Trusted Electronic Signature According to Thai Laws Using UTXO Blockchain

Utharn Buranasaksee[1] and Pitchya Tangsombatvichit[2]

[1]Department of Computer Science, Faculty of Science and Technology
Rajamangala University of Technology Suvarnabhumi
Suphanburi, Thailand
e-mail: utharn.b@rmutsb.ac.th
[2]Department of Science, Faculty of Science and Technology
Rajamangala University of Technology Suvarnabhumi
Suphanburi, Thailand
e-mail: pitchya.t@rmutsb.ac.th

Abstract—Before the COVID-19 epidemic, getting the document printed and signed among the parties in the company are not that difficult. Since everyone is working onsite, taking several hours in the company collecting for the signature on paper is worth legal enforcement. During the epidemic, many government agencies and companies have adopted a new working style by having the employee remotely work from home. However, the employees do just have only online meetings, or can the employee remotely work become a real concern. In this case, getting the signature might take several days to weeks since the parties are remotely located. According to Thai laws, signing on important matters such as accounting or legal would still require a signature on the paper or a trusted electronic signature. The general solution is to leverage digital certificates issued by Certification Authority (CA) to provide trusted electronic signatures. In this paper, we analyze the cost and security of the existing solutions. A novel trusted electronic signature solution is proposed. We show that the proposed approach greatly reduces the cost while the security level is maintained.

Keywords: Trusted, Electronic Signature, Blockchain, Laws

I. INTRODUCTION

In Thailand, electronic signature has been legalized in Electronic Transaction Act since 2001 [1]–[4]. The act defines electronic signature and sets electronic signature to be honorable as a signature on a paper. According to the Act, an electronic signature [1] is defined as letters, characters, numbers, sounds, or any other symbols created in electronic form which is used in conjunction with electronic data to show the relationship between people and electronic data to identify an individual. The owner of the electronic signature relating to that electronic data and to show that such person accepts the statements in the electronic data. While the definition of electronic signature is broad and not specific in any technology. Many people are still attached to the signature canvas drawn on the file. Therefore, most of the employees feel comfortable to take several hours getting the document signed within the company to make the document be fully legal enforcement.

During the COVID-19 epidemic, the government tries to reduce the infection rate by having all the officers in government agencies remotely work from home [5]. Many private companies also mitigate the epidemic effects, by having a schedule for the employees to work onsite and work from home. Furthermore, the trends of working from home among the new generation employees are growing [6]. Since the situation has changed, getting the signature signed on the document might take several days or weeks because the documents either needed to be sent by post or waited for the parties to sign in a specific order depending on the workflow. As a result, an information system such as an electronic document (E-Document) comes into a major player where every user can sign in to view, download, and sign the document. However, signing the document in technical might be updating a row in the database that a particular user accepts the statements in the document. One of the major issues of this type of e-Document is that the system administrator has the power to override the user's acceptance of the statements in the document. Unlike signing on the paper, the user is repudiable to the statements on the e-Document system.

Electronic Transaction Act [1] categorizes the electronic signature into three types. The first type is a general electronic signature, which is defined in section 9 of the Act. The general electronic signature that electronic information stating the user's intention to the electronic data such as sending an email or drawing a signature canvas on the document file. The second type is a trusted electronic signature, which is defined in section 26 of the Act. This type makes use of a digital certificate issued by public key infrastructure (PKI) [7]. In the PKI, a user can independently generate a cryptographic key pair that consists of a private key and a public key. The user uses a public key to register on the system and signs the document using a private key. The other can obtains the user's public key to verify if the user signs the document. The third type is a trusted electronic signature, which is defined in section 28 of the Act. This type of electronic signature does not only use a digital certificate but the certificate is also issued by

the certification authority (CA). This could be done by having the CA identify the user identity after which the CA uses its private key to encrypt the user's public key. As the public keys of all the certificate authorities are shipped with major operating systems, the users can use their system to verify the identity of the other users.

