Competitive Compliance with Blockchain

Sven Wohlgemuth*, Katsuyuki Umezawa†, Yusuke Mishina‡, and Kazuo Takaragi‡
*Research & Development Group, Hitachi, Ltd.
Yokohama, Kanagawa 244–0817, Japan Email: sven.wohlgemuth.kd@hitachi.com
†Department of Information Science, Shonan Institute of Technology
Fujisawa, Kanagawa 251–8511, Japan Email: umezawa@info.shonan-it.ac.jp
‡Cyber-Physical Security Research Center (CPSEC), National Institute of Advanced Industrial Science and Technology (AIST)
Koto-ku, Tokyo 135–0064, Japan Email: {yusuke.mishina, kazuo.takaragi}@aist.go.jp

***Abstract*—Authentication is essential for sharing information in IoT and its secondary use with AI-capable machines. The aim is to support humans in optimizing risk of supply chains for industrial manufacturing and service provisioning in a timely manner. The ultimate aim is sustainability. The problem for deciding on authentication is probably imperfect information on compliance. Its asymmetric implications of the meaning of contracts for secure information sharing may cause vulnerability of data breach and misuse. A traditional way to avoid harm of that asymmetry requires authentic and consistent sharing of audit information on violation of a certification policy to a centralized audit intelligence. This information sharing is, however, subject to the problem of single point of failure of the centralized audit intelligence.With our work on Security by Design, we show a non-central approach of clarifying accountability to reduce the risk caused by asymmetric implications of the meaning of contracts on authentication. Our signaling and screening scheme SK4SC provides personal digital evidences on compliance to multilateral policies on using information or in other words on trustworthiness. Blockchains are used to realize their symmetric distribution while users share risk on accountability with competition on incentives in a privacy-enhancing manner. Customer relationship management with royalty points, e.g., for eGovernment with taxation, is an example for using SK4SC as digital platform.**

Keywords–Security by design, risk management, accountability, identity management, social innovation

I. Introduction

In 2015 and 2017, cyberattack demonstrations were made to connected cars of Chrysler Jeep Cherokee and Tesla Model S. This became a warning that cyberattacks directly connected to life and death of people could occur in the era of Internet of Things (IoT). We have analyzed attacks and CVE vulnerability database of US MITRE Inc. using Artificial Intelligence (AI) natural language handling and show co-occurrence between attacks [1], [2]. In Security by Design of IoT, AI assistance seems to be pretty much effective. It often happens that gathering vulnerability design information on multiple enterprise products plays an important role. Then establishing both information sharing and trade secret (privacy) protection can be an important factor at AI assistance in manufacturing system (more widely, supply chain system) of IoT.

In general, IoT realizes a human-computer interaction (HCI) with abundance of information in a timely manner. IoT assigns this information to electronic identities as formalized representation for a cyber view on things and humans of a physical view on the world. The collected information is then provided to AI-capable machines to complete a defined model by searching for unknown information. The aim is to support humans in setting up adequate risk management with personal accountability. AI's superior capacity is on decidable problems and depends on authentic information or at least on information with a known error rate. The contribution of humans is, at start-up, to specify models with initial rules and criteria and then, while processing, to do expert handling that AI cannot do well. Taking full advantage of AI requires secure information sharing between models or in other words between cyber and physical representation of an environment. The selection of trusted partners depends on authentication of the claimed identity and stay in compliant to the security policy. Cybersecurity depends on authentication of defenders to adequately share security design information, e.g., a report about vulnerability and existence of active attacker.

Authentication assumes a secure exchange of an identity's information about the claimed property. This assurance and in rigorous sense a proof between the claiming identity as prover and information provider, on the one side, and a verifier as information consumer, on the other side, involves a scheme with registration, verification, and certification of personal information in accordance to a security policy. Providing a proof on security of an information exchange over an insecure channel – a secure protocol between two identities in an untrusted network – is the main objective of cryptography [3]. Our way for authentication in IoT by providing a bridge between a cyber and physical view on security is secure delegation of rights. We argue that our secure kernel for supply chains (SK4SC) realizes a probabilistic proof system for authentication and, in turn, a trustworthy supply chain in the series of design, procurement, manufacturing, inspection, shipping, operation and disposal, as a digital solution satisfying legal and economic demands in real world business [4].

Section II derives our way to cybersecurity with secure delegation of rights by SK4SC. Section III introduces SK4SC for symmetrically signaling and screening secure delegation of rights and its data provenance as Ground Truth. Section IV presents our cryptographic data provenance protocol with Hysteresis Digital Signature. Section V introduces effects of SK4SC for an open marketplace on information. Section VI proposes customer relationship management (CRM) with loyalty points as a use case for SK4SC as a digital platform. Section VII sums SK4SC up on usable HCI for a society.

