Abstracts List of Electronic Cash Papers Collected

1991

Universal electronic cash

Filename:
printed

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Okamoto, Tatsuaki
Ohta, Kazuo

This paper proposes the first ideal untraceable electronic cash system which solves the most crucial problem inherent with real cash and all previous untraceable electronic cash systems. The main advantage of the new system is that the customer can subdivide his cash balance, C (dollars), into many pieces in any way he pleases intil the total of all subdivided pieces equeals C. This system can be implemented efficiently. In a typical implementation, the data size of one piece of electronic cash is less than 1-- bytes regardless of the face value of piece. The computation time for each transaction is several seconds, assuming the existance of a Rabin scheme chip. The security of this scheme relies on the difficulty of factoring.

1992

Achieving Electronic Privacy

Filename:
Achieving Electronic Privacy.htm

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Chaum, David

A cryptographic invention known as a blind signature permits numbers to serve as electronic cash or to replace conventional identification. The author hopes it may return control of personal information to the individual.

How to Break and Repair a "Provably Secure" Untraceable Payment System

Filename:
PfWa2_92DamgZsysCr91.ps

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Pfitzmann, Birgit
Waidner, Michael

On Crypto '88, an untraceable payment system with provable security against abuse by individuals was presented by Damgard. We show how to break the untraceability of that system completely.
Next, an improved version of the system is presented. We also augment the system by security for individuals against loss of money, and we introduce the possibility of receipts for payments. Finally, whereas all this concerned an on-line system, we present a similar construction for untraceable electronic cash.

Making Electronic Refunds Safer

Filename:
printed

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Hirschfeld, Rafael

We show how to break an electronic cash protocol due to van Antwerpen (a refinement of the system proposed by Chaum, Fiat, and Naor), and give an alternative protocol that fixes the problem.

Wallet databases with observers

Filename: printed

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Chaum, David
Pedersen, Torben P.

Previously there have been essentially only two models for computers that people can use to handle ordinary consumer transactions: (1) the tamper-proof module, such as a smart card, that the person connot modify or probe, and (2) the personal workstation whose inner working is totally under control of the individuals.
The first part of this article argues that a particular combination of these two kinds of mechanism can overcome the limitations of each alone, providing both security and correctness for organizations as well as privacy and even anonymity for individuals.
Then it is shown how this combined device, called a wallet, can carry a database containing personal information. The construction presented ensures that no single part of the device (i.e. neither the tamper-proof part nor the workstation) can learn the contents of the database - this information can only be recovered by the two parts together.

1993

An Efficient Off-line Electronic Cash System Based On The Representation Problem

Filename: cs-r9323.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Brands, Stefan A.

We present a new off-line electronic cash system based on a proble, called the representation problem, of which little use has been made in literature thus far. Our system is the first to be based entirely on discrete logarithms. Using the representation problem as a basic concept, some techniques are introduced that enable us to construct protocols for withdrawal and payment that do not use cut and choose methodology of earlier systems. As a consequence, our cash system is much more efficient in both computation and communication complexity than previously proposed systems.

Improved Privacy in Wallets with Observers

Filename: printed

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Cramer, Ronald
Pedersen, Torben P.

Wallets with observers were suggested by David Chaum and have previously been described in [Ch92] and [Cp92]. These papers argue that a particular combination of a tamper-resistant-unit and a small computer controlled by the user is very suitable as a personal device in consumer transaction systems. Using such devices, protocols are constructed that, simultaneously, achieve high levels of security for organizations and anonymity to users, under the assumption that the information stored by observers is never revealed to the outside world.
This paper extends [CP92] by defining additional requirements for the protocols which make it impossible to trace the behaviour of the individuals in the system if one is also alllowed to analyze a posterioiri the information observers can collect. We propose two protocols satisfying our requirements, thus achieving a higher degree of privacy for individuals. This extra level of privacy is obtained at essentially no cost as the new protocols have the same complexity as those previously proposed.

Single Term Off-Line Coins

Filename: printed

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Ferguson, Niels

We present a new construction for off-line electronic coins that is both far more efficient and much simpler than previous systems. Instead of using many terms, each for a single bit of challenge, our system uses a single term for a large number of possible challenges. The withdrawal protocol does not use a cut-and-choose methodology as with earlier system, but uses direct constructions.

Untraceable Off-line Cash in Wallets with Observers

Filename: brands93.ps

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Brands, Stefan A.

Incorporating the property of untraceability of payments into off-line electronic cash systems has turned out to be no easy matter. Two key concepts have been proposed in order to attain the same level of security against double-spending as can be trivially attained in systems with full traceability of payments.
The first of these, one-show blind signatures, ensures traceability of double-spenders after the fact. The realizations of this concept that have been proposed unfortunately require either a great sacrifice in efficiency or seem to have questionable security, if not both.
The second concept, wallets with observers, guarantees prior restraint of double-spending, while still offering traceability of double-spenders after the fact in case tamper-resistance is compromised. No realization of this concept has yet been proposed in literature, which is a serious problem. It seems that the known cash systems cannot be extended to this important setting without significantly worsening the problems related to efficiency and security.
We introduce a new primitive that we call restrictive blind signatures. In conjunction with the so-called representation problem in groups of prime order this gives rise to highly efficient off-line cash systems that can be extended at virtually no extra cost to wallets with observers under the most stringent of privacy requirements. The workload for the observer is so small that it can be performed by a tamper-resistant smart card capable of performing the Schnorr identification scheme.
We also introduce new extensions in functionality (unconditional protection against framing, anonymous accounts, multi-spendable coins) and improve some known constructions (computional protection against framing, electronic checks).
The security of our cash system and all its extensions can be derived directly from the security of two well-known digital signature schemes (Schnorr and Okamoto) and the security of the new primitive.

1994

Blind Signatures Based on the Discrete Logarithm Problem

Filename: blindsig.ps

☑ Ecash ☐ PaymentSystem ☐ Smartcard

Author
Camenish, Jan L.
Piveteau, Jean-Marc
Stadler, Markus A.

Blind signature schemes, an important cryptographic primitive, are useful in protocols that guarantee the anonymity of the participants. Two new blind signature schemes based on the discrete logarithm problem are presented.

Electronic Cash on the Internet

Filename: e-cash.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Brands, Stefan A.

It is generally realized that the Internet will not be able to offer full-fledged electronic marketplace capabilities without suitable electronic mechanism for processing payments. The electronic payment mechanism that is presented offers a variety of fetures that are believed to be particularly appealing in this respect.
To participate, an Internet user must interface to his computer a tamper-resistant device with an ordinary 8-bit processor, typically a PCMCIA card, and install some software. Internet service providers do not need special hardware. Payments can be made off-line and are untraceable and unlinkable. Multi-party security is guaranteed without parties having to trust other parties. Transaction processing speeds are such that even modestly equipped computers will be able to meet the performance levels required by demanding Internet payment applications. One particularly interesting such application is click-and-pay ability when travelling WWW.

Off-Line Cash Transfer by Smart Cards

Filename: cs-r9455

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Brands, Stefan A.

