Efficient implementation of code-based identification/signatures schemes

Pierre-Louis Cayrel, Sidi Mohamed El Yousfi Alaoui, Felix Gunther, Gerhard Hoffmann, Holger Rother

Efficient implementation of code-based identification schemes

Pierre-Louis Cayrel, Sidi Mohamed El Yousfi Alaoui, Felix Günther, Gerhard Hoffmann and Holger Rother

CASED – Center for Advanced Security Research Darmstadt,
Mornewegstrasse, 32
64293 Darmstadt
Germany

Abstract. In this paper we present efficient implementations of several code-based identification schemes, namely the Stern scheme, the Véron scheme and the Cayrel-Véron-El Yousfi scheme. For a security of 80 bits, we obtain a signature in respectively 1.048 ms, 0.987 ms and 0.594 ms.

Keywords: Cryptography, Zero-knowledge identification, coding theory, efficient implementation.

1 Introduction

Code-based zero-knowledge identification and signature schemes are an interesting alternative to classical (number theory based) digital signatures. Supposed to resist quantum attacks, several code-based cryptosystems have been developed recently. Shor has showed a quantum algorithm which solves in polynomial time the problems of discrete logarithm and factorization in [9], but no quantum attack exists, so far, to solve the hard problems on which the code-based cryptosystems are based.

In 1993, Stern proposed in [11] the first zero-knowledge identification scheme based on the hardness of the binary syndrome decoding problem. A few years later, Véron in [12] has designed a scheme with a lower communication cost. Recently, Cayrel et al. in [3] have designed a scheme which reduce even more this communication cost.

Using quasi-cyclic and quasi-dyadic constructions, several new constructions like [1, 7] permits to reduce the size of the public matrices. We can use the same kind of matrices in the context of zero-knowledge identification and signature without lower the security of the resulting schemes.

Our contribution In this paper we provide, to our knowledge the first, efficient implementations of the previous schemes for identification and signature. In [2], the authors presented a smart implementation of the Stern scheme but it was more a proof of concept than an efficient implementation.

Organization of the paper Section 2 describes the Stern, Véron and Cayrel-Véron-ElYousfi schemes. Section 3 describes the results of our implementations. Section 4 concludes the paper.

2 Code-based zero-knowledge identification schemes

In code-based cryptography, there have been many attempts to design identification schemes. In such constructions, there are two main goals: On the one hand, a prover wants to convince a verifier of its identity. On the other hand, the prover does not want to reveal any additional information that might be used by an impersonator. In the following, we will give an overview of three proposals in this area.

2.1 Stern scheme

The first code-based zero-knowledge identification scheme was presented at Crypto'93 by Stern [11], its security is based on the syndrome decoding (SD) problem. It uses a public parity-check matrix of the code over the binary field $\mathbb{F}_2$. This scheme is a multiple-rounds identification protocol, where each round is a three-pass interaction between the prover and the verifier. A cheater has a probability of 2/3 per round to succeed in the protocol without the knowledge of the secret key. The number of rounds depends on the security level needed; for 80 bits security level, one needs about 150 rounds. For instance to achieve the weak and strong authentication probabilities of 2^{-16} and 2^{-32} according the norm ISO/IEC-9798-5, one needs respectively 28 and 56 rounds.

2.2 Véron scheme

In 1996, Véron proposed in [12] a dual version of Stern's scheme. It uses a generator matrix instead of a parity-check matrix of the code, which has the advantage to reduce slightly the communication costs. Véron's scheme, as Stern's, is a multiple rounds zero-knowledge protocol, where each round is a three-pass interaction between the prover and the verifier, for which the success probability for a cheater is 2/3. Moreover, Véron suggested in [12] to use special techniques over finite fields to reduce the computation and storage complexity of his scheme.

2.3 Cayrel-Véron-El Yousfi scheme

In 2010, Cayrel, Véron, and El Yousfi (CVE) presented in [3] a five-pass identification protocol using q-ary codes instead of binary codes. In addition to the new way to calculate the commitments, the idea of this protocol uses another improvement which is inspired by [8, 10]. The main achievement of this proposal is to decrease the cheating probability of each round from 2/3 for Stern's and Véron's schemes to 1/2. This allows to decrease the communication complexity and then to provide the desired security level in fewer rounds

compared to Stern and Véron constructions. Furthermore, this scheme offers a small public key size, about 4 kBytes, whereas that of Stern and Véron scheme is almost 15 kBytes for the same level of security. It is proven in [3] that this scheme verifies the zero-knowledge proof and its security is based on the hardness of the syndrome decoding problem defined over $\mathbb{F}_q$.

Since a large public matrix size is one of the drawbacks of code-based cryptography, there have been many proposals which consists of replacing the random codes by particular structured codes, namely quasi-cyclic proposed by Gaborit and Girault in [5] or quasi-dyadic codes proposed by Miscozki and Barreto in [7]. We can use the both variants in the three identifications schemes presented above, in order to store the public matrix more efficiently.

We can also mention that the three presented identification schemes can be turned into secure signature schemes by using the idea of Fiat-shamir paradigm.

3 Efficient implementation

3.1 Description

In total, six different schemes have been implemented in C: the Stern, Véron and CVE identification schemes and the corresponding signature schemes based on the Fiat-Shamir transform [6]. The idea of the transform is to split the identification scheme in two parts. In the first part, the signer runs the identication scheme as before, but only recording the responses without any checks. In the second part, the verifier replays the saved responses and performs the necessary checks. This also explains the relatively high signature size of schemes based on the Fiat-Shamir transform. It also shows the varying sizes of the signatures, as the given responses change from run to run with high probability.

