Towards making Private Banking Private: Updating Chaum's Vision on Banking

Yvo Desmedt*[1] and Aydin Abadi**[2]

[1] The University of Texas at Dallas
[2] University College London

Abstract. Chaum's vision on secure banking predated the internet, massive hacking, social networks, and obviously online banking. Today, investment advisers expect their clients to reveal all their assets information to them. Nevertheless, insider threats have undermined the privacy in the banking sector. The true scale of it is yet to be discovered. In this work, we revisit Chaum's vision to include these new aspects. We show how to increase privacy and protect against insider threats in this context. We conclude that a major revision of security in banking is needed. Moreover, we show how to increase privacy and protect against insider threats by proposing an Oblivious Transfer (OT) protocol in which the request is done in a distributed way, an aspect not considered before.

Keywords: privacy, oblivious transfer, pseudonyms, face recognition, cryptography.

1 Introduction

Insider attacks are real and imminent threats to banks and their customers. Insider adversaries may collude with and help external fraudsters. The data that insider adversaries can gather about their customers is extremely valuable. Although there have been ad-hoc proposals (e.g., employee training and penetrating testing) that aim to address the issue, the effectiveness of the proposals has never been scientifically evaluated and proven.

The "Swiss Leaks" [18] is a good example to illustrate the problem of insider leaks and at the same time the different viewpoints on privacy in the banking world. In the Swiss Leaks case, an insider (i.e., Mr Hervé Falciani) attempted to sell information about accounts held by over 100,000 clients and 20,000 offshore companies with HSBC in Geneva, Switzerland. Later, when he failed, he leaked the information to the public.

Today, we have essentially two models related to privacy in the banking world. In the Swiss one privacy is supposed to be absolute, while in the US system the government knows all assets. While the Swiss Leaks are well known, there are leaks in the US system too. For instance, in the case of "JPMorgan Chase Insider Thief" [10], a former JPMorgan Chase personal banker has been arrested by the FBI on charges that he stole customer account information (including customers'

* yvo.desmedt@utdallas.edu
** aydin.abadi@ucl.ac.uk

account balance) and sold it to an undercover informant. As another example, the largest federal credit union in North America, Canadian bank Desjardins Group, was the victim of an insider data breach that leaked information (e.g., transaction histories) of about 9.7 million members [22]. In 2022, Desjardins Group submitted a settlement agreement to the Superior Court of Quebec for approval which allowed for the amount of $200,852,500 to be paid out to eligible individuals who were affected by the leak [11]. However, if insiders manage to sell clients' information, then neither banks nor the public might ever find out that their information has ever been breached.

Thus, there is a pressing need to protect customers' data privacy from insiders in various sectors (e.g., healthcare, government, or airline); especially, in the financial sector that deals with considerable amounts of money. Doing so is the main goal of this paper (for details, see Sections 3 and 5).

While we propose a technique to increase privacy in the financial sector, we can as well revisit the topic in a broader context. Although Chaum's vision is credited for laying the foundations of Bitcoin and its variants, some of the approaches Chaum proposed are now outdated. Moreover, new security problems are arising besides privacy, the topic on which Chaum focused. We revisit some of these.

2 Revisiting Chaum's vision

2.1 Pseudonyms

One of Chaum's [5] main ideas was the use of pseudonyms. When it was proposed some regarded it as extreme. We now argue that the use of pseudonyms is completely outdated.

The biggest threat against privacy and the use of pseudonyms is facial recognition. Its use in the West has largely remained unnoticed. We illustrate the accuracy of the technology using a US example. The Obama administration made entering the US easier, for many, by having a pre-check which was a self service boot. The Biden administration has removed these. Instead, today people are recognized by a facial recognition system; the accuracy is so great that

"the system has stopped around 1,600 impostors from entering the country through airports and land borders" [19].

2.2 Social networks, smartphones, and webcams

The desire for privacy has clearly been undermined by social networks as stated by many[3]. Privacy has been further undermined by the use of cameras, such as webcams and CCTVs. Indeed, each modern smartphone has at least two.

Although some people use aliases on their social networks, often identities are easy to recover. For example, consider two comments made on some social network about some hotel where Financial Cryptography took place[4]. From the

[3] It is not the purpose of this paper to make a literature study of this. So, no one is cited.

