KU LEUVEN

FACULTY OF
ENGINEERING SCIENCE

The best master's thesis ever

First Author
Second Author

Thesis submitted for the degree of
Master of Science in Cybersecurity

Supervisor
Prof. dr. ir. Knows Better

Assessors
Ir. Kn. Owsmuch
K. Nowsrest

Assistant-supervisors
Ir. An Assistent
A. Friend

Academic year 2024 – 2025

Published by First Author and Second Author,
Faculty of Engineering Science, Kasteelpark Arenberg 1 bus 2200, B-3001 Leuven

Preface

I would like to thank everybody who kept me busy the last year, especially my promoter and my assistants. I would also like to thank the jury for reading the text. My sincere gratitude also goes to my wive and the rest of my family.

First Author
Second Author

Contents

Abstract

The `abstract` environment contains a more extensive overview of the work. But it should be limited to one page.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

List of Figures and Tables

List of Figures

List of Tables

List of Abbreviations and Symbols

Abbreviations

DL	Discrete Logarithm
PPT	Probabilistic Polynomial Time
NIZK	Non-Interactive Zero Knowledge
PoK	Proof of Knowledge
AoK	Arguement of Knowledge
PSSS	Packed Shamir Secret Sharing
PVSS	Publicly Verifiable Secret Sharing
PPVSS	Pre-Constructed Publicly Verifiable Secret Sharing
PPPVSS	Packed Pre-Constructed Publicly Verifiable Secret Sharing

Symbols

q	prime number
$\mathbb{G}$	Cyclic group of order q
$\mathbb{Z}_q$	Modular ring with q elements
$\mathbb{Z}_q[X]$	Univariate polynomial ring in the variable X with coefficients in $\mathbb{Z}_q$
λ	Security Parameter
$negl$	Negligible function
$\mathcal{O}$	Big-O notation

Chapter 1

Literature Review

In this chapter we sequently recall Packed Shamir secret sharing, Sigma ($\sum$) Protocols and Publicly Verifiable Secret Sharing (PVSS) followed by the recent scheme introduced in [3], namely, Pre-Constructed Publicly Verifiable Secret Sharing (PPVSS) which has versatile applications and also improves efficiency in existing applications. The agenda of this chapter is to give enough background before describing our Packed PPVSS (PPPVSS) scheme and its corresponding security guarantees in the next chapter.

1.1 Introduction

1.2 Preliminaries

1.2.1 Notation

Let $\mathbb{G}$ be a cyclic subgroup of prime order q with its generator being g, isomorphic to a subgroup of the multiplicative modular group $\mathbb{Z}_p^*$, where p is prime. Also, we write $Z_q[X]_d$ to denote the set of all d degree polynomials univariate in X with coefficients in the finite field $\mathbb{Z}_q$.

1.2.2 Packed Shamir Secret Sharing

(n, t, ℓ)-Packed Shamir secret sharing ([7],[4]) scheme is a threshold secret sharing scheme which is a variant of (n, t)-Shamir's secret sharing scheme [8]. In a nutshell, the $t + \ell - 1$ degree secret polynomial with coefficients in $\mathbb{Z}_q$ which evaluates to ℓ secrets is secret shared amongst n parties such that any $t+\ell$ parties can reconstruct back the secret polynomial. Recall that Shamir's secret sharing scheme requires at least $t + 1$ parties to reconstruct the secret polynomial in contrast to the $t + \ell$ parties in the Packed Shamir secret sharing scheme. The scheme is summarized in the Figure 1.1.

Packed Shamir Secret Sharing

Given ℓ secrets to share amongst n parties, where at most t of them can be *(passively)* corrupt, the (n, t, ℓ)-Packed Shamir secret sharing scheme description is as follows:

Sharing Algorithm:

- Dealer constructs the secret polynomial $f \in \mathbb{Z}_q[X]_{t+l-1}$ via the lagrange interpolation by choosing $t + \ell$ elements in $\mathbb{Z}_q$ where ℓ of them are secrets, $\{s_i\}_{i=0}^{\ell-1}$, with $f(-i) = s_i$ for all i and remaining t are chosen uniformly at random in $\mathbb{Z}_q$.
- Each party P_i receives their share $f(i)$ from the Dealer for each $i \in \{1, \ldots, n\}$

Reconstruction Algorithm:

- Any Q set containing at least $t + \ell$ parties can use the lagrange interpolation to compute $\{s_i\}_{i=0}^{\ell-1}$ as follows:

$$s_m = \sum_{i \in Q} f(i) \left[\prod_{j \in Q, j \neq i} \frac{-m - j}{i - j} \right] \qquad , m \in \{0, \ldots, \ell - 1\}$$

- The secrets $\{s_i\}_{i=0}^{\ell-1}$ are outputted as the result.

