Quantum Inf Process (2012) 11:455–463
DOI 10.1007/s11128-011-0258-6

One-time proxy signature based on quantum cryptography

Tian-Yin Wang · Zong-Li Wei

Received: 12 April 2011 / Accepted: 8 July 2011 / Published online: 20 July 2011

Abstract We propose a new one-time proxy signature scheme with decoherence-free states. We analyze its security and show that it is not possible to forge a valid proxy signature even if an opponent has infinite resources. Furthermore, the differences between this scheme and others are discussed.

Keywords One-time proxy signature · Decoherence-free state · Quantum cryptography

1 Introduction

Proxy signature, as an important cryptographic primitive, was firstly introduced by Mambo, Usuda and Oka-moto in 1996 [1]. In a proxy signature scheme, an original signer can authorize another person, called proxy signer, to issue signatures on behalf of him/her. Proxy signatures are useful constructions in grid computing, mobile agent, mobile communications, e-commerce etc. [2,3]

Kim et al. proposed the concept of one-time proxy signatures to restrict the power of the proxy signer, i.e., the proxy signer can sign only once in the scheme [4]. The signature is a variant of the ElGamal signature and its security rests on the discrete logarithm assumption. Since then, one-time proxy signature attracted much attention [5–7].

T.-Y. Wang (✉) · Z.-L. Wei
School of Mathematical Science, Luoyang Normal University, Luoyang 471022, Henan, China
e-mail: wangtianyin@yahoo.cn

T.-Y. Wang
State Key Laboratory of Information Security (Graduate University of Chinese Academy of Sciences), Beijing 100049, China

However, all the present schemes [4–7] for one-time proxy signature are computationally secure, which may be broken with the development of quantum computation [8,9]. Fortunately, the physics of quantum systems opens a door to tremendously intriguing possibilities for cryptography, the art and science of communicating in the presence of adversaries [10–15]. The idea of applying quantum mechanics to digital signature was firstly introduced by Gottesman and Chuang [16]. By far, various digital signature schemes based on quantum cryptography have been presented [17–22].

Yang et al. [23] proposed the concept of multi-proxy quantum group signature scheme in 2008, which can be used for signing classical message. Recently, Shi et al. [24] gave a multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform. Furthermore, the signatures in the two schemes have the properties of one-time proxy signature.

In this work, we propose a new one-time proxy signature scheme with decoherence-free states. Although we also take advantage of a cryptographic hash function, the security of this scheme is guaranteed by the laws of quantum physics alone.

2 Preliminaries

In this section, let us introduce proxy signature, hash function, decoherence-free state, and some other relevant preliminaries that are useful in presenting this new one-time proxy signature scheme.

2.1 Proxy signature

A proxy signature scheme consists of several requesters, an original signer, a proxy signer, and a verifier, and of three protocols.

- An authorizing protocol involving the original signer and the proxy signer.
- A signing protocol involving the proxy signer and a requester.
- A verifying protocol involving the verifier and the requester.

By executing the authorizing protocol, the proxy signer obtains a warrant or a proxy key from the original signer. Using the warrant or proxy key, the proxy signer can sign a message on behalf of the original signer in the signing protocol. By running the verifying protocol, the verifier can check the validity of the proxy signature.

In general, one-time proxy signature should have the following properties:

(a) Verifiability. The validity of a proxy signature as well as delegation of the original signer on a given message can be verified by the verifier.
(b) Distinguishability. The verifier can distinguish the proxy signature and the standard signature generated by the original signer.
(c) Non-forgeability. Nobody can generate a valid proxy signature except for the proxy signer.
(d) Non-deniability. Once the proxy signer issues a proxy signature, he/she cannot deny it.
(e) One-timeness. For every delegation operation, no more than one valid proxy signature can be securely generated by the proxy signer.

2.2 Hash function

A hash function is any well-defined procedure or mathematical function which converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index into an array. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes [25]. We denote a cryptographic hash function by

$$H(\cdot) : \{0, 1\}^* \longrightarrow \{0, 1\}^{k_1}, \tag{1}$$

which is used to generate a fingerprint in this paper. The notations ID_A, ID_B represent the identities of the original signer Alice and the proxy signer Bob, respectively, and the notation || denotes the concatenation of strings.

