Fair Exchange and Anonymous E-Commerce by Deploying Clone-Resistant Tokens

Ayoub Mars and Wael Adi
IDA, Institute of Computer and
Network Engineering
Technical University of Braunschweig
Braunschweig, Germany
{a.mars, w.adi}@tu-bs.de

***Abstract*—The majority of E-commerce transactions reveal private information such as customer's identity, order contents and payment information during the transaction. Other personal information such as health conditions, religion, and even ethnicity may be also deduced. Even when deploying electronic cryptocurrencies such as Bitcoin, anonymity cannot be fully guaranteed. Also, many anonymous payment schemes suffer from possible double spending circumstances. E-commerce privacy is basically a difficult problem as it involves parties with concurring interests. Three major e-commerce requirements are highly difficult to resolve: anonymous purchase, anonymous delivery and anonymous payment. This work presents a possible e-commerce system addressing all three anonymity requirements for electronic-items business on open networks. The system offers anonymous entities authentication mechanisms up to completing a fair anonymous e-commerce transaction. The system is based on deploying a physically clone-resistant hardware token for each relevant involved party. The tokens are made clone-resistant by accommodating a Secret Unknown Cipher (SUC) in each hardware-token as a digital PUF-like identity. A set of novel generic system-setups for units, protocols and e-commerce schemes is introduced. The proposed anonymization is basically attained by virtually-replacing relevant e-commerce entities by low-cost, unique and clone-resistant tokens/units using SUCs. The units act as trustable anonymous, authenticated and non-replaceable entities monitored by their acting users.**

***Keywords*—Anonymous e-commerce, e-payment, Fair Exchange, Anonymity, Secret Unknown Cipher, Physical Unclonable Functions.**

I. Introduction

E-commerce has become a viable solution for online shopping. It provides consumers with an easy way to buy items from merchants located all over the world. The purchase of digital items requires often an electronic payment (e-payment); the main concerns in any e-payment system are security and privacy of participants and the transaction's attributes. Nowadays, cryptocurrencies are increasingly used as anonymous or pseudo-anonymous e-payment systems, they either use proof of operation, such as in Bitcoin [1], or proof of stake, such as in BitcoinDark, to verify transactions and add new blocks to the blockchain which is used as a public ledger accessible to everyone. Bitcoin was introduced in [1] as a peer-to-peer electronic cryptocurrency system. Bitcoin makes intensive use of cryptographic functions to transfer crypto money from one user to another without revealing its identity. Since transactions are associated with users' public addresses, users are encouraged to create as many public addresses as possible to make it difficult to link the transactions and hence increase users' privacy [1][2].

Blockchain may solve both tampering and double spending issues in many cryptocurrencies. In Bitcoin, the difficulty of the proof of work is auto-adjusted every two weeks targeting 10 minutes block generation, this allows fast double spending when Bitcoin is used in fast payment actions [3]. In cryptocurrencies, users are anonymous and don't trust each other. However, Blockchain doesn't consider the notion of fairness [4]. Fair exchange allows two participants to exchange digital items fairly, such that delivery may not happen without payment and vice versa.

In this paper, we propose a new e-commerce system where each participant has its unique physical clone-resistant unit. Physical Unclonable Functions (PUFs) [5][6] have been proposed during the last decade to provide an intrinsic identity of electronic devices. Due to their analog nature, PUFs behavior is inconsistent by aging and under different environmental and operational conditions. This makes the use of the so called "fuzzy extractor" or helper data algorithm besides each PUF instance necessary resulting with the increase in hardware complexity in terms area and time.

Recently, Adi proposes to create digital clone-resistant units nominated later as Secret Unknown Cipher (SUC). SUC fulfil the same PUF tasks, however in digital form. SUCs are therefore consistent during the whole lifecycle of the digital system [7][8]. The proposed SUC allows counteracting the drawbacks of PUFs and creating robust clone-resistant identities. In [8], Mars et al. propose a SUC design based on Random Stream Cipher (RSC-SUC) deploying a class of T-functions as key stream generator with few random optimal involutive S-Boxes. In [9], a SUC creation process based on random block ciphers was proposed, it is deploying random optimal S-Boxes as a source of secret randomness in the SUC design in addition to the secret key. In [10], a SUC design template based on combining well-selected NLFSRs having low complexity feedback functions was proposed. Compared to the SUC designs in [8] and [9], NLFSRs can be distributed over all the FPGA area. Generic authentication protocols of SUC based on random block ciphers were proposed in [11] while [10] proposes authentication protocols of SUC based on random stream ciphers.