Using cryptographic keys alone only does not satisfy the trusted electronic signature stated in section 26 and section 28, to satisfy a trusted electronic signature, there are the other two requirements. One is that the signing process of the system should allow the users to independently use the private key to sign the document without the intervention of any others including the system administrator. Therefore, the user's private key is required to reside on the user's device and the signing is processed by the user's device. As a result, only trusted electronic signatures in the Act have non-repudiation property as the signing process can be done only by a specific user with a specific device. The other is that the system should be able to detect if someone was tampering with the electronic signature. This would require another third-party node as a witness to record the existence of the document. The simple solution is to set up a new timestamp server to record the hash of the document.

The organization in this paper starts with the introduction in Section 1. Then we discuss the related technology and the existing solutions in Section 2. After that, the proposed solution using blockchain-based electronic signature is discussed in Section 3. In Section 4, we then evaluate the proposed solution according to the laws and compare it to the existing solutions on the market. Finally, the conclusion is made in Section 5.

II. Related Work

In this section, we first discuss the related research works that provide a core feature to trusted electronic signatures. Then, the existing solutions are explained how they construct trusted electronic signatures.

A. Related Technology

The PKI was first introduced to fix the security of the Internet [7]. The system is based on the chain of trust among CA. The root CA uses its private key to sign the public key of the sub-ordinate certificate authorities to make all the sub-ordinate certificate authorities trusted. Each CA is an entity that provides the chain of trust. While the Internet becomes larger over time, the developers are not concerned of leverage the PKI system [8]. This could be the cost of purchasing digital certificates from a small group of CA. Though the cost of the digital certificate has been significantly reduced over time as the Thai government has its own CA [9], [10], the major problem is still the cost model that we have to pay for security per user per year. After the advent of the blockchain in the financial industry [11], blockchain becomes the protocol of decentralization that allows anyone to create a trusted environment from the trustless environment [12]. The PKI leveraging Blockchain gain interested from many researchers by proposing the blockchain storing domain and their associated keys of X.509 certificate [13]–[17]. Since the blockchain protocol itself provides redundancy by nature, the blockchain-based PKIs are secured and solve the problem of being a single point of failure or being compromised. Furthermore, some research works improve the privacy issues by not linking identity to the public key [18]–[20]. However, none of the existing works have adopted the blockchain to store and manage electronic signatures directly.

B. Existing Solutions

According to the trusted electronic signature solutions that are compliant with Thai laws, we surveyed and categorized the existing solution into 4 solutions as shown in Table I. The first solution [21]–[23] is that every user in the system purchases their digital certificate from the CA. This solution exchanges the low maintenance cost with the high recurring cost of a digital certificate. The second solution [21]–[23] is to use the general electronic signature which has a flaw to the user's repudiation within the company as the current workflow could be replying to an email among the employees while the management only purchases the digital certificate from the CA. This solution is cheaper than the first one does, but the trusted electronic signature is applied to external documents only. The third solution [24] is that everyone including the management uses a general electronic signature to sign. After getting the signatures from all the parties, the system uses the digital certificate of the company to sign as the last party. This solution is cheaper than the second one does, as all the signatures are not trusted but the last version of the file can get a trusted certified icon in PDF reader. The last solution is that the company deploy its self-signed certificate and use this certificate to sign its employees which can be done using an open-source toolkit such as OpenSSL [25]. This solution is the cheapest as no digital certificate from CA is purchased. However, the cost of maintaining the PKI system might be a burden. In addition, all the systems need to separately install the company self-signed certificate which might not be possible with the external document.

Though the existing solutions were proposed to solve the cost of purchasing digital certificates from CA, the security is more compromised and limited when the cost is reduced. There are three main problems with the existing solution. First, all four solutions do not solve the certificate cost model which is per person per year. Second, the company needs to handle the problem of who is responsible for the cost of the digital certificate from the CA when the company needs to use the trusted electronic signature with its customers and its employees. For example, digital certificates are typically secured by a USB token. Therefore, it is the company's responsibility or the employee's responsibility in case of a lost token. The last problem is that when the users sign the document using its private key. There is no record elsewhere except the file. Therefore, the e-Document system needs to set up a trusted timestamp server such as the TEDA e-Timestamp server [26] to witness the file existence using its hash value.

