Bringing Zero-Knowledge Proofs of Knowledge to Practice

Endre Bangerter[1], Stefania Barzan[2], Stephan Krenn[2], Ahmad-Reza Sadeghi[3], Thomas Schneider[3], and Joe-Kai Tsay[3] ⋆

[1] Bern University of Applied Sciences, Biel/Bienne, Switzerland
endre.bangerter@bfh.ch

[2] Bern University of Applied Sciences, Biel/Bienne, Switzerland, and University of Fribourg, Switzerland
{stefania.barzan, stephan.krenn}@bfh.ch

[3] Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany
{ahmad.sadeghi, thomas.schneider, joe-kai.tsay}@trust.rub.de

Abstract. Efficient zero-knowledge proofs of knowledge (ZK-PoK) are basic building blocks of many practical cryptographic applications such as identification schemes, group signatures, and secure multiparty computation. Currently, first applications that critically rely on ZK-PoKs are being deployed in the real world. The most prominent example is Direct Anonymous Attestation (DAA), which was adopted by the Trusted Computing Group (TCG) and implemented as one of the functionalities of the cryptographic Trusted Platform Module (TPM) chip.

Implementing systems using ZK-PoK turns out to be challenging, since ZK-PoK are, loosely speaking, significantly more complex than standard crypto primitives, such as encryption and signature schemes. As a result, implementation cycles of ZK-PoK are time-consuming and error-prone, in particular for developers with minor or no cryptographic skills.

In this paper we report on our ongoing and future research vision with the goal to bring ZK-PoK to practice by making them accessible to crypto and security engineers. To this end we are developing compilers and related tools that support and partially automate the design, implementation, verification and secure implementation of ZK-PoK protocols.

1 Introduction

A zero-knowledge proof of knowledge (ZK-PoK) is a two-party protocol between a prover and a verifier, which allows the prover to convince the verifier that he knows a secret value that satisfies a given relation (*proof of knowledge property*), without the verifier being able to learn anything about the secret (*zero-knowledge property*). For a formal definition we refer to [BG93]. There are fundamental results showing that all relations in NP have ZK-PoK

⋆ This work is being performed within the FP7 EU project CACE (Computer Aided Cryptography Engineering).

[DFK$^+$93,GMW91,IKOS07,PRS02]. The corresponding protocols are of theoretical relevance, but are much too inefficient to be used in practical applications.

In contrast to these generic, but practically useless protocols, there are various protocols which are efficient enough for real world use. Essentially, all ZK-PoK protocols being used in practice today are based on so called Σ-protocols. What is typically being proved using basic Σ-protocols is the knowledge of a preimage under a homomorphism (e.g., a secret discrete logarithm). Yet, there are numerous considerably more complex variations of these preimage proofs. These ZK-PoK proof techniques play an important role in applied cryptography. In fact, many practically oriented applications use such proofs as basic building blocks. Examples include identification schemes [Sch91], interactive verifiable computation [CM99], group signatures [Cam98], secure watermark detection [ARS05], and efficient secure multiparty computation [LPS08] – just to name a few.

While many of these applications typically only exist on a specification level, a direction of applied research has produced first applications using ZK-PoKs that are deployed in the real world. The probably most prominent example is Direct Anonymous Attestation (DAA) [BCC04], which was adopted by the Trusted Computing Group (TCG), an industry consortium of many IT enterprises, as a privacy enhancing mechanism for remote authentication of computing platforms.

Another example is the *identity mixer* anonymous credential system [CH02], which was released by IBM into the Eclipse Higgins project, an open source effort dedicated to developing software for user-centric identity management. Identity mixer is probably one of the most advanced protocol suites supporting the “transient relationship paradigm”.

Up to now, design, implementation and verification of the formal cryptographic security properties (i.e., zero-knowledge and proof of knowledge property) as well as code security properties (e.g., security against buffer overflows, race conditions, side channel vulnerabilities) is done “by hand”. In fact, past experiences, e.g., during the design and implementation of the preceding two examples, have shown that this is a time consuming and error prone task. This has certainly to do with the fact that ZK-PoK are considerably more complex than other crypto primitives such as signature- and encryption schemes or hash functions.