Contribution. The contribution of this paper is firstly, a new procedure is introduced for anonymous e-commerce transactions where each unit has its own clone-resistant hardware token based on digital physical clone-resistant functions. Secondly, we propose a strong and fair exchange protocol based on online trusted third party. Finally, we propose a novel use of One-Time-Coin generator through Automated Teller Machine (OTC ATM) adapted to the SUC structure to allow the exchange of OTCs with money anonymously.

The remainder of this paper is organized as follows. Section 2 describes the state of the art of anonymity and fair exchange in e-commerce and e-payment. In section 3, the anonymous e-commerce system architecture together with the commercial hardware setup and delivery are described. Section 4 presents the proposed new fair exchange protocol with its payment management concept**.** Finally, section 5 concludes the paper results.

II. Related Work

E-commerce transactions reveal usually private information of customers whose identities are disclosed during the payment process. Additional private information such as their health condition, religion, and ethnicity can be also deduced. Many e-commerce schemes have been proposed to provide user privacy protection and fairness. According to [13], the e-commerce privacy is mainly based on the following properties:

- *Customer Anonymity:* No unauthorized third party, including the Trusted Authority (TA), may acquire any identifiable information (name, address or Internet address) of an individual or customer participating in an e-commerce activity.
- *Transaction Unlinkability:* No single entity (third parties, online payment systems, etc.) should be able to link one or more shopping activities or transactions to a unique (personally identifiable) user.

In [14], a privacy preserving e-commerce protocol has been proposed. It allows unlinking online transactions from customer identities; hence the customer privacy will be preserved. Furthermore, Rial [15] categorized privacy preserving protocols as follows:

- Private purchase protocols: The protocol reveals to the service provider the identities of the users but hides from the service provider which items the users purchase. This type of protocols can only be used to purchase digital products since the delivery process can reveal the purchased items. The communication between the users and the service provider employs an authenticated channel.
- Anonymous purchase protocols: The protocol hides from the service provider the identity of the users. However, the service provider learns which items are purchased by the users. Communication between users and a service provider should be done through anonymized channels.
- Private Billing: The protocol reveals to the service provider the identity of users but hides from the service provider the consumption readings of the meter. Communication between users and service provider employs an authenticated channel.
- Anonymous Billing: The protocol hides from the service provider the identity of the users but it reveals the consumption measurements.

Our proposed anonymous e-commerce scheme based on clone resistant units with fair exchange protocol ensures customer anonymity with anonymous purchase and anonymous billing. Furthermore, the Trusted Third Party (TTP) cannot learn which items were purchased but it reveals the spending of each user for every transaction.

In traditional transactions, the customer and the merchant meet face-to-face and hence they can fairly exchange money and goods. For online transactions, fairness is unpredictable since one of the two parties can cheat the other. i.e. the customer may not receive the goods after payment or the merchant may not receive the payment after providing the goods to the customer. Fair exchange protocols ensure that, at the end of the transaction, both service provider receives the payment and the user receives the product. Otherwise none of parties would get anything. Fair exchange protocols are classified into:

- Gradual exchange protocols [16]: the two parties exchange secret data bit by bit. In normal cases, no participant has an unfair advantage over the other participant. However, it can be seen that one of the participants may get more secret data bits than the other and terminate the exchange procedure. In addition to that, this protocol requires a lot of communications during the same transaction and hence it is inefficient.
- Trusted Third Party (TTP) protocols: they involve a TTP that guarantees fairness of the transactions. TTPs may have online and offline type. In online TTP [17], whenever the two participants intend to communicate, they send their data to the TTP which checks for correctness. If it is the case, the TTP validates the transaction and the two participants get their right data, if not both parties get nothing. In offline TTP [18][19][20][21], the TTP is only involved in case of dispute.

In [22], Pagnia et al. provide a formal definition of the strong fair exchange problem and proved that it may not be reached without a trusted third party. In this paper, fairness in our proposed e-commerce system is based on the electronic commerce server that is the TTP itself.

III. E-Commerce Business Model

Traditional commerce is based on physically exchanging items between users fairly. In e-commerce, the identity of a user cannot be verified directly by the other users in an online transaction. Thus, there is a need for a TTP to realize secure and fair exchange between users. In traditional e-commerce, users are forced to reveal their identities to the TTP, which would violate anonymity and privacy of users. To ensure e-commerce participants anonymity, we propose to deploy anonymous Commercial Hardware Token (CHT) based on a SUC where the TTP will be able to verify each anonymous CHT based on its SUC. However, participants identities will not be revealed. Furthermore, the proposed anonymous e-commerce is selling e-goods where the participants are not obliged to provide a delivery address that may disclose their identity.

