Povzetek

V tem delu bomo spoznali konkreten sistem digitalnega denarja in se poskušali čimbolj približati praktični implementaciji. Najprej bomo spoznali potrebne matematične in kriptografske osnove ter nekaj osnov monetarne ekonomije. Nato bomo izbrali konkreten sistem digitalnega denarja, ki ga je iznašel Brands, in ga poskušali čimbolj prilagoditi praktičnim zahtevam. Pri tem bodo igrali bistveno vlogo certifikati s skrivnim ključem, ki so tudi njegov izum. Za nas bodo najpomembnejši omejeni slepi podpisi certifikatov s skrivnim ključem, ki bodo omogočali učinkovito izdajanje digitalnega denarja. Namen diplome je prikazati trenutno dogajanje na področju digitalnega denarja in podati dovolj informacij za praktično implementacijo.

Ključne besede: digitalni denar, elektronski kovanci, razširitve digitalnega denarja, omejeni slepi podpisi, certifikati s skrivnim ključem.

Abstract

In this thesis a practical off-line digital money system is introduced with a practical implementation in mind. First we develop some mathematical and cryptographical background and also explain some monetary economy. After that we give a description of common properties of different digital money systems and choose one for a detailed study. The chosen system was invented by Brands and is well suited for a practical implementation. The system is based on secret-key certificates that were also invented by Brands. Of our main interest are restrictive blind signatures of secret-key certificates that make possible to construct efficient withdrawal protocols. Our aim is to provide a reader with a general overview of current digital money systems and enough knowledge for a practical implementation.

Keywords: digital money, electronic coins, extensions of off-line cash, restrictive blind signatures, secret-key certificates.

Math. Subj. Class. (2000): 94A60, 94A62.

Literatura

[Bar00] J. Barbič, "Schoofov algoritem", Diplomsko delo, Fakulteta za matematiko in fiziko v Ljubljani, 2000.

[BBC+94] J.-P. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjølsnes, F. Muller, T. Pedersen, B. Pfitzmann, P. de Rooij, B. Schoenmakers, M. Schunter, L. Vallée, and M. Waidner, "The ESPRIT Project CAFE - High Security Digital Payment Systems", ESORICS 94, LNCS 875 (Berlin), Springer-Verlag, 1994, pp. 217–230.

[Ble99] G. Bleumer, "Many-Time Restrictive Blind Signatures", 1999, `http://citeseer.nj.nec.com/bleumer99manytime.html`.

[Bra] "Personal homepage of Stefan Brands", `http://www.xs4all.nl/~brands`.

[Bra93] S. Brands, "An Efficient Off-line Electronic Cash System Based On The Representation Problem.", 246, Centrum voor Wiskunde en Informatica (CWI), ISSN 0169-118X, 1993, p. 77.

[Bra94a] S. Brands, "Electronic Cash on the Internet", 1994, `http://citeseer.nj.nec.com/brands95electronic.html`.

[Bra94b] S. Brands, "Off-Line Cash Transfer by Smart Cards", Tech. Report CS-R9455, CWI, 1994.

[Bra94c] S. Brands, "Untraceable Off-line Cash in Wallets with Observers", Proc. CRYPTO '93 (Douglas R. Stinson, ed.), Springer-Verlag, 1994, pp. 302–318.

[Bra95a] S. Brands, "Off-Line Electronic Cash Based on Secret-Key Certificates", Proceedings of the Second International Symposium of Latin American Theoretical Informatics (LATIN '95) (Valparaiso, Chili), vol. 911, Springer-Verlag, 1995, pp. 131–166.

[Bra95b] S. Brands, "Restrictive Blinding of Secret-Key Certificates", 144, Centrum voor Wiskunde en Informatica (CWI), ISSN 0169-118X, 1995, p. 35.

[Bra95c] S. Brands, "Secret-Key Certificates", 103, Centrum voor Wiskunde en Informatica (CWI), ISSN 0169-118X, 1995, p. 16.

[Bra95d] S. Brands, "Secret-Key Certificates (continued)", 99, Centrum voor Wiskunde en Informatica (CWI), ISSN 0169-118X, 1995, p. 16.

[Bra97] S. Brands, "Rapid Demonstration of Linear Relations Connected by Boolean Operators", Theory and Application of Cryptographic Techniques, 1997, pp. 318–333.

[Bra98] S. Brands, "Electronic Cash", Handbook on Algorithms and Theory of Computation, CRC Press, November 1998.

[FS87] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems", Advances in Cryptology — CRYPTO '86 (New York), Springer-Verlag, 1987, pp. 186–194.

[FTY97] Y. Frankel, Y. Tsiounis, and M. Yung, "Indirect Discourse Proofs: Achieving Efficient Fair Off-Line E- cash", Asiacrypt '96, LNCS 1163 (Berlin), Springer-Verlag, 1997, pp. 287–300.

[Mik01] M. Mikac, "Evidenca poštnih plačil v digitalni dobi", Diplomsko delo, Fakulteta za matematiko in fiziko v Ljubljani, 2001.