II. Our way to cybersecurity

The aim of a secure system is to acceptably enforce safety and liveness properties for an information exchange

978-1-5386-9151-9/19/$31.00 ©2019 IEEE

in 'preventing bad things from happen' and 'that something good eventually happens' [5]. The aims of a proof system as a two-party protocol system are soundness and completeness. Concerning soundness, a compromised prover cannot show a trustworthy verifier authentication of non-authentic information. Concerning completeness, a prover can show authentication of given information to a verifier.

A. Security in a cyber view

Soundness for access control is shown, provided that the assumptions of type-safety with restrictions in formalization of rules, prohibition of cycles in information sharing, and irreversible removal of information are satisfied by the security policy for a protocol [6]. From now on, type-safety is used to mean "to ensure safety by distinguishing the types of things in IoT and limiting the operations allowed for each type". A proof on suitability of the cryptographic primitive requires its reduction to a one-way function with its inverse as a hard even if not NP hard mathematical problem [7]. The Dolev-Yao attacker model enhances this setting in that it tolerates vulnerable entities as active attackers [8] given in addition a unique cryptographic key pair for each identity, a public directory and no involvement of third party for encryption and decryption in the uniform protocol. Completeness is shown by a zero-knowledge proof (ZKP) system and witness values [9].

The random oracle model provides the representation of an unbreakable one-way function [10]. In case of a perfect ZKP, the random oracle as output of a simulator is identical to the real interaction between verifier and prover. In case of errors, a ZKP tolerates errors so that an attacker cannot be better than 50% in guessing the correct answer. This security proof of a protocol represents several symbolic executions with model checking of the required security and liveness properties. Latter is the superior capacity of AI-capable machines, whereas humans define the security policy of a protocol instance. For confidentiality of an information exchange, some proven authentic information of an identity is then re-used for encryption without disclosing the cryptograpic key [11]. The challenge is to show that a security proof holds acceptably in the corresponding physical view or in other words by cyber-physical systems (CPS).

B. Security in a physical view

Information on authentication of an entity consists of one or more of the factors of possession, knowledge, and inherent characteristics of claiming identity and their binding to a cryptographic key according to a standardized protocol [12]. Cryptographic hash function is considered for realizing the random oracle [10]. The suitability of the Dolev-Yao attacker model for security of protocols in the practice depends on soundness of its simulation. It needs to be indistinguishable whether a proof takes place in the ideal model of the cyber view or the system of the physical view. It is shown that this is impossible, if the collision-resistant hash encryption is used for encryption. A sound realization of Dolev-Yao is possible, if the hash function is used for digital signature [13]. Digital signature schemes realize accountability to an action of an identity certified by a digitally signed credential. Authentication is then decided by checking the certification path of the presented credential. Security of a cryptographic key exchange without a trusted third party (TTP) has not been demonstrated yet [14]. Authentication requires secure public key exchange for checking digital signatures by a public-key infrastructure (PKI) with a certification authority (CA) as TTP.

Language-based security [15] aims to justify this trust assumption on the reference monitor as the secure kernel of a system by a verifiable sound implementation of secure protocols. It makes use of one type-safe security policy for all users [6], a centralized reference monitor with perfect information about access to information, and certifying compiler to generate proof-carrying code. The transfer of the resulting credentials requires a public directory.

C. Accountability for cybersecurity

The problems for cybersecurity in providing a proof-system on security of an information exchange are versatile: Sometimes information on enforcement is imperfect in practice due to data breach via covert channels, phishing and spoofing of personal information, progress in scalable computing resources and algorithms for search in particular for cryptanalysis, and economic behavior. The challenge is suitable accountability to practical legal and economic requirements.

Technological development in search with quantum computing turns computational hard problems of one-way functions into solvable ones. Merkle's signature scheme is based on one-way hash function for the authentication tree by chained hash values. Its security and those of its improved realization [16] rely on a secure hash function. Quantum annealing dissolves this assumption [17] so that Merkle's signature scheme becomes vulnerable. Even though a compromise of a digital signature can be shown by the fail-stop signature scheme [18], it assumes the signer to show a compromise. In a proof on authentication, the signer of this information is, however, also its prover. In case of using the keyed-hash chain of Hysteresis Digital signature as an audit log of an identity's signatures, it is, however, still difficult for an attacker to result with falsification to a meaningful message [19]. Finding a data breach in a distributed system with current intrusion detection systems (IDS) implies an asymmetric distribution of audit logs to the audit intelligence of the central reference monitor, which can be a single weak point of failure. This reporting obligation is realizable by a usage control policy, whereas not all obligations are observable [20]. A rule-based IDS additionally requires authentic information about all potential attacks. Blockchain technology for reliable broadcast of any information implements the Byzantine fault tolerance protocol or delegate consensus to a central coordinator [21].

