Are Clouds making Our Research Irrelevant and Who Is at Fault? (Position Paper)

Yvo Desmedt[a]
Department of Computer Science, The University of Texas at Dallas, 800 W. Campbell Road, Richardson, U.S.A.

Keywords: Information Security, Cryptography, Clouds, Research, Deployment.

Abstract: Until recently, the user of a computer system was able to (at least to some degree) help decide security policies, such as which access and information flow control to use, which cryptographic algorithms to choose, how to secure databases in use, etc. Due to these choices, researchers were able to have an impact on what was deployed.
In today's world, the Chief Information Officer (CIO) outsources online communication (replacing landlines), databases, e-mail, storage, voting, WWW, etc., to clouds. These do not use open source and do not disclose their design. So, the security is left to the designer and the user is completely left in the dark. Since most programmers never took a course in information security, we should assume the worst.
In our paper we justify several positions: (i) we make the claim that clouds have lowered our information security; (ii) we wonder whether CIOs compare competing clouds on their security properties and ask independent experts for their advice; (iii) one finds that self-acclaimed experts often lack basic knowledge; (iv) that research is becoming irrelevant. We also wonder who is at fault for these problems and how we can address them.

SCITEPRESS
SCIENCE AND TECHNOLOGY PUBLICATIONS

1 INTRODUCTION

Some well known attendees of the Crypto conference announced they would no longer attend the conference because it had become irrelevant to real world problems. Indeed, despite having been co-editor of the 1982 Crypto proceedings (Chaum et al., 1983), Alan Sherman (PhD, MIT) was one of the first to make such a statement. Another example is Paul van Oorschot, who became involved with USENIX. Finally, IACR (who organizes Crypto) created "Real World Crypto" to address such concerns.

When we compare computer security with cryptography, we can hardly say that the area is dominated by theoreticians. In this paper, we will argue that a lot of the research on computer security is irrelevant to the real world today. We argue that the computer world in which we live has dramatically changed. 15 years ago any mid-size to large organization (whether business or non-profit) would run their own servers and data would be stored locally. Today, we usually find a cacophony of cloud servers. We will put forward the position that: "the computer environment has changed, but many researchers have not adapted their topics, making the research irrelevant."

Before we justify our positions, we first wonder how we came to a world in which cloud servers have taken over the role of local servers. For this, we start in Section 2 by considering the history from Windows 95[1] and dial-up internet[2] on. We also explain the dramatic impact these had on modern computer systems. In Section 3 we give concrete examples how during the last 15 years cloud servers were selected. In Section 4 we try to talk about cloud security. Indeed, since many clouds in use today are closed source, we wonder what we actually can say about their security. In particular we focus on whether information security concerns, such as privacy, received the attention they should have, when moving to a cloud based world. Before we question whether academics should study the security of particular clouds (see Section 7.1), we state our positions in Section 5. Finally we wonder In Section 7 who is at fault.

[a] https://orcid.org/0000-0002-6679-7484

[1] See: https://en.wikipedia.org/wiki/Windows_95

[2] See: https://en.wikipedia.org/wiki/Dial-up_Internet_access

Desmedt, Y.
Are Clouds making Our Research Irrelevant and Who Is at Fault? (Position Paper).
DOI: 10.5220/0011328800003283
In *Proceedings of the 19th International Conference on Security and Cryptography (SECRYPT 2022)*, pages 436-442
ISBN: 978-989-758-590-6; ISSN: 2184-7711
Copyright © 2022 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

2 THE RECENT HISTORY OF COMPUTERS REVISITED[3]

In the 1990's very few individuals had a good internet connection. Users needed to dial (phone) an internet provider to connect to the internet, blocking the phone! So, PCs at home were offline most of the time and often switched off. As a consequence, the dial-up internet providers hosted e-mail accounts and web pages. So, there was no need to have user friendly software for installing e-mail and web servers.

With the appearance of cable and DSL modems, users being on the internet 24 hours, the history of computers should have changed dramatically, but it did not. We now look at the post dial-up internet world and describe what could have happened in a parallel universe.