2.3 Decoherence-free states

Suppose that $U(t)$ denote the transformation of collective noise, where t denotes the time of transmission and means a temporal dependence. If an N-qubit state ρ_N is invariant under the collective noise $U(t)$, i.e.,

$$\rho_N = [U(t)]^{\otimes N} \rho_N [U(t)^{\dagger}]^{\otimes N}, \tag{2}$$

ρ_N is called an N-qubit decoherence-free state. The way to construct decoherence-free states has been conceived as one of the possible solutions to decoherence in quantum information processing [26–35].

The proposed scheme is based on the following four 4-qubit decoherence-free states

$$\begin{aligned}
|\Phi^0\rangle &= |\psi^-\rangle_{12} \otimes |\psi^-\rangle_{34} \\
&= \frac{1}{2}(|0101\rangle - |0110\rangle - |1001\rangle + |1010\rangle)_{1234}, && (3)\\
|\Phi^1\rangle &= \frac{1}{2\sqrt{3}}(2|0011\rangle - |0101\rangle - |0110\rangle \\
&\quad -|1001\rangle - |1010\rangle + 2|1100\rangle)_{1234}, && (4)\\
|\Psi^0\rangle &= \frac{1}{2}(|0011\rangle - |0110\rangle - |1001\rangle + |1100\rangle)_{1234}, && (5)\\
|\Psi^1\rangle &= \frac{1}{2\sqrt{3}}(2|0101\rangle - |0011\rangle - |0110\rangle \\
&\quad -|1001\rangle - |1100\rangle + 2|1010\rangle)_{1234}. && (6)
\end{aligned}$$

In fact, $|\Psi^0\rangle$ is obtained by exchanging the positions of qubits 2 and 3 in the state $|\Phi^0\rangle$, and $|\Psi^1\rangle$ is obtained by exchanging the positions of qubits 2 and 3 in the state $|\Phi^1\rangle$. By simple computation, we can get

$$\langle \Phi^0 | \Phi^1 \rangle = 0, \tag{7}$$
$$\langle \Psi^0 | \Psi^1 \rangle = 0, \tag{8}$$
$$\langle \Phi^0 | \Psi^0 \rangle = \frac{1}{2}, \tag{9}$$
$$\langle \Phi^0 | \Psi^1 \rangle = \frac{\sqrt{3}}{2}, \tag{10}$$
$$\langle \Phi^1 | \Psi^0 \rangle = \frac{\sqrt{3}}{2}, \tag{11}$$
$$\langle \Phi^1 | \Psi^1 \rangle = \frac{1}{2}. \tag{12}$$

From Eqs. (7–12), we can see that $\{|\Phi^0\rangle, |\Phi^1\rangle\}$ and $\{|\Psi^0\rangle, |\Psi^1\rangle\}$ each form an orthogonal basis and these different orthogonal bases are nonorthogonal with respect to each other. Furthermore, $|\Phi^0\rangle$ and $|\Phi^1\rangle$ can be discriminated by local single-particle measurements because no common terms exists in Eqs. (13) and (14).

$$\begin{aligned} |\Phi^0\rangle = \frac{1}{2}(&|01-+\rangle - |01+-\rangle \\ &+|10+-\rangle - |10-+\rangle)_{1234}, \end{aligned} \tag{13}$$

$$\begin{aligned} |\Phi^1\rangle = \frac{1}{2\sqrt{3}}(&|00++\rangle - |00+-\rangle - |00-+\rangle \\ &+|00--\rangle - |01++\rangle + |01--\rangle \\ &-|10++\rangle + |10--\rangle + |11++\rangle \\ &+|11+-\rangle + |11-+\rangle + |11--\rangle)_{1234}, \end{aligned} \tag{14}$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. It is evident that $|\Psi^0\rangle$ and $|\Psi^1\rangle$ also can be discriminated by local single-particle measurements.

Applying the preliminaries introduced above, we will detail this new one-time proxy signature scheme in the next section.