[4] To avoid further undermining the anonymity of the authors of the two comments, the year of the conference is not revealed here.

comments, the time of the posting, the little information the authors released it is easy to guess who the two professors were who made these comments.

Another problem, besides privacy, is that social networks are used by scammers using social engineering. Today, people are transferring large sums of money to their internet friends, who are just scammers; one concrete example is Authorised Push Payment fraud [29,1]. There are other scams, such as the money mule scam, in which the victim helps money laundering. The problem with these scams is so grave that some countries, such as Singapore, have set up webpages, posters in metro stations, etc., to warn their citizens [26]. In the UK, some are suggesting to make banks responsible to compensate victims of scams [30].

2.3 Hacking

Chaum's paper predated the internet and massive hacking. Obviously, Chaum did not take the impact of hacking into account. Often hacking is making the news. We focus only on hacking in the context of this paper.

In the context of Bitcoins, there are many examples of people who lost their Bitcoins due to hacking [9,14,27]. Hacking also allows to access personal information, which is called "Identity Theft". Social engineering, which we already mentioned in Section 2.2, is also used. Identity Theft is becoming a serious problem. For example lately roughly 3 million ID thefts occurred due to the hacking of Optus [17], an Australian telecommunication company. Hacking is also used to obtain passwords, which allow the hacker to perform internet banking.

2.4 Insider threat

Secret Sharing (SS) [4,24] is an obvious useful technique that can be used to deal with insider treats. Although SS and insider threats predated Chaum's paper, Chaum ignored insider threats. However, as we have provided several examples of insider threats in financial sector in Section 1, a lack of mechanism that can deal with such threat can have serious repercussions for financial institutes and their clients. A survey conducted by "egress" in 2021, suggests that in general 97% of IT leaders are concerned about insider data breaches – the same percentage as in 2020 [12].

3 Secret sharing to increase privacy in banking

3.1 Motivation

In Section 1, we mentioned several high-profile leaks related to financial data. We now wonder how expensive it would be to set up lower profile leaks and who might benefit of these. With today's software, bank tellers have access to the balance of customers, information they often do not need. Moreover, they also know which organizations are making deposits, for what amount and when. Again information they usually do not need. We now explain why this approach is dangerous.

Let us take the example of Latin America. The problem of kidnapping there is so serious that employers take special insurance when employees travel to such countries [16]. Some local academics[5] hire security companies to drive their children to school. Obviously, the kidnappers want to target these who have sufficient resources, in particular available cash. If police forces can be bribed, then bank tellers can for sure!

In a perfect world, bank tellers should not know all the information they know today. We now discuss at a high level how this might be achieved using cryptographic primitives.

3.2 Using secret sharing: a reflection

From a theoretician's viewpoint, the logical cryptographic technology to choose would be secret sharing [4,24]. However, one wonders whether its use in practice would make banking much harder, on which we now reflect.

We are certainly not the first to suggest making banking harder to increase security, there are numerous proposals (e.g., in [31,13,8,23,6,3]) that suggest the use of cryptographic protocols in the context of banking. Obviously, if secret sharing should be used, it should not make banking too hard.

3.3 Using secret sharing: some scenarios

We now propose scenarios on which we focus by presenting a technical solution in Section 5. In many countries banks offer to some of their customers free "premium bank accounts." The banks have certain requirements such as having on regular basis sufficiently large deposits being made, keeping a good balance, etc. Often banks do not reveal the *exact* criteria. These customers can then go negative on their balance sheet without having their account blocked. This means that there are at least two levels of customers. The question now is whether that one bit of information should be known to the bank teller, who might discriminate when dealing with a customer.

We now give a second example in the context of financial real estate advisor. Consider two types of clients who want to invest their money. The one, who wants to buy an apartment to rent out, and the other the Carlyle Group[6], who wants to buy some office building in Paris. Both entities consult some company that gives financial advice, i.e., private banking. For maximum privacy, the advisor inside this company should not know whether the client is a small customer, or the Carlyle Group. In general, private banking and wealth managements are a bit tricky, because an insider can target only a single high-profile wealthy person and sell the victim's information to its rivals who (depending on the victim's leaked information) need to make a strategic investment, which is often stealth from the victim's viewpoint. For an insider, a data breach in private banking (or private financial advising) can be more tempting than leaking hundreds of bank accounts. Indeed, the first could result in a higher payoff while at the same time have a lower chance of being exposed.