The goal of our ongoing and future research is to bring ZK-PoK to practice by making them accessible to crypto and security engineers. To this end we are working on compilers and related tools that support and partially automate the design, implementation, verification, and secure implementation of ZK-PoK protocols. For instance the compiler which is part of our toolbox, will take as input a high-level specification of the goals of a ZK-PoK, automatically find a corresponding protocol, and output its implementation in, e.g., Java or C code. We have already developed and implemented a language and compiler that automates the latter step from protocol specification to code generation. Finding a protocol from a high-level specification is subject of ongoing research.

Also, we are working on tool-based support for the verification of the security properties of ZK-PoK.

In the following we describe the challenges pertaining to using ZK-PoK in practice in Sec. 2 and give an overview of a solution blueprint and first results on solving these challenges in Sec. 3.

1.1 Related work

ZK-PoK were introduced in [GMR85], and the first efficient protocols for preimage proofs in groups of known order were given in [Sch91,GQ90]. Unified frameworks for preimage proofs in known order groups were given in the following by [CDS94,CS97b,Bra97,BS02]. A profound analysis of the Σ^{Φ}-protocol was performed by Cramer [Cra96].

The first efficient solution for proofs in unknown order groups was given in [FO97] and has been corrected by Damgård and Fujisaki [DF02]. Subsequently, other variants overcoming some of their restrictions have been proposed. In very recent work, a long overdue unified framework for exponentiation homomorphisms in arbitrary groups was given by Camenisch et al. [CKY09].

An efficient way to combine arbitrary Σ-protocols was described by Cramer et al. [CDS94].

To bridge the gap between theory and practice, a first prototype of a zero-knowledge compiler was started in [Bri04,CRS05], and was later extended in [BCK^{+}08]. Yet, its authors state explicitly that it was designed as a proof of concept prototype only. This prototype handles proofs in known order groups only, and includes neither a verification tool nor extensions to achieve concurrent ZK or non-interactivity. Unfortunately, multiple proofs are combined in a very inefficient way only. Furthermore, the input language of this compiler is less intuitive than ours.

Our input language was inspired by the commonly used notation of Camenisch and Stadler [CS97a]. Yet, this is an inprecise and ambiguous notation. Therefore we augment it by the missing parts such as group descriptions, etc.

As basic building blocks we apply the techniques from [Sch91,GQ90,Cra96] in known order groups, proofs in unknown order groups are done by applying those from [DF02,BCK^{+}08]. Predicates are combined using the method described in [CDS94] instantiated with Shamir's secret sharing scheme [Sha79]. To obtain non-interactive ZK and concurrent ZK we use the Fiat-Shamir heuristic [FS87].

Similar work to ours was performed in the field of secure function evaluation [MOR03,MNPS04]. Their compilers allow to specify the function to be evaluated in a high-level language, and output executable code. In principle, zero-knowledge proofs could be realized by secure function evaluations. Yet, the resulting protocols are significantly less efficient than those generated by our compiler.

Compiler support for an efficient and secure low-level implementation of cryptographic primitives resistant against software side-channels [BP05] and applications to elliptic curve cryptography [BMP07] is provided by Cryptography Aware language and cOmpiler (CAO) [BNPS05].

2 Challenges

In the following paragraphs we will describe the main challenges that ZK-PoK pose to crypto engineers and protocol designers, which we aim to tackle with our compiler suite.

Let us introduce some notation first. By the *semantic goal* of a ZK-PoK we refer to *what a prover wants to demonstrate in zero-knowledge.* For instance, the semantic goal can be to prove knowledge of a discrete logarithm of a group element with respect to another group element. A more complex goal is to prove that a given cipher-text encrypts a valid (with respect to some given public key) signature on a specific message. By a ZK-PoK *protocol (specification)* we refer to the actual description of a protocol (i.e., the operations of prover and verifier and the messages being exchanged). For instance, the well known Schnorr protocol [Sch91] realizes the first semantic goal mentioned above, and verifiable encryption protocols [Ate04] realize the latter. It is important to note that given a semantic goal, there can be many different protocols realizing that goal; also sometimes one does not know how to construct an efficient protocol realizing a goal (which does not mean that there is no better protocol than using a generic protocols for NP statements). Finally, by a *(protocol) implementation* we refer to actual code (e.g., in C or Java) realizing a specification.

