Extending EMV to support Murabaha transactions

Mansour A. Al-Meaither* and Chris J. Mitchell

Information Security Group, Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, United Kingdom
{M.Al-Meaither, C.Mitchell}@rhul.ac.uk

Abstract. Conventional credit card transactions are not consistent with Islamic principles, as exemplified by the Islamic banking system and the 'Murabaha sale'. On the other hand, EMV-compliant IC (Integrated Circuit) cards have been developed to secure traditional Point of Sale (POS) transactions. Thus, if Islamic principles are to be applied to card payments, a new and secure card payment process is required. In this paper, we propose a method for applying Islamic principles to card payments, where EMV IC cards are used to conduct card Murabaha transactions. After introducing the notion of Murabaha sale within the Islamic banking framework, we outline the EMV payment transaction process. Security requirements are then identified for a secure card Murabaha transaction. We then present a possible modification that allows an EMV card to conduct a Murabaha sale transaction. Finally, we analyse how the proposed scheme matches the identified security requirements.

Keywords:

Murabaha, EMV cards, electronic commerce, payment systems, security.

1 Introduction

A key concept in the Islamic economic system is the prohibition of payment and receipt of interest on deposits and loans. Instead, the sale of goods and the sharing of profits and losses among parties to any business transaction are encouraged. Islamic law puts many restrictions on contracts to attain maximal justice in a financial transaction, minimise the potential for legal disputes, and build a healthy and stable financial and economic system [1].

Modern banking systems were introduced into the Muslim countries in the late 19th century. Many Muslims confined their involvement with these banks to transaction activities such as current accounts and money transfers. Borrowing from banks was strictly avoided in order to avoid dealing in interest, which is prohibited in Islam.

* This author's work is supported by the Saudi Arabian Government

As a result, Islamic banks began to offer financial instruments consistent with Islamic religious beliefs.

Although it is difficult to obtain exact figures on the size of the Islamic financial sector, it is nevertheless experiencing strong growth. According to [7], the Islamic banks assets grew from $5 billion in 1985 to over $100 billion in the late nineties. While conventional banks guarantee the capital and rate of return, Islamic banks, working on the principle of profit and loss sharing, cannot, by definition, guarantee any fixed rate of return on deposits.

Meanwhile, the growing volume of fraud in credit/debit card transactions at the Point of Sale (POS) has led the card associations MasterCard and Visa to support their members in providing card-holders with a chip-based card. The advantages include combating fraud, validating both card and cardholder, and managing cards remotely. In order to allow a single merchant terminal to be used with cards issued by different card issuing banks and different brands, the EMV [2–5, 9] specifications have been developed, which define the physical and electrical characteristics of the IC card, the IC terminal specifications, and how the IC terminal communicates with the IC card. The security services supported by the EMV specifications include the following:

- Card authentication, where a terminal can be certain that a card is genuine,
- Risk management, where the card and the terminal independently decide which transactions need to be referred back to the card issuer at the time of the transaction,
- PIN verification on the card itself, and
- Transaction authorization by which a card issuer can be certain that a transaction has come from a specific and authentic card, as well as the card ensuring that the approval/decline response has been sent by the authentic issuer.

However, conventional credit card transactions are not consistent with Islamic principles, since they involve dealing in interest. Therefore, if Islamic principles are to be applied to card payments, a new and secure card payment process that is consistent with Islamic principles is required. Meeting this need by extending the EMV specifications to enable cards to conduct Murabaha transactions is potentially attractive for a number of reasons.

1. There will potentially be a significant reduction in Murabaha sale transaction expenses.
2. There will undoubtedly be a significant increase in Murabaha transactions, which will result in additional revenue stream for both merchants and issuers.
3. EMV is a good basis for inter-operability and global coverage.
4. Cardholders already have a trust relationship with their issuer.
5. Exploiting the existing EMV infrastructure provides a cost-effective solution.

In this paper we present a method of using EMV cards for secure card-based Murabaha transactions. After introducing the notion of Murabaha sale within the Islamic banking framework, we outline the existing EMV payment process.

Security requirements are then identified for a secure card-based Murabaha transaction. We then present a possible modification to EMV that allows the conduct of a Murabaha sale transaction, Finally, we analyse how the proposed protocol matches the identified security requirements.