A. E-commerce Model

This section describes the business model of the proposed physically anonymous e-commerce. The proposed e-commerce concept involves an Electronic Commerce Server

(ECS) which is considered as a TTP, the merchants providing e-goods, the consumers willing to get anonymously e-goods and the One Time Coin generator that can be an Automated Teller Machine (OTC ATM). The OTC ATM is able to generate one-time coins and sell them to the users. Fig. 1 describes the proposed business model. It proceeds as follows:

- **Step 1:** the customer orders a digital item anonymously from a merchant.
- **Step 2:** the merchant delivers anonymously the encrypted digital item with a secret key known only to the merchant and the ECS.
- **Step 3:** the customer orders a One Time Coin (OTC) from the OTC ATM. The ordered OTC should have a value equivalent of the ordered digital product from the merchant.
- **Step 4:** The customer sends the encrypted OTC to the merchant.
- **Step 5.a:** the merchant sends a proof to the ECS that he/she sends the encrypted digital product to the customer and confirms to the ECS that he/she gets paid for the digital product.
- **Step 5.b:** the customer confirms to the ECS that he/she got the encrypted digital product from the merchant and that he/she paid the merchant for it.
- **Step 6:** the ECS verifies that both the merchant and the customer are providing identical data with no conflict. If it is not the case, it rejects and aborts.
- **Step 7:** the ECS sends the OTC to the OTC ATM that verifies that the provided OTC is not spent before; this protect against double spending. Steps 6 and 7 ensure a fair exchange between the merchant and the customer such that even both parties get the other's item or none does.

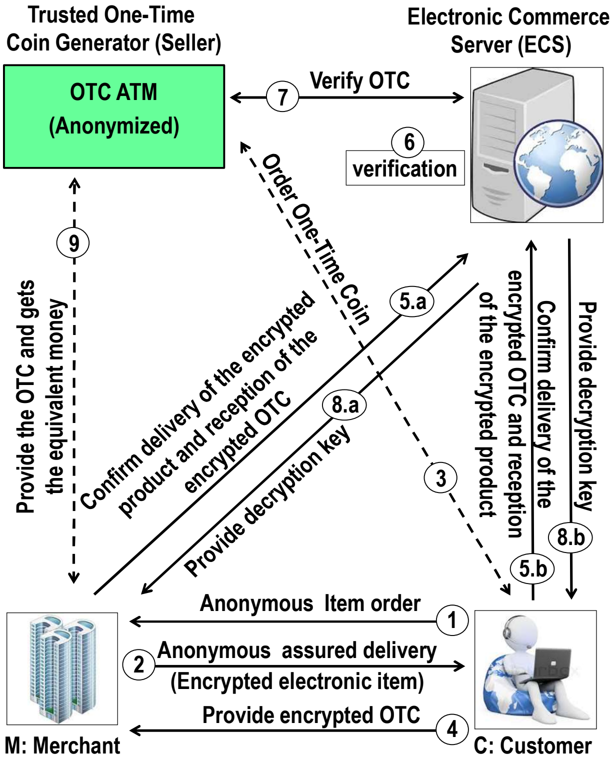


Fig. 1. E-commerce Business Model

- **Step 8.a:** The ECS provides the merchant with the decryption key of the OTC.
- **Step 8.b:** The ECS provides the merchant with the decryption key of the digital product.
- **Step 9:** the merchant provides the OTC to the OTC ATM and gets the equivalent money of the digital product even in cash or the OTC ATM transfers it to an anonymous merchant account.

B. SUC-based Commercial Hardware Token

The Commercial Hardware Token (CHT) based on SUC constitutes the heart of the proposed fair exchange physically anonymous e-commerce. Each CHT embeds its SUC as physical clone-resistant unit. SUCs have been proposed to overcome some of the PUFs drawbacks especially their inconsistency [7] [8].

