A Postprint of an NFC Mobile Payment Scheme Based on Certificateless Signcryption Technology

Authors: Liu Yi, Yu Hao

Date: 2018-09-12T00:00:00+00:00

Abstract

To address the issues of complex certificate management, insufficient consumer privacy protection, and low operational efficiency prevalent in most existing NFC mobile payment schemes, this paper proposes an efficient and secure NFC mobile payment scheme that integrates certificateless signcryption technology without bilinear pairings with anonymity techniques. The scheme utilizes dynamically updated anonymous transaction accounts to enable consumer anonymous transactions while simultaneously achieving transaction unlinkability. By serving as a communication bridge between consumers and the mobile payment service provider, merchants facilitate consumer offline payments. Analysis results indicate that the scheme delivers highly secure transactions and high-quality personal privacy protection while concurrently achieving efficient mobile payment.

Full Text

An NFC Mobile Payment Scheme Based on Certificateless Signcryption Technology

Liu Yi, Yu Hao
School of Computer Science, Guangdong University of Technology, Guangzhou 510006, China

Abstract: Most existing NFC mobile payment schemes suffer from complex certificate management, inadequate consumer privacy protection, and low operational efficiency. To address these issues, this paper proposes an efficient and secure NFC mobile payment scheme that combines certificateless signcryption technology (without bilinear pairing operations) with anonymous techniques. The scheme employs dynamically updated anonymous transaction accounts to achieve consumer anonymity and transaction unlinkability. Merchants serve as communication bridges between consumers and mobile payment service

providers, enabling offline payments for consumers. Analysis results demonstrate that the scheme provides high-security transactions, high-quality personal privacy protection, and high-efficiency mobile payments.

Key words: certificateless signcryption technology; anonymous technology; near field communication; consumer offline payment; secure payment; privacy protection

0 Introduction

With the proliferation of smart mobile terminals and rapid development of mobile payment technologies, mobile-based payment methods are gradually replacing traditional payment methods (such as card swiping or cash payments) to dominate the payment market. According to Analysys' "China Third-Party Mobile Payment Market Quarterly Monitoring Report Q2 2017," the transaction volume of China' s third-party mobile payment market reached 23.04 trillion RMB in Q2 2017, representing a 22.50% quarter-over-quarter growth. Alipay leads with 53.70% market share, followed by Tencent Finance with 39.12%. Both Alipay and WeChat Pay primarily use QR code payment technology, which is easy to implement and convenient but vulnerable to fake or malicious QR code attacks, resulting in poor security. In contrast, NFC mobile payment technology offers excellent confidentiality and security, enabling payments even when mobile phones are powered off, making it one of the most promising payment technologies for the future.

During mobile payment processes, users prioritize both convenience and security. Current NFC mobile payments primarily rely on traditional cryptographic techniques to ensure transaction data security and user identity authentication. These techniques involve substantial computational overhead and generally suffer from complex certificate management and key escrow problems.

Reference [1] utilizes certificateless signature technology and pseudo-identity techniques to achieve identity authentication and user privacy protection in mobile payments. However, this scheme involves numerous bilinear pairing operations, incurring significant time overhead. Reference [2] proposes a key authentication scheme for NFC mobile payment based on bilinear pairing operations, which also uses extensive bilinear pairing during authentication, increasing time costs. Additionally, since users employ real identity IDs during transactions, anonymous payment functionality is not provided, leaving user privacy inadequately protected. Reference [5] employs randomly changing anonymous IDs as user transaction identities, enhancing privacy protection during transactions. However, these anonymous IDs consist of public keys, private keys, and certificates, creating complex certificate management issues. Reference [6] assigns expiration dates and credit values to anonymous transaction account IDs, enabling anonymous payments while achieving transaction unlinkability, significantly improving user privacy. The drawback is that once the expiration date passes, users must manually reapply for new anonymous transaction account

IDs and virtual bank account IDs, compromising convenience. Reference [7] uses certificateless signcryption technology without bilinear pairing to achieve user identity authentication in mobile payments, substantially improving authentication efficiency. However, transaction records remain transparent to the card issuer, and offline payment is not supported—transactions cannot be completed without network support, severely limiting applicable transaction venues. Reference [8] proposes an NFC-based user anonymous mobile payment protocol where users transact with virtual accounts and virtual transaction accounts generated by themselves, with only the bank knowing the user' s real identity. However, users must update their virtual accounts after each transaction to achieve unlinkability.