2 Murabaha Sale

Murabaha sale is one of the most commonly used forms of financing provided by Islamic banks. Hasanin [6] notes that Murabaha is the mode of contract most frequently used in Islamic banking, in some cases accounting for 90% of all financing.

Murabaha is an Arabic term that means obtaining profit, and is a type of trust trading. Financially, it means cost plus profit sale, but in Islamic law it is a term that refers to a particular kind of sale [6].

A customer wishing to purchase goods requests the Islamic bank to purchase these items on his behalf and then sell them to him with a certain amount of profit agreed upon added to the initial cost. In the period up to the resale the bank has title to the goods, and hence a legal responsibility. The basic component of Murabaha is that the seller discloses the actual cost he has incurred in acquiring the goods, and then adds some profit thereon.

2.1 Rules Governing a Murabaha Sale

The validity of a Murabaha transaction depends on certain conditions, which should be properly observed to make the transaction acceptable in Islamic law. The rules that govern this principle, as stated in [6], are as follows.

- The two sale transactions making up a Murabaha payment, one through which the financial institution acquires the commodity and the other through which it sells it to the customer, should be separate and real transactions.
- The financial institution must own the commodity before it is sold to the customer.
- It is essential to the validity of the Murabaha that the customer is aware of the original price, including the costs necessary to obtain the commodity, and the profit. This is because Murabaha is a sale with a mark-up, and if the customer did not know the basic price then a violation of the Murabaha sale conditions has taken place.
- Both parties, i.e. the financial institution and the customer, have to agree on the profit for the financial institution from the sale, where the sum of the cost and profit is equal to the selling price charged by the financial institution.
- Murabaha is valid only where the exact cost of a commodity can be ascertained. If the exact cost cannot be ascertained, the commodity cannot be sold on a Murabaha basis.
- It is also necessary for the validity of Murabaha that the commodity is purchased from a third party. The purchase of the commodity from the

customer on a "buy back" agreement is not allowed in Islamic law. Murabaha based on a "buy back" agreement would be nothing more than an interest-based transaction.
- Cash is not permitted to be withdrawn on a Murabaha basis.

Unless these conditions are fully observed, a Murabaha transaction becomes invalid under Islamic law.

3 The EMV Transaction process

In this section, we give an overview of the EMV transaction flow, with a focus on the security mechanisms. A more detailed description of these mechanisms can be found in [3].

An EMV card payment transaction involves interactions between four parties: the cardholder, the merchant, the acquirer, and the issuer, with roles as follows.

- **Issuer**: A financial institution that issues a payment card to the cardholder.
- **Cardholder**: An authorised holder of an card issued by the issuer. The card stores the cardholder's payment data and is capable of generating authentication data and verifying a cardholder's PIN. During a transaction, a cardholder has a connection only to the merchant, which passes authorisation messages to the issuer (via the acquirer).
- **Merchant**: This is the business that accepts the card payment for the purchased goods. It uses a terminal to interact with the card. The terminal also interacts with the issuer (via the acquirer) to receive authorization for payment transactions.
- **Acquirer**: This is a financial institution that processes card payment authorizations and payments for the merchant. The acquirer and the issuer communicate through a secure financial network.

3.1 EMV transaction security

EMV transaction security is accomplished in two phases:

1. **Authentication.** Card authentication to the terminal is achieved using digital signatures. A chain of trust is established from the card scheme, which acts as the top-level certification authority (CA). Each terminal has a trusted copy of the CA's public key; the CA signs a certificate for the issuer public key and this certificate is stored on the card. The CA's public key and the issuer certificate are used to verify the authenticity of data stored in the card and messages sent by the card to the terminal during a transaction.
   Cardholder authentication is performed by PIN entry at the terminal. The PIN can be verified offline by the card, or online by the issuer. If supported, PIN encryption for offline PIN verification is performed by the terminal using an asymmetric encipherment mechanism [3]. The card may have a separate

key pair for PIN encryption or it may use the signature key pair. The card's public key is then used by the PIN pad to encrypt the PIN, and the private key is used by the card to decrypt and then verify the encrypted PIN.
2. **Transaction authorisation.** Transactions can be approved either offline by the card or online by the issuer. In both cases, symmetric cryptographic mechanisms are used to generate and verify Application Cryptograms (AC). The ACs exchanged by the issuer and the card are cryptographically secured using MACs (Message Authentication Codes). These are computed using a session key derived from a long term secret key shared between the card and the issuer.