3 The proposed one-time proxy signature scheme

The proposed one-time proxy signature scheme includes four phases: initializing phase, authorizing phase, signing phase, and verifying phase. An original signer Alice, a proxy signer Bob, a trusted verifier Charlie, and several requesters $U_i, i = 1, 2, \ldots, N$, are also involved.

3.1 Initializing phase

The original signer Alice establishes a k-bit key K_{AC} with Charlie in a secure manner, e.g., by using unconditionally secure quantum key distribution protocols [10,11]. The proxy signer Bob also establishes a k-bit key K_{BC} with Charlie in the same way. As

an aside, this phase is performed only once, i.e., the shared keys K_{AC} and K_{BC} could be reused, and this phase should be completed in advance.

3.2 Authorizing phase

The original signer Alice chooses a random number $r_A \in_R \{0,1\}^{k-k_1}$ and computes $R_A = H(m_\omega||r_A)$, where m_ω denotes the warrant negotiated by Alice and Bob, which includes the valid period of delegation, the identities of Alice and Bob, and the scope of authority etc. Then she generates the qubits $|s_\omega\rangle = \otimes_{i=1}^{k}|s^i\rangle$ by encoding the string $r_A||R_A$ with the key K_{AC}. The value of K_{AC}^i determines the encoding basis, i.e., if K_{AC}^i is 0, $|s^i\rangle$ is $|\Phi^0\rangle$ (or $|\Phi^1\rangle$) when $(r_A||R_A)^i = 0$ (or 1); else if K_{AC}^i is 1, $|s^i\rangle$ is $|\Psi^0\rangle$ (or $|\Psi^1\rangle$) when $(r_A||R_A)^i = 0$ (or 1), K_{AC}^i denotes the ith bit of K_{AC}, and $(r_A||R_A)^i$ denotes the ith bit of the string $r_A||R_A$. After her encoding, Alice sends these qubits $\otimes_{i=1}^{k}|s^i\rangle$ to Bob via a collective-noise quantum channel. At the same time, she sends the warrant m_ω to Bob via a classical channel.

When Bob receives the warrant m_ω and $|s_\omega\rangle$, he stores them in a secure method if he accepts Alice's delegation.

3.3 Signing phase

When the requester U_i wants to obtain the proxy signature of a message M, he sends a request to Bob, then he can obtain the proxy signature by executing the following signing protocol with Bob.

(1) The sender U_i sends the message M to Bob.
(2) When Bob receives the message M, he chooses a random number $r_B \in_R \{0,1\}^{k-k_1}$ and computes $R_B = H(m_\omega||M||r_B)$. Then he generates the qubits $|S\rangle = \otimes_{i=1}^{k}|S^i\rangle$ by encoding the string $r_B||R_B$ with the key K_{BC} in the same way as Alice does in the authorizing phase. After his encoding, he sends the qubits $|S\rangle$ and $|s_\omega\rangle$ to U_i via a collective-noise quantum channel. At the same time, he sends the warrant m_ω to U_i via a classical channel.

The resulting proxy signature that U_i obtains is $(|S\rangle, M, |s_\omega\rangle, m_\omega)$.

3.4 Verifying phase

When the proxy signature $(|S\rangle, M, |s_\omega\rangle, m_\omega)$ needs to be verified, U_i sends the qubits $|S\rangle$ and $|s_\omega\rangle$ to the verifier Charlie via a collective-noise quantum channel. At the same time, he sends the message M and m_ω to Charlie via a classical channel.

