An optimist's Poisson model of cryptanalysis

Daniel R. L. Brown[*]

December 18, 2019

Abstract

Simplistic assumptions, modeling attack discovery by a Poisson point process, lead to quantifiable statistical estimates for security assurances, supporting the wisdom that more independent effort spent on cryptanalysis leads to better security assurance, but hinting security assurance also relies significantly upon general optimism.

The estimates also suggest somewhat better security assurance from compounding two independent cryptosystems, but perhaps not enough to outweigh the extra cost.

1 Poisson model of cryptanalysis

Assume that there exists at most one practical attack on a target cryptosystem, and that the practical attack can be implemented only upon discovery of a single point-of-weakness in the cryptosystem.

Assume that t measures the independent time (or other cost) spent on cryptanalysis of a cryptosystem, with independence in the sense that the probability of discovering the single point-of-weakness in any portion t' of t depends only the size t' of the portion, with disjoint portions have independent probabilities.

These two assumptions suggest the well-known Poisson point process, implying a constant a exists such that the probability of finding no practical attack in time t is:

$$p = e^{-at}. \tag{1}$$

[*] `danibrown@blackberry.com`

Call a the **attackability** of the cryptosystem. Attackability can range from 0 to ∞. If the attack does not exist, then $a = 0$. Otherwise, attackability quantifies how easy is it to discover the single point of weakness. Well-known properties of the Poisson point process imply $1/a$ is the expected (average) time needed to discover the attack.

2 Inference by optimism

Suppose that no practical attack on the target cryptosystem has been observed after spending time t on cryptanalysis. What does this say about attackability?

Assume a general **optimism** level o, such as $o = 0.05$, meaning to assume that

$$p \geq o. \tag{2}$$

A small o means that we recognize that our observation (no attack) was perhaps only due to bad luck, a fluke, a probability as low as o. (Statistical terms related to optimism are **confidence** and **significance**, but optimism seems more appropriate here.)

Substituting equation (1) for p in bound (2) bounds attackability by

$$a \leq -\frac{\log o}{t}. \tag{3}$$

To repeat, the inference relies on three major assumptions: the Poisson model of cryptanalysis, the estimate of t, and the optimism o.

3 Adversarial cryptanalysis

If an adversary has capability to spend time T (instead of t) on cryptanalysis of the target cryptosystem, then the Poisson model says that probability the adversary fails to find an attack is

$$P = e^{-aT}. \tag{4}$$

In other words, P is the probability that the cryptosystem remains **secure** against the adversary of capability T.

Substituting the inference (3) into equation (4) bounds security by

$$P \geq o^{T/t}. \tag{5}$$

The value $o^{T/t}$ is a **security assurance**, meaning a lower bound on the probability of being secure.

For example, with fairly high optimism $o = 0.1$, we get security assurance of approximately 99.5% against a rather weak adversary of capability $T = t/1000$. This still admits a fairly high one-in-two-hundred risk of an attack.

An adversary aiming to secretly exploit an attack might be hampered by the needing to keep its cryptanalytic effort secret, for example, by reducing the number of independent researchers available to contribute to T. This offers a faint hope that $T \ll t$.

Meanwhile, as time passes, we might somehow deduce or estimate that the adversary has already spent T on cryptanalysis, and also failed to find a weakness. In this case, we may opt to replace t by $t + T$, and then re-assess the adversary's remaining capability to a new, possibly smaller value of T. This may increase security assurance.

Very recently, my estimated security assurance for elliptic curve cryptography, would have been at least $1 - 2^{-40}$, but this is not justifiable in the optimistic Poisson model. For example, at $o = 0.05$ it requires $T/t < 10^{-11}$, which seems low: one new researcher could be regarded as capable of independent cryptanalysis for two years, suggesting $T > \frac{1}{1000} \times \frac{2}{34}$. Perhaps, underlying my intuitive hunch was a more complicated model (including provable security and some inferences that the independent thought measured by t has reached its limits), a confusing of relative and absolute risk, or just plain old confirmation bias.

4 Compound cryptosystems

Assume that two cryptosystems are independent in the sense that probabilities about one system are independent of the other, per the usual meaning of independence in probability theory.

Assume that a compound of two component cryptosystems means that as long as either component of the compound is secure, then the compound is secure. (Compounding is also known as defense-in-depth, strongest-link, composite, or even hybrid.)

The security assurance of the compound of the two independent cryptosystems is a lower bound on the probability that neither component is insecure:

$$1 - (1 - o^{T_1/t_2})(1 - o^{T_2/t_2}) = o^{T_1/t_1} + o^{T_2/t_2} - o^{T_1/t_2+T_2/t_2}, \tag{6}$$

if no attacks were observed on either single cryptosystem after spending time t_i on cryptosystem i, and deeming the adversary as capable of spending time T_i on cryptosystem i.

Suppose that the adversary is constrained by $T_1+T_2=T$. The adversary can minimize the security assurance by setting $T_i = t_i(T/t)$ where $t=t_1+t_2$, giving a security assurance of:

$$1-(1-o^{T/t})^2 = o^{T/t}(2-o^{T/t}). \tag{7}$$

The final security assurance does not depend on t_1 and t_2, perhaps surprisingly.

Possibly, a simpler derivation of compound cryptosystem security assurance uses a Poisson model with two points of weakness.

An upside of the compound is that it might have twice the security assurance of a single cryptosystem (given the same t and T values), for example jumping from 0.1 to 0.19. A downside of the compound is that it might take twice the program code, run-time, and data traffic, of a single cryptosystem.

When security assurance s is close to one, it makes sense to study the upper risk $r=1-s$ of attack. If the damage caused by a practical attack can be quantified as D, then the expectation of damage is at most rD. A compound of two independent cryptosystems can have risk r^2, which could greatly reduce the expectation of damage if r is small. Unfortunately, in the optimistic Poisson model for cryptanalysis, we usually cannot infer a small enough r to make this argument compelling for a compound cryptosystem.

5 Consistency, impact, and improvement

The common and obvious wisdom of subjecting a cryptosystem to as much independent cryptanalysis (a large t) as possible is consistent with this simplistic model. Profound skepticism of the model is advised nonetheless.

General optimism still figures prominently into the estimates, which is perhaps humbling if a large effort was spent on cryptanalysis. Security assurances are perhaps disappointingly low, although arguably high enough to justify cryptosystems over doing nothing, on a relative risk basis.

Sophisticated models, such as multiple point-of-weakness attack discovery (in a Poisson point process) and formal statistical estimates for t and T, might produce more realistic results, higher security assurances, and different comparisons between compound and single systems.