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

- Step 3: The customer forwards OTC_t to the ECS.
- Step 4: The ECS extends the OTC_t to the OCT ATM to verify its validity and provides its value of 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 and verifies if it is equal to the ordered digital product value. If it is not the case, it rejects and aborts the transaction. Otherwise, it provides the merchant with the decryption key.

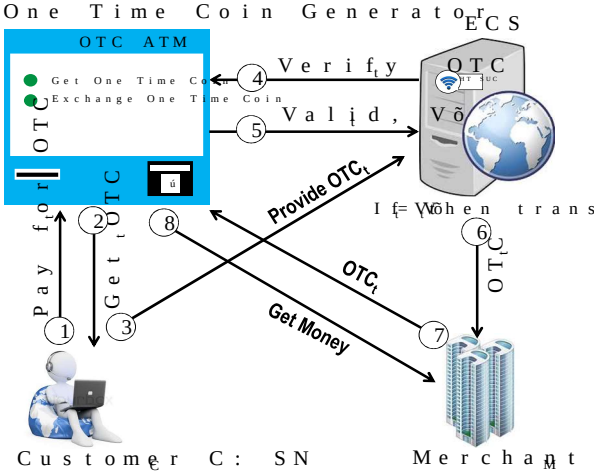

Fig. 5. Payment management system

V. Conclusion

A fair and anonymous electronic commerce protocol for dealing with e-goods on open networks is presented. The operating entities of the protocol are Clone-resistant Commercial Hardware Tokens (CHTs) and Secret Unknown Cipher (SUC) to accommodate unique digital transactions. The CHT is made clone-resistant through the event personalization process and is responsibility of trustable CHTs Dealer. A dealer should make the dealer play fair since he takes the responsibility for CHTs without being able to reveal the anonymous users of CHTs. Such CHTs offer a high degree of assurance to perfect anonymity if the tokens are tamper-proof. SUC technique allows protocol users to act as agents running transactions and offering responsibilities in dispute cases. The protocol is expected to be realizable at low price when using the emerging non-volatile FPGA technologies. The CHTs are also highly resilient with digitally altered circuitry to traditional analog PUF techniques.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," www.bitcoin.org, 2008.

[2] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," in Security and Privacy in Social Networks, Springer, 2013, pp. 197–223.

[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 Cryptology ePrint Archive, vol. 2012, p. 248, 2012.

[4] Z. Liu, W. Li, G. O. Karame, and S. Capkun, "Fast Cryptocurrency Payments," 2016, no. 2016/1043.

[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, Springer, 2010, pp. 3–37.

[6] A. Wael and M. Ayoub, "Physical Unclonable Technologies and Future Trends for Fachtagung Automotive Security," vol. 2017, p. 73195.

[7] S. Clarke, "Bio-inspired Learning and Intelligent Systems for Security," BLISS'08. ECSIS Symposium on, pp. 141–153.

[8] A. Mars, W. Adi, S. Mulhem, and S. Sharieh, "Everything you always wanted to know about cipher as a PUF-like identity," in International Conference on Emerging, 2017, pp. 209–214.

[9] A. Mars and W. Adi, "Converting Silicon Physical Resistant Units Symbol to Digital Data for Large Scale Integr. Syst.

[10] A. Mars and W. Adi, "New Family of Silicon Physical Clone-Resistant Cryptographic Primitives," 2019.

[11] W. Adi, A. Mars, and S. Mulhem, "Secure Hardware by deploying Secret Unknown Ciphers," in International Conference on Consumer Electronics-TW, 2017, pp. 255–256.

[12] W. Adi, A. Mars, and S. Mulhem, "Secure Hardware Deploying Secret Unknown Ciphers," 2017.

[13] E. Androulaki, T. Mentor, and S. Capkun, "Privacy-Preserving E-Commerce Oriented Identity Management," 2010.

[14] M. Ike and K. Sarac, "PPEP: A privacy-preserving e-commerce protocol," in Int. Conf. Comput. Commun. Netw. Secur., pp. CCNS 2012–2016, 2016.

[15] A. Rial, "Privacy-Preserving E-Commerce Protocols," 2013.

[16] D. Kania and C. Mazumdar, "Cheque Transaction (CHT) Protocol for Secure Collaborative Technique," Int. Technol. Manag. Rev., vol. 7, no. 2, p. 79, 2018.

[17] S. Asokan, "Transaction Protocols for Trading Goods in Untrusted Systems," 2000.

[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, 1997, pp. 7–17.

[19] A. Nenadić, N. Zhang, B. Cheetham, and C. Goble, "Auditing privacy-preserving e-commerce transactions," in Computer Security Applications Conference, 21st Annual, 2005, pp. 10–pp.

[20] S. Brands, "Rapid demonstration of linear relations connected by boolean operators," in Advances in Cryptology—EUROCRYPT'97, 1997, pp. 318–333.

[21] D. Chaum, "Blind signatures for untraceable payments," in Advances in cryptology, 1983, pp. 199–203.

[22] H. Pagnia and F. Gärtner, "On the impossibility of fair exchange without a trusted third party," Technical Report TUD-BS-1999-02, Darmstadt University of Technology, Department of Computer Science, 1999.