An off-line electronic cash system is presented that offers appreciably greater security and better privacy than currently considered electronic cash systems with similar functionality.
A tamper-resistant smart card, issued by the bank, controls a counter that represents the amount of electronic cash carried by the user. The use of a counter ensures that the computation and communication complexity for paying an amount are independent of the specific amount due, and that conversions between multiple currencies can be made at payment time. Smart cards can transfer electronic cash to POS terminals that need not be physically secured by the bank, without needing on-line verification.
To ensure privacy of payments, the user can insert his smart card into a user-controlled computer, such as a palm top computer or a personal computer, which acts as an intermediary between the smart card and the other party involved in the transaction. Cryptographic software in the user-controlled computer ensures that payments are information-theoretically untraceable and unlinkable.
To pay any specified amount, only 125.5 bytes of data must be transferred, and no on-line computation is required. The dynamic storage requirements per payment can be compressed to a mere 26.5 bytes for the user-controlled computer, and virtually none for the smart card. The smart card can be a smart card capable of performing the well-known Schnorr signature scheme; minor additions to the smart-card code suffice to suit the cash system requirements. Moreover, a simple optimization allows efficient implementation even when widely available smart cards with ordinary 8-bit micro-processors are used. Assuming that the tamper-resistance of the smart cards cannot be broken, the system is provably as hard to break as the Schnorr signature scheme. A build-in mechanism for traceability of double-spent transaction data, which is as hard to break as the blinded Schnorr signature scheme, ensures that the cost of breaking a smart card in practice will significantly exceed the expected financial profit that the attacker can make from this.

On-Line/Off-Line Digital Signatures

Filename: egm.ps

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Goldreich, Oded
Even, Shimon
Micali, Silvio

A new type of signature scheme is proposed. It consists of two phases. The first phase is performed off-line, before the message to be signed is even known. The second on-line phase is performed once the message to be signed is known, and is supposed to be very fast. A method for constructing such on-line/off-line signature schemes is presented. The method uses one-time signature schemes, which are very fast, for the on-line signing. An ordinary signature scheme is used for the off-line stage.
In a practical implementation of our scheme, we use a variant of Rabin's signature scheme (based on factoring) and DES. In the on-line phase, all we use is a moderate amount of DES computation and a single modular multiplication. We stress that the costly modular exponentiation operation is performed off-line. This implementation is ideally suited for electronic wallets or smart cards.

Single-Term Divisible Electronic Coins

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Okamoto, Tatsuaki
Eng, Tony

In the literature, only one 'divisible' off-line electronic cash scheme has been presented [OO91]. In this paper, we present the construction of more efficient 'divisible' off-line electronic coin schemes that are 'single-term'. We examine come coin systems based on the 'disposible authentication' paradigm [OO89], and show that a specific type of 'disposable authenticated' coin system can be extended to handle divisible coins using our techniques.

The ESPRIT Project CAFÉ: High Security Digital Payment Systems

Filename:

BBCM1_94CafeEsorics.ps

☑ Ecash ☑ PaymentSystem

☑ Smartcard

Author
Waidner, Michael
Schunter, Matthias
Pfitzmann, Birgit
Boly, Jean-Paul
Bosselaers, Antoon
Cramer, Ronald
Pedersen, Torben P.

CAFÉ (Conditional Access for Europe) is an ongoing project in the European Community ESPRIT program. The goal of CAFÉ is to develop innovative systems for conditional access, and in particular, digital payment systems. An important aspect of CAFÉ is high security of all parties concerned, with the least possible requirements that they are forced to trust other parties (so called multi-party security). This should give legal certainity to everybody at all times. Moreover, both the electronic money issuer and the individual users are less dependent on the tamper-resistance of devices than in usual digital payment systems. Since CAFÉ aims at the market of small everyday payments that is currently dominated by cash, payments are offline, and privacy is an important issue.
The basic devices used in CAFÉ are called electronic wallets, whose outlook is quite similar to pocket calculators or PDAs. Paricular advantages of the electronic wallets are that PIN can be entered directly, so that fake-terminal attacks are prevented. Other features are: loss tolerance (if a user loses an electronic wallet, or the wallet breaks or is stolen, the user can be given the money back, although it is a prepaid payment system.
The aim is to demonstrate a set of the systems developed in one or more field trials at the end of the project. Note that these will be real hardware systems, suitable for mass production. This paper concentrates on the basic techniques in the CAFÉ protocol.

Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Chan

Filename:

f11.ps

☑ Ecash ☑ PaymentSystem

☐ Smartcard

Author
Brickell, Ernie
Gemmell, Peter
Kravitz, David

While unconditionally anonymous electronic cash systems have been proposed in the literature, governmental and financial institutions are unwilling to back a completely
anonymous system. Instead, they have proposed systems with little or no protection for the users' privacy. Their reasons for opposing complete untraceability have to do with the containment of user fraud and the desire to restrict the new kinds of crime that unrestricted remotely withdrawable and spendable electronic cash could facilitate.
We introduce the first electronic cash systems which incorporate trustee-based tracing but otherwise provably protect user anonymity. We expand on the provably anonymous electronic cash systems of [B93] and [FY92]. Our systems maintain the previous papers' complete provable user anonymity except that, only with the cooperation of several publicly appointed trustees (key-escrow agents), the government can trace a user's spending with certainty, determining to whom the user gave his/her money and how much s/he gave. The trustees can answer the question of whether a particular payment was made by a particular user, without revealing any additional information. This allows for authorized forward and backward tracing that does not impinge on the privacy of anyone other than the parties of the one transaction in question. The trustee-based tracing requires no tamper-resistant hardware and can be implemented as either on-line or off-line systems.
For those concerned about the trustability of the trustees, we describe how a mutually distrustful government and user can construct an electronic trustee, a device which can be used in place of (or in addition to) ordinary human trustees. This device, which does use tamper-resistant and tamper-detecting hardware, automatically alerts the user in case his/her secret stored by the trustee is released or compromised.
Furthermore, we introduce an on-line anonymous change-making protocol that is independent of trustee-based tracing. This protocol addresses a major stumbling block for anonymous cash systems: how a user can make an anonymous purchase at a store when the user does not have correct change. We are able to provide exact, perfectly anonymous change, assuming a line of communication with a coin-minting facility. There is no need to determine on-line that the user's coins have not been spent before.

1995

An Efficient Divisible Electronic Cash Scheme

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Okamoto, Tatsuaki

Recently, several 'divisible' untraceable off-line electronic cash schemes have been presented. This paper presents the first practical divisible untraceable off-line cash scheme that is 'single-term' in which every procedure can be executed in the order of log N, where N is the precision of divisibility, i.e., N=(the total coin value)/(minimum divisible unit value). Therefore, our 'divisible' off-line cash scheme is more efficient and practical than the previous schemes. For example, when N=2^17 (e.g., the total value is about $1000, and the minimum divisible unit is 1 cent), our scheme requires only about 1 Kbyte of data be transferred from a customer to a shop for a payment and about 20 modular exponentiations for one payment, while all previous divisible cash schemes require more than several Kbytes of transferred data and more than 200 modular exponentiations for one payment.
In addition, we prove the security of the proposed cash scheme under some cryptographic assumptions. Our scheme is the first "practical divisible" untraceable off-line cash scheme whose cryptographic security assumptions are theoritically clarified.

Erratum to CS-R9534

Filename: CS-R9534_erratum.htm

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Brands, Stefan A.

Erratum to Brand's e-cash.

Fair Blind Signatures

Filename: FairBlindSignatures.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Stadler, Markus A.
Piveteau, Jean-Marc
Camenish, Jan L.