Sometimes imperfect is also the security policy model for detecting a data breach. Since language-based security follows soundness, it requires preventing false negative – there judged to be no data breach (negative) even actually there is one (positive) – on enforcing a given security policy for all protocol instances within a CPS. Completeness, however, derives a statistical statement as a mathematical logic proof on preventing false positive – there judged to be a data breach (positive) even though actually it is not (negative) – on enforcing a security policy for the given protocol instance. Completeness restricts the view on the symbolic execution traces to some protocol runs. It neither assumes a perfect system nor does it require the same security policy for any user. We achieve thereby a decidable problem within the Dolev-Yao model. Non-interactive ZKP scheme [22] is then used to

adapt to the asynchronous communication model of distributed systems. Completeness is then acceptable if the error rate of this statement as risk is acceptable for the given user. This represents individual risk preferences of humans as required for usable HCI. Even then additional access requests in the future, e.g, to support response and recovery activities with volunteers in times of a natural disaster, are not considered and so the policy for authentication is not given. Security policies need to be re-negotiable to support a proof for any situation.

On concluding our analysis, data breach is inevitable and so identity theft and misuse of information. Economics on information shows for imperfect systems a behavior of adverse selection and moral hazard [23]. In the first case, goods are indistinguishable, which leads to selecting cheaper goods with less quality. In the second case, a contract is either not entered or not enforced. An implication is market failure of CPS as considered for supply chains. We should answer this question: Is secure information sharing a matter of belief in policy enforcement and not of proven trustworthiness?

III. Signaling and Screening with Blockchain

In compliance to regulations for electronic processing of personal information [24], we assume that each identity's information system has been certified on type-safety by the contracting auditor. This is the initial screening on compliance with the resulting credential as signal. Our second assumption is that every identity has access to an electronic identity manager (iManager) as local reference monitor to decide on use of personal information including the personal key pair for accountability and anonymity [25]. Anonymity is necessary to impede compromise and misclassification, while being revocable in cooperation with the contracting auditor.

We adopt Hysteresis Digital Signature with signature log chain crossing [26] for our blockchains on AAA as public directory. We add a sound iManager with a certified device to check biometrics and bind them locally to a key pair of a traditional PKI [27]. Each crossing party stores the plaintext body of the signature target or its ciphertext in its record as evidence. We argue that if anonymizing this hash chain and proofing knowledge and correctness of a digital signature with ZKP, we achieve a one-way hash function.

Figure 1 illustrates our signaling and screening infrastructure SK4SC. There are two types of protocols: Sharing of information d and derived information d^* and d^{**} to be shown as authentic, and sharing of the witness values for a ZKP. Later are realized with personal digital evidences $\overline{d}$ and subsequent ones $\overline{d^*}$ and $\overline{d^{**}}$ as labels on events of enforcing a security policy in accordance to AAA of the IT security reference architecture [28], [29], [30]. These personal credentials on AAA are on (A)uthentication by use of anonymized digital signature keys, (A)uthorization on using d, d^*, and d^{**}, respectively, by delegation of rights in accordance to the contract of the corresponding information sharing, and (A)ccounting by audit log on granted access decisions. Their linkage by verifiable encrypted information about the contracting auditor allows to realize secure data provenance of the corresponding claim.

To achieve their symmetric distribution, they need to be reported and added to the public ledgers. We learn from the Byzantine consensus of the Bitcoin blockchain, where miners compete on the incentive of the next valid hash block while everyone can check the validity of the public hash chain [31].