TABLE I. EXISTING SOLUTION COMPARISON

Solutions	Certificate + Management cost	Trusted e-signature (Section 26)	Timestamp server
Everyone buys a certificate from CA.	High	Yes	Yes
Only management buys a certificate from CA.	Medium	No	Yes
The company buys a single certificate	Low	No	Yes
The company deploys its own PKI	Medium	Yes	Yes

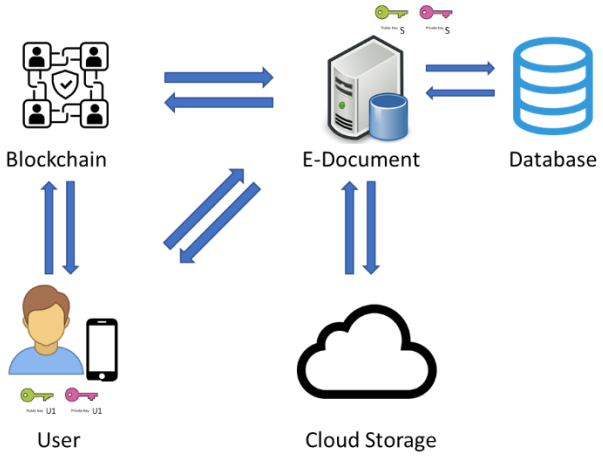

Figure 1. The system architecture

III. BLOCKCHAIN-BASED ELECTRONIC SIGNATURE

To solve the existing solution's problems, we proposed the method of using a public blockchain as an infrastructure to store and verify the electronic signature. Note that our method was registered as a patent application no. 1901000305 [27] and a petty patent application no. 1903002905 [28].

The system architecture of the blockchain-based electronic signature consists of 5 components which are shown in Fig. 1. 1) The user is the person who creates and uses an electronic signature. The user uses the mobile application which can generate the key pair according to the blockchain rule. The implementation of the mobile application is done as a crypto device with a user-defined memorized secret according to ETDA recommendation [29]. The mobile applications are available in both Play Store [30] and App Store [31] as shown in Fig. 2.

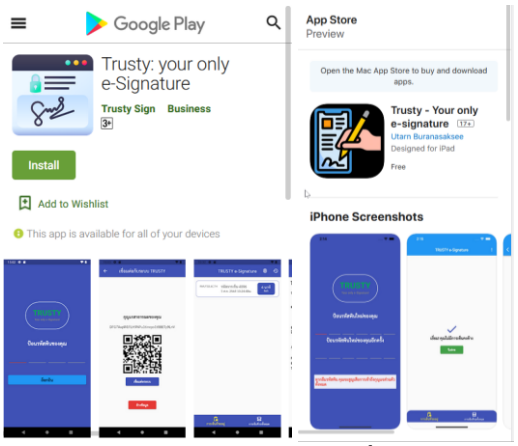

Figure 2. Mobile Application screenshot
(a) Play store (b) App Store

The key pair is encrypted using the combination of the user's secret and the developer's secret so that both the user and the developer cannot gain access to the key pair database directly. 2) Blockchain refers to a blockchain node that provides an API interface to the application and connects to the blockchain network. There are mainly two types of blockchain; one is account-based and the other is unspent transaction output (UTXO) based [32]. One of the important features in the UTXO blockchain is that the transaction creation process requires the output of the previous transaction to be an input of the newly created transaction. As a result, we take advantage of this requirement to create tightly coupled blockchain transactions between the user and the e-Document system. 3) E-Document is a web application that performs document circulation and document access control, as shown in Fig. 3. The e-Document also has a key pair generated that could represent the company. 4) Database is used to store the reference of the transaction to the blockchain. 5) Cloud storage is used to store the document to make the e-Document component stateless and scalable.

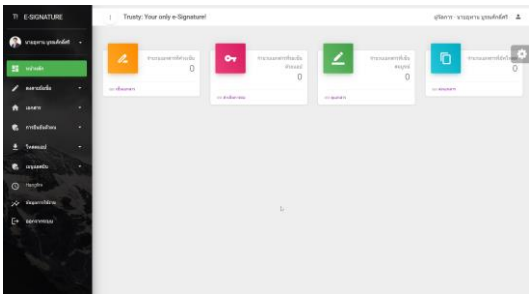

Figure 3. E-Document component screenshot

There are 7 steps for the workflow describing in Fig. 1. Step 1, the web administrator has a provisioned account for the user in the e-document system to use the existing authentication of the company such as Google Sign-in or Azure Active Directory. Step 2, the user submits the identification photos which will be stored in the cloud

storage. Step 3, the user installs the mobile application and generates the key pair. Step 4, the user submits his/her public key to the e-document system. At this point, the e-document system does not trust that the user holds the private key associated with the input public key. Therefore, the system generates a blockchain transaction storing the hash of identification photos called e-signature request and sends it to the user's public key in the blockchain. Figure 4 shows the structure of the e-signature request adapted from [27]. The e-document system uses a company private key to sign the transaction and sends it to the user's public key with the electronic signature data in the OP RETURN field. The OP_RETURN field is the data field available in the UTXO-based blockchain.

