Security Enhancement for Magnetic Data Transaction in Electronic Payment and Healthcare Systems

Lakshmisha Honnegowda, Syin Chan, and Chiew Tong Lau

***Abstract*—In recent years, the fraudulent cash withdrawal and transaction due to card skimming have become increasingly common. Even though cardholders are increasingly using smartcard and personal identification number (PIN) technology, there are businesses and services still rely on magnetic stripe data transaction in American and Asia-Pacific countries. The personal data on card's magnetic stripe is not encrypted and hence prone to identity theft and counterfeit card frauds. This paper proposes a framework to enhance the security of magnetic stripe data transaction. The proposed framework consists of two main components: Electronic Transaction Card (ETC) and Issuer Authentication Software (IAS). The ETC is embedded with magnetic stripe emulator which dynamically generates a varying electromagnetic field when the credit/debit card is being swiped across the reader head. The dynamically generated electromagnetic field corresponds to user information that is typically encoded on a static magnetic stripe. The user information can include cardholder's account number, encrypted Transaction Identification Number (TIN), and even secret codes to enhance the security. The IAS, at the card issuer's backend mainframe system, decodes the user information together with TIN received from merchant's point-of-sale terminal to authenticate the transaction. The proposed framework/infrastructure, with dynamic magnetic stripe data broadcast feature, counteracts card skimming and achieves an enhanced security for magnetic data transaction technology.**

***Index Terms*—Electronic smartcard, magnetic emulator, electronic payment system, healthcare system.**

I. Introduction

The healthcare cards or payment credit/debit cards provide portability to cardholder's personal information such as account and identification number. The mobility of personal information benefits all stakeholders involved in the system. Healthcare system stakeholders include patients, healthcare professionals/provider, and health insurer/payers, whereas payment system stakeholders include cardholder, merchants and card issuer. These plastic cards encode cardholder's personal information on magnetic stripe in Frequency/Double Frequency (F2F) format which conform to ISO/IEC-7811standard [1]. The magnetic data transaction technology is intuitively easy to use and requires minimal infrastructure.

In healthcare and payment ecosystems, the security for portable personal information transaction has become a primary requirement. Essential security requirements for cardholder's sensitive information include authentication, data integrity, confidentiality and privacy. Businesses and services in American and Asia-Pacific countries still rely on card's magnetic stripe data transaction.

The "smart" chip systems, in other parts of the world, still use the magnetic stripe as a backup. But the static magnetic stripe based healthcare or payment cards are highly susceptible to physical damage and fraudulent activities, such as identity theft and counterfeit card frauds. In recent years, the card skimming has become increasingly common and cause fraudulent cash withdrawals from automated teller machines (ATM). The fraudulent transactions cause millions to billions of dollars loss to card issuing banks [2]. The fraudulent activity, skimming, commonly takes place at ATM machines, gas pumps, and self-checkout machines at grocery stores. And card skimming scam is being driven by the low-tech nature of static magnetic stripe data on credit or ATM cards.

Currently, the card issuers/banks are fighting the trend with counter-skimming technology, where sensors in ATM machines or terminals detect skimming devices being attached and block recording and transmitting of card's magnetic stripe data and personal identification number (PIN). In addition, banks have also started to issue skimming awareness guide to their customers. But the advancement in electronic mobile devices and wireless technology made skimmers to develop piggyback skimming device, which looks exactly like a normal card entry slot, to read card data. Advanced pinhole cameras at topside of the ATM machines can easily capture cardholder's PIN.

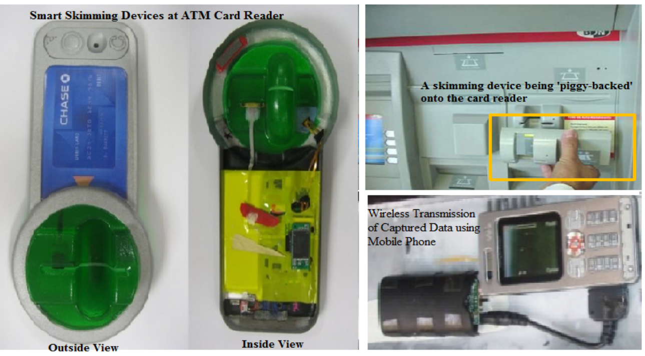

Smart Skimming Devices at ATM Card Reader
CHASE
Outside View
Inside View
A skimming device being 'piggy-backed' onto the card reader
Wireless Transmission of Captured Data using Mobile Phone

Fig. 1. Smart ATM card skimming devices to capture credit/debit card information at ATM card reader

The smart skimming devices, Fig. 1, transmit secretly scanned user information wirelessly to smart mobile devices at fraudster. Even though the introduction of cryptography based 'chip and PIN' smartcard technology has reduced the volume of fraudulent activities in Europe, the U.S. and Asian market may still take decades to completely adopt chip-and–PIN based ATMs and point-of-sale systems. The main factors such as lack of financial incentive of card issuers

Manuscript received Janaury 10, 2013; revised March 12, 2013.