First 24/7 internet connection could have allowed for users to have e-mail and web servers at home, as we now explain. Although PCs are turned off after use (PCs are noisy), home user's modems are on 24 hours! We now argue they could have hosted these servers. Modern "modems" are more than strictly modems. They also contain a firewall, router, etc. Moreover, the interface with the user is a *web interface!* So, a different design could have consisted of using the modem for a web server providing a basic web page, and internet providers could have sold/rent "sophisticated modems" that enable more advanced web pages. Moreover, for e-mail, the internet provider could have acted as a backup for incoming mail, which would had been forwarded when the home user's PC comes online, in a similar way as POP allows.

Unfortunately, these who designed modems, never provided the aforementioned service, and so when DSL, coax, fiber, etc., allowed for 24 hours service, users regarded it as normal that they needed an external e-mail address and using external tools, such as what today is called social networks, to disseminate information, which could have been done by using local web servers. So, today's social networks are centralized, while they could have been distributed, avoiding a whole range of problems, such as the censoring of Facebook, LinkedIn, Twitter[4], etc.

Another potential use of the home modem could have been to set up a VPN. This could have been used to help reroute data transmission. For example, when two persons travel to Japan, one a UK resident and the other a US one, their respectively home modems "know" they are in Japan. Indeed, the home modem would had been a basic home server. So, data that needs to be communicated between these two people does not need to travel via the US or the UK, leading to a distributed communication, instead of the centralized ones we have today. This approach seems far fetched, but mobile phone companies have been doing exactly this for decades!

The 24 hours internet could have had some other impacts, which OS (Operating Systems) designers did not realize, as we now explain. Indeed, they failed to update the concept of "user." The definition of user should be: "Anybody who uses (or should use) resources on your computer". That implies that when hosting a web server, the whole world is a potential user! Note that when being connected 24/7, from a security viewpoint, anybody should also be called a (potential) user! When we use this corrected definition of user, sharing data with a particular person (anywhere in the world) should have been made extremely user-friendly. However, since the concept of user was not adapted, this never happened, and so today clouds are being used to share data.

The anti-cloud world we described may seem unrealistic. Indeed, search engines contain so much data it can not fit on a modern PC/laptop. However, since inexpensive disks today can contain 2-3 Terra Byte (TB), a lot of information could be stored locally. Such disks could have low resolution maps, a limited Wikipedia (e.g., without pictures) and for professional users, data they might need. For example the proceedings of a conference today are typically 25Mbytes. So, a 3 TB disk could contain 120,000 of these proceedings, which is more than what is needed! The companies selling disks have not understood they could preload disks with useful data!

Anyway, we do not live in this parallel universe. Modem designers, OS designers, etc., never understood they could have provided an alternative to our cloud-centered world. To better understand how we came to this world, we illustrate in the next section how some decisions were made.

3 HOW CLOUDS WERE SELECTED

3.1 Some Examples

On 27 February 2007 the director of the Information Services Division of University College London

[3]This section is based on the author's seminar lecture "*Is The Rise of Cloud Storage, Cloud Computing and Social Networks a Consequence of a Failed OS (Operating System) Design?* at Microsoft Research, Cambridge, UK, on November 27, 2013.

[4]The writing of this paper started before Elon Musk considered buying Twitter.

(UCL) informed computer science faculty members that: "the provost had decided (without consulting CS), to switch to Hotmail for e-mail, but using a fake university address." (Microsoft already had demonstrated how to use Hotmail at some universities, e.g., in Australia earlier on.) The reasons that were given for this switch was that 2 men-year would be saved and that it was free for the first years. Whether this really resulted in some savings was never analyzed, so far the author knows. In fact a lot of extra people power was needed to make the switch, making the short term saving doubtful. One of the faculty members pointed out that one person pushing for the switch had a large extra income by being consultant for Microsoft. After UCL switched, Microsoft was able to convince other universities to stop having their own e-mail servers. We give further details, related to privacy, in Section 4.1.

We now give another example. To avoid the expense of landlines the University of Texas System decided roughly 10 years ago to switch to Voice Over IP (VOIP). Landline phones were removed from most offices and replaced by ethernet connected phones that were using TCP/IP. However, the VOIP contract ended in 2020, and all VOIP phones were removed from offices, leaving no phones in these whatsoever. As solution the cloud was used. Microsoft Teams was selected because Zoom had security problems. (For example, Zoom originally used ECB mode, which gives very poor encryption, in particular when encrypting pictures[5].) Note that the University of Texas System also uses Microsoft for e-mail! So, from a privacy viewpoint, Microsoft now is in a position to eavesdrop both "phone" conversations and e-mails!

