Discrete Choice, Social Interaction, and Policy in Encryption Technology Adoption [Short Paper]

Tristan Caulfield[1], Christos Ioannidis[2], and David Pym[1]

[1] University College London
t.caulfield@ucl.ac.uk, d.pym@ucl.ac.uk
[2] University of Bath
c.ioannidis@bath.ac.uk

Abstract We introduce a model for examining the factors that lead to the adoption of new encryption technologies. Building on the work of Brock and Durlauf, the model describes how agents make choices, in the presence of social interaction, between competing technologies given their relative cost, functionality, and usability. We apply the model to examples about the adoption of encryption in communication (email and messaging) and storage technologies (self-encrypting drives) and also consider our model's predictions for the evolution of technology adoption over time.

1 Introduction

In recent years, especially in the light of Edward Snowden's revelations, awareness of the need for enhanced privacy and confidentiality for both communications and devices has increased. In response to this, many new technologies, including various forms of encryption, have been introduced. However, the adoption of these new technologies is not guaranteed: their use depends on a number of factors, including how effective they are, how much they cost, how easy they are to use, and the social and policy contexts within which they are introduced.

The use of encryption for electronic communications and data storage is accelerating and people are increasingly shifting to new technologies for interpersonal communications. Such behavioural changes are indicative of the existence of agents revising their choices between technological alternatives to achieve their communications goals. The aim of the paper is to provide a theoretical framework which can capture such changes in the choice of technologies in the presence of external impulses emanating from either policy or other external events.

We introduce a model, based on work by Brock and Durlauf [3], that incorporates these factors into a utility-theoretic framework that describes how agents make choices between competing technologies. We use this model to analyse the adoption of encryption in a range of communication and storage technologies. We consider three examples: first, email, where we look at the use of PGP/GPG encryption; second, messaging applications, where we examine the adoption of WhatsApp compared to traditional SMS messaging; and, finally, the adoption of self-encrypting drives over standard, non-encrypted drives.

The Brock and Durlauf model captures social interactions between non-cooperative decision-making agents. This reflects the reality of decisions about the use of encryption: agents—either individuals or organizations—make decisions independently and without coordination and yet their decisions can have an effect on the utility of other agents. For example, the utility of encrypted communications technology to a user changes with the number of other users; it is low if there is nobody to communicate with, and higher if it can be used to communicate with a larger number of others.

Besides the social interactions, the Brock and Durlauf model uses the relative profitability of technologies as the main factor that determines adoption. This single factor would not give great insight into the adoption of encryption technologies. To this end, we introduce some modifications to the model that allow us to examine the influence on utility—and hence, adoption—of different technology attributes: functionality, monetary cost, and usability. These are sufficient to demonstrate the model; other attributes may also be of interest for different applications. These are multiple attributes in the sense of [6].

Other work has also looked at the adoption of security technologies. Rosasco and Larochelle [16] look at the adoption of SSH over telnet, and considers the cost and functionality of the technologies. Ozment and Schechter [15] use a model, which includes a social component, to suggest strategies to promote the adoption of DNSSEC.

In conclusion, our model is a tool for thinking about the different factors that determine adoption, such as attributes of the technologies themselves, technological innovation, or policy. Understanding how these factors affect adoption is important for decision-makers—those designing a technology, deciding whether to adopt it, or seeking to promote or inhibit adoption through policy.

2 Technology Adoption Model

We start with the discrete choice model of Brock and Durlauf [3], which, in this context, describes a system where M technologies are competing in a market for adoption by N agents. The model assigns a share of the market to each technology, based on its profitability. This profitability also includes a social component: a technology can be more profitable if more agents are using it. There can also be additional factors, such as taxes, policy, or technological innovation, but we start with the simple model and introduce the other factors below, before continuing with our extensions to apply the model to encryption technology.