The EMV Specifications allow both phases to be completed offline, without communicating with the issuer. However, the card or the terminal may force the transaction online, in which case an authorisation message is sent to the issuer for verification.

3.2 EMV transaction flow

The EMV transaction flow begins when the buyer card is inserted into the merchant terminal. The terminal reads data from the card for use in its risk management and to establish the card authenticity.

There are two types of card authentication, Static and Dynamic Data Authentication (SDA and DDA), where not all cards support DDA. For the card to support DDA it must have its own signature key pair and the means to generate signatures. In both cases the terminal uses a stored copy of the card brand public key to verify the issuer public key certificate; in DDA, the terminal also verifies an issuer-signed certificate for the card public key. In SDA, the terminal verifies the issuer's signature on critical card resident data so that unauthorised alteration of issuer data after personalisation is detected. In DDA, the terminal uses a public key based challenge response protocol to authenticate the card and verify the integrity of card resident data [3].

Next the Cardholder verification method is invoked to ensure that the person presenting the card is the one to whom the application in the card was issued. For this purpose EMV uses a secret PIN, where this PIN can be verified either offline by the card or online by the issuer. Upon successful cardholder verification, the terminal then decides whether the transaction should be approved offline, declined offline, or an online authorisation is necessary. Providing it does not reject the payment at this stage, the terminal passes the payment request to the card in the form of a GENERATE AC command. In response, the card performs 'action analysis'. Depending on the card risk management policy the card's action analysis can return one of three results [4].

1. A Transaction Certificate (TC), when the payment is approved offline.
2. An Authorisation ReQuest Cryptogram (ARQC), when either the card or the terminal want to go online so that the issuer can authorise or reject the transaction. The issuer then responds with an Authorisation ResPonse

Cryptogram (ARPC) which the card verifies and acts on. The terminal then issues a second GENERATE AC command that includes the issuer response and possibly a command script that the issuer may send. If the transaction is approved by the issuer, the card computes a transaction certificate (TC).
3. An Application Authentication Cryptogram (AAC), when the request is declined.

Finally, by returning either a TC or an AAC to either the first or second GENERATE AC command issued by the terminal, the card indicates its willingness to complete transaction processing. If the terminal decides to go online, completion shall be achieved when the second GENERATE AC command is issued.

4 Using EMV cards for a Murabaha transaction

The method proposed here for using EMV to support a Murabaha transaction involves the same participants and roles as the standard EMV payment process. However, using EMV for a Murabaha transaction requires extensions to the current security model and message flows. A key feature of a Murabaha transaction is that it is composed of two transactions, one between the merchant and the issuer, and the other between the cardholder and the issuer. Therefore, using an EMV card for a Murabaha transaction requires online communication with the issuer for every EMV Murabaha transaction that takes place. Moreover, the following assumptions are made.

1. The issuer has an agreement with the cardholder to sell him goods on a Murabaha basis. The issuer undertakes to purchase commodities as specified by a buyer, and then resell them on a Murabaha basis to the cardholder for the cost price plus a margin of profit agreed upon previously by the two parties. The issuer does not make a purchase unless the buyer requests it and makes a prior promise to purchase.
2. The EMV card is DDA capable.
3. Every acquirer participating in the scheme has their own signature key pair.
4. Every acquirer participating in the scheme has obtained a certificate for their public key from the brand CA, and this certificate is loaded into every merchant terminal supported by this acquirer.
5. Every issuer is equipped with a copy of the public key of the brand CA, as necessary to verify acquirer certificates.
6. Every terminal is equipped with its own public key certificate signed by its acquirer. [Alternatively the acquirer could append this certificate to every signed message sent from a merchant terminal to an issuer, as it passes through the acquirer network]. Additionally, it has the means to compute signatures, as well as a privacy-protected location in which to store its private key.
7. In a standard EMV transaction, terminal risk management is performed to protect the system against fraud. It provides positive issuer authorisation for

high-value transactions and ensures that transactions initiated from the card go online periodically to protect against threats that might be undetectable in an offline environment [4]. However, since this function is related to offline transactions, and the proposed extension requires the terminal to go online for every transaction, terminal risk management is not performed in the proposed extension.