3.2 Impact of COVID

To limit the impact of COVID lockdowns on meetings, teaching, etc., the world became much more virtual. CIOs decided that clouds were the fastest approach to make this virtual world a reality. Again, a non-cloud approach was not available, so far the author knows.

3.3 Abolishment of Paper

Many organizations today have dramatically reduced the use of paper in their administration. The solution CIOs have used is again the use of clouds. Some startups, established cloud servers, etc., have taken into account the hierarchical structure that exists in some organization. We describe two such examples. In a typical hierarchy, annual reports are required. Role-Based Access Control (see e.g., (Jajodia et al., 1997; Oh and Park, 2003; Joshi et al., 2005; Sandhu et al., 2006; Fadhel et al., 2015)) can then be used to decide who should have access to these reports. Another example, is the chain required to receive permission (e.g., to buy new equipment). Role-Based Access Control can be used to achieve this chain of approval.

4 CLOUD SECURITY & PRIVACY

4.1 Do CIOs Take Security and Privacy into Account?

We start by giving two concrete examples. First we go back to the example of the switch to the use of Microsoft's hotmail at UCL (see Section 3.1). Privacy concerns were almost completely ignored. The main exception was that Google's Gmail was not selected, because they could not guarantee that the data would be stored in the EU (this predates Brexit). Note however, that due to the US CLOUD Act (March 2018), Microsoft may have to turn "overseas" data to the US Department of Justice anyway!

Our second example is related to universities, particularly in the US. There the Family Educational Rights and Privacy Act of 1974 (FERPA), as amended, protects student data, such as the name of the student. Tools used in many US universities today, such as Microsoft Teams do *not* allow to hide the participants at the meeting (Microsoft Teams, 2022). Similar regulations may exist in other countries/regions and might be violated systematically today.

4.2 The Impact of Closed Source

Since the software on most cloud servers is closed source, there are a lot of things we can *not* say. For example in Section 3.3 we spoke about the potential use of Role-Based Access Control. However, since the source and the design of the software used is closed, we can not be certain that Role-Based Access Control was actually used, or whether a reinvention of some variant was used.

Since the source is closed, we can *not* evaluate the software on vulnerabilities, security and privacy properties we would expect. A concrete example is given in Section 6.

[5]https://medium.com/@TalBeerySec/zooming-on-zoom-5-encryption-cc7e9b710b9f

4.3 The Impact of Laws

In many countries attempting to hack a computer, such as a server is illegal. This restricts researchers to study which cloud servers are vulnerable to Denial of Service. Moreover there is a lack of regulations for these who design clouds. So, we end up in a world for which we no longer can estimate how vulnerable it is to cyber attacks. It is well known today that most superpowers have military hacking teams, but smaller countries such as Iran and Israel are also assumed to have these capabilities. Not knowing how vulnerable our society is today, is far from ideal.

4.4 Ignoring Privacy

When using clouds instead of distributed systems, privacy has already been undermined. However, the situation is worse than it seems. In many applications, participants should not know the names of other participants. One example is in the military context, when people are working on a classified project. We gave another example in Section 4.1.

Moreover, to cope with the COVID pandemic, Chief Information Officer were sometimes forced to choose among servers who each blatantly ignore privacy rules.

Browser security is very problematic (see e.g. (Louw et al., 2008)) and many cloud providers use these as user interface.

5 OUR POSITIONS

These are:

- Clouds have lowered our information security.
- CIOs usually do not compare competing clouds on their security properties and do not ask independent experts for their advice.
- Self-acclaimed experts often lack basic knowledge.
- Research on information security is becoming irrelevant.

We now justify some of these positions in the next section.

6 A CASE STUDY

The section is based on the author's 2022 poster (Desmedt, 2022). This poster compared the state-of-the-art on secure e-voting with a cloud based approach. We will first briefly survey the state-of-the-art in research on secure e-voting. Then we discuss a cloud based approach. We then explain how the case study inspired our positions.