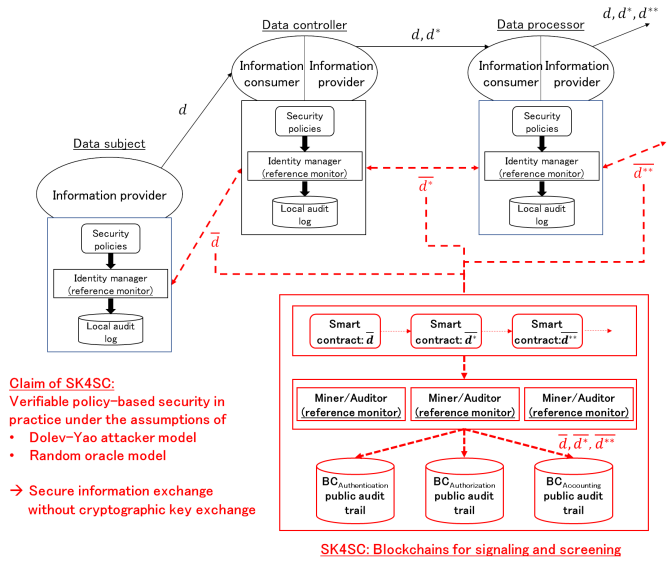

Figure 1. Our scheme for signaling and screening on authentication

If an attacker controls more than 50% of all miners, the ledger and so the witness values and, in turn, a ZKP can be forged. To check authorizations and authentication of identities, a miner needs to check if the presented credentials are in compliant to the authorization of the requester and if this identity's digital signature key is not compromised: Miners perform as an auditor a check of the data provenance of credentials. A new block is signed by an auditor O_A and represents a credential by itself. O_A is by its digital signature accountable for this proof-of-work. This provides for auditors O_A as stipulated by security regulations an additional functionality in acting as a miner O_M. In contrary to a traditional auditor, O_A has in general only knowledge about rules of information sharing.

As compensation for this task, the successful miner O_M or in general O_A gets a lump sum for the new block and a transaction fee for each transaction within the new block from each information provider. The information consumer pays for using d a financial value to information providers including the data subject, e.g., coin or profit sharing on the further processing of this information. In return, a block contains verified state transitions of information sharing transactions and so witnesses for authentication. These are incentives to follow the obligation on reporting and so this obligation of the security policies becomes observable for a verifier. By this procedure, SK4SC is the reference monitor with miners and symmetric distribution of secure data provenance.

IV. Secure Data Provenance of SK4SC

In addition to the Hysteresis Digital Signature scheme, other cryptographic building blocks of SK4SC are the (non-interactive) ZKP-based cryptographic protocols for anonymous credentials with Camenisch-Lysyanskaya (CL) signature and verifiable Camenisch-Shoup (CS) encryption scheme proven under the random oracle model [32]. The boot-up for the CL signature between the issuing party and the user starts from the traditional PKI. Then the CL signature scheme generates an anonymous credential from a set of attributes of the user, e.g., pseudonyms, cryptographic keys, biometrics, possessions,

data and everything necessary for its supply chain purpose. The advantage of the CL signature is that once the anonymous credential is issued, the user can select at one's own discretion the subset of its attributes and prove them to the verifying party in a variety of requirements. As an example, the range of the attribute can be proven without revealing the attribute value itself. The CS encryption comes from the need where the user should let a designated auditor confidentially knows some data to be used in case of a possible dispute later on. The advantage of the CS encryption is that the use of the designated auditor's public key is verifiable on the ledger by every party.

A. Initial setting: Signature, encryption, and hash chain

We adopt the definition of each parameter from the anonymous credential system of [32]. Credential issuing organization O_I generates a cryptographic key pair for CL signature.

- Secret key sk: prime numbers p, q
- Public key $pk : (n, R_0, ..., R_{L-1}, S, Z)$, where $n = pq$, L is the number of attributes to be issued per identity, and $R_0, ..., R_{L-1}, S, Z$ are random numbers generated separately.

Data controller O_C similarly generates a secret and a public key for the CL signature with prime numbers p' and q' generated separately. Auditor O_A generates a secret and a public key of the verifiable CS encryption with prime numbers P and Q generated separately.

- Secret key $Sk : (hk, N, x_1, x_2, x_3)$, where $N = PQ, x_1, x_2, x_3$ are random numbers less than $N^2/4, hk$ is a hash key for hash function H.
- Public key $Pk : (hk, N, y_1, y_2, y_3)$, where $y_1 = g^{x_1}, y_2 = g^{x_2}, y_3 = g^{x_3}, g'$ as a random number less than N^2 and $g = (g')^{2N}$.

Let $h = (1 + N \ mod \ N^2) \in Z^*_{N^2}$. To encrypt a message $m \in [N]$ with label $L \in \{0,1\}^*$ under a public key as above, choose a random $r \in_R [N/4]$ and compute $u = g^r$, $e = y_1^r h^m$, and $v = abs((y_2 y_3^{H_{hk}(u,e,L)})^r)$. Cipher is (u, e, v).

We strengthen the Hysteresis Digital Signature scheme by adopting it with blinding the use of the identity's signature key and generating the key pair in an XOR operation with a random number and O_I's unique pattern: his or her biometrics or PUF, respectively. The XOR operation works as a one-time pad and is therefore information-theoretic secure. Even if an attacker finds a collision to the hash of the first key, knowledge about the used characteristic pattern and random number is necessary for a compromise of O_I's master identity. Blinding is done by verifiable encryption of each block with pk_{O_A} of the traditional auditor O_A of O_I. As result, the CS signature of O_I within the Hysteresis Digital Signature scheme is a hash chain of anonymous credentials and verifiable on its authentication.