Now, let us turn to the challenges mentioned above.

Designing ZK-PoK. On a conceptual level ZK-PoK are easy to grasp and intuitive: formulating the semantic goal of a ZK-PoK is an easy task for a protocol designer. It essentially boils down to formulating the requirements of a ZK-PoK. Yet, finding a protocol specification realizing a semantic goal is in many cases difficult or impossible for people who don't have extensive expertise in the field. As a result, we believe that unlike other, less complex crypto primitives (such as encryption, signatures, etc.), ZK-PoK are not part of the toolbox of many crypto engineers. This in turn lets us conjecture that the potential of novel applications that can be built using ZK-PoK is only poorly exploited.

Why is it actually often hard to find a ZK-PoK protocol meeting a semantic specification? The main problem is the lack of a unified, modular, and easy to understand theoretical framework underlying the various ZK-PoK protocols and proof techniques. As a result there is no methodological formal way to guide cryptographic protocol designers. In fact, there is a large number of tricks and techniques "to prove this and that", yet combining various tricks and preserving the security properties (i.e., the ZK and PoK properties) is not straightforward and is non-modular. The composition of techniques often needs intricate knowledge of the technique at hand, and may also require modification of the technique. For instance some techniques only work under certain algebraic assumptions and preconditions. These can be conditions on the order of the algebraic group and group elements being used, conditions on whether the prover knows the factorization of a composite integer, distributions of protocol inputs etc. The algebraic conditions in turn require tuning protocol parameters. As a result, finding and designing ZK-PoK protocols is a heuristic process based on experience and a detailed understanding of the techniques being used. In contrast, encryption and signature schemes and other primitives can be composed in a modular way and are easily accessible to designers.

Efficiency of implementation process. The step going from the protocol specification of a ZK-PoK to its protocol implementation is often considered to be trivial from a conceptual point of view. Yet in practice it is not. In fact, experiences made while implementing, e.g., a prototype of the identity mixer [CH02,CL01] protocols have shown that a manual implementation can be tedious and error prone and easily takes person weeks. Moreover, protocol specifications are often written by cryptographers while the implementation is done by SW engineers. This "skill gap" may lead to implementation errors. The former often don't care sufficiently or don't have the skills to cope with implementation issues and their specifications may be slightly incomplete; the latter may have a hard time to assess implementation decisions, which depend on cryptographic subtleties.

Additionally, minor changes in the semantic goal often result in fundamental changes of the resulting protocol.

Efficiency of code. Getting efficient code, in terms of computation time, memory usage, size of messages sent over the network, number of message exchanged etc., can be of great concern when using ZK-PoK. The choice of the resource to optimize may greatly differ depending on the actual device on which the code is run. For instance, parts of the prover's algorithm in the DAA protocol [BCC04] are run inside a relatively simple and low cost TPM chip while the verifier's algorithm may run on a powerful computer.

There are at least two places where one can optimize ZK-PoK. On a high-level, there is potential for optimization by finding the most efficient protocol specification realizing a given semantic goal (this type of optimization is closely related to the "designing ZK-PoK" issue described above). On a lower level one can optimize the code implementing a given protocol, much like the optimization performed by compilers for conventional programming languages like C, Java etc., whereas one should specially focus on the optimization of crypto operations.

Optimization in general, requires substantial experience and an intricate understanding of the runtime environment.

Correctness and security of implementations. The correctness and security of the protocol implementations is primordial. One can distinguish two classes of correctness and security properties. One are the cryptographic security properties, which are formalized mathematically and are present already on a protocol specification level. These properties are: correctness (the protocol works when prover and verifier are honest), zero-knowledge and proof of knowledge. At the current state of the art, the crypto community will not accept a ZK-PoK protocol, unless these properties are formally proven on a specification level. These proofs are often non-trivial and certainly tedious and time consuming, and as a result there exist various published protocols that contain flaws in their security analysis. For instance the security proof in [FO97] was incomplete as outlined and corrected in [DF02].

Of course one also needs to assert that those security properties are indeed assured by the implementation of the protocol (i.e., that an implementation correctly reflects the specification).