A blind signature scheme is a protocol for obtaining a signature from a signer such that the signer's view of the protocol cannot be linked to the resulting message-signature pair. Blind signature schemes are used in anonymous digital payment systems. Since the existing proposals of blind signature schemes provide perfect unlinkability, such payment systems could be misused by criminals, e.g. to safely obtain a ransom or to launder money. In this paper, a new type of blind signature schemes called fair blind signature schemes is proposed. Such schemes have the additional property that a trusted entity can deliver information allowing the signer to link his view of the protocol and the message-signature pair. Two types of fair blind signature schemes are distinguished and several realizations are presented.

How to Break Another "Provably Secure" Payment System

Filename: PfSW_95adAmCr.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Pfitzmann, Birgit
Schunter, Matthias
Waidner, Michael

At Eurocrypt '94, Stefano D'Amiano and Giovanni Di Crescenzo presented a protocol for untraceable electronic cash based on non-interactive zero-knowledge proofs of knowledge with preprocessing. It was supposed to be provably secure given this and a few other general cryptographic tools.
We show that this protocol nevertheless does not provide any untraceability and has some further weaknesses. We also break another ``provably secure'' system proposed by Di Crescenzo at CIAC 94.
This is the second case of problems with 'provably secure' payment systems. Moreover, yet another system with this name tacitly solves a much weaker problem than the seminal paper by Chaum, Fiat, and Naor and most other 'practical' papers in this field (de Santis and Persiano, STACS 92). We therefore identify some principal problems with definitions and proofs of such schemes, and sketch better ways to handle them.

News from CAFÉ, June 1995

Filename: ScWe_95.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Schunter, Matthias

News on CAFÉ, April 1995

Filename: PfWe_95CAFE.Oakland.ps

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Pfitzmann, Birgit

Off-line electronic cash based on secret key certificates

Filename: cs-r9506.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Brands, Stefan A.

An off-line electronic coin system is presented that offers multi-party security and unconditional privacy of payments. The system improves significantly on the efficiency of the previously most efficient such system known in the literature, due to application of a recently proposed technique called secret-key certificates.
By definition of secret-key certificates, pairs consisting of a public key and a matching certificate can be simulated with indistinguishable probability distribution. This allows a variety of polynomial-time reductions from a well-known signature scheme to the cash system. In particular, the withdrawal protocol can be proved to be restrictive blind with respect to one account holder, relying only on a standard intractability assumption; no such result has been proved before in the literature.
Another consequence of the application of the secret-key certificate technique is that the withdrawal protocol is not a blind signature issuing protocol. This falsifies the popular belief that efficient privacy-protecting off-line electronic cash systems must be based on withdrawal protocols that are blind signature issuing protocols.

Ripping Coins for Fair Exchange

Filename: rip.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Jakobsson, Markus

A fair exchange of payments for goods and services is a barter where one of the parties cannot obtain the item desired without handing over the item he offered. We introduce the concept of ripping digital coins to solve fairness problems in payment transactions. We demonstrate how to implement coin ripping for a recently proposed payment scheme [9, 8], giving a practical and transparent coin ripping scheme. We then give a general solution that can be used in any payment scheme with a challenge. We also indicate how fairness can be obtained by building a contract into the coin.

1996

Digital Payment Systems with Passive Anonymity-Revoking Trustees

Filename: Dig_Pay_Trustees.ps (ea) & jcs.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Camenish, Jan L.
Maurer, Ueli
Stadler, Markus A.

Anonymity of the participants is an important requirement for some applications in electronic commerce, in particular for payment systems. Because anonymity could be in conflict with law enforcement, for instance in cases of blackmailing or money laundering, it has been proposed to design systems in which a trustee or a set of trustees can selectively revoke the anonymity of the participants involved in suspicious transactions. From an operational point of view, it can be an important requirement that such trustees are neither involved in payment transactions nor in the opening of an account, but only in case of a justified suspicion. In this paper we propose the first efficient anonymous digital payment systems satisfying this requirement. The described basic protocol for anonymity revocation can be used in on-line or off-line payment systems.

Revokeable and Versatile Electronic Money

Filename:

revoke.ps

☑ Ecash ☑ PaymentSystem

☐ Smartcard

Author
Jakobsson, Markus
Yung, Moti

We present an e-money system where both value of funds and user anonymity can be revoked or suspended unconditionally, but only by the cooperation of banks and consumer rights organizations. We introduce the ultimate crime, where an active attacker gets the bank's key or forces the bank to give 'unmarked bank notes'. Our system, unlike all current anonymous systems, can prevent such a crime from successfully being perpetrated, and employs revocation to do so.
The mechanisms introduced to balance the need for anonymity against the need to be able to revoke it, together with the notion of challenge semantics that we introduce, provide us with a very versatile system, a second important goal of our investigation. The proposed scheme is efficient and easily extends the basic needs of a practical payment scheme to allow for coin divisibility, checks, credit card purchases and surety bonds. Moreover, the system (unlike some previous ones) is robust against problems arising from spurious equipment.

1997

An efficient micropayment system based on probabilistic polling

Filename:

polling.pdf

☑ Ecash ☑ PaymentSystem

☑ Smartcard

Author
Odlyzko, Andrew
Jareki, Stanislaw

Existing software proposals for electronic payments can be divided into "on-line" schemes that require participation of a trusted party (the bank) in every transaction and are secure against overspending, and the "off-line" schemes that do not require a third party and guarantee only that overspending is detected when vendors submit their transaction records to the bank (usually at the end of the day).
We propose a new hybrid scheme that combines the advantages of both of the above traditional design strategies. It allows for control of overspending at a cost of only a modest increase in communication compared to the off-line schemes. Our protocol is based on probabilistic polling. During each transaction, with some small probability, the vendor forwards information about this transaction to the bank. This enables the bank to maintain an accurate approximation of a customer’s spending. The frequency of polling messages is related to the monetary value of transactions and the amount of overspending the bank is willing to risk.
The probabilistic polling model creates a natural spectrum bridging the existing on-line and off-line electronic commerce models. For transactions of high monetary value, the cost of polling approaches that of the on-line schemes, but for micropay-ments, the cost of polling is a small increase over the traffic incurred by the off-line schemes.

Anonymity Control in E-Cash Systems

Filename:

WI.ps

☑ Ecash ☑ PaymentSystem

☐ Smartcard

Author
Frankel, Yair
Tsiounis, Yiannis
Yung, Moti
Davida, George

Electronic cash, and other cryptographic payment systems, offer some level of user anonymity during a purchase, in order to emulate electronically the properties of physical cash exchange. However, it has been noted that there are crime-prevention situations where anonymity of notes is undesirable; in addition there may be regulatory and legal constraints limiting anonymous transfer of funds. Thus pure anonymity to users may be, in certain settings, unacceptable and thus a hurdle to the progress of electronic commerce.
The conceptual contribution of this work is based on the claim that given the legal, social, technical and efficiency constraints that are imposed, anonymity should be treated as a Control Parameter facilitating flexibility of the level of privacy of note holders (determined by the dynamic conditions and constraints). We review ``anonymity control'' which provides the balance between strong anonymity for the user and anonymity revocation for crime prevention and legal compliance. In light of this parameterization, we review recently developed technical tools for tracing and anonymity revocation (e.g., owner tracing and coin tracing). We elaborate on the differences in the various technologies with respect to security assumptions and we discuss practical considerations of computational, bandwidth and storage requirements for user, shop, bank and trustees as well as whether the trustees must be on-line or off-line.
We also claim that while anonymity revocation can potentially reduce crime it can also produce instances where the severity of the crime is increased as criminals try to social engineer around tracing revocation. To prevent this we suggest the notion of ``distress cash,'' a way to activate law enforcement tracing in an un-noticeable fashion. On the technical side, we provide efficiency improvements to a protocol for coin tracing and point at a technical solution for distress cash.