Building upon NFC communication technology, this paper combines certificateless signcryption technology without bilinear pairing operations and anonymous techniques to propose an NFC mobile payment scheme featuring high authentication efficiency, strong privacy protection, and wide applicability.

1.1 NFC Communication Technology

NFC (Near Field Communication) evolved from contactless RFID and represents an extension of RFID technology. Operating at 13.56 MHz with a transmission distance of 10 cm [9], NFC supports transmission speeds of 106 kbps, 212 kbps, and 424 kbps, connecting to only one device at a time. Using hardware security modules for encryption, NFC offers excellent confidentiality and security [10]. NFC has three operating modes: reader/writer mode, card emulation mode, and peer-to-peer mode [11]. Due to its convenience and security, NFC technology is widely applied in mobile payments, electronic ticketing, service discovery, data exchange, access control systems, and public transportation systems.

1.2 Certificateless Public Key Cryptography

The concept of certificateless public key cryptography (CL-PKC) was proposed by Al-Riyami and Paterson at Asiacrypt 2003 [12]. Compared with traditional PKI-based public key cryptography, CL-PKC—like identity-based cryptography—eliminates the need for public key certificates, removing complex certificate management issues. Simultaneously, in CL-PKC, the Key Generation Center (KGC) only generates partial private keys; the complete private key is formed by combining this with a secret value randomly selected by the user. Since the private key is secretly stored by the user, the KGC cannot learn the user' s complete private key, thereby overcoming the key escrow problem inherent in identity-based cryptography. CL-PKC can be considered an efficient and high-performance public key cryptography technology [13].

Public key cryptography encompasses encryption, signature, key agreement, and signcryption technologies. Zheng [14] proposed signcryption technology, which simultaneously achieves encryption and signature more efficiently than perform-

ing them separately, reducing computational and communication overhead. Certificateless signcryption technology generally consists of seven algorithms [15]:

a) **Setup**: Input security parameter k, output system private key msk, system public key mpk, and system public parameters $params$.

b) **Partial-Private-Key-Extract**: KGC inputs system public key mpk, system private key msk, user identity ID_A, and outputs user's partial private key D_A, sending D_A to user A through a secure channel.

c) **Set-Secret-Value**: User A selects a random number y_A as their secret value.

d) **Set-Private-Key**: User A inputs system public key mpk, user identity ID_A, partial private key D_A, and secret value y_A, outputting the complete private key sk_A.

e) **Set-Public-Key**: User A inputs system public key mpk, user identity ID_A, partial private key D_A, and secret value y_A, outputting public key PK_A.

f) **Signcrypt**: Input system parameters $params$, sender identity ID_A, receiver identity ID_B, receiver public key PK_B, sender public key PK_A, sender complete private key sk_A, and message m to be signcrypted, outputting ciphertext c.

g) **Unsigncrypt-Verify**: Input system parameters $params$, sender identity ID_A, receiver identity ID_B, receiver public key PK_B, receiver complete private key sk_B, and ciphertext c. If verification passes, output plaintext message m; otherwise output $\perp$.

3 Scheme Description

3.1 System Parameter Initialization

The mobile payment service provider inputs security parameter k into their cloud server to generate two large primes p and q, where $p-1$ is divisible by q. Let G be a cyclic group on elliptic curve E, and P be any generator of order q on G. Select three hash functions: $H_1 : \{0,1\}^* \times G \to Z_q^*$, $H_2 : \{0,1\}^* \to Z_q^*$, $H_3 : \{0,1\}^* \to G$. Choose a random number $s \in Z_q^*$ as the system private key and secretly store it in the cloud server, compute $P_{pub} = sP$ as the system public key. Publish system parameters $params = \{q, P, P_{pub}, H_1, H_2, H_3\}$.

3.2 Registration Phase

This payment scheme consists of a registration phase and a payment phase. The registration phase includes consumer registration and merchant registration. Consumer registration involves the consumer, mobile payment service provider, and trusted third-party anonymous generation center, where the anonymous account's legitimacy used by the consumer for registration with the service provider

is verified by the anonymous generation center. Merchant registration involves the merchant, mobile payment service provider, and real-name authentication center, where the merchant' s identity legitimacy is verified by the real-name authentication center. The payment phase involves consumers, merchants, and mobile payment service provider—consumers and merchants provide relevant information to the service provider (with consumer information forwarded by merchants), and the service provider performs identity authentication and transfer functions. For large-amount payments, consumers must also input payment passwords to complete transactions. [Figure 1: see original paper] illustrates the payment framework model.

3.2.1 Consumer Registration Consumer C registers through the mobile payment service provider S' s APP on their mobile terminal:

a) Open the APP and input registration information including username, login password lpw, payment password ppw, anonymous account $CAID$, and mobile number PN. The $CAID$ is generated by the trusted third-party anonymous generation center and serves as the consumer' s unique identity marker when registering with S. Compute $D = H(username||lpw)$ and store it locally in the secure element (SE), then send $\{CAID, PN, H(ppw), D\}$ to S through a secure channel.

b) Upon receiving the registration information, S sends an SMS verification code SMS to C' s mobile number to verify its validity and confirm the registration request is initiated by C.

c) C inputs the SMS verification code in the APP and sends it to S. S compares the received code with the previously sent SMS. If they match, S sends $CAID$ through a secure channel to the anonymous generation center for identity legitimacy authentication; otherwise, S sends a registration failure message to C.

d) The anonymous generation center searches its database upon receiving $CAID$ from S. If the anonymous account exists, it sends an identity confirmation receipt $Confirm$ to S; otherwise, it sends an authentication failure message to S, which then forwards a registration failure message to C.

e) S verifies the receipt from the anonymous generation center. If it' s an identity confirmation, S stores $\{CAID, PN, H(ppw), D\}$ locally in SE and opens a digital wallet for C, who can then recharge or withdraw funds. Simultaneously, S generates an anonymous transaction account $CTAID$ and selects a random number $r_C \in Z_q^*$ as C's partial public key and partial private key. Finally, S sends the generated partial keys and $CTAID$ to C through a secure channel.

f) Upon receiving the partial keys, C verifies the correctness of the partial private key and stores the partial keys locally in SE, then deletes r_C.

The registration symbols used in this scheme are parsed in .

3.2.2 Merchant Registration Merchant M registers on S' s official website:

a) M inputs real identity MID, phone number TN, email address $email$, and other registration information, sending them through a secure channel to S.

b) Upon receiving the registration information, S sends a verification code $Token$ to M.

c) M inputs the verification code and sends it to S.

d) S verifies the code' s correctness. If valid, S sends MID to the real-name authentication center AU for identity legitimacy verification. Upon successful authentication, AU sends an identity confirmation receipt $Confirm$ to S; otherwise, it sends an authentication failure message to S, which then forwards a registration failure message to M.

e) After receiving $Confirm$, S computes $H(MID||TN||IMSI)$, selects a random number $r_M \in Z_q^*$, then randomly selects $s_M \in Z_q^*$ to generate M' s partial public key and partial private key. S then generates a session key KEY and sends the partial keys and KEY to M through a secure channel.

f) M receives the partial keys, verifies the partial private key' s correctness, and stores the partial keys in the SIM card.

The registration flow is shown in [Figure 3: see original paper].

3.3 Identity Authentication

a) C inputs username and login password lpw on the APP login interface to enable payment functionality and inputs payment password ppw to extract the partial private key: $D = H(username||lpw)$, while extracting $CTAID$. The APP then randomly selects $r'_C \in Z_q^*$, computes $Q_C = r'_C P$, and generates C' s complete private key $sk_C = (D + r'_C)$. The APP randomly selects $r''_C \in Z_q^*$, computes $T_C = r''_C P$. Meanwhile, M extracts partial public key R_M, partial private key D_M, and $Token$ from the SIM card, selects a random number $r'_M \in Z_q^*$, and generates M' s complete private key $sk_M = (D_M + r'_M)$. M then selects another random number $r''_M \in Z_q^*$.

b) C brings the mobile terminal close to M' s POS terminal to receive M' s transmitted information $\{R_M, T_M, h_M, S_M, C_M\}$. C uses the extracted KEY to decrypt the ciphertext and obtain payment information m, computing $h_M = H_2(T_M||R_M||m)$.

c) C sends $\{R_C, T_C, h_C, S_C, C_C\}$ to M, where $h_C = H_2(T_C||R_C||m)$, $S_C = sk_C \cdot R_C + r''_C \cdot P_{pub} + h_C \cdot PK_C$, and $C_C = m \oplus H_3(sk_C \cdot Q_M)$. M forwards

$\{R_C, T_C, h_C, S_C, C_C, R_M, T_M, h_M, S_M, C_M, m\}$ to S.

d) Upon receiving the signcryption information from M, S searches its database for C and M. If they exist, S retrieves C' s partial public key R_C and M' s partial public key R_M from local SE, combines them with the transmitted public keys to obtain C' s complete public key $PK_C = R_C + Q_C$ and M' s complete public key $PK_M = R_M + Q_M$. S then computes $V_C = S_C - (h_C \cdot PK_C + T_C)$ and decrypts to obtain $m = C_C \oplus H_3(V_C)$. The decryption process is as follows:

From the above results, we can see that $m = m'$, indicating successful plaintext recovery. Similarly, the merchant' s plaintext can be obtained. After plaintext recovery, S compares m from the consumer with m from the merchant. If they match, identity authentication proceeds; otherwise, S returns authentication failure messages to both parties and aborts the transaction. C' s identity authentication process is as follows:

If the equation holds, identity authentication passes. Merchant M's identity can be authenticated similarly. After both identities are authenticated, the payment information m is accepted.

3.4 Payment Transaction

Payment transactions are divided into two types: small-amount and large-amount transactions.

1) **Small-Amount Transaction**: After completing identity authentication for both consumer and merchant, S processes the transfer based on payment information m in C' s electronic wallet. If C' s wallet balance is insufficient but bank quick payment is enabled, the consumer can choose to complete the transaction via bank quick payment. If both electronic wallet and bank account balances are insufficient, or if the consumer doesn' t select bank quick payment, the transaction fails and S sends a failure message to C and M.

2) **Large-Amount Transaction**: After completing identity authentication, S sends $\{S, h_S, C_S\}$ to C, where C_S is the ciphertext of the payment password request message. C confirms the payment amount on the POS terminal and, if correct, inputs the payment password ppw, sending $\{ppw, C_S\}$ to M, where C_S is the ciphertext of ppw. M forwards $\{ppw, C_S, m\}$ to S. S compares the received ppw with the value stored in local SE. If they match, the same payment process as small-amount transactions executes; otherwise, the transaction terminates and S sends a failure message.

The payment flow is shown in [Figure 4: see original paper] (dashed lines indicate steps only required for large-amount transactions; solid lines indicate steps required for both transaction types).

3.5 Transaction Completion

After successful transaction, S sends $\{C_S, C'_S\}$ to M, where C_S is the ciphertext of the payment success receipt encrypted with M' s public key, and C'_S is the ciphertext containing the payment success receipt and new anonymous transaction account encrypted with C' s public key. M decrypts C_S to obtain the receipt and stores it secretly, then forwards C'_S to C, who decrypts it to obtain the receipt and new $CTAID'$, stores them secretly in local SE, and deletes the old $CTAID$. The entire transaction concludes.

4 Security Analysis

4.1 Confidentiality

Payment information m transmitted between M and C is encrypted with session key KEY. Malicious users not registered with S cannot decrypt to obtain correct payment information without KEY. If C is malicious and attempts unauthorized transactions by modifying m to m', since S first compares m from C with m from M during authentication, any $m' \neq m$ proves malicious tampering and S terminates the transaction. If M is malicious, C can verify the payment amount on the POS terminal before inputting ppw and abort if unreasonable. If an attacker impersonates S to receive signcryption information and attempts to modify m, they cannot decrypt m without S' s private key, preventing successful modification.

4.2 Resistance to Impersonation Attacks

Assume an attacker attempts illegal transactions using C' s account. Since the attacker cannot obtain C' s mobile phone and C' s partial private key D is only stored in C' s phone, the attacker cannot acquire the correct D. Even if the attacker obtains C' s phone, D is stored encrypted with $H(ppw)$, so without C' s payment password, the correct D remains inaccessible. The attacker might forge C' s signature $\{R'_C, T'_C, h'_C, S'_C, C'_C\}$ and send it through M to S. S substitutes these into the authentication equation:

Since the equation fails, authentication fails and the transaction terminates.

4.3 Resistance to Replay Attacks

Assume malicious merchant M attempts illegal transactions by repeatedly sending previously completed transaction signcryption information to S. Since each transaction uses different public/private key pairs, the generated signcryption information differs. Moreover, completed transaction signcryption information remains stored on S' s server. If S detects duplicate signcryption information, it discards the request, effectively preventing replay attacks from malicious merchants.

4.4 Identity Anonymity

During transactions between C and M, C uses the anonymous transaction account $CTAID$ distributed by S, so neither M nor attackers can obtain C' s real identity. Additionally, since C registers with S using the anonymous account $CAID$ distributed by the anonymous generation center, S also doesn' t know C' s real identity. Therefore, the scheme fully achieves consumer anonymous transactions and effectively protects consumer personal privacy.

4.5 Non-repudiation

When disputes arise, C provides the payment success receipt and anonymous account $CAID$ to S, while M provides the receipt and real identity MID. S searches historical transaction records using the order number and transaction time from the receipt, then verifies whether the transaction amount and both parties' account names match those in the receipt. If all match, the transaction is normal; any discrepancy indicates anomalies. If either party attempts to deny the anomalous transaction, the signatures stored in the historical transaction records prevent repudiation.

4.6 Unlinkability

During transactions, C uses the anonymous transaction account $CTAID$ distributed by S, which updates after each transaction (one account per transaction). Even if C purchases the same product at the same store, the different $CTAID$ makes it difficult for M to obtain C' s real identity. Moreover, since each transaction uses a different $CTAID$, M cannot correlate purchased product information with the real C, making it difficult to infer C' s personal privacy information (such as occupation, interests, or health status) from product attributes. Similarly, even if encrypted information between M and S is compromised, attackers cannot infer C' s personal privacy information, achieving transaction unlinkability and effectively protecting consumer privacy.

4.7 Consumer Offline Payment

Data exchange between C and M occurs via NFC technology, with M serving as the communication bridge between C and S. Therefore, C can successfully complete transactions even without network connectivity, achieving consumer offline payment.

compares the security of our scheme with references [1] and [2], where Y indicates resistance and N indicates vulnerability.

5 Efficiency Analysis

This paper employs the methodology from reference [4] for efficiency analysis. Based on experimental data from references [1,3,4], presents time overhead for

different cryptographic operations. Server-side overhead is based on the MIRACL [16] cryptographic library running on a PIV 3 GHz processor with 512 MB memory and Windows XP. Client-side overhead is estimated on a 206 MHz ARM processor with Linux using:

$t_{client} = \frac{3000}{206} \times C_t$, where C_t represents client-side cryptographic operation time and S_t represents server-side time.

According to , in reference [1], the entire process from signature generation to identity authentication completion requires 1 bilinear pairing, 2 scalar multiplications in bilinear pairing groups, and 2 exponentiations in bilinear pairing groups on the client side, plus 2 bilinear pairings and 1 exponentiation on the server side, totaling 838.28 ms. In reference [2], the client performs 5 elliptic curve scalar multiplications and 1 bilinear pairing, while the server performs 2 elliptic curve scalar multiplications and 1 bilinear pairing, totaling 477.2 ms. In our scheme, since consumers and merchants can generate signatures simultaneously, client-side time is 3 elliptic curve scalar multiplications, and the server can authenticate both signatures concurrently, resulting in 3 elliptic curve scalar multiplications on the server side, for a total of 103.17 ms. [Figure 5: see original paper] illustrates the time overhead for each cryptographic operation.

shows the total time overhead for the entire authentication process. Our scheme is approximately 87.69% faster than reference [1] and 78.38% faster than reference [2], demonstrating superior efficiency and practicality.

6 Conclusion

This paper proposes a secure and efficient NFC mobile payment scheme combining certificateless signcryption and anonymous techniques. The consumer' s partial private key is encrypted and stored in the mobile terminal combined with their payment password, enhancing protection against key leakage. Consumers communicate with the mobile payment service provider using anonymous accounts distributed by a trusted third-party anonymous generation center, achieving communication anonymity. Consumers transact with merchants using anonymous transaction accounts distributed by the service provider that update after each transaction, achieving both anonymous communication and transaction unlinkability while improving privacy security. Each transaction uses newly generated private keys for signing (one-time-per-transaction), enhancing authentication security and providing anti-replay attack properties. Information exchange between consumers and the service provider is forwarded by merchants, enabling consumer offline payment and expanding transaction venue possibilities. Analysis demonstrates that the scheme improves NFC mobile payment security, effectively protects consumer privacy, and enhances payment efficiency, representing a secure and efficient mobile payment solution.