The utility an agent receives from technology c in time period t is

$$u_{c,t} = \lambda_c + \rho_c x_{c,t}, \tag{1}$$

where the profitability of technology c is given by λ_c and the number of agents choosing c at time t is $x_{c,t}$. The value ρ_c (where $\rho_c > 0$) defines the intensity of the social component, the term $\rho_c x_{c,t}$. The greater the value of ρ_c, the more agents' utilities and subsequently choices are influenced by the choices of others. Each agent i experiences a random utility $\tilde{u}_{i,t} = u_{i,t} + \epsilon_{i,t}$, where the noise, $\epsilon_{i,t}$,

is independently identically distributed across agents, and known to the agent at decision time. As the number of agents tends to infinity and when the noise has a double exponential distribution, the probability of adoption of technology c converges to

$$x_{c,t} = \frac{e^{\beta u_{c,t-1}}}{\sum_{j=1}^{M} e^{\beta u_{j,t-1}}} \tag{2}$$

Here, the parameter β is the intensity of choice, and is inversely related to the variance of the noise $\epsilon_{i,t}$. When $\beta \to \infty$, there is no noise and all agents choose their optimal technology. When $\beta \to 0$, agents pick technologies randomly, and the share of each technology tends towards $1/M$. Essentially, with higher values of β, the equilibria points in the model become more extreme; that is, they tend towards 'corner solutions' with only one surviving technology.

In this model, agents know only the social term $\rho_c x_{c,t}$ in Equation 1, which represents the decisions of other agents and benefits associated with them. Agents are making a choice between tech options with different profitability to themselves, using knowledge about market penetration in the last period.

Now let's consider a model with two competing technologies, c, a new technology, and d, an existing technology. Because there are just two, we need only one variable, x, which is the share of agents using technology c, to keep track of the state: $x_c = x$ and $x_d = 1 - x$. For simplicity, we also assume that the technologies experience equal increasing return on adoption; that is, $\rho_c = \rho_d = \rho$. From Equation 2, the probability of adoption (and market share) of technology c in time t is then

$$x_t = \frac{e^{\beta(\lambda_c + \rho x_{t-1})}}{e^{\beta(\lambda_c + \rho x_{t-1})} + e^{\beta(\lambda_d + \rho(1 - x_{t-1}))}} = \frac{1}{1 + e^{\beta(\lambda + \rho(1 - 2x_{t-1})}} = f(x_{t-1}) \tag{3}$$

The model is driven by the difference of utilities between the two technologies, $u_{d,t} - u_{c,t} = \lambda + \rho(1 - 2x_t)$, where $\lambda = \lambda_d - \lambda_c$. If the difference is positive, agents will prefer technology d; if it is negative, they will prefer technology c. More pronounced differences will result in ever-increasing shares for the preferred technology.

Policy We can extend the above model with an additional component that represents a policy about the choice between the two technologies. The policy is imposed by some external source, and takes the form of a penalty or incentive on one of the technologies.

As an example, assume that technology d is currently more profitable (and hence more popular) than technology c. A policy-maker, such as a government or industry-regulator, wishes to encourage the adoption of c and may introduce a tax on d or impose some regulatory restriction on its use. We represent this by adding a factor, τ, to the model: $u_{d,t} - u_{c,t} = \lambda_0 + \rho(1 - 2x_t) - \tau(1 - x)$.

As the adoption of c grows, although the taxation decreases (and vice versa) the social reinforcement from the increased adoption will still lead to an increased market share for c.

Technological Progress In the previous sections, the values λ_c and λ_d have been static, meaning that the cost difference between the two technologies remains constant over time. We can model a change in this difference over time by considering how past investment in each of the technologies affects its current profitability. We consider the impact of the cumulative investment on each technology and postulate that such impact follows the time-dependent learning curve stated as follows:

$$\lambda_{c,t} = \lambda_{c0} + \psi_c \left(\sum_{j=1}^{t} x_j \right)^{\zeta_c} \quad \text{and} \quad \lambda_{d,t} = \lambda_{d0} + \psi_d \left(\sum_{j=1}^{t} (1 - x_j) \right)^{\zeta_d} \tag{4}$$

Here, ψ_d and ψ_c are values that determine how effective investment is in making technological progress, and ζ_d and $\zeta_c \in [0, 1]$ determine the shapes of the learning curves for each of the technologies.