Anonymous Fingerprinting

Filename:

PfWa1_97AnoFing.ps

☑ Ecash ☑ PaymentSystem

☐ Smartcard

Author
Pfitzmann, Birgit
Waidner, Michael

Fingerprinting schemes deter people from illegally redistributing digital data by enabling the original merchant of the data to identify the original buyer of a redistributed copy.
Recently, asymmetric fingerprinting schemes were introduced. Here, only the buyer knows the fingerprinted copy after a sale, and if the merchant finds this copy somewhere, he obtains a proof that it was the copy of this particular buyer.
A problem with all previous fingerprinting schemes arises in the context of electronic marketplaces where untraceable electronic cash offers buyers privacy similar to that when buying books or music in normal shops with normal cash. Now buyers would have to identify themselves solely for the purpose of fingerprinting. To remedy this, we introduce and construct anonymous asymmetric fingerprinting schemes, where buyers can buy information anonymously, but can nevertheless be identified if they redistribute this information illegally.
A subresult of independent interest is an asymmetric fingerprinting protocol with reasonable collusion tolerance and 2-party trials, which have several practical advantages over the previous 3-party trials. Our results can also be applied to so-called traitor tracing, the equivalent of fingerprinting for broadcast encryption.

Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System

Filename: revoke2.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Jakobsson, Markus
Yung, Moti

Due to business relationships, alliances, trust, and distribution of liability, distribution of power is an important issue in financial systems. At the same time as the security of the scheme is strengthened by this decentralization, the perception of the security is also strengthened, which is important from a business point of view. Furthermore, apart from increasing the security, client trust and availability of the system, distribution of power can also increase its functionality, as we demonstrate.

We suggest an anti-trust mechanism, namely, a method for distribution of the centralized parties into many modules (potentially controlled by different entities), and apply it to a versatile electronic-money system.

The method diffuses a task into distributed modules using recent cryptographic technology; doing so, it achieves increased security, privacy, availability and functionality without introducing any noticeable disadvantage. It uses Magic Ink Signatures [29], which are blind signatures that are distributedly generated using a threshold of signers, and where signatures can always be unblinded using (perhaps another) threshold of signers as well. Furthermore, we combine this with recent proactive technology, which enables a stronger adversarial setting. We also suggest techniques for reorganization of data stored and used by various functions, employing secure repository.

The result is an electronic money system that allows user anonymity and its revocation (a notion recently advocated by some works so as to prevent potential criminal actions.) The control over revoking anonymity is given to distributed modules that control a hidden alarm channel. As part of the task diffusion we find ways to simplify and reduce the overall complexity of the system. The revocation ability and distribution of the trust are efficient and allow a large degree of versatility in the functionality of the system (change mechanisms, numerous financial instruments: cash, charge, check, micro-payments, etc.).

Efficient Electronic Cash with Restricted Privacy

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Radu, Cristian
Govaerts, Rene
Vandlewalle, Joos

In this paper we propose a coin-based electronic payment system suitable for small payments. It is derived from Brands' scheme presented at Crypto'93, in the sense that the coins are built using the representation problem. The main contribution of our solution consists of the speedup of the withdrawal protocol. The gain of efficiency is achieved preserving the same level of integrity for user, shop and bank. A coin remains untracable with respect to the user. This feature is fulfilled even if one assumes that the bank has unlimited computing power and colludes with shops in order to trace a coin to a specific user. However, a set of coins are linkable to a pseudonym of the user, restricting in this way his privacy. This drawback can be limited by 'rotating' coins derived from different pseudonyms in a set of consecutive payment transactions.

Efficient Electronic Cash: New Notions and Techniques

Filename: thesis.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Tsiounis, Yiannis

We provide what appear to be the two major missing links towards practical implementation of anonymous off-line electronic cash schemes, namely capability for exact payments and control of user anonymity.
We investigate both conceivable approaches towards exact payments: (a) withdrawing multiple coins of various denominations and (b) providing for coin divisibility. We present a provably optimal algorithm for maintaining multiple coins, while we improve existing results in divisible electronic cash by three orders of magnitude. We furthermore analyze the applicability of each method depending on system parameters, to conclude that our divisible approach is more efficient when a large budget and/or great precision of payments is required; the opposite is true for our multiple coin scheme.
To control user anonymity we present two modular additions that allow for tracing of malicious users by an assigned set of trusted parties (trustees), while limiting the trustees' involvement to one decryption operation per tracing request. We show how our additions can be applied to a simple token-based scheme as well as our divisible schemes, resulting into efficient and secure fair divisible electronic cash.
Throughout this thesis we focus on both efficiency and provable security of the proposed systems. We aim to provide schemes that can be applied in current smart-cards without sacrificing security. We thus provide proofs for our protocols, based on a formal security model. In the course we make some technical and theoretical contributions which enhance our understanding of electronic cash protocols.

Efficient Scalable Fair Cash with Off-line Extortion Prevention

Filename: CashSystem.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Poupard, Guillaume
Petersen, Holger

Since the invention of blind signatures in 1982 by David Chaum, there have been many proposals to realize anonymous electronic cash using this mechanism. Although these systems offer high privacy to the users, they have the disadvantage that the anonymity might be misused by criminals in order to commit a perfect crime (without being physically present, and thus with the assurance of not being caught). The recent research focuses therefore on the realization of fair electronic cash systems where the anonymity of the coins is revocable by a trustee in the case of fraudulent users. In this paper, we describe the main characteristics of these systems and give a comparison of existing ones. The analysis allows us to propose a new efficient fair cash system which offers scalable security with respect to its efficiency.
Our system is the first that prevents extortion attacks, like blackmailing or the use of blindfolding protocols under off-line payments and with the involvement of the trustee only at registration of the users. We give two applications, a highly secure one employing provable secure signature schemes for internet payments and a very efficient one for electronic purse realization.

Electronic Cash - Technology Will Denationalise Money

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Birch, David G.W.
McEvoy, Neil A.

Emerging technologies, particularly the synthesis of cryptographic software and tamper-resistant smart card hardware into the electronic purse, will make the cost of entry into the currency issuing 'market' quite small. Many organizations may then wish to enter this market, for example as a means of supplying credit (as envisaged by Frederick Hayek), of raising finance, or of encouraging customer loyalty (explorated by Edward de Bono). Whereas the world's currencies are currently organized in territorial lines, we must foresee a future in which currencies occupy (overlapping) niches according to the 'virtual', as well as geographic, communitites to which people belong and a vigorous 'foreign' exchange market where people (or, more likely, their PCs) trade these currencies. Just a couple of years ago, the concept of electronic cash was unknown to the mass market, but soom it will be taken for granted and will be as widespread as credit cards and chequebooks are today - and the ramification of such a widespread deployment deserve serious examination and debate.

Electronic Lottery Tickets as Micropayments

Filename: lottery.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Rivest, Ronald L.

We present a new micropayment scheme based on the use of 'electronic lottery tickets'. This scheme is exceptionally efficient since the bank handles only winning tickets, instead of handling each micro-payment. Electronic lottery tickets are the first payment scheme in which the bank does not have to process each payment.

Electronic Money: It's Impact On Retail Banking & Electronic Commerce

Filename: hitachi*.htm

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Ada penjelasan Mondex, VisaCash, dsb. Lumayan untuk smartcard.