Figure 1.1: Packed Shamir Secret Sharing

1.2.3 Sigma Protocols

The agenda of this subsection is to give a brief formal background about some important primitives used in the PVSS ,Π_S [2], and the PPVSS ,Λ_{RO} [3], schemes. Let X and W be two sets with R being a relation on $X \times W$, and $L = \{x \in X : \exists w \in W, xRw\}$ be the language defined by R where xRw says that w is a witness for a given $x \in L$. Also, let $\mathcal{R}$ be a PPT algorithm such that $\mathcal{R}(1^\lambda)$ outputs pairs (x, w) with $x \in L$ and xRw where λ is a security parameter.

Given a relation R and its corresponding language L, a **Sigma ($\sum$) Protocol** is a 3-round *interactive* protocol between two Probabilistic Polynomial Time (PPT) algorithms, a prover P and a verifier V. For some $x \in L$ with xRw, in the first round P sends a commitment a to V. To which V sends a challenge d to P in the second round and finally P responds back with the response z to V in the third round. V outputs **true** or **false** upon the proof verification on transcript $trans := (a, d, z)$. Informally, with a $\sum$−protocol a prover P tries to convince a verifier V that they know a witness w for a given statement $x \in L$ without revealing any information about w. To state it formally, a $\sum -$protocol is supposed to satisfy *completeness*, *Honest Verifier Zero Knowledge* (HVZK) and *Special Soundness* which are defined as follows.

Definition 1.2.1 (Completeness). *A $\sum -$protocol is said to be* ***complete*** *for $\mathcal{R}$ if the verifier V always accepts the honest prover P for any $x \in L$.*

Definition 1.2.2 (HVZK). *A $\sum -$protocol is said to be* ***HVZK*** *for $\mathcal{R}$ if there exist a PPT algorithm S that simulates trans of the scheme corresponding to a given $x \in L$ with any witness w of x. That is, given $x \in L$,*

$$trans(P(x, w) \leftrightarrow V(x)) \approx trans(S(x) \leftrightarrow V(x)) \qquad \textit{, for any witness } w \textit{ of } x.$$

Where $trans(P(\cdot) \leftrightarrow V(\cdot))$ is the transcript of the $\sum -$protocol amongst P and V and $\approx$ denotes the indistinguishability of the two transcripts.

Definition 1.2.3 (Special Soundness). *A $\sum -$protocol is said to satisfy* ***Special Soundness*** *for $\mathcal{R}$, if there exists a PPT extractor $\mathcal{E}$ for any two valid transcripts, (a, d, z) and (a, d', z'), corresponding to a given $x \in L$ with only a unique witness w and $d \neq d'$ such that $\mathcal{E}(a, d, z, d', z')$ outputs the witness w.*

It is shown that a public-coin, complete, HVZK, special soundness $\sum -$protocol can be made into a Non Interactive Zero Knowledge (NIZK) Proof of Knowledge (PoK) or Argument of Knowledge (AoK) in the Random Oracle (*RO*) model using Fiat-Shamir transform [6]. In the following subsections, we recall two important NIZK PoK schemes which are used in Π_S and Λ_{RO} schemes.

1.2.4 Chaum-Pedersen Protocol for DL Equality

Consider $\mathbb{G}$ being the cyclic group of prime order q with hard Discrete Logarithm (DL). For some $g, h \in \mathbb{G}$ consider the following relation:

$$R_{DLEQ} = \{(g, h, a, b), x : a = g^x, b = h^x\}.$$

In [5], Chaum and Pedersen proposed a NIZK PoK scheme for the DL Equality relation, R_{DLEQ}. Informally, a prover P can convince a verifier V that they know x such that it can be used with both g and h to obtain a and b respectively. This protocol is widely used in many cryptographic applications like threshold decryption, e-voting and Randomness Beacons. We summarize the protocol in Figure 1.2.