6.1 State-of-the-Art Research

The research on e-voting started with Chaum proposing MIX servers (Chaum, 1981). For a while the topic was hot and many papers were published, i.e., too many to do a proper survey. So, therefore we only mention what security properties can be achieved (some requiring unproven assumptions).

Theoretical research proposed voting systems that guarantee:

- **security against double voting**. This property is achieved by having the voter digitally sign the ballot. This signature is then checked and removed from the ballot.
- **anonymity/privacy**[6] of the vote. This can be achieved:
  - **conditionally:** MIX servers are used that permute and re-encrypt all ballots (Park et al., 1994). The ballots are encrypted by the voter. At the end threshold decryption (Desmedt, 1994) is used to decrypt the mixed ballot (Abe, 1998).
  - **unconditionally:** in Code Voting (Chaum, 2001) to each (voter, candidate) corresponds a unique random number. These are mechanically permuted and then securely send (e.g., via postal mail) to the voter. An anonymous channel is used by the voter to send in the vote.
- **correctness:** zero-knowledge interactive proofs (Goldwasser et al., 1989) are usually used to prove that the MIX server (see e.g., (Sako and Kilian, 1994)) did not introduce errors. In homomorphic voting, voters will use such proofs to demonstrate correctness of the range of their vote.
- **no need for a trusted security agent**. This property is achieved by assuming the number of untrusted parties is bounded. (Some initial protocols were described without taking into account that some of the aforementioned parties may conspire.)
- **being hacking-free.** Chaum's code voting and variants allow to vote on a computer which has been hacked. Correctness and privacy are unaffected.

[6]The crypto community uses anonymity, while the popular press talks about privacy.

- **universal verifiability:** it allows anyone in the world to check the correctness. This can be achieved when replacing interactive protocols by non-interactive ones, e.g., using the Fiat-Shamir trick (Fiat and Shamir, 1987). The security is only conditional.

Note that many of the aforementioned properties can be obtained together. Usually, conditional and unconditional security are mutual exclusive, but there are exceptions to that rule of thumb.
Note that practical problems remain, e.g.:

- Some practical systems use the WWW, but the *WWW and browsers are insecure*. For an example of a voting scheme that was hacked using a browser rootkit, see (Estehghari and Desmedt, 2010).
- Some systems are *not user-friendly*. Chaum's code voting has often been mentioned in this context, but variants were proposed that allow more classical voting (see e.g., (Desmedt and Erotokritou, 2015)).

6.2 A Cloud based Approach

We give an example of a particular cloud implementation of e-voting and we focus in particular on a real life scenario.

On April 2, 2021, at 6:32pm CDT, the Acting Head of Computer Science at University of Texas at Dallas sent an e-mail that: *48 votes were received from 40 eligible voters*! So, what went wrong?

Earlier, at 2:34 pm CDT the same day, the author informed the Acting Head that "if I go to a Hotspot which changes my IP address (and I also change my MAC address), I can vote a 2nd time!!" (Later someone else observed that you can just vote twice from the same IP address!)

The first solution that was proposed is to have someone collect votes in the clear (i.e., violate privacy). A deeper analysis, using a Google search, found that at Tufts University they explain the difference between:

- a *"Survey Link"* (which does *not prevent* repeat voting), and
- *"The Qualtrics Mailer,"* requiring an individual e-mail is sent to each authorized voter.

The last approach was eventually used to vote for the candidate to hire.

6.3 A Comparison

First of all it is clear that Qualtrics' voting system has a *major usability problem*! Indeed, anyone using it should immediately know that when using the Survey Link, that double voting is not prevented.

We now compare the Qualtrics' voting system with the state-of-the-art in e-voting, which we briefly surveyed in Section 6.1. We organize this security comparison into two categories, being these for which:

- **we can not state anything.** The black box and closed source approach that seem to have been used implies that:
  - we do not know whether these who implemented this voting system took the desired privacy and security properties of e-voting into account.
  - we also can not answer whether the designers are aware of the state-of-the-art in the area of voting.