Evaluating the Security of Electronic Money

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Lelieveldt, Simon L.

After defining electronic money it is explained that the Dutch policy stance with respect to electronic money is that issuing value is seen to be equivalent to deposit taking and therefore subject to supervision. As a result the Dutch central bank actively monitors developments with respect to electronic money and reviews the schemes under the rules of the supervision law. The most important findings of the BIS-report on security of electronic money are summarized and an ovierview is given of issues that could be studied as a part of the review of an electronic money schemes.

Indirect Discourse Proofs: Achieving Efficient Fair Off-Line E-Cash

Filename: folc.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Frankel, Yair
Tsiounis, Yiannis
Yung, Moti

Cryptography has been instrumental in reducing the involvement of over-head third parties in protocols. For example; a digital signature scheme assures a recipient that a judge who is not present at message transmission will nevertheless approve the validity of the signature. Similarly, in off-line electronic cash the bank (which is off-line during a purchase) is assured that if a user double spends he will be traced.
Here we suggest the notion of Indirect Discourse Proofs with which one can prove indirectly yet efficiently that a third party has a certain future capability (i.e., assure Trustees can trace). The efficient proofs presented here employ algebraic properties of exponentiation (or functions of similar homomorphic nature).
Employing this idea we present the concept of ``Fair Off-Line e-Cash'' (FOLC) system which enables tracing protocols for identifying either the coin or its owner. Recently, the need to trace and identify coins with owners/withdrawals was identified (to avoid blackmailing and money laundering). Previous solutions that assured this traceability (called fair e-cash as they balance the need for anonymity and the prevention of criminal activities) involved third parties at money withdrawals. In contrast, FOLC keeps any third party uninvolved, thus it is ``fully off-line e-cash'' even when law enforcement is added (i.e., it is off-line w.r.t. law enforcement at withdrawals and off-line w.r.t. the bank at payments).

Micro-Digital Money for Electronic Commerce

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Nguyen, Khanh Quoc
Mu, Yi
Varadharajan, Vijay

This paper proposes two novel cash based micropayment schemes based on a new technique. Both schemes support divisibility and transferability of digital coins in asimpler way compared to the existing solutions. The basic scheme allows full or partial use of a coin chain in a transaction; if only part of a coin chain has been used with one vendor, the rest of the chain can be used for instance in a subsequent transaction with another vendor. The modified scheme extend this to multiple chains making the scheme particularly suitable for a large number of micropayment transactions.

Mis-representation of Identities in E-cash Schemes and how to Prevent it

Filename: misr.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Chan, Agnes
Frankel, Yair
Tsiounis, Yiannis

In Crypto '93, S. Brands presented a very efficient off-line electronic cash scheme based on the representation problem in groups of prime order. In Crypto '95 a very efficient off-line divisible e-cash scheme based on factoring Williams integers was presented by T. Okamoto. We demonstrate one efficient attack on Okamoto's scheme and two on Brands' scheme which allow users to mis-represent their identities and double spend in an undetectable manner, hence defeating the most essential security aspect of the schemes. The attack on Brands' scheme (which we suspect, given his previous related results, was an inadvertent omission) is also applicable to T. Eng and T. Okamoto's divisible e-cash scheme (presented in Eurocrypt '94) which uses Brands' protocols as a building block.
We present an efficient modular fix which is applicable to any use of the Brands' idea, and we discuss how to counteract the attack on Okamoto's scheme. Hence the original results remain significant contributions to electronic cash.

On the Continum Between On-line and Off-line E-cash Systems - I

Filename: printed

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Yacobi, Yacov

Electronic cash systems for small transactions are discussed, with the functionality goal of minimizing involvment of third parties in transactions between users. To this end the potential role of randomized audit mechanisms is discussed. A continuum exist between the extermes of totally on-line and totally off-line payment systems, and there exist business motivations to establishing an intermediate 'working point'.
Our security goal is to protect the systems against economically motivated adversaries. Let the adversarial expenses (to interfere with normal operation of wallets) be Cb, and 1/d be the audit sampling rate, and for simplicity assume each payment has a value of one unit. Then when the adversarial payer breaks even with her investment, Cb, the probability not to detect her is O(exp(-Cb/d)).
A curious observation on the so called "after the fact double-spender exposure" mechanisms unexpecedly falls from the analysis of randomized audit mechanisms.

Privacy vs. Authenticity

Filename: thesis.jakobsson.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Jakobsson, Markus

Thesisnya Jakobsson pasti bagus banget.

Secure and Efficient Digital Coins

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Nguyen, Khanh Quoc
Mu, Yi
Varadharajan, Vijay

Current off-line electronic cash systems require a great number of complex online computations by clients during the payment phase. In this paper, we propose a new off-line anonymous cash scheme that greatly reduces the number of online computations that need to be done by the clients for each payment transaction. In particular, except for the first coin in a transaction, the client only needs to perform minimal computations for the remaining coins in the transaction. Our scheme also provides unconditional client anonymity and is able to detect double spending and is resistant to coin forgery and framing attacks.

Security of Blind Digital Signatures

Filename:

crypto97-blind.ps

☑ Ecash ☑ PaymentSystem

☐ Smartcard

Author
Juels, Ari
Luby, Michael
Ostrovsky, Rafail

Blind digital signatures were introduced by Chaum. In this paper, we show how security and blindness propoerties for blind digital signatures, can be simultaneously defined and satisfied, assuming an arbitrary one-way trapdoor permutation family. Thus, this paper presents the first complexity-based proof of security for digital signatures.

Some Critical Remarks on "Dynamic Data Authentication" as Specified in EMV '96

Filename:

printed

☐ Ecash ☑ PaymentSystem

☑ Smartcard

Author
Guillou, Louis Claude

Every banking card will soon include an electronic chip and, after a transitional period, the magnetic stripe will dissapear. For ensuring a world wide interchange, Europay International S.A., MasterCard and Visa have been cooperation for the last three years in the production of the so-called EMV specification; the latest release specifies a method for dynamic data authentication. We analyzed that method is highly questionable. We propose an alternate method which eliminates the detected problems while offering significant benefits at system level.

Strong Loss Tolerance of Electronic Coin Systems

Filename:

p194-pfitzman.pdf

☑ Ecash ☑ PaymentSystem

☐ Smartcard

Author
Pfitzmann, Birgit
Waidner, Michael

Untraceable electronic cash means prepaid digital payment systems, usually with offline payments, that protect user privacy. Such systems have recently been given considerable attention by both theory and development projects. However, in most current schemes, loss of a user device containing electronic cash implies a loss of money, just as with real cash. In comparison with credit schemes, this is considered a serious shortcoming. This article shows how untraceable electronic cash can be made loss tolerant, i.e., how the monetary value of the lost data can be recovered. Security against fraud and preservation of privacy are ensured; strong loss tolerance means that not even denial of recovery is possible. In particular, systems based on electronic coins are treated. We present general design principles and options and their instantiation in one concrete payment system. The measures are practical.

SVP: A Flexible Micropayment Scheme

Filename:

printed

☑ Ecash ☑ PaymentSystem

☐ Smartcard

Author
Stern, Jacques

We propose a cheap micropayment scheme based on reasonable request. It can be used for anypayment which is online beteween customer and the vendor, and offline with the broker. It is flexible in the sense that many security options are possible depending on the policy of the involved participants. We avoid large data storage, heavy computations. The scheme is software based for customer and hardware based for the vendor. Possibilities of having software-based solution for both are also presented.