1.2.5 NIZK PoK for Polynomial DL

Consider $\mathbb{G}$ being the cyclic group of prime order q with hard Discrete Logarithm (DL).

Chaum-Pedersen Protocol for DLEQ

Let $(g, h, a, b) \in L_{DLEQ}$ be a statement with its corresponding witness being x where L_{DLEQ} is the language defined by the relation R_{DLEQ}.

Prover

- Samples $r \in_R \mathbb{Z}_q$ uniformly at random and sets $c_1 = g^r$ and $c_2 = h^r$.
- Sets $d \leftarrow \mathcal{H}(a, b, c_1, c_2)$, where $\mathcal{H}$ is an agreed upon Random Oracle (RO).
- Sets $z \equiv r + dx \pmod{q}$ and returns the proof(/transcript) $\pi := (d, z)$.

Verifier

- Checks if $d \leftarrow \mathcal{H}(a, b, \frac{g^z}{a^d}, \frac{h^z}{b^d})$ and outputs **true** or **false** accordingly.

Figure 1.2: Chaum-Pedersen NIZK PoK for DLEQ

1.3 Conclusion

The final section of the chapter gives an overview of the important results of this chapter. This implies that the introductory chapter and the concluding chapter don't need a conclusion.

Chapter 2

The Next Chapter

Chapter 3

The Final Chapter

Chapter 4

Conclusion

The final chapter contains the overall conclusion. It also contains suggestions for future work and industrial applications.

Appendices

Appendix A

The First Appendix

Appendices hold useful data which is not essential to understand the work done in the master's thesis. An example is a (program) source. An appendix can also have sections as well as figures and references[1].

A.1 More Lorem

Quisque facilisis auctor sapien. Pellentesque gravida hendrerit lectus. Mauris rutrum sodales sapien. Fusce hendrerit sem vel lorem. Integer pellentesque massa vel augue. Integer elit tortor, feugiat quis, sagittis et, ornare non, lacus. Vestibulum posuere pellentesque eros. Quisque venenatis ipsum dictum nulla. Aliquam quis quam non metus eleifend interdum. Nam eget sapien ac mauris malesuada adipiscing. Etiam eleifend neque sed quam. Nulla facilisi. Proin a ligula. Sed id dui eu nibh egestas tincidunt. Suspendisse arcu.

A.1.1 Lorem 15–17

Nulla in ipsum. Praesent eros nulla, congue vitae, euismod ut, commodo a, wisi. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aenean nonummy magna non leo. Sed felis erat, ullamcorper in, dictum non, ultricies ut, lectus. Proin vel arcu a odio lobortis euismod. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Proin ut est. Aliquam odio. Pellentesque massa turpis, cursus eu, euismod nec, tempor congue, nulla. Duis viverra gravida mauris. Cras tincidunt. Curabitur eros ligula, varius ut, pulvinar in, cursus faucibus, augue.

Nulla mattis luctus nulla. Duis commodo velit at leo. Aliquam vulputate magna et leo. Nam vestibulum ullamcorper leo. Vestibulum condimentum rutrum mauris. Donec id mauris. Morbi molestie justo et pede. Vivamus eget turpis sed nisl cursus tempor. Curabitur mollis sapien condimentum nunc. In wisi nisl, malesuada at, dignissim sit amet, lobortis in, odio. Aenean consequat arcu a ante. Pellentesque porta elit sit amet orci. Etiam at turpis nec elit ultricies imperdiet. Nulla facilisi.

In hac habitasse platea dictumst. Suspendisse viverra aliquam risus. Nullam pede justo, molestie nonummy, scelerisque eu, facilisis vel, arcu.

Curabitur tellus magna, porttitor a, commodo a, commodo in, tortor. Donec interdum. Praesent scelerisque. Maecenas posuere sodales odio. Vivamus metus lacus, varius quis, imperdiet quis, rhoncus a, turpis. Etiam ligula arcu, elementum a, venenatis quis, sollicitudin sed, metus. Donec nunc pede, tincidunt in, venenatis vitae, faucibus vel, nibh. Pellentesque wisi. Nullam malesuada. Morbi ut tellus ut pede tincidunt porta. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam congue neque id dolor.