The authors are with the School of Computer Engineering, Nanyang Technological University, Singapore (email: honn0002@ntu.edu.sg, asschan@ntu.edu.sg, asctlau@ntu.edu.sg)

DOI: 10.7763/IJET.2013.V5.569

and cost to merchants to invest in new technology delay the replacement of ATMs and POS terminals with chip based systems.

In this paper, we present a novel framework in conjunction with next generation electronic transaction card which is embedded with a dynamic magnetic stripe emulator/encoder [3]-[8]. The magnetic stripe emulator mimics a traditional static magnetic stripe F2F data transmission. Electronic transaction card enables F2F data transmission only when the user swipes the card across magnetic reader head. The F2F data, generated by the magnetic emulator circuit, includes the combination of cardholder's information and unique transaction identification number (TIN). In addition, the battery-powered electronic transaction card can incorporate secure chip with multiple application to support contact (ISO/IEC-7816) and contact less (ISO/IEC-14443) smartcard interfaces. Specifically, the focus is on framework or infrastructure that takes an advantage of this dynamic magnetic stripe emulator feature to enhance the security in electronic payment and healthcare systems.

II. Static Magnetic Stripe Issues

The magnetic stripe based credit/debit cards store the cardholder's personal information, account numbers or personal identification numbers, in binary form. The data encoding in binary form is known as Frequency/Double Frequency (F2F) or Aiken Biphase technique. Before encoding, the cardholder's alphanumeric information is coded in to one (1) and zero (0) bits as per Coded Character Set tables in ISO/IEC 7811-2 standard.

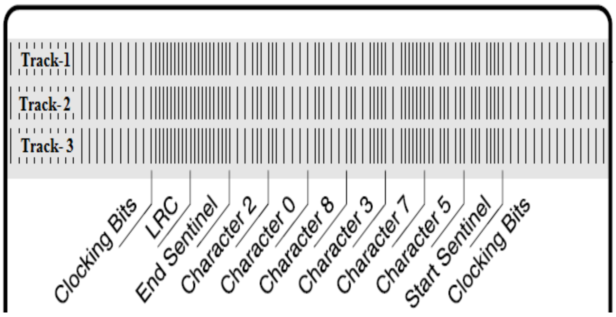


Fig. 2. F2F encoding of character code on magnetic stripe of credit/debit card

The data bits are encoded serially on the stripe with a series of magnetic flux transitions, as in Fig. 2. When the card with magnetic stripe passes the reader head, the encoded flux transitions are converted into a series of alternating positive and negative pluses, as in Fig. 3, at the reader head. The data bits that are encoded in an induced signal are decoded by the signal conditioning circuit of the card reader.

User information encoded on credit / ATM card's magnetic stripe is static. This unsecured static magnetic information can be easily captured by the skimming devices, Fig. 1, to make duplicate cards for fraudulent activities. The static magnetic technology is low-tech in nature and prone to skimming.

In order to support the magnetic transaction technology in the current market, about 90% in U.S., credit/debit cards with or without smart-chip facility must deploy these conventional static magnetic stripes for data transmission [9], [10]. Magnetic stripe cards are deficient because the magnetic stripe is highly susceptible to physical damage and data corruption due to magnetic interference. In addition, the static magnetic stripe based cards fail to protect against credit/debit card fraud where the card numbers are copied and used without cardholder's permission. These fraudulent activities cost millions to billions of dollars to card issuers/banks.