  This implies in particular that after consulting Qualtrics' documentation[7] one can still not answer the following questions:
  - What *privacy (anonymity) guarantees* does Qualtrics offer?
  - Will Qualtrics keep the votes for *eternity*?
  - What about *guaranteeing correctness*?
  - How secure is Qualtrics *server against hacking* (e.g., how easy is it to *double vote*)?
  - What *mechanisms* do they *use to guarantee* the aforementioned?
  - Has Qualtrics been *certified*?
  - What *NIST standards does Qualtrics follow*?
- **can compare with the state of the art.** In this case, such a comparison is not possible and we are even unable to state which privacy/security properties The Qualtrics Mailer lacks.

6.4 How Was This Cloud Server Chosen?

Seeing the many unanswered security questions, one can wonder how the University of Texas at Dallas (and other organizations) decided to use Qualtrics Mailer. It poses serious questions how clouds are chosen. Indeed:

- As the author already stated during his NIST talk on June 7, 2011:

  > One can wonder whether *CEO's have their head in the cloud instead of both feet on the ground, when rushing to adopt cloud technology?*

[7] https://www.qualtrics.com/marketplace/vote-rank-survey/

- Is the Chief Information Officer the sole person to decide what clouds to use, or is there an advisory board?
- Are clouds evaluated by technical experts?

6.5 How e-Voting Inspired our Positions

The huge difference with what the research on e-voting can offer, which seem not to be a part of Qualtrics Mailer, is likely just one example in the context of what the cloud offers for privacy/security compared to what it could offer. Due to the fact that many cloud servers use a closed source and a closed design approach, many of the comparison in Section 6.3 seem to extend in a context different from e-voting.

The case study, together with the two examples in Section 3.1, made us reflect on how we came to the situation we are in now. These together with Sections 3 and Sections 4 were instrumental in formulating our positions, as stated in Section 5.

7 WHO IS AT FAULT?

7.1 Research Failures

Today, research on information security is often not driven by a particular need, but by what is in fashion. We now give one concrete example. Nigel Smart, at Eurocrypt 2017, during his invited talk, pointed out that Secure Multiparty Computation (SMC) (see e.g., (Yao, 1986; Goldreich et al., 1991)) has no key application.

Today most reviewers will reject papers in which old attacks are used against new software. This might be good from a theoretical research viewpoint, but it clearly undermines the impact of research on the real world! In such a research environment, it is not attractive for researchers to analyze the security of clouds! Maybe we should be talking to engineers who have a different viewpoint on the importance of practical oriented research.

We now look at the role of funding agencies. First, in-fashion topics will receive a lot of funding, and this in different regions of the world, regardless whether there is a need for that research. Second, one needs a major initiative for a cloud-free distributed computer world based on the state-of-the-art in information security. Examples of such initiatives but in other contexts, were NASA and the TGV. In our context, large cloud servers would probably lobby against such an initiative.

7.2 Researchers Setting Bad Examples

Many researchers work in a small subarea of the huge field of information security. So, often they are not aware of the best practices. We just give two examples, without mentioning any names.

During a 2003 Summer School, one of the organizers, who teaches Computer Security, logged in to the university's computer displaying the login screen to all participants. It showed ******, implying that the password is only 6 characters! When this was pointed out, the person replied: "My password is hard to guess."

Today many people working in information security when having to copy a file from one laptop to another, just upload it to the cloud and then download it to the other computer, clearly showing they do not understand the privacy violations of their actions.

7.3 Fake Experts

A question we asked is whether CIOs are using experts before making their decision. However, some expertise is fake. As an example, some invited "expert" speakers confuse bitcoin with blockchain. Obviously, self-certified experts aggravate the problem.

7.4 Lack of Regulations

Many of today's clouds are large corporations who have been very successful in lobbying against any type of regulation. They will probably continue this practice.

7.5 Customer Reviews

Some countries have magazines such as Consumer Reports[8], which for example evaluates cars, home appliances, etc. So far we know there is no such magazine that evaluates clouds on information security aspects.

8 CONCLUSIONS

It seems that cloud severs were designed in a black box way and that they used a closed source approach. This implies that when looking at the state-of-the-art security properties, we may be unable to state whether a cloud server achieves these or not.

[8]See: https://www.consumerreports.org/

CIOs decided which cloud severs and services are being used today inside an organization. In that context it seems that for cloud servers having a good sales person is more important than having experts knowing the state-of-the-art in privacy/security. In this context, one can only conclude that:

- clouds are making our research irrelevant, and that
- technology transfer from research to practice has been a failure.