Now the difference in profitability depends on time,

$$\lambda_t = \lambda_{d,t} - \lambda_{c,t} = \lambda_0 + \psi_d \left(\sum_{j=1}^{t} (1 - x_j) \right)^{\zeta_d} - \psi_c \left(\sum_{j=1}^{t} x_j \right)^{\zeta_c}, \tag{5}$$

as does the difference in utility, $u_{d,t} - u_{c,t} = \lambda_t + \rho(1 - 2x_t)$, and the share of technology c, $x_t = \frac{1}{1+e^{\beta[\lambda_{t-1}+\rho(1-2x_{t-1})]}} = f_{t-1}(x_{t-1})$.

As an example, in the first, simple model without policy or technological progress, a new technology that starts with little market share is unlikely ever to gain very much. However, if we model the technological change, and the new technology has higher values of ψ and ζ than the existing technology, it can eventually become more profitable over time, acquiring increasing market share as a progressively increasing number of agents adopt it because of increases in their personal profitability.

Switching Costs In the models so far, every agent makes a decision about which technology to use in every time period. In reality, this is not the case because there are costs associated with switching. We can model this by assuming that a proportion, α, of agents do not switch technologies in each time period:

$$f_{\tau,\alpha}(x) = \alpha x + (1 - \alpha) \frac{1}{1 + e^{\beta[\lambda_0 + \rho(1-2x) - \tau(1-x)]}}.$$

The Cryptographic Utility Function Improvement in utility in the basic model is based on a single value, λ, which is the difference in profitabilities between the two technologies. This value, along with social externalities, policy, and technological progress then determines the adoption of the technologies.

We introduce to the model a richer concept of utility so as to be able to express the differences between encryption technologies in greater detail. Instead of a single attribute determining the utility—its profitability, in the basic model—we use a set of different attributes, A (see [5] for this multi-attribute

utility-theoretic [6] set-up in the context of security). Thus, λ becomes the difference between the values, v_a, of the attributes, $a \in A$, for the two technologies c and d: $\lambda = \sum_{a \in A}(v_{a,d} - v_{a,c})$.

We also wish to be able to express policies about each of the different attributes, so we change τ to be a function which describes the policy for each attribute. The difference in utilities is then given by $u_{d,t} - u_{c,t} = \lambda_0 + \rho(1 - 2x_t) + \sum_{a \in A} \tau_a(x)$.

Finally, we describe the development of each attribute individually as investment could affect each of the attributes in different ways. The updated model allowing for technological progress is

$$\lambda_t = \lambda_{d,t} - \lambda_{c,t} = \lambda_0 + \sum_{a \in A} \left[\psi_{a,d} \left(\sum_{j=1}^{t} (1 - x_j) \right)^{\zeta_{a,d}} - \psi_{a,c} \left(\sum_{j=1}^{t} x_j \right)^{\zeta_{a,c}} \right] \quad (6)$$

Attributes for Encryption Technologies We use a set of three attributes that capture the aspects of the technologies that we wish to discuss. These attributes are appropriate to demonstrate the model with the examples we use; other technologies and applications of the model might use different attributes.

First, monetary cost: this is different from the notion of profitability in the basic model, as this (profitability) acts as an aggregate term which includes all of the other attributes; here, we just want to consider how expensive a technology is. Second, usability: there has been a lot of research into the usability of various encryption technologies and how the ease of their use has a large role in determining whether or not people choose to use them. Finally, functionality: this expresses the range of functions that a technology or product covers that benefit the user, not just in terms of encryption. For example, consider two competing products: one has a great number of features that are useful to the user, but offers no encryption, and one that has encryption, but lacks some of the other features. The latter product, although it has increased functionality by offering encryption, may have a lower total functionality.