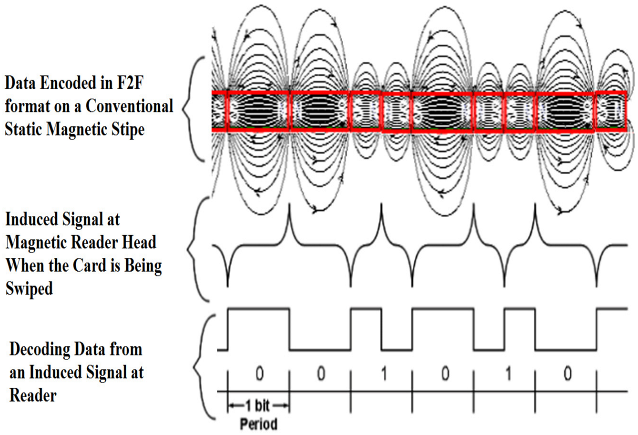

Data Encoded in F2F format on a Conventional Static Magnetic Stipe
Induced Signal at Magnetic Reader Head When the Card is Being Swiped
Decoding Data from an Induced Signal at Reader
0
0
1
0
1
0
1 bit Period

Fig. 3. Encoded data on card's magnetic stripe and decoding it at magnetic reader when the card is swiped across the reader head.

The card fraudulent activities such as lost or stolen card, Identity theft, skimming, counterfeit card, mail intercept fraud and card-not-present fraud are some of the common type of frauds in financial transactions.

Lost/Stolen Card Fraud – It is a most common type of fraud occurs when a legitimate cardholder receives the card from the issuer and losses it or someone, who is involved in criminal activities, steals the card. In this type, the fraudster easily get hold of others card information without an investment in technology. The lost/stolen card fraud occurs before the legitimate cardholder reports status to issuer.

Counterfeit and Fake Card – Together with lost/stolen card fraud, the creation of fake and counterfeit cards pose a highest threat in credit card frauds. It occurs at illegally fitted cash machines or retail outlets with sophisticated skimming device. Counterfeit and false cards are created, without the knowledge of the cardholder, from techniques such as re-embossing/re-encoding and electronically coping of magnetic stripe data. Skimming is emerging as the popular technique use for this type of card fraud.

Card-not-Present Fraud – In this type of card fraud, the fraudster steals information of the cardholder and uses them to purchase valuable stuffs over computer or smartphones which are connected to internet, email or fax.

Postal or Mail Intercepts Fraud – This type of card fraud occurs when a card is stolen from the postal service, which is initiated by user for new card, before it reaches an intended card receiver.

Identity Theft – In this type, fraudsters illegally get hold of the personal information of the legitimate cardholders and use this information to create or access card accounts.

The credit/debit card fraud experienced by cardholders in many countries, Fig. 4, is at highest rate and it has become highly mobile form of crime all over the world.

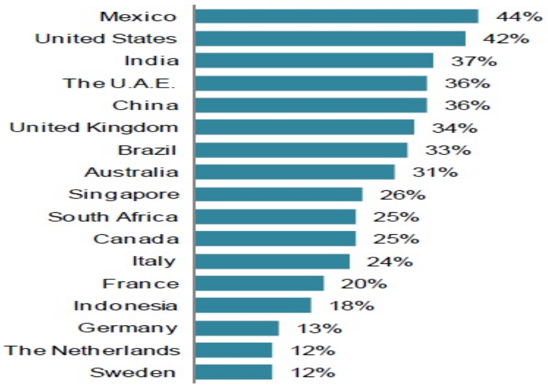


Fig. 4. Percentage of card fraud experienced by cardholders (Source: Aite group, ACI worldwide study of 5,223 consumers in 17 countries)

The comprehensive ECB report on card fraud shows card fraud analyses [11]: ATM fraud ranged from 0% to 91%, CNP fraud from 3% to 84%, and POS fraud from 7% to 65%. The global fraud report unveils that residents of U.S. and Mexico accounted the highest percentage of direct experience with card fraud, at 42% and 44% respectively [12].

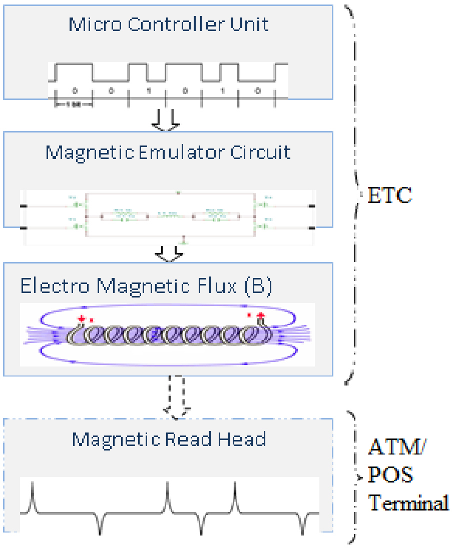


Fig. 5. Dynamic electromagnetic field generated at ETC and read signal at ATM/ POS terminal