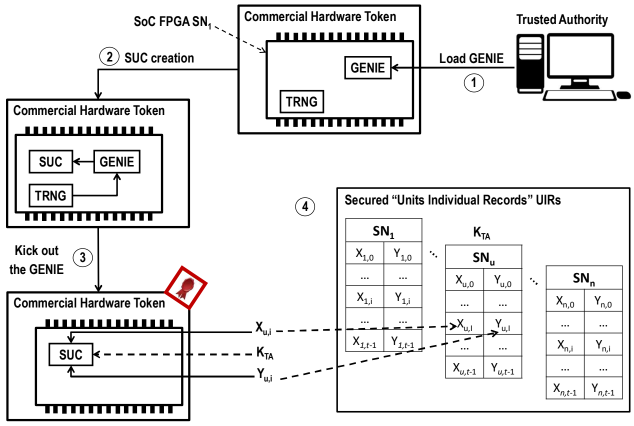
Definition. Secret Unknown Cipher is a randomly internally single-event-generated unknown cipher such that: it is unpredictable, tamper-proof and non-removable. Neither users nor manufacturer have influence or access to its creation process. Even the manufacturer should not be able to back trace the creation process and deduce the created random cipher.

Fig. 2 describes the conceptual scenario for embedding a SUC in a CHT device that includes a System on Chip (SoC) FPGA. The CHT personalization process proceeds as follows:

- **Step 1:** The Trusted Authority (TA) uploads a software package as a smart cipher designer called "GENIE".
- **Step 2:** The GENIE is then ordered to create a non-predictable cipher (SUC) with the help of the True Random Number Generator (TRNG) located within the SoC to assure randomized, unpredictable and unknown results. The GENIE stores the created SUC permanently at unknown location/s within the FPGA fabric and makes it usable only for encrypting and decrypting data.
- **Step 3:** The GENIE is then kicked-out (that is, deleted as a program and ordered to leave the device forever). The end result is a usable cipher which nobody knows. Notice that the created ciphers are basically different, even when having an unknown individual structure and unknown locations for each individual device.
- **Step 4:** In the enrollment process, the TA (or any other TA') challenges each SUC_u by a set of *t*-cleartext patterns $\{X\} = \left(X_{u,0} \dots X_{u,t-1}\right)$ to generate the corresponding t-ciphertext set $\{Y\} = \left(Y_{u,0} \dots Y_{u,t-1}\right)$ where $Y_i = SUC_u(X_i)$. Then, the TA stores the *t*-cleartext/ciphertext pairs $\{X\}/\{Y\}$ in the corresponding device records as: Units Individual Records (UIR) labeled by the serial number of the device SN_u. The $\{X\}/\{Y\}$ pairs are to be used later by the TA/TA' to identify and

authenticate devices. Notice that multiple TA's can operate completely independently for their own individual application by using the same SUC.

SUC concept is comparable to the conventional PUFs, with the advantage that it is collision-free. As a bijective cipher SUC offers higher entropy compared with a conventional PUF, which is equivalent to a collision-prone hash function. Invertibility is an advantageous property that was deployed in [23] to build a strict chain of trust for a secured vehicular software update protocol which is much more complex in traditional PUFs.



SN$_1$	
$X_{1,0}$	$Y_{1,0}$
...	...
$X_{1,i}$	$Y_{1,i}$
...	...
$X_{1,t-1}$	$Y_{1,t-1}$

SN$_u$	
$X_{u,0}$	$Y_{u,0}$
...	...
$X_{u,I}$	$Y_{u,I}$
...	...
$X_{u,t-1}$	$Y_{u,t-1}$

SN$_n$	
$X_{n,0}$	$Y_{n,0}$
...	...
$X_{n,i}$	$Y_{n,i}$
...	...
$X_{n,t-1}$	$Y_{n,t-1}$

Fig. 2. Concept for CHTs personalization

C. Commercial Hardware Token (CHT) Setup and Delivery

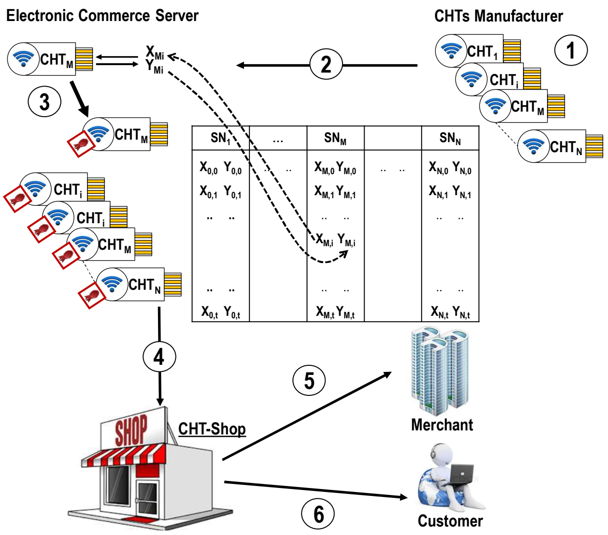
Fig. 3 describes the main personalization process of the CHTs by the ECS and the delivery to the users:

- **Step 1:** The CHTs manufacturer is responsible for producing CHTs. They are fabricated such that each CHT embeds an SUC ensuring its uniqueness and unclonablity or at least clone-resistance.
- **Step 2:** The ECS gets N CHTs from the CHTs manufacturer.
- **Step 3:** The ECS challenges each CHT, for instance CHT having serial number SN$_M$, with a set of t-challenges $X_{M,i}$ ($0 \le i \le t-1$) and gets the corresponding responses $Y_{M,i}$ and stores them in the corresponding area on the ECS UIR defined by SN$_M$.
- **Step 4:** The ECS delivers the certified CHTs to the CHT-shops.
- **Step 5:** Merchants and consumers can buy CHTs without revealing their identities to the shop.

D. The System Threat Model

The proposed e-commerce scheme assumes the following:

- *ECS is a trusted third party:* It is assumed that the trusted third party will not misbehave or collude with one of the transacting parties.
- *CHTs are clone-resistant or Unclonable:* SUC is designed to be resistant against mathematical cloning. It is also resistant to physical cloning by deploying countermeasures against side channel attacks. This results with secure CHTs, such that even the manufacturer will not be able to clone them.



SN$_1$	...	SN$_M$		SN$_N$
$X_{0,0}$ $Y_{0,0}$	.. ..	$X_{M,0}$ $Y_{M,0}$	.. ..	$X_{N,0}$ $Y_{N,0}$
$X_{0,1}$ $Y_{0,1}$		$X_{M,1}$ $Y_{M,1}$		$X_{N,1}$ $Y_{N,1}$
.. ..		.. ..		.. ..
		$X_{M,i}$ $Y_{M,i}$		
.. ..		.. ..		.. ..
$X_{0,t}$ $Y_{0,t}$		$X_{M,t}$ $Y_{M,t}$		$X_{N,t}$ $Y_{N,t}$

Fig. 3. CHTs setup and delivery

- *Merchant is not considered honest:* The merchant can try to cheat or provide counterfeit services.
- *The consumer may try to cheat:* After receiving the e-good, the consumer could claim the inverse and try not to pay the merchant.

IV. Fair Exchange and Anonymous E-Commerce Based on CHTs

Anonymity constitutes an appealing requisite in e-commerce. Anonymous e-commerce aims to protect the identity of the actors in the e-commerce scheme especially the consumers. Cryptocurrencies such as Bitcoin provide pseudo-anonymity because they are based on a public ledger blockchain making all the users transactions visible to the public [1], [2]. To improve privacy in Bitcoin, users should use different public addresses for different transactions, this makes it difficult to link users's transactions.

In our proposed scheme, each participant (ECS, Merchant and Customer) has a CHT. When a service is required by a consumer from a merchant, the ECS lets the customer and the merchant trust each other with a simple intervention by the ECS. For this purpose, the generic mutual authentication protocol in [11] can be used. A secret shared key (*Z*) between the consumer and the merchant is generated at the end of this protocol. The key *Z* will be used in the fair exchange protocol, this would allow both parties to communicate securely such that no other third party even the ECS will not be able to eavesdrop the communication and get what digital items they are exchanging.

The ECS acts like an escrow agent where it ensures fairness at the end of the exchange, but it does not have any access to the shared services between the consumer and the merchant in normal case. After completion of the exchange, if there is a dispute between the merchant and the consumer, the ECS gets the shared secret key and verifies which participant was not honest.

A. Fair Exchange Protocol

Fair exchange protocol ensures that the exchange of digital items between the merchant and the customer is fair, so at the end of the exchange, either both the merchant and customer get the other's item or neither of them does. Fig. 4 describes the proposed fair exchange protocol involving the ECS as trusted third party. The ECS acts as an escrow agent, where the customer and the merchant rely on it to ensure fairness when finishing the exchange of the digital item. The fair exchange protocol proceeds as follows:

- **Step 1:** the customer C, identified by its serial number SN$_C$, asks for a service P_t from the merchant M identified by its serial number SN$_M$.
- **Step 2.a:** Merchant M requests one response $Y_{M,j}$ from the ECS. The ECS sends $E_{X_{M,j}}(Y_{M,j})\|Y_{M,j}$ to M which computes $X_{M,j} = SUC_M^{-1}(Y_{M,j})$. M will use $X_{M,j}$ as encryption key.
- **Step 3:** Merchant M encrypts the service P_t by using the key $X_{M,j}$ and sends it to the customer as $Y_1 = E_{X_{M,j}}(P_t)$.
- **Step 4.a:** the customer receives the encrypted service Y_i and confirms that to the ECS by encrypting it using the session key Z and sends it concatenated with the encrypted: service value V_C, the required product P_t and the coin to be used to pay the service OTC_t as $E_Z(Y_1)\|E_{X_{C,i}}(V_C, OTC_t)\|Y_{C,i}$.
- **Step 4.b:** Merchant M confirms to the ECS that the service is transferred to the customer. It encrypts the sent encrypted service P_t by using the session key Z as $Y_3 = E_Z(Y_1)$ and sends it concatenated with the encrypted service value $E_{X_{M,j}}(V_M)$ to the ECS.
- **Step 5:** The ECS verifies if both received confirmations correspond. If $Y_2 = Y_3$ and $V_M = V_C$, then the ECS contacts the OTC ATM to check for the validity of the OTC$_t$. If OTC$_t$ is valid and $OTC_t = V_t$, then the ECS continues the transaction. Otherwise the transaction is rejected, the customer or the merchant or both may be cheating. At this point, the merchant did not get the service value yet and the customer still has only the encrypted service. In All cases, the ECS deletes and replace the used CRPs.
- **Step 6.a:** In case that ECS deems the service as consistent; The ECS provides the customer with the decryption key $Y_{M,j}$, to allow the customer's access to the ordered and paid service.
- **Step 6.b:** The ECS provides the merchant with the payment coin OTC$_t$ to complete the transaction.

In case of conflict, the ECS asks for the session key Z from both parties; i.e. the consumer and the merchant. It decrypts the received messages in steps 1 and 3 and compares the required service from the consumer with the sent one from the merchant.

B. Payment's Management Concept

The payment management concept is described in Fig. 5. It proceeds as follows:

- **Step 1:** the customer orders a one-time coin that has a value equal to the ordered digital product from the service OTC$_t$. The customer pays (possibly in cash) to the coin generator (seller) to get the OTC$_t$.
- **Step 2:** the OCT ATM generates OTC$_t$ and provides it to the customer.