4.1 Security requirements

No participant in any transaction want to suffer any loss. Therefore, we need to define precisely the security requirements to meet the needs of the transaction participants. We therefore next identify what security services are required for a secure card-based Murabaha transaction. The security services can be divided into four categories: authentication, confidentiality, integrity, and non-repudiation.

Authentication

Entity authentication provides assurance to one party regarding the identity of a second party involved in a protocol, and that the second has actually participated [8]. In the proposed extension to EMV, this security service can be sub-divided into the following:

1. Verification by the issuer that the merchant is as claimed.
2. The merchant needs to be sure that the payment card is genuine.
3. The merchant needs evidence that the cardholder is the legitimate owner of the payment card.
4. The issuer needs to be sure that the source of the payment instruction is a legitimate card.
5. No attacker can authorise a false EMV card-based Murabaha transaction on behalf of a cardholder.

Confidentiality

Confidentiality for information exchanged between the transaction participants is needed. The main reason for confidentiality is to prevent misuse of transaction data by unauthorised parties [8]. This security service can be sub-divided into the following:

1. The cardholder PIN must be kept secret from non-authorised parties.
2. The cardholder may require privacy of his order information.

Integrity

Integrity ensures that data is not altered in an unauthorised manner since it was created, transmitted, or stored by an authorised participant [8]. This security service can be sub-divided into the following.

1. The cardholder must be aware of the original price of the goods being purchased and the amount of profit the issuer is charging him before buying the goods. This is important for the transaction to be compatible with Murabaha sale conditions.
2. The buyer requires assurance that the issuer owns the goods being offered.
3. The cardholder payment authorisation must be protected against alteration, or any alteration must be detectable.

Non-repudiation

Non-repudiation prevents a participant from denying an action he has performed [8]. This security service can be sub-divided into the following.

1. The merchant must have evidence that the issuer has bought the goods and authorises him to sell the goods on his behalf to the cardholder.
2. The issuer must possess evidence that the cardholder has authorised payment for the goods on a Murabaha basis.

4.2 Interaction

We now describe the processes necessary to complete an EMV-based Murabaha transaction. In the description, $X||Y$ denotes the concatenation of data items X and Y and $S_X(M)$ is the signature of entity X on message M using the private signature key of entity X.

Figure 1 illustrates a transaction in which a cardholder uses his EMV card to purchase goods on a Murabaha basis from a merchant. It begins when the card is inserted into the merchant terminal (step 1). To authenticate the card, DDA is performed.

The terminal first issues the READ RECORD command (step 2) which returns the Primary Account Number (PAN), the CA identifier, the issuer public key certificate Cert_I, and the card public key certificates Cert_{IC}. In order to authenticate the card's public key in Cert_{IC}, the terminal verifies the issuer public key certificate Cert_I using its copy of the CA public key. The issuer signature on Cert_{IC} is then verified.

After successful verification of the card certificate Cert_{IC}, the terminal constructs the Purchase Information (PI), which contains a description of the goods, price and the date. Moreover, the terminal generates authentication data ($Data$) which contains a random number generated by the terminal, the current date and time, and the card PAN. The terminal then sends a challenge to the card using an INTERNAL AUTHENTICATE command containing $Data||PI$ (step 4). The EMV specification allows the INTERNAL AUTHENTICATE command to carry data of size up to 252 bytes [4], which is enough for the authentication data and the additional PI. Upon receipt of the message in step 4, the card computes the signature $S_{IC}(Data||PI)$ and sends it to the terminal (step 5). The card response (step 5) acts as a promise from the cardholder to buy the goods from the issuer on a Murabaha basis. Using the card certificate Cert_{IC}