3 Three Examples

In this section, we briefly introduce three examples of encryption technologies that we use to demonstrate different aspects of the model. Here, we only look at static situations; in Section 4, next, we explore the dynamics of these examples. Models are implemented in the julia language [12].

The models depend critically on choices of values for a number of parameters. Where possible, our choices have been informed by available data; where not, we have estimated sensible values based on our modelling experience and knowledge of the situations. Clearly, further systematic exploration of the parameter spaces and their sensitivity would be valuable.

In each of the examples, a new technology is compared to a default, incumbent technology. The attribute values for the default technology are all 1. The

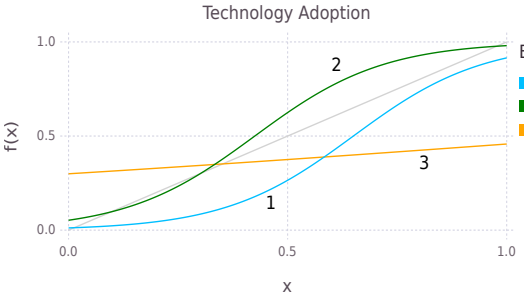

Figure 1. Adoption: all three examples.

	ρ	Cost	Usability	Funct.
Default tech	–	1.0	1.0	1.0
GPG/PGP	1.0	1.0	0.6	1.1
WhatsApp	1.0	1.05	1.0	1.1
SED	0.1	0.85	0.9	1.1

Table 1. Model parameters

values for each example are shown in Table 1. Values above 1 are better than the incumbent technology; values below are worse. We use a value of $\beta = 3.4$ in all examples.

The first two examples look at email encryption, comparing standard email to email encrypted with PGP/GPG [8], and messaging apps, comparing normal SMS messaging to the WhatsApp messenger. Both of these examples have a high social component, ρ: the utility of the technology increases as more people use it, and suffers when there are few other users. This is contrasted with the third example, which compares standard hard drives to self-encrypting drives. Here, ρ is low, as whether or not others are using the technology does not have a large influence on its utility.

Now looking at costs, encryption software is available for free, so we give it the same value as normal email. WhatsApp is potentially less costly than traditional SMS messaging, which can charge for every message sent, well above the equivalent cost of the data [9], and self-encrypting drives are more expensive than normal drives.

Usability for encrypted email is much lower than standard email. As studies have shown [14], it can be quite difficult for people to correctly encrypt their messages; more recently, Edward Snowden described GPG as 'damn near unusable' [11]. We assume that usability for WhatsApp is similar to regular messaging, and that self-encrypting drives, with the overhead of key management, are less usable than standard drives.

Finally, the functionality of all of the new technologies is greater than the incumbents. Encrypted email is encrypted, as are self-encrypting drives, and WhatsApp has additional features such as sending pictures and video messages.

Each of these examples have different equilibria, based on Equation 5, which are shown in Figure 1. For email (1), there is only one equilibrium point, where the share of encrypted email is close to zero. For WhatsApp (2), there are three equilibria: two stable equilibria, one high and one low, and a third, unstable equilibrium at $x \approx 0.3$.

If WhatsApp starts from a small market share, it will grow until it reaches the lower adoption share stable equilibrium. If there is some change or shock—a sudden increase in profitability or usage, for example—that increases its market

share beyond the unstable equilibrium point, then its share will continue to grow until it reaches the higher point and will dominate the market. This is not the case for encrypted email where the low usability means that, although its value increases with the number of people using it, without some 'external impulse' that changes the utility, the level of adoption will always return to the single, low equilibrium point.

Finally, Figure 1 (3) shows the equilibrium of the self-encrypting drive example. There is only one equilibrium (at $x \approx 0.35$) and, because of the low ρ, the value of the technology does not change a great amount based on the level of adoption, which is mainly driven by the characteristics of the technology.

