

Report on “On security of practical adaptor signatures”

This is a thesis on the security of so-called adaptor signatures. The student introduces new security definitions and proves security proofs for ECDSA algorithms.

The thesis starts with an introduction that gives definitions of notions such as random oracles, non-interactive zero-knowledge proofs. Then she proceeds with standard constructions that use DLP (discrete logarithm problem) and discusses standard security definitions and proofs by giving extended examples.

In the second chapter, the student explains the relatively new notion of adaptor signatures that has applications in Bitcoin related algorithms. The thesis then explains certain “robust” security definitions that are frequently used in the literature. The final section is the student’s contribution where she applies an attack of [19] to a specific instance of ECDSA.

In Chapter 3, the student shows that by restricting attacker’s access to the oracle in a specific way (which leads to the new security definitions, i.e., Definitions 14, 15, 16, 17) she can give security proofs for aECDSA+(DLOG) scheme.

Finally in Chapter 4 efficiency issues are considered.

I have two questions regarding the thesis and a few minor comments.

Question 1. In Chapter 4, new security definitions are introduced. The following quote is from Introduction.

We then illustrate the limits of the security definitions in [4]. Considering the security definitions for adaptor signatures for ECDSA, we show a theoretical attack in the context of Bitcoin elliptic curve, which suggests that the original security definitions in [4] are not suitable for practical adaptor signatures for ECDSA in relevant applications.

In Chapter 3, we present our main contribution. Since there is no proof of security for practical adaptor signatures for ECDSA, we present new security definitions that do not allow our attack from Chapter 2. Then, we prove that the practical adaptor signature for ECDSA satisfies our notion of security.

Could you elaborate a bit more on this? Why don’t we deduce, given the existence of an attack, that maybe ECDSA is not secure, but we deduce that security definitions are limited? Why do the new restricted definitions make sense for adaptor signatures?

Question 2. In the end of the Chapter 2, when the attack of [19] was being modified to Pollard-rho instead of BSGS, it was mentioned:

[...] it was not clear to us how to compute the following group element efficiently enough so that the time complexity of the original attack would be preserved. Specifically, it was not clear, given $(x^u)^{a_i}G$ and access to FDH_{pk} , how to efficiently compute $(x^u)^{2a_i}G$ for the unknown secret key x and an arbitrary a_i .

Doesn't $FDH(zG, zG)$ return z^2G ? Thus, when $z = (x^u)^{a_i}G$ we get $z^2 = (x^u)^{2a_i}G$. Similarly $(x^u)^{a_i}G$ can be retrieved by $O(\log a_i)$ calls to FDH , starting from x^uG and by employing a square-and-multiply algorithm. What am I missing here?

Topic of the thesis: The thesis is on cryptographic security related to the recent notion of *adaptor signature* and is suitable for a Master's thesis.

Mathematical content: The mathematical content, which includes design and analysis of cryptographic algorithms, is suitable.

Citations/References: Many sources are used which are cited carefully overall the thesis.

Student's contribution: This includes new and more adequate security definitions (Definitions 14, 15, 16 and 17 of Chapter 4), security proofs of ECDSA adaptor signatures using these new definitions, also adoption of an attack originated in [19] to an instance of ECDSA `secp256k1` elliptic-curve-group used in Bitcoin.

The level of English and writing is very good.

A few small issues:

- In the Introduction, a paragraph starting with Bob does not look good. Use of "quote" environment produces better effect.
- When citing (esp. a book), one should be more precise, e.g., [7, p. 133].
- "information additional" change to "additional information"
- When using an acronym the whole phrase (Elliptic Curve Digital Signature Algorithm) should be mentioned at least once.

Conclusion: I think the thesis is well-written. Introduction explains the subject matter clearly and leads to Chapter 2 which precisely describes the problem. Then the problem is solved in Chapter 3 with standard methods in applied cryptography – security proofs under new security definitions. This is a good contribution that deserves to be recognised as a Master's thesis.