Thus, it is not unreasonable to think that (i) it is likely that data breaches occur in private banking and in investment advice, which should be private, and this due to its very high payoff and (ii) most cases remain undetected (as the

[5] Details have been removed to maintain anonymity of the authors.

[6] https://www.carlyle.com/

recipient of the leaked information would take actions stealth from the victim's point of view).

4 Preliminaries

4.1 Diffie-Hellman Assumptions

Let G be a group-generator scheme, which on input 1^{λ} outputs $(\mathbb{G}, p, g)$ where $\mathbb{G}$ is the description of a group, p is the order of the group which is always a prime number and g is a generator of the group.

Computational Diffie-Hellman (CDH) Assumption. We say that G is hard under CDH assumption, if for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$, given (g^{a_1}, g^{a_2}) it has only negligible probability to correctly compute $g^{a_1 \cdot a_2}$. More formally, it holds that $Pr[\mathcal{A}(\mathbb{G}, p, g, g^{a_1}, g^{a_2}) \rightarrow g^{a_1 \cdot a_2}] \leq \epsilon(\lambda)$, where $(\mathbb{G}, p, g) \overset{\$}{\leftarrow} G(1^{\lambda})$, $a_1, a_2 \overset{\$}{\leftarrow} \mathbb{Z}_p$, and ϵ is a negligible function.

Decisional Diffie-Hellman (DDH) Assumption. Informally, we say that G is hard under the DDH assumption, if the distributions $(g^{a_1}, g^{a_2}, g^{a_1 \cdot a_2})$ and $(g^{a_1}, g^{a_2}, g^{w})$ are computationally indistinguishable when a_1, a_2, and w are drawn at random from $\mathbb{Z}_p$. More formally, for any PPT adversary $\mathcal{A}$, it holds that:

$$|Pr[\mathcal{A}(\mathbb{G}, p, g, g^{a_1}, g^{a_2}, g^{a_1 \cdot a_2})] - Pr[\mathcal{A}(\mathbb{G}, p, g, g^{a_1}, g^{a_2}, g^{w})]| \leq \epsilon(\lambda)$$

4.2 Oblivious Transfer (OT)

A 1-out-of-2 OT is a protocol that often involves two parties, a sender and a receiver. The sender has a pair of input messages (m_0, x_1) and the receiver has a bit/index s. The aim of OT is to allow the receiver to receive m_s, without revealing anything about s to the sender, and without allowing the receiver to learn anything about m_{1-s}. The 1-out-of-2 OT functionality is defined as $\mathcal{F}_{OT} : ((m_0, m_1), s) \rightarrow (\perp, m_s)$, where $\perp$ denotes the empty string. OT is one of the important building blocks of cryptographic protocols.

5 Distributed request OT protocol

5.1 Setting

In this section, we present DR-OT which is a new variant of OT that supports a distributed request. Specifically, DR-OT allows the receiver to delegate the generation and sending of its request (i.e., encoded index) to two non-colluding servers that are potentially passive adversaries, e.g., they may try to learn about the index in which the sender is interested, or the sender's plaintext message(s) (m_0, m_1).

Despite the fact some variants [21,7,15,28] of Bellare-Micali [2] 1-out-of-2 Oblivious Transfer (OT) are more efficient than the original scheme, we explain the distributed request for the Bellare-Micali protocol. Our motivation for this choice is primarily didactic. For a survey of the topic of OT consult [32].

For simplicity, we present only the case where we have only two parties that will share the request (in secret sharing terminology this is called 2-out-of-2). We assume a receiver (client) R needs to obtain information from a database D, to which R does not have access. However, some entities P_1 and P_2 have access to this database. (For example P_1 and P_2's organization is paying for this access.)

P_1 and P_2 individually do not know whether R wants to make a request $s = 0$ or a request $s = 1$. However, if P_1 and P_2 would collaborate/collude, they could obtain this information. Thus, we assume P_1 and P_2 do not collude with each other. P_i has share[7] s_i of this information. Note that $s_i \in Z_2$. The *request* part of the protocol is described in Figure **??**.

Note that we use multiplicative notation. (When using elliptic curves, the protocol can easily be adapted to additive notation.)