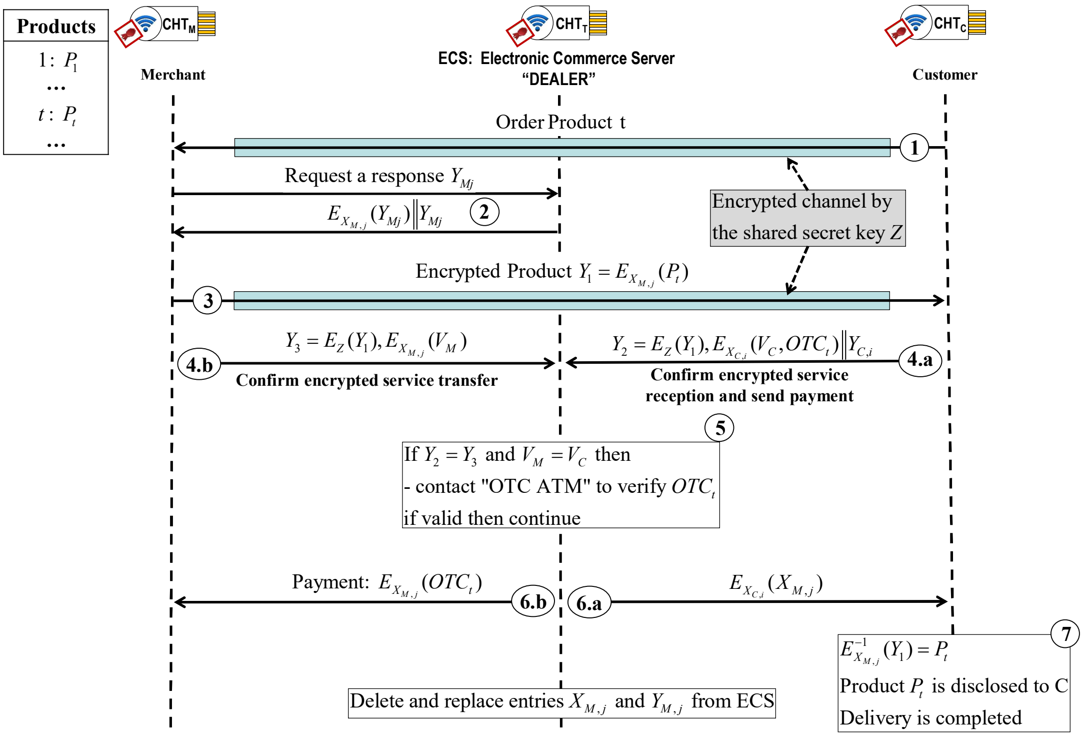

Products
1: P_1
...
t: P_t
...
CHT$_M$
Merchant
CHT$_T$
ECS: Electronic Commerce Server
"DEALER"
CHT$_C$
Customer
Order Product t
1
Request a response Y_{Mj}
$E_{X_{M,j}}(Y_{Mj})\|Y_{Mj}$
2
Encrypted channel by the shared secret key Z
Encrypted Product $Y_1 = E_{X_{M,j}}(P_t)$
3
$Y_3 = E_Z(Y_1), E_{X_{M,j}}(V_M)$
4.b
Confirm encrypted service transfer
$Y_2 = E_Z(Y_1), E_{X_{C,i}}(V_C, OTC_t)\|Y_{C,i}$
4.a
Confirm encrypted service reception and send payment
5
If $Y_2 = Y_3$ and $V_M = V_C$ then
- contact "OTC ATM" to verify OTC_t
if valid then continue
Payment: $E_{X_{M,j}}(OTC_t)$
6.b
6.a
$E_{X_{C,i}}(X_{M,j})$
7
$E^{-1}_{X_{M,j}}(Y_1) = P_t$
Product P_t is disclosed to C
Delivery is completed
Delete and replace entries $X_{M,j}$ and $Y_{M,j}$ from ECS

Fig. 4. Fair exchange protocol between the consumer and the merchant

- **Step 3:** The customer forwards OTC$_t$ to the ECS.
- **Step 4:** the ECS sends OTC$_t$ to the OTC ATM to verify its validity and provide its value to the ECS.
- **Step 5:** The OCT ATM verifies the validity of OTC$_t$. if it is valid, it will provide the ECS with its value, else it declares the invalidity of OTC$_t$.
- **Step 6:** the ECS receives the value of the OTC$_t$ and verifies if it is equal to the ordered digital product value. If it is not the case, it rejects and aborts. Else, it provides the merchant with the OTC$_t$ and the customer with the decryption key.

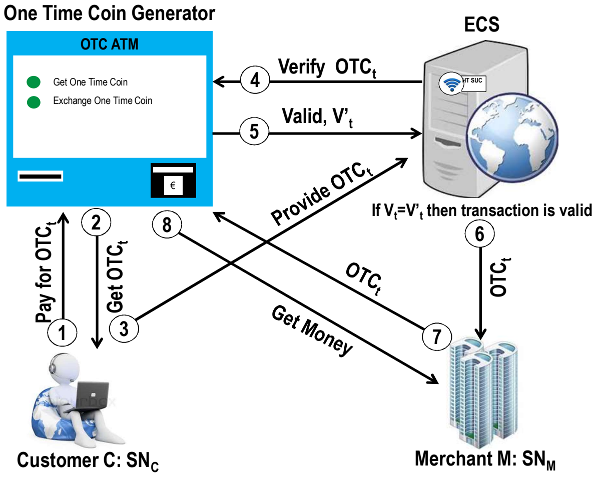


Fig. 5. Payment management system

V. Conclusion

A fair and anonymous electronic e-commerce system dealing with e-goods on open networks is presented. The key operating entities of the transactions are physical clone-resistant Commercial Hardware-Tokens (CHTs) based on Secret Unknown Cipher (SUC) technique. The CHTs accommodate unique digital SUCs as security anchors. The CHT is made clone-resistant by an initial irreversible single-event personalization process as a responsibility of a trustable CHTs Dealer. A dealer-based operation model should make the dealer play the role of just a mediator who takes the responsibility for provable CHT-Authentication without being able to reveal the anonymous users of the CHTs. Such CHTs offer a high degree of anonymity up to a perfect anonymity if the tokens are used just one time. The SUC technique allows protocols to act as agents running the transactions and offering in worst case clear tracing of responsibilities in dispute cases. The intended CHT is expected to be realizable at low-price when using the emerging non-volatile FPGA SoC technologies. The CHTs are also highly resilient as digital replacements for the traditional analog PUF technologies.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Www.Bitcoin.Org*, p. 9, 2008.