After receiving the message-signature pair $(|S\rangle, M, |s_\omega\rangle, m_\omega)$, Charlie checks whether the message M is in accord with the stipulate of the warrant m_ω or not. If it is not, the proxy signature is not valid; otherwise, he proceeds to perform single-particle measurements on the qubits $\otimes_{i=1}^{k}|s^i\rangle$ depending on the key K_{AC} shared with Alice. If K_{AC}^i=0, Charlie measures the first two qubits of the state $|s^i\rangle$ with the basis $\{|0\rangle, |1\rangle\}$ and the remaining two qubits with the basis $\{|+\rangle, |-\rangle\}$; otherwise, he

measures the first and the third qubits of the state $|s^i\rangle$ with the basis $\{|0\rangle, |1\rangle\}$ and the remaining two qubits with the basis $\{|+\rangle, |-\rangle\}$. By the same way, he measures the qubits $\otimes_{i=1}^{k}|S^i\rangle$ depending on the key K_{BC} shared with Bob. After gaining the measurement outcomes $r_A^{'}||R_A^{'}$ and $r_B^{'}||R_B^{'}$, Charlie verifies whether $R_A^{'}$ is equal to

$$H\left(m_\omega||r_A^{'}\right), \tag{15}$$

and $R_B^{'}$ is equal to

$$H\left(m_\omega||M||r_B^{'}\right). \tag{16}$$

If whichever is not true, the signature is not valid; otherwise, Charlie accepts the proxy signature and tells U_i the verification outcome.

So far, we have completed the scheme for one-time proxy signature under the condition that the error of the quantum channels is collective.

4 Security analysis and discussion

The proposed one-time proxy signature scheme is based on private key cryptosystems. The verifier Charlie knows the keys K_{AC} and K_{BC}. Moreover, he acts as the judge in the verifying phase. These enable him to generate a valid proxy signature. Therefore, the verifier Charlie must be totally credible in this scheme, i.e., he does not forge a proxy signature, or help one party to cheat the other party. In the following, we will show this scheme can satisfy the properties of one-time proxy signature suppose that Charlie is totally credible.

4.1 Verifiability

The verifying process of the proxy signature $(|S\rangle, M, |s_\omega\rangle, m_\omega)$ must use the warrant m_ω and the keys K_{AC} and K_{BC}; moreover, the warrant m_ω includes the valid period of delegation, the identities of Alice and Bob, and the scope of authority etc. Therefore, the verifier Charlie can confirm the delegation of the original signer Alice and the validity of the proxy signature $(|S\rangle, M, |s_\omega\rangle, m_\omega)$.

4.2 Distinguishability

Obviously, the proxy signature $(|S\rangle, M, |s_\omega\rangle, m_\omega)$ contains the warrant m_ω, and the proxy signer Bob's key K_{BC} must be used in the verifying phase. Therefore, the verifier Charlie can distinguish the proxy signature and the standard signature generated by the original signer easily.

4.3 Non-forgeability

Firstly, we show that it is impossible to forge Alice's delegation $(m_\omega, |s_\omega\rangle)$ except for Charlie. For the key K_{AC} is established in a secure manner [10,11], nobody can learn it through this process except for Alice and Charlie. Furtherly, if the opponent does not know the key K_{AC}, he will choose the wrong encoding bases with the probability 50% when he generates the qubits $|s_\omega\rangle$, which will introduce no less than 25% error rate, thus the probability that the opponent succeeds to forge a valid delegation $(m_\omega, |s_\omega\rangle)$ is $(\frac{3}{4})^k$. Another feasible attack is to tamper with the content of the warrant m_ω when the opponent (e.g., Bob) obtains the legitimate delegation $(m_\omega, |s_\omega\rangle)$. Unfortunately, it is impossible since he also has to prepare the corresponding qubits $|s_{\omega'}\rangle$. Therefore, it is impossible to generate a valid delegation $(m_\omega, |s_\omega\rangle)$ or tamper with the content of the warrant m_ω except for Alice and Charlie.

Secondly, we show that it is impossible to forge a valid proxy signature $(|S\rangle, M, |s_\omega\rangle, m_\omega)$ except for Charlie. For the opponent does not know the key K_{BC}, similarly, he will choose the wrong encoding bases with the probability 50% when he prepares the qubits $|S\rangle$ even if he intercepts a valid delegation $(m_\omega, |s_\omega\rangle)$, and thus the probability that the opponent succeeds to forge a valid proxy signature $(|S\rangle, M, |s_\omega\rangle, m_\omega)$ by impersonating the proxy signer Bob is $(\frac{3}{4})^k$. To tamper with the content of the message M is also impossible since the opponent must prepares the corresponding qubits $|S'\rangle$. Therefore, nobody can generate a valid proxy signature $(|S\rangle, M, |s_\omega\rangle, m_\omega)$ or tamper with the content of the message M except for Bob and Charlie.