B. Signaling: Digital evidences and their data provenance

Normally, the history of users who sent and receive d_S according to credentials issued by O_I is recorded in the block chain ledger in the form of anonymous $nym_0, nym_1, nym_2, ...$ Also, O_I can link the identity of O_j presented at the time of issue of the credential $cred_j$ with the anonymous nym_j. Therefore, O_I can obtain the identity list of the users who sent and received d_S and issued the assigned credentials. This connects the graph of the authorization to some security design information d_S of the data subject O_S to the digital evidence for further data sharing of d^*_S. d^*_S is derived information by secondary use of d_S aggregated with other data. By the mechanism of anonymous credential, O_I knows only a part of the attributes of the requester, i.e., O_C or O_P for issuance in plain text form. In other words, attributes are classified into three types, known, commitment, and hidden, and O_I knows only known-attributes in plain text form among them. Other commitment and hidden attributes use the same mechanism as bit commitment and are approved without showing clear text. The requester cannot deny that it has applied for the attributes.

The record of credential issuance is encrypted with the public key of the auditor O_{A_I} of user O_I and recorded in the block chain ledger after a miner has successfully digital signed these data. It is assumed that O_I and O_{A_I} already are in a contractual relationship for the purpose of auditing of O_I. For authentication of digital signature key, O_I proposes this new signature audit log for the next block of the distributed ledger $BC_{Authentication}$. For any entity O_j, the record includes $context_{I,j}$ and $\{m_{j,k}, k \in def\}$. def is a set of attributes that can be audited later. Let enc_D be the encryption function when using the public key of O_{A_I} in the CS encryption. Let $sign_C$ be the signature function using the private key of the data controller in traditional PKI. Here a data controller is a party who, according to domestic law, is competent to decide about the contents and use of personal data, regardless of whether or not such data is collected, stored, processed, or disseminated by that party or by an agent on its behalf [24].

Calculate $m = context_{A_I,j} \ || \ \{m_{j,k}, k \in def\}$, $t = enc_D(m) = (u, e, v)$, $M_j = (nym_j \ || \ t)$, $B_j = H(B_{j-1} \ || \ M_j)$, $S_{I,j} = sign_c(B_j)$ and generate ZKP values: $SPK = \{r, m : u = g^r, e = y_1^r h^m, \ and \ v = abs((y_2 y_3^{H_{hk}(u,e,L)})^r)\}$. This proves encryption of m using O_{A_I}'s public key without that the verifier knows the concrete value of m. O_I proposes $(M_j, B_j, S_{I,j})$ and SPK to the public hash chain as blockchain ledger. The miner O_A confirms the validity of $(M_j, B_j, S_{I,j})$ and SPK and adds it with the miner's signature to the ledger. O_S holds the credential and related attribute information about d_S. Adding credentials to the public ledgers $BC_{Authorization}$ and $BC_{Accounting}$ is done accordingly.

C. Screening: Audit of data provenance as secure search

Figure 2 illustrates the procedure of an audit by secure search, which is realized by the protocol called *ProofInequality* [32]. Information provider O_{IP} generates a random number v', calculates $U = S^{v'} \prod_{k \in (A_c \cup A_h)} R_k^{m_{j,k}} (mod \ n)$, and sends it to the requesting information consumer O_{IC} together with $\{m_{j,i}, i \in A_k\}$ and $context_j$. O_{IP} generates a random number $\{r_k, k \in A_c\}$, then generates O_{IP}'s anonymous name $nym_j = g^{m_{j,1}} h^s$, domain anonymous name $dNym_j = g_{dom}^{m_{j,1}}$, commits $\{C_{j,k} = Z_k^{m_{j,k}} S_k^{r_k}, k \in A_c\}$, and send them to O_{IC}. O_{IP} sends the ZKP values of Fiat-Shamir heuristic with respect to attribute values $\{m_{j,i}, \forall i \in (A_c \cup A_h)\}$. For above *ProofInEquality*, the ZKP that a certain attribute value m is $m > m_r$ is given with $\triangle = m - m_r - 1$ and $a = 1$: Calculate u_1, u_2, u_3, u_4 such that $\triangle := u_1^2 + u_2^2 + u_3^2 + u_4^2$. Let

$r_\triangle, r_i \in_R \{0,1\}^{l_n + l_\emptyset}$.