Of equal importance are security issues that occur at an implementation level. These include security against generic implementation errors like buffer overflows, race conditions etc., but also crypto specific code problems, such as side-channel vulnerabilities. Getting these code security issues right requires substantial know-how, which is often not part of the skill set of developers.

3 Solution blueprint and results

In the following we give a brief description of our compiler suite (see Fig. 1), and sketch how it can be used for resolving the challenges explained above. Also first results achieved for each of these challenges will be described.

From a usage perspective, our compiler suite takes a description of the semantic goal in a *high-level language*, and outputs a protocol implementation together with a formal proof of its correctness. From a technical point of view, the compiler is divided into three parts, which we want to discuss briefly now:

- The compiler will take a description of the semantic goal in a *high-level language* as input, and translate it into a *protocol specification* in a first compiler step (the *high-level compiler*) by choosing the most appropriate techniques to meet the user's requirements. This protocol specification describes a unique protocol, without containing the exact algorithms or single messages to be exchanged, etc.
- In a second step, the *protocol compiler* will expand this protocol specification into C or Java code, as well as LaTeX-code for documentation purposes.
- Both compiler steps will add annotations, including information about decisions made, to their output. The semantic goal, the protocol specification and its implementation will be given to the *protocol verification toolbox*, which using those annotations will formally verify that the implementation indeed realizes the semantic goal in a secure way.

Let us now turn to how we plan to tackle the problems stated in Sec. 2.

The "efficiency of implementation process" and "efficiency of code" challenges are equally important but less difficult to achieve than the two others; we therefore only discuss them briefly.

Efficiency of implementation process. This goal is achieved inherently by our compiler based approach, as the implementation is automatized. Our first prototype runs within less than one second, and we expect the final version to run within a couple of seconds. To ease usage of our compiler suite, a tool-chain with a consistent user interface could be given to our compiler. This could be based

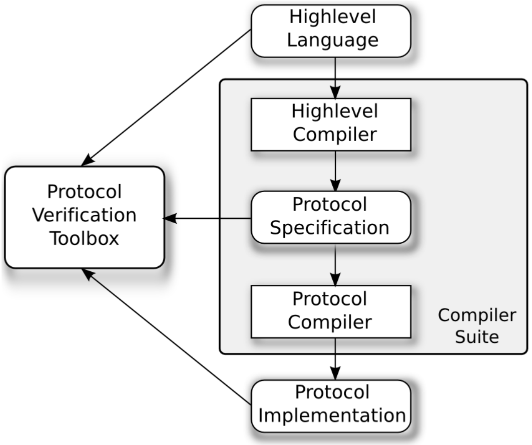

Fig. 1. Architecture of our framework for automatic generation and verification of ZK-PoK protocols.

on an IDE such as Eclipse and support the developer by syntax highlighting, performance testing, etc.

The input language is inspired by the notation introduced in [CS97a]. Yet, to remove unambiguities, some more information has to be added to this language.

Let us consider the following example:

$$ZKPoK\left[(\chi) : y = g^{\chi}\right]$$

specifies a proof of knowledge of the discrete logarithm $x \in G$ of $y \in H$ in base $g \in H$. This notation does not contain any information about the groups G, H, the order of g, y, or the knowledge error that has to be achieved.

Still, from having the above protocol description and knowledge about the groups, etc., it's straightforward to obtain the input of our compiler, such as:

```
ProtocolInputs{
  Declaration    := Prime(1024) p; Prime(160) q;
                    G=Zmod+(q) x; H=Zmod*(p) g, y;
  ProverPrivate  := x;
  ProverPublic   := p,q,g,y;
  VerifierPublic := p,q,g,y;
}

ChallengeLength     := 80;
ProtocolComposition := P_1;

Def SigmaPhi P_1 {
  Homomorphism (phi : G -> H : (a) |-> (g^a));
14:   ChallengeLength := 80;
15:   Relation ((y) = phi(x));
16: }
```

Lines 01-07 declare the protocol inputs and describe which values are known to which party. If for example the verifier did not know a public parameter, it would be sent by the prover in a synchronization step. Lines 09-10 declare the knowledge error that has to be reached, and how the predicates should be composed. Finally, lines 12-16 describe the only predicate in this example. This description is a direct analogon to the Camenisch-Stadler notation [CS97a].

