SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNICAL UNIVERSITY OF MUNICH

Bachelor's Thesis in Informatics

Formalizing the Kate-Zaverucha-Goldberg Polynomial Commitment Scheme

Tobias Rothmann

SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNICAL UNIVERSITY OF MUNICH

Bachelor's Thesis in Informatics

Formalizing the Kate-Zaverucha-Goldberg Polynomial Commitment Scheme

Eine Formalisierung des Kate-Zaverucha-Goldberg Polynomiellen Commitment Verfahrens

Author:	Tobias Rothmann
Supervisor:	Prof. Tobias Nipkow
Advisor:	Katharina Kreuzer
Submission Date:	April 15, 2024

I confirm that this bachelor's thesis is my own work and I have documented all sources and material used.

Munich, April 15, 2024 Tobias Rothmann

Acknowledgments

Abstract

Contents

1 Introduction

1.1 Section

Citation test [**latex**].

Acronyms must be added in `main.tex` and are referenced using macros. The first occurrence is automatically replaced with the long version of the acronym, while all subsequent usages use the abbreviation.

E.g. `\ac{TUM}, \ac{TUM}` ⇒ Technical University of Munich (TUM), TUM

For more details, see the documentation of the `acronym` package[1].

1.1.1 Subsection

See Table 1.1, Figure 1.1, Figure 1.2, Figure 1.3.

Table 1.1: An example for a simple table.

A	B	C	D
1	2	1	2
2	3	2	3

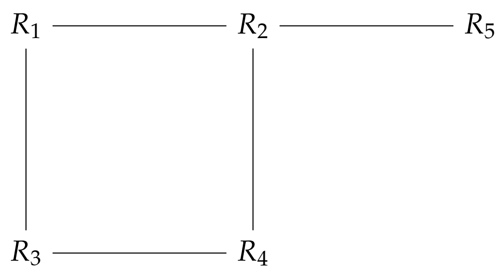

Figure 1.1: An example for a simple drawing.

[1] `https://ctan.org/pkg/acronym`

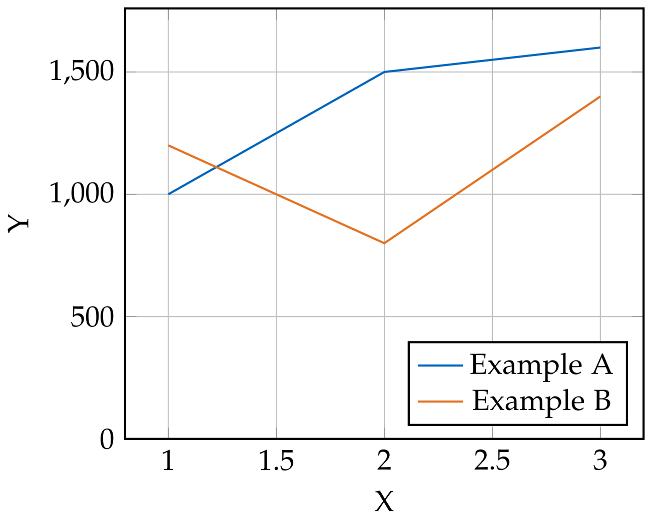

Figure 1.2: An example for a simple plot.

```
SELECT * FROM tbl WHERE tbl.str = "str"
```

Figure 1.3: An example for a source code listing.

2 related work

3 Prelimiaries

3.1 Mathematical Prelimiaries

3.1.1 General Notation

- p stands for a prime number if not specified otherwise.
- groups are written in a multiplicative way with the common operator $\cdot$ and the abbreviation ab for $a \cdot b$
- $\mathbb{Z}_p$ denotes a finite field of order p, which is isomorph to the integers modulo p [Lan02], hence we use the common integer operators for addition and multiplication.

3.1.2 cyclic group

A finite group $\mathbb{G}_p$ of order p with a generator element is a cyclic group [Lan02].

We use $\mathbf{g}$ to refer to a fixed generator of a cyclic group. Since $\mathbf{g}$ is a generator $\{1, \mathbf{g}, \mathbf{g}^2, ..., \mathbf{g}^{p-1}\}$ is isomorph to $\mathbb{G}_p$ and the power operation is closed on $\mathbb{G}_p$ [Lan02].

3.1.3 pairings

A pairing is a function: $\mathbb{G}_p \times \mathbb{G}_p \rightarrow \mathbb{G}_T$, where $\mathbb{G}_p$ and $\mathbb{G}_T$ are two groups of order p [KZG10]. From now on e will always denote a pairing function. Pairings require two properties [KZG10]:

- **Billinearity:** $\forall g, h \in \mathbb{G}_p.\ \forall a, b \in \mathbb{Z}_p.\ e(g^a, h^b) = e(g, h)^{ab}$
- **Non-degeneracy:** $\neg(\forall g, h \in \mathbb{G}_p.\ e(g, h) = 1)$

3.2 Cryptography Prelimiaries

Before we introduce the cryptographic preliminaries, we cover some general notation that is used in this paper in the context of cryptography.

- To express that an element is uniformly sampled from a set, we use the abbreviation '$\in_{\mathcal{R}}$'.
- ϵ is a function that is considered negligible in the security parameter κ, where negligibility means that for all $c > 0$ there exists a k_0 such that $\epsilon(k) < 1/k^c$ for all $k > k_0$

Note that further topic-related notation (e.g. for games) is to be found in the according topic's section.

