Group Theoretic Cryptography: The Algebraic Eraser

Lindsey Cioffi, Dr. Jonathan Katz, Jiahui Liu, Elijah Soria

University of Maryland-College Park, Combinatorics and Algorithms for Real Problems REU

INTRODUCTION

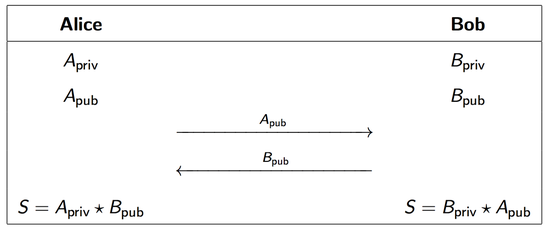
Algebraic Eraser(AE) is a function based on non-commutative group theory published in 2007, used for Diffie-Hellman key exchange protocol and designed for device with limited computing power. In 2015 and 2016 there were mainly two attacks on AE published. The Ben-Zvi, Blackburn and Tsaban Attack recovers the shared secret from a generalized version of AE key exchange protocol; the Blackburn and Robshaw Attack targets only the RFID setting with standardized parameters provided by Secure RF. But after adding a hash function to the protocol, the latter attack is not efficient anymore. In June 2016 SecureRF published a hash function based on a modified version of AE function. We've shown that the function is malleable under some input. We are still working on an attack of the AE hash function. We also explored using randomized method to solve the "Conjugacy Search Problem", a hard math problem Algebraic Eraser's security is partly based on.

OBJECTIVES

- Study the Algebraic Eraser Protocol and the attacks made against it:
  1. Find weaknesses that attacks may be able to exploit
  2. Build on previous attacks to strengthen and improve efficiency
- Explore the AE Hash function that emerges from the protocol
- Look into algorithms on the underlying problem AE 's security is partly based on: Multiple Conjugacy Search problem

PUBLIC-KEY CRYPTOGRAPHY: DIFFIE-HELLMAN APPROACH

Alice and Bob want to have a shared secret key that only they two can know so they can communicate over an insecure channel. But they don't have to meet in person to discuss this shared secret:



Most important: design this star operation such that Alice and Bob can get the same shared secret.

Classical Diffie–Hellman protocol builds on hard math problems such as the discrete logarithm problem.

Algebraic Eraser provides a new way to realize this communication.

AIGEBRAIC ERASER FUNCTION

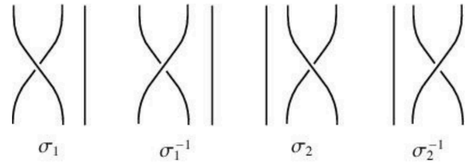
- Utilizes braid groups, matrices, and group actions to manipulate and disguise the private keys
- A **braid** is represented as a matrix, permutation pair
- **Group actions** are specifically defined operations that are performed on group elements

Braid Group:

The elements of the braid group B_n are n-stranded braids. We multiply braids by concatenation. The braid group has a presentation

$$\langle \sigma_1, ..., \sigma_{n-1} \mid \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1},\ \sigma_i\sigma_j = \sigma_j\sigma_i \rangle,$$

where $i = 1, ..., n-2$ and $j = 1, ..., n-1$, $|i-j| > 1$.



- Operation $\circ : (m_1, \sigma_1) \circ (m_2, \sigma_2) = (m_1^{\sigma_1} m_2, \sigma_1\sigma_2)$
- ${}^{\sigma_1}m_2$ is the action of σ_1 on m_2 in which the indeterminates $t_1, \ldots, t_n$ are permuted according to σ_1
- AE function $* : (n, \sigma_1) * (m, \sigma_2) = (n\varphi({}^{\sigma_1}m), \sigma_1\sigma_2)$

The braid group elements are represented as a pair of matrix and a permutation. By the Algebraic Eraser function, the information of the secret matrix is hidden by the permutation and evaluation process. (That's why it's called "eraser".)

Most parameters used by Alice and Bob will be provided by a Trusted Third Party(TTP).

ATTACKS on AE

Ben-Zvi, Blackburn, and Tsaban Attack (2015)

- Assumes all public parameters are known to the attacker.
- Using public parameters, generates a product of elements that is equal to Alice's public key.
- Uses Alice's (imitated) public key, Attacker calculates the shared secret between Alice and Bob.
- Attacks a stronger, more general version of the Algebraic Eraser

Blackburn and Robshaw Attack (2016)

- Attacker challenges the tag multiple times.
- Uses structure of the protocol to recover private keys.
- Attack assumes structure that was proposed for standardization.
- Attack assumes that the Shared Secret can be accessed through enough interrogations.
- Refuted attack by modifying protocol to make shared secret more secure.

AE HASH FUNCTION

A modified version of the Algebraic Eraser has been proposed for use in a hash function.