Efficiency of code. As mentioned above, the "efficiency of code" challenge has to be dealt with on two levels. On a high level, the compiler has to find the most efficient protocol specification meeting a given semantic proof goal. The choice of the proof technique to use will depend on the priorities the user gives to communicational- respectively computational complexity, as there is often a tradeoff between those. A deeper discussion is given in the next paragraph. On a low level, we'll provide a compiler backend that outputs code in the CAO ("Cryptography Aware language and cOmpiler") language [BNPS05]. This is a language and a compiler geared towards the generation of an efficient and secure low-level implementation of cryptographic primitives; CAO is also being developed within the CACE project.

Let us discuss the remaining challenges in more detail.

Designing ZK-PoK. At the moment we are designing a high-level language in which the semantic goal of a ZK-PoK together with its non-functional properties can be formulated in a user-friendly way. The language is inspired by the well-known Camenisch-Stadler notation [CS97a] which is used to formulate the intended semantic goal. We enrich this with non-functional properties which allow to specify optimization goals (e.g., optimize computational or communicational complexity) and the security level (e.g., knowledge error, tightness of the statistical zero-knowledge property, etc.) of the protocol being generated. In this high-level language, we abstract away as many technical details as possible to ease design and usage of ZK-PoK for non-experts.

In our architecture (cf. Fig. 1) the high-level compiler is responsible for finding a protocol specification that realizes the semantic proof goal and simultaneously takes into consideration the user's non-functional specifications. To enable the compiler to make "good" decisions, the compiler backend reports the costs on a specific target platform upwards to the high-level compiler. For example efficient interval proofs can be realized either with the techniques of [Bou00] or [Lip03] with different costs.

To be able to actually build a compiler for the semantics of that high-level language we are currently working on a unified theoretical framework for the various ZK-PoK techniques. For this, we extend the existing theory for zero-knowledge proofs which by now mainly deals with known order groups

[Bra97,BS02,Cra96,CDS94]. Our extended theoretical framework is capable to cope with arbitrary combinations of protocols in hidden order groups (e.g., RSA groups) as well [BCM05,CKY09,DF02]. To this end, we have conceived the new Σ^{exp} protocol [BCK$^+$08], which yields efficient ZK-PoK in a more modular manner than the existing protocols [BCM05,CKY09,DF02].

A first prototype of our compiler and semantic language [BCK$^+$08] implements a subset of the envisaged compiler framework. It already supports the generation of various crypto-systems such as Pedersen commitments/verifiable secret sharing [Ped92], Schnorr authentication/signatures [Sch91], electronic cash [Bra94,CFT98,Oka95], group signatures [CL04], or ring signatures [CDS94].

Correctness and security of implementations. One of our main goals concerning the security of the code output by the compiler, is to formally verify the zero-knowledge and proof of knowledge properties. To this end we are developing a protocol verification toolbox as part of our compiler framework (see Fig. 1). Its task is to accomplish a semi- or (ideally) fully automatic formal verification of these properties.

We currently focus on the proof of knowledge property. The toolbox takes as input the user's description of the semantic goal and the protocol implementation (output by the compiler). It then interprets this information in order to assemble a proof goal for the Isabelle/HOL theorem prover [PNW93]. The theorem prover then formally verifies whether the protocol is indeed a proof of knowledge for the given goal (by constructing a knowledge extractor).

One step towards automating this verification process is to consider the most relevant proof strategies used in existing published proofs and to develop corresponding proof tactics for the theorem prover. Also, to facilitate this automated verification, the different parts of our compiler (i.e., the high-level compiler respectively the protocol compiler) annotate helper data to the code they output.

We have already formally verified the proof of knowledge property for basic protocols such as those in [DF02,Sch91] and generic AND– and OR– compositions among those. Currently, we are tackling more complex protocols.

Last but not least, also to assert code security properties (e.g., against buffer overflows and side channel attacks) we rely on the verified compiler backend to output CAO-code [BNPS05] (see above). The CAO language is designed to automatically generate secure implementations resistant against software side-channels.