III. Electronic Transaction Card

An electronic transaction card (ETC) is a battery-operated standalone embedded device which is deployed with dynamic magnetic stripe emulator/encoder. The microcontroller driven magnetic stripe emulator energizes and generates F2F data format, Fig. 5, only when the card is swiped across the magnetic data reader head of ATM or POS terminal. The magnetic emulator/encoder module include: dynamically writable magnetic stripe or an electronic circuit which generates electromagnetic field corresponding to F2F data to be transmitted. The most feasible electronic circuit based magnetic emulator/encoder may include planar spiral inductor, planar solenoid inductor, on-package solenoid inductor, or planar transmission line inductor with different iron core material to generate electromagnetic field. The generated electromagnetic field strength mimics the magnetic field strength from a traditional static magnetic stripe. The solenoid inductor with iron core generates a variable electromagnetic field with strength (B) has direct relationship with a driving current (I), number of coil turn per unit length (N/L) and relative permeability (μ_0) of core material, as in (1).

$$B = \mu_0 I(N/L) \tag{1}$$

The electromagnetic field strength must be designed such that the induced peak-peak voltage at the magnetic reader head should be high enough to decode the encoded character from F2F data format.

Magnetic emulator circuit with planar solenoid inductor (3.5mH) and 20mA driving current can generate a required peak-peak voltage, Fig. 6, at the reader head to decode the F2F data transmission.

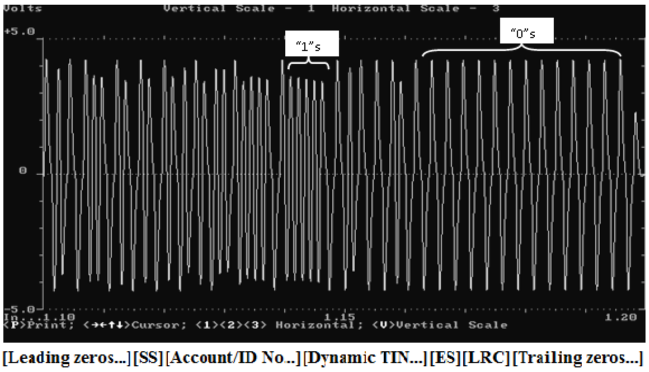
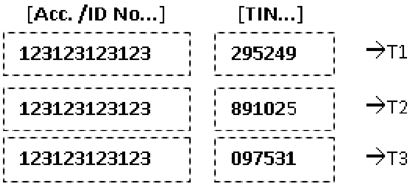

Volts
Vertical Scale - 1 Horizontal Scale - 3
+5.0
"1"s
"0"s
0
-5.0
In...1.10
1.15
1.20
<P>Print; <→←↑↓>Cursor; <1><2><3> Horizontal; <V>Vertical Scale
[Leading zeros...][SS][Account/ID No..][Dynamic TIN...][ES][LRC][Trailing zeros...]

Fig. 6. Mag3 magnetic stripe analyzer captures ETC magnetic emulator circuit output.

In order to enhance the security of the magnetic data transaction, the ETC takes an advantage of magnetic emulator/encoder to append the secret code or transaction identification number (TIN) to user information, account/ ID number, for every transaction. The secret code/TIN changes dynamically for every transaction, as in Fig. 7. The secure-chip or microprocessor at ETC generates TIN based on public/private key, counter, time, PIN, or equation. Upon receive, the issuer system decodes and verifies the TIN to authenticate the transaction.



[Acc. /ID No...]	[TIN...]	
123123123123	295249	→T1
123123123123	891025	→T2
123123123123	097531	→T3

Fig. 7. Transaction identification number (TIN) appended to acc/ID number changes at every transaction T1, T2 and T3

In addition, the ETC can incorporate additional modules such as secure-chip and RF-chip, Fig. 8, to facilitate smartcard contact (ISO/IEC-7816) and contactless (ISO/IEC-14443) interfaces.

IV. Security Enhanced Framework

In a classical electronic payment transaction system, the cardholder performs the transaction on the POS terminal at the merchant. Upon receive of transaction from merchant

POS terminal, the acquirer system connects to issuer system via domestic or international network in order to authorize and complete the transaction. Similarly, healthcare professionals/providers are equipped with POS terminals to enable authentication of patient information in healthcare system. In many cases, healthcare POS terminals support combination of healthcare and payment related transactions.