4.4 Non-deniability

Only Bob and Charlie can generate a valid proxy signature; in addition, Charlie is totally trusted; moreover, the key K_{BC} is included in the verifying phase. Therefore, once the proxy signer Bob issues a proxy signature $(|S\rangle, M, |s_\omega\rangle, m_\omega)$, he cannot deny it.

4.5 One-timeness

The proxy signer Bob does not know the exact quantum state of the qubits $|s_\omega\rangle$, so he cannot generate a copy of the delegation $(m_\omega, |s_\omega\rangle)$ according to quantum no-cloning theorem. Therefore, Bob can use the delegation $(m_\omega, |s_\omega\rangle)$ only once, i.e., he can generate no more than one valid proxy signature on behalf of Alice.

From the above analysis, it can be seen that the proxy signature in the proposed scheme has all necessary properties of one-time proxy signature.

5 Discussions and conclusions

In the proposed scheme, the proxy signature $(|S\rangle, M, |s_\omega\rangle, m_\omega)$ are unknown non-orthogonal quantum states to the opponent, which cannot be perfectly distinguished

according to the measurement postulate of the quantum theory for the opponent. So, the opponent cannot acquire the hash value, which means that the proposed scheme can resist collision attacks. Therefore, although the proposed scheme also require a cryptographic hash function, this requirement is not strict as that in [4–7], i.e., we do not need a collision-free hash function and only require a general cryptographic hash function such as MD4, MD5 and SHA-1 etc.

Compared with the preceding works [4–7], the security of this scheme is based on fundamental properties of quantum mechanics and has nothing to do with the opponent's computing power. Moreover, this scheme has the advantage of low computational complexity since only single hash operations are required. Nevertheless, it is noted that this scheme is not easily realized with present technology because the proxy signer Bob and every requester have to store qubits.

In summary, we propose an information-theoretic secure one-time proxy signature scheme, in which Bob, the proxy signer can sign only once on behalf of the original signer. With the development of quantum technology, this scheme may have a wide application in grid computing, mobile agent, and e-commerce etc.

Acknowledgments We are grateful to the anonymous reviewers for help comments. This work was supported by the Natural Science Foundation of Henan Province (Grant No. 112300410192), the Open Foundation of State Key Laboratory of Information Security (Grant No. 01-04-2), and the Natural Science Foundation of Education Bureau of Henan Province (Grant Nos. 2010B120008, 2011A120006).

References

1. Mambo, M., Usuda, K., Okamoto, E.: Proxy signature: delegation of the power to sign messages. IEICE Trans. Fundam. **E79**(A(9)), 1338–1353 (1996)
2. Wang, T.Y., Cai, X.Q., Zhang, J.Z.: Off-line e-cash system with multiple banks based on elliptic curve. Comput. Eng. Appl. **33**(15), 155–157 (2007)
3. Cao, F., Cao, Z.F.: A secure identity-based proxy multi-signature scheme. Inf. Sci. **179**(3), 292–302 (2009)
4. Kim, H., Baek, J., Lee, B., et al.: Secret computation with secrets for mobile agent using one-time proxy signature. In: Proceedings of SCIS'2001, pp. 845–850. Oiso, Japan (2001)
5. Wang, H., Pieprzyk, J.: Efficient one-time proxy signatures. In: Proceedings of Asiacrypt 2003, pp. 507–522. Springer, Berlin (2003)
6. Mehta, M., Harn, L.: Efficient one-time proxy signatures. IEE Proc. Commun. **152**(2), 129–133 (2005)
7. Bicakci, K.: One-time proxy signatures revisited. Comput. Stand. Interfaces **29**(4), 499–505 (2007)
8. Shor, P.: Polynomial-time algorithms for prime factorization and discrete logrithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
9. Grover, L.K.: Quantum computers can search rapidly by using almost any transformation. Phys. Rev. Lett. **80**(19), 4329–4332 (1998)
10. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE Press, London (1984)
11. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121–3124 (1992)
12. Wang, T.Y., Wen, Q.Y., Chen, X.B., et al.: An efficient and secure multiparty quantum secret sharing scheme based on single photons. Opt. Commun. **281**(24), 6130–6134 (2008)
13. Wang, T.Y., Wen, Q.Y., Gao, F., et al.: Cryptanalysis and improvement of multiparty quantum secret sharing schemes. Phys. Lett. A **373**(1), 65–68 (2008)
14. Wang, T.Y., Wen, Q.Y., Zhu, F.C.: Economical quantum anonymous transmissions. J. Phys. B: At. Mol. Opt. Phys. **43**(24), 245501 (2010)