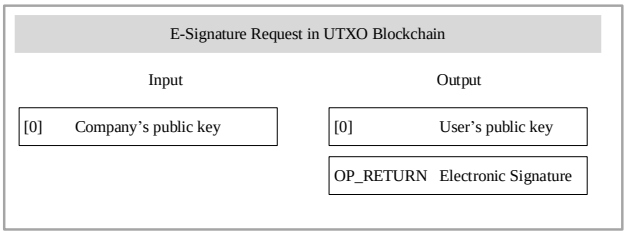

Figure 4. E-Signature Request Data Structure

Step 5, if the user's input public key is correct, the user could use the mobile application to download the transaction associated with its public key, create a new transaction called e-signature response shown in Fig. 5. In the e-signature response, which is adapted from [27], the user's device uses the output of the e-signature request to be as an output in an e-signature response while the output of the e-signature response is pointed back to the company's public key. For the electronic signature data, we design it to offload the computational task to support low processing power like a low-price phone or internet of things device. Therefore, the mobile application does not need to calculate the hash value as the value is stored in the transaction that was sent to the user's public key.

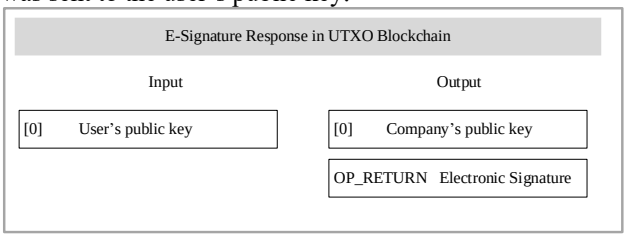

Figure 5. E-Signature Response Data Structure

Step 6, the user uses his/her private to sign a new transaction and send it to the blockchain. After that, in step 7, the e-document system can obtain the transaction using its public key. If the data store in the transaction is matched to the transaction that was sent by the e-document system, this proves that the user holds the private key according to the submitted public key.

Note that before using an electronic signature in our solution, the user must perform an identification process. The electronic signature on the document process is done as the same identification process does but the hash value is calculated and combined from the user's intention and the document using Merkle tree [33] is used instead of that from the identification photos.

IV. Proposed Architecture Evaluation

In this section, we evaluate the proposed architecture in 2 issues. One issue is the law-related issue and the other issue is the digital certificate issue.

A. Law-related issue

We evaluate if the electronic signature is compliant with the trusted electronic signature according to the Act. According to Electronic Transaction Act. section 26, the trusted electronic signature must satisfy all 3 requirements.

1) The electronic signature must link the owner

The e-document system does not trust the input public key that the user added to the system. But the e-document system makes specific information and sends it to the public key of the user via the blockchain. The user needs to use the private key to sign the transaction back to the blockchain. With the cryptographic process, any transactions sign by the private key can be linked to the owner.

2) The electronic signature must be under the owner control only

As the user does not send the electronic signature directly between the e-Document system. The signing process is performed in the user device, not in the server. Therefore, only the owner can use his/her electronic signature.

3) Electronic signature tampering can be detected.

Using blockchain protocol, it is known that the data store in the blockchain is immutable. Therefore, there is no chance that someone could tamper with the electronic signature.

B. Digital Certificate issue

The latter issue is whether the proposed solution can solve the problems in the existing solution. We compare the proposed solution to the existing solution on the market as shown in Table II.

1) Digital certificate cost model

As we proposed the electronic signature solution that leverages the blockchain, we recommend using a public blockchain as we need to have only one provisioned node connecting to the blockchain network. Therefore, every time the users identify themselves or the documents get signed, we need to pay the transaction fee to the blockchain network which changes the cost model to pay per sign instead of per user per year in the existing solution.