A.1.2 Lorem 18–19

Donec et nisl at wisi luctus bibendum. Nam interdum tellus ac libero. Sed sem justo, laoreet vitae, fringilla at, adipiscing ut, nibh. Maecenas non sem quis tortor eleifend fermentum. Etiam id tortor ac mauris porta vulputate. Integer porta neque vitae massa. Maecenas tempus libero a libero posuere dictum. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aenean quis mauris sed elit commodo placerat. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Vivamus rhoncus tincidunt libero. Etiam elementum pretium justo. Vivamus est. Morbi a tellus eget pede tristique commodo. Nulla nisl. Vestibulum sed nisl eu sapien cursus rutrum.

Nulla non mauris vitae wisi posuere convallis. Sed eu nulla nec eros scelerisque pharetra. Nullam varius. Etiam dignissim elementum metus. Vestibulum faucibus, metus sit amet mattis rhoncus, sapien dui laoreet odio, nec ultricies nibh augue a enim. Fusce in ligula. Quisque at magna et nulla commodo consequat. Proin accumsan imperdiet sem. Nunc porta. Donec feugiat mi at justo. Phasellus facilisis ipsum quis ante. In ac elit eget ipsum pharetra faucibus. Maecenas viverra nulla in massa.

A.2 Lorem 51

Maecenas dui. Aliquam volutpat auctor lorem. Cras placerat est vitae lectus. Curabitur massa lectus, rutrum euismod, dignissim ut, dapibus a, odio. Ut eros erat, vulputate ut, interdum non, porta eu, erat. Cras fermentum, felis in porta congue, velit leo facilisis odio, vitae consectetuer lorem quam vitae orci. Sed ultrices, pede eu placerat auctor, ante ligula rutrum tellus, vel posuere nibh lacus nec nibh. Maecenas laoreet dolor at enim. Donec molestie dolor nec metus. Vestibulum libero. Sed quis erat. Sed tristique. Duis pede leo, fermentum quis, consectetuer eget, vulputate sit amet, erat.

Appendix B

The Last Appendix

Appendices are numbered with letters, but the sections and subsections use arabic numerals, as can be seen below.

B.1 Lorem 20-24

Nulla ac nisl. Nullam urna nulla, ullamcorper in, interdum sit amet, gravida ut, risus. Aenean ac enim. In luctus. Phasellus eu quam vitae turpis viverra pellentesque. Duis feugiat felis ut enim. Phasellus pharetra, sem id porttitor sodales, magna nunc aliquet nibh, nec blandit nisl mauris at pede. Suspendisse risus risus, lobortis eget, semper at, imperdiet sit amet, quam. Quisque scelerisque dapibus nibh. Nam enim. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Nunc ut metus. Ut metus justo, auctor at, ultrices eu, sagittis ut, purus. Aliquam aliquam.

Etiam pede massa, dapibus vitae, rhoncus in, placerat posuere, odio. Vestibulum luctus commodo lacus. Morbi lacus dui, tempor sed, euismod eget, condimentum at, tortor. Phasellus aliquet odio ac lacus tempor faucibus. Praesent sed sem. Praesent iaculis. Cras rhoncus tellus sed justo ullamcorper sagittis. Donec quis orci. Sed ut tortor quis tellus euismod tincidunt. Suspendisse congue nisl eu elit. Aliquam tortor diam, tempus id, tristique eget, sodales vel, nulla. Praesent tellus mi, condimentum sed, viverra at, consectetuer quis, lectus. In auctor vehicula orci. Sed pede sapien, euismod in, suscipit in, pharetra placerat, metus. Vivamus commodo dui non odio. Donec et felis.

Etiam suscipit aliquam arcu. Aliquam sit amet est ac purus bibendum congue. Sed in eros. Morbi non orci. Pellentesque mattis lacinia elit. Fusce molestie velit in ligula. Nullam et orci vitae nibh vulputate auctor. Aliquam eget purus. Nulla auctor wisi sed ipsum. Morbi porttitor tellus ac enim. Fusce ornare. Proin ipsum enim, tincidunt in, ornare venenatis, molestie a, augue. Donec vel pede in lacus sagittis porta. Sed hendrerit ipsum quis nisl. Suspendisse quis massa ac nibh pretium cursus. Sed sodales. Nam eu neque quis pede dignissim ornare. Maecenas eu purus ac urna tincidunt congue.