4 Dynamics of the Model and Discussion

So far, the models have been deployed to display the equilibria which can be used for the comparative statics of technology adoption. We proceed by extending the email encryption example to study the evolution of technology adoption over time, in the presence of both exogenous policy influences and endogenous technology changes.

The policy influences take the form of functions that influence the behaviour of agents by changing the value of the utility of the different technologies. Technology changes are modelled within the existing model structure as either changes in the returns on investment over time, or instantaneous shocks to utility-attribute parameters.

We analyse two dynamic aspects of the email encryption example. First, the effect of events such as the Snowden revelations on its use, and, second, how increases in the usability of the encryption software can increase its adoption.

On 5 June 2013, the first of the newspaper articles containing information disclosed by Edward Snowden was published. The documents he released shed light on the expansive electronic surveillance programs being run by the American and British governments. These revelations led to an increased desire to protect the privacy of electronic communications. This can be seen directly in Figure 2, which shows the total number of PGP/GPG keys registered on public keyservers daily over several years [10]. The vertical line indicates the date of the first Snowden article, immediately after which the rate at which keys were added markedly increased.

While this doesn't determine the exact number of people using encrypted email—people can have multiple keys, some keys may be abandoned, etc.—it clearly demonstrates that the revelations had an impact. We can model this as a revelation of government policy: it adds additional costs to using regular email. We can implement this as a function for the functionality attribute $\tau_{functionality}(x) = -0.2$, which returns a constant value, rather than being dependent on the share of adoption: insecure email is less useful, no matter how many people are using it.

Figure 3 shows the effects of the policy compared to the previous case without such policy (essentially, $\tau_{functionality}(x) = 0$). There are now two stable equilib-

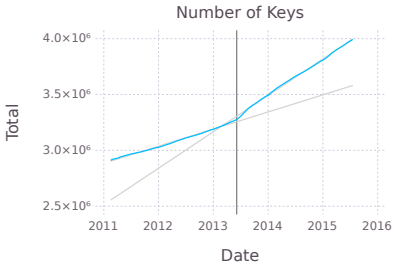

Figure 2. Daily number of PGP keys on keyservers. The vertical line indicates the first Snowden news article.

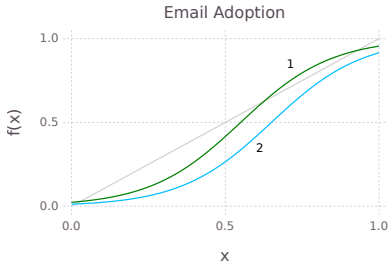

Figure 3. Email adoption (1) with and (2) without government surveillance policy.

ria, instead of just one. Unlike before, if, somehow, there was now a sudden large increase in encrypted email use—to over 62 percent adoption, the location of the unstable equilibrium—the system would change to the higher stable equilibrium and encrypted email use would be dominant. However, a sudden increase of such size is not likely, and the probable result is that the system stays at the lower equilibrium, which has shifted slightly higher (from $x \approx 0.013$ to $x \approx 0.028$), showing a small increase in the adoption of encrypted email.

These developments are assuming that there is no innovation around encrypted email and the technology and user experience stay constant. In reality, the usability of encryption software is being improved. For example, Google and Yahoo are working on a web browser plugin that provides end-to-end encryption for their respective webmail services [4,13]. This plugin also manages key distribution, aiming to make things easier for users than PGP/GPG's Web of Trust model. Other services, such as Keybase [7], which uses social network identities as a means of verifying the identity of a key's owner, are also attempting to improve key distribution. How much efforts such as these will increase the use of email encryption largely depends on how much they improve usability.