5.2 Analysis

The algebra that drives the first part of the protocol is that $Z_2(+)$ is isomorphic[8] to S_2, i.e., the symmetric group. This isomorphism implies that a 2-out-of-2 secret sharing over Z_2 can easily be transformed into one over S_2.

In Table 1 we show what δ_i and β_j are for the different values of s_1 and s_2. Note that a (i.e., the discrete log of C) appears in β_0 when $s = s_1 \oplus s_2 = 1$, and appears in β_1 when $s = s_1 \oplus s_2 = 0$. This guarantees that when one requests s, but shared differently, it will result in the same final request being made to the database.

	$s_2 = 0$	$s_2 = 1$
$s_1 = 0$	$\delta_0 = g^{r_2}$,$\delta_1 = g^{a-r_2}$ $\beta_0 = g^{r_2+r_1}$,$\beta_1 = g^{a-r_2-r_1}$	$\delta_0 = g^{a-r_2}$,$\delta_1 = g^{r_2}$ $\beta_0 = g^{a-r_2+r_1}$,$\beta_1 = g^{r_2-r_1}$
$s_1 = 1$	$\delta_0 = g^{r_2}$,$\delta_1 = g^{a-r_2}$ $\beta_0 = g^{a-r_2-r_1}$,$\beta_1 = g^{r_2+r_1}$	$\delta_0 = g^{a-r_2}$,$\delta_1 = g^{r_2}$ $\beta_0 = g^{r_2-r_1}$,$\beta_1 = g^{a-r_2+r_1}$

Table 1: δ_i and β_j are for the different values of s_1 and s_2. We express each value as a power of g.

5.3 The rest of the protocol

The database D will, similarly to Bellare-Micali, send R the following: $\alpha_i = g^{y_i}$, where $y_i \in_R Z_q$ $(i \in 0, 1)$ and $c_0 = m_0 \oplus \beta_0^{y_0}$ and $c_1 = m_1 \oplus \beta_1^{y_1}$, where m_i is the plaintext in the database.

When P_i privately give s_i, r_i $(i \in \{1, 2\})$ to R, then R can decrypt in a straightforward way. (Note that s_i might have been chosen by R, in which case only r_i is needed.) We now motivate an alternative approach to R decrypting.

[7] In our aforementioned example about the financial real estate advisor we have two clients R_1 and R_2. In such circumstances, P_i will have shares for each such client R_j. In that example, P_i knows the client, but does not know the wealth of R_j. P_1 and P_2 will use the share associated to this client.

[8] The mapping takes $0 \in Z_2$ to the identity permutation and 1 to the swap in S_2.

	Sender	P_1	P_2	**Receiver**
1 :				$\mathtt{SS}(s) \rightarrow (s_1, s_2)$
2 :				$r_1, r_2 \overset{\$}{\leftarrow} \mathbb{Z}_p$
3 :			$\xleftarrow{(s_2, r_2)}$	
4 :		$\xleftarrow{(s_1, r_1)}$		
5 :			$\delta_{s_2} = g^{r_2}$	
6 :			$\delta_{1-s_2} = \dfrac{C}{g^{r_2}}$	
7 :		$\xleftarrow{(\delta_0, \delta_1)}$		
8 :		$\beta_{s_1} = \delta_0 \cdot g^{r_1}$		
9 :		$\beta_{1-s_1} = \dfrac{\delta_1}{g^{r_1}}$		
10 :	$\xleftarrow{(\beta_0, \beta_1)}$			
11 :	abort if $C \neq \beta_0 \cdot \beta_1$			
12 :	$y_0, y_1 \overset{\$}{\leftarrow} \mathbb{Z}_{p-1}$			
13 :	$e_0 = (g^{y_0}, \mathtt{H}(\beta_0^{y_0}) \oplus m_0)$			
14 :	$e_1 = (g^{y_1}, \mathtt{H}(\beta_1^{y_1}) \oplus m_1)$			
15 :	$\xrightarrow{(e_0, e_1)}$			
16 :				$x = \begin{cases} r_2 + r_1, \text{if} \begin{cases} \begin{cases} s = 0, \\ s_1 = 0, \\ s_2 = 0 \end{cases} \\ or \\ \begin{cases} s = 1, \\ s_1 = 1, \\ s_2 = 0 \end{cases} \end{cases} \\ r_2 - r_1, \text{if} \begin{cases} \begin{cases} s = 0, \\ s_1 = 1, \\ s_2 = 1 \end{cases} \\ or \\ \begin{cases} s = 1, \\ s_1 = 0, \\ s_2 = 1 \end{cases} \end{cases} \end{cases}$
17 :				$m_s = \mathtt{H}((g^{y_s})^x) \oplus$ $\mathtt{H}(\beta_s^{y_s}) \oplus m_s$

Fig. 1: DR-OT: our 1-out-of-2 OT that supports a distributed request.