All implementations use the SHA-3 finalist Keccak [4], both as hash function and as random oracle. All tests have been carried out on an Intel(R) Core(TM)2 Duo CPU E8400@3.00GHz machine, the source code is publicly available.[1].

3.2 Results

The following tables give the timings of some test runs. For the signature schemes files of size about 1 MB, 10 MB and 25 MB have been used. As expected, the actual responses (i.e. challenges) vary from run to run. The signatures sizes in Table 2 are taken as approximate values across multiple runs.

As the code of the implementations does not use any object-oriented features, a straightforward efficient Java implementation should be possible as well.

[1] `http://cayrel.net/spip.php?article189`

	Stern	Véron	CVE
Rounds	28	28	16
n, r, w	768, 384, 76	768, 384, 76	144, 72, 55
Security level	2^{80}	2^{80}	2^{80}
Random	1.048 ms	0.987 ms	0.594 ms
n, r, w	1024, 512, 128	1024, 512, 128	256, 128, 97, 256
Security level	2^{73}	2^{73}	2^{143}
Quasi-Cyclic	1.893 ms	1.634 ms	1.829 ms
Quasi-Dyadic	2.655 ms	2.522 ms	1.775 ms

Table 1. Timing results for Stern, Véron and Cayrel, Véron, and El Yousfi (CVE) identification schemes.

	Stern	Véron	CVE
Rounds	28	28	16
n, r, w	768, 384, 76	768, 384, 76	144, 72, 55
Security level	2^{80}	2^{80}	2^{80}
Message size [by.]	**Random (Sign/Verify [ms])**		
1.363.024	0.008/0.007	0.008/0.007	0.013/0.012
10.317.040	0.055/0.054	0.054/0.054	0.106/0.118
23.766.127	0.126/0.125	0.124/0.124	0.247/0.243
Signature size [by.]	60.000	60.000	15.000
n, r, w	1024, 512, 128	1024, 512, 128	256, 128, 97, 256
Security level	2^{73}	2^{73}	2^{143}
Message size [by.]	**Quasi-Cyclic (Sign/Verify [ms])**		
1.363.024	0.008/0.007	0.008/0.007	0.014/0.013
10.317.040	0.056/0.053	0.055/0.054	0.108/0.105
23.766.127	0.129/0.126	0.125/0.125	0.247/0.243
Message size [by.]	**Quasi-Dyadic (Sign/Verify [ms])**		
1.363.024	0.009/0.008	0.009/0.008	0.014/0.013
10.317.040	0.056/0.054	0.056/0.055	0.104/0.108
23.766.127	0.127/0.125	0.126/0.126	0.247/0.243
Signature size [by.]	80.000	80.000	25.000

Table 2. Timing results for Stern, Véron and Cayrel, Véron, and El Yousfi (CVE) signature schemes. The signature sizes are approximate values.

4 Conclusion

In this paper, we have described three existing code-based identification and signature and have provided a detailed comparison of their implementation. As a result, we obtain three very fast signature (in less than 1ms) but very long signature size from 25.000 for CVE to 80.000 bytes for Stern and Véron. The security of the implementations faces side-channel attacks (like SAP and first order DPA) has been studied in [2] but the security of those implementations faces fault-injection or higher order DPA has not been studied yet. The source codes are available here : `http://cayrel.net/spip.php?article199`.

References

1. T. P. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing Key Length of the McEliece Cryptosystem. In *Progress in Cryptology – Africacrypt'2009*, volume 5580 of *LNCS*, pages 77–97. Springer, 2009.
2. P.-L. Cayrel, P. Gaborit, and E. Prouff. Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices. *CARDIS*, 2008.
3. P.-L. Cayrel, P. Véron, and S. M. Y. Alaoui. A Zero-Knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem. In *Selected Areas in Cryptography*, pages 171–186, 2010.
4. G. Bertoni, J. Daemen, M. Peeters and G. V. Assche. The Keccak sponge function family. `http://keccak.noekeon.org/`.
5. P. Gaborit and M. Girault. Lightweight Code-based Authentication and Signature. In *IEEE International Symposium on Information Theory – ISIT'2007*, pages 191–195, Nice, France, 2007. IEEE.
6. M. Abdalla and J.H. An and M. Bellare and C. Namprempre. From Identification to Signatures Via the Fiat-Shamir Transform: Necessary and Sufficient Conditions for Security and Forward-Security. *IEEE Transactions on Information Theory*, pages 3631–3646, 2008.
7. R. Misoczki and P. S. L. M. Barreto. Compact McEliece Keys from Goppa Codes. Preprint, 2009. `http://eprint.iacr.org/2009/187.pdf`.
8. A. Shamir. An Efficient Identification Scheme Based on Permuted Kernels. In *Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '89, pages 606–609, London, UK, 1990. Springer-Verlag.
9. P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26:1484–1509, 1995.
10. J. Stern. Designing Identification Schemes with Keys of Short Size. In *Advances in Cryptology – Proceedings of CRYPTO '94*, volume 839, pages 164–173, 1994.
11. J. Stern. A New Identification Scheme Based on Syndrome Decoding. In *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology*, pages 13–21, New York, NY, USA, 1994. Springer-Verlag New York, Inc.
12. P. Véron. Improved Identification Schemes Based on Error-Correcting Codes. *Appl. Algebra Eng. Commun. Comput.*, 8(1):57–69, 1996.