2) Digital certificate generation cost model

The proposed solution solves the certificate sovereign problem by allowing the users to generate a random key pair without any fee. Furthermore, the process of identification can be done without depending on a third party like CA. In addition, the keys are stored in the user's device such as mobile phone. The user could notice quickly if the mobile is lost.

3) Timestamp server requirement

The proposed solution makes use of the blockchain as a trusted witness as the electronic signature data sent between the user and the e-document is stored as a transaction in the blockchain. The blockchain acts as a trusted third party that has no conflicts of interest with anyone as it works by electronic instruction. In addition, each block in the blockchain is associated with its block time. The block time of the block is the timestamp that all nodes in the network record the same value. Therefore, there is no need to set up a timestamp server. Though the time precision could range from few seconds to a few minutes, the signing document does not require that high level of time precision. For example, the director signs the document at 10:00 AM but it would not matter if the block that contains the signature has a block time at 10:01 AM.

V. CONCLUSION

In this paper, we have discussed the need for electronic signatures in the epidemic era. Then, the shortcomings of existing solutions and the related work were discussed. After that, the workflow of the proposed approach was explained. Using a public blockchain, the proposed approach uses the blockchain as a third-party witness which removes the need for a separate timestamp server. We then evaluated the proposed method to Thai laws and compared it to the existing solutions. The proposed method showed that the trusted electronic signature according to Thai laws could be done without purchasing a digital certificate from CA, setting up company-owned PKI, and requiring a timestamp server.

TABLE II. PROPOSED SOLUTION COMPARISON

Solutions	Certificate + Management cost	Trusted e-signature (Section 26)	Timestamp server
Everyone buys a certificate from CA.	High	Yes	Yes
Only management buys a certificate from CA.	Medium	No	Yes
The company buys a single certificate	Low	No	Yes
The company deploys its own PKI	Medium	Yes	Yes
Use public blockchain as PKI (Proposed method)	Low	Yes	No

REFERENCES

[1] Electronic Transactions Development Agency, "Electronic Transaction Act. (1) 2001." https://ictlawcenter.etda.or.th/laws/detail/eta-act-2544 (accessed Oct. 01, 2021).

[2] Electronic Transactions Development Agency, "Electronic Transaction Act. (2) 2008." https://ictlawcenter.etda.or.th/laws/detail/eta-2-act-2551 (accessed Oct. 01, 2021).

[3] Electronic Transactions Development Agency, "Electronic Transaction Act. (3) 2019." https://ictlawcenter.etda.or.th/laws/detail/eta-3-act-2562 (accessed Oct. 01, 2021).

[4] Electronic Transactions Development Agency, "Electronic Transaction Act. (4) 2019." https://ictlawcenter.etda.or.th/laws/detail/eta-4-act-2562 (accessed Oct. 01, 2021).

[5] The Government Public Relations Department, "The government asks to work from home as much as possible." https://www.prd.go.th/th/content/category/detail/id/39/iid/16723 (accessed Oct. 02, 2021).

[6] Adobe Inc., "2021 Digital Trends Experience Index," 2021. https://business.adobe.com/content/dam/dx/us/en/resources/reports/digital-trends-2021-core/digital-trends-2021-full-report-EN.pdf (accessed Oct. 01, 2021).

[7] R. Perlman, "Overview of PKI trust models," *IEEE Network*, vol. 13, no. 6, pp. 38–43, Nov. 1999, doi: 10.1109/65.806987.

[8] H. Orman, "Blockchain: The emperors new PKI?," *IEEE Internet Computing*, vol. 22, no. 2, pp. 23–28, Mar. 2018, doi: 10.1109/MIC.2018.022021659.

[9] National Root Certification Authority of Thailand, "Thailand National Root Certification Authority." https://www.nrca.go.th/ (accessed Oct. 02, 2021).

[10] Thai Digital ID Co.Ltd., "Thai Digital ID Company Limited." https://www.thaidigitalid.com/homepage/ (accessed Oct. 02, 2021).

[11] S. Nakamoto, "Bitcoin A Peer-to-Peer Electronic Cash System," 2008, doi: 10.1016/j.irfa.2018.07.010.