3.2.1 Game-based Proofs

Games are a method to define security for cryptographic protocols, they are composed of probabilistic functions and played against a probabilistic Adversary [Sho04]. Bellare, Rogaway and Shoup state that game-based proofs are a particularly rigor and thus secure proving approach, referring to game-based proofs as a sequence of game-hops that bound the probability of one game to another [BR04; Sho04]. The two types of game hops we will use in our proofs are:

- **game hop as a bridging step**
  A bridging step is changing the function definitions, such that the game's probability does not change [Sho04].
- **game hop based on a failure event**
  In a game hop based on a failure event, two games are equal except if a specific failure event occurs [Sho04]. The failure event should have a negligible probability for the game-based proof to hold.

We write games as a sequence of functions where '$\leftarrow$' followed by a set means uniform sampling from that set, '$\leftarrow$' followed by a probability mass function means sampling from that function space, and '=' is an assignment of a deterministic value. Moreover, we write ':' followed by a condition to assure that the condition has to hold at this point. To give an example, think of the following game as "sampling a uniformly random a from $\mathbb{Z}_p$, get the probabilistic result from $\mathcal{A}$ as b, computing c as F applied to a and b, and assert that P holds for c":

$$
\begin{aligned}
a &\leftarrow \mathbb{Z}_p, \\
b &\leftarrow \mathcal{A}, \\
c &= \mathrm{F}\ a\ b, \\
&: \mathrm{P}\ c
\end{aligned}
$$

3.2.2 Hardness Assumptions

Hardness assumptions are problems that are generally assumed to be hard. Security games for cryptographic protocols are bound to hardness assumptions via game hops to obtain game-based security proofs [BS23]. We will need three specific hardness assumptions for our proofs, all of which are defined in [KZG10]:

Definition 3.2.1 (Discrete Logarithm (DL) Assumption)**.** For $a \in_{\mathcal{R}} \mathbb{Z}_p$, holds for every Adversary $\mathcal{A}$: $\Pr[a = \mathcal{A}(\mathbf{g}^a)] = \epsilon$ [KZG10].

Formally We define the DL game as:

$$\begin{aligned} a &\leftarrow \mathbb{Z}_p, \\ a' &\leftarrow \mathcal{A}\ \mathbf{g}^a, \\ &: a = a' \end{aligned}$$

t-strong Diffie-Hellman (t-SDH) Assumption

Let t be fixed. For $\alpha \in_{\mathcal{R}} \mathbb{Z}_p$, holds for every Adversary $\mathcal{A}$: $\Pr\left[(c, \mathbf{g}^{\frac{1}{\alpha+c}}) = \mathcal{A}\ [\mathbf{g}, \mathbf{g}^{\alpha}, \mathbf{g}^{(\alpha^2)}, \ldots, \mathbf{g}^{(\alpha^t)}]\right] = \epsilon$ for all c $\in \mathbb{Z}_p \backslash \{\alpha\}$ [KZG10].

Formally We define the t-SDH game as:

$$\begin{aligned} \alpha &\leftarrow \mathbb{Z}_p, \\ (c, g') &\leftarrow \mathcal{A}\ [\mathbf{g}, \mathbf{g}^{\alpha}, \mathbf{g}^{(\alpha^2)}, \ldots, \mathbf{g}^{(\alpha^t)}] \\ &: \mathbf{g}^{\frac{1}{\alpha+c}} = g' \end{aligned}$$

t-Bilinear Strong Diffie-Hellman (t-BSDH) Assumption

This definition is analogous to the previous one, except that the result is passed through a pairing function. Nevertheless, we define the property formally for completeness.

Let t be fixed. For $\alpha \in_{\mathcal{R}} \mathbb{Z}_p$, holds for every Adversary $\mathcal{A}$: $\Pr\left[(c, \mathrm{e}(\mathbf{g}, \mathbf{g})^{\frac{1}{\alpha+c}}) = \mathcal{A}\ [\mathbf{g}, \mathbf{g}^{\alpha}, \mathbf{g}^{(\alpha^2)}, \ldots, \mathbf{g}^{(\alpha^t)}]\right] = \epsilon$ for all c $\in \mathbb{Z}_p \backslash \{\alpha\}$ [KZG10].

Formally We define the t-BSDH game as:

$$\begin{aligned} \alpha &\leftarrow \mathbb{Z}_p, \\ (c, g') &\leftarrow \mathcal{A}\ [\mathbf{g}, \mathbf{g}^{\alpha}, \mathbf{g}^{(\alpha^2)}, \ldots, \mathbf{g}^{(\alpha^t)}] \\ &: \mathrm{e}(\mathbf{g}, \mathbf{g})^{\frac{1}{\alpha+c}} = g' \end{aligned}$$

3.2.3 Commitment Schemes

[Tha22]

3.3 Isabelle Prelimiaries

3.3.1 Isabelle based Notation

3.3.2 CryptHOL

Abbreviations

TUM Technical University of Munich

List of Figures

List of Tables

Bibliography

[BR04] M. Bellare and P. Rogaway. *Code-Based Game-Playing Proofs and the Security of Triple Encryption*. Cryptology ePrint Archive, Paper 2004/331. https://eprint.iacr.org/2004/331. 2004.

[BS23] D. Boneh and V. Shoup. *A Graduate Course in Applied Cryptography*. http://toc.cryptobook.us/book.pdf. 2023.

[KZG10] A. Kate, G. M. Zaverucha, and I. Goldberg. "Constant-Size Commitments to Polynomials and Their Applications." In: *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 6477. Lecture Notes in Computer Science. Springer, 2010, pp. 177–194. DOI: 10.1007/978-3-642-17373-8_11.

[Lan02] S. Lang. *Algebra*. Vol. 3. Springer New York, NY, 2002.

[Sho04] V. Shoup. *Sequences of games: a tool for taming complexity in security proofs*. Cryptology ePrint Archive, Paper 2004/332. https://eprint.iacr.org/2004/332. 2004.

[Tha22] J. Thaler. *Proofs, Arguments, and Zero-Knowledge*. Now Publishers Inc, 2022.