[Oka95] T. Okamoto, "An Efficient Divisible Electronic Cash Scheme", Proc. of CRYPTO '95, 1995, pp. 438–451.

[OO88] K. Ohta and T. Okamoto, "A modification to the Fiat-Shamir scheme", Proc. of CRYPTO '88, Springer-Verlag, 1988.

[OO89] T. Okamoto and K. Ohta, "Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducibility", Advances in Cryptology – EUROCRYPT '89, LNCS 434, Springer-Verlag, 1989, pp. 481–496.

[OO90] T. Okamoto and K. Ohta, "Disposable Zero-Knowledge Authentication and their Applications to Untraceable Electronic Cash", Advances in Cryptology — CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 134–149.

[OO92] T. Okamoto and K. Ohta, "Universal Electronic Cash", Proc. of CRYPTO '91, LNCS 576, Springer-Verlag, 1992, pp. 324–337.

[Pes00] L. Pesonen, "A Comparison of Chaum's and Brands' Electronic Cash Schemes", 2000, `http://citeseer.nj.nec.com/401417.html`.

[PS96] D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes", Theory and Application of Cryptographic Techniques, 1996, pp. 387–398.

[sciAJ97] A. Jurišić in A. J.Menezes, "Elliptic Curves and Cryptography", Dr. Dobbs Journal (1997), 26–37.

[SPC95] M. Stadler, J.-M. Piveteau, and J. Camenisch, "Fair Blind Signatures", Theory and Application of Cryptographic Techniques, 1995, pp. 209–219.

[Sti95] Douglas R. Stinson, "Cryptography: Theory and Practice", CRC Press, 1995.

[vA90] H. van Antwerpen, "Electronic cash", Magistersko delo, CWI, 1990.

[Vid89] I. Vidav, "Algebra", Mladinska knjiga, 1989.

[Way96] Peter Wayner, "Digital Cash: Commerce on the Net", Academic Press, 1996.

[Bra00] S. Brands, "Rethinking Public Key Infrastructure and Digital Signatures", MIT Press, 2000.

[CAFa] "CAFE - Conditional Access For Europe", `http://www.semper.org/sirene/projects/cafe`.

[CAFb] "CAFE - OPERA", `http://www.ercim.org/publication/Ercim_News/enw30/hirschfeld.html`.

[Can97] R. Canneti, "Toward realizing random oracles: Hash functions that hide all partial information", Proc. of CRYPTO '97, 1997, pp. 455–469.

[CFT98] A. H. Chan, Y. Frankel, and Y. Tsiounis, "Easy Come - Easy Go Divisible Cash", Theory and Application of Cryptographic Techniques, 1998, pp. 561–575.

[Cha83] D. Chaum, "Blind Signatures for Untraceable Payments", Proc. CRYPTO '82 (New York) (R. L. Rivest, A. Sherman, and D. Chaum, eds.), Plenum Press, 1983, pp. 199–203.

[Cha90] D. Chaum, "Zero-Knowledge Undeniable Signatures", Theory and Application of Cryptographic Techniques, 1990, pp. 458–464.

[CP] R. Cramer and T. Pedersen, "Improved Privacy in Wallets with Observers", `http://citeseer.nj.nec.com/366607.html`.

[CP93a] D. Chaum and T. Pedersen, "Transferred cash grows in size", Proc. EUROCRYPT '92, LNCS 658 (New York), Springer-Verlag, 1993, pp. 390–407.

[CP93b] D. Chaum and T. Pedersen, "Wallet Databases with Observers", Advances in Cryptology: Proc. of CRYPTO '92, LCNS 740, Springer-Verlag, 1993, pp. 89–105.

[CPS96] J. Camenisch, J.-M. Piveteau, and M. Stadler, "An Efficient Fair Payment System", ACM Conference on Computer and Communications Security, 1996, pp. 88–94.

[CvA90] D. Chaum and H. van Antwerpen, "Undeniable signatures", Proc. CRYPTO 89, Springer-Verlag, 1990, pp. 212–217.

[DN88] A. Fiat D. Chaum and M. Naor, "Untraceable Electronic Cash", Advances in Cryptology - CRYPTO '88, 1988, pp. 319–327.

[eCa] "eCash Technologies, Inc.", `http://www.digicash.com`.

[ECT] "Eliptic Curve Online Tutorial", `http://www.certicom.ca`.

[EO94] T. Eng and T. Okamoto, "Single-Term Divisible Electronic Coins", Theory and Application of Cryptographic Techniques, 1994, pp. 306–319.

[Esp] "Esprit, the EU information technologies programme", `http://www.cordis.lu/esprit/home.html`.

[Fer93] N. Ferguson, "Single Term Off-Line Coins", Theory and Application of Cryptographic Techniques, 1993, pp. 318–328.

[Fer94] N. Ferguson, "Extensions of single-term coins", Advances in Cryptology — CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 292–301.