$$T_1 := Z^{u_1} S^{r_1} (mod\ n)$$
$$T_2 := Z^{u_2} S^{r_2} (mod\ n)$$
$$T_3 := Z^{u_3} S^{r_3} (mod\ n)$$
$$T_4 := Z^{u_4} S^{r_4} (mod\ n)$$
$$T_\triangle := Z^{\triangle} S^{r_\triangle} (mod\ n)$$
$$\alpha = r_\triangle - \sum_{j=1}^{4} u_j r_j$$
$$SPK\{(m, r_\triangle, \{u_1, ..., u_4\}, \{r_1, ..., r_4\}, \alpha) :$$
$$\wedge\, T_\triangle^a Z^b \equiv \pm Z^m (S^a)^{r_\triangle} (mod\ n)$$
$$\wedge\, T_j \equiv \pm Z^{u_j S^{r_j}} (mod\ n), for\ j = 1, 2, 3, 4$$
$$\wedge\, T\triangle \equiv T_1^{u_1} ... T_4^{u_4} S^{\alpha} (mod\ n)\}(n_1)$$

Since *ProofInequality* is not limited to $m > m_r$, SPK can be configured similarly for another inequality. An audit of the data provenance is done recursively for each certification path of the corresponding credentials in accordance to the contract.

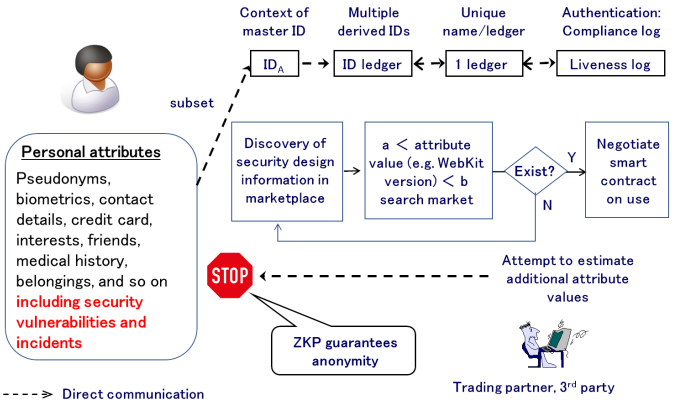

Figure 2. Secure search with digital evidences from SK4SC

V. An Open Secure Marketplace on Information

The current way for secure information sharing without cryptography is anonymization [33]. It should reduce vulnerability of the data subject while making the anonymized data available, e.g., as Open Data. Anonymization is done by randomization by adding noise or generalization by removing information. This modification is not known to an information consumer. It increases the statistical error rate of secondary use, since optimal anonymization is a NP hard problem [34]. Our way with SK4SC has another effect: Sharing information is in economics a trade of property rights on shared goods. With our scheme on secure delegation of rights, we introduce the verifiable kernel as the trusted computing base for a secure open marketplace on trading rights on use of security design information including secondary use. This introduces price discrimination for a trade of rights in addition to the current practice of k-anonymity and differential privacy.

Symmetric distribution of information on authentication with SK4SC counteracts vulnerabilities of adverse selection and moral hazard [23]. Adverse selection occurs in IoT if information is indistinguishable. With SK4SC and secure search information is distinguishable. Public authentic attributes of an identity can then be used as a kind of public key for secure exchange of symmetric encryption key in accordance to identity-based encryption [11], whereas the corresponding private key remains confidential with ZKP and the symmetric key in accordance to the identity-based encryption scheme. Moral hazard is still possible, however SK4SC then provides no evidence on authentication. SK4SC contributes to an open marketplace for trading rights on using security reports. Its digital evidences are Open Data for privacy-enhancing information flow control.

VI. Potential Use for CRM

The information usage model of SK4SC with incentives is similar to CRM with royalty points. Here, royalty is a counter value payback paid by a user who uses specific rights to a person having rights. A royalty program aims to commit customers to the royalty program provider and its partner companies. These companies delegate their CRM to the royalty program provider. The royalty program provider manages the profiles of the customers, offers personalized services and advertisements based on aggregated personal information, and rewards customers with royalty points, whenever they buy goods or services at partner companies. Royalty points are a virtual currency. The royalty program provider sells also royalty points to its partners, if they want directly give them as an incentive to information providers. Each customer has a registered unique identity certified by the royalty provider and shown with the royalty card as credential. In case of frequent-flyer programs, such an incentive program has shown competitive advantage with price discrimination [35]. It allows an air carrier to charge higher prices, push cheap competitors at its dominant hub airport aside, and leads also to an increased benefit of partners. Authentication and confidentiality of personal information is of interest for royalty program providers. If it is possible to aggregate customers' information without the royalty program provider, latter would not benefit from its secondary use.