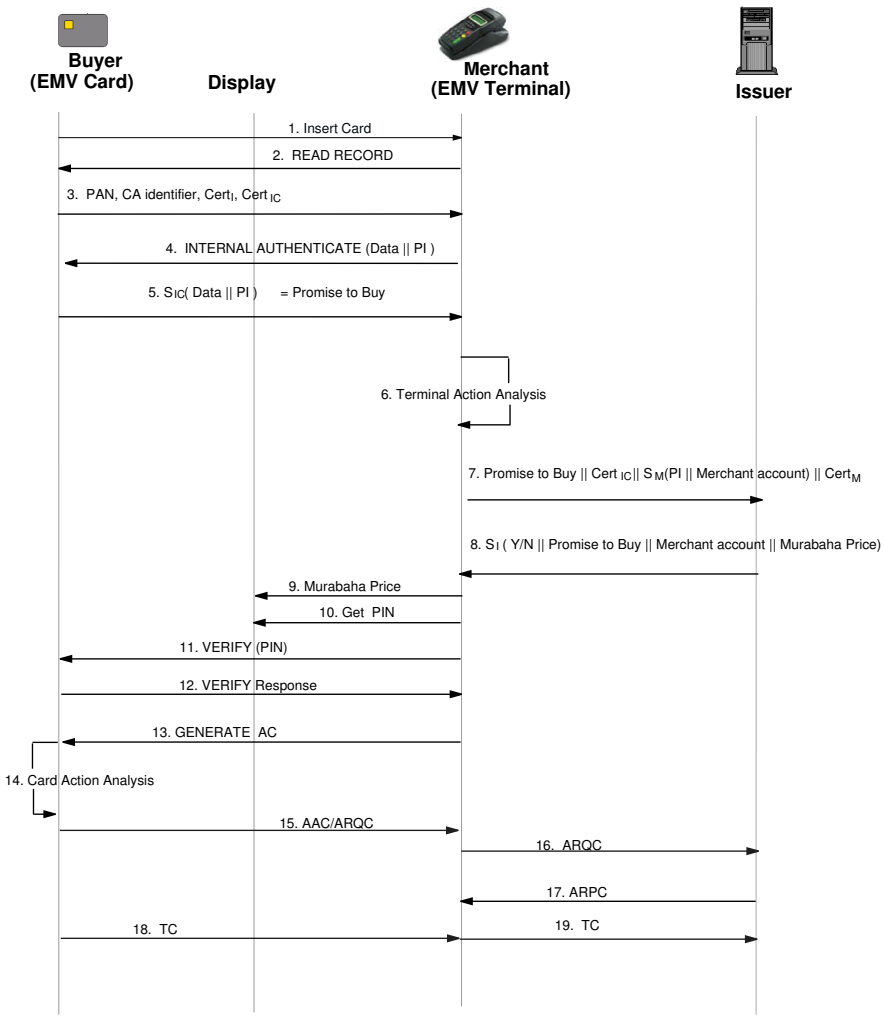

Fig. 1. EMV card-based Murabaha transaction

retrieved in step 3, the terminal verifies the signature $S_{IC}(Data||PI)$. Then, it checks that the same random number sent in step 5 is present in the signed data.

After successful verification of the signature received in step 5, the terminal action analysis is performed (step 6), where the decision is made as to whether the transaction should be declined offline, or continue online. If the decision is to reject the transaction, the terminal will issue a GENERATE AC (step 13) asking for an Application Authentication Cryptogram (AAC) from the card. If the outcome of the decision is to go online, the terminal constructs a message that contains the cardholder promise to buy the goods made in step 5 and the merchant signature over its bank details ('Merchant account') and PI. The terminal then sends this message (step 7) to the issuer along with its public key certificate Cert_M and the card public key certificate Cert_{IC}.

The information sent in step 7 notifies the issuer that a cardholder wishes to buy the goods, with the description given in PI, on a Murabaha basis. The issuer checks the cardholder promise to buy. If the issuer decides to proceed with the transaction, he first buys the goods from the merchant by crediting the goods price to the ('Merchant account') received in step 7. Then, the issuer constructs and sends a signed authorisation message to the terminal (step 8). This message contains the issuer decision as to whether to proceed or decline the transaction, and the price at which the goods will be sold to the cardholder ('Murabaha price'). In addition, this message authorises the merchant to sell and deliver the goods on behalf of the issuer to the cardholder. The signature in step 8 can be verified by the merchant terminal using the issuer's public key obtained during step 2.

After successful verification of the signature received in step 8, the terminal displays the 'Murabaha price' to the cardholder (step 9) and requests the buyer to enter his PIN (step 10). EMV allows the PIN to be verified offline by the card or online by the issuer. In the proposed scheme, both options remain valid. If the decision is to perform offline verification, the terminal sends a VERIFY command to the card (step 11). On receipt of the VERIFY command, the card returns a VERIFY response message (step 12), which indicates success or failure. In addition to ensuring that the person presenting the card is the person to whom it was issued, correct PIN entry by the cardholder is regarded as agreement by the cardholder to purchase the goods from the issuer on a Murabaha basis at the specified price (the 'Murabaha price').