ACKNOWLEDGEMENTS

Travel made possible by the Jonsson Endowment.

REFERENCES

Abe, M. (1998). Universally verifiable Mix-net with verification work independent of the number of Mix-centers. In Nyberg, K., editor, *Advances in Cryptology — Eurocrypt '98, Proceedings (Lecture Notes in Computer Science 1403)*, pages 437–447. Springer-Verlag. Espoo, Finland, May 31–June 4.

Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–88.

Chaum, D. (2001). Surevote: Technical overview. In *Proceedings of the Workshop on Trustworthy Elections (WOTE '01), August 2001*.

Chaum, D., Rivest, R. L., and Sherman, A. T., editors (1983). *Advances in Cryptology. Proc. of CRYPTO'82*. Plenum Press N.Y.

Desmedt, Y. (2022). Can we trust cloud voting? Poster at Finanicial Cryptography 2022 (not in the proceedings).

Desmedt, Y. and Erotokritou, S. (2015). Making code voting secure against insider threats using unconditionally secure MIX schemes and human PSMT protocols. In *Vote ID*, volume 9269 of *Lecture Notes in Computer Science*. Springer.

Desmedt, Y. G. (1994). Threshold cryptography. *European Trans. on Telecommunications*, 5(4):449–457. (Invited paper).

Estehghari, S. and Desmedt, Y. (2010). Exploiting the client vulnerabilities in internet e-voting systems: Hacking Helios 2.0 as an example. In *2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '10), August 9–10, 2010.*

Fadhel, A. B., Bianculli, D., and Briand, L. (2015). A comprehensive modeling framework for role-based access control policies. *Journal of Systems and Software*.

Fiat, A. and Shamir, A. (1987). How to prove yourself: Practical solutions to identification and signature problems. In Odlyzko, A., editor, *Advances in Cryptology, Proc. of Crypto '86 (Lecture Notes in Computer Science 263)*, pages 186–194. Springer-Verlag. Santa Barbara, California, U. S. A., August 11–15.

Goldreich, O., Micali, S., and Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(1):691–729.

Goldwasser, S., Micali, S., and Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208.

Jajodia, S., Samarati, P., Subrahmanian, V., and Bertino, E. (1997). A unified framework for enforcing multiple access control policies. In *SIGMOD'97*, pages 474–485. Tucson, AZ.

Joshi, J. B., Bertino, E., Latif, U., and Ghafoor, A. (2005). A generalized temporal role-based access control model. *Knowledge and Data Engineering, IEEE Transactions on*, 17(1):4–23.

Louw, M. T., Lim, J. S., and Venkatakrishnan, V. N. (2008). Enhancing web browser security against malware extensions. *J. Comput. Virol.*, 4(3):179–195.

Microsoft Teams (2022). Teams - live event / webinar - hide participants. https://answers.microsoft.com/en-us/msteams/forum/all/teams-live-event-webinar-hide-participants/27a824d3-4488-47ac-8d33-eb5c6bae02ad.

Oh, S. and Park, S. (2003). Task–role-based access control model. *Information systems*, 28(6):533–562.

Park, C., Itoh, K., and Kurosawa, K. (1994). All/nothing election scheme and anonymous channel. In Helleseth, T., editor, *Advances in Cryptology — Eurocrypt '93, Proceedings (Lecture Notes in Computer Science 765)*, pages 248–259. Springer-Verlag. Lofthus, Norway, May, 1993.

Sako, K. and Kilian, J. (1994). Secure voting using partially compatible homomorphisms. In Desmedt, Y. G., editor, *Advances in Cryptology — Crypto '94, Proceedings (Lecture Notes in Computer Science 839)*, pages 411–424. Springer-Verlag. Santa Barbara, California, U.S.A., August 22–25.

Sandhu, R., Ranganathan, K., and Zhang, X. (2006). Secure information sharing enabled by trusted computing and pei models. In *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, pages 2–12. ACM.

Yao, A. C. (1986). How to generate and exchange secrets. In *27th Annual Symp. on Foundations of Computer Science (FOCS)*, pages 162–167. IEEE Computer Society Press. Toronto, Ontario, Canada, October 27–29, 1986.