15. Wang, T.Y., Wen, Q.Y.: Security of a kind of quantum secret sharing with single photons. Quant. Inf. Comput. **11**(5–6), 0434–0443 (2011)
16. Gottesman, D., Chuang, I.: Quantum digital signatures. arXiv:quant-ph/0105032
17. Zeng, G.H., Christoph, H.K.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**(4), 042312 (2002)
18. Lee, H., Hong, C., Kim, H., Lim, J., et al.: Arbitrated quantum signature scheme with message recovery. Phys. Lett. A **321**(5–6), 295–300 (2004)
19. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A **79**(5), 054307 (2009)
20. Wen, X.J., Niu, X.M., Jia, L.P., et al.: A weak blind signature scheme based on quantum cryptography. Opt. Commun. **282**(5), 666–669 (2009)
21. Wang, T.Y., Wen, Q.Y.: Fair quantum blind signatures. Chin. Phys. B **19**(6), 060307 (2010)
22. Yang, Y.G., Zhou, Z., Teng, Y.W., et al.: Arbitrated quantum signature with an untrusted arbitrator. The Euro. Phys. J. D **61**(3), 773–778 (2011)
23. Yang, Y.G., Wen, Q.Y., Zhu, F.C.: Multi-proxy quantum group signature scheme with threshold shared verification. Chin. Phys. B **17**(2), 415–418 (2008)
24. Shi, J.J., Shi, R.H., Tang, Y., et al.: A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform. Quant. Inf. Proc. doi:10.1007/s11128-010-0225-7
25. Damgård, I.: A design principle for hash functions. In: Proceedings of the Crypto'89, pp. 416–427. Springer, Berlin (1990)
26. Lidar, D.A., Chang, I.L., Whaley, K.B.: Decoherence-free subspaces for quantum computation. Phys. Rev. Lett. **81**(12), 2594–2597 (1998)
27. Walton, Z.D., Abouraddy, A.F., Sergienko, A.V., et al.: Decoherence-free subspaces in quantum key distribution. Phys. Rev. Lett. **91**(8), 087901 (2003)
28. Boileau, J.C, Laflamme, R., Laforest, M., et al.: Robust quantum communication using a polarization-entangled photon pair. Phys. Rev. Lett. **93**(22), 220501 (2004)
29. Wang, X.B.: Fault tolerant quantum key distribution protocol with collective random unitary noise. Phys. Rev. A **72**(5), 050304 (2005)
30. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**(2), 022321 (2008)
31. Cabello, A.: Six-qubit permutation-based decoherence-free orthogonal basis. Phys. Rev. A **75**(2), 020301 (2007)
32. Sun, Y., Wen, Q.Y., Gao, F., et al.: Robust variations of the Bennett-Brassard 1984 protocol against collective noise. Phys. Rev. A **80**(3), 032321 (2009)
33. Qin, S.J., Wen, Q.Y., Meng, L.M., et al.: Quantum secure direct communication over the collective amplitude damping channel. Sci. China. Ser. G **52**(8), 1208–1212 (2009)
34. Wang, T.Y., Wen, Q.Y., Zhu, F.C.: Secure authentication of classical messages with decoherence-free states. Opt. Commun. **282**(16), 3382–3385 (2009)
35. Majgier, K., Maassen, H., Zyczkowski, K.: Protected subspaces in quantum information. Quant. Inf. Proc. **9**(3), 343–367 (2010)