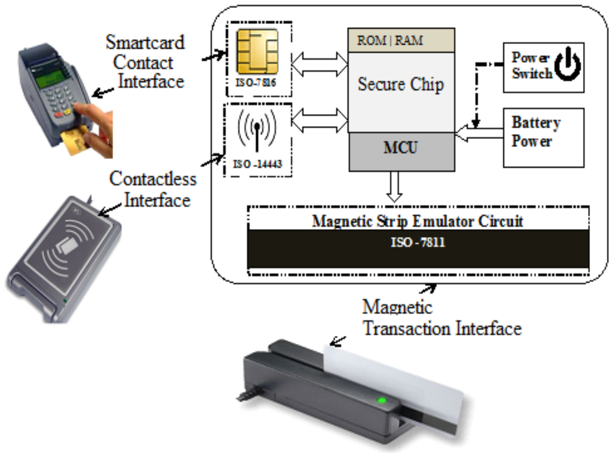


Fig. 8. Electronic transaction smartcard with multiple ISO/IEC interfaces

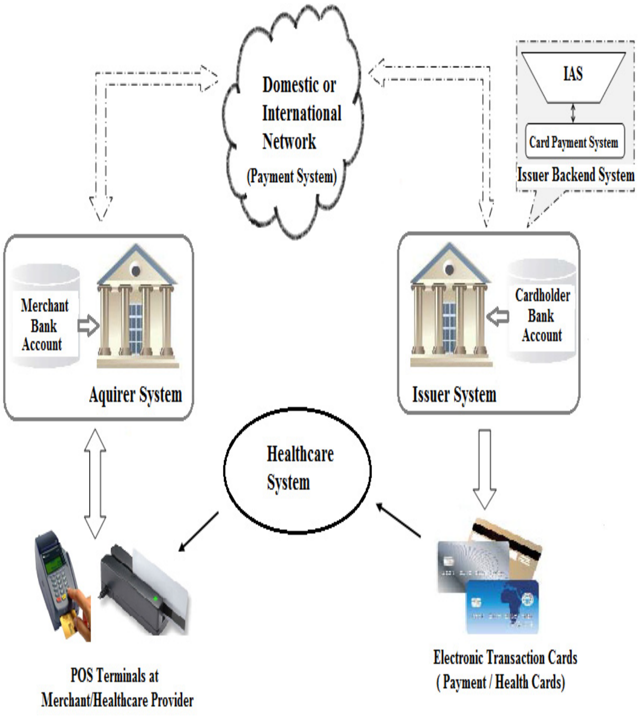


Fig. 9. Issuer authentication software (IAS) at card issuer backend system

Even though the POS terminals guarantee the security of transactions with an associated hardware and software security measures, the percentage of card fraud still remains at high level [13]. The proposed framework/ infrastructure, with an electronic transaction card (ETC) and an issuer authentication system (IAS) at the issuer backend system, enhances the security of magnetic data based transactions.

Secure Framework: The patented magnetic stripe emulator/encoder in ETC dynamically generates the magnetic data, in F2F format, when the card passes the reader head. This dynamic magnetic data incorporates cardholder's account number and encrypted transaction identification number (TIN) to secure the cardholder's information. The microprocessor uses cryptographic algorithms such as private or public key based encryption methods to generate the unique TIN for every new transaction [14]-[15].

In order to take advantage of the features offered by electronic transaction card, issuer authentication software (IAS) is integrated with issuer's existing card authorization mainframe backend system, as in Fig. 9. The host at issuer backend system invokes IAS to decode an encrypted transaction identification number (TIN) received from merchant's POS terminal/ATM to authenticate the transaction.

V. Conclusion

According to experts, it takes a very long time to replace all legacy point-of-sale terminals, which are based on magnetic stripe data transaction, in an existing market. The POS terminals at U.S. merchants, about 90%, are not EMV-complaint and more than 30% outside U.S. are yet to catch on. Card issuers are pushing for an evolution of plastic cards, credit/debit, where a single card can accommodate multiple accounts and multiple secured interfaces (ISO/IEC -7811, 7816, and 14443).

The electronic transaction card's novel feature of dynamic magnetic stripe, data disappear when the card is not being used, makes the card immune to fraud by skimming. The real time generation of magnetic data allows ETC to change the track data for each transaction. With all these features, the ETC achieves major benefits that cannot be matched by a traditional static magnetic stripe card: Secure the magnetic stripe data and support multiple accounts on a single plastic card. In addition, the ETC can incorporate secure-chip to facilitate smartcard contact (ISO/IEC-7816) and contactless (ISO/IEC-14443) interfaces. The electronic smartcard's dual capability makes a bridging technology to support both EMV- compliant as well as magnetic stripe transaction. Moreover, this kind of secure technology helps to avoid fraudulent activities such as counterfeit and identity theft in an electronic payment and healthcare systems.