Towards Multiple-Payment Schemes for Digital Money

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Pagina, H.
Jansen, R.

Recently, many payment schemes for digital money have been proposed. In most of these schemes money can be spent only once and must then immediately be returned to the bank. The purpose of this paper is to show the advantages of a scheme which allows the recipient of the money to use it directly for further purchases. We discuss why most existing schemes do not support such a payment scheme and make a proposal of how to overcome this drawback. Furthermore, we address the problem of achieving a fair exchange of money against service between the customer and the vendor. Few solutions to this problem have been published and all involve a trusted third party which actively supports the exchange. Using such a trustee has the disadvantage that - for high transaction rates - he easily constitutes a bottleneck. We present an alternative solution based on a 'passive' trustee thereby avoiding the former disadvantage.

1998

A More Efficient Untraceable E-Cash System with Partially Blind Signatures Based on the Di

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Miyazaki, Shingo
Sakurai, Kouichi

We propose a new untraceable electronic money system based on the discrete logarithm problem. Our system improves the efficiency of Yacobi's E-money system by making the applied blind signature 'partial'. We compare our system to the previous e-money systems which use the El-Gamal-type scheme in their tracing a double spender.
We also remark a double-registration problem on a digital caash system, recently presenteed by Nguyen, Mu & Varadharajan, based on the blind Nyberg-Rueppel signature.

A Platform of Privately Defined Currencies, Loyalty Credits, and Play Money

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Maher, David P.

We use techniques from financial cryptography to define new electronic currencies that are suitable for many applications. We use a platform approach to allow a single, world wide infrastructure to support a practically unlimited number of new currencies. The platform permits new currencies to be defined with little effort, and allows an individual to effectively manage and use perhaps a few dozen of those currencies that he finds personally useful. We describe the structures and mechanisms of the platform, various applications, and the risks associated with its use.

An Efficient Fair Off-Line Electronic Cash System with Extensions to Checks and Wallets wit

Filename: printed

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
de Solages, Aymeric
Traore, Jacques

In this paper, we present a privacy-protecting off-line electronic cash system which is fair, that is, the transactions are (potentially) traceable by a trusted authority bu anonymous otherwise. Our scheme, based on a modification of Brand's restrictive blind signature scheme [2], is significantly more efficient thant of Frankel, Tsiounis & Yung's [11], while offering the same functionalities (off-line trusted authority, direct identification of the coin owner when the tracing of a user from his coin is performed by the trusted authority).
Furthermore, we show how to extend our system to wallets with observers [9] and to electronic checks [1, 2, 15]. These two extensions are more efficient than previous ones [2, 6]. The first extension is featured by a high computational efficiency and low storage requirements for observers. The second extension provides checks which are more efficiently computed than checks in [2] (twice as fast) and which also require less memory for their storage (half as much).

Assesment of Threats for Smart Card based Electronic Cash

Filename: printed

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Ezawa, Kazuo J.

The security of smart card based electronic cash have been receiving significant attention recently. However, there has been little systematic analysis or qualification of the impact of the security break on the smart card based electronic cash economy. This paper discusses the assessment of threats in two phaaases using two different methodologies. The first is the assessment of overall therat using the business system analysis model called 'value chain' - the methodology to evaluate the activities necessary to achieve the final objectives of the counterfeiting organization. It is a qualitative method. The second is the quantification of such a threat using micro dynamic simulation.

Breaking Up Is Hard To Do: Modeling Security Threats for Smart Cards

Filename: smart-card-threats.pdf

☐ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Schneier, Bruce
Shostack, Adam

Smart card systems differ from conventional computer systems in that different aspects of the system are not under a single trust boundary. The processor, I/O, data, programs, and network may be controlled by different, and hostile, parties. We discuss the security ramifcations of these "splits" in trust, showing that they are fundamental to a proper understanding of the security of systems that include smart cards.

Distributed "Magic Ink" Signatures

Filename: magic.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Jakobsson, Markus
Yung, Moti

The physical analog of ``blind signatures'' of Chaum is a document and a carbon paper put into an envelope, allowing the signer to transfer his signature onto the document by signing on the envelope, and without opening it. Only the receiver can present the signed document while the signer cannot ``unblind'' its signature and get the document signed.
When an authority signs ``access tokens'', ``electronic coins'', ``credentials'' or ``passports'', it makes sense to assume that whereas the users can typically enjoy the disassociation of the blindly signed token and the token itself (i.e. anonymity and privacy), there may be cases which require ``unblinding'' of a signature by the signing authority itself (to establish what is known as ``audit trail'' and to ``revoke anonymity'' in case of criminal activity).
This leads us to consider a new notion of signature with the following physical parallel: The signer places a piece of paper with a carbon paper on top in an envelope as before (but the document on the paper is not yet written). The receiver then writes the document on the envelope using magic ink, e.g., ink that is only visible after being ``developed''. Due to
the carbon copy, this results in the document being written in visible ink on the internal paper. Then, the signer signs the envelope (so its signature on the document is made available). The receiver gets the internal paper and the signer retains the envelope with the magic ink copy. Should the signer need to unblind the document, he can develop the magic ink and get the document copy on the envelope. Note that the signing is not blinded forever to the signer. We call this new type of signature a magic ink signature.
We present an efficient method for distributively generating magic ink signatures, requiring a quorum of servers to produce a signature and a (possibly different) quorum to unblind a signature. The scheme is robust, and the unblinding is guaranteed to work even if a set of up to a threshold of signers refuses to cooperate, or actively cheats during either the signing or the unblinding protocol. We base our specific implementation on the DSS algorithm. Our construction demonstrates the extended power of distributed signing.

Easy come - easy go divisable cash

Filename:
ec98.ps

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Frankel, Yair
Tsiounis, Yiannis
Chan, Agnes

Recently, there has been an interest in creating practical anonymous electronic cash with the ability to conduct payments of exact amounts, as is typically the practice in physical payment systems.
The most general solution for such payments is to allow electronic coins to be divisible (e.g., each coin can be spent incrementally but total purchases are limited to the monetary value of the coin). In Crypto'95, T. Okamoto presented the first efficient divisible, anonymous (but linkable) off-line e-cash scheme requiring only O(log N) computations for each of the withdrawal, payment and deposit procedures, where N = (total coin value)/ (smallest divisible unit) is the divisibility precision. However, the zero-knowledge protocol used for the creation of a blinded unlinkable coin by Okamoto is quite inefficient and is used only at set-up to make the system efficient. Incorporating ``unlinkable'' blinding only in the setup, however, limits the level of anonymity offered by allowing the linking of all coins withdrawn---rather than a more desirable anonymity which allows only linking of subcoins of a withdrawn coin.
In this paper we make a further step towards practicality of complete (i.e., divisible) anonymous e-cash by presenting a solution where all procedures (set-up, withdrawal, payment and deposit) are bounded by tens of exponentiations; in particular we improve on Okamoto's result by 3 orders of magnitude, while the size of the coin remains about 300 Bytes, based on a 512 bit modulus. Moreover, the protocols are compatible with tracing methods used for ``fair'' or ``revokable'' anonymous cash.

Electronic Cash Scheme for Home Shopping

Filename:
printed

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Li, Jian Bao
Lam, Kwok Yan

Following the development of Internet trade, e-cash has become a very active area. Since it is first introduced by Chaum, Fiat & Naor, there have been several improvements and constructions. In a general e-cash scheme, each coin has the same value. However in real life, it is inefficient. In this paper we gave a new e-cash scheme that supports variable value. Based on this scheme we peresent a concept of 'e-cash scheme for home shopping'. This scheme is based on the scheme introduced by Ferguson. From a practical point of view, our scheme is more efficient and simpler than that of Ferguson's. The concept of the system is similar to credit card system or electronic check system.