[12] M. Pilkington, "Blockchain technology: Principles and applications," *Research Handbooks on Digital Transformations*, pp. 225–253, Sep. 2016, doi: 10.4337/9781784717766.00019.

[13] C. Fromknecht and S. Yakoubov, "CertCoin: A NameCoin Based Decentralized Authentication System 6.857 Class Project," 2014.

[14] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, "Cecoin: A decentralized PKI mitigating MitM attacks," *Future Generation Computer Systems*, vol. 107, pp. 805–815, Jun. 2020, doi: 10.1016/J.FUTURE.2017.08.025.

[15] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, *Blockstack: A Global Naming and Storage System Secured by Blockchains*. 2016. Accessed: Oct. 01, 2021. [Online]. Available: https://www.usenix.org/conference/atc16/technical-sessions/presentation/vesuna

[16] M. Y. Kubilay, M. S. Kiraz, and H. A. Mantar, "CertLedger: A new PKI model with Certificate Transparency based on blockchain," *Computers & Security*, vol. 85, pp. 333–352, Aug. 2019, doi: 10.1016/J.COSE.2019.05.013.

[17] A. Yakubov, W. Shbair, A. Wallbom, D. Sanda, and R. State, "A Blockchain-Based PKI Management Framework," 2018, Accessed: Oct. 01, 2021. [Online]. Available: https://orbilu.uni.lu/handle/10993/35468

[18] L. Axon, "Privacy-awareness in blockchain-based PKI," 2015.

[19] F. Li, Z. Liu, T. Li, H. Ju, H. Wang, and H. Zhou, "Privacy-aware PKI model with strong forward security," *International Journal of Intelligent Systems*, 2020, doi: 10.1002/INT.22283.

[20] L. Axon and M. Goldsmith, "PB-PKI: A Privacy-aware Blockchain-based PKI," 2017, doi: 10.5220/0006419203110318.

[21] Internet Thailand Co.Ltd., "One Authen." https://www.inet.co.th/services.php?s=one-authen (accessed Oct. 02, 2021).

[22] Fusion Solution Co.Ltd., "Design and Implement Digital E Signature Solution." https://www.fusionsol.com/products/digital-signature-solution/ (accessed Oct. 02, 2021).

[23] Digitech One Co.Ltd., "Digitech One Solutions." https://www.digitechone.co.th/solution/ (accessed Oct. 02, 2021).

[24] Creden Asia Co.Ltd., "Creden.co." https://creden.co/ (accessed Oct. 02, 2021).

[25] The OpenSSL Project Authors, "OpenSSL Cryptography and SSL/TLS Toolkit." https://www.openssl.org/ (accessed Oct. 02, 2021).

[26] Electronic Transactions Development Agency, “e-Timestamping - ETDA.” https://www.etda.or.th/th/Our-Service/Digital-Trusted-services-Infrastructure/TEDA/e-Timestamping.aspx (accessed Oct. 02, 2021).

[27] Department of Intellectual Property, “DIP :Thailand Patent Search.” https://patentsearch.ipthailand.go.th/DIP2013/view_public_data.php?appno=11901600280 (accessed Oct. 02, 2021).

[28] Department of Intellectual Property, “DIP :Thailand Patent Search.” https://patentsearch.ipthailand.go.th/DIP2013/view_public_data.php?appno=11931100513 (accessed Oct. 01, 2021).

[29] Electronic Transactions Development Agency, “ETDA Recommendation on ICT Standard for Electronic Transactions.” https://standard.etda.or.th/?p=11755 (accessed Oct. 02, 2021).

[30] Utharn Buranasaksee, “Trusty: your only e-Signature - Apps on Google Play.” https://play.google.com/store/apps/details?id=com.thaismartcontract.trusty (accessed Oct. 02, 2021).

[31] Utharn Buranasaksee, “Trusty - Your only e-signature on the App Store.” https://apps.apple.com/th/app/trusty-your-only-e-signature/id1587105289 (accessed Oct. 02, 2021).

[32] L. Brünjes and M. J. Gabbay, “UTxO- vs Account-Based Smart Contract Blockchain Programming Paradigms,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12478 LNCS, pp. 73–88, Oct. 2020, doi: 10.1007/978-3-030-61467-6_6.

[33] G. Becker and S. Ruhr, “Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis”.