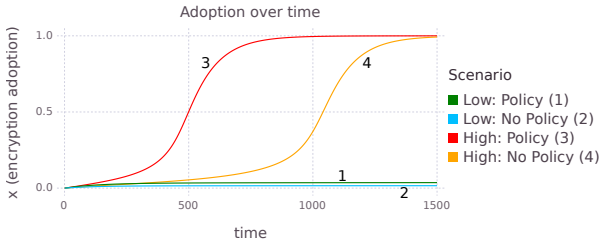

Figure 4. Email adoption over time

We can use the technological progress model to look at how investment in improving usability will affect adoption. Figure 4 shows the adoption over time for four different scenarios. The first two have a low rate of return for invest-

ment in usability, one with the government policy and one without ($\psi_{usability,c} = 0.05, \zeta_{usability,c} = 0.1$). The second two have a very high rate of return on investment, again with and without policy ($\psi_{usability,c} = 0.2, \zeta_{usability,c} = 0.3$). In all cases, the values for non-encryption are the same: $\psi_{usability,d} = 0.01, \zeta_{usability,d} = 0.01$. We use $\alpha = 0.99$ for the switching rate.

In the high-return cases, the investment causes the system to switch to an equilibrium with high adoption of email encryption. The transition happens much sooner with the government policy than without. In both of the low-return cases, encryption never gets a large market share.

References

1. W.B. Arthur. Competing Technologies, Increasing Returns, and Lock-In by Historical Events. *The Economic Journal* 99(394):116–131, 1989.
2. T. August and T. Tunca. Network Software Security and User Incentives. *Management Science* 52(11):1703–1720, 2006.
3. W.A. Brock and S.N. Durlauf. Discrete Choice with Social Interactions. *The Review of Economic Studies*, 68(2):235–260, 2001.
4. *Google Online Security Blog: Making End-to-End Encryption Easier to Use.* 2014. `http://googleonlinesecurity.blogspot.co.uk/2014/06/making-end-to-end-encryption-easier-to.html` (visited 20/09/2015).
5. C. Ioannidis and D. Pym and J. Williams. Investments and Trade-offs in the Economics of Information Security. In: *Proc. Financial Cryptography and Data Security '09* (R. Dingledine and P. Golle, editors). LNCS 5628:148–166, 2009.
6. R.L. Keeney and H. Raiffa. *Decisions with Multiple Objectives: Preferences and Value Trade-offs.* Wiley, 1976.
7. *Keybase.* 2015. `https://keybase.io/` (visited 20/09/2015).
8. *OpenPGP.org.* 2015. `http://www.openpgp.org` (visited 30/09/2015).
9. R. Shambare. The Adoption of Whatsapp: Breaking the Vicious Cycle of Technological Poverty in South Africa. *J. Econ. Behav. Stud.* 6(7):542–550, 2014.
10. *SKS Keyservers: History of Number of OpenPGP Keys.* 2015. `https://sks-keyservers.net/status/key_development.php` (visited 30/09/2015).
11. *The Guardian: Snowden Implores Hackers to Focus on Protecting Users' Rights.* 2014. `http://www.theguardian.com/technology/2014/jul/21/edward-snowden-hackers-encryption-patriot` (visited 07/10/2015).
12. The julia language. 2015. `http://julialang.org/` (visited 30/09/2015).
13. *User-Focused Security: End-to-End Encryption Extension for Yahoo Mail.* 2015. `http://yahoo.tumblr.com/post/113708033335/user-focused-security-end-to-end-encryption` (visited 30/09/2015).
14. A. Whitten and J.D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proc. 8th Conference on USENIX Security Symposium — Volume 8*, SSYM '99, pp. 14–14, Berkeley, CA, USA, 1999. USENIX Association.
15. A. Ozment and S.E. Schechter. Bootstrapping the Adoption of Internet Security Protocols In *WEIS 2006*: `http://www.econinfosec.org/archive/weis2006/docs/46.pdf` (visited 02/01/2016).
16. N. Rosasco and D. Larochelle. How and Why More Secure Technologies Succeed in Legacy Markets: Lessons from the Success of SSH. In *Economics of Information Security* (L. Jean Camp and Stephen Lewis, editors). Kluwer, 2004. pp. 247–254.