Figure 3 illustrates the expected effect of SK4SC to CRM with royalty points. The example is eGovernment with taxation. SK4SC realizes a Chinese-Wall between supply chains of information of a citizen's transactions with his or her royalty program identity. The royalty program provider is the root CA of a traditional PKI for identity management, who provides SK4SC as the trust infrastructure. Actually, this is the role of the government with accountability for providing authentic registered electronic identities. The master identity of each user is the national identity or visa, respectively. The government issues royalty points as virtual money of the national currency. Thereby it controls the cash flow of national currency. Information consumers buy royalty points from the government, i.e., paying a kind of tax for providing information services within this infrastructure. A registered entity gets royalty points as a payment for documented information processing, or earn them from the government as compensation for being an accountable successful miner. Any registered identity is free to contribute.

VII. Summary

The challenge of a society with imperfect information is how to secure the best use of resources known to any of the members of a society, for ends whose relative importance

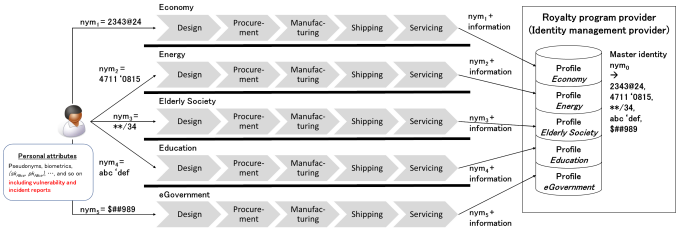

Figure 3. Expected effect of using SK4SC for CRM with royalty points

only these individuals know [36]. We introduce with SK4SC a probabilistic proof system with blockchain for cybersecurity. Secure search proves trustworthiness of potential partners. Compliance to privacy as information self-determination is then a competitive factor for selection. We are looking forward to evaluating its effects on usable HCI for knowledge societies.

ACKNOWLEDGMENT

This work was supported by Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), "Cyber-Security for Critical Infrastructure" (funding agency: NEDO).

REFERENCES

[1] Y. Mishina, K. Takaragi, and K. Umezawa, "A Method of Threat Analysis for Cyber-Physical System using Vulnerability Databases," in 18th Annual IEEE Symposium on Technologies for Homeland Security (HST '18), 2018.

[2] K. Umezawa, Y. Mishina, S. Wohlgemuth, and K. Takaragi, "Threat Analysis using Vulnerability Databases – Matching Attack Cases to Vulnerability Database by Topic Model Analysis –," in The Third International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2018), 2018.

[3] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," CACM, vol. 21, no. 12, 1978, pp. 993–999.

[4] J. Boyens, C. Paulsen, R. Moorthy, and N. Bartol, "Supply Chain Risk Management Practies for Federal Inofmration Systemsn and Organizations," NIST Special Publication 800-161, 2015.

[5] M. R. Clarkson and F. B. Schneider, "Hyperproperties," Journal of Computer Security, vol. 18, no. 6, 2010, pp. 1157–1210.

[6] R. S. Sandhu, "The Typed Access Matrix Model," in Prof. of the 1992 IEEE Smposium on Security and Privacy. IEEE, 1992, pp. 122–.

[7] M. Bellare, "Practice-Orinted Provable-Security," in ISW 97, ser. LNCS, vol. 1396. Springer, 1998, pp. 221–231.

[8] D. Dolev and A. C. Yao, "On the security of public key protocols," IEEE Trans. Inf. Theory, vol. 29, no. 2, 1983, pp. 198–208.

[9] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems," J. ACM, vol. 38, no. 2, 1991, pp. 690–728.

[10] M. Bellare and P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," in 1st ACM CCS. ACM, 1993, pp. 62–73.

[11] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in Advances in Cryptology. CRYPTO 1984, ser. LNCS, vol. 196. Springer, 1984, pp. 47–53.

[12] ISO/IEC, ISO/IEC 24761:2009 Information technology – Security techniques – Authentication context for biometrics, ISO/IEC Std., 2009.

[13] M. Backes, B. Pfitzmann, and M. Waidner, "Limits of the Reactive Simulatability/UC of Dolev-Yao Models with Hashes," IACR Eprint archive, 2006. [Online]. Available: http://eprint.iacr.org/2006/068

[14] E. Freire, D. Hofheinz, E. Kiltz, and K. Paterson, "Non-Interactive Key Exchange," in PKC 2013, ser. LNCS, vol. 7778. Springer, 2013, pp. 254–271.