References

[ARS05] A. Adelsbach, M. Rohe, and A.-R. Sadeghi. Complementing zero-knowledge watermark detection: Proving properties of embedded information without revealing it. *Multimedia Systems*, 11(2):143–158, 2005.

[Ate04] G. Ateniese. Verifiable encryption of digital signatures and applications. *ACM Transactions on Information and System Security*, 7(1):1–20, February 2004.

[Ban05] E. Bangerter. *Efficient Zero-Knowledge Proofs of Knowledge for Homomorphisms.* PhD thesis, Ruhr-University Bochum, 2005.

[BCC04] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In *Proc. ACM CCS 2004*, pages 132–145. ACM, 2004.

[BCK$^+$08] E. Bangerter, J. Camenisch, S. Krenn, A.-R. Sadeghi, and T. Schneider. Automatic generation of sound zero-knowledge protocols. Cryptology ePrint Archive, Report 2008/471, 2008.

[BCM05] E. Bangerter, J. Camenisch, and U. Maurer. Efficient proofs of knowledge of discrete logarithms and representations in groups with hidden order. In *International Workshop on Practice and Theory in Public-Key Cryptography – PKC 05*, volume 3386 of *LNCS*, pages 154–171. Springer, 2005.

[BG93] M. Bellare and O. Goldreich. On defining proofs of knowledge. In *Advances in Cryptology – CRYPTO 92*, volume 740 of *LNCS*, pages 390–420. Springer, 1993.

[BMP07] M. Barbosa, A. Moss, and D. Page. Compiler assisted elliptic curve cryptography. In *Information Security (IS)*, volume 4804 of *LNCS*, pages 1785–1802. Springer, 2007.

[BNPS05] M. Barbosa, R. Noad, D. Page, and N.P. Smart. First steps toward a cryptography-aware language and compiler. Cryptology ePrint Archive, Report 2005/160, 2005.

[Bou00] F. Boudot. Efficient proofs that a committed number lies in an interval. In *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 431–444. Springer, 2000.

[BP05] M. Barbosa and D. Page. On the automatic construction of indistinguishable operations. Cryptology ePrint Archive, Report 2005/174, 2005.

[Bra94] S. Brands. Untraceable off-line cash in wallet with observers. In *Advances in Cryptology – CRYPTO 93*, volume 773 of *LNCS*, pages 302–318. Springer, 1994.

[Bra97] S. Brands. Rapid demonstration of linear relations connected by boolean operators. In *Advances in Cryptology – EUROCRYPT 97*, volume 1233 of *LNCS*, pages 318–333. Springer, 1997.

[Bri04] T. Briner. Compiler for zero-knowledge proof-of-knowledge protocols. Master's thesis, ETH Zurich, 2004.

[BS02] E. Bresson and J. Stern. Proofs of knowledge for non-monotone discrete-log formulae and applications. In *ISC '02: Proceedings of the 5th International Conference on Information Security*, pages 272–288. Springer, 2002.

[Cam98] J. Camenisch. *Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem.* PhD thesis, ETH Zurich, Konstanz, 1998.

[CDS94] R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Advances in Cryptology – CRYPTO 94*, volume 839 of *LNCS*, pages 174–187. Springer, 1994.

[CFT98] A. Chan, Y. Frankel, and Y. Tsiounis. Easy come - easy go divisible cash. Technical Report TR-0371-05-98-582, GTE, 1998. Updated version with corrections.

[CH02] J. Camenisch and E. V. Herreweghen. Design and implementation of the idemix anonymous credential system. In *Proc. ACM CCS 2002*, pages 21–30. ACM, 2002. `http://www.zurich.ibm.com/security/idemix/`.

[CKY09] J. Camenisch, A. Kiayias, and M. Yung. On the portability of generalized schnorr proofs. Cryptology ePrint Archive, Report 2009/050, 2009. To appear at *EUROCRYPT 2009*.

[CL01] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Advances in Cryptology – EUROCRYPT 2001*, volume 2045, pages 93–118. Springer, 2001.

[CL04] J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *LNCS*, pages 56–72. Springer, 2004.

[CM99] J. Camenisch and M. Michels. Proving in zero-knowledge that a number is the product of two safe primes. In *Advances in Cryptology – EUROCRYPT 99*, volume 1592 of *LNCS*, pages 107–122. Springer, 1999.

