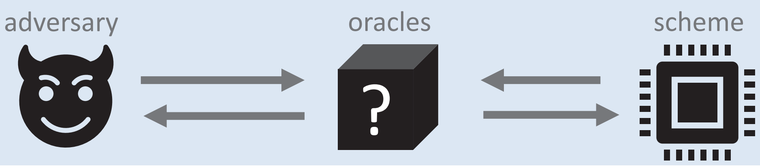
NEW SPAKE FORMALISMS AND SECURITY PROOFS IN THE BELLARE-ROGAWAY GAME-PLAYING MODEL

Security Game

The Bellare-Rogaway Game-Playing Model

Attacks are modelled by an adversary playing a *game* with the user running scheme

- ✓ can state adversary and its advantage precisely
- ✓ allows proving of security bounds of the scheme



PAKE

Password-Authenticated Key Exchange

is a family of schemes to get a **strong** session key (high-entropy) from a **weak** shared password (low-entropy).

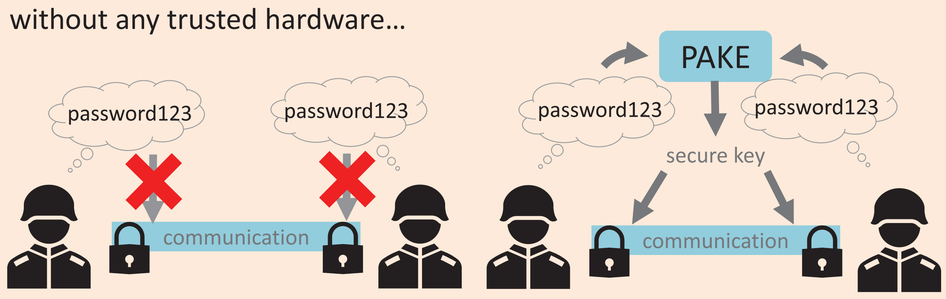
SPAKE1 is a secure and efficient PAKE scheme introduced by Abdalla and Pointcheval in 2005.

SPAKE? Is a strawman scheme introduced in the same paper.

Motivation

Why study PAKEs?

Suppose two officers wanted to communicate over the public internet without any trusted hardware…



Using the password directly as the key makes **offline brute-forcing** possible…
We have to use PAKE scheme to generate a **secure session key**!

Contributions

Two main contributions

1. Described SPAKE? and SPAKE1 in the **concrete** model (vs semi-asymptotic), allowing easier comparison with other schemes due to **more precise bounds**
2. Gave a **mathematical proof** of SPAKE?'s insecurity (by constructing an adversary and measuring its advantage)

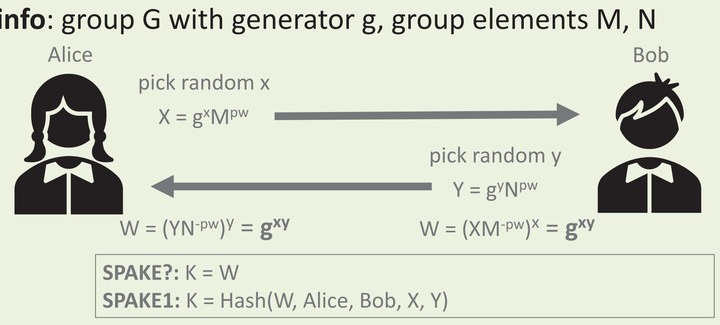
additional probability of winning the game, discounting random guessing

parameterises **all** adversarial resources, including all computational power, oracle queries, etc.

SPAKE? and SPAKE1

Two similar schemes

Private info: pw, x, y
Public info: group G with generator g, group elements M, N



SPAKE?: K = W
SPAKE1: K = Hash(W, Alice, Bob, X, Y)

While the difference between them is small, one is secure while the other is not! Here is the security *lower-bound* for SPAKE?:

$$\boldsymbol{Adv}^{\text{pake}}_{\text{SPAKE ?,freq },N}(\mathcal{A}) \geq (1-|\mathbb{G}|^{-1}) \prod_{i=0}^{q+1} \text{freq}\big(\text{rank}(\text{freq},i)\big)$$