Fair Off-line E-Cash Made Easy

Filename:
folc-es.ps

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Frankel, Yair
Tsiounis, Yiannis
Yung, Moti

The major considerations in designing a secure system are (1) simplicity of the algorithms involved, (2) efficiency of the implementation, and (3) provable security; these attributes contribute to the ``elegance'' of a system, easing its implementation (and limiting the possibility of errors) and the burden on system resources.
Anonymous off-line electronic cash (e-cash) systems provide transactions that retain the anonymity of the payer, similar to physical cash exchanges, without requiring the issuing bank to be on-line at payment. Fair off-line e-cash extend this capability to allow a qualified third party (a ``trustee'') to revoke this anonymity under a warrant or other specified ``suspicious'' activity. In fair off-line e-cash, simplicity and efficiency are of high importance, as the systems are inherently complex and prone to design and implementation errors. Security must also be guaranteed yet, to date, there have been no systems that offer provable security.
In this work we make a step towards ``elegant'' fair off-line e-cash by proposing a system which is provably anonymous (i.e., secure for legitimate users) while its design is simple and its efficiency is similar to the most efficient systems to date. Security for the bank and shops is unchanged from the security of non-traceable e-cash. We also present ways to adapt the functionality of ``fairness'' into existing (legacy) e-cash systems in a modular way, thus easing advancement and maintaining version compatibility; these extensions are also provably anonymous.
We prove anonymity based on the decision Diffie-Hellman assumption. This assumption has been used recently for other purposes, such as implementations of unconditionally-hiding hash functions.

Group Blind Digital Signatures: A Scalable Solution to Electronic Cash

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Lysyanskaya, Anna
Ramzan, Zulfikar

In this paper we construct a practical group blind isgnature scheme. Our scheme combines the already existing notions of blind signatures and group signatures. It is an extension of Camenish and Stadler's Group Signature Scheme [5] that adds the blindness property. We show how to use our group blind signatures to construct an electronic cash system in which multiple banks can securely distribute anonymous and untraceable e-cash. Moreover, the identity of the e-cash issuing bank is concealed, which is conceptually novel. The space, time and communication complexities of the relefant parameters and operations are independent of the group size.

Micropayments via Efficient Coin-Flipping

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Lipton, Richard J.
Ostrovsky, Rafail

We present an authenticated coin-flipping protocol and its proof of security. We demontrate the applicability of our scheme for on-line randomized micro-payment protocols. We also review some essential aspects of other micro-payment proposals (including SET, PayWord & MicroMint, PayTree, NetCheque, NetCash, Agora, NetCard, CAFÉ, Pederson's proposal, micro-iKP, Milicent, proposal of Jarecki-Odlyzko, proposal of Yacobi, SVP, Digicash, Rivest 'Lottery Ticket As MicroCash" and Wheeler's proposal) and compare it with our scheme.

One Time Zero-Knowledge Authentications and Their Application to Untraceable Electronic

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Okamoto, Tatsuaki
Ohta, Kazuo

In this paper, we propose a new type of authentication system, one-time zero-knowledge authentication system. Informally speaking, in this scheme, double usage of the same authentication is prevented. Based on these one-time zero-knowledge authentication system, we propose a new untraceable electronic cash scheme satisfying both untraceability and unreusability. This scheme overcomes the problem of the previous scheme by Chaum, Fiat, and Naor through greater efficiency and provable security under reasonable cryptographic assumptions. We also propose a scheme, 'transferable untraceable e-cash' satisfying transferability as well as the above two criteria. We also propose untraceable coupon ticket, in which the value of one piece of the e-cash can be subdivided into many pieces.

Practical Escrow Cash Schemes

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Okamoto, Tatsuaki
Fujisaki, Eiichiro

This paper proposes practical escrow cash schemes with particular emphasis on countermeasures against social crimes such as money laundring and extortion. The proposed cash schemes restrict "unconditional" privacy in order to prevent these social crimes while preserving off-line-ness, divisibility and transferability, properties listed in [25- OkaOhta91] as criteria for ideal cash system.

Risk and Potentials of Using EMV for Internet Payments

Filename: VHW98.ps

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Van Herreweghen, Els
Wille, Uta

Existing payment smartcards developed for traditional point-of-sale transactions are being considered for use in Internet transactions. Such solutions have been suggested as alternatives to using payment protocols more specifically designed for Internet (such as SET) but often lacking smartcard support. In this paper, we analyze EMV'96, a representative example of an existing payment smartcard specification. We investigate which security requirements for an Internet payment system can and cannot be met when using EMV for Internet payments. We suggest possible modifications that can enhance the security of an Internet payment cheme based on EMV.

Smartcard-Supported Internet Payments

Filename: Sasse98.ps

☐ Ecash ☑ PaymentSystem ☑ Smartcard

Author

Good for payment system categorization.

Threshold Traitor Tracing

Filename: 14620502

☑ Ecash ☐ PaymentSystem ☐ Smartcard

Author
Naor, Moni
Pinkas, Benny

Vulnerability of Anonymous E-cash System to Insider-Attacks from Untrusted Authorities

Filename: printed

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Miyazaki, Shingo
Sakurai, Kouichi

We consider security of anonymous e-cash system against insider attacks of bank and/or of third authorities, which have been assumed to be trusted in the previous models. In order to clarify the role of these assumptions, we classify known electronic money system, which are based on the Chaum-Fiat-Naor paradigm, into four types according to how information on customers is stored in banks.

X-Cash: Executable Digital Cash

Filename: xcash.ps

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Jakobsson, Markus
Juels, Ari

In this paper, we propose a new financial instrument known as executable digital cash, or X-cash. X-cash is a means of binding an offer to the accompanying goods or payment, enabling the processes of searching and paying to be unified. The result is a mechanism by which electronic trades can occur in a highly distributed setting with strong security guarantees. When a party receives an X-cash offer, he or she can verify that it is bona fide and can initiate a trade immediately, without contacting the originator directly. X-cash may therefore be used, among other things, to enable mobile agents to carry funds and make payments on-site without running the risk of ''pick-pocketing''. In this paper, we introduce X-cash, describe some variants, and sketch proofs of its security properties.

1999

A New Type of Magic Ink Signatures - Towards Transcript-Irrelevant Anonymity Revocation

Filename: 15600001

☑ Ecash ☐ PaymentSystem ☐ Smartcard

Author
Feng, Bao
Deng, Robert H.

Assessment of Effectiveness of Counterfeit Transaction Detection Systems for Smart Card

Filename:
16480072.pdf

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Ezawa, Kazuo J.
Napiorkowski, Gregory
Kossarski, Mariusz

In this paper, we discuss a process to evaluate the effectiveness of counterfeit detection systems for an electronic cash scheme which is not fully accounted (i.e., off line, peer to peer transactions are allowed, and no shadow accounting for each purse). The process includes a use of a micro dynamic simulator to simulate various counterfeit scenarios (in addition to testing on the actual non-counterfeit transaction data sets from the real deployment) and generate transaction data sets for detection systems to use for the counterfeit detection systems training and testing. A case study of preliminary test results related to the effectiveness of the detection systems in a simulated counterfeit scenario is also provided.