[15] F. B. Schneider, G. Morrisett, and R. Harper, "A Language-Based Approach to Security," in Informatics 10 Years Back, 10 Years Ahead, ser. LNCS, vol. 2000. Springer, 2001, pp. 86–101.

[16] J. Buchmann, L. C. C. Garcia, E. Dahmen, M. Döhring, and E. Klintsevich, "CMSS – An Improved Merkle Signature Scheme," in INDOCRYPT 2006, ser. LNCS, vol. 4329. Springer, 2006, pp. 349–363.

[17] K. Imafuku, T. Katashita, S. Kawabata, H. Koike, and M. Maezawa, "Application of Quantum Annealer to Circuit Satisfiability Problem and Cryptanalysis," Poster at AIST-RIKEN 2nd Quantum Technology Innovation Core Workshop, Tokyo, Japan, Nov. 2016.

[18] B. Pfitzmann, "Fail-stop Signaturs; Principles and Applications," in Proc. Compsec '91, 8th world conf. on computer securitym audit and control. Elsevier, 1991, pp. 125–134.

[19] D. Basin, K. Miyazaki, and K. Takaragi, "A Formal Analysis of a Digital Signature Scheme," in Integrity and Internal Control in Information Systems VI. IICIS 2003, ser. IFIP, vol. 140. Springer, 2003, pp. 31–47.

[20] M. Hilty, D. Basin, and A. Pretschner, "On obligations," in ESORICS'05, ser. LNCS, no. 3679. Springer, 2005, pp. 98–117.

[21] J. Liu, W. Li, G. O. Karame, and N. Asokan, "Scalable Byzantince Consensus via Hardware-assisted Secret Sharing," IEEE Transactions on Computers, 2018.

[22] U. Feige, D. Lapidot, and A. Shamir, "Mulitple Non-Interactive Zero Knowledge Proofs Based on a Single Random String," in FOCS 1990. IEEE, 1990, pp. 308–317.

[23] J. E. Stiglitz, "Information and the Change in the Paradigm of Economics," The American Economic Review, vol. 92, no. 3, 2002, pp. 460–501.

[24] European Commission, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Official Journal of the European Union, vol. L 199, 2016, pp. 1–88.

[25] U. Jendricke and D. G. tom Markotten, "Usability Meets Security - the Identity-Manager As Your Personal Security Assistant for the Internet," in ACSAC '00. IEEE Computer Society, 2000, pp. 344–354.

[26] H. Toyoshima and K. Miyazaki, "Hyteresis Signature and Its Related Technologies to Maintain the Digital Evidence for Network Activities in Future Society," Journal of the National Institute of Information and Communications Technology, vol. 52, no. 1/2, 2005.

[27] A. Yamada, "A Generalization of ISO/IEC 24761 to Enhance Remote Authentication with Trusted Product at Claimant," in ICT Systems Security and Privacy Protection, vol. 455. Springer International Publishing, 2015, pp. 145–168.

[28] J. H. Saltzer and M. D. Schroeder, "The Protection of Information in Computer Systems," Proc. of the IEEE, vol. 63, no. 9, 1975, pp. 1278–1308.

[29] M. A. Harrison, W. L. Ruzzo, and J. D. Ullman, "Protection in Operating Systems," CACM, vol. 19, no. 8, 1976, pp. 461–471.

[30] OASIS, eXtensible Access Control Markup Language (XACML) Version 3.0, OASIS Standard Std., 2013.

[31] N. Stifter, A. Judmayer, P. Schindler, A. Zamyatin, and E. Weippl, "Agreement with Satoshi – On the Formalization of Nakamoto Consensus," Cryptology ePrint Archive, Report 2018/400, 2018.

[32] IBM Research Zurich Security Team, "Specification on the identity mixer cryprographic library, version 2.3.40," IBM Research Zurich, techreport, 2013.

[33] Article 29 Data Protection Working Party, "Opinion 05/2014 on Anonymisation Techniques. Adopted on 10 Apirl 2014," European Commission, Tech. Rep. 0829/14/EN WP216, 2014.

[34] G. Aggarwal, T. Feder, K. Kenthapadi, R. Motwani, R. Panigrahy, D. Thomas, and A. Zhu, "Approximation Algorithms for k-Anonymity," in ICDT 2005, 2005.

[35] M. Lederman, "Are Frequent-Flyer Programs a Cause of the "Hub Premium"?" Journal of Economics & Management Strategy, vol. 17, no. 1, 2008, pp. 35–66.

[36] F. Hayek, "The Use of Knowledge in Society," The American Economic Review, vol. 35, no. 4, 1945, pp. 519–530.