Donec et nisl id sapien blandit mattis. Aenean dictum odio sit amet risus. Morbi purus. Nulla a est sit amet purus venenatis iaculis. Vivamus viverra purus vel magna. Donec in justo sed odio malesuada dapibus. Nunc ultrices aliquam nunc. Vivamus facilisis pellentesque velit. Nulla nunc velit, vulputate dapibus, vulputate id, mattis ac, justo. Nam mattis elit dapibus purus. Quisque enim risus, congue non, elementum ut, mattis quis, sem. Quisque elit.

Maecenas non massa. Vestibulum pharetra nulla at lorem. Duis quis quam id lacus dapibus interdum. Nulla lorem. Donec ut ante quis dolor bibendum condimentum. Etiam egestas tortor vitae lacus. Praesent cursus. Mauris bibendum pede at elit. Morbi et felis a lectus interdum facilisis. Sed suscipit gravida turpis. Nulla at lectus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Praesent nonummy luctus nibh. Proin turpis nunc, congue eu, egestas ut, fringilla at, tellus. In hac habitasse platea dictumst.

B.2 Lorem 25-27

Vivamus eu tellus sed tellus consequat suscipit. Nam orci orci, malesuada id, gravida nec, ultricies vitae, erat. Donec risus turpis, luctus sit amet, interdum quis, porta sed, ipsum. Suspendisse condimentum, tortor at egestas posuere, neque metus tempor orci, et tincidunt urna nunc a purus. Sed facilisis blandit tellus. Nunc risus sem, suscipit nec, eleifend quis, cursus quis, libero. Curabitur et dolor. Sed vitae sem. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Maecenas ante. Duis ullamcorper enim. Donec tristique enim eu leo. Nullam molestie elit eu dolor. Nullam bibendum, turpis vitae tristique gravida, quam sapien tempor lectus, quis pretium tellus purus ac quam. Nulla facilisi.

Duis aliquet dui in est. Donec eget est. Nunc lectus odio, varius at, fermentum in, accumsan non, enim. Aliquam erat volutpat. Proin sit amet nulla ut eros consectetuer cursus. Phasellus dapibus aliquam justo. Nunc laoreet. Donec consequat placerat magna. Duis pretium tincidunt justo. Sed sollicitudin vestibulum quam. Nam quis ligula. Vivamus at metus. Etiam imperdiet imperdiet pede. Aenean turpis. Fusce augue velit, scelerisque sollicitudin, dictum vitae, tempor et, pede. Donec wisi sapien, feugiat in, fermentum ut, sollicitudin adipiscing, metus.

Donec vel nibh ut felis consectetuer laoreet. Donec pede. Sed id quam id wisi laoreet suscipit. Nulla lectus dolor, aliquam ac, fringilla eget, mollis ut, orci. In pellentesque justo in ligula. Maecenas turpis. Donec eleifend leo at felis tincidunt consequat. Aenean turpis metus, malesuada sed, condimentum sit amet, auctor a, wisi. Pellentesque sapien elit, bibendum ac, posuere et, congue eu, felis. Vestibulum mattis libero quis metus scelerisque ultrices. Sed purus.

Bibliography

[1] D. Adams. *The Hitchhiker's Guide to the Galaxy.* Del Rey (reprint), 1995. ISBN-13: 978-0345391803.

[2] K. Baghery. π: A unified framework for computational verifiable secret sharing. Cryptology ePrint Archive, Paper 2023/1669, 2023.

[3] K. Baghery, N. Knapen, G. Nicolas, and M. Rahimi. Pre-constructed publicly verifiable secret sharing and applications. Cryptology ePrint Archive, Paper 2025/576, 2025.

[4] G. R. Blakley and C. Meadows. Security of ramp schemes. In *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, volume 196 of *Lecture Notes in Computer Science*, pages 242–268. Springer, 1984.

[5] D. Chaum and T. P. Pedersen. Wallet databases with observers. In E. F. Brickell, editor, *Advances in Cryptology — CRYPTO' 92*, pages 89–105, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.

[6] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. M. Odlyzko, editor, *Advances in Cryptology — CRYPTO' 86*, pages 186–194, Berlin, Heidelberg, 1987. Springer Berlin Heidelberg.

[7] M. Franklin and M. Yung. Communication complexity of secure computation (extended abstract). In *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, STOC '92, page 699–710, New York, NY, USA, 1992. Association for Computing Machinery.

[8] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, Nov. 1979.