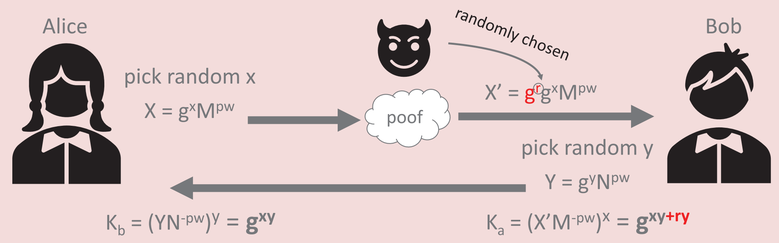
And here is an *upper-bound* for SPAKE1:

$$\boldsymbol{Adv}^{\text{pake}}_{\text{SPAKE1 ,freq },N}(\mathcal{A}) \leq 2\left(\frac{q_{\text{send}}}{2^L} + \left(2^{14-2L}\boldsymbol{Adv}^{\text{cdh}}_{\mathbb{G}}(\mathcal{B}) + \frac{2^{15}q_H^4}{2^{2L}|\mathbb{G}|}\right)^{\frac{1}{6}}\right) + 2\left(\frac{(q_{\text{exe}}+q_{\text{send}})^2}{2|\mathbb{G}|} + q_H\boldsymbol{Adv}^{\text{cdh}}_{\mathbb{G}}(\mathcal{C})\right)$$

SPAKE? attack!

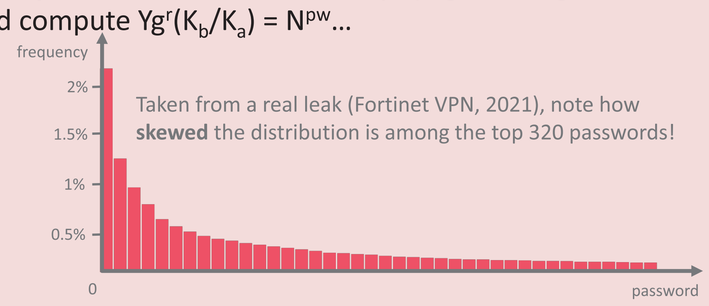
A concrete adversary

Here, our adversary is a man-in-the-middle, intercepting and modifying messages, and (as per the security model) distinguishing a session key.



Now our adversary can **compromise** the two session keys (e.g. hacking Alice and Bob's computers) and compute $Yg^r(K_b/K_a) = N^{pw}$…

…and now it can just try all possible values of pw (starting with the most common one); if it succeeds in finding pw, it can impersonate Bob!



To formally give the advantage of this adversary, we had to create a new game for the above password-guessing situation, and a minimal adversary, whose advantage is as follows:

$$\boldsymbol{Adv}^{\text{dlp}-\text{dict}}_{\mathbb{G},\text{freq },N}(\mathcal{A}) = \prod_{i=0}^{q+1} \text{freq}\big(\text{rank}(\text{freq},i)\big)$$

Conclusion

Impact, takeaways, and future work

PAKE researchers can benefit from the more **precise** measure of insecurity for SPAKE? and the more **practical** bound given for SPAKE1 for future development of other PAKE schemes, and app/website builders looking to select a PAKE scheme to use to secure their communications can now better **evaluate** and **compare** the security of competing PAKE schemes.

Future work could explore the proof for SPAKE1 and a full security analysis of SPAKE2 (another scheme presented in the original paper), and then compare the practical usages of SPAKE1 and SPAKE2.

References

Michel Abdalla and David Pointcheval. "Simple Password-Based Encrypted Key Exchange Protocols". San Francisco, CA, USA: Springer Heidelberg, Germany, 2005.
Mihir Bellare, David Pointcheval, and Phillip Rogaway. "Authenticated Key Exchange Secure Against Dictionary Attacks." Cryptology ePrint Archive, 2000.

Apart from the above authors whose work has been invaluable to our research, we would also like to thank our mentor Dr Ruth Ng for her unwavering support for our project, and many others like Dr Sim Siang Meng and Choo Jia Guang who have helped us along the way.

Members:
Tricia Chia Kee Ann, Raffles Institution
Yeo Jie Xuan Isaac, Raffles Institution
Mentor:
Dr Ruth Ng Ii-Yung, DSO National Laboratories

YDSP Young Defence Scientists Programme
DSTA Defence Science & Technology Agency
DSO NATIONAL LABORATORIES