Auditable, Anonymous Electronic Cash

Filename:
printed 16660555

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Sander, Tomas
Ta-Shma, Amnon

Most anonymous, e-cash systems are signature based. A side effect of these systems, the bank has the technical ability to issue unreported, valid money. It has been noticed in the past that this may lead to a disaster if the secret key of the bank is compromised. Furthermore, the above feature prevents any effective monitoring of the system.
In this paper we build a fully anonymous, auditable system, by constructing an electronic cash system that is signature free, and where the bank needs to have no secret at all. The security of the system instead relies on the ability of the bank to maintain the integrity of a public database. Our system takes a completely new direction for meeting the above requirement, and in particular, it is the first to do so without the necessity of making individual transaction potentially traceable: payers enjoy unconditional anonymity for their payment transactions. The system is theorethically efficient but not yet practical.

Coin-Based Anonymous Fingerprinting

Filename:
15920150.pdf

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Pfitzmann, Birgit
Sadeghi, Ahmad-Reza

Dynamic Traitor Tracing

Filename:
16660354

☑ Ecash ☐ PaymentSystem
☐ Smartcard

Author
Fiat, Amos
Tassa, Tamir

Electronic Payment: where do we go from here?

Filename:
17400043.pdf

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Jakobsson, Markus
M'Raihi, David
Tsiounis, Yiannis
Yung, Moti

Currently, the Internet and the World Wide Web on-line business is booming, with traffic, advertising and content growing at sustained exponential rates. However, the full potential of on-line commerce has not been possible to realize due to the lack of convenient and secure electronic payment methods (e.g., for buying e-goods and paying with e-money). Although it became clear very early that it is vital for payments to be safe and efficient, and to avoid requiring complicated user intervention, it is still the case that the Internet payment method of choice today is that of traditional credit cards. Despite their widespread use and market penetration, these have a number of significant limitations and shortcomings, including lack of security, lack of anonymity, inability to reach all audiences due to credit requirements, large overhead with respect to payments, and the related inefficiency in processing small payment amounts.
These limitations (some of which are present in the real world) prompted the design of alternative electronic payment systems very early in the Internet age -- even before the conception of the World Wide Web. Such designs promised the security, anonymity, efficiency, and universal appeal of cash transactions, but in an electronic form. Some early schemes, such as the one proposed by First Virtual, were built around the credit card structure; others, such as the scheme developed by DigiCash, offered a solution with cryptographic security and payer anonymity. Still others, such as Millicent, introduced micropayment solutions. However, none of these systems managed to proliferate in the marketplace, and most have either ceased to exist or have only reached a limited audience.
This paper is associated with a panel discussion whose purpose is to address the reasons why the international e-commerce market has rejected proposed solutions, and to suggest new ways for electronic payments to be used over the Internet, avoiding the problems inherent in credit card transactions. The purpose of this paper is to set the stage for such a discussion by presenting, in brief, some of the payment schemes currently available and to discuss some of the basic problems in the area

Engineering an eCash System

Filename:
172900032

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Ebringer, Tim
Thorne, Peter

Flow Control: A New Approach for Anonymity Control in Electronic Cash Systems

Filename:
16480046.pdf

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Sander, Tomas
Ta-Shma, Amnon

Anonymity features of electronic payment systems are important for protecting privacy in an electronic world. However, complete anonymity prevents monitoring financial transactions and following the money trail, which are important tools for fghting serious crimes. To solve these type of problems several "escrowed cash" systems, that allow a "Trustee" to trace electronic money, were suggested. In this paper we suggest a completely different approach to anonymity control based on the fact that law enforcement is mainly concerned with large anonymous electronic payments. We describe a payment system that effectively limits the amount of money a user can spend anonymously in a given time frame. To achieve this we describe a technique to make electronic money strongly non-transferable. Our payment system protects the privacy of the honest user who plays by the rules, while introducing significant hurdles for several criminal abuses of the system.

Micropayments and Anonymous E-Cash (ppt)

Filename:
micro-ecash.ppt

☑ Ecash ☑ PaymentSystem
☐ Smartcard

Author
Tsiounis, Yiannis

Mini-Cash: A Minimalistic Approach to E-Commerce

Filename: minicash.ps

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Jakobsson, Markus

By introducint a new e-commerce paradigm - that od disposable anonymous accounts - we are able to reduce storage requirements, while protecting against strong attacks on the system, and keeping computational requirements low. Our proposed scheme reduces storage costs of payers and merchants to the lowest theoritically possible, offers users computational (but revokeable) privacy, and protects against the bank robbery attack. Furthermore, by being practically impelementable as a smartcard payment scheme, it avoids the threats of viral attacks on users. The scheme allows the notion of 'pre-paid' cards by not requireing a link to the identity of the card owner.

Mix-based Electronic Payments

Filename: mixpay.ps

☑ Ecash ☑ PaymentSystem ☑ Smartcard

Author
Jakobsson, Markus
M'Raihi, David

We introduce a new payment architecture that limits the power of an attacker, and improves the efficientcy of the resulting scheme. Our proposed method defends against all known attacks, implements revocable privacy, and is well-suited for smartcard-based payment schemes over the Internet.

Money Conservation via Atomicity in Fair Off-Line E-Cash

Filename: 17290014.pdf

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Yung, Moti
Xu, Shouhuai
Zhang, Gendu

On Anonymous Electronic Cash and Crime

Filename: 17290202.pdf

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Sander, Tomas
Ta-Shma, Amnon

Risk Management for E-cash Systems with Partial Real-Time Audit

Filename: 16480062

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Yacobi, Yacov

We analyze "coin-wallet" and "balance-wallet" under partial real-time audit, and compute upper bounds on theft due to the fact that not all the transactions are audited in real time, assuming that everything else is perfect. In particular, we assume that the audit regime holds for innocent players. Let v be the maximum allowed balance in a wallet, 0 1 be the fraction of transactions that are audited in real time in an audit round that includes overall n transactions. Assume one unit transactions. We show that for <<1 the upper bound on expected theft for coin-wallet is v e 2 v .. .. .. while for plausible parameter choice the bound for a balance-wallet is O(exp(v 2 =n)). This last bound can become huge in some cases, implying that partial audit, while suitable for coin-wallets with low denomination coins, may be too risky for balance-wallet. Some implications to the design of anonymous and non-anonymous systems are discussed.

Spending Programs: A Tool for Flexible Micropayments

Filename: 17290001.pdf

☑ Ecash ☑ PaymentSystem ☐ Smartcard

Author
Domingo-Ferrer, Josep
Herrera-Joancomarti, Jordi

Trustee Tokens: Simple and Practical Anonymous Digital Coin Tracing

Filename:

16480029.pdf

☑ Ecash ☑ PaymentSystem

☐ Smartcard

Author
Juels, Ari

We introduce a trustee-based tracing mechanism for anonymous digital cash that is simple, effcient, and provably secure relative to its underlying cryptographic primitives. In contrast to previous schemes, ours may be built on top of a real-world anonymous cash system, such as the DigiCash TM system, with minimal modification to the underlying protocols. In addition, our scheme involves no change to the structure of the coins. On the other hand, our scheme requires user interaction with a trustee, while many other such systems do not. This interaction occurs infrequently, however, and is e cient both in terms of computation and storage requirements. Our scheme also achieves more limited security guarantees in the presence of malicious trustees than many other systems do. While this is a disadvantage, it represents a tradeoff enabling us to achieve the high level of practicality of our system.