The modified operation $*'$ permutes both the indeterminates t and the t-value set.

$$\begin{array}{lcccccc} t: & t_1 & t_2 & t_3 & t_4 & & \\ & \downarrow & \downarrow & \downarrow & \downarrow & \Longrightarrow & \\ T: & 10 & 4 & 6 & 2 & & \end{array} \qquad \begin{array}{lcccc} t: & t_1 & t_2 & t_3 & t_4 \\ & \downarrow & \downarrow & \downarrow & \downarrow \\ {}^{\sigma}T: & 6 & 4 & 10 & 2 \end{array}.$$

Now, for $i \in \{1, 2, \ldots, n-1\}$, let $s_i = (i\ \ i+1) \in S_n$ be the transposition of elements i and $i+1$. (Elements of S_n can be represented either as a product of transpositions or in cyclic notation, as these are polynomially equivalent.) Let $(n_0, s_{i_0}) \in \mathrm{GL}_n(\mathbb{F}_q) \times S_n$, and let $(x_{i_1}^{\epsilon_1}, s_{i_1}), (x_{i_2}^{\epsilon_2}, s_{i_2}), \ldots, (x_{i_k}^{\epsilon_k}, s_{i_k}) \in \mathrm{GL}_n(\mathbb{F}_q[t]), S_n$ where each $x_{i_j}^{\epsilon_j}$ are matrices of the form found in equations 1.1, 1.2, 1.3, or 1.4. The operation $\star'$ is defined as

$$\begin{aligned}(n_0, s_{i_0}) \star' (x_{i_1}^{\epsilon_1}, s_{i_1}) \star' (x_{i_2}^{\epsilon_2}, s_{i_2}) \star' \cdots \star' (x_{i_k}^{\epsilon_k}, s_{i_k}) \\ = \left(n_0 \cdot {}^{s_{i_0}} x_{i_1}^{\epsilon_1} \downarrow_{T_1} \cdot {}^{s_{i_0}s_{i_1}} x_{i_2}^{\epsilon_2} \downarrow_{T_2} \cdots {}^{s_{i_0}s_{i_1}s_{i_2}\cdots s_{i_{k-1}}} x_{i_k}^{\epsilon_k} \downarrow_{T_k}, s_{i_0}s_{i_1}s_{i_2}\cdots s_{i_{k-1}}s_{i_k}\right)\end{aligned}$$

Where $T_1 = \{\tau_1, \tau_2, \ldots, \tau_n\} \subset \mathbb{F}_q$ is our original t-values, and

$$\begin{aligned} T_2 &= {}^{s_{i_0}s_{i_1}}T_1 \\ T_3 &= {}^{s_{i_0}s_{i_1}s_{i_2}}T_1 \\ &\vdots \\ T_k &= {}^{s_{i_0}s_{i_1}s_{i_2}\cdots s_{i_{k-1}}}T_1. \end{aligned}$$

The basic idea of Algebraic Eraser hash is dividing the input message, a string S into blocks:

$$S = \bigcup_{i=1}^{D_S} \mathrm{Block}(i)$$

Each block is then represented in binary. And compute each block using the AE hash *' operation together with an initial ordered pair :

$$(n_0, \sigma_0) \star' (c_{v(1)}, \sigma_{v(1)}) \star' (c_{v(2)}, \sigma_{v(2)}) \star' \cdots \star' (c_{v(D_S)}, \sigma_{v(D_S)})$$

CONJUGACY SEARCH PROBLEM

The security of the Algebraic Eraser is partly based on the hardness of the *generalized simultaneous conjugacy search problem:*

G is a group, given $y_1, y_2, ..., y_n \in G$ and $x_1, x_2, ..., x_n \in G$, find z such that $y_i = zx_iz^{-1}$ for all i.

Attacks on Conjugacy Search Problem

- Length-Based Attacks: compare ``lengths" of group elements in a braid group Bn using:
  1. Garside Normal Length function
  2. Dehornoy's word shortening algorithm
- Recursively reduce the lengths of group elements through generator relations (very hard for groups with complicated relations)
- Idea: reduce the elements heuristically; combine two methods to formulate a cost function

RESULTS, CONCLUSION, FUTURE WORK

- Showed that the attack on the AE protocol proposed for standardizaton after the modifications are in place was not feasible.
- Combined randomized algorithms with Length-based Attack on the Multiple Conjugacy Search problem :
  1. Simulated Annealing
  2. Genetic Algorithms
- Proved relations about the modified Algebraic Eraser that decrease the security of the hash
- Showed that the hash function is malleable for certain inputs: given hash outputs h(x) and h(y), we can calculate h(x||y) using h(x) and h(y) alone.

The Algebraic Eraser is quick and simple enough for low powered devices. But based on current analysis it does not provide enough security.

For future research:

- Attack on Algebraic Eraser hash function
- Fix the key exchange protocol to defeat the BBT attack
- Modify the Ben-Zvi et al. attack to derive more than just the shared secret, e.g. recovering full private keys.

REFERENCES

[1] I. Anshel, M. Anshel, D. Goldfeld, and S. Lemieux, Key agreement, the algebraic erasertm, and lightweight cryptography, Contemporary Mathematics 418 (2007), 1–34.

[2] D. Atkins and D. Goldfeld, Addressing the algebraic eraser diffie–hellman over-the-air protocol.

[3] A. Ben-Zvi, S. R. Blackburn, and B. Tsaban, A practical cryptanalysis of the algebraic eraser, 2015. http://eprint.iacr.org/.

[4] S. R Blackburn and M. Robshaw, On the security of the algebraic eraser tag authentication protocol, International conference on applied cryptography and network security, 2016, pp. 3–17.

[5] S. R. Corporation, Algebraic eraser ota authentication (2016), 1–60.

[6] J. L. J. K. Elijah Soria Lindsey Cioffi, On the algebraic eraser and the ben-zvi, blackburn, and tsaban attack (2016).

[7] A. Kalka, M. Teicher, and B. Tsaban, Short expressions of permutations as products and cryptanalysis of the algebraic eraser, Advances in Applied Mathematics 49 (2012), no. 1, 57–76.

[8] C. Kassel, O. Dodane, and V. Turaev, Braid groups, Graduate Texts in Mathematics, Springer New York, 2008.

ACKNOWLEDGEMENTS

This research was part of the 2016 Combinatorics and Algorithms for Real Problems REU program at University of Maryland College Park.

NSF

UNIVERSITY OF MARYLAND

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK