A secure quantum group signature scheme based on Bell states

Article *in* Physica Scripta · March 2013

DOI: 10.1088/0031-8949/87/04/045012

4 authors, including:

Ke-Jia Zhang
Heilongjiang University
26 PUBLICATIONS **224** CITATIONS
SEE PROFILE

Ting-Ting Song
Jinan University (Guangzhou, China)
19 PUBLICATIONS **220** CITATIONS
SEE PROFILE

Huijuan Zuo
Hebei Normal University
35 PUBLICATIONS **161** CITATIONS
SEE PROFILE

A secure quantum group signature scheme based on Bell states

2013 Phys. Scr. 87 045012

(http://iopscience.iop.org/1402-4896/87/4/045012)

IOP Publishing Physica Scripta
Phys. Scr. **87** (2013) 045012 (5pp) doi:10.1088/0031-8949/87/04/045012

A secure quantum group signature scheme based on Bell states

Kejia Zhang[1,2], Tingting Song[1], Huijuan Zuo[1] and Weiwei Zhang[1]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, People's Republic of China
[2] State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, People's Republic of China

E-mail: zhangkejia.bupt@gmail.com

Received 22 October 2012
Accepted for publication 26 February 2013
Published 18 March 2013
Online at stacks.iop.org/PhysScr/87/045012

Abstract
In this paper, we propose a new secure quantum group signature with Bell states, which may have applications in e-payment system, e-government, e-business, etc. Compared with the recent quantum group signature protocols, our scheme is focused on the most general situation in practice, i.e. only the arbitrator is trusted and no intermediate information needs to be stored in the signing phase to ensure the security. Furthermore, our scheme has achieved all the characteristics of group signature—anonymity, verifiability, traceability, unforgetability and undeniability, by using some current developed quantum and classical technologies. Finally, a feasible security analysis model for quantum group signature is presented.

PACS numbers: 03.67.Dd, 03.67.Ac

1. Introduction

Digital signature, which is an important branch of cryptography, has been widely used in practical applications. In real life, some specific requirements may be needed and group signature is an important model which is used in e-payment system, e-government, e-business, etc [1–3]. In group signature schemes, a cluster of entities forms a group and any group member can sign messages on behalf of his group in anonymity. The verifier cannot know the specific signer but can only check the validity of the signature. Furthermore, the group manager, who is considered as the arbitrator, can open the signature to reveal the identity of the signer when dispute happens.

To the best of our knowledge, the security of most classical digital signature protocols is based on the assumption of computational complexity (e.g. the factoring problem and discrete logarithm problem) and might be susceptible to the strong ability of quantum computation [4, 5]. In order to improve the security, many quantum signature schemes have been proposed in recent years. Quantum signature was first investigated by Gottesman and Chuang in 2001 [6]. Then, Barnum *et al* [7] pointed out a no-go theorem for the application of the quantum signature in 2002. Although Barnum *et al*'s conclusion created a serious obstacle for quantum signature, the study of the quantum signature scheme has not stopped. In 2002, Zeng and Keitel [8] first proposed an arbitrated quantum signature (AQS) protocol, which is called the ZK protocol, to sign a quantum message. This work gave an elementary model to overcome Barnum *et al*'s no-go theorem for quantum signature [7]. In 2009, Li *et al* [9] presented a Bell-states-based AQS protocol, which simplified the ZK protocol by replacing the Greenberger–Horne–Zeilinger states with Bell ones as the carrier. Then, Zou and Qiu [10] provided an AQS protocol without entangled states. Meanwhile, some quantum signature protocols to solve the specific requirements in practice have been presented. From 2008, Yang *et al* [11–13] successively proposed some multiparty quantum signature schemes. In 2011, they also gave an AQS scheme against collective amplitude damping noise [14]. At the same time, Wang *et al* also presented some contributions to the practical quantum signature schemes. In 2010, Wang and Wen [15] proposed a fair quantum blind signature scheme based on the fundamental properties of quantum mechanics. A one-time proxy signature with decoherence-free states was also presented to prevent the collective noise in 2012 [16].

During the development, the research on quantum group signature has drawn more and more attention. In 2011, Wen *et al* [17] proposed the first quantum group signature scheme, whose implementation depends on the participation of a trusted third arbitrator. This work made a breakthrough on quantum group signature and their model is still feasible now. Later, Wen *et al* designed an e-cash system with the Greenberger–Horne–Zeilinger states based on group signature [18]. In 2011, Xu *et al* [19] proposed a new quantum

group signature scheme without entanglement. In Xu *et al*'s group signature scheme, the receiver of the signature uses the session keys based on symmetric cryptography to achieve the verifiability.

In this paper, we propose a new secure quantum group signature scheme, which is based on the most general situation in practice. In our scheme, only the arbitrator is trusted and no intermediate information needs to be stored in the signing phase to ensure its security. Furthermore, our scheme is able to make up some secure loopholes in previous quantum group signature ones and achieves all the characteristics of group signature, i.e. anonymity, verifiability, traceability, unforgetability and undeniability. Our scheme can be realized in practice because it uses some current developed quantum and classic technologies. The rest of this paper is organized as follows. In section 2, we describe our quantum group signature scheme in detail. Then the security analysis is proposed in section 3. A further discussion and the conclusion are provided in section 4.

2. Our quantum group signature scheme

2.1. Characteristics of quantum group signature

Before describing our quantum group signature scheme, let us point out the characteristics of quantum group signature in general:

1. *Anonymity*: the receiver of the signature can decide whether the signature was signed by a group member, but he cannot know which member signed it. That is to say, the signer's identity is anonymous to the receiver.
2. *Verifiability*: a designated verifier is able to verify the validity of a signature without knowledge of the identity of the signer.
3. *Unforgetability*: nobody can generate a valid signature except for the legal signer.
4. *Undeniability*: any member of a group can get the signature of his message with the help of the group manager. After signing that, the signer cannot deny it.
5. *Traceability*: if there exists a dispute between the signer and the receiver, the arbitrator could open the signature to check the identity of the signer.

2.2. Our quantum group signature scheme

In order to clarify our quantum group signature scheme, three characters are defined:

1. *Alice-i*: a member of the group who wants to sign the message M.
2. *Bob*: the receiver of the signature who can verify the validity of a signature.
3. *Trent*: the group manager who is considered as a trusted arbitrator. When a dispute happens, Trent can open the signature to identify the signer.

We are now ready to introduce our quantum group signature scheme which consists of the following three phases:

Initializing phase.

(I1) The signer Alice-i ($i = 1, 2, \ldots, n$) and the receiver Bob each shares a secret key string with the arbitrator Trent, which is denoted as K_{AT} and K_{BT}, respectively. This can be achieved by using some practical quantum key distribution (QKD) techniques [20–24].

(I2) The signed information $M = (m(1), m(2), \ldots, m(i), \ldots, m(n))$ is encoded into two selected states $\{|L\rangle = a|0\rangle + b|1\rangle, |R\rangle = b|0\rangle - a|1\rangle\}$ by the signer Alice-i, i.e.

$$\begin{aligned} m(i) = 0 &\rightarrow |L\rangle, \\ m(i) = 1 &\rightarrow |R\rangle, \end{aligned} \tag{1}$$

where $|a|^2 + |b|^2 = 1$.

(I3) Bob and Trent prepare n pairs of $|\Psi^+\rangle_{B_1B_2} = |\Psi^+\rangle_{T_1T_2} = (|01\rangle + |10\rangle)/\sqrt{2}$, respectively. Here the subscripts denote the states which belong to Bob or Trent. In addition, B_1, T_1 represent the first qubit sequence and B_2, T_2 represent the second qubit sequence.

Signing phase.

(S1) Alice-i wants to generate a signature for Bob and sends a request to Trent. Trent then informs Bob.

(S2) After receiving Trent's notification, Bob first creates a unique serial number SN_B to distinguish each signature task. Then he keeps B_2 and sends $|S_{BT}\rangle$ to Trent, where

$$|S_{BT}\rangle = E_{K_{BT}}(B_1 \otimes |SN_B\rangle). \tag{2}$$

Here E_k represents the quantum encryption algorithm with classical bits [25–27] and the classical information is encoded into quantum states to be encrypted and transferred. It should be pointed that the encryption algorithms can be applied with unconditional security.

(S3) Trent decrypts $|S_{BT}\rangle$ with K_{BT} and gets B_1 and SN_B. Then he chooses a random number r and obtains $R = r \parallel H(r \parallel \mathrm{ID}_{A_i} \parallel SN_B)$, $l = H(K_{BT} \parallel R)$. Trent's goal is to hide the signer's identity in R and ensure its integrity by the use of l. Here ID_{A_i} represents the identity of the signer and it is only known to Trent and Alice-i, '$\parallel$' denotes 'concatenate', and $H(\cdot)$ is a hash function. Afterwards, Trent makes the measurement of $B_1 \otimes T_1$ with Bell states and obtains the result $|S'_T\rangle$. After that, Trent transmits $|S_{TA}\rangle$ to Alice-i, where

$$\begin{aligned} |S_{TA}\rangle &= E_{K_{AT}}(|S_T\rangle \otimes T_2 \otimes |R\rangle \otimes |SN_B\rangle), \\ |S_T\rangle &= E_l(|S'_T\rangle). \end{aligned} \tag{3}$$

It can be seen that Trent uses this method to provide the necessary information to sign the message and verify the signature.

(S4) Alice-i prepares three copies of the message M, and encodes one of them into the quantum state $|M\rangle$. After Alice-i decrypts $|S_{TA}\rangle$ with K_{TA}, she firstly makes the measurement of $|M\rangle \otimes T_2$ with Bell states, and obtains the result $|S_A\rangle$. Then Alice-i hides the second copy of M into M_0,

$$M_0 = H(M \| \mathrm{ID}_{A_i} \| K_{AT}). \tag{4}$$

Finally, Alice-i makes the resulting records into classical bits, and sends the message pair (SN_B, M, M_0), the signature pair (S_A, S_T, R) on a public board. Here the public board cannot be controlled by anyone, therefore none can recognize the identity of the Alice-i.

Verifying phase.

(V1) Bob gets the pair of information $(SN_B, M, M_0, S_A, S_T, R)$ from the public board and recovers the

quantum states $|S_A\rangle$, $|S_T\rangle$. Besides, he informs Trent to verify the signature together.

(V2) According to $|S_T\rangle$ and R, Bob gets $|S'_T\rangle$ with the key K_{BT}. With the help of SN_B, $|S'_T\rangle$ and $|S_A\rangle$, he performs one of the corresponding reverse Pauli transformations on each photon of B_2 in his hand and extracts M' from the message states. If $M' = M$, Bob announces $r_B = 0$.

(V3) At the same time, Trent can also obtain the signer's identity ID'_{A_i} from R and verifies whether $M_0 = H(M \| ID'_{A_i} \| K_{AT})$ or not. If the result is positive, Trent announces $r_T = 0$.

(V4) Bob accepts the signature pair $(SN_B, M, M_0, S_A, S_T, R)$ in the case of $r_B = r_T = 0$; otherwise, the signature is rejected.

3. The security analysis of our scheme

With the development of quantum cryptography, some feasible attack strategies have been proposed such as intercept-resend attacks [28], entanglement-swapping attacks [29, 30], teleportation attacks [31], dense-coding attacks [32, 33], channel-loss attacks [34, 35], denial-of-service attacks [36, 37], correlation-extractability attacks [38–40], Trojan horse attacks [41, 42], participant attacks [30, 33] and so on. Furthermore, some cryptanalysis of quantum signature has been presented [43, 44]. Here we analyze the security of our quantum group signature scheme according to Gao *et al*'s idea in [43]. In fact, the security analysis model may have applications in future.

3.1. Traceability

Obviously, the traceability will be seen in step V3. With the assumption of Trent, the identity number ID_{A_i} is only known to Trent and Alice-i. In order to check the identity of the signer, Trent computes $R' = H(r \| ID_{A_i} \| SN_B)$ with ID_{A_i} $i = 1, 2, \ldots, n$ of his group. The identity of the signer will be obtained in the case of $R = R'$.

3.2. Verifiability

Here we know the message M has been sent to Bob in three forms. Firstly, Bob will verify the equivalence of the message M and the message transferred by the teleportation. Given a six-tuple $(SN_B, M, M_0, S_A, S_T, R)$, Bob will get $|S'_T\rangle$ with the key K_{BT} and R. With the technique of teleportation based on entanglement swapping, it can be seen that

$$
\begin{aligned}
|\Psi^\dagger\rangle_{T_1T_2}|\Psi^\dagger\rangle_{B_1B_2} &= \frac{1}{2}(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle)_{T_1T_2B_1B_2} \\
&= \frac{1}{2}(|0011\rangle + |0110\rangle + |1001\rangle + |1100\rangle)_{T_1B_1T_2B_2} \\
&= \frac{1}{2}(|\Psi^\dagger\rangle|\Psi^\dagger\rangle - |\Psi^-\rangle|\Psi^-\rangle + |\Phi^\dagger\rangle|\Phi^\dagger\rangle \\
&\quad - |\Phi^-\rangle|\Phi^-\rangle)_{T_1B_1T_2B_2}. \qquad (5)
\end{aligned}
$$

In the view of this, if $|S'_T\rangle$ is determined, each qubit in T_2 and the corresponding qubit in B_2 will be entangled in one Bell state. Based on the values of SN_B and $|S_A\rangle$, Bob will perform one of the following corresponding Pauli transformations on each photon of B_2 in his hand to extract the message M'. Here the corresponding reverse Pauli transformation can be seen in table 1.

Table 1. Bob's corresponding reverse Pauli transformation to B_2.

	$\|S'_T\rangle$			
$\|S_A\rangle$	$\|\Phi^\dagger\rangle$	$\|\Phi^-\rangle$	$\|\Psi^\dagger\rangle$	$\|\Psi^-\rangle$
$\|\Phi^\dagger\rangle$	I	σ_z	σ_x	$i\sigma_y$
$\|\Psi^\dagger\rangle$	σ_x	$i\sigma_y$	I	σ_z
$\|\Phi^-\rangle$	σ_z	I	$i\sigma_y$	σ_x
$\|\Psi^-\rangle$	$i\sigma_y$	σ_x	σ_z	I

Secondly, Trent is informed to verify the integrity of the message hidden in M_0. With the traceability of Trent, he can get the identity number ID'_{A_i}. Here he computes $M'_0 = H(M \| ID'_{A_i} \| K_{AT})$ to check whether $M'_0 = M_0$. If the result is positive, it means the message, which is signed by Alice-i, is not changed by anyone else. Until now, the validity of the signature pair has been verified by Bob and Trent together.

3.3. Unforgetability

Here we analyze the unforgetability from two aspects as follows:

1. Assume that the attacker Eve is an external attacker who wants to imitate Alice-i to sign a message M_E. With the excellent ability assumptions of the attacker, she can capture the photons transmitted in a quantum channel and make possible forgery strategies which do not violate the principle of quantum mechanics. However, the message and signature pair is determined by the secret information including the random numbers and the shared keys between the legal participator in advance. Hence Eve's possible forgery will not pass Bob and Trent's verification and the external attack is not available to our scheme.
2. Assume that the receiver Bob wants to forge Alice-i's signature, she should get her identity number ID'_{A_i}. With the property of the Hash function, Bob cannot recognize ID'_{A_i} and get the accurate value. Therefore, she is not able to compute a corresponding M'_0 to pass Trent's verification. Furthermore, even Bob gets the identity of Alice-i and wants to frame her; the shared key K_{AT} is able to prevent this.

3.4. Undeniability

It is not difficult to consider a situation where if Alice-i wants to deny the signature, there would exist some modifications to the initial signature pair $(SN_B, M, M_0, S_A, S_T, R)$ to pass Bob and Trent's verification. Here we should point out that any modification of (SN_B, M, S_A, S_T, R) will be found by Bob. That is because Bob's verification is determined by all of them and Alice-i's modification must destroy their correlation. Meanwhile, any attempt to forge M_0 will be detected by Trent. Therefore, it can be see that Bob and Trent's cooperative verification has prevented Alice's denial of the signature.

Until now, we have analyzed the security of our quantum group signature. Compared with Wen *et al*'s scheme, we

make the arbitrator, Trent, hide the identity information in the signature. Therefore, Trent could recognize who tells a lie if disputes happen. Furthermore, different from Xu *et al*'s model, only the arbitrator is trusted in our scheme and he does not need to store any intermediate information in the signing phase to achieve the traceability. The general assumptions may make our scheme easily applicable in practice.

4. Conclusion and further discussions

In this paper, we have proposed a secure quantum group signature of the classical messages. Our scheme can be realized in practice, because it is based on some current developed quantum and classical technologies (teleportation, QKD, quantum encryption and Hash function). With these techniques, all the characteristics of quantum group signature are truly achieved and some potential security loopholes have been prevented. Furthermore, our scheme is focused on the most general situation in practice, i.e. only the arbitrator is trusted and he does not need to store any intermediate information in signing phase. Therefore it will be easily applicable in the e-payment system, e-government, e-business, etc.

Until now, although a secure quantum group signature for the classical messages has been proposed, the feasible one for a quantum message has not been provided. To our knowledge, the greatest difficulty in designing a quantum group signature scheme for a quantum message is to find a suitable quantum message authentication method for ensuring its integrity. However, the quantum authentication scheme still needs further study. In addition, the noise in a real channel and the imperfect quantum encryption may also influence the validity of the quantum group signature. We hope that some significant results will be obtained in further research.

Acknowledgments

This work was supported by the NSFC (grant numbers 61272057, 61202434, 61170270, 61100203, 61003286 and 61121061), NCET (grant number NCET-10-0260), Beijing Natural Science Foundation (grant numbers 4112040 and 4122054) and the Fundamental Research Funds for the Central Universities (grant numbers 2011YB01 and 2012RC0612).

References

[1] Maitland G and Boyd C 2001 *ICICS 2001: Int. Conf. on Information and Communications Security* (*Lecture Notes in Computer Science* vol 2229) (Berlin: Springer) pp 461–5
[2] Canard S and Traoré J 2003 *ACISP 2003: Australasian Conf. on Information Security and Privacy* (*Lecture Notes in Computer Science* vol 2727) (Heidelberg: Springer) pp 237–48
[3] Qiu W, Chen K and Gu D 2002 *Proc. Information Security Conf.—ISC* (Berlin: Springer) pp 177–90
[4] Shor P 1997 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer *SIAM J. Comput.* **26** 1484–509
[5] Grover L 1996 A fast quantum mechanical algorithm for database search arXiv:quant-ph/9605043v3
[6] Gottesman D and Chuang I 2001 Quantum digital signatures arXiv:quant-ph/0105032v2
[7] Barnum H, Crepeau C, Gottesman D *et al* 2002 *Authentication of Quantum Messages* (Washington, DC: IEEE Computer Society) pp 449–58
[8] Zeng G and Keitel C 2002 Arbitrated quantum-signature scheme *Phys. Rev.* A **65** 042312
[9] Li Q, Chan W and Long D 2009 Arbitrated quantum signature scheme using Bell states *Phys. Rev.* A **79** 054307
[10] Zou X and Qiu D 2010 Security analysis and improvements of arbitrated quantum signature schemes *Phys. Rev.* A **82** 042325
[11] Yang Y 2008 Multi-proxy quantum group signature scheme with threshold shared verification *Chin. Phys.* B **17** 415
[12] Yang Y and Wen Q 2008 Threshold proxy quantum signature scheme with threshold shared verification *Sci. Chin. Ser.* G **51** 1079–88
[13] Yang Y, Wang Y, Teng Y, Chai H and Wen Q 2010 Scalable arbitrated quantum signature of classical messages with multi-signers *Commun. Theor. Phys.* **54** 84
[14] Yang Y and Wen Q 2010 Arbitrated quantum signature of classical messages against collective amplitude damping noise *Opt. Commun.* **283** 3198–201
[15] Wang T and Wen Q 2010 Fair quantum blind signatures *Chin. Phys.* B **19** 060307
[16] Wang T and Wei Z 2012 One-time proxy signature based on quantum cryptography *Quantum Inform. Process.* **11** 455–63
[17] Wen X, Tian Y, Ji L and Niu X 2010 A group signature scheme based on quantum teleportation *Phys. Scr.* **81** 055001
[18] Wen X 2010 Quantum group blind signature scheme without entanglement *Phys. Scr.* **82** 065403
[19] Xu R, Huang L, Yang W and He L 2011 Quantum group blind signature scheme without entanglement *Opt. Commun.* **284** 3654–8
[20] Bennett C and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (Bangalore: IEEE) pp 175–9
[21] Ekert A 1991 Quantum cryptography based on bell theorem *Phys. Rev. Lett.* **67** 661–3
[22] Bennett C 1992 Quantum cryptography using any two nonorthogonal states *Phys. Rev. Lett.* **68** 3121–4
[23] Bennett C, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels *Phys. Rev. Lett.* **70** 1895–9
[24] Gao F, Guo F, Wen Q and Zhu F 2006 Quantum key distribution without alternative measurements and rotations *Phys. Lett.* A **349** 53–8
[25] Buhrman H, Cleve R, Watrous J and Wolf R 2001 Quantum fingerprinting *Phys. Rev. Lett.* **87** 167902
[26] Boykin P and Roychowdhury V 2003 Optimal encryption of quantum bits *Phys. Rev.* A **67** 042317
[27] Zhou N, Liu Y, Zeng G, Xiong J and Zhu F 2007 Novel qubit block encryption algorithm with hybrid keys *Physica* A **375** 693–8
[28] Gao F, Guo F, Wen Q and Zhu F 2008 Comment on 'Experimental demonstration of a quantum protocol for byzantine agreement and liar detection' *Phys. Rev. Lett.* **101** 208901
[29] Zhang Y, Li C and Guo G 2001 Comment on 'Quantum key distribution without alternative measurements' *Phys. Rev.* A **63** 036301
[30] Gao F, Qin S, Wen Q and Zhu F 2007 A simple participant attack on the Bradler–Dusek protocol *Quantum Inform. Comput.* **7** 329–34
[31] Gao F, Wen Q and Zhu F 2008 Teleportation attack on the QSDC protocol with a random basis and order *Chin. Phys.* B **17** 3189

[32] Gao F, Qin S, Guo F and Wen Q 2011 Dense-coding attack on three-party quantum key distribution protocols *IEEE J. Quantum Electron.* **47** 630–5
[33] Qin S, Gao F, Wen Q and Zhu F 2006 Improving the security of multiparty quantum secret sharing against an attack with a fake signal *Phys. Lett.* A **357** 101–3
[34] W'ojcik A 2003 Eavesdropping on the 'Ping-Pong' quantum communication protocol *Phys. Rev. Lett.* **90** 157901
[35] W'ojcik A 2005 Comment on 'Quantum dense key distribution' *Phys. Rev.* A **71** 016301
[36] Cai Q 2003 The 'Ping-Pong' protocol can be attacked without eavesdropping *Phys. Rev. Lett.* **91** 109801
[37] Gao F, Guo F, Wen Q and Zhu F 2008 Consistency of shared reference frames should be reexamined *Phys. Rev.* A **77** 014302
[38] Gao F, Wen Q and Zhu F 2007 Comment on: 'Quantum exam' *Phys. Lett.* A **360** 748–50
[39] Gao F, Lin S, Wen Q and Zhu F 2008 A special eavesdropping on one-sender versus N-receiver QSDC protocol *Chin. Phys. Lett.* **25** 1561
[40] Gao F, Lin S, Wen Q and Zhu F 2010 Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state *Opt. Commun.* **283** 192–5
[41] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 Trojan-horse attacks on quantum-key-distribution systems *Phys. Rev.* A **73** 022320
[42] Deng F, Li X, Zhou H and Zhang Z 2005 Improving the security of multiparty quantum secret sharing against Trojan horse attack *Phys. Rev.* A **72** 044302
[43] Gao F, Qin S, Guo F and Wen Q 2011 Cryptanalysis of the arbitrated quantum signature protocols *Phys. Rev.* A **84** 022344
[44] Choi J, Chang K and Hong D 2011 Security problem on arbitrated quantum signature schemes *Phys. Rev.* A **84** 062330