After successful cardholder verification, the terminal sends a GENERATE AC command to the card (step 13). Next, the card action analysis process (step 14) begins, where a card performs its own risk management to protect against fraud or excessive credit risk [4]. Details of card risk management algorithms within the card are specific to the issuer. A card may decide to complete the transaction online or reject the transaction offline. If the outcome of the decision is to reject the transaction offline, an AAC is returned by the card to the terminal (step 15) and the transaction ends. If the outcome of the decision is to complete the transaction online, an ARQC is generated and sent by the card to the terminal (step 15) and then forwarded to the issuer (step 16). The issuer

responds to the ARQC with an ARPC (step 17). If the transaction is accepted, the card generates a TC (step 18) and sends it to the terminal which forwards it to the issuer (step 19) and the transaction ends.

In the proposed extension, most of the transaction procedures are similar to those in the standard EMV payment process. However, some messages have been modified and additional messages have been added to satisfy the Murabaha sale rules. For example, the INTERNAL AUTHENTICATE command (step 4) includes the Purchase Information (PI) in addition to the authentication data required by the EMV specifications. Therefore, the response signature (step 5) computed by the card must be computed on the PI in addition to the authentication data. Moreover, completely new messages (steps 7&8) have been added between the merchant and the issuer. These messages are necessary to complete the first transaction as specified in section 2.1, which is not part of the EMV standard.

Extending the EMV standard payment process requires that the terminal firmware be upgraded to allow the storage of a terminal-specific signature key pair. Additionally, the acquirer and the issuer transaction processing software must be modified to carry the new EMV messages.

An advantage of the proposed extension is that the existing EMV card needs not be changed to perform the extended transaction. The proposed changes affect only the merchant, the acquirer, and the issuer.

5 Security analysis

In this section, we examine to what extent the generic security requirements outlined in section 4.1 are met by the extended EMV transaction.

5.1 Authentication

1. *Verification by the issuer that the merchant is as claimed.* The "standard" EMV transaction does not provide mechanisms to authenticate the merchant terminal to the cardholder and the issuer [10]. However, in our extension, the merchant terminal has its own public key certificate Cert_M, which is sent along with the terminal signature in step 7 to the issuer. The issuer verifies the merchant certificate and that the merchant signature is valid; if this verification process fails then the transaction is not completed. Nevertheless, it is still possible for the cardholder to interact with a different merchant than intended.
2. *The merchant needs to be sure that the payment card is genuine.* This is performed using DDA. The merchant terminal verifies that the card certificate Cert_{IC} retrieved in step 3 is valid. In addition, the terminal verifies the validity of the card response (step 5).
3. *The merchant needs evidence that the cardholder is the legitimate owner of the payment card.* This is accomplished using PIN entry which can be verified either offline by the card or online by the issuer. An authentic cardholder will

enter the correct PIN. Moreover, the EMV Specifications limit the number of unsuccessful PIN entries [4].

4. *The issuer needs to be sure that the source of the payment instruction is a legitimate card.* The issuer can use the *Promise-To-Buy* and Cert_{IC} received in step 7 to verify the legitimacy of the card. Moreover, the ARQC (step 16) and TC (step 19) are generated using a key shared between the card and the issuer.
5. *No attacker can authorise a false EMV card-based Murabaha transaction on behalf of a cardholder.* The cardholder PIN is assumed to be a secret known only to the cardholder. Therefore, nobody but the cardholder can authorise an EMV card-based Murabaha transaction. This is based on the assumption that the merchant terminal displays the correct transaction data to the cardholder. This is a standard assumption for merchant terminals, where the cardholder is required to trust the reputation of the merchant when using a card in the merchant premises. In addition a fraudulent merchant is easy to track and prosecute.

5.2 Confidentiality

1. *The cardholder PIN must be kept secret from non-authorised parties.* If PIN verification is done using the card (offline), then the terminal can encrypt the cardholder PIN when sent from the PIN pad to the card. The card might use a separate key pair for PIN encryption or use its signature key pair. The card public key is used by the terminal (PIN pad) to encrypt the PIN, and the private key is used by the card to decrypt the encrypted PIN [3] in order to verify it.
2. *The cardholder may require privacy of his order information.* Order information is not encrypted and can be read by the terminal, the acquirer, and the issuer. Therefore, this requirement is not satisfied.

