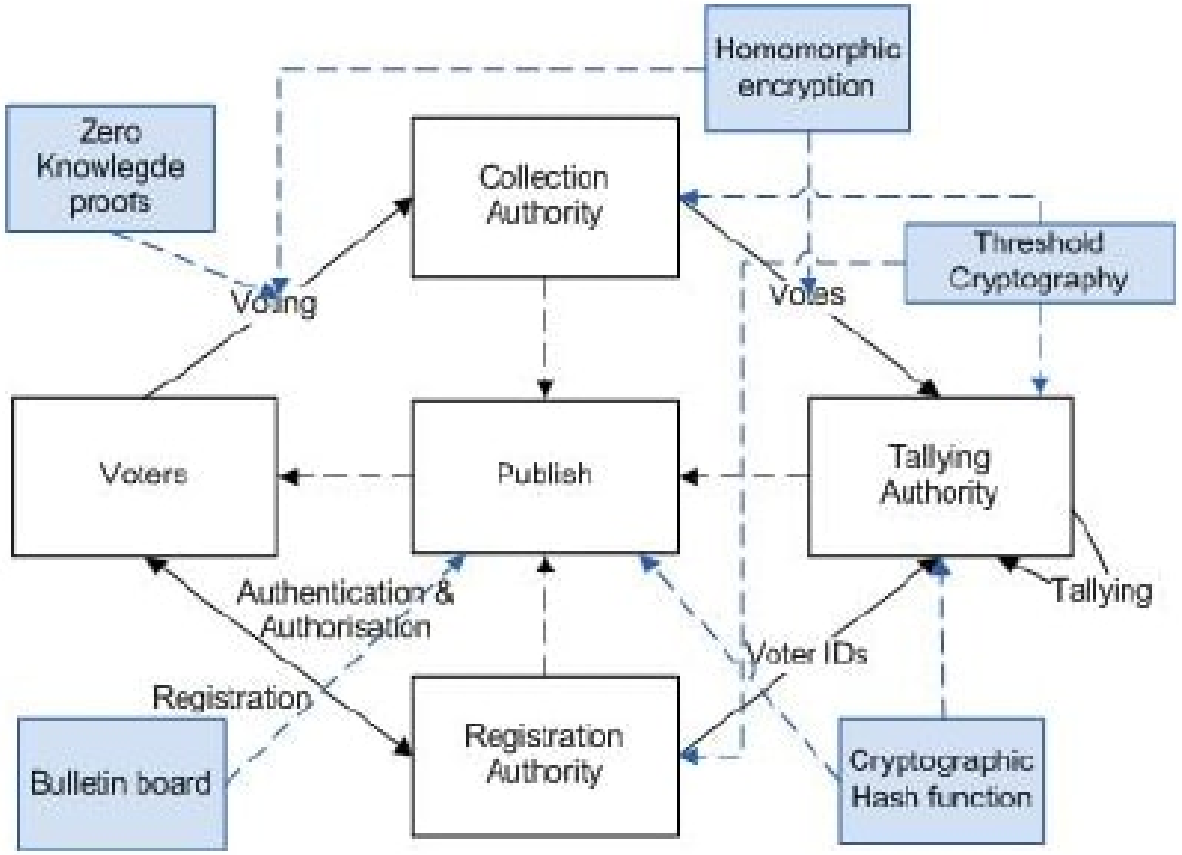
Applications - Electronic Voting

- Secure
- Anonymous
- Verifiable



S. Jepsen, K. Lemming. *Electronic Voting Application Based on Public Verifiable Secret Sharing.* Masters Thesis, Department of Mathematics, Aalborg University, 2016

Applications – Electronic Voting

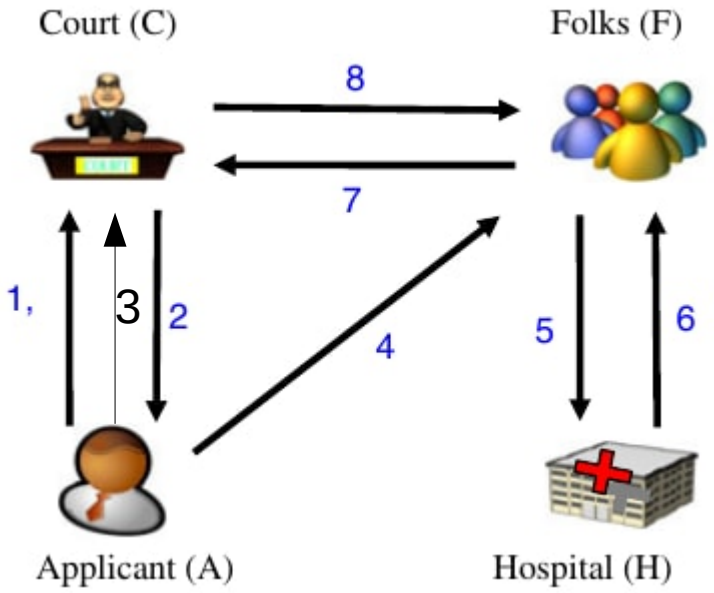


S. Jepsen, K. Lemming. *Electronic Voting Application Based on Public Verifiable Secret Sharing.* Masters Thesis, Department of Mathematics, Aalborg University, 2016

Applications – Electronic Wills

- Electronically Sealed wills
- Publicly verifiable
  - Probate Court
  - Testator/ix
  - Heirs
- Self proving
- Revocable

Applications – Electronic Wills



1. Applicant creates registry
2. Court approves registry
3. Applicant sends share to court
4. Applicant distributes shares
5. After death heirs get certificate
6. Death certificate
7. Shares and certificate to court
8. Will reconstructed.

Applications

- PVSS is a growing field with opportunities.
- PVSS has a number of applications being developed (2011) including:
  - Key Software Escrow
  - Electronic Cash

References

- M. Nojoumian, Lecture Notes, COT6427 Secret Sharing Protocols, Florida Atlantic University, Spring 2018
- B.Chor, S. Goldwasser, S. Micali, B. Awerbuch. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. *Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science (FOCS),* pp. 383-395, 1985
- M. Stadler. Publicly Verifiable Secret Sharing. U. Mauer(Ed.) *Advances in Cryptography – EUROCRYPT '96, LNCS 1070,*
- S. Jepsen, K. Lemming. *Electronic Voting Application Based on Public Verifiable Secret Sharing.* Masters Thesis, Department of Mathematics, Aalborg University, 2016
- T. Wu, Y. TSENG. *A Pairing-Based Publicly Verifiable Secret Sharing Scheme,* Journal of Systems Science & Complexity, Feb 2011 24:186-194
- Anna Nicole Smith image by Toby Forage - Flickr, CC BY-SA 2.0, https://commons.wikimedia.org/w/index.php?curid=1659458