References

[1] *International Organization for Standardization ISO/IEC*, 2008.

[2] D. Robertson. (November 2011). U.S. Leads the World in Credit Card Fraud. The Nilson Report. [Online]. Available: http://www.nilsonreport.com/pdf/news/112111.pdf

[3] H. Lakshmisha, S. Chan, and C. T. Lau, "Embedded Electronic Smartcard for Financial and Healthcare Information Transaction," *Journal of Advance in Computer* Networks *(JACN)*, vol. 1, no. 1, pp. 57-60, January 2013.

[4] H. Lakshmisha, W. C. Weng, L. Chang, and E. Foo, "Method for Broadcasting a Magnetic Stripe Data Packet from an Electronic Smart Card," U.S. Patent 8226001 B1, July 24, 2012.

[5] J. D. Mullen and B. Cloutier, "Payment Cards and Devices with Display, Chips, RFIDs, Magnetic Emulators, Magnetic Decoders, and Other Components," U.S. Patent 7784687 B2, August 31, 2010.

[6] E. Foo, J. Ziegler, Z. Alon, M. Poidomani, C. Guire, and L. Rouhthenstein, "Electronic Card and Methods for Making Same," U.S. Patent 7954724 B2, June 7, 2011.

[7] S. G. Narendra, P. Tadepalli, and T. N. Spitzer, "Electronic Transaction Card Powered by Mobile Device," U.S. Patent 7954716 B2, June 7, 2011.

[8] S. G. Narendra, P. Tadepalli, T. N. Spitzer, "Electronic Stripe Cards," U.S. Patent 7364092 B2, April 29, 2008.

[9] D. Robertson. (February 2012). EMV/Dynamic Stripe Combo Card. The Nilson Report. [Online]. Available: http://www.fiteq.com/pdf/FiTeq_Nilson_Report_Feb_2012.pdf

[10] K. Foster, E. Meijer, S. Schuh, and M. A. Zabek, "The 2009 Survey of Consumer Payment Choice," *Public Policy Discussion Paper*, Federal Reserve Bank of Boston, April 2011.

[11] European Central Bank. (July 2012). Report on card fraud. [Online]. Available: http://www.ecb.int/pub/pdf/other/cardfraudreport201207en.pdf

[12] ACI Payment Systems. (October 2012). Annual ACI Worldwide Global Fraud Report. [Online]. Available: http://www.aciworldwide.com/en/News-and-events/Press-releases/Annual-ACI-Worldwide-Global-Fraud-Report-Finds-One-in-Four-Consumers-Victims-of-Card-Fraud.aspx

[13] S. W. Inscoe. (October 2012). Global Consumer React to Rising Fraud. *Aite Group with ACI Worldwide Study*. [Online]. pp. 9-13. Available: http://www.aciworldwide.com/~/media/Files/Collateral/ACI_Aite_Global_Consumers_React_to_Rising_Fraud_1012

[14] H. Feistel, "Cryptography and Computer Privacy," *Scientific American*, vol. 228, no. 5, pp. 15-23, May 1973.

[15] W. Diffie and M. E. Hellman, "New Directions in Cryptography," in *Proc. IEEE Trans. Inform. Theory*, vol. 22, no.6, pp. 644-654, Nov. 1976.

Lakshmisha Honnegowda obtained B.Eng.(First Class with Distinction) degree from Visvesvaraya Technological University, India in 2003 and M.Sc. degree from the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore in 2006. He is currently pursuing Ph.D. degree from the School of Computer Engineering, Nanyang Technological University, Singapore. His research interests include computer vision, embedded systems and energy harvesting.

Chan Syin received her Bachelor Degree (First Class Honours) in Electrical Engineering from the National University of Singapore in 1987, and PhD in Computer Science from the University of Kent, United Kingdom in 1993. She is an Associate Professor at the School of Computer Engineering, Nanyang Technological University, Singapore. Her research interests include mobile healthcare applications and multimedia information systems.

Lau Chiew Tong received B.Eng. degree from Lakehead University in 1983 and M.A.Sc. and Ph.D. degrees in Electrical Engineering from the University of British Columbia in 1985 and 1990, respectively. He is currently an Associate Professor in the School of Computer Engineering, Nanyang Technological University, Singapore. His main research interests are in wireless communications.