5.3 Integrity

1. *The cardholder must be aware of the original price of the goods being purchased and the amount of profit the issuer is charging him before buying the goods.* Since the cardholder chose the goods that are to be bought on a Murabaha basis from the merchant, we assume that he/she is aware of the original price of the goods. Moreover, in step 8 of the interaction, the terminal receives confirmation of the issuer willingness to sell the goods on a Murabaha basis with the 'Murabaha price' being the price at which the goods should be sold to the cardholder. This is followed by the terminal asking the cardholder for PIN entry. Entry of the correct PIN is taken as confirmation of the willingness of the cardholder to continue the transaction.
2. *The buyer requires assurance that the issuer owns the goods being offered.* By sending the message in step 8 to the terminal, the issuer provides an undeniable assurance to the terminal that it has purchased the goods. The buyer has to trust the merchant terminal to display the 'Murabaha price'

only if the message in step 8 is verified correctly and indicates that the issuer has credited the 'Merchant account'.

3. *The cardholder payment authorisation must be protected against alteration, or any alteration must be detectable.* This requirement is met, because MACs are used to protect the integrity of the AC generated by the card. The card and the issuer can verify MACs generated by each other using a shared key.

5.4 Non-repudiation

1. *The merchant must have evidence that the issuer has bought the goods.* The merchant can verify the message received in step 8 from the issuer. If it verifies successfully, then it provides a payment guarantee from the issuer, because it contains the issuer agreement to buy the goods, the goods description, and the merchant bank details ('Merchant account').
2. *The issuer must possess evidence that the cardholder has authorised payment for the goods on a Murabaha basis.* Entry of the correct PIN by the cardholder upon the display of the 'Murabaha price' will trigger the generation of an ARQC and a TC by the card. The TC sent to the issuer in step 19 can be regarded as evidence of cardholder authorisation; however, the TC is generated using a shared key with the issuer. Therefore it is of no value in providing non-repudiation unless combined with evidence from audit trails, e.g. held by the acquirer.

6 Conclusion

In this paper, we have proposed an extension to the EMV specifications to enable cards to conduct Murabaha transactions at POS terminals. We described the extension in detail, and explained how it meets the identified security requirements. In the proposed extension, most of the transaction procedures are similar to those in the standard EMV payment process. However, additional messages have been included to satisfy the Murabaha sale rules. The proposed extension can be seen as a step towards adapting electronic payment schemes to the Islamic economic system.

Finally, a future possible research area is to see how to conduct a Murabaha transaction using a mobile phone.

7 Acknowledgement

The authors thank Sami Al-Suwailem from the Center for Research and Development of Al-Rajhi Banking and Investment Corporation, for discussions that helped shape some of the ideas in this paper.

References

1. Mahmoud Amin El-Gamal. *A Basic Guide to Contemporary Islamic Banking and Finance*. Islamic Society of North America, Plainfield, IN, USA, 2000.
2. EMV. *EMV2000 Integrated Circuit Card Specification for Payment Systems Version 4.0 — Book 1: Application Independent IC Card to Terminal Interface Requirements*. EMVCo, 2000.
3. EMV. *EMV2000 Integrated Circuit Card Specification for Payment Systems Version 4.0 — Book 2: Security and Key Management*. EMVCo, 2000.
4. EMV. *EMV2000 Integrated Circuit Card Specification for Payment Systems Version 4.0 — Book 3: Application Specification*. EMVCo, 2000.
5. EMV. *EMV2000 Integrated Circuit Card Specification for Payment Systems Version 4.0 — Book 4: Cardholder, Attendant, and Acquirer Interface Requirements*. EMVCo, 2000.
6. Fayad Hasanin. *Murabaha Sale in Islamic Banks*. The International Institute of Islamic Thought, Herndon, VA, USA, 1996.
7. Zamir Iqbal and Abbas Mirakhor. Progress and challenges of Islamic banking. *Thunderbird International Business Review*, 41(4–5):381–405, 1999.
8. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography*. CRC Press, Boca Raton, FL, USA, 1997.
9. Donal O'Mahony, Micheal Peirce, and Hitesh Tewari. *Electronic Payment Systems for E-Commerce*. Artech House, Norwood, MA, USA, 2001.
10. Mostafa Hashem Sherif. *Protocols for Secure Electronic Commerce*. CRC Press, Boca Raton, FL, USA, 2000.