In certain circumstances the receiver does not know the value s. An example in the context of banks is that the customer R does not know to be premium or not. In that case only r_2 needs to be revealed to R; as we explain in Section 5.4.

5.4 Alternative decryption

In our alternative approach, in order to maintain the security, P_2 will encrypt the δ_i in a way only P_1 can decrypt these.

We now reflect on Table 1. When considering β_i in this table, and comparing the case $s_1 = 0$ with the case $s_1 = 1$, we see that the role of r_1 and $-r_1$ interchanged. So, if P_1 provides r_1 to D in the case $s_1 = 0$ and $-r_1$ to D in the other case, then D can remove this r_1 from β_i without being told the value of s_1. For all practical purposes D then learned the δ's, but without knowing whether these were permuted or not. D can then use these obtained δ's instead of β_i when constructing c_0 and c_1. R having received r_1 from P_1 can then decrypt and obtain one of the two plaintexts.

5.5 Security proof

The security proof is rather straightforward. (Note that Bellare-Micali [2] did not even bother giving one.)

First of all it is trivial to see that due to the property of the one-time pad, as proven by Shannon [25], β_2 is independent of s_2, and so s_2 is not leaked to P_1. (Note that choosing $-r_1$ is indistinguishable from r_1.)

When wondering whether P_1 learn s_1, note that P_1 is in the same situation as D in Bellare-Micali.

5.6 Generalizations

It is well known how to convert a 1-out-of-2 OT into a 1-out-of-n OT (see [32] for various variants of 1-out-of-n OT). It is trivial to adapt our protocol to that setting. In the 1-out-of-n OT the database has n records/plaintexts, while the case we considered the database has only 2 records/plaintexts.

Moreover, our distributed request can be generalized to some variants of Bellare-Micali, as can easily be verified. For more details see the final paper.

5.7 Recipient without the knowledge of s_i

There are cases where the recipient/customer does/must not know the index s_i; for instance, when P_1 and P_2 need to make a decision based on whether the customer is a premium member, without telling the customer whether it is not a premium member that might annoy it.

In this case, s_i can be the output of a secure Muti-Party Computation or a third-party secret shares it and sends a share to P_1 and P_2.

6 Conclusions and Open Problems

We presented the first distributed request in OT. Note that the use of a distributed database in OT was addressed earlier [20].

There are several open problems which we now pose. First the distributed request is sequential. Can this be made parallel? Secondly, how to generalize this to a t-out-of-n distributed request in which $t \neq n$?

In this work, we have highlighted serious security/privacy issues in the banking sector. However, so far these issues have been overlooked by the information security and by the cryptography research community. We hope this paper initiates future discussion and research to tackle such issues at their roots.