[2] F. Reid and M. Harrigan, “An analysis of anonymity in the bitcoin system,” *Secur. Priv. Soc. Networks*, pp. 197–223, 2013.

[3] G. O. Karame, E. Androulaki, and S. Capkun, “Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin.,” *IACR Cryptol. ePrint*, pp. 1–17, 2012.

[4] J. Liu, W. Li, G. O. Karame, and N. Asokan, “Towards Fairness of Cryptocurrency Payments,” 2016, no. September.

[5] R. Maes and I. Verbauwhede, “Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions,” in *Towards Hardware-Intrinsic Security*, no. 71369, Springer, 2010, pp. 3–37.

[6] A. Wael and M. Ayoub, “Physical and Mechatronic Security, Technologies and Future Trends for Vehicular Environment,” in *VDI-Fachtagung Automotive Security, VDI Berichte*, 2017, vol. 2310, pp. 73–95.

[7] W. Adi, “Clone-resistant DNA-like secured dynamic identity,” in *Bio-inspired Learning and Intelligent Systems for Security, 2008. BLISS'08. ECSIS Symposium on*, 2008, pp. 148–153.

[8] A. Mars, W. Adi, S. Mulhem, and E. Hamadaqa, “Random stream cipher as a PUF-like identity in FPGA environment,” in *Seventh International Conference on Emerging Security Technologies (EST)*, 2017, pp. 209–214.

[9] A. Mars and W. Adi, “Converting NV-FPGAs into Physically Clone-Resistant Units by Digital Mutations,” *Submitt. to IEEE Trans. Very Large Scale Integr. Syst.*, 2019.

[10] A. Mars and W. Adi, “New Family of Stream Ciphers as Physically Clone-Resistant VLSI-Structures,” *Cryptography*, 2019.

[11] W. Adi, A. Mars, and S. Mulhem, “Generic identification protocols by deploying Secret Unknown Ciphers (SUCs),” in *2017 IEEE International Conference on Consumer Electronics - Taiwan, ICCE-TW 2017*, 2017, pp. 255–256.

[12] W. Adi, A. Mars, and S. Mulhem, “Identification Protocols by Deploying Secret Unknown Ciphers (SUCs),” 10 2017 005 422.3, 2017.

[13] E. Androulaki, T. Mentor, and S. Bellovin, “A Privacy Preserving ECommerce Oriented Identity Management Architecture,” 2011.

[14] M. Ike and K. Sarac, “PPEP: A deployable privacy preserving E-commerce protocol for electronic goods,” *6th Int. Conf. Commun. Netw. Secur. ICCNS 2016*, pp. 101–109, 2016.

[15] A. Rial, “Privacy-Preserving E-Commerce Protocols,” KU Leuven, 2013.

[16] D. Konar and C. Mazumdar, “Generalized GSR model of fair exchange in E-contracting,” in *2009 International Symposium on Collaborative Technologies and Systems, CTS 2009*, 2009.

[17] S. Ketchpel, “Transaction Protection for Information Buyers and Sellers,” in *Proceedings of the Dartmouth institute for advanced graduate studies*, 1995.

[18] N. Asokan, M. Schunter, and M. Waidner, “Optimistic protocols for fair exchange,” in *Proceedings of the 4th ACM conference on Computer and communications security - CCS '97*, 1997, pp. 7–17.

[19] A. Nenadić, N. Zhang, B. Cheetham, and C. Goble, “RSA-based certified delivery of e-goods using verifiable and recoverable signature encryption,” *J. Univers. Comput. Sci.*, vol. 11, no. 1, pp. 175–192, 2005.

[20] I. Ray, I. Ray, and N. Natarajan, “An anonymous and failure resilient fair-exchange e-commerce protocol,” *Decis. Support Syst.*, vol. 39, no. 3, pp. 267–292, 2005.

[21] I. Ray and I. Ray, “An optimistic fair exchange E-commerce protocol with automated dispute resolution,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1875, pp. 84–93, 2000.

[22] H. Pagnia and F. Gärtner, “On the impossibility of fair exchange without a trusted third party,” *Darmstadt Univ. Technol. Dep. Comput. Sci. Tech. Rep. TUD-BS-1999-02*, no. TUD-BS-1999-02, 1999.

[23] A. Mars and W. Adi, “Clone-Resistant Entities for Vehicular Security,” in *IEEE 13th International Conference on Innovations in Information Technology (IIT)*, 2018.