[Cra96] R. Cramer. *Modular Design of Secure yet Practical Cryptographic Protocols*. PhD thesis, CWI and University of Amsterdam, 1996.

[CRS05] J. Camenisch, M. Rohe, and A.-R. Sadeghi. Sokrates - a compiler framework for zero-knowledge protocols. In *Western European Workshop on Research in Cryptology – WEWoRC 05*, 2005.

[CS97a] J. Camenisch and M. Stadler. Efficient group signature schemes for large groups (extended abstract). In *Advances in Cryptology – CRYPTO 97*, volume 1294, pages 410–424. Springer, 1997.

[CS97b] J. Camenisch and M. Stadler. Proof systems for general statements about discrete logarithms. Technical Report 260, Institute for Theoretical Computer Science, ETH Zürich, 1997.

[DF02] I. Damgård and E. Fujisaki. A statistically-hiding integer commitment scheme based on groups with hidden order. In *Advances in Cryptology – ASIACRYPT 2000*, volume 2501 of *LNCS*, pages 77–85. Springer, 2002.

[DFK$^+$93] C. Dwork, U. Feige, J. Kilian, M. Naor, and M. Safra. Low communication 2-prover zero-knowledge proofs for np. In *Advances in Cryptology – CRYPTO 92*, volume 740 of *LNCS*, pages 215–227, London, UK, 1993. Springer.

[FO97] E. Fujisaki and T. Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In *Advances in Cryptology – CRYPTO 97*, volume 1294, pages 16–30. Springer, 1997.

[FS87] A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. In *Advances in Cryptology – CRYPTO 86*, volume 263 of *LNCS*, pages 186–194. Springer, 1987.

[GMR85] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Proc. 17th ACM Symp. on Theory of Computing*, pages 291–304, New York, NY, USA, 1985. ACM.

[GMW91] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(1):691–729, 1991. Preliminary version in 27th FOCS, 1986.

[GQ90] L. Guillou and J. Quisquater. A "paradoxical" identity-based signature scheme resulting from zero-knowledge. In *Advances in Cryptology – CRYPTO 88*, volume 403 of *LNCS*, pages 216–231. Springer, 1990.

[IKOS07] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai. Zero-knowledge from secure multiparty computation. In *Proc. 39th ACM Symp. on Theory of Computing – STOC 07*, pages 21–30, New York, NY, USA, 2007. ACM.

[Lip03] H. Lipmaa. On diophantine complexity and statistical zeroknowledge arguments. In *Advances in Cryptology – ASIACRYPT 2000*, volume 2894 of *LNCS*. Springer, 2003.

[LPS08] Y. Lindell, B. Pinkas, and N. Smart. Implementing two-party computation efficiently with security against malicious adversaries. In *Security in Communication Networks – SCN 2008*, volume 5229 of *LNCS*, pages 2–20. Springer, 2008.

[MNPS04] D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella. Fairplay — a secure two-party computation system. In *USENIX Security '04*, 2004. `http://www.cs.huji.ac.il/project/Fairplay/fairplay.html`.

[MOR03] P. MacKenzie, A. Oprea, and M. K. Reiter. Automatic generation of two-party computations. In *Proc. ACM CCS 2003*, pages 210–219. ACM, 2003.

[Oka95] T. Okamoto. An efficient divisible electronic cash scheme. In *Advances in Cryptology – CRYPTO 95*, volume 963 of *LNCS*, pages 438–451. Springer, 1995.

[Ped92] T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Advances in Cryptology – CRYPTO 91*, volume 576 of *LNCS*, pages 129–140. Springer, 1992.

[PNW93] L. C. Paulson, T. Nipkow, and M. Wenzel. The isabelle reference manual. Technical report, 1993.

[PRS02] M. Prabhakaran, A. Rosen, and A. Sahai. Concurrent zero knowledge with logarithmic round-complexity. In *Proc. 43rd IEEE Symp. on Foundations of Comp. Science – FOCS 02*, pages 366–375, Washington, DC, USA, 2002. IEEE Computer Society.

[Sch91] C. Schnorr. Efficient signature generation by smart cards. *Journal Of Cryptology*, 4(3):161–174, 1991.

[Sha79] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.