References

1. Abadi, A., Murdoch, S. J.: Payment with dispute resolution: A protocol for reimbursing frauds' victims. IACR Cryptol. ePrint Arch. (2022).
2. Bellare, M., Micali, S.:. Non-interactive oblivious transfer and applications. In Conference on the Theory and Application of Cryptology (1989) Springer.
3. Blakley, B., Blakley, G. R.:. All sail, no anchor III: risk aggregation and time's arrow. In Information Security and Privacy, 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005, Proceedings (2005) Springer.
4. Blakley, G. R.:. Safeguarding cryptographic keys. In Proc. Nat. Computer Conf. AFIPS Conf. Proc. (1979) pp. 313–317.
5. Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM **24** (1981) 84–88.
6. Chen, L., Huang, X., You, J.:. Fair tracing without trustees for multiple banks. In Computational and Information Science, First International Symposium, CIS 2004, Shanghai, China, December 16-18, 2004, Proceedings (2004).
7. Chou, T., Orlandi, C.:. The simplest protocol for oblivious transfer. In Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings (2015).
8. Darbha, S., Arora, R.:. Privacy in CBDC technology. Tech. rep. Bank of Canada 2020.
9. Department of Justice:. Two arrested for alleged conspiracy to launder $4.5 billion in stolen cryptocurrency 2022. https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.
10. Department of Justice–U.S. Attorney's Office:. Former JP Morgan Chase Bank employee sentenced to four years in prison for selling customer account information 2018. https://www.justice.gov/usao-edny/pr/former-jp-morgan-chase-bank-employee-sentenced-four-years-prison-selling-customer.
11. Desjardins Group:. Privacy breach: Class action settlement agreement submitted to the Superior Court of Quebec for approval 2022. https://www.desjardins.com/qc/en/news/desjardins-settlement-agreement.html.
12. egress:. Insider data breach survey 2021. https://www.egress.com/media/4kqhlafh/egress-insider-data-breach-survey-2021.pdf.
13. Hegde, C., Manu, S., Shenoy, P. D., Venugopal, K., Patnaik, L.:. Secure authentication using image processing and visual cryptography for banking applications. In 2008 16th International Conference on Advanced Computing and Communications (2008) IEEE.
14. Hern, A.:. A history of bitcoin hacks 2014. https://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency.
15. Ishai, Y., Kilian, J., Nissim, K., Petrank, E.:. Extending oblivious transfers efficiently. In Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings (2003) Springer.

16. Kenney, S.: Regional shortcomings and global solutions: Kidnap, ransom and insurance in Latin America. Conn. Ins. LJ **14** (2007) 557.
17. Kurmelovs, R.:. Optus cyber-attack leaves customers feeling powerless over risk of identity theft 2022. https://www.theguardian.com/australia-news/2022/sep/23/optus-cyber-attack-leaves-customers-feeling-powerless-over-risk-of-identity-theft.
18. Leigh, D., Ball, J., Garside, J., Pegg, D.: HSBC files timeline: From Swiss bank leak to fallout. The Guardian **12** (2015).
19. Murphy, H.:. Whatever happened to those self-service passport kiosks at airports? 2022. https://www.nytimes.com/2022/10/05/travel/customs-kiosks-facial-recognition.html.
20. Naor, M., Pinkas, B.:. Distributed oblivious transfer. In Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings (2000) vol. 1976 of Lecture Notes in Computer Science Springer pp. 205–219.
21. Naor, M., Pinkas, B.:. Efficient oblivious transfer protocols. SODA '01 Society for Industrial and Applied Mathematics.
22. Office of the Privacy Commissioner of Canada:. Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019 2020. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-005/.
23. Perlman, R., Kaufman, C., Perlner, R.:. Privacy-preserving DRM. In Proceedings of the 9th Symposium on Identity and Trust on the Internet (2010).
24. Shamir, A.: How to share a secret. Commun. ACM **22** (1979) 612–613.
25. Shannon, C. E.: Communication theory of secrecy systems. Bell System Techn. Jour. **28** (1949) 656–715.
26. Syam Roslan:. Let's fight scams 2020. https://www.police.gov.sg/media-room/features/lets-fight-scams.
27. Tidy, J.:. Ronin network: What a $600m hack says about the state of crypto 2022. https://www.bbc.co.uk/news/technology-60933174.
28. Tzeng, W.:. Efficient 1-out-n oblivious transfer schemes. In Public Key Cryptography, 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002, Paris, France, February 12-14, 2002, Proceedings (2002) D. Naccache and P. Paillier, Eds. Lecture Notes in Computer Science.
29. UK Finance:. 2021 half year fraud update 2021. https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf.
30. Venkataramakrishnan, S.:. Regulator to force UK banks to offer scam victims compensation 2022. https://www.ft.com/content/aabeea7a-324c-4850-a91d-fc41aa6d8802.
31. Wu, T. D., Malkin, M., Boneh, D.:. Building intrusion-tolerant applications. In Proceedings of the 8th USENIX Security Symposium, Washington, DC, USA, August 23-26, 1999 (1999) USENIX Association.
32. Yadav, V. K., Andola, N., Verma, S., Venkatesan, S.: A survey of oblivious transfer protocol. ACM Comput. Surv. (2022).