References

[1] Qin Zhen, Sun Jianfei, Wahaballa A, et al. A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing [J]. Computer Standards & Interfaces, 2017, 54: 55-60.

[2] Chen Xinyi, Choi K, Chae K. A secure and efficient key authentication using bilinear pairing for NFC mobile payment service [J]. Wireless Personal Communications, 2017, 97 (1): 1-17.

[3] He Debiao, Chen Jianhua, Zhang Rui. Efficient and provably-secure certificateless signature scheme without bilinear pairings. [J]. International Journal of Communication Systems, 2014, 25 (11): 1432–1442.

[4] Cao Xuefei, Zeng Xingwen, Kou Weidong, et al. Identity-based anonymous remote authentication for value-added services in mobile networks [J]. IEEE Trans on Vehicular Technology, 2009, 58 (7): 3508-3517.

[5] Eun H, Lee H, Oh H. Conditional privacy preserving security protocol for NFC applications [J]. IEEE Trans on Consumer Electronics, 2013, 59 (1): 153-159.

[6] Luo Jianing, Yang M H, Huang S Y. An unlinkable anonymous payment scheme based on near field communication [J]. Computers & Electrical Engineering, 2016, 49: 198-206.

[7] 王亚涛, 赵波, 陶威. 基于无证书公钥密码的 HCE 移动支付方案 [J]. 计算机工程与设计, 2017, 38 (1): 32-36. (Wang Yatao, Zhao Bo, Tao Wei. HCE mobile payment scheme on CL-PKC [J]. Computer Engineering and Design, 2017, 38 (1): 32-36.)

[8] Chen Shangwen, Tso R. NFC-based Mobile Payment Protocol with User Anonymity [C]// Proc of the 11th Asia Joint Conference on Information Security. 2016: 24-30.

[9] 贾凡, 佟鑫. NFC 手机支付系统的安全威胁建模 [J]. 清华大学学报: 自然科学版, 2012, 52 (10): 1460-1464. (Jia Fan, Tong Xin. Threat modeling for mobile payments using NFC phones [J]. Journal of Tsinghua University (Science and Technology), 2012, 52 (10): 1460-1464.)

[10] 张玉清, 王志强, 刘奇旭, 等. 近场通信技术的安全研究进展与发展趋势 [J]. 计算机学报, 2016, 39 (6): 1190-1207. (Zhang Yuqing, Wang Zhiqiang, Liu Qixu, et al. Research progress and trends on the security of near field communication [J]. Chinese Journal of Computers, 2016, 39 (6): 1190-1207.)

[11] Rajesh G P, Pattar P, Divya M N, et al. Near field application: NFC smart notice board [C]// Proc of the 13th International Conference on Wireless and Optical Communications Networks. 2016: 1-5.

[12] 刘文浩, 许春香. 无双线性配对的无证书签密方案 [J]. 软件学报, 2011, 22 (8): 1918-1926. (Liu Wenhao, Xu Chunxiang. Certificateless signcryption scheme without bilinear pairing [J]. Journal of Software, 2011, 22 (8): 1918-1926.)

[13] 张福泰, 孙银霞, 张磊, 等. 无证书公钥密码体制研究 [J]. 软件学报, 2011, 22 (6): 1316-1332. (Zhang Futai, Sun Yinxia, Zhang Lei, et al. Research on Certificateless Public Key Cryptography [J]. Journal of Software, 2011, 22 (6): 1316-1332.)

[14] Zheng Yuliang. Digital signcryption or how to achieve cost(signature & encryption) cost(signature) + cost(encryption) [C]// Advances in Cryptology. Berlin: Springer, 1997, 1294: 165-179.

[15] Selvi S S D, Vivek S S, Rangan C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing [C]// Proc of International Conference on Information Security and Cryptology. Berlin: Springer-Verlag, 2009: 75-92.

[16] Shamus Software Ltd. Miracl library [EB/OL]. [2018-05-10]. http://www.shamus.ie/index.php?page=home

Note: Figure translations are in progress. See original paper for figures.